|  |  |
| --- | --- |
|  | ToR STF BF (TC CYBER) |
| Version: 0.3 |
| Author: Giovanni Bartolomeo – Date:05 August 2016 |
| Last updated by: Y. Sakho/S. Compans – Date: 16 February 2017 |
| page 1 of |

Terms of Reference – Specialist Task Force

STF BF (TC CYBER)

Attribute Based Encryption – Common protocol for data access control for Cloud, Mobile and IoT

Summary information

|  |  |
| --- | --- |
| Approval status | approved by TC CYBER (RC CYBER(16)DEC005, ended 10-Nov)  Approved by Board#110 (1 December 2016) |
| Funding | **Maximum budget: 154 200 €**  Contractors: 149 400 €  Travel costs: 4 800 € |
| Time scale | February 2017 to December 2017 |
| Work Items | DTS/CYBER-00025 |
| Board priority | [ETSI STF funding criteria](https://portal.etsi.org/STF/STFs/Funding.aspx): Horizontal activities (security) in innovative domain for ETSI |

Part I – Reason for proposing the STF

# Rationale

The EU Regulation 910/2014 on “electronic identification and trust services for electronic transactions in the European internal market” (eIDAS) and the Regulation 2016/679 on “the protection of natural persons with regard to the processing of personal data and on the free movement of such data” (General Data Protection Regulation, GDPR) have provided a legal framework to address challenges raising from the digital age and its “app economy”. In particular, among various challenges raised by the Regulation 2016/679, protection of data, especially data that may contain or may be Personally Identifiable Information (PII), or allow to infer information of private nature, is one of major technically challenging aspects.

In the ICT landscape records potentially containing PII appear as large distributed datasets, retained in data centres located in many different EU and non-EU Countries and managed by various stakeholders with different levels of trust. In order to prevent undesirable use of PII there is a need to enable security controls of some complexity covering the complete life-cycle of the PII.

Encryption is widely used to protect confidentiality of data in untrusted environments. In traditional public key encryption, in order to encrypt the message, the sender must know in advance the identity and public key of each individual to whom the data should be disclosed. When subsequently encrypted with the public key of the intended recipient only that recipient, in possession of the matching private key, is able to decrypt the message. Where a message has to be transmitted to several parties, it has to be encrypted separately for each party. Such encryption schemes provide a simple solution to access control – allowing only the sender and recipient access to the message (during transmission). But, in general, encryption schemes should not of themselves be considered as access control schemes even if they form part of one.

To provide secure access control, therefore, traditional encryption schemes are sided with a software infrastructure. The general structure adopted to date is that of policy based access control. In Attribute Based Access Control (ABAC), in particular, policies are based on attributes that are provided to parties by one or more authorities. Policies are evaluated by a Policy Enforcement Point (PEP), which permits or denies access to a resource. However, several threats may compromise the software infrastructure and the Policy Enforcement Point in particular.

Attribute Based Encryption (ABE) is a cryptographic scheme that provides a level of protection similar to ABAC but exclusively leveraging on cryptographic algorithms, without relying on a software based PEP. This makes ABE ideal for not fully trusted environments where the PEP may be compromised – e.g., Cloud based environments, but also the IoT domain and some Mobile contexts. Moreover, providing a standard mechanism, ABE might side different proprietary access control solutions, making platforms interoperable and providing a technical basis for the “right to data portability” included in the GDPR that will effectively come into force in Q2/2018.

With its expertise on security and network architectures, TC CYBER is already providing voluntary work to include PII protection through ABE reference points in standard network and Cloud architectures. However, specific competences are required to rapidly work out details at interface level, create protocols to request, distribute, and revoke attributes and policies through the use of standard certificates, standardize naming scheme, define the integration with traditional Attribute Based Access Control standards like XACML and assertion protocols like SAML, and help to lower the barriers to adopt such data protection mechanisms for users and vendors.

Therefore, it is proposed that an STF will assist the ongoing work of CYBER delegates and accelerate the work.

# Objective

ABE mathematically moves the authorisation decision from the access control system to the protected data itself (i.e., the ABE ciphertext). One challenge is to map ABE-based access control to traditional access control so that the former can be a superset of the latter in terms of capabilities. A second challenge is to accommodate both the Ciphertext-Policy and the Key-Policy variants of ABE, which handle access control differently and consequently address different but similarly important use cases.

The proposed STF is tasked to provide an ETSI Technical Specification to define a protocol for ABE addressing the following key elements:

* Definition of interactions between the actors and stakeholders (e.g. principal, the service provider, the authority releasing attributes)
* Standardisation of a naming scheme for attributes
* Standardisation of an access policy schema
* Definition of a standard set of mechanisms to distribute and revoke attributes and policies using certificates in a standard public key infrastructure (PKIX)
* Mapping to a standard assertion mechanism (SAML) and to a standard Attribute Based Access Control language (XACML)
* Bindings to transport protocols when existing standards do not cover the foreseen use cases

To accomplish its task, the proposed STF will collect feedback from various stakeholders (TC CYBER, other ETSI TCs and members, other SDOs, developer communities)

# Relation with ETSI strategy and priorities

ETSI long-term strategy states that “ICT, and in particular telecommunications, is at the heart of an increasingly dependent and interacting family of systems that will be critical to all aspects of life and national infrastructure”. In several sectors – including the Health, Public Administration, Education, Financial and Legal sectors just to quote but a few – there will be an increasing need of protection of electronic information that are or might be personally identifiable.

Ensuring privacy by improving existing standards has been (and is still) a priority for the latest EU standardization rolling plans. In Rolling Plan 2017, for instance, Action 1 of chapter 3.5.6. (Network and Information Security) clearly states a need for “ensuring privacy and improving existing standards regarding the protection of individuals with regards to the processing of personal data”.

Privacy protection is an emerging but important domain for ETSI that will be explicitly addressed by TC CYBER. During their latest meeting, TC CYBER updated its terms of reference to add the “provision of security mechanisms to protect privacy” in its scope.

In this respect, ETSI is already participating in CEN/CENELEC JWG8 activities in response to EU Mandate 530[[1]](#footnote-1). Furthermore and after a successful coordination with ISO JTC1 SC27.5 (Identity management and privacy technologies), ETSI has recently published TR 103 304, a technical report describing a general framework for 5G and Cloud-based services in which PII protection mechanisms may be implemented.

Enhancements to access control mechanisms would be of natural interest within ETSI (various Technical Bodies), partnership projects (3GPP, OneM2M), and for the wider industry (e.g. for the data analytics industry). Thus, activities in this area would contribute to strengthening the relevance of ETSI as an SDO.

Following up this framework, TC CYBER decided to start drafting technical specifications for data access control based on Attribute Based Encryption (DTS/CYBER-0020), with three main use cases to be addressed: Cloud, 5G and IoT. The proposed STF will assist TC CYBER in completing this work item providing expertise and manpower that delegates might lack of. Section 4.3 provides details on specific tasks to be performed within the proposed STF.

# Context of the proposal

## ETSI Members support

|  |  |  |
| --- | --- | --- |
| **ETSI Member** | **Supporting delegate** | **Motivation** |
| CNIT | Giovanni Bartolomeo | CNIT strongly supports this STF in order to help the ongoing work in TC CYBER (DTS/CYBER-0020), to provide detailed and standardized protocol specifications for ABE and to ease the realisation of a future reference implementation. |
| Telecom Italia | Paolo De Lutiis | 3GPP document TR22.891 presents scenarios of mobile user access from less trusted networks. Leveraging on ABE, this STF could provide a standardized protocol that may be a solution to prevent user data disclosure to unauthorized entities when roaming to untrusted networks. Telecom Italia strongly supports this STF. |
| Ente Normazione Informatica (UNINFO) | Alessandro Guarino | The GDPR will become applicable in Q2/2018 and by that time ETSI should ensure that proper technical standards for the processing of personal data will be available – especially for new domains like Cloud and IoT. PII protection is indeed one of the focus and ABE may be a key technology when holding data on less trusted environments. UNINFO strongly supports the request for this STF. |
| Istituto Superiore Mario Boella (ISBM) | Antonio Lotito | This STF will provide a new key standard based on ABE for data protection in complex and sensitive scenarios related to the Cloud, IoT and Mobile (e.g., Emergency, Electronic Health, Financial, etc.). Moreover, it will be useful to evaluate applicability of ABE implementations against hybrid (i.e., attribute and role-based) encryptions’ techniques, analysing both performances and policies. ISMB supports this STF. |
| Cadzow Consulting | Scott Cadzow | Given that privacy is a qualified right and that PII is a controlled set of data, the use of ABE in protecting PII is to be explored as a means of giving assurance to the holder of the PII, and the authorities (civil, commercial, governmental), that access is controlled under the widest set of conditions without inhibiting the availability of services to users. Cadzow Consulting supports the request for this STF. |
| IBIT Ambrosini | Francois Ambrosini | The STF work will enable the unification of traditional Attribute Based Access Control and ABE access control through attribute semantics and policy translation. This will be the key to protect PII in a wide range of contexts with different degrees of trust. IBIT supports the request for this STF. |
| Intellinium | Mathieu Destrian | Intellilium supports this STF and recommend to address and answer needs from our industry customers who want to be GDPR-compliant for connected worker solutions involving end-user private data. |

## Market impact

**Benefits for vendors and providers**

Understanding the connection between privacy protection and interoperability, GDPR has explicitly acknowledged a right to “data portability” to citizens and customers of the EU Digital Single Market. Member States have started to promote interoperability agreements for the Public and private sector under the “Connecting Europe Facility” programme. This programme at the time, has provided specifications for five service “building blocks”: eID, eDelivery, eSignature, eInvoicing, eTranslation.

However, achieving full interoperability without addressing data protection mechanisms and access control in particular might be difficult. Existing mechanisms are today primarily focused on legacy enterprise solutions and there is not yet any standard “block” – protocol – implementing fine-grained data access control for distributed, not fully trusted environments like Cloud platforms and IoT deployments (24 or even more billion devices in 2020, according to most forecasts).

Attribute Based Encryption is seen as a core capability that may be deployed in solutions to extend the benefits of fine-grained data access control to these environments. The mathematically enforced access controls, and mathematically verifiable resilience to a large class of software compromise, particularly for data-at-rest, offers additional strategies to designers. ABE has been the subject of hundreds of academic publications over the past decade and is now starting its commercial deployment, having been implemented in several solutions by independent vendors. However, at the time these solutions use different and incompatible protocols and that is going to get worse in next years without standardizing implementations.

The release of a standardized protocol may unlock citizen’s and customer’s data from proprietary platforms, encouraging interoperability and controlled flow of data, which is vital for the rising transnational Digital Single Market. At the same time, this may benefit vendors and providers offering enhanced capabilities to their existing solutions.

**Benefits for customers and citizens**

A standardized ABE-based protocol will enhance interoperability and increase the security and privacy assurance of the data over its lifetime.

One can note that around the 2000s trust in public and private online services increased when transparent and uniform mechanisms for protection of transactions appeared, with an enormous impact on the electronic market. Today, especially in the public sector, the debate focuses on the added value of connecting citizen’s data in the Cloud. Their trust in Cloud services may increase with the provision of a transparent, uniform and mathematically proved protocol for governing access control to their data. The same would go for IoT as current deployments regularly make the headlines in the press due to poor security choices.

## Tasks for which the STF support is necessary

The expertise needed is not commonly available to standardization bodies, but is considered to be available from experts in research organizations and academia and is not available using a voluntary model for financing the necessary time and effort of experts. In particular, the following activities requires domain specific expertise:

* Investigate the relationship with traditional access control mechanisms, define a subset of ABAC which can be implemented by ABE, and determine how ABE can complement traditional ABAC.
* Specify a new standardized protocol for key and attribute distribution, expiration and revocation for use in ABE. This activity also includes the definition of semantics for a basic set of attributes to ensure interoperability.
* Mapping the protocol to a standard Public Key Infrastructure X.509 (PKIX). This activity includes mapping of the authority role in ABE into certification authorities, define standard naming scheme for attributes, include attributes into digital certificate extensions, etc.
* Mapping the protocol to SAML standard assertion mechanism for the generation, distribution, and revocation of ABE keys and ciphertext.
* Define bindings to communication protocols that are adapted to constrained environments, such as the IoT.

## Related voluntary activities in the TB

TC CYBER delegates are already working on a number of items related to PII protection and ABE in particular. These include:

* A preliminary study on use cases and related architectural aspects has been provided in TR 103 304. In particular, Use Case 1 and Use Case 2 in clause 7 provide details on the role of the PII processor and mapping to standard Cloud architecture.
* A liaison with ISO JTC1 SC27.5 (Identity management and privacy technologies) was set up at CYBER#6. Consequently, SC27.5 has revised drafts of TR 103 304 before its publication as v.1.1.1. The liaison is still ongoing and SC27.5 is periodically updating TC CYBER about its work.
* As a follow up of TR 103 304, TC CYBER delegates will provide the following voluntary work in the context of work item DTS/CYBER-0020 that was approved at CYBER#7:
* Integration with standard Cloud architecture: functional architecture based on use cases from ISO 19944. A liaison with ISO JTC1 SC38.5 has been set up at CYBER#7, regarding project ISO 19944 on Data and their Flow across Devices and Cloud Services. SC38.5 will inform TC CYBER about changes in ISO 19944.
* Integration with standard Network architecture: functional architecture based on use cases from 3GPP SA-1 document TR 22.891 (SMARTER) dealing with 5G networks. A liaison with 3GPP-SA3 has been set up at CYBER#8 and it is expected that SA3 will provide feedback to delegates on this work.
* Integration with IoT, functional architecture covering both oneM2M and non-oneM2M. An important aspect here is to cover protection of the data both in the field and in the support infrastructure. A liaison statement to oneM2M will be proposed in order to collect relevant feedback.

TC CYBER will also select members for the Steering Group of the STF.

## Previous funded activities in the same domain

None.

## Consequences if not agreed

Governing access to citizen and customer’s account data has an ever-growing relevance in today and future Internet where different datasets need to be connected to derive added value. This applies to both the private and the public sector.

In past years, the standardization of XACML has promoted common terminology and interoperability between Attribute Based Access Control implementations by multiple vendors. Attribute Based Encryption (ABE) is today acknowledged to be an ideal solution to extend this kind of protection to novel and not fully trusted environments like Cloud and IoT platforms, because mathematically enforced and implicitly resilient to software compromise. Nevertheless, there is currently a proliferation of solutions based on ABE with no common approach for attribute and key distribution, revocation, expiration etc. This leaves each vendor the freedom to implement different and generally not compatible protocols around possibly different variants of the ABE scheme.

Having a standard based, transparent – because mathematically proved – and uniform mechanism governing data access control may pave the way for the interoperability of public and private services. Actually, citizens’ and customers’ data continue to be locked into specific platforms where data access is governed by internal proprietary mechanisms. Without a standard, customers’ data may remain locked-in on these platforms, practically leading to data unavailability when the platform provider is changed. A de facto denial of that “right to data portability” that the GDPR acknowledges to every EU citizen.

Similarly, without a standard, citizens’ data will remain locked-in on national Administration, discouraging the flow and reuse of data across different EU Organizations, which is instead highly recommended to support the free movements of people, services, goods and capital (the “four freedoms” of the European Single Market Strategy).

As part of its strategy, ETSI, through TC CYBER in particular, is today in the position of promoting such a standard, in line, and with no overlapping, with the work of other standardization bodies – noticeable ISO SC27.5 on identity and privacy and specifically the work SC38.5 on data flow, data categories and data use. With the GDPR effectively coming into force in Q2/2018, ETSI might miss the time if this work were delayed.

Part II – Execution of the work

# Technical Bodies and other stakeholders

## Reference TB

ETSI TC CYBER.

## Other interested ETSI Technical Bodies

The interaction with 3GPP will be based on inputs from SA-1 document TR22.891 “Study on New Services and Markets Technology Enablers” describing scenarios of user access from less trusted networks. Under the liaison established at CYBER#8, the STF will interact with SA-3, which is actually specifying the security architectures and protocols for new enablers. It is expected that SA3 will provide feedback to TC CYBER delegates on work item DTS/CYBER-0020 and the new ones that might be created because of this STF proposal.

It is also expected that a liaison will be established with OneM2M for comments and feedback on the work of the proposed STF.

## Other stakeholders

A liaison with ISO JTC1 SC38.5 has been set up at CYBER#7, regarding project ISO 19944 on Data and their Flow across Devices and Cloud Services. SC38.5 will inform TC CYBER about changes in ISO 19944. Note that the STF work will not overlap with this project, as the latter actually provides groundwork for categorising data, understanding its flows in the context of Cloud computing and the need for protection. ISO 19944 nevertheless does not mandate any protocol specifications for implementing the framework it describes.

Further interactions with ISO will happen with JTC1 SC27.5 (Identity management and privacy technologies) under the liaison set up at CYBER#6. SC27.5 has already revised drafts of TR 103 304 before its publication and is periodically updating TC CYBER about their ongoing work.

# Base documents and deliverables

## Base documents

|  |  |  |  |
| --- | --- | --- | --- |
| **Document** | **Title** | **Current Status** | **Expected date for stable document** |
| ETSI TR 103 304 | CYBER; Personally Identifiable Information (PII) Protection in mobile and cloud services | Published | - |
| ETSI TS 103 486 | CYBER; Identity management and naming schema protection mechanisms | Early Draft | November 2017 |
| 3GPP TR 22.891 | Study on New Services and Markets Technology Enablers | Published | - |
| ISO project 19944 | Information technology – Cloud computing – Cloud services and devices: data flow, data categories and data use | Committee Draft | **Stage code 40.00** Draft international standard registered |
| ISO/IEC 27018 | Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors | Published | - |
| OneM2M R2 architecture | OneM2M Release 2 Functional Architecture, TS-0001-V2.10.0 | Published | - |
| OASIS SAML 2.0 core | Assertions and Protocols for the OASIS Security Assertion Markup  Language (SAML) V2.0 | Published | - |
| OASIS SAML 2.0 security | Security and Privacy Considerations for  the OASIS Security Assertion Markup Language (SAML) V2.0 | Published | - |
| OASIS XACML 3.0 core | eXtensible Access Control Markup Language (XACML) Version 3.0 | Published | - |
| IETF RFC 5280 | Internet X.509 Public Key Infrastructure Certificate and  Certificate Revocation List (CRL) Profile | Published | - |

## Deliverables

|  |  |  |
| --- | --- | --- |
| **Deliv.** | **Work Item code**  **Standard number** | **Working title**  **Scope** |
| D1 | DTS/CYBER-0025 | Working title: Attribute Based Encryption for Attribute Based Access Control  Scope: This WI specifies standard features needed to use ABE as ABAC. It specifies a toolbox of protocols including the following features:  - Interactions between the principal, the service provider, the authority releasing attributed  - The policy schema for data access control  - Key, policy, and attribute distribution  - Key, policy, and attribute expiration and revocation  - Definition of what subset of ABAC (e.g. XACML) may be mapped into the protocol  -Definition of semantics for a basic set of attributes to ensure interoperability  - Identification of additional attributes required by the protocol that would require an extension to traditional ABAC (e.g. an extension to XACML)  - Mapping the protocol to a standard Public Key Infrastructure X.509 (PKIX)  - Mapping the protocol to a standard assertion protocol (e.g. SAML)  - Definition of new protocol bindings when existing bindings do not cover the deployment scenario (e.g. a CoAP binding for the IoT case)  The deliverable will cover both the Ciphertext-Policy (CP-ABE) and Key-Policy (KP-ABE) variants of Attribute-Based Encryption.  NOTE: This WI will be companion of DTS/CYBER-0020 which is performed by TC CYBER delegates as voluntary work. DTS/CYBER-0020 describes network architectures and related reference points for Cloud, mobile and IoT where the protocol specified in DTS/CYBER-xxxx0025is to be applied. |

The STF Leader should submit the changes on the Work Item scope to TC CYBER (scheduled on 24 Mar 17)

## Deliverable schedule:

DTS/CYBER-0025 Attribute Based Encryption for Attribute Based Access Control

* Start of work 06 Mar 2017
* ToC & scope 24 Mar 2017
* Early draft 23 May 2017 CYBER#10
* Stable draft 15 Sept 2017 CYBER#11
* Final draft 19 Jan 2018 CYBER#12
* TB approval 07 Feb 2018 CYBER#12
* Publication 28 Feb 2018

|  |  |  |
| --- | --- | --- |
| **Deliv.** | **Work Item code**  **Standard number** | **Working title**  **Scope** |
| D1 | DTS/CYBER-0025 | Working title: Attribute Based Encryption for Attribute Based Access Control  Scope: This WI specifies standard features needed to use ABE as ABAC. It specifies a toolbox of protocols including the following features:  - Interactions between the principal, the service provider, the authority releasing attributed  - The policy schema for data access control  - Key, policy, and attribute distribution  - Key, policy, and attribute expiration and revocation  - Definition of what subset of ABAC (e.g. XACML) may be mapped into the protocol  -Definition of semantics for a basic set of attributes to ensure interoperability  - Identification of additional attributes required by the protocol that would require an extension to traditional ABAC (e.g. an extension to XACML)  - Mapping the protocol to a standard Public Key Infrastructure X.509 (PKIX)  - Mapping the protocol to a standard assertion protocol (e.g. SAML)  - Definition of new protocol bindings when existing bindings do not cover the deployment scenario (e.g. a CoAP binding for the IoT case)  The deliverable will cover both the Ciphertext-Policy (CP-ABE) and Key-Policy (KP-ABE) variants of Attribute-Based Encryption.  NOTE: This WI will be companion of DTS/CYBER-0020 which is performed by TC CYBER delegates as voluntary work. DTS/CYBER-0020 describes network architectures and related reference points for Cloud, mobile and IoT where the protocol specified in DTS/CYBER-xxxx0025is to be applied. |

## Deliverable schedule:

DTS/CYBER-0025 Attribute Based Encryption for Attribute Based Access Control

* Start of work 06 Mar 2017
* ToC & scope 24 Mar 2017
* Early draft 23 May 2017 CYBER#10
* Stable draft 15 Sept 2017 CYBER#11
* Final draft 19 Jan 2018 CYBER#12
* TB approval 07 Feb 2018 CYBER#12
* Publication 28 Feb 2018

# Work plan, time scale and resources

## Organization of the work

STF will perform its work by face-to-face sessions as well as remotely. Some sessions may occur in connection with the relevant TC meetings. Contractors will perform part of their work at their premises using their own means. Calls restricted to STF experts may be held to synchronize the work from remote locations.

The work of the STF will be supervised by a Steering group whose members may include: TC CYBER delegates, ABE leading researchers, delegates from other standardization bodies – in particular for those where there are established liaisons (e.g., ISO SC27.5 and SC38.5/ 3GPP SA-3/ oneM2M), experts from ETSI CTI. Steering group members will work mostly remotely but might be invited to attend TC CYBER meetings in order to discuss with other TC CYBER delegates.

Early and stable drafts and the final draft will be available as milestones at regular intervals and will be either delivered in time for discussion and decision at TC CYBER meetings or submitted for approval by correspondence. Under established liaisons, drafts will be made available for comments and feedback to other external stakeholders.

## Task description

Task 1 – Core ABE based data protection protocol specification

Objectives

This task will work out detailed specifications for a toolbox based on ABE data protection protocols. The task will take inputs (1) from the results of inputs, which provides groundwork for categorising data, understanding its flows and use in the context of Cloud computing, IoT, mobile applications and related needs for protection; and (2) from DTS-CYBER/0020, which is defining functional architectures and reference points.

The task will define a toolbox of standardized protocols and mechanisms for handling: interactions between the principal, the service provider, the authorities releasing keys and attributes; key, policy and attribute distribution; key, policy and attribute expiration and revocation. This task will cover both the Ciphertext-Policy (CP-ABE) and Key-Policy (KP-ABE) variants of ABE.

Inputs

* ISO/IEC/JTC1/SC38/WG5 19944
* ETSI TR 103 304
* DTS/CYBER-0020
* 3GPP document TR22.891 “Smarter”
* OneM2M Release 2 Architecture
* ISO/IEC/JTC1/SC27/WG5 27551

Output

Specifications for a toolbox of standardized protocols and mechanisms based on ABE, also to be used as input for Tasks 2, 3 and 4.

Interactions

TC CYBER delegates will provide voluntary contributions to define the functional architectures for the three use cases identified in DTS/CYBER-0020. The STF will present working drafts for review and present progress reports for TC approval. During the whole project the STF will be presenting interim results to the Steering group and will use their guidance to continue the work.

Working drafts will be sent to external stakeholders (ISO JTC1/SC38.5, 3GPP SA-1, oneM2M) for comments and feedback.

Resources required

System architects, security engineers

**Working method**

This task has 2 parts, one related to the architecture and the other one related to the underlying cryptographic primitives. There will be continuous interactions in order to find the best solution fitting with requirements.

Task 2 – Mapping into a standard Public Key Infrastructure X.509 (PKIX)

Objectives

This task will work out specifications based on the toolbox defined in Task 1 for mapping key and attribute distribution to standard PKIX infrastructure. It will include: requirements to map the authority role in ABE into a standard certification authority; definition of standard naming scheme for attributes; integration of attributes into X.509 digital certificate extensions.

Input

Based on the output from task 1 and on the feedback received, plus:

* DTS/CYBER-0020
* IETF RFC 5280, Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile

Output

Specifications of mapping into a standard Public Key Infrastructure.

Interactions

* ETSI Centre for Testing and Interoperability (CTI)
* TC CYBER

Resources required

System architects, security engineers

Task 3 – Protocol bindings for Access control

Objectives

This task will work out specifications for mapping a subset based on the toolbox defined in Task 1 of standard ABAC structures into ABE. It will include definition of what subset of ABAC may be mapped into the protocol; policy translation from legacy and upcoming access control standards (XACML, NGAC, SDDL…); definition of semantics for a basic set of attributes to ensure interoperability.

As a proof of feasibility, the task will examine ISO project 19944 in order to provide an implementation of the typical patterns and policies presented in that framework.

Input

Based on the output from task 1 and on the feedback received, plus:

* OASIS xacml-3.0-core-spec-os, eXtensible Access Control Markup Language (XACML) Version 3.0
* Microsoft Security Descriptor Definition Language, <https://msdn.microsoft.com/en-us/library/windows/desktop/aa379567(v=vs.85).aspx>
* NIST SP 800-178, "A Comparison of Attribute Based Access Control (ABAC) Standards for Data Service Applications; Extensible Access Control Markup Language (XACML) and Next Generation Access Control (NGAC)"
* American National Standards Institute, Information technology - Next Generation Access Control - Functional Architecture (NGAC-FA), INCITS 499-2013, American National Standard for Information Technology, March 2013.
* American National Standards Institute, Information technology – Next Generation Access Control – Generic Operations and Data Structures (GOADS), INCITS 5262016, American National Standard for Information Technology, January 2016.
* oneM2M TS-0012, "Base Ontology"
* ETSI TS 103 264, "SmartM2M; Smart Appliances; Reference Ontology and oneM2M Mapping"
* ETSI TS 103 378, "Smart Body Area Networks (SmartBAN); Unified data representation formats, semantic and open data model"
* ISO/IEC/JTC1/SC38/WG5 19944

Output

A set of specifications allowing ABAC structures to be translated into ABE policies.

Interactions

* ETSI Centre for Testing and Interoperability (CTI)
* TC CYBER

Resources required

System architects, security engineers

Task 4 – Protocol bindings for Assertion

Objectives

This task will focus on verifying the suitability of protocol bindings defined in assertion protocols including SAML to the expected deployment scenarios of the ABE core protocol in the Cloud, 5G and IoT cases. It will identify gaps, and specify any necessary extensions to the SAML assertion protocol (e.g., new profile, elements) that would be needed in order to validate the trustworthiness of the information required for key and attribute generation, distribution and revocation. Of particular importance for this task is the IoT domain, for which no binding for optimised protocols – e.g. CoAP – exist.

Input

Based on the output from task 1 and on the feedback received, plus:

* OASIS saml-core-0.2-os, Assertions and Protocols for the OASIS Security Assertion Markup
* Language (SAML) V2.0
* OASIS saml-sec-consider-2.0-os, Security and Privacy Considerations for the OASIS Security Assertion Markup Language (SAML) V2.0
* OASIS xacml-3.0-core-spec-os, eXtensible Access Control Markup Language (XACML) Version 3.0
* ABC 4 Trust: Deliverable D2.2: "Architecture for Attribute-based Credential Technologies - Final Version " , https://abc4trust.eu/download/Deliverable\_D2.2.pdf

**Output**

A specification of the required protocol bindings for each domain (Cloud, Mobile, IoT).

Interactions

* ETSI Centre for Testing and Interoperability (CTI)
* TC CYBER

Resources required

System architects, security engineers

Task 5 – Technical leadership and coordination

Objectives

Technical leadership of the team of experts as well as coordination of relationship with other relevant ETSI TBs. This task will include organisation and preparation of expert sessions, interactions with the Steering group, presentation to TC CYBER meetings and presentation of the STF work at ETSI Security Week 2017. The task will also include all relevant planning and reporting activities up to the final STF report.

Input

Output from task 1 to task 4.

Output

Progress reports, communication with external stakeholders, presentation atETSI Security Week 2017, communication with the Steering group.

Interactions

* ETSI TCs and members
* other TBs: ISO JTC1/SC38.5, 3GPP SA-1, oneM2M

Resources required

Security technical experts able to lead the work and coordinate with TC CYBER and other stakeholders.

## Milestones

Milestone 0 – Start of the work

Appointment of the STF Steering group at CYBER#9 (13-15 Feb 2017).

NOTE: in case of delay in the start of the work (i.e. for administrative reasons), the appointment of the Steering group will happen by Approval by Correspondence after CYBER#9.

Milestone 1 – TS – Early draft for review

TS draft including:

* A Table of Content
* Use cases consolidated
* Selection of cryptographic primitives
* Access control groups
* Identification of ontologies
* Expected properties from access control standards
* Identification of information to assert.
* Identification of either existing hooks in X.509 certificates or possible extension of X.509 certificates for ABE specific parameters

Reviewed at CYBER#10 (31 May - 02 June 2017) and made available to TC CYBER for comments and feedback one week before the meeting.

STF Progress report submitted one week before the meeting and to be approved by TC CYBER.

Milestone 2 – Presentation to stakeholders

Experts’ work official presentation to stakeholders during ETSI Security week. Not subject to any payment.

Milestone 3 – TS – stable draft for review

TS stable draft reviewed at CYBER#11 (25-27 Sept 2017) and made available one week before the meeting. STF Progress report submitted one week before the meeting and to be approved by TC CYBER.

Milestone 4 – Final deliverable for approval, STF final report

TS final deliverable reviewed at CYBER#12 should be available two weeks before the meeting. Final report reviewed at CYBER#12 should be available one week before the meeting.

TS Final deliverable and Final report to be approved by TC CYBER.

## Task summary

|  |  |  |
| --- | --- | --- |
| **N** | **Task / Milestone / Deliverable** | Target date |
|
| M0 | Start of work | 06 Mar 2017 |
| T1 | Core ABE protocol specifications | 06 Mar 2017  1 Dec 2017 |
| T2 | Mapping into standard Public Key Infrastructure X.509 | 10 Apr 2017  27 Oct 2017 |
| T3 | Protocol bindings for XACML | 10 Apr 2017  27 Oct 2017 |
| T4 | Protocol bindings for SAML | 10 Apr 2017  27 Oct 2017 |
| M1 | TS – early draft for review | **CYBER#10**  31-May – 02 June 2017 |
| M2 | Presentation to stakeholders | June 2017 |
| M3 | TS – stable draft for review | **CYBER#11**  25-27 Sept 2017 |
| T5 | Technical leadership and coordination | 06 Mar 2017  Feb 2017 |
| M4 | Final drafts, STF final report | **09 Feb 2018** |
| **Total** | | |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Task Milest.** | **Description** | **J** | **F** | **M** | **A** | **M** | **J** | **J** | **A** | **S** | **O** | **N** | **D** | **J** | F |
| M0 | Start of work |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T1 | Core ABE protocol specifications |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T2 | Mapping into a standard Public Key Infrastructure X.509 |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T3 | Protocol bindings for XACML |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T4 | Protocol bindings for SAML |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| M1 | TS – early draft for review |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| M2 | Presentation to stakeholders |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| M3 | TS – stable draft for review |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| T5 | Technical leadership and coordination |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| M4 | Final drafts, STF final report |  |  |  |  |  |  |  |  |  |  |  |  |  |  |

## Working methods and travel cost

Travel cost for working sessions will be included in the contract compensation. Presentation of results to the reference TB and other TBs will be reimbursed as real cost from the travel budget. Travel cost for the presentation to stakeholders will be reimbursed as real cost from the travel budget.

The STF (Specialist Task Force) will be under the monitoring and responsibility of TC CYBER. The STF will be coordinating the work with the ETSI CTI (Centre for Testing and Interoperability).

A Steering Group (SG) will be formed comprising members of TC CYBER.

The STF will provide regular reports to the Steering Group. Conference calls will be held when appropriate. Face-to-face meetings will occur in connection with the relevant TC meetings.

The total action cost includes the travels required to attend the following events:

* Present STF Progress Report and deliverable to TC CYBER meetings (3 meetings #9,#10,#11)
* Presenting the results of the STF to stakeholders
* Other relevant TB meetings (e.g., ISO, 3GPP, oneM2M)

# Expertise required

## Team structure

Up to 5 providers to ensure the following mix of competences:

* Deep understanding of Attribute Based Access Control techniques
* Deep understanding of functional encryption (Attribute Based Encryption)
* Good knowledge of standard functional architectures (Cloud, 5G, IoT) and related protocols
* Good knowledge of OASIS XACML and SAML
* Good knowledge of Public Key Infrastructure/X.509
* Good knowledge of ISO/IEC 19944 and 27018
* Past experience in designing and development of cybersecurity solutions

Part III: Financial conditions

# Maximum budget

## *Manpower cost*

|  |  |  |  |
| --- | --- | --- | --- |
| ***Description*** | ***Working days*** | ***Rate (eur/day)*** | ***Total Cost*** |
| Contracted Expertise |  |  | 149 400 |
| ***Total*** |  |  | ***149.400*** |

## *Travel cost*

|  |  |
| --- | --- |
| ***Expected travels*** | ***Cost estimate*** |
| stakeholders’ meeting | 1.200 |
| CYBER#9 13-15 Feb 2017, Sophia Antipolis, FR | 600 |
| CYBER#10 07-09 June 2017, Sophia Antipolis, FR | 600 |
| CYBER#11 25-27 Sep 2017, TBD | 600 |
| CYBER#12 07-09 Feb 2018, TBD | 600 |
| Other TB meetings (OneM2M/3GPP/ISO) or events or contingency | 1.200 |
| **Total** | **4.800** |

Part IV: STF performance evaluation criteria

# Key Performance Indicators

Contribution from ETSI Members to STF work

* Steering Group meetings (number of meetings / participants / duration)
* Contributions/comments from TC CYBER delegates
* Contributions/comments from other TBs/SDOs
* Delegates attending meetings and events related to STF activities

Contribution from providers to ETSI work

* Number and type of contributions to TC CYBER meetings (number of documents / meetings / participants)
* Presentations in workshops, conferences, stakeholder meetings

(e.g ETSI Security Week 2017 )

* Number of articles/press releases
* Contributions/presentations to other ETSI TBs
* Contributions received from other ETSI TBs

Liaison with other stakeholders

* Stakeholder participation in the project (category, business area)
* Cooperation with other standardization bodies
* Potential interest of new members to join ETSI
* Liaison to identify requirements and raise awareness on ETSI deliverables
* Comments received on drafts (e.g. at meetings, mailing lists, etc.)

Quality of deliverables

* Approval of deliverables according to schedule
* Respect of time scale, with reference to start/end dates in the approved ToR
* Quality review by TB
* Quality review by ETSI Secretariat

Time recording

For reporting purposes, the STF experts shall fill in the time sheet provided by ETSI with the days spent for the performance of the services.

In the course of the activity, the STF Leader shall collect the relevant information, as necessary to measure the performance indicators. The result will be presented in the Final Report.

# Document history

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Date | Author | Status | Comments |
| 0.1 | 05-Aug-2016 | CNIT | Draft |  |
| 0.3 | 26-Aug-2016 | CNIT | Draft |  |
| 0.5 | 06-Sep-2016 | CNIT | Draft |  |
| 0.7 | 23-Sep-2016 | CNIT | Draft |  |
| 0.9 | 30-Sep-2016 | CNIT | Draft |  |
| 0.10 | 10-Oct-2016 | CNIT | Draft |  |
| 0.11 | 17-Oct-2016 | CNIT  IBIT  CTI  TI | Draft |  |
| 0.12 | 20-Oct-2016 | CNIT  CTI | Draft |  |
| 0.13 | 21-Oct-2016 | CNIT  CTI | Draft |  |
| 0.14 | 24-Oct-2016 | CNIT  CTI | Draft |  |
| 0.15 | 25-Oct-2016 | C3L | Draft |  |
| 0.16 | 26-Oct-2016 | CNIT | Stable |  |
| 0.17 | 26-Oct-2016 | CNIT | For RC approval |  |
| 0.18 | 27-Oct-2016 | Alberto Berrini | For OCG/Board consult. | Editorials |
| 0.19 | 14-Nov-2016 | A. Berrini,  S. Compans | TB approved | Editorials |
| 0.20 | 14-Dec-2016 | Y. Sakho  S. Compans  G. Craik | Board#110 Approved | Editorials |
| 0.3 | 16-Feb-2017 | Y. Sakho | STF Preparatory Meeting | Editorials |

1. M/530 COMMISSION IMPLEMENTING DECISION C(2015) 102 final of 20.1.2015 on a standardisation request to the European standardisation organisations as regards European standards and European standardisation deliverables for privacy and personal data protection management pursuant to Article 10(1) of Regulation (EU) No 1025/2012 of the European Parliament and of the Council in support of Directive 95/46/EC of the European Parliament and of the Council and in support of Union’s security industrial policy. [↑](#footnote-ref-1)