ETSI draft SR 000 000 V0.0.2 (2011-08)

Special Report

Rationalised Framework for Electronic Signature Standardisation Annex C - Inventory

Reference
DSR/ESI-000099

Keywords
e-commerce, electronic signature, security

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Important notice

Individual copies of the present document can be downloaded from:
http://www.etsC.2.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsC.2.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsC.2.org/chaircor/ETSI_support.asp

Copyright Notification

No part may be reproduced except as authorized by written permissioC.4.
The copyright and the foregoing restriction extend to reproduction in all media.

© European Telecommunications Standards Institute 2011
© Comité Européen de Normalisation Electrotechnique 2011.
All rights reserved.

DECT™, **PLUGTESTS**™, **UMTS**™ and the ETSI logo are Trade Marks of ETSI registered for the benefit of its Members.
3GPP™ and **LTE**™ are Trade Marks of ETSI registered for the benefit of its Members and
of the 3GPP Organizational Partners.
GSM® and the GSM logo are Trade Marks registered and owned by the GSM Association.

Contents

Contents 3

Annex C Inventory 13

C.1 Introduction 13
C.1.1 Aim 13
C.1.2 Organisation of Data 13
C.1.3 Source Bodies 14

C.2 International 17

C.2.1: Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems based on the Conformity Assessment standard ISO/IEC 17021 17

C.2.2: Conformity assessment — Requirements for bodies providing audit and certification of management systems 18

C.2.3: Conformity assessment — Requirements for bodies certifying products, processes and services 19

C.2.5: Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms 20

C.2.6: Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms 21

C.2.7: Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher 22

C.2.8: Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function 24

C.2.9: Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 3: Mechanisms using a universal hash-fun 25

C.2.10: Information technology -- Security techniques -- Entity authentication -- Part 1: General 26

C.2.11: Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms 27

C.2.12: Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques 28

C.2.13: Information technology -- Security techniques -- Modes of operation for an n-bit block cipher 29

C.2.14: Information technology -- Security techniques -- Hash-functions -- Part 1: General 30

C.2.15: Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher 31

C.2.16: Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions 32

C.2.17: Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functions using modular arithmetic 33

C.2.18: Information technology -- Trusted Platform Module -- Part 1: Overview 34

C.2.19: Information technology -- Trusted Platform Module -- Part 2: Design principles 35

C.2.20: Information technology -- Trusted Platform Module -- Part 3: Structures 36

C.2.21: Information technology -- Trusted Platform Module -- Part 4: Commands 37

C.2.22: Information technology -- Security techniques -- Non-repudiation -- Part 1: General 38

C.2.23: Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques 39

C.2.24: Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General 40

C.2.25: Information technology -- Security techniques -- Digital signatures with appendix -- Part 2: Integer factorization based mechanisms....41

C.2.26: Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms 42

C.2.27: Elliptic Curve Russian Digital Signature Algorithm, Schnorr Digital Signature Algorithm, Elliptic Curve Schnorr Digital Signature Algorithm, and Elliptic Curve Full Schnorr Digital Signature Algorithm....43

C.2.28: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model....44

C.2.29: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components 45

C.2.30: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components....46

C.2.31: Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework....47

C.2.32: Information technology -- Security techniques -- A framework for IT security assurance -- Part 2: Assurance methods....48

C.2.33: Information technology -- Security techniques -- A framework for IT security assurance -- Part 3: Analysis of assurance methods 49

C.2.34: Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets....50

C.2.35: Information technology -- Security techniques -- Specification of TTP services to support the application of digital signatures 51

C.2.36: Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General....52

C.2.37: Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 5: Elliptic curve generation....53

C.2.38: Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework 54

C.2.39: Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens....55

C.2.40: Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens 56

C.2.41: Information technology -- Security techniques -- Random bit generation 57

C.2.42: Information technology -- Security techniques -- Prime number generation 58

C.2.43: Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers 59

C.2.44: Information technology -- Security techniques -- Security requirements for cryptographic modules 60

C.2.45: Information technology -- Security techniques -- Anonymous digital signatures 61

C.2.46: Information technology -- Security techniques -- Anonymous digital signature -- Part 2: Mechanisms using a group public key 62

C.2.47: Information technology -- Security techniques -- Anonymous entity authentication -- Part 2: Mechanisms based on anonymous digital signature schemes 63

C.2.48: Information technology -- Security techniques -- Test requirements for cryptographic modules 64

C.2.49: Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary 65

C.2.50: Information technology -- Security techniques -- Information security management systems -- Requirements 66

C.2.51: Information technology -- Security techniques -- Code of practice for information security management 67

C.2.52: Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems 68

C.2.53: Information technology - Security techniques - 69

C.2.54: Information technology - Security techniques - 70

C.2.55: Information technology -- Business Operational View -- Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints 71

C.2.56: Information technology -- Procedures for achieving metadata registry content consistency -- Part 1: Data elements 72

C.2.57: Information technology -- Procedures for achieving metadata registry content consistency -- Part 3: Value domains 73

C.2.58: Information technology -- Biometric data interchange formats -- Part 7: Signature/sign time series data 74

C.2.59: Information technology -- Biometric performance testing and reporting -- Part 7: Testing of on-card biometric comparison algorithms 75

C.2.60: Information technology -- Web Services Interoperability -- WS-I Basic Profile Version 1.1 76

C.2.61: Information technology -- Web Services Interoperability -- WS-I Attachments Profile Version 1.0 77

C.2.62: Information technology -- Web Services Interoperability -- WS-I Simple SOAP Binding Profile Version 1.0 78

C.2.63: Identification cards -- Machine readable travel documents -- Part 1: Machine readable passport 79

C.2.64: Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application 80

C.2.65: Information technology -- Personal identification -- ISO-compliant driving licence -- Part 3: Access control, authentication and integrity validation 81

C.2.66: Information and documentation -- Records management processes -- Metadata for records -- Part 1: Principles 82

C.2.67: Information and documentation -- Managing metadata for records -- Part 2: Conceptual and implementation issues 83

C.2.68: Document management -- Portable document format -- Part 1: PDF 1.7 84

C.2.69: Document management -- Engineering document format using PDF -- Part 1: Use of PDF 1.6 (PDF/E-1) 85

C.2.70: Information technology – Security techniques – Specification of TTP services to support the application of digital signatures 86

C.2.71: Information Technology - Security techniques - Guidelines for the use of Trusted Third Party services 87

C.2.72: 88

C.2.73: Information technology -- Security techniques -- Entity authentication assurance framework.....89
C.2.74: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP 90
C.2.75: Internet X.509 Public Key Infrastructure 91
C.2.76: Diffie-Hellman Proof-of-Possession Algorithms 92
C.2.77: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP).....93
C.2.78: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile 94
C.2.79: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework 95
C.2.80: Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates 96
C.2.81: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile 97
C.2.82: Internet X.509 Public Key Infrastructure Permanent Identifier.....98
C.2.83: Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP) 99
C.2.84: Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF).....100
C.2.85: Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP.....101
C.2.86: Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates 102
C.2.87: The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments 103
C.2.88: Server-Based Certificate Validation Protocol (SCVP) 104
C.2.89: Certificate Management over CMS (CMC).....105
C.2.90: Certificate Management over CMS (CMC): Transport Protocols.....106
C.2.91: Certificate Management Messages over CMS (CMC): Compliance Requirements.....107
C.2.92: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.....108
C.2.93: Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA.....109
C.2.94: ESSCertIDv2 Update for RFC 3161.....110
C.2.95: Trust Anchor Format 111
C.2.96: Trust Anchor Management Protocol (TAMP).....112
C.2.97: Internet X.509 Public Key Infrastructure -- Certificate Image 113
C.2.98: CMS Advanced Electronic Signatures (CAdES).....114
C.2.99: Cryptographic Message Syntax (CMS) 115
C.2.100: Digital Signature Services v1.0, DSS Core Protocols, Elements, and Bindings v1.0 116
C.2.101: German Signature Law Profile of the OASIS Digital Signature Service, version 1.0.....117
C.2.102: Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 1.0 118
C.2.103: Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services Version 1.0.....119
C.2.104: J2ME Code-Signing Profile of the OASIS Digital Signature Services 120
C.2.105: Abstract Code-Signing Profile of the OASIS Digital Signature Services 121

C.2.106: Electronic PostMark (EPM) Profile of the OASIS Digital Signature Service Version 1.0 122
C.2.107: Entity Seal Profile of the OASIS Digital Signature Service 123
C.2.108: Signature Gateway Profile of the OASIS Digital Signature Service Version 1.0 124
C.2.109: XML Timestamping Profile of the OASIS Digital Signature Services Version 1.0 125
C.2.110: Security Assertion Markup Languague (SAML) V2.0 126
C.2.111: Web Services Security: SOAP Message Security 1.0 (WS-Security 2004) 127
C.2.112: WS-Security Policy 1.2 128
C.2.113: WS-Trust 1.4 129
C.2.114: WS-Secure Conversation 1.4 130
C.2.115: XML Signature Syntax and Processing (Second Edition) 131
C.2.116: Canonical XML Version 1.0 132
C.2.117: Exclusive XML Canonicalization Version 1.0 133
C.2.118: Canonical XML Version 1.1 134
C.2.119: XML-Signature Xpath Filter 2.0 135
C.2.120: XML Path Language (Xpath) Version 1.0 136
C.2.121: XSL Transformations (XSLT) Version 1.0 137
C.2.122: Decryption Transform for XML Signature 138
C.2.123: Visible Signature Profile of the OASIS Digital Signature Services Version 1.0 139
C.2.124: OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0 ..140
C.2.125: Signature Policy Profile of the OASIS Digital Signature Services Version 1.0 141
C.2.126: Information technology — Long term signature profiles — 142
C.2.127: Information technology — Long term signature profiles — 143
C.2.128: XML Signature Syntax and Processing Version 1.1 144
C.2.129: XML Signature Properties 145
C.2.130: XML Security 1.1 Requirements and Design Considerations 146
C.2.131: XML Signature Best Practices 147
C.2.132: XML Signature Syntax and Processing Version 2.0 148
C.2.133: XML Signature Streaming Profile of XPath 1.0 149
C.2.134: Canonical XML Version 2.0 150
C.2.135: XML Security Algorithm Cross-Reference 151
C.2.136: XML Security 2.0 Requirements and Design Considerations 152
C.3 Pan European 153
C.3.1: Policy requirements for certification authorities issuing qualified certificates 153
C.3.2: Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates 154
C.3.3: Mapping Comparison Matrix between the US Federal Bridge CA Certificate Policy and the European Qualified Certificate Policy (TS 101 456) 155
C.3.4: CMS Advanced Electronic Signatures (CAdES) 156
C.3.5: Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES) 157

C.3.6: XML Advanced Electronic Signatures (XAdES) 158
C.3.7: Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES) 159
C.3.8: Time stamping profile 160
C.3.9: Qualified Certificate profile 161
C.3.10: Policy requirements for time-stamping authorities 162
C.3.11: Policy requirements for certification authorities issuing public key certificates 163
C.3.12: Algorithms and Parameters for Secure Electronic Signatures; 164
C.3.13: Algorithms and Parameters for Secure Electronic Signatures;Part 2: Secure channel protocols and algorithms for signature creation devices 165
C.3.14: Provision of harmonized Trust-service status information 166
C.3.15: Signature policy for extended business model 167
C.3.16: XML format for signature policies 168
C.3.17: Signature Policies Report 169
C.3.18: ASC.4.1 format for signature policies 170
C.3.19: X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons 171
C.3.20: Registered Electronic Mail (REM);Part 1: Architecture 172
C.3.21: Registered Electronic Mail (REM);Part 2: Data requirements, Formats and Signatures for REM 173
C.3.22: Registered Electronic Mail (REM);Part 3: Information Security Policy Requirements for REM Management Domains 174
C.3.23: Registered Electronic Mail (REM);Part 4: REM-MD Conformance Profiles 175
C.3.24: Registered Electronic Mail (REM);Part 5: REM-MD Interoperability Profiles 176
C.3.25: PDF Advanced Electronic Signature Profiles;Part 1: PAdES Overview - a framework document for PAdES 177
C.3.26: PDF Advanced Electronic Signature Profiles;Part 2: PAdES Basic - Profile based on ISO 32000-1 178
C.3.27: PDF Advanced Electronic Signature Profiles;Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles 179
C.3.28: PDF Advanced Electronic Signature Profiles;Part 4: PAdES Long Term - PAdES LTV Profile 180
C.3.29: PDF Advanced Electronic Signature Profiles;Part 5: PAdES for XML Content - Profiles for XAdES signatures 181
C.3.30: PDF Advanced Electronic Signature Profiles;Part 6: Visual Representations of Electronic Signatures 182
C.3.31: Information Preservation Systems Security 183
C.3.32: Information Preservation Systems Security 184
C.3.33: Associated Signature Containers (ASiC) 185
C.3.34: Policy requirements for Certification Service Providers 186
C.3.35: Requirements for role and attribute certificates 187
C.3.36: International Harmonization of Electronic Signature Formats 188
C.3.37: International Harmonization 189
C.3.38: Best Practices for handling electronic signatures and signed data for digital accounting 190

C.3.39: Policy requirements for trust service providers signing and/or storing data for digital accounting ..191

C.3.40: Registered E-Mail 192

C.3.41: General requirements for bodies operating product certification systems (ISO/IEC Guide 65:1996) 193

C.3.42: Application interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services 194

C.3.43: Application interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional services 195

C.3.44: Identification card systems -European Citizen Card -Part 0: General Introduction 196

C.3.45: Identification card systems -European Citizen Card -Part 1: Physical, electrical and transport protocol characteristics 197

C.3.46: Identification card systems - European Citizen Card -Part 2: Logical data structures and card services 198

C.3.47: Identification card systems - European citizen card - Part 3: ECC interoperability using an application interface 199

C.3.48: Identification card systems - European citizen card - Part 4: Recommendations for ECC issuance, operation and use 200

C.3.49: EESSI Conformity Assessment Guidance - Part 1: General introduction 201

C.3.50: EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes 202

C.3.51: EESSI Conformity Assessment Guidance - Part 3: Trustworthy sustems managing certificates for electronic signatures 203

C.3.52: EESSI Conformity Assessment Guidance - Part 4: Signature-creation applications and general guidelines for electronic signature verification 204

C.3.53: EESSI Conformity Assessment Guidance - Part 5: Secure signature-creation devices....205

C.3.54: EESSI Conformity Assessment Guidance - Part 6: Signature-creation device supporting signatures other than qualified 206

C.3.55: EESSI Conformity Assessment Guidance - Part 7: Cryptographic modules used by Certification Service Providers for signing operations and key generation services 207

C.3.56: EESSI Conformity Assessment Guidance - Part 8: Time-stamping Authority services and processes 208

C.3.57: Guidelines for the implementation of Secure Signature-Creation Devices 209

C.3.58: Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects 210

C.3.59: General guidelines for electronic signature verification 211

C.3.60: Security requirements for trustworthy systems managing certificates for electronic signatures - Part 1: System security requirements 212

C.3.61: Cryptographic Module for CSP Signing Operations with Backup – Protection Profile (CMCSOB-PP) 213

C.3.62: Cryptographic Module for CSP Key Generation Services – Protection Profile (CMCKG-PP) 214

C.3.63: Cryptographic Module for CSP Signing Operations – Protection Profile (CMCSO-PP) 215

C.3.64: Secure Signature-Creation Devices “EAL4” 216

C.3.65: Secure signature-creation devices “EAL 4+” 217

C.3.67: Protection profiles for Secure signature creation device – Part1: Overview 218

C.3.68: Protection profiles for Secure signature creation device – Part2: Device with key generation 219

C.3.69: Protection profiles for Secure signature creation device – Part3: Device with key import 220

C.3.70: Protection profiles for Secure signature creation device – Part4: Extension for device with key generation and trusted communication with certificate generation application 221

C.3.71: Protection profiles for Secure signature creation device – Part5: Extension for device with key generation and trusted communication with signature creation application 222

C.3.72: Protection profiles for Secure signature creation device – Part6: Extension for device with key import and trusted communication with signature creation application 223

C.3.73: Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software 224

C.3.74: Security requirements for device for authentication - Part 1: Protection Profile for core functionality 225

C.3.75: Security requirements for device for authentication - Part 2: Protection Profile for extension for trusted channel to certificate generation application 226

C.3.76: Security requirements for device for authentication - Part 3: Additional functionality for security targets 227

C.3.77: Protection profiles for signature creation and verification application – Part1: Introduction to the European Norm 228

C.3.78: Protection profiles for signature creation and verification application – Part2: Signature creation application - Core PP.....229

C.3.79: Protection profiles for signature creation and verification application – Part3: Signature creation application - Possible Extensions 230

C.3.80: Protection profiles for signature creation and verification application – Part4: Signature verification application - Core PP 231

C.3.81: Protection profiles for signature creation and verification application – Part5: Signature verification application - Possible Extensions.....232

C.4 National and Sector 233

C.4.1: Personal Identity Verification (PIV) of Federal Employees and Contractors 233

C.4.2: Security Requirements for Cryptographic Modules 234

C.4.3: Certificate management for financial services -- Part 1: Public key certificates 235

C.4.4: Banking -- Certificate management -- Part 2: Certificate extensions 236

C.4.5: Public key infrastructure for financial services -- Practices and policy framework 237

C.4.6: tScheme Approval profiles for PKI-related Services.....238

C.4.7: Approval Scheme for EPC Approved CAs for e-Mandate Services 239

C.4.8: Signatures and Authentication for Everyone (SAFE-BioPharma) Standard 240

C.4.9: eInvoicing & Digital Signatures 241

C.4.10: The practical use of Electronic signatures in E-Commerce: a Guide for SMEs.....242

C.4.11: Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique 243

C.4.12: Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique 244

C.4.13: Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés.....245

C.4.14: Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique 246

C.4.15: Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information 247

C.4.16: Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation 248

C.4.17: Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation 249

C.4.18: FAQ - Décret relatif à la signature électronique 250

C.4.19: Signature électronique Point de situation - Memento - Version 0.94 251

C.4.20: Dispositifs sécurisés de création de signature électronique (SSCD) 252

C.4.21: Tableau des produits certifiés conformes SSCD 253

C.4.22: Ressources cryptographiques pour autorités de certification (PSC) 254

C.4.23: Tableau des produits certifiés conformes PSC 255

C.4.24: Référentiel Général de Sécurité (RGS) version 1.0 256

C.4.25: Référentiel Général de Sécurité (RGS) version 1.0 - Annexe 3: Fonction de sécurité "signature" version 2.3 257

C.4.26: Interoperability of the electronic European Health Insurance Cards (WS/eEHIC) 258

C.4.27: Health Informatics - Public key infrastructure: Overview of digital certificate services 259

C.4.28: Health Informatics - Public key infrastructure: Certificate profile 260

C.4.29: Health Informatics - Public key infrastructure: Policy management of certification authority 261

C.4.30: Standard Practice for Healthcare Certificate Policy 262

C.4.31: OASIS ebXML Messaging Transport Binding for Digital Signature Services Version 1.0 263

C.4.32: Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — 264

C.4.33: Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — 265

C.4.34: Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — 266

C.4.35: Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) — 267

C.4.36: Asia PKI Interoperability GuidelinC.3. (Version 2.0, Draft). Book 2 268

C.4.37: Electronic Administration Act 269

C.4.38: Decree of the President of the Council of Ministers of March 30, 2009. Technical rules relating to generation, and setting and verification of digital signatures and time validation of electronic documents. (09A06300) 270

C.4.39: CNIPA Resolution 45 271

C.4.40: Italian Tax Agency. Disposition on how to communicate to the Tax Agency the "closure evidence" of fiscally relevant electronic documents 272

C.4.41: DECREE of MINISTRY OF FINANCE AND ECONOMY. Manners to accomplish fiscal obligations relevant to electronic documents and to their copy on various media. 273

C.4.42: CNIPA Resolution of 19 February 2004 274

C.4.43: Decree 52 of 20 March 2004 275

C.4.44: Decree of the President of the Council of Ministers of 11 May 2005 C.4. 68: "Regulation laying down rules for the use of registered electronic mail" 276

C.4.45: Decree of the President of the Council of Ministers of 6 May 2009 277

C.4.46: Decree 29 November 2008, No 185 - Act 2 / 2009 278

C.4.47: Circular No CNIPA 56 279

C.4.48: Circular No CNIPA 51 280

C.4.49: Decree of the Minister for Innovation and Technologies: "Technical rules for the creation, transmission and validation, including time, certified electronic mail." 281

C.4.50: Annex to the Decree of 2 November 2005: "Technical rules of service for the transmission of electronic documents by certified mail" 282

C.4.51: Decree of the President of the Republic No 68: "Regulation laying down rules for the use of certified mail, pursuant to Article 27 of Law January 16, 2003, No. 3." 283

C.4.52: CNIPA Technical Annex:RECOMMENDATIONS ON THE METHOD AND REGISTRATION PROCEDURES 284

C.4.53: CNIPA Technical Specification: "Technical specification for the transmission of electronic documents by registered electronic mail." 285

C.4.54: Aplicaciones con Documento Nacional de Identidad Electrónico (DNIe). Creación y verificación de firma electrónica. Tipo 1 para plataformas TI que permiten un control exclusivo de los interfaces con el firmante, y con un nivel de garantía de evaluación «EAL1» 286

C.4.55: Aplicaciones con Documento Nacional de Identidad Electrónico (DNIe). Creación y verificación de firma electrónica. Tipo 1 para plataformas TI que permiten un control exclusivo de los interfaces con el firmante, y con un nivel de garantía de evaluación «EAL3» 287

C.4.56: Aplicaciones con DNIC.3. Creación y verificación de firma electrónica. Tipo 2 para ordenadores personales, y con un nivel de garantía de evaluación «EAL1» 288

C.4.57: Aplicaciones con DNIC.3. Creación y verificación de firma electrónica. Tipo 2 para ordenadores personales, y con un nivel de garantía de evaluación «EAL3» 289

C.4.58: Real Decreto 4/2010 Esquema Nacional de Interoperabilidad/ Spanish National Interoperability Framework (Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica) 290

C.4.59: Esquema Nacional de Seguridad/ National Security Framework of Spain (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica) 291

C.4.60: Act on Strong Electronic Identification and Electronic Signatures 292

C.4.61: Common PKI V2.0 Part 1, Certificate and CRL Profiles 293

C.4.62: Common PKI V2.0 Part 2, PKI Management 294

C.4.63: Common PKI V2.0 Part 3, CMS based Message Formats 295

C.4.64: Common PKI V2.0 Part 4, Operational Protocol 296

C.4.65: Common PKI V2.0 Part 5, Certificate Path Validation 297

C.4.66: Common PKI V2.0 Part 6, Cryptographic Algorithms 298

C.4.67: Common PKI V2.0 Part 7, Signature API 299

C.4.68: Common PKI V2.0 Part 8, XML based Message Formats 300

C.4.69: Common PKI V2.0 Part 9, SigG Profile 301

History 302
History box entries.....**Error! Bookmark not defined.**

Annex C
Inventory

C.1 Introduction

C.1.1 Aim

This Annex contains the inventory of existing electronic signature standards used as the basis of this rationalised framework.

C.1.2 Organisation of Data

The inventory is organised under the following domains of standardisation:

International: Inventory of internationally recognised specifications (e.g. from ISO, ITU-T, IETF, W3C, OASIS …), excluding sector specific specifications.

Pan European: Inventory of pan European specifications (e.g. from ETSI, CEN)

National + Sector: Inventory of national and sector specific specifications

For each entry in the inventory the following information is provided as appropriate:

Source Identifies body which issued document (see C.1.3 for further information on document source)

Reference number Reference as used by source body

Publication Date Date when latest version published as indicated by source body.

Title Document title as indicated by source body

Description Description of document scope

Equivalent to Reference of specification which has equivalent text to a publication by another committee (e.g. ITU X.509 and ISO 9594-8)

Based on Reference to any primary source(s) on which the document is based.

URL Web URL where document may be obtained.

Rationalised Framework reference Framework reference - to be added as part of gap analysis

Technical Area Functional area (this is to be later aligned with framework)

Sub Area Sub-area (this is later to be aligned with framework)

Type of document Classification of the document type (this is later to be aligned with the framework

Level of Standardisation The level of standardisation (e.g. internationally recognised standards, European Norm, industry standard, regulation)

Status The status of the agreement with the document (classified in accordance with classification used by source)

Maturity Whether document is draft, publish or under revision.

Geographic general Whether the document applicability is International, European, other region, EU nation or non-EU nation.

Geographic details Any further details of geographic region that the document is applicable to.

Sector Sector to which the document is applicable.

C.1.3 Source Bodies

The sources of information are identified in the inventory using an abbreviated form.

AENOR	Asociación Española de Normalización	"AENOR is the Spanish Stantdardization Body, and one of the conformance certification bodies, that mirrors ISO and CEN/CENELEC commetees.
ANSSI	Agence Nationale de la Sécurité des Systèmes d'Information	"ANSSI is the French Network and Information Security Agency (former DCSSI).
A-SIT	Austria Secure Information Technology Center	"A-SIT is a competence center for IT-Security, whose members are the Federal Ministry of Finance, The Central bank of the Republic of Austria and the Graz University of Technology Activities include technical evaluations, top-level support for public bodies, observing of existing and emerging technologies and boosting the IT-Security awareness,
ASTM	International (formerly American) Society for Testing and Materials	International (formerly American) Society for Testing and Materials
CEN	"Comité Européen de Normalisation (European Committee for Standardization)	European standards body with European national standards institutes as members
DigitPA (formerly CNIPA)	Ente nazionale per la digitalizzazione della pubblica amministrazione	DigitPA is the national body for the digitization of public administration. Implements its mission through an accompanying government in the process of technological innovation by providing their technical expertise in the field of information technology and communications with an advisory role and given to the PA.
EPC	European Payments Council	The EPC is the decision-making and coordination body of the European banking industry in relation to payments
ETSI	European Telecommuncation Standards Institute	An official European Standards Organisation standards body for globally-applicable standards in Information and Communications Technologies (ICT)
ISO	International Standandards Organisation	International standards body with network of the national standards institutes of 159 countries
ISO JTC 1/SC 17	International Standandards Organisation, Joint Technical Committee 1 , SubCommittee 17	Under the JTC 1 scope "Information Technology", the SC17 develops standards on cards and personal identification
ISO JTC 1/SC 37	International Standandards Organisation, Joint Technical Committee 1 , SubCommittee 37	Under the JTC 1 scope "Information Technology", ISO Sub committtee concerned with Biometrics
ISO TC	International Standandards Organisation, Joint	Under the JTC 1 scope "Information Technology", ISO Sub committtee

1/SC 38	Technical Committee 1 , SubCommittee 38	concerned with Distributed application platforms and services (DAPS)
ISO TC 154	International Standandards Organisation, Technical Committee 154	"International standardization and registration of business, and administration processes and supporting data used for information interchange between and within individual organizations and support for standardization activities in the field of industrial data.
ISO TC 171/SC 2	International Standandards Organisation, Technical Committee 171 SubCommittee 2	Under the TC 171 scope "Application issues", the Joint TC 171/SC 2 - TC 42 - TC 46/SC 11 - TC 130 WG develops standards on document management applications - Application issues - PDF/A
ISO TC 46/SC 11	International Standandards Organisation, Technical Committee 46, SubCommittee 11	ISO Committee concerned with Archives/records management
ISO TC 68	International Standandards Organisation, Technical Committee 68	ISO Technical committee: Standardization in the field of banking, securities and other financial services.
ITU-T	"International Telecommunication Union-Telecommunication Standardization Sector"	United Nations agency for information and communication technology issues
JIPDEC	Japan Institute for Promotion of Digital Economy and Community	"Since its establishment in 1967, as a nonprofit organization under the laws of Japan, JIPDEC has worked to advance computer technologies and ensure the security of information systems. JIPDEC was designated as a ""Designated Investigative Organization"" pursuant to Act on Electronic Signatures and Certification Business by the competent ministers* in 2003"
NIST	(USA) National Institute of Standards and Technology	USA federal technology agency that works with industry to develop and apply technology, measurements, and standards
OASIS	Organization for the Advancement of Structured Information Standards	OASIS is a not-for-profit consortium that drives the development, convergence and adoption of open standards for security, Cloud computing, SOA, Web services, the Smart Grid, electronic publishing, emergency management, and other areas.
SAFE	Signatures and Authentication for Everyone (biopharmaceutical and healthcare)	"The Signatures and Authentication for Everyone (SAFE-BioPharma) Standard provides the framework for assured identity and a legally binding, regulatory compliant digital signature."
T7	T7 registered association team of the trust centre operators	T7 registered association is the team of trust centre operators and certification - service providers. Its members are publishers of chip cards and certificates which are a prerequisite for qualified electronic signatures after the German Digital Signature Act. T6 members are D-Trust GmbH, DATEV eG, Deutsche Post Com GmbH, German for savings bank publishing house, Deutsche Telekom AG and TC Trustcenter GmbH. The team existing since 1999 has been a registered association and professional organization since January 2005. It represents the interests of the German trust centre operators and promotes the possible applications and the application kindness of the qualified electronic signature.
tScheme	Trust Scheme	tScheme is the independent, industry-led, self-regulatory scheme set up to create strict assessment criteria, against which it will approve Trust Services.

W3C	World Wide Web Consortium	The World Wide Web Consortium (W3C) is an international community where Member organizations, a full-time staff, and the public work together to develop Web standards. W3C's mission is to lead the Web to its full potential.

C.2 International

C.2.1: Guidelines for the Accreditation of Bodies Operating Certification/Registration of Information Security Management Systems based on the Conformity Assessment standard ISO/IEC 17021

Source: ISO

Reference Number:	**Revised version of EA-7/03**
Publication Date:	
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP certification bodies acreditation
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This publication provides guidance and interpretation of the requirements from ISO/IEC 17021 for a third-party body operating ISMS certification/ registration to meet, if it is to be recognised as competent and reliable in the operation of ISMS certification/ registration. NOTE 1 In some countries, the bodies which verify conformity of ISMS to specified standards are called “certification bodies”, in others “registration bodies”, in others “assessment and registration bodies”, or “certification/ registration bodies”, and in others still, “registrars”. For ease of understanding, this publication always refers to such bodies as “certification/ registration bodies”. This should not be understood to be limiting. The requirements contained in this publication are written, above all, to be considered as general requirements for any body operating ISMS certification/ registration.

C.2.2: Conformity assessment — Requirements for bodies providing audit and certification of management systems

Source: ISO

Reference Number:	**ISO/IEC 17021:2011**
Publication Date:	2011
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP certification bodies acreditation
Type of Document:	Requirements
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This International Standard contains principles and requirements for the competence, consistency and impartiality of the audit and certification of management systems of all types (e.g. quality management systems or environmental management systems) and for bodies providing these activities. Certification bodies operating to this International Standard need not offer all types of management system certification. Certification of management systems (named in this International Standard “certification”) is a third-party conformity assessment activity (see ISO/IEC 17000:2004, 5.5). Bodies performing this activity are therefore third-party conformity assessment bodies (named in this International Standard “certification body/bodies”). NOTE 1 Certification of a management system is sometimes also called “registration”, and certification bodies are sometimes called “registrars”. NOTE 2 A certification body can be non-governmental or governmental (with or without regulatory authority). NOTE 3 This International Standard can be used as a criteria document for accreditation or peer assessment or other audit processes.

C.2.3: Conformity assessment — Requirements for bodies certifying products, processes and services

Source: ISO

Reference Number:	**ISO/IEC DIS 17065 (2011)**
Publication Date:	2011
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP certification bodies acreditation
Type of Document:	Requirements
Level of Standard:	Internationally recognised standard
Status:	DIS
Maturity:	Pending final balloting/publication
Geographic general:	International
Geographic details:	
Sector:	

Description:

This International Standard contains requirements for the competence, consistent operation and impartiality of product, process and service certification bodies. Certification bodies operating to this International Standard need not offer all types of products, processes and services certification. Certification of products, processes and services is a third party conformity assessment activity (5.5 of ISO/IEC 17000:2004). In the text the term "product" can be read as "process" or "service", except in those instances where separate provisions are stated for "processes" or "services" (Annex B).

C.2.5: Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 2: Integer factorization based mechanisms

Source: ISO

Reference Number:	**ISO/IEC 9796-2:2010**
Publication Date:	2010
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

ISO/IEC 9796-2:2010 specifies three digital signature schemes giving message recovery, two of which are deterministic (non-randomized) and one of which is randomized. The security of all three schemes is based on the difficulty of factorizing large numbers. All three schemes can provide either total or partial message recovery. ISO/IEC 9796-2:2010 specifies the method for key production for the three signature schemes. However, techniques for key management and for random number generation (as required for the randomized signature scheme), are outside the scope of ISO/IEC 9796-2:2010. The first mechanism specified in ISO/IEC 9796-2:2010 is only applicable for existing implementations, and is retained for reasons of backward compatibility.

C.2.6: Information technology -- Security techniques -- Digital signature schemes giving message recovery -- Part 3: Discrete logarithm based mechanisms

Source: ISO

Reference Number:	**ISO/IEC 9796-3:2006**
Publication Date:	2006
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

A digital signature in electronic exchange of information provides the same kind of facilities that are expected from a handwritten signature in paper-based mail. Hence it is applicable to providing entity authentication, data origin authentication, non-repudiation, and integrity of data. ISO/IEC 9796-3:2006 specifies digital signature mechanisms giving partial or total message recovery aiming at reducing storage and transmission overhead. ISO/IEC 9796-3:2006 specifies mechanisms based on the discrete logarithm problem of a finite field or an elliptic curve over a finite field. ISO/IEC 9796-3:2006 defines types of redundancy: natural redundancy, added redundancy, or both. ISO/IEC 9796-3:2006 gives the general model for digital signatures giving partial or total message recovery aiming at reducing storage and transmission overhead. ISO/IEC 9796-3:2006 specifies six digital signature schemes giving data recovery: NR, ECNR, ECMR, ECAO, ECPV, and ECKNR. NR is defined on a prime field; ECNR, ECMR, ECAO, ECPV, and ECKNR are defined on an elliptic curve over a finite field.

C.2.7: Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher

Source: ISO

Reference Number:	**ISO/IEC 9797-1:2011**
Publication Date:	2011
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

Message Authentication Code (MAC) Algorithms are data integrity mechanisms that compute a short string (the Message Authentication Code or MAC) as a complex function of every bit of the data and of a secret key. Their main security property is unforgeability: someone who does not know the secret key should not be able to predict the MAC on any new data string.

MAC algorithms can be used to provide data integrity. Their purpose is the detection of any unauthorized modification of the data such as deletion, insertion, or transportation of items within data. This includes both malicious and accidental modifications. MAC algorithms can also provide data origin authentication. This means that they can provide assurance that a message has been originated by an entity in possession of a specific secret key.

ISO/IEC 9797-1 specifies six MAC algorithms that use secret key and an n-bit block cipher to calculate a MAC.

This edition of this part of ISO/IEC 9797 also contains six mechanisms. Four of them are the same as the first four mechanisms in the second edition. However, the fifth and sixth mechanisms in the second edition have been removed and replaced by two new mechanisms, both designed to maximise efficiency by minimising the number of block cipher computations required to compute a MAC. These two mechanisms are known as OMAC1 (or CMAC) and LMAC. ISO/IEC 9797-1 specifies six MAC algorithms which are all based on the CBC mode of a block cipher. It also describes three padding methods. Padding is required to take into account the fact that the length of the data string may not be a multiple of the block length n.

The strength of the data integrity mechanism and message authentication mechanism is dependent on the length k (in bits) and secrecy of the key, on the block length n (in bits) and strength of the block cipher, on the length m (in bits) of the MAC, and on the specific mechanism.

The first three mechanisms specified in ISO/IEC 9797-1 are commonly known as CBC-MAC (CBC is the abbreviation of Cipher Block Chaining). The calculation of a MAC as described in ISO 8731-1 and ANSI X9.9 is a specific case of ISO/IEC 9797-1 when n=64, m=32, MAC Algorithm 1 and Padding Method 1 are used, and the block cipher is DEA (ANSI X3.92:1981). The calculation of a MAC as described in ANSI X9.19 and ISO 9807 is a specific case of this part of ISO/IEC 9797 when n=64, m=32, either MAC Algorithm 1 or MAC Algorithm 3 is used (both with Padding Method 1), and the block cipher is DEA (ANSIX3.92:1981).

The fourth mechanism is a variant of CBC-MAC with a special initial transformation. It is recommended for applications which require that the key length of the MAC algorithm is twice that of the block cipher.

The fifth and sixth mechanism use two parallel instances of the first and fourth mechanism respectively, and combine the two results with a bitwise exclusive-or operation. They are recommended for applications which require an increased security level against forgery attacks.

The fifth mechanism uses a single length MAC algorithm key, while the sixth mechanism doubles the MAC algorithm key length.

Annex A provides test values and Annex B provides extensive guidance on the selection of a MAC algorithm and a Padding Method.

This edition of this part of ISO/IEC 9797 also contains six mechanisms. Four of them are the same as the first four mechanisms in the second edition. However, the fifth and sixth mechanisms in the second edition have been removed and replaced by two new mechanisms, both designed to maximise efficiency by minimising the number of block cipher computations required to compute a MAC. These two mechanisms are known as OMAC1 (or CMAC) and LMAC.

Dependencies ISO/IEC 9797 uses terms defined in: ISO 7498-2: 1989, Information processing systems - Open systems interconnection - Basic reference model - Part 2: Security architecture ISO/IEC 10116: 1997, Information technology - Security techniques - Modes of operation for an n-bit block cipher

C.2.8: Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 2: Mechanisms using a dedicated hash-function

Source: ISO

Reference Number:	**ISO/IEC 9797-2:2010**
Publication Date:	2010
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

Message Authentication Code (MAC) Algorithms are data integrity mechanisms that compute a short string (the Message Authentication Code or MAC) as a complex function of every bit of the data and of a secret key Their main security property is unforgeability: someone who does not know the secret key should not be able to predict the MAC on any new data string.

MAC algorithms can be used to provide data integrity. Their purpose is the detection of any unauthorized modification of the data such as deletion, insertion, or transportation of items within data. This includes both malicious and accidental modifications. MAC algorithms can also provide data origin authentication. This means that they can provide assurance that a message has been originated by an entity in possession of a specific secret key.

ISO/IEC 9797-2 specifies three MAC algorithms that are based on a dedicated hash-function (selected from ISO/IEC 10118-3).

ISO/IEC 9797-2 specifies three MAC algorithms that use a secret key and a hash-function (or its round-function) with an n-bit result to calculate an m-bit MAC.

The strength of the data integrity mechanism and message authentication mechanism is dependent on the length (in bits) k and secrecy of the key, on the length (in bits) n of the hash-function and its strength, on the length (in bits) m of the MAC, and on the specific mechanism.

The first mechanism specified in ISO/IEC 9797-2 is commonly known as MDx-MAC. It calls the complete hash-function once, but it makes a small modification to the round-function by adding a key to the additive constants in the round-function. The second mechanism specified in ISO/IEC 9797-2 is commonly known as HMAC. It calls the complete hash-function twice. The third mechanism specified in ISO/IEC 9797-2 is a variant of MDx-MAC that takes as input only short strings (at most 256 bits). It offers a higher performance for applications that work with short input strings only.

Annex A provides test values and Annex B provides guidance on the security of the MAC algorithms.

5. Dependencies ISO/IEC 9797-1: 1999, Message authentication codes (MACs) - Part 1: Mechanisms using a block cipher ISO 7498-2: 1989, Information processing systems - Open systems interconnection - Basic reference model - Part 2: Security architecture ISO/IEC 10118-1: 2000, Information technology - Security techniques - Hash-function - Part 1: General ISO/IEC 10118-3: 1998, Information technology - Security techniques - Hash-function - Part 3: Dedicated hash-functions

C.2.9: Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 3: Mechanisms using a universal hash-fun

Source: ISO

Reference Number:	**ISO/IEC 9797-3:2010**
Publication Date:	2010
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This part of ISO/IEC 9797 specifies four MAC algorithms that use a secret key and a universal hash-function with an n-bit result to calculate an m-bit MAC. These mechanisms can be used as data integrity mechanisms to verify that data has not been altered in an unauthorised manner. They can also be used as message authentication mechanisms to provide assurance that a message has been originated by an entity in possession of the secret key. The strength of the data integrity mechanism and message authentication mechanism is dependent on the length (in bits) k and secrecy of the key, on the length (in bits) n of a hash-code produced by the hash-function, on the strength of the hash-function, on the length (in bits) m of the MAC, and on the specific mechanism.

The four mechanisms specified in this part of ISO/IEC 9797 are based on the dedicated hash-functions specified in ISO/IEC 10118-3, the block ciphers specified in ISO/IEC 18033-3 and the stream ciphers specified in ISO/IEC 18033-4.

```
* 1) The first mechanism specified in this part of ISO/IEC 9797 is commonly
known as UMAC.
* 2) The second mechanism specified in this part of ISO/IEC 9797 is commonly
known as Badger.
* 3) The third mechanism specified in this part of ISO/IEC 9797 is known as
Poly1305-AES.
* 4) The fourth mechanism specifid in this part of ISO/IEC 9797 is known as
GMAC.
```

This part of ISO/IEC 9797 can be applied to the security services of any security architecture, process, or application.

C.2.10: Information technology -- Security techniques -- Entity authentication -- Part 1: General

Source: ISO

Reference Number:	**ISO/IEC 9798-1:2010**
Publication Date:	2010
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

ISO/IEC 9798-1:2010 specifies an authentication model and general requirements and constraints for entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is the one that is claimed. An entity to be authenticated proves its identity by showing its knowledge of a secret. The mechanisms are defined as exchanges of information between entities and, where required, exchanges with a trusted third party. The details of the mechanisms and the contents of the authentication exchanges are given in subsequent parts of ISO/IEC 9798.

C.2.11: Information technology -- Security techniques -- Entity authentication -- Part 2: Mechanisms using symmetric encipherment algorithms

Source: ISO

Reference Number:	**ISO/IEC 9798-2:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

ISO/IEC 9798-2:2008 specifies entity authentication mechanisms using symmetric encipherment algorithms. Four of the mechanisms provide entity authentication between two entities where no trusted third party is involved; two of these are mechanisms to unilaterally authenticate one entity to another, while the other two are mechanisms for mutual authentication of two entities. The remaining mechanisms require a trusted third party for the establishment of a common secret key, and realize mutual or unilateral entity authentication. The mechanisms specified in ISO/IEC 9798-2:2008 use time variant parameters such as time stamps, sequence numbers, or random numbers to prevent valid authentication information from being accepted at a later time or more than once. If no trusted third party is involved and a time stamp or sequence number is used, one pass is needed for unilateral authentication, while two passes are needed to achieve mutual authentication. If no trusted third party is involved and a challenge and response method employing random numbers is used, two passes are needed for unilateral authentication, while three passes are required to achieve mutual authentication. If a trusted third party is involved, any additional communication between an entity and the trusted third party requires two extra passes in the communication exchange.

C.2.12: Information technology -- Security techniques -- Entity authentication -- Part 3: Mechanisms using digital signature techniques

Source: ISO

Reference Number:	**ISO/IEC 9798-3:1998**
Publication Date:	1998
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

The purpose of entity authentication is the corroboration that an entity is the one claimed. This part of ISO/IEC 9798 specifies entity authentication mechanisms employing a public key algorithm and a digital signature for the verification of the identity of an entity. The use of this standard is not restricted to a particular algorithm; any public key algorithm satisfying the requirements of the authentication mechanism(s) specified may be employed.

Entity authentication mechanisms based on a public key algorithm are characterized by the fact that the entity to be authenticated corroborates its identity by demonstrating its knowledge of its secret signature key. This key is used to digitally sign specific data. The signature can be verified by anyone knowing the entity's public verification key. It is thus of importance that the public verification key is valid and authentic. One way of obtaining a valid public key is by means of certificates distributed, for instance, by a trusted third party. Another way would be to distribute the public key by mutually agreed means. The means of obtaining a valid public verification key are outside the scope of the standard. The use of certificates is, therefore, only discussed in an informative annex.

The standard describes two mechanisms for unilateral authentication and three mechanisms for mutual authentication. In a unilateral authentication mechanism only one of the two entities is authenticated while in a procedure for mutual authentication the two communicating entities authenticate each other. Messages are sent between the claimant and the verifier for the verification of the claimant's identity. A message contains a signed part and an unsigned part. If information in the signed part of the message is already known to the verifier then it needs not be contained in the unsigned part. The provision of data in the unsigned part may also depend on the properties of the algorithm employed. To control uniqueness/timeliness of the messages class=GramE>(which, for example, prevents valid authentication information from being accepted at a later time) the messages contain time variant parameters such as time stamps, sequence numbers and random numbers. Their properties are described as in an informative annex. Implementation requirements may make different time variant parameters preferable in different applications.

Messages may contain text fields the use and relationship of which is not specified in this standard. The standard contains an informative annex on their use which could, for instance, be key distribution. Some of the key distribution mechanisms specified in ISO/IEC 11770-3 makes use of the mechanisms specified in this part of ISO/IEC 9798.

C.2.13: Information technology -- Security techniques -- Modes of operation for an n-bit block cipher

Source: ISO

Reference Number:	**ISO/IEC 10116:2006**
Publication Date:	2006
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: process
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 10116:2006 specifies modes of operation for an n-bit block cipher. These modes provide methods for encrypting and decrypting data where the bit length of the data may exceed the size of the block cipher. The modes specified in ISO/IEC 10116:2006 only provide protection of data confidentiality. Protection of data integrity and requirements for padding the data are not within the scope of ISO/IEC 10116:2006. ISO/IEC 10116:2006 specifies five modes of operation: 1. Electronic Codebook (ECB); 2. Cipher Block Chaining (CBC), with optional interleaving; 3. Cipher Feedback (CFB); 4. Output Feedback (OFB); and 5. Counter (CTR). The Annexes of ISO/IEC 10166:2006 provide object identifiers (according to ISO/IEC 9834) for each mode, a description of the properties of each mode, and diagrams and examples of each mode. Block ciphers are specified in ISO/IEC 18033-3.

C.2.14: Information technology -- Security techniques -- Hash-functions -- Part 1: General

Source: ISO

Reference Number:	**ISO/IEC 10118-1:2000**
Publication Date:	2000
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Format
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

Hash-functions map arbitrary strings of bits to a given range. They can be used for reducing a message to a short imprint for input to a digital signature mechanism, or for committing the user to a given string of bits without revealing this string. The input string of a hash- function is called a data string class=GramE>an the output string is called a hash-code.

This part of ISO/IEC 10118 contains definitions, symbols, abbreviations and requirements which are common to all the other parts of ISO/IEC 10118.

Abstract of objectives The document gives the definition of the terms "hash-function", "collision-resistant hash-function", "data string (or data)", "hash-code", "initializing value" and "padding", as well as the related notation. (Note: for the purpose of ISO/IEC 10118, a hash- function is defined as being what is generally called a one-way hash-function in the literature.)

It is required that the parties involved operate upon precisely the same data, use the same initializing values (if any) and the same padding methods (if any).

There are three informative annexes: Annex A provides some guidance on the choice of the initializing value. Annex B proposes two padding methods (method 1: append '0' bits if necessary; method 2: append a '1' bit then '0' bits if necessary). Annex C is bibliography.

Dependencies There are no dependencies but the padding methods are the same as those standardized in ISO/IEC 9797.

C.2.15: Information technology -- Security techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit block cipher

Source: ISO

Reference Number:	**ISO/IEC 10118-2:2010**
Publication Date:	2010
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: format
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 10118-2:2010 specifies hash-functions which make use of an n-bit block cipher algorithm. They are therefore suitable for an environment in which such an algorithm is already implemented. Block ciphers are specified in ISO/IEC 18033-3. Four hash-functions are specified. The first provides hash-codes of length less than or equal to n, where n is the block-length of the algorithm used. The second provides hash-codes of length less than or equal to 2n; the third provides hash-codes of length equal to 2n; and the fourth provides hash-codes of length 3n. All four of the hash-functions specified in ISO/IEC 10118-2:2010 conform to the general model specified in ISO/IEC 10118-1.

C.2.16: Information technology -- Security techniques -- Hash-functions -- Part 3: Dedicated hash-functions

Source: ISO

Reference Number:	**ISO/IEC 10118-3:2004**
Publication Date:	2004
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: format
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 10118-3:2004 specifies the following seven dedicated hash-functions, i.e. specially-designed hash-functions: • the first hash-function (RIPEMD-160) in Clause 7 provides hash-codes of lengths up to 160 bits; • the second hash-function (RIPEMD-128) in Clause 8 provides hash-codes of lengths up to 128 bits; • the third hash-function (SHA-1) in Clause 9 provides hash-codes of lengths up to 160 bits; • the fourth hash-function (SHA-256) in Clause 10 provides hash-codes of lengths up to 256 bits; • the fifth hash-function (SHA-512) in Clause 11 provides hash-codes of lengths up to 512 bits; • the sixth hash-function (SHA-384) in Clause 12 provides hash-codes of a fixed length, 384 bits; and • the seventh hash-function (WHIRLPOOL) in Clause 13 provides hash-codes of lengths up to 512 bits. For each of these dedicated hash-functions, ISO/IEC 10118-3:2004 specifies a round-function that consists of a sequence of sub-functions, a padding method, initializing values, parameters, constants, and an object identifier as normative information, and also specifies several computation examples as informative information.

C.2.17: Information technology -- Security techniques -- Hash-functions -- Part 4: Hash-functions using modular arithmetic

Source: ISO

Reference Number:	**ISO/IEC 10118-4:1998**
Publication Date:	1998
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: format
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

Scope Hash-functions map arbitrary strings of bits to a given range. They can be used for reducing a message to a short imprint for input to a digital signature mechanism, or for committing the user to a given string of bits without revealing this string.

This part of ISO/IEC 10118 specifies two collision-resistant hash-functions which make use of modular arithmetic employing a round-function using a composite modulus as a product of two large primes, and a reduction-function using a prime number only. These hash-functions compress messages of arbitrary but limited length to a hash-code whose length is determined by the length of the prime number used in the reduction-function. Thus, the hash- code is easily scaled to the input length of any mechanism (e.g., signature algorithm, identification scheme).

Abstract of objectives The hash-functions specified in this part of ISO/IEC 10118, known as MASH-1 and MASH-2 (Modular Arithmetic Secure Hash) are particularly suitable for environments in which implementations of modular arithmetic of sufficient length are already available. The two hash-functions differ only in the exponent used in the round-function. The length of the prime number used in the reduction-function shall be at most half of the length of the modulus used in the round-function.

Dependencies The hash-functions make use of a padding rule specified in Annex B of: ISO/IEC 10118-1: 1994, Information technology - Security techniques - Hash-functions - Part 1: General

C.2.18: Information technology -- Trusted Platform Module -- Part 1: Overview

Source: ISO

Reference Number:	**ISO/IEC 11889-1:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Trust service status provider
Subarea:	Trust platform
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 11889 defines the Trusted Platform Module (TPM), a device that enables trust in computing platforms in general. ISO/IEC 11889-1:2009 is an overview of the TPM. It describes the TPM and how it fits into the trusted platform. ISO/IEC 11889-1:2009 describes trusted platform concepts such as the trust boundary, transitive trust, integrity measurement, and integrity reporting.

C.2.19: Information technology -- Trusted Platform Module -- Part 2: Design principles

Source: ISO

Reference Number:	**ISO/IEC 11889-2:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Trust service status provider
Subarea:	Trust platform
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 11889 defines the Trusted Platform Module (TPM), a device that enables trust in computing platforms in general. ISO/IEC 11889-2:2009 defines the principles of TPM operation. These include base operating modes, cryptographic algorithms and key sizes for the algorithms, basic interoperability requirements, basic protocols and the use of the protocols, and use of TPM resources.

C.2.20: Information technology -- Trusted Platform Module -- Part 3: Structures

Source: ISO

Reference Number:	**ISO/IEC 11889-3:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Trust service status provider
Subarea:	Trust platform
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 11889 defines the Trusted Platform Module (TPM), a device that enables trust in computing platforms in general. ISO/IEC 11889-3:2009 defines the structures and constants that enable the interoperability between TPM implementations.

C.2.21: Information technology -- Trusted Platform Module -- Part 4: Commands

Source: ISO

Reference Number:	**ISO/IEC 11889-4:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Trust service status provider
Subarea:	Trust platform
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 11889 defines the Trusted Platform Module (TPM), a device that enables trust in computing platforms in general. ISO/IEC 11889-4:2009 defines the commands, actions of the commands, and the parameters to the commands that provide the TPM functionality.

C.2.22: Information technology -- Security techniques -- Non-repudiation -- Part 1: General

Source: ISO

Reference Number:	**ISO/IEC 13888-1:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 13888 is concerned with non-repudiation. ISO/IEC 13888-1:2009 is a general part which defines a model for non-repudiation mechanisms providing evidence based on cryptographic check values generated using symmetric or asymmetric cryptographic techniques. Non-repudiation mechanisms provide protocols for the exchange of non-repudiation tokens for non-repudiation services. Specific and additional non-repudiation services are described.

C.2.23: Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques

Source: ISO

Reference Number:	**ISO/IEC 13888-3:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 13888-3:2009 specifies mechanisms for the provision of specific, communication related, non-repudiation services using asymmetric cryptographic techniques.

C.2.24: Information technology -- Security techniques -- Digital signatures with appendix -- Part 1: General

Source: ISO

Reference Number:	**ISO/IEC 14888-1:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

There are two types of digital signature mechanism: • When the verification process needs the message as part of the input, the mechanism is called "signature mechanism with appendix". A hash-function is in used in the calculation of the appendix. • When the verification process reveals all or part of the message, the mechanism is called a "signature mechanism giving message recovery". A hash-function is also used in the generation and verification of these signatures. ISO/IEC 14888 specifies digital signatures with appendix. ISO/IEC 14888-1:2008 specifies general principles and requirements for digital signatures with appendix. ISO/IEC 14888-2 addresses digital signatures based on integer factoring, and ISO/IEC 14888-3 addresses digital signatures based on discrete logarithm. Signature mechanisms giving message recovery are specified in ISO/IEC 9796. Hash-functions are specified in ISO/IEC 10118.

C.2.25: Information technology -- Security techniques -- Digital signatures with appendix -- Part 2: Integer factorization based mechanisms

Source: ISO

Reference Number:	**ISO/IEC 14888-2:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

NOTE: This used to be entitled identity based scheme assume that scope of content has not changed. ISO/IEC 14888 specifies digital signature with appendix. As no part of the message is recovered from the signature (the recoverable part of the message is empty), the signed message consists of the signature and the whole message. NOTE ISO/IEC 9796 specifies digital signature giving message recovery. As all or part of the message is recovered from the signature, the recoverable part of the message is not empty. The signed message consists of either the signature only (when the non-recoverable part of the message is empty), or both the signature and the non-recoverable part. ISO/IEC 14888-2:2008 specifies digital signatures with appendix whose security is based on the difficulty of factoring the modulus in use. For each signature scheme, it specifies: • the relationships and constraints between all the data elements required for signing and verifying; • a signature mechanism, i.e. how to produce a signature of a message with the data elements required for signing; • a verification mechanism, i.e. how to verify a signature of a message with the data elements required for verifying. The title of ISO/IEC 14888-2 has changed from Identity-based mechanisms (first edition) to Integer factorization based mechanisms (second edition). 1. ISO/IEC 14888-2:2008 includes the identity-based scheme specified in ISO/IEC 14888-2:1999, namely the GQ1 scheme. This scheme has been revised due to the withdrawal of ISO/IEC 9796:1991 in 1999. 2. Among the certificate-based schemes specified in ISO/IEC 14888-3:1998, it includes all the schemes based on the difficulty of factoring the modulus in use, namely, the RSA, RW and ESIGN schemes. These schemes have been revised due to the withdrawal of ISO/IEC 9796:1991 in 1999. 3. It takes into account ISO/IEC 14888-3:1998/Cor.1:2001, technical corrigendum of the ESIGN scheme. 4. It includes a format mechanism, namely the PSS mechanism, also specified in ISO/IEC 9796-2:2002, and details of how to use it in each of the RSA, RW, GQ1 and ESIGN schemes. 5. It includes new certificate-based schemes that use no format mechanism, namely, the GQ2, GPS1 and GPS2 schemes. 6. For each scheme and its options, as needed, it provides an object identifier.

C.2.26: Information technology -- Security techniques -- Digital signatures with appendix -- Part 3: Discrete logarithm based mechanisms

Source: ISO

Reference Number:	**ISO/IEC 14888-3:2006**
Publication Date:	2006
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 14888-3:2006 specifies digital signature mechanisms with appendix whose security is based on the discrete logarithm problem. It provides a general description of a digital signature with appendix mechanism, and a variety of mechanisms that provide digital signatures with appendix. For each mechanism, ISO/IEC 14888-3:2006 specifies the process of generating keys, the process of producing signatures, and the process of verifying signatures. The verification of a digital signature requires the signing entity's verification key. It is thus essential for a verifier to be able to associate the correct verification key with the signing entity, or more precisely, with (parts of) the signing entity's identification data. This association may be provided by another means that is not covered in ISO/IEC 14888-3:2006. Whatever the nature of such means, the scheme is then said to be 'certificate-based'. If not, the association between the correct verification key and the signing entity's identification data is somehow inherent in the verification key itself. In such a case, the scheme is said to be 'identity-based'. Depending on the two different ways of checking the correctness of the verification keys, the digital signature mechanisms specified in ISO/IEC 14888-3:2006 are categorized in two groups: certificate-based and identity-based.

C.2.27: Elliptic Curve Russian Digital Signature Algorithm, Schnorr Digital Signature Algorithm, Elliptic Curve Schnorr Digital Signature Algorithm, and Elliptic Curve Full Schnorr Digital Signature Algorithm

Source: ISO

Reference Number:	**ISO/IEC 14888-3:2006/Amd 1:2010**
Publication Date:	2010
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech.specs: Mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

Scope Amendment 1 to ISO/IEC 14888-3:2006 introduces four digital signature algorithms: Elliptic Curve Russian Digital Signature Algorithm EC-RDSA, Schnorr Digital Signature Algorithm SDSA, Elliptic Curve Schnorr Digital Signature Algorithm EC-SDSA, and Elliptic Curve Full Schnorr Digital Signature Algorithm EC-FSDSA.

Abstract of objectives EC-RDSA is specified in Subclause 6.7; SDSA is specified in Subclause 6.8; EC-SDSA is specified in Subclause 6.9; and EC-FSDSA is specified in Subclause 6.10. Object identifiers are given in Annex A, test vectors are given in Annex F, a comparison of certificate-based mechanisms is given in Annex G Table G.1 and Table G.2, and claimed features for choosing a mechanism are given in Annex H.

Dependencies Some of the mechanisms specified in this document make use of the techniques specified in

C.2.28: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 1: Introduction and general model

Source: ISO

Reference Number:	**ISO/IEC 15408-1:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Conformity assurance
Subarea:	Protection profiles
Type of Document:	Requirements
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 15408-1:2009 establishes the general concepts and principles of IT security evaluation and specifies the general model of evaluation given by various parts of ISO/IEC 15408 which in its entirety is meant to be used as the basis for evaluation of security properties of IT products. It provides an overview of all parts of ISO/IEC 15408. It describes the various parts of ISO/IEC 15408; defines the terms and abbreviations to be used in all parts ISO/IEC 15408; establishes the core concept of a Target of Evaluation (TOE); the evaluation context; and describes the audience to which the evaluation criteria are addressed. An introduction to the basic security concepts necessary for evaluation of IT products is given. It defines the various operations by which the functional and assurance components given in ISO/IEC 15408-2 and ISO/IEC 15408-3 may be tailored through the use of permitted operations. The key concepts of protection profiles (PP), packages of security requirements and the topic of conformance are specified and the consequences of evaluation and evaluation results are described. ISO/IEC 15408-1:2009 gives guidelines for the specification of Security Targets (ST) and provides a description of the organization of components throughout the model. General information about the evaluation methodology is given in ISO/IEC 18045 and the scope of evaluation schemes is provided.

C.2.29: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 2: Security functional components

Source: ISO

Reference Number:	**ISO/IEC 15408-2:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Conformity assurance
Subarea:	Protection profiles
Type of Document:	Requirements
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 15408-2:2008 defines the content and presentation of the security functional requirements to be assessed in a security evaluation using ISO/IEC 15408. It contains a comprehensive catalogue of predefined security functional components that will meet most common security needs of the marketplace. These are organized using a hierarchical structure of classes, families and components, and supported by comprehensive user notes. ISO/IEC 15408-2:2008 also provides guidance on the specification of customized security requirements where no suitable predefined security functional components exist.

C.2.30: Information technology -- Security techniques -- Evaluation criteria for IT security -- Part 3: Security assurance components

Source: ISO

Reference Number:	**ISO/IEC 15408-3:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Conformity assurance
Subarea:	Protection profiles
Type of Document:	Requirements
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 15408-3:2008 defines the assurance requirements of the evaluation criteria. It includes the evaluation assurance levels that define a scale for measuring assurance for component targets of evaluation (TOEs), the composed assurance packages that define a scale for measuring assurance for composed TOEs, the individual assurance components from which the assurance levels and packages are composed, and the criteria for evaluation of protection profiles and security targets. ISO/IEC 15408-3:2008 defines the content and presentation of the assurance requirements in the form of assurance classes, families and components and provides guidance on the organization of new assurance requirements. The assurance components within the assurance families are presented in a hierarchical order.

C.2.31: Information technology -- Security techniques -- A framework for IT security assurance -- Part 1: Overview and framework

Source: ISO

Reference Number:	**ISO/IEC TR 15443-1:2005**
Publication Date:	2005
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Conformity assurance
Subarea:	IS security
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	TR
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC TR 15443 is a multi-part type 3 Technical Report to guide the IT security professional in the selection of an appropriate assurance method when specifying, selecting, or deploying a security service, product, or environmental factor such as an organization or personnel (known as a deliverable). The aim is to understand the assurance type and amount required to achieve confidence that the deliverable satisfies the stated IT security assurance requirements and consequently its security policy. ISO/IEC TR 15443-1:2005 describes the fundamentals of security assurance and its relation to other security concepts. This is to clarify why security assurance is required and dispel common misconceptions such as that increased assurance is gained by increasing the strength of a security mechanism. The framework includes a categorization of assurance types and a generic lifecycle model to identify the appropriate assurance types required for the deliverable with respect to the deliverable's lifecycle. The model also demonstrates how security assurance must be managed throughout the deliverable's lifecycle requiring assurance decisions to be made by several assurance authorities for the lifecycle stage relevant to their organization (i.e. developer, standards, consumer). The framework has been developed to be general enough to accommodate different assurance types and map into any lifecycle approach so as not to dictate any particular design. Advanced security assurance concepts, such as combining security assurance methods, are addressed briefly as they are to be addressed in later parts of ISO/IEC TR 15443. ISO/IEC TR 15443 targets IT security managers and other security professionals responsible for developing a security assurance program, engineering security into a deliverable, determining the security assurance of their deliverable, entering an assurance assessment audit (e.g. ISO 9000, SSE-CMM (ISO/IEC 21827), ISO/IEC 15408-3), or other assurance activities.

C.2.32: Information technology -- Security techniques -- A framework for IT security assurance -- Part 2: Assurance methods

Source: ISO

Reference Number:	**ISO/IEC TR 15443-2:2005**
Publication Date:	2005
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Conformity assurance
Subarea:	IS security
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	TR
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC TR 15443-2:2005 describes a variety of IT security assurance methods and approaches and relates them to the IT security assurance framework in ISO/IEC TR 15443-1. The emphasis is to identify qualitative properties of the assurance methods and elements that contribute to assurance, and where possible, to define assurance ratings. This material is intended for IT security professionals for the understanding of how to obtain assurance in a given life-cycle stage of a product or service. The objective is to describe and categorize assurance methods and approaches in a manner enabling a review of their comparable and synergetic properties. This will facilitate selection of the appropriate assurance method or and possible combination of assurance methods for a given IT security product, system, or service and its specific environment.

C.2.33: Information technology -- Security techniques -- A framework for IT security assurance -- Part 3: Analysis of assurance methods

Source: ISO

Reference Number:	**ISO/IEC TR 15443-3:2007**
Publication Date:	2007
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Conformity assurance
Subarea:	IS security
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	TR
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC TR 15443-3:2007 provides general guidance to an assurance authority in the choice of the appropriate type of international communications techology (ICT) assurance methods and to lay the framework for the analysis of specific assurance methods for specific environments. ISO/IEC TR 15443-3:2007 will allow the user to match specific assurance requirements and/or typical assurance situations with the general characteristics offered by available assurance methods. The guidance of ISO/IEC TR 15443-3:2007 is applicable to the development, implementation and operation of ICT product and ICT systems with security requirements. The advice given in ISO/IEC TR 15443-3:2007 will be qualitative and summary, and the user may need to analyse which methods presented in ISO/IEC TR 15443-2 will suit best his specific deliverables and organisational security requirements

C.2.34: Information technology -- Security techniques -- Guide for the production of Protection Profiles and Security Targets

Source: ISO

Reference Number:	**ISO/IEC TR 15446:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Conformity assurance
Subarea:	Protection profiles
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	TR
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC TR15446:2009 provides guidance relating to the construction of Protection Profiles (PPs) and Security Targets (STs) that are intended to be compliant with the third edition of ISO/IEC 15408. It is also applicable to PPs and STs compliant with Common Criteria Version 3.1, a technically identical standard published by the Common Criteria Management Board, a consortium of governmental organizations involved in IT security evaluation and certification. ISO/IEC TR15446:2009 is not intended as an introduction to evaluation using ISO/IEC 15408. Readers who seek such an introduction should consult ISO/IEC 15408-1. ISO/IEC TR15446:2009 does not deal with associated tasks beyond PP and ST specifications such as PP registration and the handling of protected intellectual property.

C.2.35: Information technology -- Security techniques -- Specification of TTP services to support the application of digital signatures

Source: ISO

Reference Number:	**ISO/IEC 15945:2002**
Publication Date:	2002
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Trust service status provider
Subarea:	TTP services and related commercial applications.
Type of Document:	Tech.specs: Protocol
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

Scope Technical services definitions and protocols are required to allow for the implementation of TTP services and related commercial applications. This IS focuses on

```
* implementation and interoperability,
* service specifications and,
* technical requirements.
```

Abstract of objectives This International Standard will define those TTP services needed to support the application of digital signatures in commercial applications.

This standard will also define interfaces and protocols to enable interoperability between entities associated with these TTP services.

This standard does not describe the management of TTPs or other organizational, operational or personal issues. Those topics are mainly covered in TR 14516.

Dependencies ISO/IEC 9594-8: 1997, Information technology - Open Systems Interconnection - The Directory - Part 8: Authentication framework ISO/IEC 9798-1: 1997, Information technology - Security techniques - Entity authentication - Part 1: General ISO/IEC 10118-1: 2000, Information technology - Security techniques - Hash-functions - Part 1: Hash-functions using an n-block cipher algorithm ISO/IEC 10118-2: 2000, Information technology - Security techniques - Hash-functions - Part 2: Hash-functions using an n-block cipher algorithm ISO/IEC 10118-3: 1998, Information technology - Security techniques - Hash-functions - Part 3: Dedicated Hash-functions ISO/IEC 10118-4: 1998, Information technology - Security techniques - Hash-functions - Part 4: Hash-functions using modular arithmetic ISO/IEC 11770-1: 1996, Information technology - Security techniques - Key management - Part 1: Framework ISO/IEC 11770-3: 1999, Information technology - Security techniques - Key management - Part 3: Mechanisms using asymmetric techniques ISO/IEC 14888-2: 1999, Information technology - Security techniques - Digital signatures with appendix - Part 2: Identity-based mechanisms ISO/IEC 14888-3: 1999, Information technology - Security techniques - Digital signatures with appendix - Part 3: Certificate-based mechanisms ISO/IEC TR 13335-1: 1996, Guidelines for the management of IT Security - Part 1: Concepts and models IT Security (cancelled and replaced by ISO/IEC 13335-1: 2004) ISO/IEC TR 13335-2: 1997, Guidelines for the management of IT Security - Part 2: Managing and planning IT Security (cancelled and replaced by ISO/IEC 13335-1: 2004) ISO/IEC TR 13335-3: 1998, Guidelines for the Management of IT Security - Part 3: Techniques for the management of IT Security (cancelled and replaced by ISO/IEC 27005: 2008) ISO/IEC TR 13335-4: 2000, Guidelines for the management of IT Security - Part 4: Selection of safeguards (cancelled and replaced by ISO/IEC 27005: 2008) ISO/IEC TR 13335-5: 2001, Guidelines for the Management of IT Security - Part 5: Management guidance on network security (cancelled and replaced by ISO/IEC 18028-1: 2006) ISO/IEC 13888-1: 1997, Information technology - Security techniques - Non-repudation - Part 1: General ISO/IEC 13888-2: 1998, Information technology - Security techniques - Non-repudation - Part 2: Mechanisms using symmetric techniques ISO/IEC 13888-3: 1997, Information technology - Security techniques - Non-repudation - Part 3: Mechanisms using asymmetric techniques

C.2.36: Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 1: General

Source: ISO

Reference Number:	**ISO/IEC 15946-1:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 15946 specifies public-key cryptographic techniques based on elliptic curves. It consists of five parts and includes the establishment of keys for symmetric cryptographic techniques, and digital signature mechanisms. ISO/IEC 15946-1:2008 specifically addresses the general techniques based on elliptic curves. It describes the mathematical background and specifies the general techniques necessary for implementing mechanisms based on elliptic curves defined over finite fields or pairings based on elliptic curves. ISO/IEC 15946-1:2008 specifies • conventional functions, • elliptic curves over any finite field such as a prime field and an extension field with characteristic two or three together with coordinates, • pairings over an elliptic curve.

C.2.37: Information technology -- Security techniques -- Cryptographic techniques based on elliptic curves -- Part 5: Elliptic curve generation

Source: ISO

Reference Number:	**ISO/IEC 15946-5:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 15946 specifies public-key cryptographic techniques based on elliptic curves. They include the establishment of keys for secret-key systems and digital signature mechanisms. ISO/IEC 15946-5:2009 defines the elliptic curve generation techniques useful for implementing the mechanisms defined in ISO/IEC 9796-3, ISO/IEC 11770-3, ISO/IEC 14888-3, and ISO/IEC 18033-2. The scope of ISO/IEC 15946-5:2009 is restricted to cryptographic techniques based on elliptic curves defined over finite fields of prime power order (including the special cases of prime order and characteristic two). The representation of elements of the underlying finite field (i.e. which basis is used) is outside the scope of ISO/IEC 15946-5:2009. ISO/IEC 15946 does not specify the implementation of the techniques it defines. Interoperability of products complying with ISO/IEC 15946 will not be guaranteed.

C.2.38: Information technology -- Security techniques -- Time-stamping services -- Part 1: Framework

Source: ISO

Reference Number:	**ISO/IEC 18014-1:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Time Stamping
Subarea:	Generic
Type of Document:	Framework
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 18014 specifies time-stamping techniques. It consists of three parts, which include the general notion, models for a time-stamping service, data structures, and protocols. ISO/IEC 18014-1:2008 describes a framework and defines the basic notion, the data structures, and protocols which are used for any time-stamping technique. ISO/IEC 18014-1:2008: • identifies the objective of a time-stamping authority; • describes a general model on which time-stamping services are based; • describes a process of generating and verifying time-stamp; • defines the data structures of time-stamp token; • defines the basic protocols of time-stamping; • specifies the protocols between the involved entities.

C.2.39: Information technology -- Security techniques -- Time-stamping services -- Part 2: Mechanisms producing independent tokens

Source: ISO

Reference Number:	**ISO/IEC 18014-2:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Time Stamping
Subarea:	Time-stamping authority
Type of Document:	Tech. Specs: mechanism
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 18014-2:2009 presents a general framework for the provision of time-stamping services. Time-stamping services may generate, renew and verify time-stamp tokens. Time-stamp tokens are associations between data and points in time, and are created in a way that aims to provide evidence that the data existed at the associated date and time. In addition, the evidence may be used by non-repudiation services. ISO/IEC 18014-2:2004 specifies mechanisms that generate independent time-stamps: in order to verify an independent time-stamp token, verifiers do not need access to any other time-stamp tokens. That is, time-stamp tokens are not linked, as is the case for the token types defined in ISO/IEC 18014-3.

C.2.40: Information technology -- Security techniques -- Time-stamping services -- Part 3: Mechanisms producing linked tokens

Source: ISO

Reference Number:	**ISO/IEC 18014-3:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Time Stamping
Subarea:	Time-stamping authority
Type of Document:	Tech. Specs: protocol
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 18014-3:2009 • describes a general model for time-stamping services producing linked tokens, • describes the basic components used to construct a time-stamping service producing linked tokens, • defines the data structures used to interact with a time-stamping service producing linked tokens, • describes specific instances of time-stamping services producing linked tokens, and defines a protocol to be utilized by time-stamping services producing linked tokens for the purpose of extending linked tokens to published values.

C.2.41: Information technology -- Security techniques -- Random bit generation

Source: ISO

Reference Number:	**ISO/IEC 18031:2005**
Publication Date:	2005
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: format
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 18031:2005 specifies a conceptual model for a random bit generator for cryptographic purposes, together with the elements of this model. ISO/IEC 18031:2005 also includes • the description of the main elements required for a non-deterministic random bit generator; • the description of the main elements required for a deterministic random bit generator; • their characteristics; • their security requirements. Techniques for statistical testing of random bit generators for the purposes of independent verification or validation, and detailed designs for such generators, are outside the scope of ISO/IEC 18031:2005.

C.2.42: Information technology -- Security techniques -- Prime number generation

Source: ISO

Reference Number:	**ISO/IEC 18032:2005**
Publication Date:	2005
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: methods
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 18032:2005 specifies methods for generating and testing prime numbers. Prime numbers are used in various cryptographic algorithms, mainly in asymmetric encryption algorithms and digital signature algorithms. Firstly, ISO/IEC 18032:2005 specifies methods for testing whether a given number is prime. The testing methods included in ISO/IEC 18032:2005 can be divided into two groups: • Probabilistic primality tests, which have a small error probability. All probabilistic tests described here may declare a composite to be a prime. One test described here may declare a prime to be composite. • Deterministic methods, which are guaranteed to give the right verdict. These methods use so-called primality certificates. Secondly, ISO/IEC 18032:2005 specifies methods to generate prime numbers. Again, both probabilistic and deterministic methods are presented.

C.2.43: Information technology -- Security techniques -- Encryption algorithms -- Part 2: Asymmetric ciphers

Source: ISO

Reference Number:	**ISO/IEC 18033-2:2006**
Publication Date:	2006
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: format
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 18033-2:2006 specifies encryption systems (ciphers) for the purpose of data confidentiality. The primary purpose of encryption (or encipherment) techniques is to protect the confidentiality of stored or transmitted data. An encryption algorithm is applied to data (often called plaintext or cleartext) to yield encrypted data (or ciphertext); this process is known as encryption. The encryption algorithm should be designed so that the ciphertext yields no information about the plaintext except, perhaps, its length. Associated with every encryption algorithm is a corresponding decryption algorithm, which transforms ciphertext back into its original plaintext. An asymmetric, i.e. public-key, encryption scheme allows a sender to use a recipient's public key to transmit an encryption of a message to the receiver, who can use his secret key to decrypt the given ciphertext, thereby obtaining the original message. Such a scheme should be secure in the sense that no information about the message should be leaked to a (resource-bounded) attacker, even if that attacker mounts a so-called 'chosen ciphertext' attack, in which he may obtain decryptions of other ciphertexts. This is the strongest type of attack that has been proposed for a public-key encryption scheme. ISO/IEC 18033-2:2006 specifies the functional interface of such a scheme, and in addition specifies a number of particular schemes that appear to be secure against chosen ciphertext attack. The different schemes offer different trade-offs between security properties and efficiency.

C.2.44: Information technology -- Security techniques -- Security requirements for cryptographic modules

Source: ISO

Reference Number:	**ISO/IEC 19790:2006**
Publication Date:	2006
URL:	
Equivalent to:	ISO/IEC 19790:2006 is derived from NIST Federal Information Processing Standard PUB 140-2 May 25, 2001.
Based on:	
Framework reference:	
Technical Area:	Conformity assurance
Subarea:	Security for cryptographic modules
Type of Document:	Requirements
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 19790:2006 specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems. ISO/IEC 19790:2006 specifies the following. • Four levels of increasing security for cryptographic modules. Each level offers an increase in security over the preceding level. • The following functional security objectives: o module specification; o ports and interfaces; o roles, services and authentication; o finite state model; o physical security; o operational environment; o cryptographic key management; o self-tests; o design assurance; o mitigation of other attacks. ISO/IEC 19790:2006 will be complemented by a future International Standard defining the associated evaluation and test methods.

C.2.45: Information technology -- Security techniques -- Anonymous digital signatures

Source: ISO

Reference Number:	**ISO/IEC WD 20008-1**
Publication Date:	
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: mechanism
Level of Standard:	Internationally recognised standard
Status:	Working Draft
Maturity:	Draft
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 20008 specifies anonymous digital signature mechanisms. In an anonymous digital signature mechanism, given a digital signature, an unauthorised entity cannot discover the signer's identifier. In some mechanisms, an authorized entity is allowed to trace a signature to its signer. In other mechanisms, there is no such authorized entity involved; as an alternative, an authorized entity is allowed to link two signatures signed by the same signer. All the mechanisms specified in this standard have the unforgeability property that only a legitimate signer can provide a signature.

C.2.46: Information technology -- Security techniques -- Anonymous digital signature -- Part 2: Mechanisms using a group public key

Source: ISO

Reference Number:	**ISO/IEC WD 20008-2**
Publication Date:	
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: mechanism
Level of Standard:	Internationally recognised standard
Status:	Working Draft
Maturity:	Draft
Geographic general:	
Geographic details:	
Sector:	

Description:

This part of ISO/IEC 20008 contains general principles and requirements for anonymous digital signatures. It also contains definitions and symbols which are used in all parts of ISO/IEC 20008.

There are two categories of anonymous digital signature mechanisms specified in this standard. The first category is the signature mechanisms using a group verification key; the second one is the signature mechanisms using multiple verification keys.

This part of ISO/IEC 20008 covers both of these two categories of mechanisms. A number of mechanisms of the first category are specified in ISO/IEC 20008 Part 2.

C.2.47: Information technology -- Security techniques -- Anonymous entity authentication -- Part 2: Mechanisms based on anonymous digital signature schemes

Source: ISO

Reference Number:	**ISO/IEC WD 20009-2**
Publication Date:	
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: mechanism
Level of Standard:	Internationally recognised standard
Status:	Working Draft
Maturity:	Draft
Geographic general:	
Geographic details:	
Sector:	

Description:

Scope

Anonymous authenticated communication involves hiding the identifier of an authenticated entity to its communicating partner and/or to a third party, whilst retaining the property that a verifier can reliably determine that its communication partner is authentic. Anonymous entity authentication mechanisms are designed to support such anonymous communications.

In an anonymous authentication mechanism, given complete knowledge of the messages exchanged between the parties, an unauthorised entity cannot discover the identifier of the entity being authenticated (i.e., the claimant). At the same time, an authorised verifier can obtain assurance that the claimant is authentic, i.e. a member of a predefined group of entities.

Abstract of objectives

This part of ISO/IEC 20009 specifies a general model, general requirements and constraints for anonymous entity authentication mechanisms which use security techniques. These mechanisms are used to corroborate that an entity is legitimate. The entity to be authenticated (the claimant) provides evidence to a verifier that it has knowledge of a secret, without revealing its identifier to any unauthorised entity. The mechanisms are defined as exchanges of information between entities, and where required, exchanges with a trusted third party.

The details of the mechanisms and the contents of the authentication exchanges are not specified in this part of ISO/IEC 20009, but in the following parts of this multipart International Standard.

C.2.48: Information technology -- Security techniques -- Test requirements for cryptographic modules

Source: ISO

Reference Number:	**ISO/IEC 24759:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Conformity assurance
Subarea:	Methods for testing
Type of Document:	Requirements
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 24759:2008 specifies the methods to be used by testing laboratories to test whether a cryptographic module conforms to the requirements specified in ISO/IEC 19790:2006. The methods are developed to provide a high degree of objectivity during the testing process and to ensure consistency across the testing laboratories. Within each subclause of the security requirements clause of ISO/IEC 24759:2008, the corresponding security requirements from ISO/IEC 19790:2006 are divided into a set of assertions (i.e. statements that have to be true for the module to satisfy the requirement of a given area at a given level). All of the assertions are direct quotations from ISO/IEC 19790:2006. Following each assertion is a set of requirements levied on the vendor. These specify the types of documentation or explicit information that the vendor is required to provide in order for the tester to verify conformance to the given assertion. Also following each assertion and the requirements levied on the vendor is a set of requirements levied on the tester of the cryptographic module. These specify what the tester needs to do in order to test the cryptographic module with respect to the given assertion. Vendors can use ISO/IEC 24759:2008 as guidance in trying to verify whether their cryptographic modules satisfy the requirements specified in ISO/IEC 19790:2006 before they apply to the testing laboratory for testing.

C.2.49: Information technology -- Security techniques -- Information security management systems -- Overview and vocabulary

Source: ISO

Reference Number:	**ISO/IEC 27000:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	IS security
Type of Document:	Framework
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published (under revision)
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 27000:2009 provides an overview of information security management systems, which form the subject of the information security management system (ISMS) family of standards, and defines related terms. As a result of implementing ISO/IEC 27000:2009, all types of organization (e.g. commercial enterprises, government agencies and non-profit organizations) are expected to obtain: 1. an overview of the ISMS family of standards; 2. an introduction to information security management systems (ISMS); 3. a brief description of the Plan-Do-Check-Act (PDCA) process; and 4. an understanding of terms and definitions in use throughout the ISMS family of standards. The objectives of ISO/IEC 27000:2009 are to provide terms and definitions, and an introduction to the ISMS family of standards that: 1. define requirements for an ISMS and for those certifying such systems; 2. provide direct support, detailed guidance and/or interpretation for the overall Plan-Do-Check-Act (PDCA) processes and requirements; 3. address sector-specific guidelines for ISMS; and 4. address conformity assessment for ISMS.

C.2.50: Information technology -- Security techniques -- Information security management systems -- Requirements

Source: ISO

Reference Number:	**ISO/IEC 27001:2005**
Publication Date:	2005
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	IS security
Type of Document:	Requirements
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published (under revision)
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 27001:2005 covers all types of organizations (e.g. commercial enterprises, government agencies, not-for profit organizations). ISO/IEC 27001:2005 specifies the requirements for establishing, implementing, operating, monitoring, reviewing, maintaining and improving a documented Information Security Management System within the context of the organization's overall business risks. It specifies requirements for the implementation of security controls customized to the needs of individual organizations or parts thereof. ISO/IEC 27001:2005 is designed to ensure the selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties. ISO/IEC 27001:2005 is intended to be suitable for several different types of use, including the following: • use within organizations to formulate security requirements and objectives; • use within organizations as a way to ensure that security risks are cost effectively managed; • use within organizations to ensure compliance with laws and regulations; • use within an organization as a process framework for the implementation and management of controls to ensure that the specific security objectives of an organization are met; • definition of new information security management processes; • identification and clarification of existing information security management processes; • use by the management of organizations to determine the status of information security management activities; • use by the internal and external auditors of organizations to determine the degree of compliance with the policies, directives and standards adopted by an organization; • use by organizations to provide relevant information about information security policies, directives, standards and procedures to trading partners and other organizations with whom they interact for operational or commercial reasons; • implementation of business-enabling information security; • use by organizations to provide relevant information about information security to customers.

C.2.51: Information technology -- Security techniques -- Code of practice for information security management

Source: ISO

Reference Number:	**ISO/IEC 27002:2005**
Publication Date:	2005
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	IS security
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published (under revision)
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 27002:2005 comprises ISO/IEC 17799:2005 and ISO/IEC 17799:2005/Cor.1:2007. Its technical content is identical to that of ISO/IEC 17799:2005. ISO/IEC 17799:2005/Cor.1:2007 changes the reference number of the standard from 17799 to 27002. ISO/IEC 27002:2005 establishes guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization. The objectives outlined provide general guidance on the commonly accepted goals of information security management. ISO/IEC 27002:2005 contains best practices of control objectives and controls in the following areas of information security management: • security policy; • organization of information security; • asset management; • human resources security; • physical and environmental security; • communications and operations management; • access control; • information systems acquisition, development and maintenance; • information security incident management; • business continuity management; • compliance. The control objectives and controls in ISO/IEC 27002:2005 are intended to be implemented to meet the requirements identified by a risk assessment. ISO/IEC 27002:2005 is intended as a common basis and practical guideline for developing organizational security standards and effective security management practices, and to help build confidence in inter-organizational activities.

C.2.52: Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems

Source: ISO

Reference Number:	**ISO/IEC 27006:2007**
Publication Date:	2007
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP certification and audit
Subarea:	IS security
Type of Document:	Requirements
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published (under revision)
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 27006:2007 specifies requirements and provides guidance for bodies providing audit and certification of an information security management system (ISMS), in addition to the requirements contained within ISO/IEC 17021 and ISO/IEC 27001. It is primarily intended to support the accreditation of certification bodies providing ISMS certification. The requirements contained in ISO/IEC 27006:2007 need to be demonstrated in terms of competence and reliability by any body providing ISMS certification, and the guidance contained in ISO/IEC 27006:2007 provides additional interpretation of these requirements for any body providing ISMS certification.

C.2.53: Information technology - Security techniques -

Guidelines for information security management systems auditing

Source: ISO

Reference Number:	**ISO/IEC FCD 27007**
Publication Date:	
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP certification and audit
Subarea:	IS security
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	Final CD
Maturity:	Draft
Geographic general:	
Geographic details:	
Sector:	

Description:

Scope This International Standard provides guidance on conducting information security management system (ISMS) audits, as well as guidance on the competence of ISMS auditors, in addition to the guidance contained in ISO 19011.

It is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.

Abstract of objectives This International Standard follows the structure of ISO 19011 with the inclusion of additional information security management system (ISMS) guidance on the application of ISO 19011 for ISMS audits as well as guidance on the competence and evaluation of ISMS auditors. This International Standard provides guidance on the management of an ISMS audit programme and the conduct of the internal or external audits in accordance with ISO/IEC 27001:2005.

This International Standard provides guidance on managing an information security management system (ISMS) audit programme, conducting the audits, and competence of ISMS auditors, in addition to the guidance contained in ISO 19011. This International Standard follows the structure of ISO 19011 and is applicable to those needing to understand or conduct internal or external audits of an ISMS or to manage an ISMS audit programme.

C.2.54: Information technology - Security techniques -

Best practice on the provision of time-stamping services

Source: ISO

Reference Number:	**ISO/IEC 2nd PDTR 29149: 2010**
Publication Date:	2010
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Time Stamping
Subarea:	Time-stamping authority
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	2nd PDTR
Maturity:	Draft
Geographic general:	
Geographic details:	
Sector:	

Description:

This Technical Report explains how to provide and use time-stamping services so that time-stamp tokens are effective when used to provide timeliness, data integrity, and non-repudiation services in conjunction with other mechanisms. It defines: - How time-stamp requesters should use time-stamp token generation services. -How TSAs (time-stamping authorities) should provide a service of guaranteed quality. -How TSAs should deserve trust based on good practices. - Which algorithms and parameters should be used in TST (time-stamp token) generation and TST renewal, so that TSTs resist during the time period during which the TSTs can be verified as being valid. - How time-stamp verifiers should use the time-stamp token verification services, both when validating individual TSTs, and when validating sequences of renewal TSTs.

C.2.55: Information technology -- Business Operational View -- Part 5: Identification and referencing of requirements of jurisdictional domains as sources of external constraints

Source: ISO

Reference Number:	**ISO/IEC 15944-5:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Business cases
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 15944-5:2008 is directed at being able to identify and reference laws and regulations impacting eBusiness scenarios and scenario components as external constraints. The primary source of such external constraints is jurisdictional domains. ISO/IEC 15944-5:2008 focuses on addressing the simple, i.e. definable, aspects of external constraints for which the source is a jurisdictional domain. A useful characteristic of external constraints is that at the sectoral, national and international levels, etc. focal points and recognized authorities often already exist. The rules and common business practices in many sectoral areas are already known. Use of ISO/IEC 15944-5:2008 (and related standards) will facilitate the transformation of these external constraints (business rules) into specified, registered and reusable scenarios and scenario components. The Business Transaction Model, explained in ISO/IEC 15944-1, has two classes of constraints, namely: • those which are self-imposed and agreed to as commitments among the parties themselves, i.e. internal constraints; and • those which are imposed on the parties to a business transaction based on the nature of the good, service and/or rights exchanged, and the nature of the commitment made among the parties (including ability to make commitments, the location, etc.), i.e. external constraints. The focus of ISO/IEC 15944-5:2008 is on external constraints. Jurisdictional domains are the primary source of external constraints. ISO/IEC 15944-5:2008 provides the key concepts required for addressing the legal environment in developing the Business Operational View of business transactions and scenarios which involve and are required to support external constraints. It begins with an exploration of the jurisdictional domain as a source of external constraint on the business process, both from the perspective of a Person and as a Public Administration. It then presents key constraints governing ISO/IEC 15944-5:2008 through principles and rules. It examines a key element in business transactions, that of the use of language. Jurisdictions can identify and, in some cases, impose the use of language in a business transaction. In this regard, the ISO/IEC 15944-5:2008 looks at the relationship of the constraint imposed by a jurisdictional domain on the choice of language used. Public policy constraints are also examined and key requirements for their inclusion in external constraints are identified, especially where they can affect the modelling of Open-edi scenarios and the business transaction components of Persons, data and processes. In particular, there is a set of rules that govern the identification and categories of jurisdictional domains as individual states as well as sets of entities, both regional and international. ISO/IEC 15944-5:2008 also focuses on the identification of rules governing the formation and identification of jurisdictional domains. It identifies the more primitive subtypes of jurisdictional domains and includes two approaches for the unambiguous identification of referencing of (subtypes of) jurisdictional domain. ISO/IEC 15944-5:2008 also provides checklists, through the use of templates, to guide the user through the mechanics of determining the source of the external constraint(s) where these are jurisdictional domains and determining the adequacy of the scenario specification as well as those of the scenario components. Annexes provide elaboration on the points raised in the main body.

C.2.56: Information technology -- Procedures for achieving metadata registry content consistency -- Part 1: Data elements

Source: ISO

Reference Number:	**ISO/IEC TR 20943-1:2003**
Publication Date:	2003
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Long Term Preservation (metadata)
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	TR
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

"Data management and interchange An ISO/IEC 11179-based metadata registry (MDR) (hereafter referred to as a "registry") is a tool for the management of shareable data; a comprehensive, authoritative source of reference information about data. It supports the standardization and harmonization processes by recording and disseminating data standards, which facilitates data sharing among organizations and users. It provides links to documents that refer to data elements and to information systems where data elements are used. When used in conjunction with an information database, the registry enables users to better understand the information obtained. A registry does not contain data itself. It contains the metadata that is necessary to clearly describe, inventory, analyze, and classify data. It provides an understanding of the meaning, representation, and identification of units of data. The standard identifies the information elements that need to be available for determining the meaning of a data element (DE) to be shared between systems. The purpose of ISO/IEC TR 20943-1:2003 is to describe a set of procedures for the consistent registration of data elements and their attributes in a registry. ISO/IEC TR 20943-1:2003 is not a data entry manual, but a user's guide for conceptualizing a data element and its associated metadata items for the purpose of consistently establishing good quality data elements. An organization may adapt and/or add to these procedures as necessary. The scope of ISO/IEC TR 20943-1:2003 is limited to the associated items of a data element: the data element identifier, names and definitions in particular contexts, and examples; data element concept; conceptual domain with its value meanings; and value domain with its permissible values. There is a choice when registering code sets and other value domains in an ISO/IEC 11179 metadata registry. Some Registration Authorities treat these sets as value domains, and others treat them as data elements. For the purposes of ISO/IEC TR 20943-1:2003, the choice will always be to treat the sets as data elements unless explicitly stated. This choice is made to help illustrate the way to register many different kinds of data elements, including examples for registering standard code sets as data elements.

C.2.57: Information technology -- Procedures for achieving metadata registry content consistency -- Part 3: Value domains

Source: ISO

Reference Number:	**ISO/IEC TR 20943-3:2004**
Publication Date:	2004
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Long Term Preservation (metadata)
Type of Document:	Guidelines
Level of Standard:	Internationally recognised standard
Status:	TR
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

The purpose of this technical report is to describe a set of procedures for the consistent registration of value domains and their attributes in a registry. This technical report is not a data entry manual, but a user's guide for conceptualizing a value domain and its components for the purpose of consistently establishing good quality metadata. An organization may adapt and/or add to these procedures as necessary.

C.2.58: Information technology -- Biometric data interchange formats -- Part 7: Signature/sign time series data

Source: ISO JTC 1/SC 37

Reference Number:	**ISO/IEC 19794-7:2007**
Publication Date:	2007
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: format
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 19794-7:2007 specifies two data interchange formats for signature/sign behavioural data captured in the form of time series using devices such as digitizing tablets or advanced pen systems. One data interchange format is for general use and the other one is a compact format for use with smart cards or other tokens. Both data interchange formats can be used for both acquired signature/sign samples (serving as a starting point for feature extraction) and for time-series features (to be compared directly by time-series based comparison algorithms). Abstract syntax notation one (ASN.1) specifications of the data interchange formats and encoding instructions are provided in an informative annex.

C.2.59: Information technology -- Biometric performance testing and reporting -- Part 7: Testing of on-card biometric comparison algorithms

Source:

Reference Number:	**ISO/IEC 19795-7:2011**
Publication Date:	2011
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification procedures
Type of Document:	Tech. Specs: procedures
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 19795-7:2011 establishes a mechanism for measuring the core algorithmic capabilities of biometric comparison algorithms running on ISO/IEC 7816 integrated circuit cards. Specifically, ISO/IEC 19795-7:2011 • instantiates a mechanism for on-card biometric comparison testing; • standardizes procedures for the measurement of the accuracy of on-card biometric comparison implementations running on object-based, test-specific sample cards; • standardizes procedures for the measurement of durations of the various operations; • gives examples for matching ISO/IEC 19794-2:2005 compact card minutiae templates. The following are specifically not within the scope of ISO/IEC 19795-7:2011: • procedures for securing the communications channel, including cryptographic protection of the biometric templates; • procedures for protection of sample or template integrity using digital signatures; • authentication of the card and reader; • selection or use of transmission protocols (e.g. contactless); • profiles of specific data interchange standards; • procedures for evaluation of readers, including performance, conformance and interoperability; • procedures for evaluation of ruggedness or durability of the card; • on-card template generation (e.g. extraction of minutiae from images); • template update or adaptation; • formal conformance tests of ISO/IEC 7816-4 and ISO/IEC 7816-11; • testing of devices not conforming to ISO/IEC 7816, including all system-on-card devices.

C.2.60: Information technology -- Web Services Interoperability -- WS-I Basic Profile Version 1.1

Source: ISO TC 1/SC 38

Reference Number:	**ISO/IEC 29361:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	e-delivery and web services
Type of Document:	Profiles
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 29361:2008 defines the WS-I Basic Profile 1.1, consisting of a set of non-proprietary Web services specifications, along with clarifications, refinements, interpretations and amplifications of those specifications which promote interoperability.

C.2.61: Information technology -- Web Services Interoperability -- WS-I Attachments Profile Version 1.0

Source:

Reference Number:	**ISO/IEC 29362:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	SOAP
Type of Document:	Profiles
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 29362:2008 defines the WS-I Attachments Profile 1.0, consisting of a set of non-proprietary Web services specifications, along with clarifications and amendments to those specifications that are intended to promote interoperability. It complements the WS-I Basic Profile 1.1 (ISO/IEC 29361:2008) to add support for interoperable SOAP Messages with Attachments-based Web services.

C.2.62: Information technology -- Web Services Interoperability -- WS-I Simple SOAP Binding Profile Version 1.0

Source:

Reference Number:	**ISO/IEC 29363:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	SOAP
Type of Document:	Profiles
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 29363:2008 defines the WS-I Simple SOAP Binding Profile 1.0, consisting of a set of non-proprietary Web services specifications, along with clarifications and amendments to those specifications which promote interoperability.

C.2.63: Identification cards -- Machine readable travel documents -- Part 1: Machine readable passport

Source: ISO JTC 1/SC 17

Reference Number:	**ISO/IEC 7501-1:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	e-Passport
Type of Document:	formats
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 7501-1:2008 is intended for use in all applications relating to machine readable passports (MRPs). It specifies the form and provides guidance on the construction of MRPs, in particular in relation to those aspects of the MRP where details of the rightful holder are presented in a form which is both visual and machine readable. It equally defines the specifications to be used by States wishing to issue an electronically enabled version of the MRP (ePassport) for secure carriage and access to an expanded set of details, including globally interoperable biometric data for confirming the presenter as the rightful holder of the ePassport.

C.2.64: Identification cards -- Integrated circuit cards -- Part 15: Cryptographic information application

Source:

Reference Number:	**ISO/IEC 7816-15:2004**
Publication Date:	2004
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	e-ID
Type of Document:	formats
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 7816-15:2004 specifies a card application. This application contains information on cryptographic functionality. Further, ISO/IEC 7816-15:2004 defines a common syntax (in ASN.1) and format for the cryptographic information and mechanisms to share this information whenever appropriate.

C.2.65: Information technology -- Personal identification -- ISO-compliant driving licence -- Part 3: Access control, authentication and integrity validation

Source:

Reference Number:	**ISO/IEC 18013-3:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	e-driving licence
Type of Document:	Guidelines on formats
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/IEC 18013 establishes guidelines for the design format and data content of an ISO-compliant driving licence (IDL) with regard to human-readable features (ISO/IEC 18013-1), machine-readable technologies (ISO/IEC 18013-2), and access control, authentication and integrity validation (ISO/IEC 18013-3). It creates a common basis for international use and mutual recognition of the IDL without impeding individual countries/states to apply their privacy rules and national/community/regional motor vehicle authorities in taking care of their specific needs. ISO/IEC 18013-3:2009 • is based on the machine-readable data content specified in ISO/IEC 18013-2; • specifies mechanisms and rules available to issuing authorities (IAs) for o access control (i.e. limiting access to the machine-readable data recorded on the IDL), o document authentication (i.e. confirming that the document was issued by the claimed IA), o data integrity validation (i.e. confirming that the data has not been changed since issuing).

ISO/IEC 18013-3:2009 does not address issues related to the subsequent use of data obtained from the IDL, e.g. privacy issues. • storage of multiple instances of cryptographic information in a card; • use of the cryptographic information; • retrieval of the cryptographic information; • cross-referencing of the cryptographic information with DOs defined in ISO/IEC 7816 when appropriate; • different authentication mechanisms; and • multiple cryptographic algorithms. • e-mail print

C.2.66: Information and documentation -- Records management processes -- Metadata for records -- Part 1: Principles

Source: ISO TC 46/SC 11

Reference Number:	**ISO 23081-1:2006**
Publication Date:	2006
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Long Term Preservation (metadata)
Type of Document:	Processes
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO 23081-1:2006 covers the principles that underpin and govern records management metadata. These principles apply through time to: • records and their metadata; • all processes that affect them; • any system in which they reside; • any organization that is responsible for their management.

C.2.67: Information and documentation -- Managing metadata for records -- Part 2: Conceptual and implementation issues

Source:

Reference Number:	**ISO 23081-2:2009**
Publication Date:	2009
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Long Term Preservation (metadata)
Type of Document:	Formats
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO/TS 23081-2:2009 establishes a framework for defining metadata elements consistent with the principles and implementation considerations outlined in ISO 23081-1:2006. The purpose of this framework is to: 1. to enable standardized description of records and critical contextual entities for records, 2. to provide common understanding of fixed points of aggregation to enable interoperability of records, and information relevant to records, between organizational systems, 3. to enable re-use and standardization of metadata for managing records over time, space and across applications. It further identifies some of the critical decision points that need to be addressed and documented to enable implementation of metadata for managing records. It aims • to identify the issues that need to be addressed in implementing metadata for managing records, • to identify and explain the various options for addressing the issues, and • to identify various paths for making decisions and choosing options in implementing metadata for managing records.

C.2.68: Document management -- Portable document format -- Part 1: PDF 1.7

Source:

Reference Number:	**ISO 32000-1:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Long Term Preservation (metadata)
Type of Document:	formats
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO 32000-1:2008 specifies a digital form for representing electronic documents to enable users to exchange and view electronic documents independent of the environment in which they were created or the environment in which they are viewed or printed. It is intended for the developer of software that creates PDF files (conforming writers), software that reads existing PDF files and interprets their contents for display and interaction (conforming readers) and PDF products that read and/or write PDF files for a variety of other purposes (conforming products). ISO 32000-1:2008 does not specify the following: • specific processes for converting paper or electronic documents to the PDF format; • specific technical design, user interface or implementation or operational details of rendering; • specific physical methods of storing these documents such as media and storage conditions; • methods for validating the conformance of PDF files or readers; • required computer hardware and/or operating system.

C.2.69: Document management -- Engineering document format using PDF -- Part 1: Use of PDF 1.6 (PDF/E-1)

Source: ISO TC 171/SC 2

Reference Number:	**ISO 24517-1:2008**
Publication Date:	2008
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Long Term Preservation (metadata)
Type of Document:	formats
Level of Standard:	Internationally recognised standard
Status:	International Standard
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

ISO 24517-:2008 specifies the use of the Portable Document Format (PDF) Version 1.6 for the creation of documents used in engineering workflows. ISO 24517-:2008 does not define the following: • method of electronic distribution; • method of creation or conversion from paper or electronic documents to the PDF/E format; • specific technical design, user interface, or implementation; • required computer hardware and/operating systems; or • methods for validating the conformance of PDF/E files or readers.

C.2.70: Information technology – Security techniques – Specification of TTP services to support the application of digital signatures

Source: ITU-T

Reference Number:	**X.843**
Publication Date:	Oct 00
URL:	http://www.itu.int/rec/T-REC-X.843/e
Equivalent to:	ISO/IEC 15945:2002
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP issuing qualified and non-qualified certificates
Type of Document:	Protocol
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	Joint Internation standard | Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This Recommendation | International Standard defines the services required to support the application of digital signatures for non-repudiation of creation of a document. Since this implies integrity of the document and authenticity of the creator, the services described can also be combined to implement integrity and authenticity services. This document describes services for: - Certificate Management (Registration, Public key certification, Revocation, Certificate update, Key update) - Key Management (Generation, distribution, personalization) - Other services (cross certification, public key validation, certificate validation, archival) It specifies: - minimum Certificate and CRL profiles - certificate management messages in accordance with RFC documents RFC 2510 and RFC 2511. - Online Certificate Status Protocol in accordance with RFC 2560

C.2.71: Information Technology - Security techniques - Guidelines for the use of Trusted Third Party services

Source: ITU-T

Reference Number:	**X.842**
Publication Date:	Oct 00
URL:	http://www.itu.int/rec/T-REC-X.842/e
Equivalent to:	ISO/IEC TR 14516
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Generic
Type of Document:	Policy requirements
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This Recommendation | Technical Report provides guidance for the use and management of Trusted Third Party (TTP) services, a clear definition of the basic duties and services provided, their description and their purpose, and the roles and liabilities of TTPs and entities using their services.

This Recommendation | Technical Report identifies different major categories of TTP services including time stamping, non-repudiation, key management, certificate management, and electronic notary public.

C.2.72:

Source: ITU-T

Reference Number:	**X.509**
Publication Date:	Nov 08
URL:	http://www.itu.int/rec/T-REC-X.509/en
Equivalent to:	ISO/IEC 9594-8
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP issuing qualified and non-qualified certificates
Type of Document:	Tech specs: Format
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	Joint Internation standard | Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

ITU-T Recommendation X.509 | ISO/IEC 9594-8 defines a framework for public-key certificates and attribute certificates. These frameworks may be used by other standards bodies to profile their application to Public Key Infrastructures (PKI) and Privilege Management Infrastructures (PMI). Also, this Recommendation | International Standard defines a framework for the provision of authentication services by Directory to its users. It describes two levels of authentication: simple authentication, using a password as a verification of claimed identity; and strong authentication, involving credentials formed using cryptographic techniques. While simple authentication offers some limited protection against unauthorized access, only strong authentication should be used as the basis for providing secure services.

C.2.73: Information technology -- Security techniques -- Entity authentication assurance framework

Source: ITU-T

Reference Number:	**X.eaa**
Publication Date:	
URL:	
Equivalent to:	ISO/IEC CD 29115
Based on:	
Framework reference:	
Technical Area:	Covers more than 1 area
Subarea:	Generic
Type of Document:	Architecture
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	Joint Internation standard | Recommendation
Maturity:	Draft
Geographic general:	International
Geographic details:	
Sector:	

Description:

This Recommendation | International Standard provides a framework for managing entity authentication assurance in a given context. In particular, it: - specifies four levels of entity authentication assurance; - specifies criteria and guidelines for each of the four levels of entity authentication assurance; - provides guidance for mapping the four levels of assurance to other authentication assurance schemes; - provides guidance concerning controls that should be used to mitigate authentication threats; - provides guidance for exchanging the results of authentication that are based on the four levels of assurance.

C.2.74: X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

Source: IETF

Reference Number:	**RFC 2560**
Publication Date:	Apr 99
URL:	http://datatracker.ietf.org/doc/rfc2559/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate validation
Type of Document:	Protocol
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

The protocol described in this document is designed to satisfy some of the operational requirements within the Internet X.509 Public Key Infrastructure (IPKI). Specifically, this document addresses requirements to provide access to Public Key Infrastructure (PKI) repositories for the purposes of retrieving PKI information and managing that same information. The mechanism described in this document is based on the Lightweight Directory Access Protocol (LDAP) v2, defined in RFC 1777, defining a profile of that protocol for use within the IPKI and updates encodings for certificates and revocation lists from RFC 1778. Additional mechanisms addressing PKIX operational requirements are specified in separate documents.

C.2.75: Internet X.509 Public Key Infrastructure

Operational Protocols: FTP and HTTP

Source: IETF

Reference Number:	**RFC 2585**
Publication Date:	May 99
URL:	http://datatracker.ietf.org/doc/rfc2585/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate validation
Type of Document:	Protocol
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

The protocol conventions described in this document satisfy some of the operational requirements of the Internet Public Key Infrastructure (PKI). This document specifies the conventions for using the File Transfer Protocol (FTP) and the Hypertext Transfer Protocol (HTTP) to obtain certificates and certificate revocation lists (CRLs) from PKI repositories. Additional mechanisms addressing PKIX operational requirements are specified in separate documents.

C.2.76: Diffie-Hellman Proof-of-Possession Algorithms

Source: IETF

Reference Number:	**RFC 2875**
Publication Date:	Jun 06
URL:	http://datatracker.ietf.org/doc/rfc2875/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Poof of possession
Type of Document:	Algorithm
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document describes two methods for producing an integrity check value from a Diffie-Hellman key pair. This behavior is needed for such operations as creating the signature of a PKCS #10 certification request. These algorithms are designed to provide a proof-of- possession rather than general purpose signing.

C.2.77: Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)

Source: IETF

Reference Number:	**RFC 3161**
Publication Date:	Aug 01
URL:	http://datatracker.ietf.org/doc/rfc3161/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Time-stamping
Type of Document:	Protocol
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document describes the format of a request sent to a Time Stamping Authority (TSA) and of the response that is returned. It also establishes several security-relevant requirements for TSA operation, with regards to processing requests to generate responses. Updated by RFC 5816

C.2.78: Algorithms and Identifiers for the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Source: IETF

Reference Number:	**RFC 3279**
Publication Date:	Aug 02
URL:	http://datatracker.ietf.org/doc/rfc3279/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Cryptographic Suites
Subarea:	Algorithm
Type of Document:	identifiers
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies algorithm identifiers and ASN.1 encoding formats for digital signatures and subject public keys used in the Internet X.509 Public Key Infrastructure (PKI). Digital signatures are used to sign certificates and certificate revocation list (CRLs). Certificates include the public key of the named subject. Updated by RFC 4055, RFC 4491, RFC 5480, RFC 5758

C.2.79: Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework

Source: IETF

Reference Number:	**RFC 3647**
Publication Date:	Feb 04
URL:	http://datatracker.ietf.org/doc/rfc3647/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP Issuing Certificates
Type of Document:	Policy requirements
Level of Standard:	Industry standard
Status:	Informational
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document presents a framework to assist the writers of certificate policies or certification practice statements for participants within public key infrastructures, such as certification authorities, policy authorities, and communities of interest that wish to rely on certificates. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a certificate policy or a certification practice statement. This document supersedes RFC 2527.

C.2.80: Internet X.509 Public Key Infrastructure: Logotypes in X.509 Certificates

Source: IETF

Reference Number:	**RFC 3709**
Publication Date:	Feb 04
URL:	http://datatracker.ietf.org/doc/rfc3709/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate
Type of Document:	Data format
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies a certificate extension for including logotypes in public key certificates and attribute certificates Updated by RFC 6170

C.2.81: Internet X.509 Public Key Infrastructure: Qualified Certificates Profile

Source: IETF

Reference Number:	**RFC 3739**
Publication Date:	Mar 04
URL:	http://datatracker.ietf.org/doc/rfc3739/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate
Type of Document:	Profile
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document forms a certificate profile, based on RFC 3280, for identity certificates issued to natural persons. The profile defines specific conventions for certificates that are qualified within a defined legal framework, named Qualified Certificates. However, the profile does not define any legal requirements for such Qualified Certificates. The goal of this document is to define a certificate profile that supports the issuance of Qualified Certificates independent of local legal requirements. The profile is however not limited to Qualified Certificates and further profiling may facilitate specific local needs.

C.2.82: Internet X.509 Public Key Infrastructure Permanent Identifier

Source: IETF

Reference Number:	**RFC 4043**
Publication Date:	May 05
URL:	http://datatracker.ietf.org/doc/rfc4043/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate
Type of Document:	Format
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document defines a new form of name, called permanent identifier, that may be included in the subjectAltName extension of a public key certificate issued to an entity. The permanent identifier is an optional feature that may be used by a CA to indicate that two or more certificates relate to the same entity, even if they contain different subject name (DNs) or different names in the subjectAltName extension, or if the name or the affiliation of that entity stored in the subject or another name form in the subjectAltName extension has changed. The subject name, carried in the subject field, is only unique for each subject entity certified by the one CA as defined by the issuer name field. However, the new name form can carry a name that is unique for each subject entity certified by a CA.

C.2.83: Internet X.509 Public Key Infrastructure Certificate Management Protocol (CMP)

Source: IETF

Reference Number:	**RFC 4210**
Publication Date:	Sep 05
URL:	http://datatracker.ietf.org/doc/rfc4210/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate management
Type of Document:	Protocol
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document describes the Internet X.509 Public Key Infrastructure (PKI) Certificate Management Protocol (CMP). Protocol messages are defined for X.509v3 certificate creation and management. CMP provides on-line interactions between PKI components, including an exchange between a Certification Authority (CA) and a client system.

C.2.84: Internet X.509 Public Key Infrastructure Certificate Request Message Format (CRMF)

Source: IETF

Reference Number:	**RFC 4211**
Publication Date:	Sep 05
URL:	http://datatracker.ietf.org/doc/rfc4211/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate management
Type of Document:	Protocol
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document describes the Certificate Request Message Format (CRMF) syntax and semantics. This syntax is used to convey a request for a certificate to a Certification Authority (CA), possibly via a Registration Authority (RA), for the purposes of X.509 certificate production. The request will typically include a public key and the associated registration information. This document does not define a certificate request protocol.

C.2.85: Internet X.509 Public Key Infrastructure Operational Protocols: Certificate Store Access via HTTP

Source: IETF

Reference Number:	**RFC 4387**
Publication Date:	May 06
URL:	http://datatracker.ietf.org/doc/rfc4386/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate access
Type of Document:	Protocol
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

The protocol conventions described in this document satisfy some of the operational requirements of the Internet Public Key Infrastructure (PKI). This document specifies the conventions for using the Hypertext Transfer Protocol (HTTP/HTTPS) as an interface mechanism to obtain certificates and certificate revocation lists (CRLs) from PKI repositories. Additional mechanisms addressing PKIX operational requirements are specified in separate documents.

C.2.86: Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates

Source: IETF

Reference Number:	**RFC 4523**
Publication Date:	Jun 06
URL:	http://datatracker.ietf.org/doc/rfc2587/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Directory
Type of Document:	Data format
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document describes schema for representing X.509 certificates, X.521 security information, and related elements in directories accessible using the Lightweight Directory Access Protocol (LDAP). The LDAP definitions for these X.509 and X.521 schema elements replace those provided in RFCs 2252 and 2256.

C.2.87: The Lightweight Online Certificate Status Protocol (OCSP) Profile for High-Volume Environments

Source: IETF

Reference Number:	**RFC 5019**
Publication Date:	Sep 07
URL:	http://datatracker.ietf.org/doc/rfc5019/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate validation
Type of Document:	Protocol
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This specification defines a profile of the Online Certificate Status Protocol (OCSP) that addresses the scalability issues inherent when using OCSP in large scale (high volume) Public Key Infrastructure (PKI) environments and/or in PKI environments that require a lightweight solution to minimize communication bandwidth and client- side processing.

C.2.88: Server-Based Certificate Validation Protocol (SCVP)

Source: IETF

Reference Number:	**RFC 5055**
Publication Date:	Dec 07
URL:	http://datatracker.ietf.org/doc/rfc5055/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate validation
Type of Document:	Protocol
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

The Server-Based Certificate Validation Protocol (SCVP) allows a client to delegate certification path construction and certification path validation to a server. The path construction or validation (e.g., making sure that none of the certificates in the path are revoked) is performed according to a validation policy, which contains one or more trust anchors. It allows simplification of client implementations and use of a set of predefined validation policies.

C.2.89: Certificate Management over CMS (CMC)

Source: IETF

Reference Number:	**RFC 5272**
Publication Date:	Jun 08
URL:	http://datatracker.ietf.org/doc/rfc5272/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate management
Type of Document:	Protocol
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document defines the base syntax for CMC, a Certificate Management protocol using the Cryptographic Message Syntax (CMS). This protocol addresses two immediate needs within the Internet Public Key Infrastructure (PKI) community: 1. The need for an interface to public key certification products and services based on CMS and PKCS #10 (Public Key Cryptography Standard), and 2. The need for a PKI enrollment protocol for encryption only keys due to algorithm or hardware design. CMC also requires the use of the transport document and the requirements usage document along with this document for a full definition.

C.2.90: Certificate Management over CMS (CMC): Transport Protocols

Source: IETF

Reference Number:	**RFC 5273**
Publication Date:	Jun 08
URL:	http://datatracker.ietf.org/doc/rfc5273/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate management
Type of Document:	Protocol
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document defines a number of transport mechanisms that are used to move CMC (Certificate Management over CMS (Cryptographic Message Syntax)) messages. The transport mechanisms described in this document are HTTP, file, mail, and TCP.

C.2.91: Certificate Management Messages over CMS (CMC): Compliance Requirements

Source: IETF

Reference Number:	**RFC 5274**
Publication Date:	Jun 08
URL:	http://datatracker.ietf.org/doc/rfc5274/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate management
Type of Document:	Confromity assessment
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document provides a set of compliance statements about the CMC (Certificate Management over CMS) enrollment protocol. The ASN.1 structures and the transport mechanisms for the CMC enrollment protocol are covered in other documents. This document provides the information needed to make a compliant version of CMC.

C.2.92: Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Source: IETF

Reference Number:	**RFC 5280**
Publication Date:	May 08
URL:	http://datatracker.ietf.org/doc/rfc5280/
Equivalent to:	
Based on:	ITU-T X.509
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate
Type of Document:	Profile
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This memo profiles the X.509 v3 certificate and X.509 v2 certificate revocation list (CRL) for use in the Internet. An overview of this approach and model is provided as an introduction. The X.509 v3 certificate format is described in detail, with additional information regarding the format and semantics of Internet name forms. Standard certificate extensions are described and two Internet-specific extensions are defined. A set of required certificate extensions is specified. The X.509 v2 CRL format is described in detail along with standard and Internet-specific extensions. An algorithm for X.509 certification path validation is described. An ASN.1 module and examples are provided in the appendices.

C.2.93: Internet X.509 Public Key Infrastructure: Additional Algorithms and Identifiers for DSA and ECDSA

Source: IETF

Reference Number:	**RFC 5758**
Publication Date:	Aug 09
URL:	http://datatracker.ietf.org/doc/rfc5758/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Cryptographic Suites
Subarea:	Algorithm
Type of Document:	Algorithm Identifiers
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document updates RFC 3279 to specify algorithm identifiers and ASN.1 encoding rules for the Digital Signature Algorithm (DSA) and Elliptic Curve Digital Signature Algorithm (ECDSA) digital signatures when using SHA-224, SHA-256, SHA-384, or SHA-512 as the hashing algorithm. This specification applies to the Internet X.509 Public Key infrastructure (PKI) when digital signatures are used to sign certificates and certificate revocation lists (CRLs). This document also identifies all four SHA2 hash algorithms for use in the Internet X.509 PKI.

C.2.94: ESSCertIDv2 Update for RFC 3161

Source: IETF

Reference Number:	**RC C 5816**
Publication Date:	Apr 10
URL:	http://datatracker.ietf.org/doc/rfc5816/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Time-stamping
Type of Document:	Data format
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document updates RFC 3161. It allows the use of ESSCertIDv2, as defined in RFC 5035, to specify the hash of a signer certificate when the hash is calculated with a function other than the Secure Hash Algorithm (SHA-1).

C.2.95: Trust Anchor Format

Source: IETF

Reference Number:	**RFC 5914**
Publication Date:	Jun 10
URL:	http://datatracker.ietf.org/doc/rfc5914/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Trust service status provider
Subarea:	Trust anchor management
Type of Document:	Data format
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document describes a structure for representing trust anchor information. A trust anchor is an authoritative entity represented by a public key and associated data. The public key is used to verify digital signatures, and the associated data is used to constrain the types of information or actions for which the trust anchor is authoritative. The structures defined in this document are intended to satisfy the format-related requirements defined in Trust Anchor Management Requirements.

C.2.96: Trust Anchor Management Protocol (TAMP)

Source: IETF

Reference Number:	**RFC 5934**
Publication Date:	Aug 10
URL:	http://datatracker.ietf.org/doc/rfc5934/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Trust service status provider
Subarea:	Trust anchor management
Type of Document:	Protocol
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document describes a transport independent protocol for the management of trust anchors (TAs) and community identifiers stored in a trust anchor store. The protocol makes use of the Cryptographic Message Syntax (CMS), and a digital signature is used to provide integrity protection and data origin authentication. The protocol can be used to manage trust anchor stores containing trust anchors represented as Certificate, TBSCertificate, or TrustAnchorInfo objects.

C.2.97: Internet X.509 Public Key Infrastructure -- Certificate Image

Source: IETF

Reference Number:	**RFC 6170**
Publication Date:	May 11
URL:	http://datatracker.ietf.org/doc/rfc6170/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Certificate
Type of Document:	Format
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies a method to bind a visual representation of a certificate in the form of a certificate image to a public key certificate as defined in RFC 5280, by defining a new "otherLogos" image type according to RFC 3709.

C.2.98: CMS Advanced Electronic Signatures (CAdES)

Source: IETF

Reference Number:	**RFC 5126**
Publication Date:	Mar 08
URL:	http://datatracker.ietf.org/doc/rfc5652/
Equivalent to:	ETSi TS 101 733
Based on:	RFC 3852 (RFC 5652)
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Format
Level of Standard:	Industry standard
Status:	Informational
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document defines the format of an electronic signature that can remain valid over long periods. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (i.e., repudiates) the validity of the signature. The format can be considered as an extension to RFC 3852 and RFC 2634, where, when appropriate, additional signed and unsigned attributes have been defined. The contents of this Informational RFC amount to a transposition of the ETSI Technical Specification (TS) 101 733 V.1.7.4 (CMS Advanced Electronic Signatures -- CAdES) and is technically equivalent to it.

C.2.99: Cryptographic Message Syntax (CMS)

Source: IETF

Reference Number:	**RFC 5652**
Publication Date:	Sep 09
URL:	http://datatracker.ietf.org/doc/rfc5652/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Format
Level of Standard:	Industry standard
Status:	Proposed standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document describes the Cryptographic Message Syntax (CMS). This syntax is used to digitally sign, digest, authenticate, or encrypt arbitrary message content. This obsolete RFC 3852

C.2.100: Digital Signature Services v1.0, DSS Core Protocols, Elements, and Bindings v1.0

Source: OASIS

Reference Number:	**oasis-dss-core-spec-v1.0-os**
Publication Date:	11. Apr 07
URL:	http://docs.oasis-open.org/dss/v1.0/oasis-dss-core-spec-v1.0-os.pdf
Equivalent to:	na
Based on: W3C Recommendation 12 Febr	XML-Signature Syntax and Processing, uary 2002; RFC 3161, RFC 3852, RFC 2440, SOAP 1.2
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	XML
Type of Document:	Technical Specification
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	General

Description:

This document defines XML request/response protocols for signing and verifying XML documents and other data. It also defines an XML timestamp format, and an XML signature property for use with these protocols. Finally, it defines transport and security bindings for the protocols.

C.2.101: German Signature Law Profile of the OASIS Digital Signature Service, version 1.0

Source: OASIS

Reference Number:	**oasis-dss-profiles-german-signature-law-spec-1.0-os**
Publication Date:	11. Apr 07
URL:	http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles_german_signature_law-spec-v1.0-os.pdf
Equivalent to:	na
Based on:	DSS Core
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	
Type of Document:	Technical Specification
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	Europe
Geographic details:	Germany
Sector:	General

Description:

DSS profile to support creation and validation of qualified signatures according to the guidelines given by the German signature law (SigG) and its associated regulations.

C.2.102: Advanced Electronic Signature Profiles of the OASIS Digital Signature Service Version 1.0

Source: OASIS

Reference Number:	**oasis-dss-profiles-AdES-spec-v1.0-os**
Publication Date:	11. Apr 07
URL:	http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-AdES-spec-v1.0-os.pdf
Equivalent to:	na
Based on:	
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	
Type of Document:	Technical Specification
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	General

Description:

This document defines one abstract profile of the OASIS DSS protocols for the purpose of creating and verifying XML or CMS based Advanced Electronic Signatures. It also defines two concrete sub-profiles: one for creating and verifying XML Advanced Electronic Signatures and the other for creating and verifying CMS based Advanced Electronic Signatures

C.2.103: Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services Version 1.0

Source: OASIS

Reference Number:	**oasis-dss-profiles-asynchronous_processing-spec-v1.0-os**
Publication Date:	11. Apr 07
URL:	http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-asynchronous_processing-spec-v1.0-os.pdf
Equivalent to:	na
Based on:	
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	
Type of Document:	Technical Specification
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	Germany
Sector:	General

Description:

This document defines protocol profiles and processing profiles for the purpose of creating and verifying German Signature Law signatures.

C.2.104: J2ME Code-Signing Profile of the OASIS Digital Signature Services

Source: OASIS

Reference Number:	**oasis-dss-profiles-codesigning-j2me-spec-v1.0-os**
Publication Date:	11. Apr 07
URL:	http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-codesigning-j2me-spec-v1.0-os.pdf
Equivalent to:	na
Based on:	
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	
Type of Document:	Technical Specification
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	General

Description:

This document profiles the OASIS DSS core protocols and the OASIS DSS Abstract Code-Signing Profile for the purpose of creating J2ME code-signing signatures.

C.2.105: Abstract Code-Signing Profile of the OASIS Digital Signature Services

Source: OASIS

Reference Number:	**oasis-dss-profiles-codesigning-spec-v1.0-os**
Publication Date:	11. Apr 07
URL:	http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-codesigning-spec-v1.0-os.pdf
Equivalent to:	na
Based on:	
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	
Type of Document:	Technical Specification
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	General

Description:

This document profiles the OASIS DSS core protocols and the Asynchronous Processing Abstract Profile of the OASIS Digital Signature Services for the purpose of creating code-signing signatures.

C.2.106: Electronic PostMark (EPM) Profile of the OASIS Digital Signature Service Version 1.0

Source: OASIS

Reference Number:	**oasis-dss-profiles-epm-spec-v1.0-os**
Publication Date:	11. Apr 07
URL:	http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-epm-spec-v1.0-os.pdf
Equivalent to:	na
Based on:	
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	
Type of Document:	Technical Specification
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	Postal services

Description:

This document defines a profile of the OASIS DSS protocol for the purpose of creating and verifying signatures and timestamps which support the extended features of the Universal Postal Union's Electronic PostMarking service.

C.2.107: Entity Seal Profile of the OASIS Digital Signature Service

Source: OASIS

Reference Number:	**oasis-dss-profiles-eseal-spec-v1.0-os**
Publication Date:	11. Apr 07
URL:	http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-eseal-spec-v1.0-os.pdf
Equivalent to:	na
Based on:	
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	
Type of Document:	Technical Specification
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	General

Description:

This document defines a profile of the OASIS DSS protocol and XML signature for the purpose of creating and verifying entity seals.

C.2.108: Signature Gateway Profile of the OASIS Digital Signature Service Version 1.0

Source: OASIS

Reference Number:	**oasis-dss-profiles-SignatureGateway-spec-v1.0-os**
Publication Date:	11. Apr 07
URL:	http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-SignatureGateway-spec-v1.0-os.pdf
Equivalent to:	na
Based on:	
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	
Type of Document:	Technical Specification
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	General

Description:

This document profiles the OASIS DSS core protocol for signature gateway transformation processing. This profile is intended to be generic, so it may be combined with other profiles freely.

C.2.109: XML Timestamping Profile of the OASIS Digital Signature Services Version 1.0

Source: OASIS

Reference Number:	**oasis-dss-profiles-timestamping-spec-v0.1-os**
Publication Date:	11. Apr 07
URL:	http://docs.oasis-open.org/dss/v1.0/oasis-dss-profiles-timestamping-spec-v1.0-os.pdf
Equivalent to:	na
Based on:	
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	Time-stamping
Type of Document:	Technical Specification
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	General

Description:

This document profiles the OASIS DSS core protocols for the purpose of creating and verifying XML-encoded time-stamps.

C.2.110: Security Assertion Markup Languague (SAML) V2.0

Source: OASIS

Reference Number:	**saml-core-2.0-os**
Publication Date:	15 March 2005
URL:	http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
Equivalent to:	na
Based on:	
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	
Type of Document:	Technical Specification
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	General

Description:

This specification defines the syntax and semantics for XML-encoded assertions about authentication, attributes, and authorization, and for the protocols that convey this information.

C.2.111: Web Services Security: SOAP Message Security 1.0 (WS-Security 2004)

Source: OASIS

Reference Number:	**OASIS Standard 200401; WSS: SOAP Message Security (WS-Security 2004)**
Publication Date:	March 2004
URL:	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf
Equivalent to:	na
Based on:	
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	
Type of Document:	Technical Specification
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	General

Description:

This specification describes enhancements to SOAP messaging to provide message integrity and confidentiality. The specified mechanisms can be used to accommodate a wide variety of security models and encryption technologies.

C.2.112: WS-Security Policy 1.2

Source: OASIS

Reference Number:	**ws-securitypolicy-1.2-spec-os**
Publication Date:	1 July 2007
URL:	http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.pdf
Equivalent to:	na
Based on:	WS-Policy
Framework reference:	A.4.3
Technical Area:	Signature creation / verification
Subarea:	
Type of Document:	Policy Requirements
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	General

Description:

This document defines a set of security policy assertions for use with the WS-Policy framework with respect to security features provided in WSS: SOAP Message Security , WS-Trust and WS-SecureConversation.

C.2.113: WS-Trust 1.4

Source: OASIS

Reference Number:	**ws-trust-1.4-os**
Publication Date:	2 February 2009
URL:	http://docs.oasis-open.org/ws-sx/ws-trust/v1.4/os/ws-trust-1.4-spec-os.pdf
Equivalent to:	na
Based on:	WS-Security
Framework reference:	
Technical Area:	Covers more than 1 area
Subarea:	
Type of Document:	
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	General

Description:

This specification defines extensions that build on WS-Security to provide a framework for requesting and issuing security tokens, and to broker trust relationships.

C.2.114: WS-Secure Conversation 1.4

Source: OASIS

Reference Number:	**ws-secureconversation-1.4-os**
Publication Date:	2 February 2009
URL:	http://docs.oasis-open.org/ws-sx/ws-secureconversation/v1.4/os/ws-secureconversation-1.4-spec-os.pdf
Equivalent to:	na
Based on:	WS-Security
Framework reference:	
Technical Area:	Covers more than 1 area
Subarea:	
Type of Document:	
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	General

Description:

This specification defines extensions that build on WS-Security to provide a framework for requesting and issuing security tokens, and to broker trust relationships.

C.2.115: XML Signature Syntax and Processing (Second Edition)

Source: W3C

Reference Number:	**N/A**
Publication Date:	2008
URL:	http://www.w3.org/TR/2008/REC-xmldsig-core-20080610/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats (XAdES), signature creation, signature verification (for XMLDSig)
Type of Document:	Tech. Specification (Format and protocol)
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	W3C Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies XML digital signatures syntax and processing rules. This second edition fixes certain bugs identified in the first edition and adds Canonical XML 1.1 as a required canonicalization algorithm, recommending its use for inclusive canonicalization instead of XML Canonicalization Version 1.0

C.2.116: Canonical XML Version 1.0

Source: W3C

Reference Number:	**N/A**
Publication Date:	2001
URL:	http://www.w3.org/TR/2001/REC-xml-c14n-20010315
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats (XAdES), signature creation, signature verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	W3C Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document defines a method for obtaining a unique physical representation (called canonical representaion) of a certain XML Document. The actual truth is that, given a XML document, two different applications could produce, after serializing it, two different octet strings, and any XML signature produced using the serialization mechanism by the first one, could not be verified with another application using the serialization mechanism by the second one. Some immediate elements that might generate problems and in consequence justify the definition of such a canonicalization form are: order in which the attributes of the elements appear in the serialized output, order and set of namespaces URIs for elements, appearance of default attributes, etc.

C.2.117: Exclusive XML Canonicalization Version 1.0

Source: W3C

Reference Number:	**N/A**
Publication Date:	2002
URL:	http://www.w3.org/TR/2002/REC-xml-exc-c14n-20020718/
Equivalent to:	
Based on:	Canonical XML Version 1.0
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats (XAdES), signature creation, signature verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	W3C Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

Canonical XML version 1.0 establishes that descendant elements inherit context (namespaces and attributes defined in "xml:" namespace, for instance) of their ascendant elements. With this canonicalization, if a XML Signature is applied on a payload that is part of a certain document (subdocument), and this payload is moved to other document, or extracted from its oreiginal document, the signature verification process would break as the context of the payload when the signature was generated and the context of the payload when the signature is verified, are different. This document specifies a method for serializing XML that excludes the context inheritance, ensuring that signed payloads can be extracted and moved from one document to another one without breaking the signature verification.

C.2.118: Canonical XML Version 1.1

Source: W3C

Reference Number:	**N/A**
Publication Date:	2008
URL:	http://www.w3.org/TR/2008/REC-xml-c14n11-20080502/
Equivalent to:	
Based on:	Canonical XML Version 1.0
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats (XAdES), signature creation, signature verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	W3C Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

After Canonical XML Version 1.0 was specified, the W3C specified new attributes within the XML ("xml:") namespace including particular processing rules for each. The result was that the general rules governing the inheritance of these attributes as specified in Canonical XML Version 1.0 for processing attributes within XML namespace did not properly take into account the semantics of the new defined attributes. Particularly, the xml:id attribute (unique within a XML document) must not be inherited, and xml:base requires a more complex processing than simple inheritance. This document is a revision to Canonical XML Version 1.0 for addressing the correct processing of attributes defined within the XML namespace. As mentioned before, XML Signature Syntax and Processing (Second Edition) recommending its use for inclusive canonicalization instead of XML Canonicalization Version 1.0.

C.2.119: XML-Signature Xpath Filter 2.0

Source: W3C

Reference Number:	**N/A**
Publication Date:	2002
URL:	http://www.w3.org/TR/2002/REC-xmldsig-filter2-20021108/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats (XAdES), signature creation, signature verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	W3C Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

XML Signatures may use XPath transforms for specifying a certain subset of a given XML document as the data that will actually be signed. XPath transform, as specified within the XML Signature Syntax and Processing may be difficult to implement efficiently with currently existing technologies (as roughly speaking it requires the evaluation of a regular XPath expression for EACH node within the input node-set to the signature, and its conversion to a boolean value). This document specifies a new XML Signature Transform that improves the efficiency in the selection process by reducing the actual number of of XPath expressions evaluations and instead applying set operations (intersection, usnion, substract) in the computation of the final set of nodes to be signed.

C.2.120: XML Path Language (Xpath) Version 1.0

Source: W3C

Reference Number:	**N/A**
Publication Date:	1999
URL:	http://www.w3.org/TR/1999/REC-xpath-19991116/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats (XAdES), signature creation, signature verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	W3C Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies a language for addressing parts of a certain XML document. It also introduces basic facilities for manipulation of strings, booleans and numbers. XPath is designed in a way that XPath expressions may be used within URIs and XML attribute values. XPath expressions may be used within the XPath transform element defined by XML Signature Syntax and Processing for selecting those parts of a XML Document that will actually be signed.

C.2.121: XSL Transformations (XSLT) Version 1.0

Source: W3C

Reference Number:	**N/A**
Publication Date:	1999
URL:	http://www.w3.org/TR/1999/REC-xslt-19991116
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats (XAdES), signature creation, signature verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	W3C Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies the syntax and semantics of a XML language for transforming XML documents in other XML documents. Within the context of XML Signature management, XSLT transformations (generating HTML documents from the original XML input document) may be used as one of the mechanisms that could give support to the feature of "What you see is what you sign" in different ways.

C.2.122: Decryption Transform for XML Signature

Source: W3C

Reference Number:	**N/A**
Publication Date:	2002
URL:	http://www.w3.org/TR/2002/REC-xmlenc-decrypt-20021210
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats (XAdES), signature creation, signature verification (for XMLDSig)
Type of Document:	Technical Specification (Format and processing rules)
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	W3C Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

An XML document may be partially encrypted and signed. The encrypted XML structures are substituted by XML Encryption elements. Some of the XML structures may be encrypted before signing and some others may be encrypted after signing. A verifying application needs to distinguish which XML elements were encrypted before signing and which ones were encrypted after, as it needs to decrypt the last ones before actually proceeding to verify the signature. This document specifies a specific transformation that allows XML Signature applications to distinguish between those XML structures that were encryted before signing and those ones that were encrypted after signing.

C.2.123: Visible Signature Profile of the OASIS Digital Signature Services Version 1.0

Source: OASIS

Reference Number:	**N/A**
Publication Date:	2010
URL:	http://docs.oasis-open.org/dss-x/profiles/visualsig/v1.0/cs01/oasis-dssx-1.0-profiles-visualsig-cs1.doc
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Centralized signature creation /verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	OASIS Committe Specification
Maturity:	Draft
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specify mechanism that enable clients that interact with a central digital signature service, based on OASIS DSS core and also aligned with this specification, to request to the server the incorporation of visible signatures in certain position/field of the document as part of the digital signature generation operation. IT also specifies mechanisms allowing clients to request verification of only certain signed fields and request the incorporation within the document of visual indications of the verification process result (a verification mark, the verification time and optionaly the verification scope indication)

C.2.124: OASIS DSS v1.0 Profile for Comprehensive Multi-Signature Verification Reports Version 1.0

Source: OASIS

Reference Number:	**N/A**
Publication Date:	2010
URL:	http://docs.oasis-open.org/dss-x/profiles/verificationreport/oasis-dssx-1.0-profiles-vr-cs01.doc
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Centralized signature creation /verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	OASIS Committe Specification
Maturity:	Draft
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies mechanisms that enable clients that interact with a central digital signature service, based on OASIS DSS core and also aligned with this specification, to request the verification of more than one signature on one or several documents, and the provision of individual reports on the verification process on each signature with different levels of details: "basic", "comprehensive" and "Convenient". The" basic" level is an indication of verification successful, unsuccsesful or uncomplete with some additional information of the reason, indicated by URI values. At the "Comprehensive" level the server returns within each individual report indication of all the validation material managed during the verification of the signature. At the "Convenient" level, the server returns within each individual report an indication of all the validation material used during the verification process AND XML representation of their most relevant fields. At present is the only technical specification being developed at international level on how to provide structured information on the signature verification process.

C.2.125: Signature Policy Profile of the OASIS Digital Signature Services Version 1.0

Source: OASIS

Reference Number:	**N/A**
Publication Date:	2009
URL:	http://docs.oasis-open.org/dss-x/profiles/sigpolicy/oasis-dssx-1.0-profiles-sigpolicy-cd01.doc
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Centralized signature creation /verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard (This includes Technical specification, CWAs, IETF RFC, OASIS specification..)
Status:	OASIS Committe Draft
Maturity:	Draft
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies mechanisms that enable clients that interact with a central digital signature service, based on OASIS DSS core and also aligned with this specification, to request generation or verification of electronic signature following a certain signature policy.

C.2.126: Information technology — Long term signature profiles —

Part 1: Long term signature profiles for CMS Advanced Electronic Signatures (CAdES)

Source: ISO/TC 154

Reference Number:	**ISO/DIS 14533-1**
Publication Date:	2011
URL:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56024
Equivalent to:	
Based on:	ETSI TS 101 733 and ETSI TS 102 734
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats , signature creation, signature verification
Type of Document:	Tech.specs: Format
Level of Standard:	Internationally recognised standard
Status:	DIS
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

The purpose of this standard is to ensure the interoperability of implementations with respect to long term signatures that make electronic signatures verifiable for a long term. Long term signature specifications referenced by each implementation cover CMS Advanced Electronic Signatures (CAdES) developed by the European Telecommunications Standards Institute (ETSI). This standard specifies the requirement for enabling verification of a digital signature over a long period of time. Thisstandard specifies which elements should be chosen, in order to enable verification of a digital signature overa long period of time among the elements defined in CMS Advanced Electronic Signatures (CAdES) which is the extended specification of Cryptographic message syntax (CMS) used widely.

C.2.127: Information technology — Long term signature profiles —

Part 2: Long term signature profiles for XML Advanced Electronic Signatures (XAdES)

Source: ISO/TC 154

Reference Number:	**ISO/DIS 14533-2**
Publication Date:	2011
URL:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=56024
Equivalent to:	
Based on:	ETSI TS 101 903 and ETSI TS 102 904
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats , signature creation, signature verification
Type of Document:	Tech.specs: Format
Level of Standard:	Industry standard
Status:	DIS
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

The purpose of this standard is to ensure the interoperability of implementations with respect to long term signatures that make electronic signatures verifiable for a long term. Long term signature specifications referenced by each implementation cover XML Advanced Electronic Signatures (XAdES) developed by the European Telecommunications Standards Institute (ETSI). This standard specifies the requirement for enabling verification of a digital signature over a long period of time. Thisstandard specifies which elements should be chosen, in order to enable verification of a digital signature overa long period of time among the elements defined in XML Advanced Electronic Signatures (XAdES) which is the extended specification of "XML-Signature Syntax and Processing" used widely.

C.2.128: XML Signature Syntax and Processing Version 1.1

Source: W3C

Reference Number:	**N/A**
Publication Date:	2011
URL:	http://www.w3.org/TR/2011/CR-xmldsig-core1-20110303/
Equivalent to:	
Based on:	XML Signature Syntax and Processing Version 1.0
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats , signature creation, signature verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard
Status:	Candidate Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document updates XML Signature version 1.0 second edition. This document specifies a new XML structure for supporting Eliptic Curves pùblic key support. In addition to that it also specifies new XML elements for containing the digest of a X509Certificate and the digest algorithm. It also specifies a new element able to convey an OCSP response. All these elements are used as descendant of the ds:KeyInfo element, which also incorporate capability for incorporating encrypted key information and references to the key material that is conveyed elsewhere.

C.2.129: XML Signature Properties

Source: W3C

Reference Number:	**N/A**
Publication Date:	2011
URL:	http://www.w3.org/TR/2011/CR-xmldsig-properties-20110303/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats , signature creation, signature verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard
Status:	Candidate Recommendation
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document defines specific signature properties that may be used by various applications of XML Signature, without requiring those applications to define such properties on a per case basis. This document defines how these properties are to be specified and processed when used but does not require their use - specifications that reference this document may or may not require their use. Specifically this document defines a Profile property to identify a Profile specification that details how the XML signature is to be used; Role property, to indicate the specific role for the signature; Identifier property that associates to the signature a unique identifier; the Created property for indicating the creation time of the signature; the Expires property, to indicate the expiration time of the signature; ReplayProtect property, a nonce against reuse of the signature. This specification explictly references XAdES as follows: "XAdES specification defines signature property formats for advanced electronic signatures that remain valid over long periods, are compliant with the European Directive and incorporate additional useful information in common uses cases " .

C.2.130: XML Security 1.1 Requirements and Design Considerations

Source: W3C

Reference Number:	**N/A**
Publication Date:	2011
URL:	http://www.w3.org/TR/2011/WD-xmlsec-reqs-20110303/#Introduction
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification
Type of Document:	Requirements
Level of Standard:	Industry standard
Status:	Working Draft
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This use case and requirements document is intended to summarize use cases and requirements driving revisions to XML Signature 2nd Edition, XML Encryption, and Canonical XML 1.1. It is not intended to define all possible use cases for these Recommendations, but rather to provide rationale for decisions leading to XML Signature 1.1, XML Encryption 1.1, XML Signature Properties and XML Security Generic Hybrid Ciphers. This document outlines general principles and use cases leading to requirements and offers some design options. It elaborates on principles and updates requirements expressed for the original XML Security work including original requirements documents. This document also reflects material from a W3C workshop on next steps for XML Security and position papers associated with the workshop.

C.2.131: XML Signature Best Practices

Source: W3C

Reference Number:	**N/A**
Publication Date:	2010
URL:	http://www.w3.org/TR/2010/WD-xmldsig-bestpractices-20100831/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	Working Draft
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document collects best practices for implementers and users of the XML Signature specification [XMLDSIG-CORE1]. Most of these best practices are related to improving security and mitigating attacks, yet others are for best practices in the practical use of XML Signature, such as signing XML that doesn't use namespaces, for example.

C.2.132: XML Signature Syntax and Processing Version 2.0

Source: W3C

Reference Number:	**N/A**
Publication Date:	2010
URL:	http://www.w3.org/TR/2010/WD-xmldsig-core2-20100831/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats , signature creation, signature verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard
Status:	Working Draft
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies a new version of XML digital signatures syntax and processing rules. Signature 2.0 includes a new transform model designed to address a number of requirements including performance, simplicity and streamability. This model is significantly different than in XML Signature 1.x. Nevertheless, XML Signature 2.0 is designed to be backward compatible, however, enabling the XML Signature 1.x model to be used where necessary.

C.2.133: XML Signature Streaming Profile of XPath 1.0

Source: W3C

Reference Number:	**N/A**
Publication Date:	2010
URL:	http://www.w3.org/TR/2010/WD-xmldsig-xpath-20100831/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard
Status:	Working Draft
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document defines a streamable profile of XPath 1.0 suitable for use with XML Signature 2.0. It aims at simplifying the selection of XML parts to be signed and overcoming the problems associated to the XPath Filter Transform specified in XML Signature 1.0 and the XPath Filter Transform 2. In addition it aims at achieving that it is possible to evaluate these XPath expressions on large XML documents without having having to load the entire document into memory.

C.2.134: Canonical XML Version 2.0

Source: W3C

Reference Number:	**N/A**
Publication Date:	2011
URL:	http://www.w3.org/2008/xmlsec/Drafts/c14n-20/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard
Status:	Working Draft
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

Canonical XML Version 2.0 is canonicalization algorithm for XML Signature 2.0. It addresses issues around performance, streaming, hardware implementation, robustness, minimizing attack surface, determining what is signed and more.

C.2.135: XML Security Algorithm Cross-Reference

Source: W3C

Reference Number:	**N/A**
Publication Date:	2010
URL:	http://www.w3.org/TR/2010/WD-xmlsec-algorithms-20100513/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification
Type of Document:	Tech. Specification (format)
Level of Standard:	Industry standard
Status:	Working Draft
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document summarizes XML Security algorithm URI identifiers and the specifications associated with them. This document is not intended as an exhaustive list of all known related identifiers, some of which may have been defined by other standards or specifications. Furthermore, this note is not to be taken as normative regarding the information provided; if information here conflicts with the referenced specification, the specification takes precedence in all cases.

C.2.136: XML Security 2.0 Requirements and Design Considerations

Source: W3C

Reference Number:	**N/A**
Publication Date:	2010
URL:	http://www.w3.org/TR/2010/WD-xmlsec-reqs2-20100204/
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification
Type of Document:	Requirements
Level of Standard:	Industry standard
Status:	Working Draft
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document outlines use cases, requirements and design choices for XML Security 2.0, specifically Canonical XML 2.0 and XML Signature 2.0. It includes a proposed simplification of the XML Signature Transform mechanism, intended to enhance security, performance, streamability and to ease adoption.

C.3 Pan European

C.3.1: Policy requirements for certification authorities issuing qualified certificates

Source: ETSI

Reference Number:	**TS 101 456**
Publication Date:	May 07
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	IETF RFC 3647
Framework reference:	
Technical Area:	CSP
Subarea:	CSP Issuing qualified certificates
Type of Document:	Policy requirements
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

This document specifies policy requirements relating to Certification Authorities (CAs) issuing qualified certificates . It defines policy requirements on the operation and management practices of certification authorities issuing qualified certificates such that subscribers, subjects certified by the CA and relying parties may have confidence in the applicability of the certificate in support of electronic signatures.

C.3.2: Guidance on TS 101 456 (Policy Requirements for certification authorities issuing qualified certificates

Source: ETSI

Reference Number:	**TR 102 437**
Publication Date:	Oct 06
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	ETSI TS 101 456
Framework reference:	
Technical Area:	CSP
Subarea:	CSP Issuing qualified certificates
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

This document provides guidance on interpreting the requirements specified in TS 101 456 . This guidance is intended for use by bodies that supervise (e.g. as per Directive articles 3.3), approve or accredit CAs (e.g. as per articles 3.2 of Directive), assessors, certification service providers and other interested parties.

C.3.3: Mapping Comparison Matrix between the US Federal Bridge CA Certificate Policy and the European Qualified Certificate Policy (TS 101 456)

Source: ETSI

Reference Number:	**TR 102 458**
Publication Date:	Apr 06
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on: FBCA Policy	ETSI TS 101 456
Framework reference:	
Technical Area:	CSP
Subarea:	CSP Issuing qualified certificates
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document compares the United States Federal Bridge Certification Authority (FBCA) Certificate Policy, and the European Qualified Certificate Policy (QCP) as specified in TS 101 456 in order to identify to what extent which stipulations FBCA CP match those of QCP. This document is out of date and no applicable to current US situation.

C.3.4: CMS Advanced Electronic Signatures (CAdES)

Source: ETSI

Reference Number:	**TS 101 733**
Publication Date:	Jan 11
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	IETF RFC 3852
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Tech specs: Format
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document defines a number of electronic signature formats, including electronic signatures that can remain valid over long periods. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the electronic signature. It describes formats for advanced electronic signatures using ASN.1 (Abstract Syntax Notation 1). These formats are based on CMS (Cryptographic Message Syntax) defined in RFC 3852.

C.3.5: Profiles of CMS Advanced Electronic Signatures based on TS 101 733 (CAdES)

Source: ETSI

Reference Number:	**TS 102 734**
Publication Date:	Feb 07
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	ETSI TS 101 733
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Tech specs: Profile
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Under revision
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document profiles the use of TS 101 733 (CAdES) signatures, based on CMS for its use within the following specific environments as follows: • e-Invoicing area. • e-government area. • a baseline for other application areas.

C.3.6: XML Advanced Electronic Signatures (XAdES)

Source: ETSI

Reference Number:	**TS 101 903**
Publication Date:	Dec 10
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	W3C XMLDSig
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Tech specs: Format
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document defines XML formats for advanced electronic signatures that remain valid over long periods, are compliant with the European Directive and incorporate additional useful information in common uses cases. This includes evidence as to its validity even if the signer or verifying party later attempts to deny (repudiates) the validity of the signature. It defines signature formats using on XML Notation based on IETF / W3C "XML Signature Syntax and Processing"

C.3.7: Profiles of XML Advanced Electronic Signatures based on TS 101 903 (XAdES)

Source: ETSI

Reference Number:	**TS 102 904**
Publication Date:	Feb 07
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	ETSI TS 102 903
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Tech specs: Profile
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Under revision
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document profiles the use of TS 101 903 (XAdES) [1] signatures, based on XML SIG [2] for its use within the following specific environments as follows: • e-Invoicing area. • e-government area. • a baseline for other application areas.

C.3.8: Time stamping profile

Source: ETSI

Reference Number:	**TS 101 861**
Publication Date:	Jan 06
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	RFC 3161
Framework reference:	
Technical Area:	CSP
Subarea:	Time-stamping
Type of Document:	Tech specs: Profile
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Under revision
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document is defines a profile for a time-stamping based on RFC 3161 which uses advanced electronic signatures to protect the time-stamp. It defines what a Time Stamping client must support and what a Time Stamping Server must support. Such time-stamps may be used to assure the time related to an electronic signature (e.g. signing time, verification time)

C.3.9: Qualified Certificate profile

Source: ETSI

Reference Number:	**TS 101 862**
Publication Date:	Jan 06
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on: IETF RFC 3739	IETF RFC 3280
Framework reference:	
Technical Area:	CSP
Subarea:	CSP issuing qualified certificates
Type of Document:	Tech specs: Profile
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Under revision
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document defines a profile for Qualified Certificates, based on the technical definitions in RFC 3739 [4], that may be used by issuers of Qualified Certificates complying with Annex I and II of the European Electronic Signature Directive 1999/93/EC.

C.3.10: Policy requirements for time-stamping authorities

Source: ETSI

Reference Number:	**TS 102 023**
Publication Date:	Oct 10
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	RFC 316
Framework reference:	
Technical Area:	CSP
Subarea:	Time-stamping
Type of Document:	Policy requirements
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document specifies policy requirements relating to the operation of Time-stamping Authorities (TSAs). The present document defines policy requirements on the operation and management practices of TSAs such that subscribers and relying parties may have confidence in the operation of the time-stamping services. These policy requirements are primarily aimed at time-stamping services used in support of qualified electronic signatures (i.e. in line with article 5.1 of the European Directive on a community framework for electronic signatures) but may be applied to any application requiring to prove that a datum existed before a particular time.

C.3.11: Policy requirements for certification authorities issuing public key certificates

Source: ETSI

Reference Number:	**TS 102 042**
Publication Date:	Apr 10
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	IETF RFC 3647
Framework reference:	
Technical Area:	CSP
Subarea:	CSP issuing non-qualified certificates
Type of Document:	Policy requirements
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document specifies policy requirements relating to Certification Authorities (CAs) issuing public key certificates, including Extended Validation Certificates (EVC). It defines policy requirements on the operation and management practices of certification authorities issuing and managing certificates such that subscribers, subjects certified by the CA and relying parties may have confidence in the applicability of the certificate in support of cryptographic mechanisms.

C.3.12: Algorithms and Parameters for Secure Electronic Signatures;

Part 1: Hash functions and asymmetric algorithms

Source: ETSI

Reference Number:	**TS 102 176-1**
Publication Date:	Dec 07
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Cryptographic Suites
Subarea:	Signature algorithms
Type of Document:	Tech specs: Algorithm
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Under revision
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document is targeted to support advanced electronic signatures and the related infrastructure. The present document defines a list of hash functions and a list of signature schemes, as well as the recommended combinations of hash functions and signatures schemes in the form of "signature suites". The primary criteria for inclusion of an algorithm in the present document are: • the algorithm is considered as secure; • the algorithm is commonly used; and • the algorithm can easily be referenced (for example by means of an OID).

C.3.13: Algorithms and Parameters for Secure Electronic Signatures;Part 2: Secure channel protocols and algorithms for signature creation devices

Source: ETSI

Reference Number:	**TS 102 176-2**
Publication Date:	Jul 05
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Cryptographic Suites
Subarea:	Cryptographic algorithms
Type of Document:	Tech specs: Algorithm
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document defines a set of symmetric algorithms and protocols to be used to construct a secure channel between an application and a signature creation device providing either only integrity or both integrity and confidentiality. Such a secure channel is required during the operational phase of a signature creation device to remotely download a private key in the signature creation device, remotely extract a public key from the signature creation device when the key pair has been generated by the signature creation device or/and remotely download a public key certificate and associate it with a private key already stored in the signature creation device.

C.3.14: Provision of harmonized Trust-service status information

Source: ETSI

Reference Number:	**TS 102 231**
Publication Date:	Dec 09
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Trust service status provider
Subarea:	Trust status list
Type of Document:	Tech specs: Format
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document specifies a standard for a Trust-service Status List (TSL) which makes available trust service status information such that interested parties may determine whether a trust service is or was operating under the approval of any recognized scheme at either the time the service was provided, or the time at which a transaction reliant on that service took place.

C.3.15: Signature policy for extended business model

Source: ETSI

Reference Number:	**TR 102 045**
Publication Date:	Mar 03
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on: ETSI TR 102 041	ETSI TS 102 038
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature policies
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document on signature policies elaborates on the signature policy concept (defining the meaning of the signature e.g. what the signature is meant to endorse), addresses certain aspects of multiple signatures (especially with respect to their current application in the paper world) whilst recognizing their applicability in all EC countries and for global trade, and if necessary propose extensions of the standard

C.3.16: XML format for signature policies

Source: ETSI

Reference Number:	**TR 102 038**
Publication Date:	Apr 02
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature policies
Type of Document:	Tech specs: Format
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document represents a very first version of a XML format for Signature Policies able to contain information on Signature Policies as specified by TS 101 733 . The specifications given being so preliminary, a number of open issues for discussion and even definitions appear throughout the document.

C.3.17: Signature Policies Report

Source: ETSI

Reference Number:	**TR 102 041**
Publication Date:	Feb 02
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature policies
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document gives guidance on the technical, organizational and legal issues related to a signature policy. The present document can best be seen in conjunction with published documents TS 101 733 [2] and ES 201 733 [1] upon which it builds.

C.3.18: ASC.4.1 format for signature policies

Source: ETSI

Reference Number:	**TR 102 272**
Publication Date:	Dec 03
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature policies
Type of Document:	Tech specs: Format
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document specifies the various components of a signature policy and one specific format using an ASN.1 syntax and DER encoding.

C.3.19: X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons

Source: ETSI

Reference Number:	**TS 102 280**
Publication Date:	Mar 04
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	ETSI TS 101 862
Framework reference:	
Technical Area:	CSP
Subarea:	CSP Issuing certificates
Type of Document:	Tech specs: Profile
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document defines a common profile for ITU-T Recommendation X.509 based certificates issued to natural persons. The scope of the present document is to provide a certificate profile, which will allow actual interoperability of certificates issued for the purposes of qualified electronic signatures, peer entity authentication and data authentication.

C.3.20: Registered Electronic Mail (REM);Part 1: Architecture

Source: ETSI

Reference Number:	**TS 102 640-1**
Publication Date:	Jan 10
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Registered eMail and eDelivery
Type of Document:	Architecture
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document specifies an architectural structure of Registered E- Mail (REM). The basic purpose of Registered E-Mail service is to provide users, in addition to the usual services supplied by the ordinary e-mail service providers, with a set of Evidence suitable to uphold assertions of acceptance (i.e. of "shipment"), of delivery/non delivery, of retrieval, etc. of e-mails sent/delivered through such service. REM is an trusted service which uses electronic signatures to assure the integrity and authenticity of registered e-mail.

C.3.21: Registered Electronic Mail (REM);Part 2: Data requirements, Formats and Signatures for REM

Source: ETSI

Reference Number:	**TS 102 640-2**
Publication Date:	Jan 10
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Registered eMail and eDelivery
Type of Document:	Protocol
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document provides: a) Rules for building a REM-MD Envelope and, consequently, a REM Dispatch or a REM-MD Message. b) Syntax and semantics of REM-MD Evidence to be produced by a REM Management Domain. c) Rules on the signature to be used within REM-MD Envelopes. The basic purpose of Registered E-Mail service is to provide users, in addition to the usual services supplied by the ordinary e-mail service providers, with a set of Evidence suitable to uphold assertions of acceptance (i.e. of "shipment"), of delivery/non delivery, of retrieval, etc. of e-mails sent/delivered through such service. REM is an trusted service which uses electronic signatures to assure the integrity and authenticity of registered e-mail.

C.3.22: Registered Electronic Mail (REM);Part 3: Information Security Policy Requirements for REM Management Domains

Source: ETSI

Reference Number:	**TS 102 640-3**
Publication Date:	Jan 10
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Registered eMail and eDelivery
Type of Document:	Policy requirements
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document specifies requirements on the security of a Registered E-Mail Management Domain (REM-MD). These requirements are based on the REM-MD operating an Information Security Management System as specified in ISO/IEC 27001 [1]. The basic purpose of Registered E-Mail service is to provide users, in addition to the usual services supplied by the ordinary e-mail service providers, with a set of Evidence suitable to uphold assertions of acceptance (i.e. of "shipment"), of delivery/non delivery, of retrieval, etc. of e-mails sent/delivered through such service. REM is an trusted service which uses electronic signatures to assure the integrity and authenticity of registered e-mail.

C.3.23: Registered Electronic Mail (REM);Part 4: REM-MD Conformance Profiles

Source: ETSI

Reference Number:	**TS 102 640-4**
Publication Date:	Jan 10
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Registered eMail and eDelivery
Type of Document:	Tech specs: Profile
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document specifies two levels of conformance requirements for Registered Electronic Mail (REM): • Basic Conformance Profile that indicates the minimum set of mandatory requirements that are to be met by any REM-MD that claims to be conformant with TS 102 640-1 [1], TS 102 640-2 [2] and TS 102 640-3 [3]; and • Advanced Conformance Profile that includes a set of voluntary additional requirements to the Basic Conformance Profile for enhanced security and advanced evidential services. The basic purpose of Registered E-Mail service is to provide users, in addition to the usual services supplied by the ordinary e-mail service providers, with a set of Evidence suitable to uphold assertions of acceptance (i.e. of "shipment"), of delivery/non delivery, of retrieval, etc. of e-mails sent/delivered through such service. REM is an trusted service which uses electronic signatures to assure the integrity and authenticity of registered e-mail.

C.3.24: Registered Electronic Mail (REM);Part 5: REM-MD Interoperability Profiles

Source: ETSI

Reference Number:	**TS 102 640-5**
Publication Date:	Jan 10
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Registered eMail and eDelivery
Type of Document:	Tech specs: Profile
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document profiles the implementation of TS 102 640 Registered E-Mail based systems, addressing issues relating to authentication, authenticity and integrity of the information to achieve interoperability between such systems.

C.3.25: PDF Advanced Electronic Signature Profiles;Part 1: PAdES Overview - a framework document for PAdES

Source: ETSI

Reference Number:	**TS 102 778-1**
Publication Date:	Jul 09
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	ISO 32000-1
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Architecture
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document provides a framework for the set of profiles for PDF (Portable Document Format - as specified in ISO 32000-1) Advanced Electronic Signatures specified in this multi-part deliverable. This multi-part deliverable profiles and extends the support for electronic signatures specified in ISO 32000-1 to include the enhanced features for advanced electronic signatures. These profiles include features equivalent to those specified in TS 101 733 (CAdES) and TS 101 903 (XAdES) and include support for validation of signed documents stored over long periods.

C.3.26: PDF Advanced Electronic Signature Profiles;Part 2: PAdES Basic - Profile based on ISO 32000-1

Source: ETSI

Reference Number:	**TS 102 778-2**
Publication Date:	Jul 09
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	ISO 32000-1
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Tech specs: Profile
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document profiles the use of PDF signatures, as described in ISO 32000-1 and based on CMS [i.3], for its use in any application areas where PDF is the appropriate technology for exchange of digital documents including interactive forms. This profile does not repeat the base requirements of the referenced standards, but instead aims to maximize interoperability of CMS-based electronic signatures in various business areas.

C.3.27: PDF Advanced Electronic Signature Profiles;Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles

Source: ETSI

Reference Number:	**TS 102 778-3**
Publication Date:	Jul 09
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on: ETSI TS 101 733	ISO 32000-1,
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Tech specs: Profile
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document profiles the use of PDF Signatures specified in ISO 32000-1 with an alternative signature encoding to support signature formats equivalent to the signature forms CAdES-BES, CAdES-EPES and CAdES-T as specified in TS 101 733. The PAdES-BES profile supports basic CMS (RFC 3852) signature features as specified TS 102 778-2 with the additional protection against signing certificate substitution. The PAdES-EPES profile extends the PAdES-BES profile to include signature policies. Both profiles, PAdES-BES and PAdES-EPES allow the inclusion of a signature time stamp creating a signature similar to the CAdES-T form.

C.3.28: PDF Advanced Electronic Signature Profiles;Part 4: PAdES Long Term - PAdES LTV Profile

Source: ETSI

Reference Number:	**TS 102 778-4**
Publication Date:	Dec 09
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	ISO 32000-1
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Tech specs: Profile
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document profiles the electronic signature formats found in ISO 32000-1 to support Long Term Validation (LTV) of PDF Signatures. This profile does not repeat the base requirements of the referenced standards, but instead aims to disambiguate between the techniques used in the different referenced standards. The present document specifies how to include validation information in a PDF Document and to further protect the document using time-stamps so that it is possible to subsequently verify a PDF Signature long after it was signed. This profile may be used to support long term validation of: a) PDF Signatures to profiles specified in TS 102 778-2 ; or b) PDF Signatures to profiles specified in TS 102 778-3; or c) PDF Signatures to profiles specified in TS 102 778-5.

C.3.29: PDF Advanced Electronic Signature Profiles;Part 5: PAdES for XML Content - Profiles for XAdES signatures

Source: ETSI

Reference Number:	**TS 102 778-5**
Publication Date:	Dec 09
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on: ETSI TS 101 903	ISO 32000-1,
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Tech specs: Profile
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document defines four profiles that together profile the usage of XAdES signatures, as defined in TS 101 903, for signing XML content within the PDF containers. The scope of the present document is limited to the following cases: 1) One XML document (compliant with an arbitrary XML language, like UBL for e-Invoicing) that is completely or partially signed with at least one enveloped XAdES signature and that is incorporated within a PDF container as a so-called "embedded" document. In this situation, both the XML document and the XAdES signature(s) are created independently of the PDF container and after their creation, embedded within this container. 2) Signed (with XML Sig or XAdES signature) dynamic XFA (XML forms architecture for PDF) forms. The present document specifies profiles that apply to two different scenarios, namely: signing only the XML data of the XFA form, or signing any part of the XFA form that may be signed with a XML Sig signature.

C.3.30: PDF Advanced Electronic Signature Profiles;Part 6: Visual Representations of Electronic Signatures

Source: ETSI

Reference Number:	**TS 102 778-6**
Publication Date:	Jul 10
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document specifies requirements and recommendations for the visual representations of advanced electronic signatures (AdES) in PDFs. This covers: a) Signature appearance: The visual representation of the human act of signing placed within a PDF document at signing time and linked to an advanced electronic signature; and b) Signature verification representation: The visual representation of the verification of an advanced electronic signature. The aim of the present document is to provide requirements and recommendations for signature appearances and the visual representation of advanced electronic signatures. This is particularly aimed to help the untrained human understanding of the signature and to further consistency between the signature appearance and the visual representations of the AdES verification in order to help human comparison.

C.3.31: Information Preservation Systems Security

Part 1: Requirements for Implementation and Management

Source: ETSI

Reference Number:	**TS 101 533-01**
Publication Date:	
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Long term storage
Type of Document:	Policy requirements
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Ratified
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document addresses the Information Security Management System of Information Preservation Systems, by specifying Security requirements for Information Preservation Service Providers to abide by, when implementing and managing an IPS, in order to provide Information Preservation Services that are trustable and reliable from the Information Security viewpoint.

C.3.32: Information Preservation Systems Security

Part 2: Guidelines for Assessors

Source: ETSI

Reference Number:	**TS 101 533-02**
Publication Date:	
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Long term storage
Type of Document:	Conformity assessment (audit / evaluation)
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Ratified
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document addresses the assessment of the Information Security Management System ("ISMS") of an Information Preservation System, by specifying guidelines for Assessors when reviewing and auditing an IPS.

C.3.33: Associated Signature Containers (ASiC)

Source: ETSI

Reference Number:	**TS 102 918**
Publication Date:	
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on: ETSI TS 101 733, ETSI TS 101 903, RFC 3161	PKWARE ZIP
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	tech specs: Format
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Ratified
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document specifies the use of container structures, to bind together a number of signed objects (e.g. documents, XML structured data, spreadsheet, multimedia content) with either advanced electronic signatures or time-stamp tokens into one single digital container. This uses package formats based on ZIP [8] and supports the following signature and time-stamp token formats: • CAdES (TS 101 733); • XAdES (TS 101 903) detached signature(s); • RFC 3161 time-stamp tokens.

C.3.34: Policy requirements for Certification Service Providers

issuing attribute certificates usable with Qualified certificates

Source: ETSI

Reference Number:	**TS 102 158**
Publication Date:	Oct 03
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP issuing attribute certificates
Type of Document:	Policy requirements
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document specifies policy requirements relating to Attribute Authorities (AAs) which are a type of certification-service-providers as defined in Directive 1999/93/EC. The present document specifies policy requirements on the operation and management practices of Attribute Authorities issuing Attribute Certificates such that subscribers, subjects and relying parties may have confidence in the applicability of the Attribute Certificate in support of electronic signatures.

C.3.35: Requirements for role and attribute certificates

Source: ETSI

Reference Number:	**TS 102 044**
Publication Date:	Dec 02
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP issuing attribute certificates
Type of Document:	tech specs: Format
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document identifies a set of requirements that will provide a basis for a subsequent standard, which will then build policy requirements for attributes certified by Attribute Authorities or Certification Authorities complying with X.509 and related standards. In some electronic signature applications, roles and attributes can be exerted only if a claimer's right to use them is certified by one competent authority which is trusted by the signed document users. The scope of the present document is to investigate on the attribute certification related topics in order to cover the general use of certified attributes in the context of electronic signatures. Attributes that can be used in such a context can also be used for other reasons, e.g. for authorization.

C.3.36: International Harmonization of Electronic Signature Formats

Source: ETSI

Reference Number:	**TR 102 047**
Publication Date:	Mar 05
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature formats
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document presents the results of ongoing work to harmonize existing ETSI technical specifications on electronic signature formats (TS 101 733 [1] and TS 101 903 [2]) with other internationally recognized standards and related activities.

C.3.37: International Harmonization

of Policy Requirements for CAs issuing Certificates

Source: ETSI

Reference Number:	**TR 102 040**
Publication Date:	Mar 05
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP issuing non-qualified certificates
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document presents the results of ongoing work to harmonize existing ETSI Technical Specification (TS) on policy requirements for certification authorities (TS 101 456 [1] and TS 102 042 [2]) with other internationally recognized standards and related activities. The aim of the present document is to identify the way forward to meet the requirements of European Electronic Signature Directive 1999/93/EC [6] whilst operating within an internationally harmonized certificate policy framework to facilitate cross recognition between PKI policy environments.

C.3.38: Best Practices for handling electronic signatures and signed data for digital accounting

Source: ETSI

Reference Number:	**TR 102 572**
Publication Date:	Jul 07
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Digital accounting
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document has the purpose to propose a set of practices applicable to the various security related aspects of signing fiscally relevant documents when issued and storing them for the legally required time. It is based on the results of a survey carried out on what practices are actually in place in the five most populated European Union Member States (France, Germany, Italy, Spain, UK). The present document specifically addresses trust service providers supporting signing and storage services for fiscally relevant documents, regarding business accounting for corporate entities in several European Member States. In particular it is suitable for Value Added Tax (VAT) purposes although it is applicable also to other fiscally relevant documents. The present document does not directly address requirements for accounting for individuals. The practices identified in the present document are independent of the type of document or information being protected. The present document addresses solely the Advanced Electronic Signature based solution. It is recognized that other suitable measures, not employing Advanced Electronic Signatures, and hence are outside the scope of the present document, may be applied to assure the authenticity and integrity of digital accounting documents. It should be noted that the reliability of such alternative measures generally depend on the trustworthiness of the organization and may require independent assessment of the technical and organizational measures applied. Advanced Electronic Signature may be used to augment existing measures to provide even higher security, or to reduce the need for other controls.

C.3.39: Policy requirements for trust service providers signing and/or storing data for digital accounting

Source: ETSI

Reference Number:	**TS 102 573**
Publication Date:	Jul 07
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Digital accounting
Type of Document:	Policy requirements
Level of Standard:	Industry standard
Status:	Technical specification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document specifies policy requirements applicable to Trusted Service Providers (TSP) that sign fiscally relevant electronically documents and/or store them on behalf of taxable persons. The present document aims to address regulatory requirements to produce and reliably keep, even beyond ten years, signed electronic invoices as well as other fiscally relevant documents. The practices identified in the present document are independent of the type of document or information being protected. The present document is directed at policies involving the use of the Advanced Electronic Signatures or Qualified Electronic Signatures. The primary aim of the application of signatures is to protect the integrity and provide data origin authentication of fiscally relevant documents in communication and storage. However, signatures may also be used, where required, to provide content commitment (i.e. non-repudiation). The present document addresses solely the Advanced Electronic Signature based solution. It is recognized that other suitable measures, not employing Advanced Electronic Signatures, and hence that are outside the scope of the present document, may be applied to assure the authenticity and integrity of digital accounting documents. It should be noted that the reliability of such alternative measures generally depend on the trustworthiness of the organization and may require independent assessment of the technical and organizational measures applied. Advanced Electronic Signature may be used to augment existing measures to provide even higher security, or to reduce the need for other controls. The present document may be used by competent independent bodies as the basis for confirming that an organization is trustworthy in issuing and storing signed fiscally relevant electronic document on behalf of other taxable persons or on its own behalf.

C.3.40: Registered E-Mail

Source: ETSI

Reference Number:	**TR 102 065**
Publication Date:	Sep 07
URL:	http://pda.etsi.org/pda/queryform.asp
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	Registered eMail and eDelivery
Type of Document:	Survey
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The present document summarizes the results of a survey among organizations with interests in Registered E-Mail services for Europe including state authorities, standardization bodies, e-mail product and service providers, local experts. The survey included information on Registered E-Mail services outside Europe to place the work within a global context. The survey investigated current and prospective Registered E-Mail implementations with the aim of identifying requirements for standardization in this area.

C.3.41: General requirements for bodies operating product certification systems (ISO/IEC Guide 65:1996)

Source: CEN/CENELEC

Reference Number:	**EN 45011:1998**
Publication Date:	Jun 05
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP certification bodies acreditation
Type of Document:	Requirements
Level of Standard:	European Norm
Status:	European Standard
Maturity:	Published
Geographic general:	European
Geographic details:	
Sector:	

Description:

This European Standard specifies general requirements that a third-party operating a product certification system shall meet if it is to be recognized as competent and reliable. In this European Standard the term "certification body" is used to cover any body operating a product certification system. The word "product" is used in its widest sense and includes processes and services; the word "standard" is used to include other normative documents such as specifications or technical regulations. The certification system used by the certification body may include one or more of the following, which could be coupled with production surveillance or assessment and surveillance of the supplier's quality system or both, as described in ISO/IEC Guide 53: type testing or examination; testing or inspection of samples taken from the market or from supplier's stock or from a combination of both; testing or inspection of every product or of a particular product, whether new or already in use; batch testing or inspection; design appraisal. NOTE 1 ISO/IEC Guide 28 may be consulted for a model of one form of a third-party product certification system.

C.3.42: Application interface for smart cards used as Secure Signature Creation Devices - Part 1: Basic services

Source: CEN

Reference Number:	**14890-1**
Publication Date:	Last published in 2008
URL: Extract can be found here: http://www.evs.ee/Checkout	CEN documents are not for free /tabid/36/screen/freedownload/productid/164744/doclang/en/preview/1/EVS_EN _14890_1;2009_en_preview.aspx
Equivalent to:	-
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	SSCD
Type of Document:	Tech.specs: Protocol
Level of Standard:	European Norm (EN)
Status:	European Norm (EN)
Maturity: Publication planned March	Under Revision 2014
Geographic general:	Europe
Geographic details:	
Sector:	Smart card

Description:

This standard describes an application interface and behavior of the SSCD in the context of Identification, Authentication and Electronic Signature (IAS) services. It will will enable the development of interoperable cards issued by any card industry sector. In Part 1, the standard allows to support the implementation of the European legal framework for electronic signatures, defining the functional and security features for a smart card intended to be used as a Secure Signature Creation Device according to the Terms of the European Directive on Electronic Signature 1999/93. A card compliant to the standard will be able to produce a Qualified electronic signature. that fulfils the requirements of Article 5.1 of the Electronic Signature Directive and therefore can be considered equivalent to hand-written signatures. This part specifies mandatory mechanisms for smart cards to be used as secure signature creation devices covering user verification, signature creation, device authentication, establishment of a secure channel and key generation.

C.3.43: Application interface for smart cards used as Secure Signature Creation Devices - Part 2: Additional services

Source: CEN

Reference Number:	**14890-2**
Publication Date:	Last published in 2008
URL: Extract can be found here: http://www.evs.ee/Checkout	CEN documents are not for free /tabid/36/screen/freedownload/productid/164074/doclang/en/preview/1/EVS_EN _14890_2;2008_en_preview.aspx
Equivalent to:	-
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	SSCD
Type of Document:	Tech.specs: Protocol
Level of Standard:	European Norm (EN)
Status:	European Norm (EN)
Maturity: Publication planned March	Under Revision 2014
Geographic general:	Europe
Geographic details:	
Sector:	Smart card

Description:

This standard describes an application interface and behavior of the SSCD in the context of Identification, Authentication and Electronic Signature (IAS) services. It will will enable the development of interoperable cards issued by any card industry sector. In Part 2, the standard specifies mechanisms to support other services around IAS like Client/Server authentication, Role authentication, Symmetric key transmission between a remote server and a smart card, and signature verification.

C.3.44: Identification card systems -European Citizen Card -Part 0: General Introduction

Source: CEN

Reference Number:	**15480-0**
Publication Date:	Publication planned Q1 2012
URL:	Not available yet
Equivalent to:	-
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	SSCD
Type of Document:	General Description
Level of Standard:	Industry standard
Status:	Technical specification (TS)
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	Government

Description:

The scope of this part of the standard is to provide a general description of the standard together with an introduction to each part of the standard. In addition, this part of the standard explains the use in other parts of the standard of some of commonly referred to concepts such as interoperability and privacy. Informative Annex A introduces various usage scenarios for the ECC as a Framework for ECC Deployment which are referred to and detailed in other parts of the standard (primarily Part 4). Informative Annex B maps the relationship between the various parts of the ECC standard and other ISO/IEC standards relating to the card platform. Informative Annex C identifies other European initiatives relevant to the ECC

C.3.45: Identification card systems -European Citizen Card -Part 1: Physical, electrical and transport protocol characteristics

Source: CEN

Reference Number:	**15480-1**
Publication Date:	Last published in 2007.
URL: Extract can be found here: http://www.evs.ee/Checkout	CEN documents are not for free /tabid/36/screen/freedownload/productid/165215/doclang/en/preview/1/CEN_TS _15480_1;2007_en_preview.aspx
Equivalent to:	-
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	SSCD
Type of Document:	Tech.specs: Format
Level of Standard:	Industry standard
Status:	Technical specification (TS)
Maturity: Publication planned Februa	Under Revision ry 2012
Geographic general:	Europe
Geographic details:	
Sector:	Government

Description:

This Technical Specification describes the specifications for the European Citizen Card (ECC) including electronic identity cards, with smart card format, defining identity justification with emphasis on remote civil service procedures requiring the generation and/or verification by the ECC card of electronic signatures and electronic certificates. In particular it defines a plastic body card with associated physical and logical securities, specifies the electrical interface and data transport protocols for the ECC and supports the basic set of Identification and, authentication elements visible at the card surface. Part 1 also contains a possible methodology for ECC durability testing in informative Annex B as well as a recommended Physical Layouts for cards

C.3.46: Identification card systems - European Citizen Card -Part 2: Logical data structures and card services

Source: CEN

Reference Number:	**15480-2**
Publication Date:	Last published in 2007.
URL: Extract can be found here: http://www.evs.ee/Checkout	CEN documents are not for free /tabid/36/screen/freedownload/productid/165216/doclang/en/preview/1/CEN_TS _15480_2;2007_en_preview.aspx
Equivalent to:	-
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	SSCD
Type of Document:	Tech.specs: Protocols
Level of Standard:	Industry standard
Status:	Technical specification (TS)
Maturity: Publication planned Februa	Under Revision ry 2012
Geographic general:	Europe
Geographic details:	
Sector:	Government

Description:

This Technical Specification specifies the logical characteristics and security features at the card/system interface for the European Citizen Card (ECC). Part 2 fully defines a series of Applicative Profiles corresponding to typical use cases for the ECC. For each Application Profile a list of supported services (with the notion of mandatory and optional features), supported data structures and command set is specified. Part 2 also provides other features including biometric on card matching, command chaining, role authentication ….

C.3.47: Identification card systems - European citizen card - Part 3: ECC interoperability using an application interface

Source: CEN

Reference Number:	**15480-3**
Publication Date:	December 2010
URL: Extract can be found here: http://www.evs.ee/Checkout	CEN documents are not for free /tabid/36/screen/freedownload/productid/197754/doclang/en/preview/1/CEN_TS_15480_3;2010_en_preview.aspx
Equivalent to:	-
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	SSCD
Type of Document:	Tech.specs: Protocols
Level of Standard:	Industry standard
Status:	Technical specification (TS)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	Government

Description:

This Technical Specification provides an Interoperability Model , which will enable an eService compliant with technical requirements, to interoperate with different implementations of the ECC. Starting from Part 2, Part 3 provides additional technical specifications for a middleware architecture based first on ISO/IEC 24727 and second on Web Service.

C.3.48: Identification card systems - European citizen card - Part 4: Recommendations for ECC issuance, operation and use

Source: CEN

Reference Number:	**15480-4**
Publication Date:	
URL:	CEN documents are not for free
Equivalent to:	-
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	SSCD
Type of Document:	Tech.specs: Profiles
Level of Standard:	Industry standard
Status:	Technical specification (TS)
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	Government

Description:

This Technical Specification recommends card issuance and operational procedures including citizen registration. Part 4 gives specific recommendations with regard to the end user relating to data protection, accessibility and usability issues. Part 4 also identifies a set of standard ECC card profiles (e.g. for national ID card, signature card, electronic services card) to facilitate the deployment of interoperable solutions. For each card profile the standard selects a subset of technical requirements from ECC parts 1, 2 and 3.

C.3.49: EESSI Conformity Assessment Guidance - Part 1: General introduction

Source: CEN

Reference Number:	**14172-1**
Publication Date:	March 2004
URL:	ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-01-2004-Mar.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP conformance assessment
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

This document provides the rationale for the guidance on conformity assessment concerning the services, processes, systems and products addressed by the following EESSI generally recognised standards related to electronic signatures,

C.3.50: EESSI Conformity Assessment Guidance - Part 2: Certification Authority services and processes

Source: CEN

Reference Number:	**14172-2**
Publication Date:	March 2004
URL:	ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-02-2004-Mar.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP conformance assessment
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The purpose of this CWA is to provide guidance with a view to harmonise the application of the standards for services, processes, systems and products for Electronic Signatures. The CWA is intended for use by certification-service-providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories involved in assessing conformance to the related EESSI deliverables. Part 2 provides guidance on conformity assessment of Certification Authorities (CAs) against the following standards: · ETSI TS 101 456 “Policy requirements for certification authorities issuing qualified certificates”; · ETSI TS 102 042 “Policy requirements for certification authorities issuing public key certificates”.

C.3.51: EESSI Conformity Assessment Guidance - Part 3: Trustworthy sustems managing certificates for electronic signatures

Source: CEN

Reference Number:	**14172-3**
Publication Date:	March 2004
URL:	ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-03-2004-Mar.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	conformance assessment of signing devices
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The purpose of this CWA is to provide guidance with a view to harmonise the application of the standards for services, processes, systems and products for Electronic Signatures. The CWA is intended for use by certification-service-providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories involved in assessing conformance to the related EESSI deliverables. Part 3 provides guidance on conformity assessment of Trustworthy Systems against the standard CWA 14167-1 “Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements”.

C.3.52: EESSI Conformity Assessment Guidance - Part 4: Signature-creation applications and general guidelines for electronic signature verification

Source: CEN

Reference Number:	**14172-4**
Publication Date:	March 2004
URL:	ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-04-2004-Mar.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	conformance assessment of signing devices
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The purpose of this CWA is to provide guidance with a view to harmonise the application of the standards for services, processes, systems and products for Electronic Signatures. The CWA is intended for use by certification-service-providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories involved in assessing conformance to the related EESSI deliverables. Part 4 provides guidance on conformity assessment of products, systems and applications against the specifications CWA 14170 “Security Requirements for Signature Creation Applications” and CWA 14171 “General Guidelines for Electronic Signature Verification”.

C.3.53: EESSI Conformity Assessment Guidance - Part 5: Secure signature-creation devices

Source: CEN

Reference Number:	**14172-5**
Publication Date:	March 2004
URL:	ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-05-2004-Mar.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	conformance assessment of signing devices
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The purpose of this CWA is to provide guidance with a view to harmonise the application of the standards for services, processes, systems and products for Electronic Signatures. The CWA is intended for use by certification-service-providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories involved in assessing conformance to the related EESSI deliverables. Part 5 provides guidance on conformity assessment of Secure Signature Creation Devices against the specification CWA 14169 “Secure Electronic Signature Devices, version EAL4+”.

C.3.54: EESSI Conformity Assessment Guidance - Part 6: Signature-creation device supporting signatures other than qualified

Source: CEN

Reference Number:	**14172-6**
Publication Date:	March 2004
URL:	ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-06-2004-Mar.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	conformance assessment of signing devices
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The purpose of this CWA is to provide guidance with a view to harmonise the application of the standards for services, processes, systems and products for Electronic Signatures. The CWA is intended for use by certification-service-providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories involved in assessing conformance to the related EESSI deliverables. Part 6

C.3.55: EESSI Conformity Assessment Guidance - Part 7: Cryptographic modules used by Certification Service Providers for signing operations and key generation services

Source: CEN

Reference Number:	**14172-7**
Publication Date:	March 2004
URL:	ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-07-2004-Mar.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	conformance assessment of signing devices
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The purpose of this CWA is to provide guidance with a view to harmonise the application of the standards for services, processes, systems and products for Electronic Signatures. The CWA is intended for use by certification-service-providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories involved in assessing conformance to the related EESSI deliverables. Part 7 provides guidance on conformity assessment of cryptographic modules used by CSPs for signing operations and key generation services against the following standards: · CWA 14167-2 "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 2: Cryptographic Module for CSP Signing Operations with Backup - Protection Profile (CMCSOB-PP)"; · CWA 14167-3 "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 3: Cryptographic Module for CSP Key Generation Services - Protection Profile (CMCKG-PP)"; · CWA 14167-4 "Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 4: Cryptographic Module for CSP Signing Operations — Protection Profile (CMCSOPP)".

C.3.56: EESSI Conformity Assessment Guidance - Part 8: Time-stamping Authority services and processes

Source: CEN

Reference Number:	**14172-8**
Publication Date:	March 2004
URL:	ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14172-08-2004-Mar.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	Policy Requirements of Other CSP serviczs supporting electronic signautres including time-stamping
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The purpose of this CWA is to provide guidance with a view to harmonise the application of the standards for services, processes, systems and products for Electronic Signatures. The CWA is intended for use by certification-service-providers, manufacturers, operators, independent bodies, assessors, evaluators and testing laboratories involved in assessing conformance to the related EESSI deliverables. Part 8 provides guidance on conformity assessment of Time-stamping Authorities (TSAs) against the following standard: · ETSI TS 102 023 “Policy requirements for time-stamping authorities”.

C.3.57: Guidelines for the implementation of Secure Signature-Creation Devices

Source: CEN

Reference Number:	**14355**
Publication Date:	March 2004
URL:	ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14355-00-2004-Mar.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	Protection Profile for SSCD
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The document gives guidance on the implementation of SSCD PP for specific platforms (e.g. smartcards, personal data assistants, mobile phones, or PCs) and the operation in specific environments (e.g. public terminals or secured environments). A further objective of the document is to compare SSCD PP to similar PPs or other well established evaluation standards. The document limits its scope to electronic signatures based on asymmetric cryptography, i.e. to digital signatures based on private key – public key

C.3.58: Guide on the Use of Electronic Signatures - Part 1: Legal and Technical Aspects

Source: CEN

Reference Number:	**14365-1**
Publication Date:	March 2004
URL:	ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14365-01-2004-Mar.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signing Devices
Subarea:	
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The purpose of this CWA is to give guidance on the use of electronic signatures. Whilst the focus often has been on "qualified electronic signatures" as specified in Article 5.1 of the Directive, a side effect was that the requirements of employing general electronic signatures (referred to as "5.2 signatures") in e-commerce were not sufficiently addressed. The purpose of this part of the CWA is therefore to describe the general legal and technical aspects of electronic signatures, and thus extend the work to e-commerce scenarios, paying special attention to technologies with a high deployment capacity, to enable trust, without the need to meet all the strict requirements for "Article 5.1 Signatures". Part 1 is on the latter –electronic signatures that do not fulfil all the requirements laid down for qualified electronic signatures in article 5.1 of the Directive. The document therefore analyses the differences between cryptographic mechanism of digital signatures, qualified electronic signatures (according to article 5.1 of the Directive), and electronic signatures (according to article 5.2 of the Directive). In addition, a set of use cases of electronic signatures which do not fulfil some of the requirements laid down in article 5.1 are discussed in order to point out its effectiveness in ecommerce environments or in various application fields asking for authentication measures. In addition to the use cases, the evidence that is provided by electronic signatures is discussed. The electronic signatures and certification-services are broken up into its basic elements and the proof provided by each element is discussed from a legal perspective in order to establish the coherence between the technical elements and its legal effect.

C.3.59: General guidelines for electronic signature verification

Source: CEN

Reference Number:	**14171**
Publication Date:	May 2004
URL:	ftp://ftp.cen.eu/CEN/Sectors/TCandWorkshops/Workshops/eSIGN_CWAs/cwa14171-00-2004-May.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation and verification
Subarea:	Signature verification
Type of Document:	Guidelines and Recommendations
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

This document sets out general guidelines on the recommended functionality and assurances for electronic signature verification, in the light of the recommendations in Annex IV from Dir.1999/93/EC and in the interest of the consumer. Its primary purpose is to provide guidance on the way to verify qualified electronic signatures that are equivalent to handwritten signatures according to Article 5.1 of Dir.1999/93/EC , and to complement them with additional data that may help in assessing their validity long after their signing time. Signatures with such additional data have been called “Enhanced Electronic Signatures”.

C.3.60: Security requirements for trustworthy systems managing certificates for electronic signatures - Part 1: System security requirements

Source: CEN

Reference Number:	**14167-1**
Publication Date:	Jun 03
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	Tech. specs: Security requirements
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

This CWA is specifically relevant for manufacturers of Trustworthy Systems (TWSs) used for managing certificates, but may be adopted by anyone deploying trusted systems and wanting to meet the requirements of [Dir.1999/93/EC]. It provides an overview of a CSP system broken down into a number of services. Some of these services are mandatory, termed ‘Core Services' whereas others are optional, ‘Supplementary Services'. Core Services covers the following CSP services: • Registration Service - to verify the identity and, if applicable, any specific attributes of a Subject • Certificate Generation Service - to create certificates; • Dissemination Service - to provide certificates and policy information to Subjects and Relying Parties; • Revocation Management Service - to allow the processing of revocation requests; • Revocation Status Service - to provide certificate revocation status information to relying parties. Supplementary Services covers two optional CSP services: • Subject Device Provision Service – to prepare and provide a Signature Creation Device (SCDev) to Subjects. This includes Secure-Signature-Creation Device (SSCD) provision; • Time-stampingService – provides a Time-stamping Service which may be needed for signature verification purposes.

C.3.61: Cryptographic Module for CSP Signing Operations with Backup – Protection Profile (CMCSOB-PP)

Source: CEN

Reference Number:	**14167-2**
Publication Date:	May 04
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

CC2.3 EAL4+ AVA_VLA.4 Certified by ANSSI under PP0308

C.3.62: Cryptographic Module for CSP Key Generation Services – Protection Profile (CMCKG-PP)

Source: CEN

Reference Number:	**14167-3**
Publication Date:	May 04
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

CC2.3 EAL4+ AVA_VLA.4 Not certified

C.3.63: Cryptographic Module for CSP Signing Operations – Protection Profile (CMCSO-PP)

Source: CEN

Reference Number:	**14167-4**
Publication Date:	May 04
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

CC2.3 EAL4+ AVA_VLA.4 Certified by ANSSI under PP0309

C.3.64: Secure Signature-Creation Devices "EAL4"

Source: CEN

Reference Number:	**14168**
Publication Date:	07/2001
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signing devices
Subarea:	Protection Profile for SSCD
Type of Document:	
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

CC2.3 EAL4:AVLA_VLA.2 Not certified Same as CWA 14169, but lower EAL

C.3.65: Secure signature-creation devices “EAL 4+”

Source: CEN

Reference Number:	**14169**
Publication Date:	03/2004
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signing devices
Subarea:	Protection Profile for SSCD
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

This document specifies the security requirements for a SSCD which is the TOE. It is formulated as three Protection Profiles (PPs) following the rules and formats of the Common Criteria [cc211]. SSCDs are mandatory for implementing signatures fulfilling the requirements of Article 5.1 of the EU Directive. The PPs are an integral part of this document and included as normative Annexes A, B and C. The Protection Profiles themselves have been evaluated according to Common Criteria and certified by BSI, Germany. The Protection Profiles have been registered as follows: - Protection Profile - Secure Signature-Creation Device Type 1, Version 1.05 EAL 4+ BSI-PP-0004-2002 03.04.2002 - Protection Profile - Secure Signature-Creation Device Type 2, Version 1.04 EAL 4+ BSI-PP-0005-2002 03.04.2002 - Protection Profile - Secure Signature-Creation Device Type 3, Version 1.05 EAL 4+ BSI-PP-0006-2002 03.04.2002

CC2,3 EAL4+: AVLA_VLA.4

C.3.67: Protection profiles for Secure signature creation device – Part1: Overview

Source: CEN

Reference Number:	**14169-1**
Publication Date:	Mid 2012
URL:	
Equivalent to:	
Based on:	CWA 14169
Framework reference:	
Technical Area:	Signing devices
Subarea:	Protection Profile for SSCD
Type of Document:	Tech. specs: Security requirements
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

Part 1 is an introduction.

C.3.68: Protection profiles for Secure signature creation device – Part2: Device with key generation

Source: CEN

Reference Number:	**14169-2**
Publication Date:	Mid 2012
URL:	
Equivalent to:	
Based on:	CWA 14169
Framework reference:	
Technical Area:	Signing devices
Subarea:	Protection Profile for SSCD
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

Part 2 of this series of European standards specifies a protection profile for an SSCD that performs its core operations including the generation of signature keys in the device. An SSCD that fulfils only the security requirements in this protection profile may be operated in a secure environment to create either an advanced electronic signature or a qualified electronic signature. Part 2, with it extensions EN 14169-4 and EN 14169-5, aim at replacing CWA 14169 type 3. It is certified

C.3.69: Protection profiles for Secure signature creation device – Part3: Device with key import

Source: CEN

Reference Number:	**14169-3**
Publication Date:	Mid 2012
URL:	
Equivalent to:	
Based on:	CWA 14169
Framework reference:	
Technical Area:	Signing devices
Subarea:	Protection Profile for SSCD
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

Part 3 of this series of European standards specifies a protection profile for an SSCD that performs its core operations including import of the signature key generated in a trusted manner outside the device. An SSCD that fulfils only the security requirements in this protection profile may be operated in a secure environment to create either an advanced electronic signature or a qualified electronic signature. Part 3, with it extension EN 14169-6, aim at replacing CWA 14169 type 2.

C.3.70: Protection profiles for Secure signature creation device – Part4: Extension for device with key generation and trusted communication with certificate generation application

Source: CEN

Reference Number:	**14169-4**
Publication Date:	Mid 2012
URL:	
Equivalent to:	
Based on:	CWA 14169
Framework reference:	
Technical Area:	Signing devices
Subarea:	Protection Profile for SSCD
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

Part 4 of this series of European standards specifies an extension protection profile for an SSCD with key generation that support establishing a trusted channel with a certificate-generating application.

C.3.71: Protection profiles for Secure signature creation device – Part5: Extension for device with key generation and trusted communication with signature creation application

Source: CEN

Reference Number:	**14169-5**
Publication Date:	Mid 2012
URL:	
Equivalent to:	
Based on:	CWA 14169
Framework reference:	
Technical Area:	Signing devices
Subarea:	Protection Profile for SSCD
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

Part 5 of this series of European standards specifies an extension protection profile for an SSCD with key generation that additionally supports establishing a trusted channel with a signature-creation application.

C.3.72: Protection profiles for Secure signature creation device – Part6: Extension for device with key import and trusted communication with signature creation application

Source: CEN

Reference Number:	**14169-6**
Publication Date:	Mid 2012
URL:	
Equivalent to:	
Based on:	CWA 14169
Framework reference:	
Technical Area:	Signing devices
Subarea:	Protection Profile for SSCD
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

Part 6 of this series of European standards specifies an extension protection profile for an SSCD with key import that additionally supports establishing a trusted channel with a signature-creation application.

C.3.73: Guide on the Use of Electronic Signatures - Part 2: Protection Profile for Software

Signature Creation Devices

Source: CEN

Reference Number:	**14365-2**
Publication Date:	May 04
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signing devices
Subarea:	Protection Profile for SW signature
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

This document is a PP for Software signature creation devices. EAL3: AVA_VLA.1 Key generation Signature generation TC with CGA for SVD export

C.3.74: Security requirements for device for authentication - Part 1: Protection Profile for core functionality

Source: CEN

Reference Number:	**16248-1**
Publication Date:	End 2012
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	Protection Profile for authentication device
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The aimed objective is to define security requirements that an authentication device shall conform to in the perspective of a security evaluation. The Target of Evaluation (TOE) considered in this PP corresponds to a hardware device (such as, for example, a smart card or USB token) allowing its legitimate holder to authenticate himself when accessing an on-line service or to guarantee the origin authentication of data sent by the User to a distant agent. Part1 defines a PP for a device with only the core features and key import. It is the minimum product. The requirements present in this PP define the minimum security rules an ST of an authentication device shall conform to but are in no way exhaustive. It remains indeed possible to add functionalities or also refer to another PP. • Core group applies to all Configurations. It contains the basic security features for all Authentication devices. • KeyImp group contains the security features directly linked to the import of the Authentication Private Key into the card.

C.3.75: Security requirements for device for authentication - Part 2: Protection Profile for extension for trusted channel to certificate generation application

Source: CEN

Reference Number:	**16248-2**
Publication Date:	End 2012
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	Protection Profile for authentication device
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The aimed objective is to define security requirements that an authentication device shall conform to in the perspective of a security evaluation. The Target of Evaluation (TOE) considered in this PP corresponds to a hardware device (such as, for example, a smart card or USB token) allowing its legitimate holder to authenticate himself when accessing an on-line service or to guarantee the origin authentication of data sent by the User to a distant agent. Part2 defines a PP for a device with key import, key generation, trusted channel with the CA, trusted channel with the Administration application, and administration; • Core group applies to all Configurations. It contains the basic security features for all Authentication devices. • KeyImp group contains the security features directly linked to the import of the Authentication Private Key into the card. • Admin group contains the security features directly linked to the following Administration functions, which take place during the Usage phase: o Import and export of the public key and certificate by administrator. o Storage and export of log data by administrator. o Reset of Holder authentication failures counter by administrator. • Untrusted CA group contains the security features directly linked to the transfer of sensitive data between the CA and the TOE when these transfers do not take place in a protected environment. This means that the TOE has to establish a trusted channel with the CA. • Untrusted AdminAppli group contains the security features directly linked to the transfer of sensitive data between the Administration application and the TOE when these transfers do not take place in a protected environment. This means that the TOE has to establish a trusted channel with the Administration application.

C.3.76: Security requirements for device for authentication - Part 3: Additional functionality for security targets

Source: CEN

Reference Number:	**16248-3**
Publication Date:	End 2012
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	Protection Profile for authentication device
Type of Document:	Tech. specs: Security requirements
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

The aimed objective is to define security requirements that an authentication device shall conform to in the perspective of a security evaluation. The Target of Evaluation (TOE) considered in this PP corresponds to a hardware device (such as, for example, a smart card or USB token) allowing its legitimate holder to authenticate himself when accessing an on-line service or to guarantee the origin authentication of data sent by the User to a distant agent. Part3 defines additional features that can be added to part 1 or part2 in order to define a new PP with enhanced features.

C.3.77: Protection profiles for signature creation and verification application – Part1: Introduction to the European Norm

Source: CEN

Reference Number:	**14170-1**
Publication Date:	End 2013
URL:	
Equivalent to:	
Based on:	CWA 14170
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Protection Profile for SCA/SVA
Type of Document:	Tech. specs: Security requirements
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

This EN contains Protection Profiles that define the security requirements for Signature Creation Applications (SCA) and Signature Verification applications (SVA). Part1 is an introduction to the European Norm that contains Protection Profiles that define the security requirements for Signature Creation (SCA) and Signature Verification (SVA) applications, including its functions and its environment.

C.3.78: Protection profiles for signature creation and verification application – Part2: Signature creation application - Core PP

Source: CEN

Reference Number:	**14170-2**
Publication Date:	End 2013
URL:	
Equivalent to:	
Based on:	CWA 14170
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Protection Profile for SCA/SVA
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

This EN contains Protection Profiles that define the security requirements for Signature Creation Applications (SCA) and Signature Verification applications (SVA). Part2 is the core PP for an SCA, defining security requirements that an SCA shall conform to in the perspective of a security evaluation. The Target of Evaluation (TOE) considered in this PP corresponds to software, running on an operating system and hardware, the SCP. The TOE, using services provided by the SCP and by an SSCD allows the signatory to generate an electronic signature.

C.3.79: Protection profiles for signature creation and verification application – Part3: Signature creation application - Possible Extensions

Source: CEN

Reference Number:	**14170-3**
Publication Date:	End 2013
URL:	
Equivalent to:	
Based on:	CWA 14170
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Protection Profile for SCA/SVA
Type of Document:	Tech. specs: Security requirements
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

This EN contains Protection Profiles that define the security requirements for Signature Creation Applications (SCA) and Signature Verification applications (SVA). Part3 proposes extensions to Part2.

C.3.80: Protection profiles for signature creation and verification application – Part4: Signature verification application - Core PP

Source: CEN

Reference Number:	**14170-4**
Publication Date:	End 2013
URL:	
Equivalent to:	
Based on:	CWA 14170
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Protection Profile for SCA/SVA
Type of Document:	Protection Profile
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

This EN contains Protection Profiles that define the security requirements for Signature Creation Applications (SCA) and Signature Verification applications (SVA). Part4 is the core PP for an SVA, defining security requirements that an SVA shall conform to in the perspective of a security evaluation. The Target of Evaluation (TOE) considered in this PP corresponds to software, running on an operating system and hardware, the SVP. The TOE, using services provided by the SVP and by the environment allows the verifier to check an electronic signature.

C.3.81: Protection profiles for signature creation and verification application – Part5: Signature verification application - Possible Extensions

Source: CEN

Reference Number:	**14170-5**
Publication Date:	End 2013
URL:	
Equivalent to:	
Based on:	CWA 14170
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Protection Profile for SCA/SVA
Type of Document:	Tech. specs: Security requirements
Level of Standard:	Industry standard
Status:	EN
Maturity:	Draft
Geographic general:	Europe
Geographic details:	
Sector:	

Description:

This EN contains Protection Profiles that define the security requirements for Signature Creation Applications (SCA) and Signature Verification applications (SVA). Part5 proposes extensions to Part4.

C.4 National and Sector

C.4.1: Personal Identity Verification (PIV) of Federal Employees and Contractors

Source: NIST

Reference Number:	**FIPS PUB 201-1**
Publication Date:	Mar 06
URL:	http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Covers more than 1 area
Subarea:	Generic
Type of Document:	
Level of Standard:	National standard
Status:	Federal Information Processing Standards
Maturity:	Under revision
Geographic general:	Non EU nation
Geographic details:	USA
Sector:	Government

Description:

This standard specifies the architecture and technical requirements for a common identification standard for Federal employees and contractors. The overall goal is to achieve appropriate security assurance for multiple applications by efficiently verifying the claimed identity of individuals seeking physical access to Federally controlled government facilities and electronic access to government information systems. Features of a FIPS 201 device is digital signatures. Associated with FIPS 201 are a range of special publications which specifies further technical requirements including: - SP 800-78 Cryptographic Algorithms and Key Sizes for PIV - SP 800-73 Interfaces for Personal Identity Verification - SP 800-76 Biometric Data Specification for Personal Identity Verification - SP 800-104 A Scheme for PIV Visual Card Topography - SP 800-96 PIV Card / Reader Interoperability Guidelines - SP 800-79 Guidelines for the Accreditation of Personal Identity Verification (PIV) Card Issuers (PCI's)

C.4.2: Security Requirements for Cryptographic Modules

Source: NIST

Reference Number:	**FIPS 140-2**
Publication Date:	May 01
URL:	http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf
Equivalent to:	ISO/IEC 19790
Based on:	
Framework reference:	
Technical Area:	Signing devices
Subarea:	HSM
Type of Document:	Security requirements
Level of Standard:	National standard
Status:	Federal Information Processing Standards
Maturity:	Under revision
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies the security requirements for a cryptographic module utilized within a security system protecting sensitive information in computer and telecommunication systems. This document defines four security levels for cryptographic modules to provide for a wide spectrum of data sensitivity (e.g., low value administrative data, million dollar funds transfers, and life protecting data) and a diversity of application environments (e.g., a guarded facility, an office, and a completely unprotected location). Four security levels are specified for each of 10 requirement areas. Each security level offers an increase in security over the preceding level. While the security requirements specified in this International Standard are intended to maintain the security provided by a cryptographic module, compliance to this document is not sufficient to ensure that a particular module is secure or that the security provided by the module is sufficient and acceptable to the owner of the information that is being protected.

C.4.3: Certificate management for financial services -- Part 1: Public key certificates

Source: ISO TC 68

Reference Number:	**ISO 15782-1**
Publication Date:	Jul 05
URL:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=46547
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP issuing non-qualified certificates
Type of Document:	Tech specs: Profile
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	Banking

Description:

ISO 15782-1:2009 defines a certificate management system for financial industry use for legal and natural persons that includes: • credentials and certificate contents, • Certification Authority systems, including certificates for digital signatures and for encryption key management, • certificate generation, distribution, validation and renewal, • authentication structure and certification paths, and • revocation and recovery procedures. ISO 15782-1:2009 also recommends some useful operational procedures (e.g. distribution mechanisms, acceptance criteria for submitted credentials).

ISO 15782-1:2009 does not include: • the protocol messages used between the participants in the certificate management process, • requirements for notary and time stamping, • Certificate Policy and Certification Practices requirements, or • Attribute Certificates. While ISO 15782-1:2009 provides for the generation of certificates that could include a public key used for encryption key management, it does not address the generation or transport of keys used for encryption.

C.4.4: Banking -- Certificate management -- Part 2: Certificate extensions

Source: ISO TC 68

Reference Number:	**15782-2**
Publication Date:	Jun 05
URL:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=30969
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP issuing non-qualified certificates
Type of Document:	Format
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	Banking

Description:

This part of ISO 15782 extracts and adopts selected definitions of certificate extensions from ISO/IEC 9594-8; specifies additional requirements when certificate extensions are used by the financial services industry. This part of ISO 15782 is to be used with financial institution standards, including ISO 15782-1.

C.4.5: Public key infrastructure for financial services -- Practices and policy framework

Source: ISO TC 68

Reference Number:	**21188**
Publication Date:	Jun 05
URL:	http://www.iso.org/iso/catalogue_detail?csnumber=35707
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	CSP
Subarea:	CSP issuing non-qualified certificates
Type of Document:	Policy requirements
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	Banking

Description:

ISO 21188:2006 sets out a framework of requirements to manage a PKI through certificate policies and certification practice statements and to enable the use of public key certificates in the financial services industry. It also defines control objectives and supporting procedures to manage risks.

ISO 21188:2006 draws a distinction between PKI systems used in open, closed and contractual environments. It further defines the operational practices relative to financial services industry accepted information systems control objectives. ISO 21188:2006 is intended to help implementers to define PKI practices that can support multiple certificate policies that include the use of digital signature, remote authentication and data encryption.

ISO 21188:2006 facilitates the implementation of operational, baseline PKI control practices that satisfy the requirements for the financial services industry in a contractual environment. While the focus of ISO 21188:2006 is on the contractual environment, application of this document to other environments is not specifically precluded. For the purposes of this document, the term "certificate" refers to public key certificates. Attribute certificates are outside the scope of ISO 21188:2006.

C.4.6: tScheme Approval profiles for PKI-related Services

Source: tScheme

Reference Number:	**tSd0102**
Publication Date:	
URL:	http://www.tscheme.org/profiles/CA_digest_3.html#ca
Equivalent to:	
Based on:	ISO 27000
Framework reference:	
Technical Area:	CSP
Subarea:	CSP Issuing Certificates
Type of Document:	Policy requirements
Level of Standard:	National standard
Status:	Technical specification
Maturity:	Published
Geographic general:	EU nation
Geographic details:	UK
Sector:	

Description:

The tScheme approval profiles cover the criteria against which Electronic Trust Service Providers are assessed when applying for a tScheme Grant of Approval (c.f. CSP Accrediation). The most relevant profile is: Approval Profile for a Certification Authority [[QC: issuing Qualified Certificates]] - tSd 0102 (Issue 3.01)

The criteria given in this Approval Profile are related to the overall provision and life-cycle management of certification services [[QC: issuing Qualified Certificates]]. Life-cycle management provides for Services supporting the registration and verification of key holders, initial creation and personalisation of encryption keys, tokens and certificates, the secure distribution of keys/tokens and publication of certificates, the maintenance of certificate currency and validity through re-certification and revocation processes.

C.4.7: Approval Scheme for EPC Approved CAs for e-Mandate Services

Source: EPC

Reference Number:	**EPC292-09**
Publication Date:	Feb 11
URL:	http://www.europeanpaymentscouncil.eu/knowledge_bank_detail.cfm?documents_id=486
Equivalent to:	
Based on:	ETSI TS 102 231
Framework reference:	
Technical Area:	CSP
Subarea:	CSP issuing non-qualified certificates
Type of Document:	Conformity assessment (audit / evaluation)
Level of Standard:	Industry standard
Status:	Technical sepcification
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	Banking

Description:

According to the EPC June 2009 Plenary decision on the recommendation on the establishment and the Governance of "EPC Approved Certification Authorities" in support of the e-Mandates Scheme for SEPA Direct Debit, EPC will allow any established CA, which has been approved by the EPC according to the dedicated approval process for e-Mandate Service CAs, to provide certificates to the market. The technical requirements and specifications for the CA services are described in a separate document "Requirements and Specification for EPC Approved Server CAs for e-Mandate Services" (EPC291-09) . The present document aims to specify the EPC approval process for these CAs.

The EPC follows the general approach of multiple CAs, each offering one or more CA services, with the establishment of a so-called Trust-Service Status List (TSL) for e-Mandate Services (based on ETSI 102 231) that contains all relevant public key certificates of all EPC Approved CAs for e-Mandate Services. EPC has contracted a Trust Body to establish and maintain this TSL, known as the "TSL Trust Body".

C.4.8: Signatures and Authentication for Everyone (SAFE-BioPharma) Standard

Source: SAFE

Reference Number:

Publication Date:
URL: http://www.safe-biopharma.org/
Equivalent to:
Based on:
Framework reference:
Technical Area: Covers more than 1 area
Subarea:
Type of Document:
Level of Standard: Industry standard
Status: Technical specification
Maturity: Published
Geographic general: International
Geographic details:
Sector: biopharmaceutical and healthcare
Description:

The Signatures and Authentication for Everyone (SAFE□BioPharma) Standard provides the framework for assured identity and a legally binding, regulatory compliant digital signature. The scope of this framework is business□to□business and business□to□government transactions across the bio□pharmaceutical community. The SAFE□BioPharma Standard provides the framework for strong authentication events at levels 2 and 3 assurance as define in NIST SP 800□63. SAFEBioPharma Subscriber Systems, as implemented by SAFE□BioPharma, represent a key SAFEBioPharma technology group for achieving the objectives noted below: • Reduce Industry barriers to SAFE□BioPharma adoption by both large and small participants by limiting the required internal infrastructure investment by each SAFE□BioPharma Member • Protect a Subscriber's Credential from compromise. • Establish uniform levels of trust for identity credentials by ensuring uniform protections of and controls for use. • Minimize the potential for legal repudiation of a SAFE□BioPharma transactions based on undetected compromise or use of the credential.

C.4.9: eInvoicing & Digital Signatures

Source: CEN

Reference Number:	**15579**
Publication Date:	October 2007
URL:	ftp://ftp.cenorm.be/PUBLIC/CWAs/e-Europe/eInvoicing/CWA15579-00-2007-Oct.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying electronic signatures
Subarea:	eInvoicing
Type of Document:	Finding and issues
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	e-trade

Description:

Electronic signatures are a valuable technique to ensure the integrity and authenticity of electronic business data such as invoices. This value, which is based on electronic signatures – under certain conditions – providing integrity and authenticity assurances regardless of time and type of electronic (transport or storage) medium, has been recognized within the EU through the e-Signature Directive, as well as more recently through Council Directive 2001/115/EC where they are one of a limited set of compliance options for sending and storage of electronic invoices. This CWA summarizes findings and issues identified by the e-Invoicing Focus Group set up by CEN/ISSS regarding electronic invoicing using electronic signatures. Issues surrounding electronic signatures relating to e-Invoicing and VAT in relation to the Council Directive 2001/115/EC are covered, which had to be implemented by Member States by 1st January 2004. Council Directive 2001/115/EC, details the requirements on taxable persons and their service providers to guarantee the integrity and the authenticity of electronic invoices for VAT purposes.

C.4.10: The practical use of Electronic signatures in E-Commerce: a Guide for SMEs

Source: CEN

Reference Number:	**14708**
Publication Date:	March 2003
URL:	ftp://cenftp1.cenorm.be/PUBLIC/CWAs/e-Europe/e-Commerce/cwa14708-00-2003-Mar.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying electronic signatures
Subarea:	e-commerce
Type of Document:	Guidelines
Level of Standard:	Industry standard
Status:	CEN Workshop Agreement (CWA)
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	e-commerce

Description:

This Guide is needed because the traditional way of doing business has now changed and as we move into the electronic world of eBusiness new competence and tools are needed. There is, therefore, the need to use Electronic Identification and Electronic Signature for the purpose of making online transactions legally binding and more efficient while reducing business risks. The Guide answers the following questions: · Why is trust needed in eBusiness? (Chapter 2) · Why are Electronic Identification and Electronic Signatures needed? (Chapter 3) · What are Electronic Identification and Electronic Signatures and how are they used? (Chapter 4) · What are the legal issues, risks and responsibilities involved in implementing Electronic Signatures? (Chapter 5 and 6) · How can I make use of it? Are there good examples to look at? (Chapter 7 and 8)

C.4.11: Loi n°2000-230 du 13 mars 2000 portant adaptation du droit de la preuve aux technologies de l'information et relative à la signature électronique

Source: French legislation

Reference Number:	**2000-230**
Publication Date:	Mar 00
URL:	http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005629200&dateTexte=vig
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	Law
Maturity:	Published
Geographic general:	
Geographic details:	
Sector:	

Description:

This law is an adaptation of the right of proof to information technologies and relative to electronic signature. In particular, the text details in Article 4 the definition of electronic signature, and affirms that all electronic signatures are legally recognised if they guarantee, with a confident process, the identification of signer and integrity of act, being thus equivalent to handwritten signature.

C.4.12: Loi n°2004-575 du 21 juin 2004 pour la confiance dans l'économie numérique

Source: French legislation

Reference Number:	**2004-575**
Publication Date:	Jun 04
URL:	http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000801164&dateTexte=
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	Law
Maturity:	Published
Geographic general:	EU nation
Geographic details:	France
Sector:	

Description:

This law for the trust in the digital economy has a dedicated Article (33) relative to the responsibility of providers of electronic certification service, producing qualified certificates.

C.4.13: Loi n°2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n°78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés

Source: French legislation

Reference Number:	**2004-801**
Publication Date:	Aug 04
URL:	http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441676
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	Law
Maturity:	Published
Geographic general:	EU nation
Geographic details:	France
Sector:	

Description:

This law is relative to the protection of physical people for personal data.

C.4.14: Décret n°2001-272 du 30 mars 2001 pris pour l'application de l'article 1316-4 du code civil et relatif à la signature électronique

Source: French legislation

Reference Number:	**2001-272**
Publication Date:	30/03/2001, consolidated 09/07/2009
URL:	http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005630796&dateTexte=vig
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	Decree
Maturity:	Published
Geographic general:	EU nation
Geographic details:	France
Sector:	

Description:

This decree is a summarized translation of the European Directive 1999/93/EC and its Articles. This French version describes 11 Articles, including definitions for electronic signature and secure electronic signature, electronic signature creation, electronic signature verification, qualified certificates,

C.4.15: Décret n°2002-535 du 18 avril 2002 relatif à l'évaluation et à la certification de la sécurité offerte par les produits et les systèmes des technologies de l'information

Source: French legislation

Reference Number:	**2002-535**
Publication Date:	Apr 02
URL:	http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000005632663&dateTexte=vig
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	Decree
Maturity:	Published
Geographic general:	EU nation
Geographic details:	France
Sector:	

Description:

This decree describes the procedures for evaluation and certification. It also describes the process for becoming accredited evaluation center.

C.4.16: Arrêté du 26 juillet 2004 relatif à la reconnaissance de la qualification des prestataires de services de certification électronique et à l'accréditation des organismes qui procèdent à leur évaluation

Source: French legislation

Reference Number: JORF n°182 du 7 août 2004 page 14104 texte n° 17
Publication Date: Jul 04

URL: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000441678&dateTexte=vig

Equivalent to:

Based on:

Framework reference:

Technical Area:

Subarea:

Type of Document:

Level of Standard: National regulation

Status: Departmental order

Maturity: Published

Geographic general: EU nation

Geographic details: France

Sector:
Description:

This industry departmental order is relative to the recognition of the qualification of providers of electronic certification and the accreditation of organizations in charge of evaluation (as mentionned in article 7 of Decree 2002-535). It Defines the French scheme for qualification of "Prestataires de Service de Certification" (PSC). In France, COFRAC is the organization in charge of accreditation.

C.4.17: Arrêté du 31 mai 2002 relatif à la reconnaissance de la qualification des prestataires de certification électronique et à l'accréditation des organismes chargés de l'évaluation

Source: French legislation

Reference Number: JORF n°132 du 8 juin 2002 page 10223 texte n° 16
Publication Date: May 02

URL: http://www.legifrance.gouv.fr/affichTexte.do?cidTexte=JORFTEXT000000596280&dateTexte=vig

Equivalent to:

Based on:

Framework reference:

Technical Area:

Subarea:

Type of Document:

Level of Standard: National regulation

Status: Departmental order

Maturity: Published

Geographic general: EU nation

Geographic details: France

Sector:
Description:

This economy, finance and industry departmental order is relative to the recognition of qualification of electronic certification providers and to the accreditation of organizations in charge of evaluation.

C.4.18: FAQ - Décret relatif à la signature électronique

Source: French legislation

Reference Number:	
Publication Date:	
URL:	http://www.ssi.gouv.fr/site_article23.html
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	FAQ
Level of Standard:	National regulation
Status:	
Maturity:	Published
Geographic general:	EU nation
Geographic details:	France
Sector:	

Description:

This FAQ is about Decree n°2001-272 of 30 march 2001 taken for application of Article 1316-4 of civil code and relative to electronic signature.

C.4.19: Signature électronique Point de situation - Memento - Version 0.94

Source: ANSSI

Reference Number:

Publication Date:	Aug 04
URL:	http://www.ssi.gouv.fr/IMG/pdf/signature-memento-v0-94.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	Memento
Level of Standard:	National regulation
Status:	
Maturity:	Published
Geographic general:	EU nation
Geographic details:	France
Sector:	

Description:

This document recalls first the legal context of elec tronic signature, including the European Directive and its translation to France, second the secure mechanism for signature creation, third the qualified certificate.

C.4.20: Dispositifs sécurisés de création de signature électronique (SSCD)

Source: ANSSI

Reference Number:	**872/SGDN/DCSSI/SDR: SIG/P/01.1**
Publication Date:	Apr 03
URL:	http://www.ssi.gouv.fr/IMG/pdf/Document_descriptif_de_la_procedure_Certification_de_conformite_des_dispositifs_de_creation_de_signature_electronique.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	National procedure
Maturity:	Published
Geographic general:	EU nation
Geographic details:	France
Sector:	

Description:

This procedure defines the process of delivery of a certificate of conformity relative to requirements in Article 3.I of Decree 2001-272 (30 march 2001, electronic signature) for a SSCD.

C.4.21: Tableau des produits certifiés conformes SSCD

Source: ANSSI

Reference Number:	
Publication Date:	
URL:	http://www.ssi.gouv.fr/site_article36.html
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	Published
Geographic general:	EU nation
Geographic details:	France
Sector:	

Description:

This page contains a complete list of SSCD compliant products (under the process defined above)

C.4.22: Ressources cryptographiques pour autorités de certification (PSC)

Source: ANSSI

Reference Number: Référence : PSC/P/01.1	**N°3033/SGDN/DCSSI/SDR**
Publication Date:	Oct 05
URL:	http://www.ssi.gouv.fr/IMG/pdf/Document_descriptif_de_la_procedure_Certification_de_conformite_des_modules_cryptographiques_des_PSC.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	National procedure
Maturity:	Published
Geographic general:	EU nation
Geographic details:	France
Sector:	

Description:

This procedure is intented for providers of cryptographic modules used by certification providers to produce qualified certificates. The conformity certificate delivered following this procedure guarantees that the cryptographic module respects the set of requirements of point 2 of the annex of the departmental order of 26/07/2004.

C.4.23: Tableau des produits certifiés conformes PSC

Source: ANSSI

Reference Number:	
Publication Date:	
URL:	http://www.ssi.gouv.fr/site_article37.html
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	Published
Geographic general:	EU nation
Geographic details:	France
Sector:	

Description:

This page contains a complete list of PSC compliant products (under the process defined above)

C.4.24: Référentiel Général de Sécurité (RGS) version 1.0

Source: ANSSI

Reference Number:

Publication Date:	May 10
URL:	http://references.modernisation.gouv.fr/sites/default/files/RGSv1.0.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	National Recommendations
Maturity:	Published
Geographic general:	EU nation
Geographic details:	France
Sector:	

Description:

This Security General Referential defines a set of rules for security to be used by french administrations to secure their information systems. This document proposes in addition good practices for security of information systems.

C.4.25: Référentiel Général de Sécurité (RGS) version 1.0 - Annexe 3: Fonction de sécurité "signature" version 2.3

Source: ANSSI

Reference Number:

Publication Date:	Feb 10
URL:	http://references.modernisation.gouv.fr/sites/default/files/RGSv1.0.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	National Recommendations
Maturity:	Published
Geographic general:	EU nation
Geographic details:	France
Sector:	

Description:

This document is an annex of full RGS and regroups all rules dedicated to the various modules required for the "signature", including keys and certificates, electronic signature creation and verification.

C.4.26: Interoperability of the electronic European Health Insurance Cards (WS/eEHIC)

Source: CEN

Reference Number:	**CWA 15974: 2009**
Publication Date:	1 May 2009
URL:	ftp://cenftp1.cenorm.be/PUBLIC/CWAs/e-Europe/eEHIC/CWA15974_2009.pdf
Equivalent to:	na
Based on:	ISO/IEC 7816, EN 15480-2, ISO/IEC 24727
Framework reference:	A.6.3
Technical Area:	Signing devices
Subarea:	
Type of Document:	Technical Specification
Level of Standard:	Industry standard
Status:	CWA
Maturity:	Published
Geographic general:	Europe
Geographic details:	
Sector:	Health

Description:

CWA 15974 defines the electronic European Health Insurance Card (eEHIC). It may support electronic signature functionality, but is not mandated to be a signing card. CWA 15974 refers to existing standards regarding electronic signatures, namely ISO/IEC 7816, to CEN/TS 15480-2 (based on EN 14890-1&2) and to ISO/IEC 24727.

C.4.27: Health Informatics - Public key infrastructure: Overview of digital certificate services

Source: ISO

Reference Number:	**17090-1**
Publication Date:	15 February 2008
URL:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39845
Equivalent to:	na
Based on:	
Framework reference:	A.1.x.1
Technical Area:	CSP
Subarea:	CSP_QC and CSP_nonQC
Type of Document:	Guideline
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	Health

Description:

ISO 17090-1:2008 defines the basic concepts underlying use of digital certificates in healthcare and provides a scheme of interoperability requirements to establish a digital certificate-enabled secure communication of health information. It also identifies the major stakeholders who are communicating health-related information, as well as the main security services required for health communication where digital certificates may be required.

ISO 17090-1:2008 gives a brief introduction to public key cryptography and the basic components needed to deploy digital certificates in healthcare. It further introduces different types of digital certificate — identity certificates and associated attribute certificates for relying parties, self-signed certification authority (CA) certificates, and CA hierarchies and bridging structures.

C.4.28: Health Informatics - Public key infrastructure: Certificate profile

Source: ISO

Reference Number:	**17090-2**
Publication Date:	15 February 2008
URL:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39846
Equivalent to:	na
Based on:	
Framework reference:	A.1.x.3
Technical Area:	CSP
Subarea:	CSP_QC and CSP_nonQC
Type of Document:	Technical Specification
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	Health

Description:

ISO 17090-2:2008 specifies the certificate profiles required to interchange healthcare information within a single organization, between different organizations and across jurisdictional boundaries. It details the use made of digital certificates in the health industry and focuses, in particular, on specific healthcare issues relating to certificate profiles.

C.4.29: Health Informatics - Public key infrastructure: Policy management of certification authority

Source: ISO

Reference Number:	**17090-3**
Publication Date:	15 February 2008
URL:	http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=39847
Equivalent to:	na
Based on:	
Framework reference:	A.1.x.2
Technical Area:	CSP
Subarea:	CSP_QC and CSP_nonQC
Type of Document:	Policy Requirements
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	Health

Description:

ISO 17090-3:2008 gives guidelines for certificate management issues involved in deploying digital certificates in healthcare. It specifies a structure and minimum requirements for certificate policies, as well as a structure for associated certification practice statements.

ISO 17090-3:2008 also identifies the principles needed in a healthcare security policy for cross-border communication and defines the minimum levels of security required, concentrating on aspects unique to healthcare.

C.4.30: Standard Practice for Healthcare Certificate Policy

Source: ASTM International

Reference Number:	**E2212 - 02a (2010)**
Publication Date:	Jul 05
URL:	http://www.astm.org/Standards/E2212.htm (cost $45)
Equivalent to:	na
Based on:	RFC2560, InternetX.509PublicKeyInfrastructureOnlineCertificateStatusProtocol, OCSP June 1999
Framework reference:	A.1.x.2
Technical Area:	CSP
Subarea:	CSP_QC and CSP_nonQC
Type of Document:	Policy Requirements
Level of Standard:	Industry standard
Status:	Approved standard
Maturity:	Published
Geographic general:	International
Geographic details:	U.S.
Sector:	Health

Description:

It defines a set of requirements to ensure that certificates, used for authentication, authorization, confidentiality, integrity, and nonrepudiation of health information by healthcare organizations and persons, have a minimally sufficient assurance level.

This policy defines a healthcare public key infrastructure that can be used to implement other ASTM standards.

C.4.31: OASIS ebXML Messaging Transport Binding for Digital Signature Services Version 1.0

Source: OASIS

Reference Number:	**N/A**
Publication Date:	Jun 05
URL:	http://docs.oasis-open.org/dss-x/profiles/ebxml/v1.0/cs01/oasis-dss-1.0-profiles-ebxml-cs01.doc
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Centralized signature creation /verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Industry standard
Status:	OASIS Committe Specification
Maturity:	Draft
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies an ebXML transport binding for DSS messages, i.e., how DSS messages are encoded and carried using as transport protocol the OASIS ebXML Messaging Service (ebMS).

C.4.32: Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) —

Part 5: Security rules for batch EDI (authenticity, integrity and non-repudiation of origin)

Source: ISO/TC 154 -UN/CEFACT (JSWG)

Reference Number:	**ISO 9735-5**
Publication Date:	Jun 05
URL:	http://www.gefeg.com/jswg/v41/data/V41-9735-5.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats , signature creation, signature verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies digital signatures in EDIFACT syntax and mechanisms for applying them to indivicual EDIFACT messages () or to individual EDIFACT packages. This document also specifies a format fot EDIFACT certificates (USC,USA and USR EDIFACT segments). This document does not defines extensions equivalent to the ones specified in XAdES, CAdES or PAdES.

C.4.33: Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) —

Part 6: Secure authentication and acknowledgement message (message type -AUTACK)

Source: ISO/TC 154 -UN/CEFACT (JSWG)

Reference Number:	**ISO 9735-6**
Publication Date:	Jun 05
URL:	http://www.gefeg.com/jswg/v41/data/V41-9735-6.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats , signature creation, signature verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies AUTACK, an EDIFACT message that may be used for applyint EDIFACT digital signatures to messages, packages, groups of messages or Interchanges. This message compiles a set of digital signatures on referenced EDIFACT structures within the message. In addition to that AUTACK may also be used to provide secure acknowledgement or non-repudiation to the receipt to secured (for instance signed) messages, packages, groups or interchanges.

C.4.34: Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) —

Part 8: Associated data in EDI

Source: ISO/TC 154 -UN/CEFACT (JSWG)

Reference Number:	**ISO 9735-8**
Publication Date:	Jun 05
URL:	http://www.gefeg.com/jswg/v41/data/V41-9735-8.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature Formats , signature creation, signature verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies mechanisms to incorporate within an EDIFACT interchange data that do not follow EDIFACT syntax. These are the mechanisms currently used for transporting X509 certificates within an EDIFACT interchange.

C.4.35: Electronic data interchange for administration, commerce and transport (EDIFACT) — Application level syntax rules (Syntax version number: 4, Syntax release number: 1) —

Part 9: Secure key and certificate management message (message type - KEYMAN)

Source: ISO/TC 154 -UN/CEFACT (JSWG)

Reference Number:	**ISO 9735-8**
Publication Date:	Jun 05
URL:	http://www.gefeg.com/jswg/v41/data/V41-9735-9.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification
Type of Document:	Tech. Specification (protocol)
Level of Standard:	Internationally recognised standard (e.g.ISO/ITU)
Status:	International Standard
Maturity:	Published
Geographic general:	International
Geographic details:	
Sector:	

Description:

This document specifies EDIFACT KEYMAN message, which may be used to request or deliver: security keys, certificates, certification paths, replacement of certificates, revocation of certificates, certificate revocation lists, and also to request and notify certificate status

C.4.36: Asia PKI Interoperability GuidelinC.3. (Version 2.0, Draft). Book 2

Source: Asia PKI Forum

Reference Number:	
Publication Date:	Jun 05
URL:	http://www.oasis-open.org/committees/download.php/13085/APKI_IG_ver2_0_Book2.doc
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature creation / verification
Type of Document:	Technical specification & Conformance & interoperability testing
Level of Standard:	Industry standard
Status:	Working Draft
Maturity:	Published
Geographic general:	Other region
Geographic details:	
Sector:	

Description:

This document, produced by the Asia PKI Forum Interoperability Working Group, specifies algorithms for certification path validation and CRL validation and restricted certificate path construction. In addition to that it specifies a test suite for certificate path processing and a common API for PKI applications as well as APKI-F conformance profile for the members of this forum

C.4.37: Electronic Administration Act

Source: Italian Legislation

Reference Number:

Publication Date:	Mar 05
URL:	http://www.digitpa.gov.it/sites/default/files/normativa/CAD_Codice_Amministrazione_Digitale.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Covers more than 1 area
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	Electronic Administration

Description:

This act establishes the legal framework for the Italian Electronic Administration. Its scope includes electronic identity card, electronic document, electronic signature, signed electronic documents, notarized signature, qualified certificates, CSP Providers of qualified certificates, electronic payments, registered electronic email, electronic democratic participation, the role of the National Centre for ICT (CNI) for the development of the Electronic Administration

C.4.38: Decree of the President of the Council of Ministers of March 30, 2009. Technical rules relating to generation, and setting and verification of digital signatures and time validation of electronic documents. (09A06300)

Source: Italian Legislation

Reference Number:

Publication Date:	Mar 09
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Covers more than 1 area
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	

Description:

This decree provides the technical rules for the generation, and verification of qualified signatures and time-stamps, and for the performance of CSPs issuing qualified certificates. It also establishes provisions for accredited CSPs or CSPs seeking accreditation.
It also defines provisions for accredited CSPs to make available to its holders a time validation system in accordance with its Title IV.
Finally, it also establishes that products developed or marketed in one of the EU Member States and the European Economic Area in accordance with national regulations transposing Directive 1999/93/EC of the European Parliament and Council, published in the Official Journal of the European Union Series L, No 13 of 19 January 2000, are allowed to move freely within the internalItalian market.

C.4.39: CNIPA Resolution 45

Source: Italian Legislation

Reference Number:

Publication Date: May 09
URL:
Equivalent to:
Based on:
Framework reference:
Technical Area: Covers more than 1 area
Subarea:
Type of Document:
Level of Standard: National regulation
Status:
Maturity:
Geographic general: EU Nation
Geographic details: Italy
Sector:
Description:

This resolution establishes the rules for acknowledging and verifying electronic documents to be adhered to by accredited certifiers. The provisions of Heading II set out the algorithms for generating and checking digital signatures. The provisions of Heading III define the profile of qualified certificates and the information they must contain. The provisions of Heading IV define the profile of electronic certificates used in certification and time stamping, and the information they must contain. The provisions of Heading V set out the rules for time stamping, and the format and information to be contained in time stamps used by document time-stamping systems, as set out under Heading IV of the technical rules. The provisions of Heading VI define the formats and means of accessing information on certificate revocation and suspension, pursuant to Article 30 of the technical rules. The provisions of Heading VII define the formats of cryptographic envelopes used to hold objects signed with a digital signature. The provisions of Heading VIII set out the requirements for the applications used to affix and check digital signatures pursuant to Articles 9.10 and 10 of the technical rules.

C.4.40: Italian Tax Agency. Disposition on how to communicate to the Tax Agency the "closure evidence" of fiscally relevant electronic documents

Source: Italian Legislation

Reference Number:	
Publication Date:	Oct 10
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Trust service status provider
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	Taxes

Description:

This Disposition establishes the provisions allowing to communicate by electronic means the "closure evidence" of an electronic documents with relevant tax information, as well as its contents. In its annex 1 it provides the technical mechanisms for such a communication as well as the "closure evidence" content.

C.4.41: DECREE of MINISTRY OF FINANCE AND ECONOMY. Manners to accomplish fiscal obligations relevant to electronic documents and to their copy on various media.

Source: Italian Legislation

Reference Number:

Publication Date:	Jan 04
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	Taxes

Description:

This decree establishes provisions for the issuance, storage and exhibition of fiscally relevant electronic documents.

C.4.42: CNIPA Resolution of 19 February 2004

Source: Italian Legislation

Reference Number:	
Publication Date:	Feb 04
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	

Description:

This resolucion establishes technical rules for the reproduction and conservation of documents on media suitable to ensure accordance of these documents to the original.

C.4.43: Decree 52 of 20 March 2004

Source: Italian Legislation

Reference Number:	
Publication Date:	Mar 04
URL:	
Equivalent to:	
Based on:	http://gazzette.comune.jesi.an.it/2004/49/7.htm
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	

Description:

This Decree is the Italian Implementation of Directive 2001/115/EC, which simplifies and harmonises the VAT invoicing.

C.4.44: Decree of the President of the Council of Ministers of 11 May 2005 C.4. 68: "Regulation laying down rules for the use of registered electronic mail"

Source: Italian Legislation

Reference Number:	
Publication Date:	May 05
URL:	
Equivalent to:	
Based on:	http://www.digitpa.gov.it/sites/default/files/normativa/DPR_11-feb-2005_n.68.pdf
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	REM

Description:

Self explanatory.

C.4.45: Decree of the President of the Council of Ministers of 6 May 2009

Source: Italian Legislation

Reference Number:	
Publication Date:	May 09
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	REM

Description:

This decree establishes provisions relating to issue and use of registered electronic mail box assigned to nationals.The decree states to grant a free box of certified mail to all citizens who request them, in implementation of Article 8 of the CAD.

C.4.46: Decree 29 November 2008, No 185 - Act 2 / 2009

Source: Italian Legislation

Reference Number:	
Publication Date:	Nov 08
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	REM

Description:

The law introduces mandatory PEC for firms established in corporate form for professionals and for members of the Orders. Public bodies are required to publish their addresses on the Index of PEC PA. In addition, all communications between public agencies, professionals and businesses can be by PEC, unless the recipient has to declare its readiness to accept the application.

C.4.47: Circular No CNIPA 56

Source: Italian Legislation

Reference Number:	
Publication Date:	May 09
URL:	
Equivalent to:	
Based on:	http://www.digitpa.gov.it/sites/default/files/normativa/Circolare_Cnipa_56-2009.pdf
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	REM

Description:

Procedures for applying for inclusion on the list of public managers registered electronic mail (PEC) of Article 14 of Decree of the President February 11, 2005, No. 68" (Official Gazette of July 22, 2009, n . 168)

C.4.48: Circular No CNIPA 51

Source: Italian Legislation

Reference Number:	
Publication Date:	Dec 06
URL:	
Equivalent to:	
Based on:	http://www.digitpa.gov.it/sites/default/files/normativa/Circolare_Cnipa_51-2006.pdf
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	REM

Description:

The circular provides for the surveillance and monitoring activities undertaken by CNIPA (DigitPA today) against the operators of PEC.

C.4.49: Decree of the Minister for Innovation and Technologies: "Technical rules for the creation, transmission and validation, including time, certified electronic mail."

Source: Italian Legislation

Reference Number:	
Publication Date:	Dec 05
URL:	
Equivalent to:	
Based on:	http://www.digitpa.gov.it/sites/default/files/normativa/DM_2-nov-2005.pdf
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	REM

Description:

Self explanatory

C.4.50: Annex to the Decree of 2 November 2005: "Technical rules of service for the transmission of electronic documents by certified mail"

Source: Italian Legislation

Reference Number:	
Publication Date:	Nov 05
URL:	
Equivalent to:	
Based on:	http://www.digitpa.gov.it/sites/default/files/normativa/Pec_regole_tecniche_DM_2-nov-2005.pdf
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	REM

Description:

It contains all the rules and specifications for the use of the PEC.

C.4.51: Decree of the President of the Republic No 68: "Regulation laying down rules for the use of certified mail, pursuant to Article 27 of Law January 16, 2003, No. 3."

Source: Italian Legislation

Reference Number:	
Publication Date:	Feb 05
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	REM

Description:

The Decree regulates the modes of operation of the PEC, not only in relations with the PA, but also between individuals.

C.4.52: CNIPA Technical Annex:RECOMMENDATIONS ON THE METHOD AND REGISTRATION PROCEDURES

IN THE PUBLIC LIST OF REGISTERED ELECTRONIC MAIL PROVIDERS

Source: Italian Legislation

Reference Number:	
Publication Date:	Feb 06
URL:	
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	REM

Description:

Self explanatory

C.4.53: CNIPA Technical Specification: "Technical specification for the transmission of electronic documents by registered electronic mail."

Source: Italian Legislation

Reference Number:	
Publication Date:	May 05
URL:	
Equivalent to:	
Based on:	http://www.interlex.it/testi/pdf/pec_regtecn.pdf
Framework reference:	
Technical Area:	TSP applying eSignatures
Subarea:	
Type of Document:	
Level of Standard:	National regulation
Status:	
Maturity:	
Geographic general:	EU Nation
Geographic details:	Italy
Sector:	REM

Description:

This document provides the technical specifications that define the provision of registered electronic mail services.

C.4.54: Aplicaciones con Documento Nacional de Identidad Electrónico (DNIe). Creación y verificación de firma electrónica. Tipo 1 para plataformas TI que permiten un control exclusivo de los interfaces con el firmante, y con un nivel de garantía de evaluación «EAL1»

Source: AENOR

Reference Number:	**NE 71510**
Publication Date:	December 2010
URL:	
Equivalent to:	
Based on:	Common Criteria
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Protection profiles
Type of Document:	Policy requirement
Level of Standard:	Industry standard
Status:	National Standard
Maturity:	Published
Geographic general:	EU nation
Geographic details:	
Sector:	

Description:

This is a document of a standard family on Spanish electronic ID protection profiles that contain the requirements necessary to ensure secure use of certificates that the DNIe contains, will guide developers in creating the electronic signature verification software. These profiles will facilitate the arrival to market of signature software guaranteed to be secure for use in DNIe certification. Currently more than 7 million DNIes have been issued in Spain.

The electronic signature software developed according to these Protection Profiles will be able to be run on a PC, or be integrated into other types of equipment (decoders, TDT, PDAs, etc.), enabling the credentials of the user to be obtained directly from the DNIe.

C.4.55: Aplicaciones con Documento Nacional de Identidad Electrónico (DNIe). Creación y verificación de firma electrónica. Tipo 1 para plataformas TI que permiten un control exclusivo de los interfaces con el firmante, y con un nivel de garantía de evaluación «EAL3»

Source: AENOR

Reference Number:	**NE 71511**
Publication Date:	Dec 10
URL:	
Equivalent to:	
Based on:	Common Criteria
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Protection profiles
Type of Document:	Policy requirement
Level of Standard:	Industry standard
Status:	National Standard
Maturity:	Published
Geographic general:	EU nation
Geographic details:	
Sector:	

Description:

This is a document of a standard family on Spanish electronic ID protection profiles that contain the requirements necessary to ensure secure use of certificates that the DNIe contains, will guide developers in creating the electronic signature verification software. These profiles will facilitate the arrival to market of signature software guaranteed to be secure for use in DNIe certification. Currently more than 7 million DNIes have been issued in Spain.

The electronic signature software developed according to these Protection Profiles will be able to be run on a PC, or be integrated into other types of equipment (decoders, TDT, PDAs, etc.), enabling the credentials of the user to be obtained directly from the DNIe.

C.4.56: Aplicaciones con DNIC.3. Creación y verificación de firma electrónica. Tipo 2 para ordenadores personales, y con un nivel de garantía de evaluación «EAL1»

Source: AENOR

Reference Number:	**NE 71512**
Publication Date:	Dec 10
URL:	
Equivalent to:	
Based on:	Common Criteria
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Protection profiles
Type of Document:	Policy requirement
Level of Standard:	Industry standard
Status:	National Standard
Maturity:	Published
Geographic general:	EU nation
Geographic details:	
Sector:	

Description:

This is a document of a standard family on Spanish electronic ID protection profiles that contain the requirements necessary to ensure secure use of certificates that the DNIe contains, will guide developers in creating the electronic signature verification software. These profiles will facilitate the arrival to market of signature software guaranteed to be secure for use in DNIe certification. Currently more than 7 million DNIes have been issued in Spain.

The electronic signature software developed according to these Protection Profiles will be able to be run on a PC, or be integrated into other types of equipment (decoders, TDT, PDAs, etc.), enabling the credentials of the user to be obtained directly from the DNIe.

C.4.57: Aplicaciones con DNIC.3. Creación y verificación de firma electrónica. Tipo 2 para ordenadores personales, y con un nivel de garantía de evaluación «EAL3»

Source: AENOR

Reference Number:	**NE 71513**
Publication Date:	Dec 10
URL:	
Equivalent to:	
Based on:	Common Criteria
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Protection profiles
Type of Document:	Policy requirement
Level of Standard:	Industry standard
Status:	National Standard
Maturity:	Published
Geographic general:	EU nation
Geographic details:	
Sector:	

Description:

This is a document of a standard family on Spanish electronic ID protection profiles that contain the requirements necessary to ensure secure use of certificates that the DNIe contains, will guide developers in creating the electronic signature verification software. These profiles will facilitate the arrival to market of signature software guaranteed to be secure for use in DNIe certification. Currently more than 7 million DNIes have been issued in Spain.

The electronic signature software developed according to these Protection Profiles will be able to be run on a PC, or be integrated into other types of equipment (decoders, TDT, PDAs, etc.), enabling the credentials of the user to be obtained directly from the DNIe.

C.4.58: Real Decreto 4/2010 Esquema Nacional de Interoperabilidad/ Spanish National Interoperability Framework (Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica)

Source: Spanish Legislation

Reference Number:	**RD Real Decreto 4/2010**
Publication Date:	Jan 10
URL:	http://www.csae.map.es/csi/pdf/ENI_INTEROPERA...
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Covers more than 1 area
Subarea:	
Type of Document:	Requirements
Level of Standard:	National regulation
Status:	Regulation
Maturity:	Published
Geographic general:	EU nation
Geographic details:	
Sector:	

Description:

The Real Decreto (Royal Decree) 4/2010, dated January 8th (Official Gazette, January 29th) regulates the National Interoperability Framework foreseen in article 42 of the eGovernment Law 11/2007, heavily based on the use of the Spanish electronic ID. This Framework includes criteria and recommendations about standardization of information, formats and applications and about preservation of information to be taken into account by Public Administrations when adopting technological decisions so as to ensure interoperability. For security issues the reference is the National Security Framework. The National Interoperability Framework pursues the creation of the necessary conditions to ensure an adequate level of organizational, semantic and technical interoperability of systems and applications used by Public Administrations that permits the exercise of rights and the fulfillment of duties through the electronic access to public services; it also pursues providing benefits in terms of effectiveness and effectiveness. In order to create such conditions, the National Interoperability Scheme introduces the common elements that have to guide the action of the Public Administrations regarding interoperability. Particularly, it introduces the following principal elements: · The specific principles of interoperability are defined; · The dimensions of interoperability, organizational, semantic and technical, are taken into account, as they were explicitly mentioned in article 41 of Law 11/2007; · Common infrastructures and services are recognized to be relevant instruments that contribute to the simplification and propagation of interoperability and that facilitate multilateral interactions; · The concept of 'reuse' applied to applications of Public Administrations, associated information and to other objects of information, given the fact that together with 'share' and 'collaborate' is relevant for interoperability, and all of them are recognized by EU policies; · The interoperability of electronic signature and electronic certificates; · Preservation of the electronic documents, considering the effect of time in interoperability; · Finally, it is created a series of technical guides and instruments for interoperability, in order to facilitate the implementation of the Framework.

C.4.59: Esquema Nacional de Seguridad/ National Security Framework of Spain (Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica)

Source: Spanish Legislation

Reference Number:	**RD Real Decreto 3/2010**
Publication Date:	Jan 10
URL:	http://www.csae.map.es/csi/pdf/ENS_SECURITY_E...
Equivalent to:	
Based on:	ISO 27001/27002
Framework reference:	
Technical Area:	Covers more than 1 area
Subarea:	
Type of Document:	Requirements
Level of Standard:	National regulation
Status:	Regulation
Maturity:	Published
Geographic general:	EU nation
Geographic details:	
Sector:	

Description:

The Real Decreto (Royal Decree) 3/2010, of January 8th (Official Gazette, January 29th) regulates the National Security Framework foreseen in the article 42 of the eGovernment Law 11/2007, heavily based on the use of the Spanish electronic ID. This Framework establishes the security policy in the use of electronic means in the scope of the eGovernment Law 11/2007; this security policy will be formed by the basic principles and minimum requirements for an adequate protection of information. The National Security Framework pursues the creation of the necessary conditions of confidence in the use of electronic means, through measures to ensure the security of systems, data, communications and electronic services that permits the exercise of rights and the fulfilment of duties through the electronic access to public services; to ensure that information systems will provide their services in accordance with their functional specifications and will protect information. In order to create such conditions, the National Security Scheme introduces the common elements that have to guide the action of the Public Administrations regarding security. Particularly it introduces the following principal elements: · The basic principles to be taken into account when adopting decisions about security; · The minimum requirements for the adequate protection of information; · The procedure to fulfill the basic principles and minimum requirements by means of the adoption of proportionate security measures.

C.4.60: Act on Strong Electronic Identification and Electronic Signatures

Source: Finnish Legislation

Reference Number:	**617/2009 English**
Publication Date:	(Translation completed) 04/2010
URL:	http://www.finlex.fi/en/laki/kaannokset/2009/en20090617
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	Signature algorithms
Type of Document:	Guidelines
Level of Standard:	National regulation
Status:	Technical Specification
Maturity:	Published
Geographic general:	EU nation
Geographic details:	Austria
Sector:	eGovernment

Description:

This is English translation of the Finnish law (produced by Ministry of Transport and Communications) related to, among other things, electronic signature.

C.4.61: Common PKI V2.0 Part 1, Certificate and CRL Profiles

Source: T7

Reference Number:

Publication Date:	Jan 09
URL:	http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf
Equivalent to:	
Based on:	X.509:2005 and RFC 5280
Framework reference:	
Technical Area:	CSP
Subarea:	Generic
Type of Document:	Techs specs: Profile
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	EU nation
Geographic details:	Germany
Sector:	eGovernment

Description:

This part of the Common PKI specification describes certificate and certificate revocation list (CRL) formats. It is based on and profiles ITU-T X.509 and PKIX RFC 5280.

C.4.62: Common PKI V2.0 Part 2, PKI Management

Source: T7

Reference Number:

Publication Date:	Jan 09
URL:	http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf
Equivalent to:	
Based on:	RFC 5272, RFC 5273, RFC 5274
Framework reference:	
Technical Area:	CSP
Subarea:	CSP- generic
Type of Document:	Techs specs: Profile
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	EU nation
Geographic details:	Germany
Sector:	eGovernment

Description:

This part of the Common PKI specification addresses online communication between PKI components. It is based on PKIX RFCs 5272-5274 and defines procedures for certificate enrollment.

C.4.63: Common PKI V2.0 Part 3, CMS based Message Formats

Source: T7

Reference Number:

Publication Date:	Jan 09
URL:	http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf
Equivalent to:	
Based on:	RFC 3851, RFC 2045, RFC 2046, RFC 3852
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	signature creation / verification procedures
Type of Document:	Techs specs: Profile
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	EU nation
Geographic details:	Germany
Sector:	eGovernment

Description:

This part of the Common PKI specification addresses message formats to be used during the exchange of data between PKI components. It defines a profile for Common PKI message formats that is mainly based on the Internet documents for S/MIME [RFC 3851], MIME [RFC 2045, RFC 2046], and CMS [RFC 3851].

C.4.64: Common PKI V2.0 Part 4, Operational Protocol

Source: T7

Reference Number:

Publication Date:	Jan 09
URL:	http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf
Equivalent to:	
Based on:	RFC 1777, RFC 4510, RFC 2560, RFC 3161, ETSI TSP
Framework reference:	
Technical Area:	CSP
Subarea:	Generic
Type of Document:	Techs specs: Profile
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	EU nation
Geographic details:	Germany
Sector:	eGovernment

Description:

This Common PKI standard defines operational protocols for distributing certificates and revocation material. It is based on LDAP v3 (Light Weight Directory Access, Version 3) and OCSP v1 (Online Certificate Status Protocol) as well as LDAP and HTTP for transport.

C.4.65: Common PKI V2.0 Part 5, Certificate Path Validation

Source: T7

Reference Number:

Publication Date:	Jan 09
URL:	http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	signature creation / verification procedures
Type of Document:	Techs specs: Profile
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	EU nation
Geographic details:	Germany
Sector:	eGovernment

Description:

Specifies an algorithm for automating the certificate path validation procedure. Conforming applications are not required to implement exactly this algorithm, but they MUST be functionally equivalent with respect to the external behaviour.

C.4.66: Common PKI V2.0 Part 6, Cryptographic Algorithms

Source: T7

Reference Number:

Publication Date:	Jan 09
URL:	http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Covers more than 1 area
Subarea:	Generic
Type of Document:	Techs specs: Profile
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	EU nation
Geographic details:	Germany
Sector:	eGovernment

Description:

This part of the Common PKI specification defines a list of approved cryptographic algorithms for digital signatures, encryption and subject public keys to be supported by implementations that comply with the Common PKI specification.

C.4.67: Common PKI V2.0 Part 7, Signature API

Source: T7

Reference Number:

Publication Date:	Jan 09
URL:	http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf
Equivalent to:	
Based on:	OASIS-DSS, SOAP, TS 101 903, TS 101 733
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	signature creation / verification procedures
Type of Document:	Techs specs: Profile
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	EU nation
Geographic details:	Germany
Sector:	eGovernment

Description:

This part of the Common PKI specification defines a profile of the eCard API framework (BSI Technische Richtlinie TR-03112 as defined in the seven documents [TR-03112-1] to [TR03112-7]) that is specified for use in German governmental smart card applications. The eCard API is in turn mainly based on international standards, in particular [SOAP], [OASIS-DSS], [ISO24727-3], [XAdES] and [CAdES].

C.4.68: Common PKI V2.0 Part 8, XML based Message Formats

Source: T7

Reference Number:

Publication Date:	Jan 09
URL:	http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf
Equivalent to:	
Based on:	XML-DSIG, OSCI
Framework reference:	
Technical Area:	Signature creation / verification
Subarea:	signature creation / verification procedures
Type of Document:	Techs specs: Profile
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	EU nation
Geographic details:	Germany
Sector:	eGovernment

Description:

This part of the Common PKI specification provides the Common PKI profile for XML signatures and conforms to the XML_DSIG standard [XML_DSIG] and to the OSCI-profile [OSCI]. OSCI has been issued to trim the XML_DSIG format to the needs of eGovernment and allows wide interoperability of the applications by restricting the formats and contents to a well-defined subset of possible options allowed by XML_DSIG.

C.4.69: Common PKI V2.0 Part 9, SigG Profile

Source: T7

Reference Number:

Publication Date:	Jan 09
URL:	http://www.t7ev.org/uploads/media/Common-PKI_v2.0.pdf
Equivalent to:	
Based on:	
Framework reference:	
Technical Area:	Covers more than 1 area
Subarea:	Generic
Type of Document:	Techs specs: Profile
Level of Standard:	Industry standard
Status:	Technical report
Maturity:	Published
Geographic general:	EU nation
Geographic details:	Germany
Sector:	eGovernment

Description:

The German Signature Act (SigG) and the Ordinance on Digital Signatures (SigV) raise a couple of special requirements on technical components as well as on the certificate policy of certification service providers (CSPs). This profile addresses these technical requirements

History

Document history		
0.0.1	21 July 2011	Draft for public review