ATTPS | Achieving The Trust Paradigm Shift

Deliverable D2.1

Recommendations to standardisation bodies

Version 0.8

Editor: Felix Gomez Marmol (NEC)

Contributors: All ATTPS partners

2015-10-29

Table of content

1. Introduction

As one of the three key objectives of the ATTPS project, this document describes how project partners actively contribute to interoperability and standardisation at European level on trustworthy information and communication technology (ICT) solutions by means of:

- Identifying relevant standardisation bodies and contributing to selected bodies to promote the trust paradigm shift and ensure that trust issues are sufficiently covered in the most relevant standardisation bodies.
- Developing generic trust architectures for mobile service and platform integrity, trusted stack, data life cycle management and e-authentication.
- Driving an interoperable identity meta system with European partners as a best practice example.
- Adoption of standardisation and interoperability recommendations by exiting standardisation bodies and national governments.
- Contributing to the price reduction of trustworthy ICT solutions.
- Monitoring and reporting on trust in standardisation bodies.

Already demonstrated and documented in the ATTPS deliverables “D3.1 End report generic trust architectures” [1], “D3.2 Interoperable identity meta system with European partners” [2] and “D3.5 Harmonized e-authentication architecture in collaboration with STORK platform” [3], this document focuses on the standardisation part of the above mentioned objectives. In section 2 we first identify and summarize relevant existing standardisation bodies (SDOs) and national government. Section 3 emphasizes how project partners have been involved in relevant SDOs and how achieved results of ATTPS are actively contributed to existing SDOs. Section 4 describes the current future plans on standardisation activities of ATTPS partners, followed by section 5 which concludes this document.

2. Summary of Relevant Existing Standardisation Bodies and National Governments

This section summarises the most important Standards Developing Organizations (SDO), relevant for the topics and achievements of the ATTPS project. Each SDO has been analysed and observed if results of ATTPS can or should be introduced and implemented to it.

2.1 ITU-T Study Group 17

ITU-T Study Group 17 (SG17) [4] coordinates security-related work across all ITU-T Study Groups. Often working in cooperation with other SDOs and various ICT industry consortia, SG17 deals with a broad range of standardization issues.

To give a few examples, SG17 is currently working on cybersecurity; security management; security architectures and frameworks; countering spam; identity management; the protection of personally identifiable information; and the security of applications and services for the Internet of Things (IoT), smart grids, smartphones, web services, social networks, cloud computing, mobile financial systems, IPTV and telebiometrics.

One key reference for security standards in use today is *Recommendation ITU-T X.509* for electronic authentication over public networks. ITU-T X.509, a cornerstone in designing applications relating to public key infrastructure (PKI), is used in a wide range of applications; from securing the connection between a browser and a server on the web, to providing digital signatures that enable e-commerce transactions to be conducted with the same confidence as in a traditional system. Without wide acceptance of the standard, the rise of e-business would have been impossible.

Cybersecurity remains high on SG17's agenda. Additionally, SG17 is coordinating standardization work covering e-health, open identity trust framework, Near Field Communication (NFC) security, and Child Online Protection.

2.2 ISO/IEC/JTC1/SC27

ISO/IEC JTC 1/SC 27 IT Security techniques [5] is a standardization subcommittee of the Joint Technical Committee ISO/IEC JTC 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). ISO/IEC JTC 1/SC 27 develops International Standards, Technical Reports, and Technical Specifications within the field of information and IT security. Standardization activity by this subcommittee includes general methods, management system requirements, techniques and guidelines to address both information security and privacy. Drafts of International Standards by ISO/IEC JTC 1 or any of its subcommittees are sent out to participating national standardization bodies for ballot, comments and contributions. Publication as an ISO/IEC International Standard requires approval by a minimum of 75% of the national bodies casting a vote. The international secretariat of ISO/IEC JTC 1/SC 27 is the Deutsches Institut für Normung (DIN) located in Germany.

The scope of ISO/IEC JTC 1/SC 27 is "the development of standards for the protection of information and ICT. This includes generic methods, techniques and guidelines to address both security and privacy aspects, such as:

- Security requirements capture methodology;
- Management of information and ICT security; in particular information security management systems, security processes, security controls and services;
- Cryptographic and other security mechanisms, including but not limited to mechanisms for protecting the accountability, availability, integrity and confidentiality of information;
- Security management support documentation including terminology, guidelines as well as procedures for the registration of security components;
- Security aspects of identity management, biometrics and privacy;

- Conformance assessment, accreditation and auditing requirements in the area of information security management systems;
- Security evaluation criteria and methodology.

ISO/IEC JTC 1/SC 27 engages in active liaison and collaboration with appropriate bodies to ensure the proper development and application of SC 27 standards and technical reports in relevant areas."

2.3 CEN / ETSI (activities on Trust Service Providers)

The European Telecommunications Standards Institute (ETSI) is an independent, not-for-profit, standardization organization in the telecommunications industry (equipment makers and network operators) in Europe, with worldwide projection. ETSI produces globally-applicable standards for Information and Communications Technologies (ICT), including fixed, mobile, radio, converged, broadcast and Internet technologies. Significant ETSI technical committees and Industry Specification Groups (ISGs) include SmartM2M (for machine-to-machine communications), Intelligent Transport Systems, Network Functions Virtualisation, *Cyber Security*, Electronic Signatures and Infrastructures, etc.

Regarding the current standards for Certification and Other Trust Service Providers [6], ETSI provides the following ones:

- EN 319 403 v2.2.2: Trust Service Provider Conformity Assessment - Requirements for conformity assessment bodies assessing Trust Service Providers
- EN 319 411-2: Policy requirements for certification authorities issuing qualified certificates
- EN 319 411-3: Policy requirements for Certification Authorities issuing public key certificates. Note: Excludes web site certificates based on CAB Forum requirements

- TS 102 042: Policy requirements for Certification Authorities issuing public key certificates. Note: Includes requirements for web site certificates based on CAB Forum requirements
- TS 102 023: Policy requirements for time-stamping authorities
- TS 102 158: Policy requirements for Certification Service Providers issuing attribute certificates usable with Qualified certificates
- TS 119 412-2: Profiles for Trust Service Providers issuing certificates; Part 2: Certificate Profile for certificates issued to natural persons
- EN 319 412-5: Profiles for Trust Service Providers issuing certificates; Part 5: Extension for Qualified Certificate profile
- TS 119 612: Trusted Lists

By the time of writing this deliverable, these are the standards for Certification and Other Trust Service Providers currently under development or review in ETSI:

- EN 319 401 v2.0.0: General Policy Requirements for Trust Service Providers
- EN 319 411-1 v1.0.0: Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General Requirements. Note: Incorporates requirements for web site certificates with requirements previously specified in 319 411-3
- EN 319 411-2 v2.0.6: Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. Note: Extends requirements in part 1 with specific requirements for EU qualified certificates
- EN 319 421 v1.0.0: Policy and Security Requirements for Trust Service Providers issuing Electronic Time-Stamps

- EN 319 412-1 v1.0.0: Certificate Profiles; Part 1: Overview and common data structures
- EN 319 412-2 v2.0.15: Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
- EN 319 412-3 v1.0.0: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
- EN 319 412-4 v1.0.0: Certificate Profiles; Part 4: Certificate profile for web site certificates issued to organisations
- EN 319 412-5 v2.0.12: Certificate Profiles; Part 5: QCStatements
- EN 319 422 v1.0.0: Time stamping protocol and electronic time-tamp profiles

2.4 ETSI (activities on Identity and Access Management for Networks and Services)

The Industry Specification Group (ISG) Identity and access management for Networks and Services (INS) [7] takes Identity and Access Management beyond the current prime focus on the web and application domains and some limited NGN (Next Generation Network) areas, to focus on networks and services in the future digital space. A major goal is to enable new service and business approaches to drive economy in Europe and beyond by applying advanced IdM standards to the Future Internet and the IoT. The ISG supports convergence between networks, services and applications, emphasizing the need for user-centrism.

A major concern is to support interoperability as well as federation at all levels including networks, such as among operators, enterprise and home.

The ISG provides group specifications for which four key work items have been defined to address questions such as:

- How can identity management solutions in the domains of operators or ISPs interoperate with the enterprise and home domains?
- How can distributed access control mechanisms be handled and thereby deal sufficiently with the privacy of data, as well as with strict service, user and legal policies?
- How can user profiles be managed in a distributed manner, and in particular how can operators act as identity brokers in such an environment?
- How can trust be negotiated and managed among (or within) federated identity management systems?

2.5 ENISA

The European Union Agency for Network and Information Security, originally European Network and Information Security Agency (ENISA) [8], is an agency of the European Union. ENISA was created in 2004 by EU Regulation No 460/2004 and is fully operational since September 1, 2005. It has its seat in Heraklion, Crete (Greece). ENISA supported 2010-, 2012- and Cyber Europe 2014 pan-European cybersecurity exercises.

The objective of ENISA is to improve network and information security in the European Union. The agency has to contribute to the development of a culture of network and information security for the benefit of the citizens, consumers, enterprises and public sector organisations of the European Union, and consequently will contribute to the smooth functioning of the EU Internal Market. ENISA assists the Commission, the Member States and, consequently, the business community in meeting the requirements of network and information security, including present and future EU legislation. ENISA ultimately strives to serve as a centre of expertise for both Member States and EU Institutions to seek advice on matters related to network and information security.

The agency's regulation tasks focus on:

- Advising and assisting the Commission and the Member States on information security and in their dialogue with industry to address security-related problems in hardware and software products.
- Collecting and analysing data on security incidents in Europe and emerging risks.
- Promoting risk assessment and risk management methods to enhance our capability to deal with information security threats.
- Awareness-raising and co-operation between different actors in the information security field, notably by developing public / private partnerships with industry in this field.
- More concretely, see our activities in Computer Emergency Response Teams, CIIP & Resilience, Risk Management-Risk Assessment and Identity & Trust, directly per section, or for an overview, in “our activities".

The five main areas of activity of ENISA are as follows:

- CERT (Computer Emergency Response Team)
- CIIP (Critical Information Infrastructure Protection) and Resilience
- Identity & Trust
- Risk Management
- Stakeholder Relations

In particular, the identity and trust team supports European Commission on the implementation of the Digital Agenda for Europe, in the reform and implementation of couple of policy documents. For instance, ENISA supports EC in its efforts to guide National Regulatory Agencies (NRAs) in the implementation of article 4 of the ePrivacy Directive and is consulting with stakeholders on the development of an integrated approach for secure services supporting data protection. The team summarises information for the MSs and

European Commission in the form of recommendations. It also contributes to EC's policy and strategic initiatives and monitors those actions and recommendations are properly addressed by the stakeholders. The overall objectives of the team are:

- Identifying results to be used in awareness raising activities such as trainings, media campaigns targeting specific audiences;
- Investigating the discrepancies between legal fundamental rights expectation and the practice in online services with regard to the principle of minimal disclosure and the "right to be forgotten";
- Increasing the trust in the online services and the infrastructure supporting them;
- Supporting the implementation of a pan European of Trust-marks (seals) in line with the EC's actions in this field with focus in specific areas of application (e-government services, etc.).

2.6 3GPP SA3

The 3rd Generation Partnership Project (3GPP) unites [Seven] telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as "Organizational Partners" and provides their members with a stable environment to produce the Reports and Specifications that define 3GPP technologies.

The project covers cellular telecommunications network technologies, including radio access, the core transport network, and service capabilities - including work on codecs, security, quality of service - and thus provides complete system specifications. The specifications also provide hooks for non-radio access to the core network, and for interworking with Wi-Fi networks.

In particular, SA WG3 [9] is responsible for security and privacy in 3GPP systems, determining the security and privacy requirements, and specifying the security

architectures and protocols. The WG also ensures the availability of cryptographic algorithms which need to be part of the specifications.

SA WG3 has the overall responsibility for security and privacy in 3GPP systems. The WG will perform analysis of potential threats to these systems. Based on the threat analysis, the WG will determine the security and privacy requirements for 3GPP systems, and specify the security architectures and protocols. The WG will ensure the availability of any cryptographic algorithms which need to be part of the specifications. The WG will accommodate, as far as is practicable, any regional regulatory variations in security objectives and priorities for 3GPP partners. The WG will further accommodate, as far as is practicable, regional regulatory requirements that are related to the processing of personal data and privacy.

The subworking group SA WG3-LI will detail the requirements for lawful interception in 3GPP systems, and produce all specifications needed to meet those requirements. This work shall be performed in conjunction with the regional standards bodies.

2.7 OASIS Cloud TC and ORMS (activities on Reputation Management)

The Organization for the Advancement of Structured Information Standards (OASIS) is a global nonprofit consortium that works on the development, convergence, and adoption of standards for security, IoT, energy, content technologies, emergency management, and other areas.

The purpose of the OASIS Identity in the Cloud TC [10] is to collect and harmonize definitions, terminologies and vocabulary of Cloud Computing, and develop profiles of open standards for identity deployment, provisioning and management. If needed, the TC will seek to re-use existing work. The TC will collect use cases to help identify gaps in existing Identity Management standards. The use cases will be used to identify gaps in current standards and investigate the need for profiles for achieving interoperability within current standards, with a preference for widely interoperable and modular methods.

Additionally, the use cases may be used to perform risk and threat analyses. Suggestions to mitigate the identified risks and the threats and vulnerabilities will be provided.

The TC will focus on collaborating with relevant standards organizations such as the Cloud Security Alliance and the ITU-T, in the area of cloud security and Identity Management. Liaisons will be identified with other standards bodies, and strong content-sharing arrangements sought where possible, subject to applicable OASIS policies.

Additionally, the purpose of the OASIS ORMS TC [11] is to develop an Open Reputation Management System (ORMS) that provides the ability to use common data formats for representing reputation data, and standard definitions of reputation scores. The system will not define algorithms for computing the scores. However, it will provide the means for understanding the relevancy of a score within a given transaction. The TC's output will enable the deployment of a distributed reputation systems that can be either centralized or decentralized with the ability for aggregators and intermediaries to be part of the business model.

2.8 Kantara

Kantara Initiative [12] provides strategic vision and real world innovation for the digital identity transformation. Developing initiatives including: Identity Relationship Management, User Managed Access (EIC Award Winner for Innovation in Information Security 2014), Identities of Things, and Minimum Viable Consent Receipt, Kantara Initiative connects a global, open, and transparent leadership community.

Kantara Initiative members take the lead to discover strategic issues at the intersection of identity, IoT, and usability. This is what they call “connected life.” Their Members develop strategies and innovations that simplify our increasingly complex connected lives. Networked devices and sensors make up the fabric of the IoT. Leveraging mobile devices, sensors, and wearables is the future of identity and personal data. Kantara Initiative

develops innovations to solve real world problems for the identity based digital transformation.

While connections to digital services and technologies grow, data generated by those connections is a challenge to manage. In the landscape of identity, security, and access technology and policy, varying national approaches and schemes exist. Governments and industry are connecting more and more to leverage their strengths for provision of services. This is the world of borderless IdM, where governments and industry seek to harmonize. Kantara Initiative develops assurance and interoperability programs to support the trust layer of on-line transactions.

The Trust Services interoperability groups are:

- Identity Assurance: Develops the Identity Assurance Framework as the controlling documents for the Kantara Identity Assurance Program.
- Health Identity Assurance: Provides review and expertise of the Identity Assurance Framework with a special focus on eHealth policy and technical interoperability.
- eGovernment: Provides industry expert insight with regard to national identity policy and interoperability programs.
- Federation Interoperability: Develops profiles and supporting materials for Kantara Initiative Federation Interoperability efforts including technical profiles development and harmonization of business cases for trusted federation and trust framework meta-model.
- Cloud Identity & Security Best Practices: Develops industry expert input with regard to cloud security and best practices.

3. ATTPS Relevant Activities in Important Standardisation Bodies (SDOs)

According to the Standardisation Bodies (SDOs) introduced in Section 2, this section describes in more detail which SDOs discussed or standardised technologies, relevant for ATTPS related activities. This section also includes specific contributions of ATTPS partners, relevant to some of the SDOs introduced in Section 2.

Several project partners participated in ETSI Cloud Standards Coordination [13] meeting (17 April 2013, Brussels, Belgium) to promote inclusion of data-centric security and trust solutions on the cloud standardisation roadmap.

3.1 GEMALTO

The key role of Standard Bodies in the digital security eco-system

As a member of ATTPS and a leader in Digital Security, Gemalto is actively participating to 30+ industry associations and standard bodies covering all aspects of digital services from payments, enterprise security, government programs and telecoms. Standardization bodies are key factors for the success of digital services by providing clear and formal paths for ICT solutions deployment: products and services specifications are made available to the entire developer's community, interoperability requirements and universal definitions of deliverables are set to facilitate the go-to-market for all stakeholders within the eco-system.

To name a few very important standard bodies for Gemalto, the FIDO alliance [33] is setting new standards for strong authentication for mobile devices, GSMA [34] is ruling 2G, 3G and 4G network management standards, ICAO [35] is managing interoperability and specs for travel documents such as ePassports, NFC Forum [36] is setting specifications for Mobile Contactless communication and security, EMVco [37] is ruling cards and Mobile NFC payments specifications and interoperability. 100% of Gemalto products and services

are designed to be in compliance with such key standard bodies; that is why it is key to bring innovative ideas, innovative architecture proposals early on in the process of standardization to ensure we develop products and services that meet the market demand and that our innovations are part of future evolutions of standards. Unlike industry consortia looking for architectural visions and best practices, standard bodies are about detailed specifications negotiations often from competitive technical routes. Industry consortia look for broad consensus, standards are all about negotiations and convergence toward specifications.

Individual contributions tested first via industry associations

Gemalto, like most ATTPS members as individual entities, contribute to security working groups of key Standard Bodies. As a member of ATTPS, Gemalto benefits from the outputs of a leading industry and academics group to validate its strategy and technologies pushed through standard bodies. ATTPS as an entity can efficiently contribute to initiatives like NIST because it represents one voice from a cluster of contributors bringing a first level of consensus on key architectural choices. On the other hand, ATTPS by nature is not a direct technology contributor to standard bodies, since ATTPS remains agnostic on detailed technical choices to implement a given trust architecture. ATTPS members as individual entities bring that type of contributions, knowing that ATTPS is one of the ways to test technical contributions toward globally approved trust architecture.

The ATTPS SRA and the proposed Trust Architecture

ATTPS recommendations for a trustworthy ICT provide precise guidance on three key areas:

i) the need for ICT services to implement a strong user authentication mechanism.

ii) the need to ensure a complete data life-cycle management solution.

iii) ways to ensure applications integrity.

Each of these pillars can be addressed with a very diverse portfolio of technologies, and pretty much all these key topics are currently under definition within the standard bodies. Bottom line ATTPS acts for its member as a testbed to propose solutions within the generally approved trust architecture [1] and that comforts individual members' effort with their technology bricks at the standards discussions level.

3.2 KTH

The Networked Systems Security (NSS) group does not currently contribute to standards. In the past, work of their members and their participation in relevant projects has influenced standards. Currently, they remain active in a relevant consortium that acts as an international harmonization body. The rest of work relates to standards but does not actively works towards changing them.

More specifically, their active involvement led to contributions to the IEEE 1609.* (notably, the 1609.2 part, the standard for security for the "Wireless Access in Vehicular Environments"), as well as the ETSI standardization body ("Intelligent transport systems (ITS); security; security services and architecture" and "Intelligent transport systems (ITS); security; trust and privacy management"). Currently, they are an active member of a harmonization body, the Car2Car Communication Consortium (C2C-CC) [32].

KTH has done extensive efforts in previous EU projects, i.e., SeVeCOM, PRESERVE, and also contributed to the C2C-CC documentation. Their work on networked systems security and privacy, with emphasis on mobile systems, simply relates to and leverages standards. As an example, relevant works (also to the demo shown in an earlier ATTPS event) include research in the areas of Vehicular Communication Systems [23][25][24][26][31], Mobile Communication [27][30] and Participatory Sensing Networks [28][29].

3.3 NEC

As OASIS has been identified to one of the relevant SDOs, NEC also actively participated in:

1. OASIS Identity in the Cloud [10], where the focus is on how identities can be represented in the area of Cloud Computing. In this context, NEC has contributed and participated in the following documents:

   - The "Identity in the Cloud Use Cases" document [14], intended to provide a set of representative use cases that examine the requirements on identity management functions as they are applied to cloud based interactions using commonly defined cloud deployment and service models. These use cases are intended to be used for further analysis to determine if functional gaps exist in current identity management standards that additional open standards activities could address.
   - The "Identity in the Cloud Gap Analysis" document [15], providing an analysis of gaps or requirements that may exist in current identity management standards. The basis for the gap analysis is the normative use cases from Identity in the Cloud Use Cases Version 1.0.
   - "Identity in the Cloud PaaS Profile" document [16], intended to provide a profile for Identity Management in Platform as a Service (PaaS) model of Cloud Computing.
   - "Mobile Cloud Identity Profile" document [17], intended to provide a profile for Mobile Identity Management.
   - "Identity in the Cloud Outsourcing Profile" document [18], intended to provide a profile for Identity Management outsourcing in Cloud Computing.

2. OASIS Cloud Authorization (CloudAuthZ) TC [19], developing enhanced models for managing authorizations and entitlements in SaaS, PaaS, and IaaS contexts. CloudAuthZ enables contextual attributes and contextual entitlements sets to be delivered to Policy Enforcement Points in real time. With CloudAuthZ, authorization decisions can be informed by data such as where users are, what they are doing, which device they are using, etc. In this context, NEC has contributed and participated in the following documents:

- "Cloud Authorization Use Cases" document [20][18], intended to provide a set of representative use cases that examine the requirements on Cloud Authorization using commonly defined cloud deployment and service models. These use cases are intended to be used for further analysis to determine if functional gaps exist in current identity management standards that additional open standards activities could address.

Since one of the main achievements of the project has been a new generic trust architecture (see: "D3.1 End report generic trust architectures" [1]), it has been investigated for which SDOs this architecture is relevant and might be standardised. As a result of our study, ITU-T "X.805: Security architecture for systems providing end-to-end communications" [21] has been selected to be most interesting to change existing standards to implement details of the ATTPS Generic Trust Architecture. It is originated by the "ITU-T Study Group (SG) 17: Security" [4] and is currently maintained under "Q2: Security architecture and framework" in SG17 [22]. Even though X.805 is already more than 10 years old, the related topics are still in discussion in Q2.

3.4 Philips

The Storage Networking Industry Association (SNIA) [38] is made up of around 400 member companies active on advancing IT technologies and standards for end to end storage and management of data. The main goal of SNIA is developing technologies, standards and educational services that make data storage less complicated for the end user. In the last decade, storage services of cloud computing have been the main focus of the use cases. Currently, SNIA has several technical committees consisting of cloud computing data storage and management, analytics and big data, cloud storage security and data protection systems in cloud computing.

Philips is a member of SNIA and active participant in the Cloud Storage TWG (Technical Work Group), which is mostly working on CDMI (Cloud Data Management Interface) [39].

CDMI is a standard proposed by SNIA with the purpose of addressing data management protocols and interfaces to interact with cloud based storage services. CDMI provides functionalities that allow storage, modification/update, and retrieval of the data to/from cloud for the end users that consume cloud services. This standard allows sharing of data with other cloud services and applications, while also allowing users to detect capabilities of the cloud computing services. In a common work with ISO, SNIA is also developing ISO 27040 which defines requirements and countermeasures of cloud computing security. All these developments and advancements are relevant for ATTPS because they are increasing the trustworthiness of the cloud that is using them.

While from the data management point of view, CDMI can be used for a wide number of use cases, from the security perspective this standard has a couple of restrictions. The reason is that CDMI addresses basic security functionalities for authentication and authorization of access requestors for data. More specifically, CDMI uses password credentials for authentication and Access Control List (ACL) for authorization and policy management/enforcement, which is coarse-grained. These limited security functionalities make CDMI suitable for the use cases where a cloud client stores data and specifies a limited number of users access the data.

This year within the Cloud Storage TWG a whitepaper called “Towards a CDMI Health Care Profile” was written [40]. This document describes a use case in which CDMI is used to handle patient records. This whitepaper has been picked up and led to the active development of two CDMI extensions. The first is a CDMI extension for the use of encrypted objects, the second is an extension for delegating access control. Both extensions are planned for publishing as public draft before the end of the year. These extensions will turn into an annex of the CDMI specification when a first implementation exists. They will be completely included in the CDMI specification as soon as a second implementation exists.

3.5 Thales

Next we list relevant standards identified per each of the major building blocks of the ATTPS generic trust architecture [1], where Thales is contributing or has contributed.

A) Identity and Access Management

There exist a number of relevant standards most of which being used since mature enough. We can quote:

- The eXtensible Access Control Markup Language (XACML) [41] is an OASIS standard, which defines a declarative access control policy language implemented in XML and a processing model describing how to evaluate authorization requests according to the rules defined in policies.
- The Security Assertion Markup Language (SAML) [42] is an OASIS open standard for exchanging authentication and authorization data between security domains, that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions).
- OAuth (Open Authorization) [43][44] is an open standard for authorization. It allows users to share their private resources (e.g. photos, videos, contact lists) stored on one site with another site without having to hand out their credentials, typically username and password.

  OAuth allows users to hand out tokens instead of credentials to their data hosted by a given service provider. Each token grants access to a specific site for specific resources and for a defined duration. This allows a user to grant a third party site access to their information stored with another service provider, without sharing their access permissions or the full extent of their data.

  OAuth 2.0 [45] is the next evolution of the OAuth protocol and is not backwards compatible with OAuth 1.0. OAuth 2.0 focuses on client developer simplicity while

providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices.

- OpenID [46] is an open standard that describes how users can be authenticated in a decentralized manner, eliminating the need for services to provide their own ad hoc systems and allowing users to consolidate their digital identities. Users may create accounts with their preferred OpenID identity providers, and then use those accounts as the basis for signing on to any website which accepts OpenID authentication.

  The OpenID protocol does not rely on a central authority to authenticate a user's identity. Moreover, neither services nor the OpenID standard may mandate a specific means by which to authenticate users, allowing for approaches ranging from the common to the novel.

- System for Cross-domain Identity Management (SCIM) [47] is an open standard for automating the exchange of user identity information between identity domains, or IT systems.

  In addition to simple user-record management (creating & deleting), SCIM can also be used to share information about user attributes, attribute schema, and group membership. Attributes could range from user contact information to group membership. Group membership or other attribute values are generally used to manage user permissions. Attribute values and group assignments can change, adding to the challenge of maintaining the relevant data across multiple identity domains. SCIM uses a standardised API through REST with data formatted in JSON or XML.

B) Secure Monitoring

In the area of Security Monitoring there is also a number of relevant standards to use but also a number to monitor since aiming at closing some of the (major) gaps. The latter being

especially true for what concerns Cyber Security where a significant initiative was launched by the NIST aiming at completing the Security Content Automation Protocol (SCAP) [48] standards focusing on capabilities for the detection, description, scoring, and reporting of flaws, misconfigurations, and attacks by a set of additional ones targeting the standardization of actions to take in response to the vulnerability indicators. This work was monitored by Thales within ATTPS but also within other flagship project (e.g. FI-PPP FI-WARE) and this is worth to continue since standardization of remediation actions is a hot topic in the context of the Security Monitoring.

- The purpose of IDMEF (Intrusion Detection Message Exchange Format) [49] is to define data formats and exchange procedures for sharing information of interest to intrusion detection and response systems and to the management systems that may need to interact with them. It is used in computer security for incidents reporting and exchanging. It is intended for easy automatic processing. Format details are described in the RFC 4765. An implementation of the data model in the Extensible Markup Language (XML) is presented and XML Document Type Definition is developed.
- Currently the standards contained within SCAP (Security Content Automation Protocol) [48] focus on capabilities for the detection, description, scoring, and reporting of flaws, misconfigurations, and attacks. A couple of representative examples are Open Vulnerability and Assessment Language (OVAL) [50] and Common Vulnerability Scoring System (CVSS) [51].
- OVAL [50] is an information security community effort to standardize how to assess and report upon the machine state of computer systems. OVAL includes a language to encode system details, and an assortment of content repositories held throughout the community.

Tools and services that use OVAL for the three steps of system assessment — representing system information, expressing specific machine states, and reporting the results of an assessment — provide enterprises with accurate, consistent, and actionable information so they may improve their security. Use of OVAL also provides for reliable and reproducible information assurance metrics and enables interoperability and automation among security tools and services.

- The Common Vulnerability Scoring System (CVSS) [51] provides an open framework for communicating the characteristics and impacts of IT vulnerabilities. Its quantitative model ensures repeatable accurate measurement while enabling users to see the underlying vulnerability characteristics that were used to generate the scores. Thus, CVSS is well suited as a standard measurement system for industries, organizations, and governments that need accurate and consistent vulnerability impact scores. Two common uses of CVSS are prioritization of vulnerability remediation activities and in calculating the severity of vulnerabilities discovered on one's systems. The National Vulnerability Database (NVD) [52] provides CVSS scores for almost all known vulnerabilities.

  In particular, NVD supports the Common Vulnerability Scoring System (CVSS) version 2 standards for all CVE vulnerabilities [53]. NVD provides CVSS 'base scores' which represent the innate characteristics of each vulnerability.

4. Future Plans and Recommendations to Standardisation Bodies

This section focusses on current approaches and future plans of standardising ATTPS relevant topics in the introduced (or additional) SDOs. It also indicates recommendations for relevant standardisation bodies, reflecting most relevant SDOs for ATTPS relevant topics.

Regarding the ATTPS Generic Trust Architecture it is planned to intensify the contact with ITU-T and initiate an ATTPS/TDL group of partners to continually adopt the architecture and standards to achieve a satisfying overlap, so that our initial design of the ATTPS Generic Trust Architecture will evolve into an architecture that is standardised in a well-known and recognized SDO.

In addition to SDOs mentioned in Sections 2 and 3, NEC actively participates in 3GPP standardization. It is currently planned to closer collaborate with the EU-GreenICN project [54], where NEC Laboratories Europe also coordinated the writing and submission of a joint Internet draft on using Information-centric networking (ICN) in disaster scenarios [55][56]. Jan Seedorf from NEC presented this contribution on disaster scenarios at the IETF-87 and IETF-88 meetings. Although disaster scenarios do not yet have a focus on security, it is foreseen that Privacy, Trust and Security will increase in its importance also in these fields of applications, thus, introducing ATTPS topics also to their focused SDOs will be one of the future goals of NEC.

With regards to security monitoring, most relevant standards are from the National Institute of Standards and Technology (NIST) and the US, due to the lack of standards on the Cyber Security field in EU. This situation may change, considering that ETSI, the leading ICT standards organization, has opened in March 2014 a new technical committee on Cybersecurity called TC Cyber [57] to address the growing demands for standards in this field. This SDO constitutes, therefore, a great candidate where to propose many of the lessons learnt in the ATTPS project on how to achieve the trust paradigm shift.

Based on the detailed work performed and reported in Section 3.5, Thales will continue to monitor relevant standards in security areas of concerns (i.e. IAM and security monitoring although not uniquely) and contribute whenever possible (e.g. ETSI TC Cyber) with a clear focus on standards less mature.

In turn, Gemalto is very active with standards bodies in the fields of Telecom, Payment, Government programs and also core technology forums such as NFC Forum, Global Platform, etc., looking at solutions for securing Identities, securing applications integrity and securing users Data. All the components provided by Gemalto to the generic trust architecture [1] and the developers tools via GTAC are core technologies that Gemalto promotes to the standard bodies.

Because of the rapid digitalization of many new markets, the activity in standard bodies is growing exponentially. Just to give a few examples about ongoing efforts: GSMA is currently in the process of defining security for IoT, using Secure Elements technology and over-the-air remote SE management. EMVco is in the process of defining its standards for Tokenization and processing for Mobile Payment services. The Common criterion is working on Mobile Security certification models to support the emergence of secure services such as Payment, Transport and Mobile ID: all these initiatives are touching key architectural elements supported by the ATTPS SRA. The foundation of ATTPS generic trust architecture includes all the components that are on tracks with standards in the making.

5. Conclusion

This deliverable, entitled “Recommendations to standardisation bodies”, starts by summarizing the existing standardization bodies that are relevant for achieving the trust paradigm shift. To this end, a number of SDOs has been identified and their main activities have been described.

Next, it also reports on the activities performed by those ATTPS members involved in some of the previously identified relevant SDOs, indicating how some of the lessons learnt in the ATTPS EU project have been brought to standardization entities.

Last, but not least, the standardization roadmap of certain ATTPS partners with regards to their security and privacy solutions is presented, ensuring this way the continuation of the

close relationship with standardization bodies that has happened all along the ATTPS project.

References

[1] "Deliverable D3.1: End report generic trust architectures", ATTPS: Achieving The Trust Paradigm Shift, European Commission, Coordination and Support Actions, 317665

[2] "Deliverable D3.2: Interoperable identity meta system with European partners", ATTPS: Achieving The Trust Paradigm Shift, European Commission, Coordination and Support Actions, 317665
http://www.trustindigitallife.eu/uploads/ATTPS%20Deliverables/ATTPS%20Deliverable%203%202%20Verizon.pdf

[3] "Deliverable D3.5: Harmonized e-authentication architecture in collaboration with STORK platform", ATTPS: Achieving The Trust Paradigm Shift, European Commission, Coordination and Support Actions, 317665

[4] ITU-T Study Group 17: Security, ITU Telecommunication Standardization Sector (ITU-T)
http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/default.aspx

[5] ISO/IEC JTC 1/SC 27 IT Security techniques, Joint Technical Committee ISO/IEC JTC 1 of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC)
http://www.iso.org/iso/iso_technical_committee?commid=45306

[6] Certification Authorities and other Trust Service Providers, European Telecommunications Standards Institute (ETSI)
https://portal.etsi.org/TBSiteMap/ESI/TrustServiceProviders.aspx

[7] Industry Specification Group (ISG) Identity and access management for Networks and Services (INS) , European Telecommunications Standards Institute (ETSI)
http://www.etsi.org/images/files/ETSITechnologyLeaflets/IdentityandaccessmanagementforNetworksandServices.pdf

[8] ENISA, European Union Agency for Network and Information Security
https://www.enisa.europa.eu

[9] SA WG3 - Security, 3rd Generation Partnership Project (3GPP)
http://www.3gpp.org/specifications-groups/sa-plenary/sa3-security

[10] OASIS Identity in the Cloud TC, OASIS | Advancing open standards for the information society
https://www.oasis-open.org/committees/id-cloud

[11] OASIS Open Reputation Management Systems (ORMS) TC, OASIS | Advancing open standards for the information society
https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=orms

[12] Kantara Initiative
https://kantarainitiative.org

[13] Cloud Standards Coordination, European Telecommunications Standards Institute (ETSI)
http://csc.etsi.org

[14] "Identity in the Cloud Use Cases Version 1.0", OASIS Identity in the Cloud TC, OASIS | Advancing open standards for the information society http://docs.oasis-open.org/id-cloud/IDCloud-usecases/v1.0/IDCloud-usecases-v1.0.pdf
[15] "Identity in the Cloud Gap Analysis Version 1.0", OASIS Identity in the Cloud TC, OASIS | Advancing open standards for the information society http://docs.oasis-open.org/id-cloud/IDCloud-gap/v1.0/IDCloud-gap-v1.0.pdf
[16] "Identity in the Cloud PaaS Profile Version 1.0", OASIS Identity in the Cloud TC, OASIS | Advancing open standards for the information society http://docs.oasis-open.org/id-cloud/IDCloud-paas/v1.0/cn01/IDCloud-paas-v1.0-cn01.html
[17] "Mobile Cloud Identity Profile Version 1.0", OASIS Identity in the Cloud TC, OASIS | Advancing open standards for the information society http://docs.oasis-open.org/id-cloud/IDCloud-mobile/v1.0/IDCloud-mobile-v1.0.pdf
[18] "Identity in the Cloud Outsourcing Profile Version 1.0", OASIS Identity in the Cloud TC, OASIS | Advancing open standards for the information society http://docs.oasis-open.org/id-cloud/IDCloud-outsourcing/v1.0/cnd01/IDCloud-outsourcing-v1.0-cnd01.html
[19] OASIS Cloud Authorization (CloudAuthZ) TC, OASIS | Advancing open standards for the information society https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=cloudauthz
[20] "Cloud Authorization Use Cases Version 1.0", OASIS Cloud Authorization (CloudAuthZ) TC, OASIS | Advancing open standards for the information society http://docs.oasis-open.org/cloudauthz/CloudAuthZ-usecases/v1.0/CloudAuthZ-usecases-v1.0.html
[21] X.805 : Security architecture for systems providing end-to-end communications, ITU Telecommunication Standardization Sector (ITU-T) https://www.itu.int/rec/T-REC-X.805-200310-I/en
[22] Question 2/17 - Security architecture and framework, ITU-T Study Group 17: Security, ITU Telecommunication Standardization Sector (ITU-T) http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/Pages/q2.aspx
[23] N. Alexiou, M. Lagan`a, S. Gisdakis, M. Khodaei, and P. Papadimitratos, ''Vespa: Vehicular security and privacy-preserving architecture,'' in ACM HotWiSec, Budapest, Hungary, Apr. 2013.
[24] S. Gisdakis, M. Lagan`a, T. Giannetsos, and P. Papadimitratos, ''SEROSA: Service oriented security architecture for vehicular communications,'' in IEEE VNC, Boston, MA, USA, Dec. 2013.
[25] N. Alexiou, S. Gisdakis, M. Lagan, and P. Papadimitratos, ''Towards a secure and privacy-preserving multi-service vehicular architecture,'' in D-SPAN, Madrid, Spain, Jun. 2013.
[26] M. Khodaei, H. Jin, and P. Papadimitratos, ''Towards deploying a scalable & robust vehicular identity and credential management infrastructure,'' in IEEE VNC, Paderborn, Germany, Dec. 2014.
[27] S. Gisdakis et al. "Secure and Privacy-Preserving Smartphone Based Traffic Information Systems". in: IEEE TITS, PP.99 (2014), pp. 1–11.
[28] S. Gisdakis, T. Giannetsos, and P. Papadimitratos. "SPPEAR: Security & Privacy-preserving Architecture for Participatory sensing Applications". in ACM WiSec. Oxford, UK, 2014.

[29] Gisdakis, Stylianos, Thanassis Giannetsos, and Panos Papadimitratos."SHIELD: A Data Verification Framework for Participatory Sensing Systems." in ACM WiSec., New York, NY, USA, Jun., 2015.
[30] H. Jin, and P. Papadimitratos. "Resilient Collaborative Privacy for Location-Based Services." in NordSec, Stockholm, Sweden, Oct. 2015.
[31] M. Khodaei and P. Papadimitratos, ‘‘Identity and Credential Management in Vehicular Communication Systems’’ to appear in IEEE VT Magazine, Dec. 2015.
[32] Car2Car Communication Consortium
https://www.car-2-car.org
[33] FIDO (Fast IDentity Online) Alliance
https://fidoalliance.org/
[34] GSMA (Groupe Speciale Mobile Association)
http://www.gsma.com/
[35] ICAO (International Civil Aviation Organization)
http://www.icao.int/
[36] NFC Forum
http://nfc-forum.org/
[37] EMVco (Europay, MasterCard, and Visa Consortium)
https://www.emvco.com/
[38] Storage Networking Industry Association (SNIA)
http://www.snia.org/
[39] Cloud Data Management Interface (CDMI), Storage Networking Industry Association (SNIA)
http://www.snia.org/cdmi
[40] “Towards a CDMI Health Care Profile”, Cloud Storage TWG, Storage Networking Industry Association (SNIA)
http://www.snia.org/sites/default/files/Towards%20a%20CDMI%20Health%20Care%20Profile%20%281%29.pdf
[41] OASIS eXtensible Access Control Markup Language (XACML) TC, OASIS | Advancing open standards for the information society
https://www.oasis-open.org/committees/xacml/
[42] OASIS Security Services (SAML) TC, OASIS | Advancing open standards for the information society
https://www.oasis-open.org/committees/security/
[43] OAuth (Open Authorization) Community Site
http://oauth.net/
[44] “The OAuth 1.0 Protocol”, Internet Engineering Task Force (IETF), RFC5849
https://tools.ietf.org/html/rfc5849
[45] “The OAuth 2.0 Authorization Framework”, Internet Engineering Task Force (IETF), RFC6749
https://tools.ietf.org/html/rfc6749
[46] OpenID Foundation website
http://openid.net/
[47] System for Cross-domain Identity Management (SCIM)

http://www.simplecloud.info/
[48] Security Content Automation Protocol (SCAP), National Institute of Standards and Technology (NIST)
http://scap.nist.gov/
[49] The Intrusion Detection Message Exchange Format (IDMEF), Internet Engineering Task Force (IETF), RFC4765
https://tools.ietf.org/html/rfc4765
[50] Open Vulnerability and Assessment Language (OVAL), The MITRE Corporation
https://oval.mitre.org/
[51] Common Vulnerability Scoring System (CVSS), Forum of Incident Response and Security Teams (FIRST)
https://www.first.org/cvss
[52] National Vulnerability Database (NVD), National Institute of Standards and Technology (NIST)
https://nvd.nist.gov/
[53] Common Vulnerabilities and Exposures (CVE), The MITRE Corporation
https://cve.mitre.org/
[54] Architecture and Applications of Green Information Centric Networking (GreenICN), European Union Seventh Framework Programme (FP7/2007-2013), grant agreement 608518
http://www.greenicn.org/
[55] J. Seedorf and Y. Yang: “CDNI footprint and capabilities advertisement using alto”, Internet-Draft draft-seedorf-cdni-request-routing-alto-06, Internet Engineering Task Force, February 2014. Work in progress.
[56] M. Arumaithurai, J. Seedorf, A. Tagami, K. Ramakrishnan, and N. Blefari Melazzi: “Using ICN in disaster scenarios”, Internet-Draft draft-seedorf-icn-disaster-00, Internet Engineering Task Force, July 2013. Work in progress.
[57] TC Cyber, European Telecommunications Standards Institute (ETSI)
https://portal.etsi.org/tb.aspx?tbid=824&SubTB=824