D8.12 Architecture for Standardization V2

*Fatbardh Veseli, Dieter M. Sommer, Jan Schallaöck,
Ioannis Krontiris*

Editor:	*Fatbardh Veseli (Goethe University Frankfurt)*
Reviewers:	*Ioannis Stamatiou (Computer Technology Institute and Press "Diophantus"), Michael Østergaard Pedersen (Miracle A/S)*
Identifier:	*D8.12*
Type:	*Deliverable*
Version:	*2.0*
Date:	*2014-11-06*
Status:	*Final*
Class:	*Public*

Abstract

Standardization is considered of particular importance for the dissemination of ABC4Trust results. This deliverable marks the final version of the architecture for standardization. It provides a number of useful standardization projects and bodies, for which the ABC4Trust architecture is relevant, and describes the key areas of our contribution in drafting these standardization projects. We look closer at two particular standardization projects within the Joint Technical Committee ISO/IEC JTC 1, *Information technology*, Subcommittee SC 27, *IT Security techniques* Working Group WG 5 *Identity Management and Privacy Technologies*, namely ISO/IEC 24760 and ISO/IEC 29101, and have a general overview of the standardization ecosystem with a number of other projects. In addition, the deliverable identifies potential risks to privacy caused by malicious Verifiers and proposes standardization of presentation policies as a way to overcome such risks. Finally, we also describe additional standardization efforts that are based on Privacy-ABC technologies, and give an overview of further standardization projects that are related to the architecture of Privacy-ABC technologies.

The research leading to these results has received funding from the European Community's Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 257782 for the project Attribute-based Credentials for Trust (ABC4Trust) as part of the "ICT Trust and Security Research" theme.

Members of the ABC4TRUST consortium

1.	Alexandra Institute AS	ALX	Denmark
2.	CryptoExperts SAS	CRX	France
3.	Eurodocs AB	EDOC	Sweden
4.	IBM Research – Zurich	IBM	Switzerland
5.	Johann Wolfgang Goethe-Universität Frankfurt	GUF	Germany
6.	Microsoft Belgium NV	MS	Belgium
7.	Miracle A/S	MCL	Denmark
8.	Nokia	NSN	Germany
9.	Computer Technology Institute and Press “Diophantus”	CTI	Greece
10.	Söderhamn Kommun	SK	Sweden
11.	Technische Universität Darmstadt	TUD	Germany
12.	Unabhängiges Landeszentrum für Datenschutz	ULD	Germany

***Disclaimer**: The information in this document is provided "as is", and no guarantee or warranty is given that the information is fit for any particular purpose. The above referenced consortium members shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of these materials subject to any liability which is mandatory due to applicable law.*

List of Contributors

Chapter	Author(s)
Executive Summary	Fatbardh Veseli (GUF), Ioannis Krontiris (GUF)
Chapter 1	Fatbardh Veseli (GUF), Jan Schallaböck (ULD), Ioannis Krontiris (GUF)
Chapter 2	Fatbardh Veseli (GUF)
Chapter 3	Fatbardh Veseli (GUF)
Chapter 4	Fatbardh Veseli (GUF)
Chapter 5	Fatbardh Veseli (GUF), Dieter M. Sommer (IBM), Jan Schallaböck (ULD)

Executive Summary

ABC4Trust considers standardization to be a strong outreach activity, which has thus gained considerable attention from the project. The final version of the ABC4Trust architecture [12] has been published and provides a high level of maturity. This deliverable outlines the landscape of the relevant standardization bodies and projects, and describes the major contributions from the architecture of ABC4Trust to international standardization projects. In this regard, ABC4Trust has identified two projects of high relevance within ISO/IEC JTC 1/SC 27/WG 5.

The first project is ISO/IEC 24760: Information Technology – Security Techniques – *A framework for identity management*, which consists of three parts, namely Part 1 – *Terminology*, Part 2 – *Reference architecture and requirements*, and Part 3 – *Practice*. We present a number of key contributions from the ABC4Trust architecture to Part 2 and Part 3 of this standard during their drafting stages, including inclusion of some key privacy features of Privacy-ABC technologies within the architecture framework in Part 2, and providing an overview of ABC4Trust architecture as part of Part 3.

The second project is ISO/IEC 29101: Information Technology – Security Techniques – *Privacy Architecture Framework*, which now contains a special annex on the architecture of an application that uses Privacy-ABC technologies. This annex outlines how applications that use Privacy-ABC technologies can comply with the privacy principles of ISO/IEC 29100 and require thus a minimal number of extra controls to be implemented in order to comply with ISO/IEC 29101.

Taking an additional and different perspective on standardization, we look at the possibility of using standardization and certification of presentation policies to increase trust in infrastructures and applications using Privacy-ABC technologies.

Furthermore, we present an overview of additional standardization projects within ISO, which we also considered relevant, namely we briefly describe ISO/IEC 29115: Information technology – Security techniques - Entity authentication assurance, which delivers metrics for four levels of authentication assurances; ISO/IEC CD 29146 – Information technology – Security techniques – A framework for access management, which provides a framework for the definition of access management and the secure management of the process to access information; and ISO 29191: Information technology - Security techniques – Requirements for partially anonymous, partially unlinkable authentication, which defines requirements for partially anonymous, partially unlinkable authentication. In addition, we also present a description of recent proposal for a joint study period within ISO/IEC JTC 1/SC 27 WG 2 and WG 5 on “A privacy-respecting identity management scheme using attribute-based credentials”. Finally, we provide a number of different prospects and an outlook on other standardization projects of relevance.

Table of Contents

1 Introduction 8

1.1 Standardization and privacy legislation 8
1.2 An Overview of the ABC4Trust Architecture 9
1.3 Organization of the document 12

2 ABC4Trust architecture and ISO/IEC 24760 13

2.1 ISO/IEC 24760 – An Overview 13
2.2 ABC4Trust architecture and ISO/IEC 24760-2 13
2.3 ABC4Trust architecture and ISO/IEC 24760-3 14
2.4 Summary 15

3 ABC4Trust architecture and ISO/IEC 29101 16

3.1 Terminology 16
3.2 ABC4Trust contribution to ISO/IEC 29101 16
3.3 Summary 17

4 Policy standardization and certification 19

4.1 Identification of practical privacy risks 19
4.2 Certification and standardization as a solution 19

5 Other related projects in standardization and Outlook 21

5.1 Further relevant standards within ISO/IEC JTC 1/SC 27/WG 5 21
5.2 New Study Period based on Privacy-ABC technologies 22
5.3 Other prospects and outlook 22

6 References 23

Index of Figures

Figure 1.1: Entities and Interactions Diagram 9
Figure 1.2: A Sample Presentation Scenario 10
Figure 1.3: An overview of the interaction between the User and the Verifier, and involved components 12

Index of Tables

Table 3.1 - Main actors in ISO/IEC 29100 framework 16

1 Introduction

ABC4Trust has brought together industry, academia and others to address the federation and interchangeability of technologies that support trustworthy yet privacy-preserving Attribute-based Credentials (Privacy-ABCs) [1]. Privacy-ABC technologies are an important building block of identity management systems, which enable the privacy-enhancing features for the users, and at the same time achieve strong authentication for service providers. Among the main privacy features of Privacy-ABCs include *selective (minimal) disclosure* of attributes, *unlinkability* of issuance to presentation, and different levels of (un)linkability during interactions of the user with service providers.

This chapter discusses the motivation for standardization, namely a relation between standardization and privacy legislation. Further, it provides an overview on the features of Privacy-ABC technologies, as described in the deliverable on the architecture of Privacy-ABC technologies [10], and describes briefly the organization of this document.

1.1 Standardization and privacy legislation

Especially in the European Union's privacy legislation technical standards are given significant role, e.g. when the law requires technical mechanisms to be put in place to protect the privacy of users. The specific mechanisms are usually not spelled out in the law itself, as the regulation aims to be “technology neutral”.[1] Instead, the term “state of the art” is often referred to, cf. art. 4 para 1 in [2] recital 46 and art. 17 para 1 in [3]. How is this term then related to international standards? one might ask. There is currently little legal research in this specific field, so the details may still be vague. From earlier discussions in other areas such as technical regulation as nuclear safety, waste, etc we probably can safely assume that standards give high prejudice whether or not the state of the art has been met.[2] In other words: In borderline cases, courts will draw to existing standards to determine whether or not legal compliance has been met, whenever the understanding of the legal term “state of the art” is in question.

Likewise data protection agencies recognize international standards when inspecting the implementation of technical means of a service provider [4]. Consequentially procurement often requires products or services to meet certain standards. This even furthers the relevancy of technical standards as a whole.

In European data protection legislation the aforementioned is given emphasis already in the `95 Directive on data protection [3] as well as in the E-Privacy directive [2]. On January 25th, 2012, the European Commission officially published a first proposal for a new regulation on data protection [5] which will be superseding the `95 Directive and effectively will communitarize (as well as

[1] For a more thorough discussion of the term and its implications, cf. 2.

[2] cf, eg. Bundesverfassungsgericht (Verfassungsgericht der Bundesrepublik Deutschland), Beschluß des Zweiten Senats vom 8. August 1978, Geschäftszeichen 2 BvL 8/77, amtliche Sammlung BVerfGE 49, 89; sogenannte

[2] cf, eg. Bundesverfassungsgericht (Verfassungsgericht der Bundesrepublik Deutschland), Beschluß des Zweiten Senats vom 8. August 1978, Geschäftszeichen 2 BvL 8/77, amtliche Sammlung BVerfGE 49, 89; sogenannte
„Kalkar I"-Entscheidung, cit. in Wikipedia: http://de.wikipedia.org/wiki/Anerkannte_Regeln_der_Technik

"lisbonize"[3] as we will describe in the following) this field of regulation. This proposal appears to further strengthen the relevancy of technical standards. Namely, its recital 66 and in Article 23 para 1 thereof explicitly refers to the state of the art, with the latter being augmented by the process of the superseded comitology process, cf. [6] for a more detailed analysis. The latter gives the commission the power to mandate specific standards pending lack of objection by the parliament. Effectively, such regulation would allow for a strong harmonization of technical measures in specific domains under the control of the Commission.

1.2 An Overview of the ABC4Trust Architecture[4]

Before giving an overview of the ABC4Trust architecture we first need to introduce the different involved entities, and the type of interactions that they engage in.

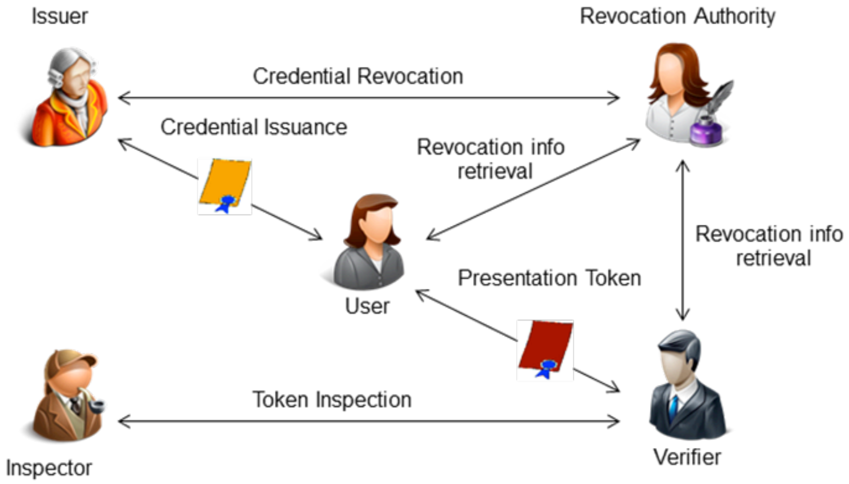

Figure 1.1: Entities and Interactions Diagram

As shown in Figure 1.1, the following five architectural entities can interact in the various possible scenarios:

- The *User* is at the centre of the picture, collecting *Credentials* from various Issuers and controlling which information from which credentials she presents to which verifiers. The human User is represented by her *User Agent*, a software component running either on a local device (e.g., on the User's computer or mobile phone) or remotely on a trusted cloud service. The User may own special hardware tokens to which credentials can be bound to improve security. In the identity management literature, the User is sometimes referred to as the requestor or the subject.

[3] The term has been coined for the new powers granted to the commission as part of the Lisbon treaty, which are herein referred to as the amended comitology procedure, which, of course is slightly misleading, as the underlying regulation 182/2011, cf. [6], is in fact not really amending but replacing the comitology process.

[4] The text for this chapter is an abbreviated version of "Chapter 2 – Features and Concepts of Privacy-ABCs", which is published in "Deliverable 2.2 – Architecture for Privacy-ABC technologies – Final Version" [10].

- An *Issuer* issues credentials to Users, thereby vouching for the correctness of the information contained in the credential with respect to the User to whom the credential is issued. Before issuing a credential, the Issuer may have to authenticate the User, which it may do using Privacy-ABCs, using a different online mechanism (e.g., username and password), or using out-of-band communication (e.g., by requiring the User to physically present herself at the Issuer's office). In the identity management literature, the Issuer is sometimes referred to as the identity provider or attributes authority.
- A *Verifier* protects access to a resource or service that it offers by imposing restrictions on the credentials that Users must own and the information from these credentials that Users must present in order to access the service. The Verifier's restrictions are described in its presentation policy. The User generates from her credentials a presentation token that contains the required information and the supporting cryptographic evidence. In the identity management literature, the Verifier is sometimes also referred to as the relying party, the server, or the service provider.
- A *Revocation Authority* is responsible for revoking issued credentials, so that these credentials can no longer be used to generate a presentation token. The use of a particular Revocation Authority may be imposed by the Issuer, in which case the revoked credentials cannot be used with any Verifier for any purpose, or by the Verifier, in which case the effect of the revocation is local to the Verifier and does not affect presentations with other Verifiers. Both the User and the Verifier must obtain the most recent revocation information from the Revocation Authority to generate, respectively verify, presentation tokens.
- An *Inspector* is a trusted authority who can, under specific circumstances, de-anonymize presentation tokens. To make use of this feature, the Verifier must specify in the presentation policy the Inspector authority that should be able to recover specific attribute(s) should the predefined circumstances arise. The User is therefore aware of the de-anonymization possibility when the token is generated and actively participates to make this possible; therefore the User can make a conscious decision based on her trust in the Inspector.

In an actual deployment, some of the above roles may actually be fulfilled by the same entity or split among many. For example, an Issuer can at the same time play the role of Revocation Authority and/or Inspector, or an Issuer could later also be the Verifier of tokens derived from credentials that it issued.

A *credential* is a certified container of attributes issued by an *Issuer* to a *User*. An attribute is described by the *attribute type*, determining the semantics of the attribute (e.g., first name), and the *attribute value*, determining its contents (e.g., John). By issuing a credential, the Issuer vouches for the correctness of the contained attributes with respect to the User. The User can then later use her credentials to derive *presentation tokens* that reveal *partial* information about the encoded attributes to a Verifier.

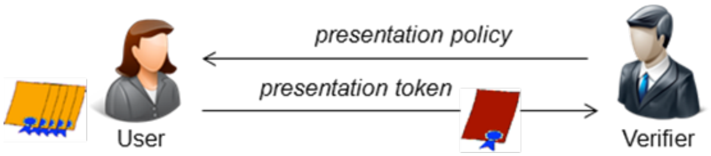

Figure 1.2: A Sample Presentation Scenario

In a typical scenario (Figure 1.2), a Verifier announces in its *presentation policy* which credentials from which Issuers it accepts and which attributes from the credential(s) must be disclosed. The

Verifier can cryptographically verify the authenticity of a received presentation token using the credential specifications and issuer parameters of all credentials involved in the presentation token. The Verifier must obtain the credential specifications and issuer parameters in a trusted manner, e.g., by using a traditional PKI to authenticate them or retrieving them from a trusted location.

To provide certified information to a Verifier (for authentication or an access decision), the User uses one or more of her credentials to derive a *presentation token* and sends it to the Verifier. A single presentation token can contain information from any number of credentials. The token can reveal a subset of the attribute values in the credentials (e.g., IDcard.firstname = "John"), prove that a value satisfies a certain predicate (e.g., IDcard.birthdate < 1993/01/01) or that two values satisfy a predicate (e.g., IDcard.lastname = creditcard.lastname).

The presentation token created in response to such a presentation policy consists of the *presentation token description,* containing a mechanism-agnostic description of the revealed information, and the *presentation token evidence,* containing opaque technology-specific cryptographic data in support of the token description.

Presentation tokens based on Privacy-ABCs are cryptographically proven to be unlinkable and untraceable, meaning that Verifiers cannot tell whether two presentation tokens were derived from the same or from different credentials, and that Issuers cannot trace a presentation token back to the issuance of the underlying credentials. However, we have considered additional mechanisms so that, with the User's consent, it enables a dedicated third party to recover this link again.

In particular, the architecture has been designed to decompose future (reference) implementations of Privacy-ABC technologies, into sets of modules and specify the abstract functionality of these components in such a way that they are independent from the cryptographic mechanisms used underneath. Currently the Reference Implementation allows instantiations of two main technologies, namely Idemix or U-Prove, which implement different signature schemes, but can share a large part of the other building blocks, such as encryption and revocation schemes.

The functional decomposition foresees possible architectural extensions to additional functional modules that may be desirable and feasible using future Privacy-ABC technologies or extensions of existing ones, so that new building blocks can be used, such as zero knowledge proofs, inspection, revocation, or signature schemes.

Figure 1.3 shows how ABC4Trust architectural modules are divided into the three abstract layers, namely *Application*, *ABC-Engine (ABCE)* and *CryptoEngine (CE)*. The ABCE *layer* contains all cryptography-agnostic methods and components for a Privacy-ABC system. That is, it contains e.g. the methods to parse an obtained presentation policy, perform the selection of applicable credentials for a given policy or trigger the mechanism-specific generation or verification of the cryptographic evidence. The ABCE-layer is invoked by the application-layer and calls out the *CryptoEngine* to obtain the mechanism-specific cryptographic data.

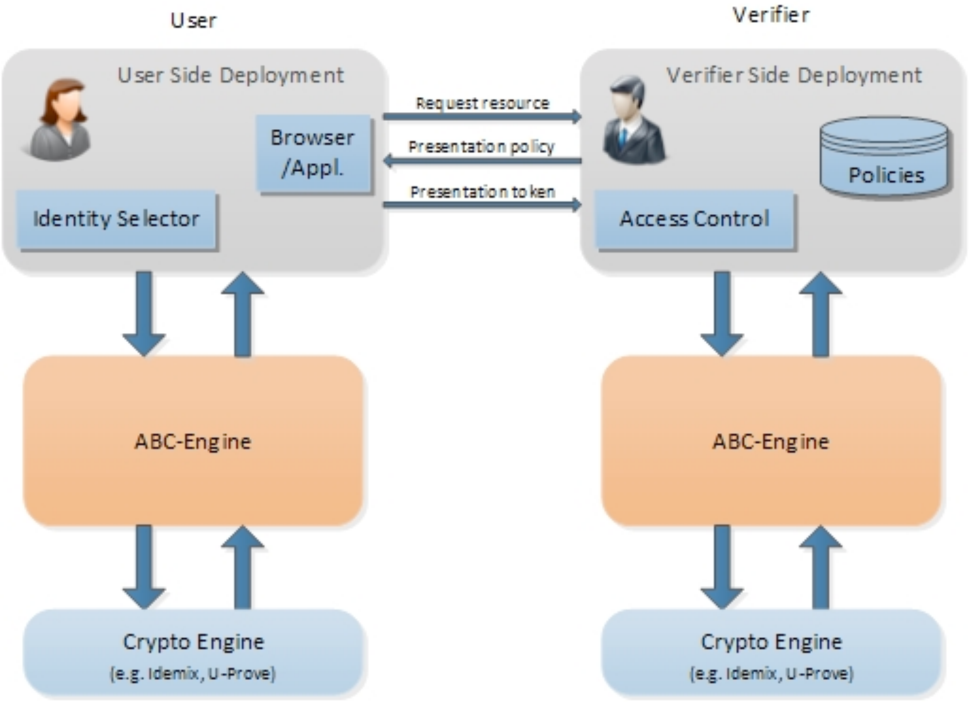

Figure 1.3: An overview of the three layers of ABC4Trust architecture at the User and Verifier side

Equally important in the architecture is the specification of the data artefacts exchanged between the implicated actors, in such a way that the underlying differences of concrete Privacy-ABC technologies are abstracted away through the definition of formats that can convey information independently from the mechanism-specific cryptographic data.

1.3 Organization of the document

The rest of this deliverable goes directly into specific standardization projects and issues, relevant for the ABC4Trust architecture. Chapter 2 gives a closer explanation of the relevance of ISO/IEC 24760 and –Taking an additional and different perspective on standardization, we provide in Chapter 4 a potential new standardization and certification possibility to overcome some potential misuse scenarios to Privacy-ABC technologies. Finally, an overview of other projects within ISO and beyond, their relationship to and their perspective for standardizing work of ABC4Trust is described in the outlook chapter (Chapter 5).

2 ABC4Trust architecture and ISO/IEC 24760

ABC4Trust defined a unified architecture for Privacy-ABC technologies. On a slightly different level but on a similar domain, ISO/IEC 24760 focuses on defining an architecture for identity management systems, and providing guidelines on their successful implementation and operationalization. In this chapter, we will present briefly the focus of three parts within ISO/IEC 24760, and have a closer look at the main contribution of ABC4Trust to two parts within the standard.

2.1 ISO/IEC 24760 – An Overview

”ISO/IEC 24760 – Information Technology – Security Techniques – A framework for identity management” is a multi-part standard that addresses the issue of efficient and effective implementation of systems that make identity-based decisions. This standard “specifies a framework for the issuance, administration, and use of data that serves to characterize individuals, organizations or information technology components, which operate on behalf of individuals or organizations.” [7] Furthermore, it “specifies fundamental concepts and operational structures of identity management.” [7].

The standard is organized into three parts:

- Part 1: Terminology and concepts,
- Part 2: Reference architecture and requirements, and
- Part 3: Practice

While Part 1 (ISO/IEC 24760-1) has already been published as an International Standard, Part 2 (ISO/IEC 24760-2) is currently at FDIS (Final Draft International Standard) stage, whereas for Part 3 (ISO/IEC 24760-3) the 2nd Committee Draft (CD) is currently prepared.

In 24760-1, the main focus of the standard is on the definition of terms for identity management, specification of core concepts for identity and identity management, as well as explanation of their relationships [7]. Part 2 provides a reference architecture for identity management, describes the lifecycle model of identity information, providing guidelines for the implementation of systems for the management of identity information, and specifying requirements for the implementation and operation of a framework for identity management [8]. Part 3 provides practical guidance for the design, implementation and operation of systems for the management of identity information [9].

Overall, the standard deals with processes around identity management and contains some of the privacy requirements in place, while the architecture of ABC4Trust provides a specific infrastructure, which has been designed having in mind the need for privacy. We will have a closer look at the contribution from the ABC4Trust architecture to Parts 2 and 3 of ISO/IEC 24760 in the following sections.

2.2 ABC4Trust architecture and ISO/IEC 24760-2

On the one hand, we have the ABC4Trust architecture, which provides a unified terminology and list of actors for Privacy-ABC technologies, which are specific enough and can be aligned together. On the other hand, ISO/IEC 24760-2 has a broader focus on a more generic architecture for identity management systems, therefore ending up on a different layer of abstraction. This results in having some of the actors in both architectures in common, although sometimes being differently labelled, such as the ABC4Trust User being identified as Principal in the ISO/IEC 24760-2 architecture, whereas some other actors have a similar notation, such as the Verifier. However, ABC4Trust does not explicitly distinguish between a Verifier and a Relying Party compared to ISO/IEC 24760-2. In addition, the ABC4Trust role of an Issuer does not have an equivalent entity in ISO/IEC 24760-2, but its role can be rather split among a number of identity-related authorities.

ABC4Trust has actively contributed to drafting Part 2 of ISO/IEC 24760. The main contribution was constantly making sure that the definitions and architecture design of the standard were made in accordance with the ABC4Trust concepts and features. This is particularly important considering the broader focus of the standard.

Two of the most prominent contributions to Part 2 come from the features of Privacy-ABC technologies, which were previously not taken into account. One came from the idea that a typical identity management system should "call home" (to the Issuer) during the presentation to get the necessary proof to authenticate the User, which constitutes one of the privacy violations of having the Issuer "track" the transactions of the User with different Relying Parties. The fact that Privacy-ABC technologies do not require such a "call-back" had to be constantly explained and corrected during different stages of the project.

A second major contribution to Part 2 was related to the incorporation of "long-lived credentials" concept. Even though the *credential* and *identity* definition in Part 1 are in line with both short- and long-lived credentials, the architecture description in Part 2 does not fully support the concept of long-lived credentials, which are core to the ABC4Trust architecture. In the concept of ABC4Trust, a credential is issued to the User, but not necessarily disclosed at the same form as received during issuance. The User can transform the credential that was issued into a *presentation token,* which is unlinkable to its issuance and may perform a number of cryptographic operations on the original credential(s) under possession. Therefore, our focus was mainly to have this privacy feature of Privacy-ABC technologies supported in this standardization project.

2.3 ABC4Trust architecture and ISO/IEC 24760-3

Part 3 of ISO/IEC 24760 is currently at a Committee Draft stage and it is focused on providing guidance for good practice in administrating identity management systems in accordance with the two previous parts of the same standard, namely Part 1 and Part 2. As such, it is less mature than Part 2, but provides a good opportunity to show Privacy-ABC technologies as good example for such an important building block of identity management.

ABC4Trust's major contribution to Part 3 is a chapter on the ABC4Trust architecture as a normative annex to the current draft. This annex shows a detailed description of an identity management scheme using attribute-based credentials. It shows the main elements (actors) of the architecture, and the main processes in this architecture, both adopted in the terminology of ISO/IEC 24760. It also includes the control steps at a management/administrative level for these technologies, as well as a description of the main layers of the ABC4Trust architecture, including the application-level components at the User side, as well as the core ABCE components layer, including the crypto engines, similar to the model depicted in Figure 1.3. Parts of these components had to be adapted with respect to terminology, but some of them reflect the actual model of the ABC4Trust architecture as defined in Deliverable D2.2 [10].

2.4 Summary

ISO/IEC 24760 is a relevant standard to compare with the architecture of ABC4Trust, since both deal with the issue of Identity Management. We have, therefore, constantly been active and continue to contribute to the projects within this series of standards, particularly to Parts 2 and 3.

The main contribution of ABC4Trust was the inclusion of the privacy-respecting concepts of Privacy-ABCs in Part 2, such as the concept of long-lived credentials and avoiding the “calling home problem” during presentation, among others. In Part 3, the draft currently contains a description of the ABC4Trust architecture among its normative annexes, which puts it among the good practice architectures.

3 ABC4Trust architecture and ISO/IEC 29101

Another important international standard with a high relevance for ABC4Trust is ISO/IEC 29101: Information technology – Security techniques – Privacy architecture framework, which was published in 2013. ISO/IEC 29101 builds on the privacy framework provided by ISO/IEC 29100 and "describes a high-level architecture framework and associated controls for the safeguarding of privacy in information and communication technology (ICT) systems that store and process personally identifiable information (PII)." [12] It "focuses on ICT systems that are designed to interact with PII principals" [12] and shows how privacy-enhancing technologies can be used to build better privacy controls.

3.1 Terminology

ISO/IEC 29101 applies the terminology defined in ISO/IEC 29100 [11]. For the purposes of the discussion presented in this chapter, the definitions presented in Table 3.1 will suffice.

Table 3.1 - Main actors in ISO/IEC 29100 framework

Term	**Definition in ISO/IEC 29100 [2]**
Personally identifiable information (PII)	any information that (a) can be used to identify the PII Principal to whom such information relates, or (b) might be directly or indirectly used to identify the PII principal
PII Principal	natural person to whom the personally identifiable information (PII) relates
PII Controller	privacy stakeholder (or stakeholders) that determines the purposes and means for processing personally identifiable information (PII) other than natural persons who use data for personal purposes
PII Processor	privacy stakeholder that processes personally identifiable information (PII) on behalf of and in accordance with the instructions of a PII controller

3.2 ABC4Trust contribution to ISO/IEC 29101

The common denominator for ABC4Trust architecture and for ISO/IEC 29101 is the focus on privacy. In comparison to ISO/IEC 24760 series, which had a more general focus on identity management systems, the focus of ISO/IEC 29101 is particularly tailored for the protection of privacy, with the protection of personally identifying information (PII) being its main focus.

Having a look at the main entities defined in Table 3.1, it is clear that the main actors differ from the ABC4Trust ones, at least from the naming perspective. The *PII Principal* is basically the same entity as the ABC4Trust *User,* whereas a *PII Controller* may typically correspond to the ABC4Trust *Verifier,* but it also includes the *Issuer,* and if applicable, one could argue whether also *Inspector* and *Revocation Authority* can be treated as PII Controllers. In practice, these entities could then use additional *PII Processors,* but that is not crucial to the ABC4Trust architecture at the current level of abstraction.

ISO/IEC 29101 considers the ICT systems of the three main actors (PII Principal, PII Controller, and PII Processor) separately. It describes the requirements for adhering to the privacy principles of ISO/IEC 29100, namely on the required technical controls that would enable respecting the following privacy principles of ISO/IEC 29100 [11]:

1) *consent and choice;*
2) *purpose legitimacy and specification;*
3) *collection limitation;*
4) *data minimization;*
5) *use, retention and disclosure limitation;*
6) *accuracy and quality;*
7) *openness, transparency and notice;*
8) *individual participation and access;*
9) *accountability;*
10) *information security; and*
11) *privacy compliance.*

From the ABC4Trust point of view, the above principles are necessary to enable and preserve user's privacy, and deploying Privacy-ABC technologies is a very effective way that supports the above principles by design. While ISO/IEC 29101 identifies a number of techniques and technologies that could be used to enable a number of these principles, mostly including a number of cryptographic techniques in combination with non-technical controls, ABC4Trust contributed to ISO/IEC 29101 by showing how its architecture already incorporates these principles without requiring the implementation of all the mentioned privacy controls in the standard.

This is well documented in the language of the ISO/IEC 29101 and included in its Annex C – "A privacy-friendly, pseudonymous system for identity and access control management". The annex describes an example architecture of an electronic university course evaluation application, depicting the separate entities (actors), their interactions, as well as technical controls that are implemented at each entity. The architecture was designed with Privacy-ABC technologies. It is meant to enable university students to evaluate courses, while providing privacy for the students and at the same time strong authentication towards the application. The design of this application is similar to the architecture implemented in one of the ABC4Trust pilots. Consequently, the annex shows how Privacy-ABC technologies can be used for a clean design of a system that complies with the privacy principles of ISO/IEC 29100.

3.3 Summary

Annex C of ISO/IEC 29101 shows the architecture of an ICT system that uses Privacy-ABC technologies to enable students to anonymously evaluate a university course. Of course, the capabilities of the Privacy-ABC technologies and the ABC4Trust architecture go beyond course evaluation applications, but focusing on a particular ICT system enabled a more precise description of the main architecture components and the protection of privacy principles they correspond to. Being included in an annex of an international standard defining a privacy architecture framework is not only a strategic asset, but also implicitly shows the feasibility of achieving privacy by design in ICT systems and the appropriateness of the ABC4Trust architecture in this regard.

4 Policy standardization and certification

In this chapter, we discuss an important aspect of privacy, namely identifying potential risk that could be exploited by malicious Verifiers and mitigation mechanisms against those. First, we provide a description of the identified potential risks in a bit more detail and then propose an approach using standardization to overcome such risks.

4.1 Identification of practical privacy risks

In the architecture of ABC4Trust [10], but also in any other system that requires authentication of the Users, the Verifier (Relying Party) defines the conditions that must be fulfilled in order for the User to get verified or authenticated. In the ABC4Trust architecture, this is done through the *presentation policy*, which defines, among other things, also the attributes of the credential(s) that the User must disclose.

Privacy-ABCs enable *selective disclosure* of attributes, which is one of the privacy features of the technology behind Privacy-ABCs. In line with the respect for users' privacy and avoiding collection of excessive amounts of personal data beyond the legitimate purpose, a Relying Party should only require disclosure of those attributes proportionate to the purpose of such disclosure.

Nevertheless, there is some potential to violating the privacy of the users even when using Privacy-ABC technologies. One of such potential risks to users' privacy may come from malicious Verifiers, who may ask for excessive amount of attributes to be disclosed during presentations. Technically, a Verifier could define such presentation policies, which would request the User to reveal all or more than necessary attributes.

Furthermore, even in the case when not all attributes are asked for, not all credential attributes have the same identification power. While some attributes may be similar for more people, it may be that some of the attributes may uniquely identify a User, as can be the case of a unique identifier of a credential, e.g. a *revocation handle* used to revoke a credential [10]. Therefore, a presentation policy should never ask for the revocation handle, as this would then kill some of the main privacy-features of Privacy-ABCs, namely this would enable linkability of user's transactions on a different level. While the architecture of Privacy-ABCs explicitly states that such unique attributes should never be disclosed (or asked for), it does not specify technical means to limit such misuse scenarios per se.

Needless to say, the above-mentioned privacy risks are not specific to Privacy-ABC technologies, but they could deserve attention in order to avoid potential risk of malicious Verifiers promoting the use of Privacy-ABC technologies, whilst at the same time exploiting them in ways they were not designed for.

4.2 Certification and standardization as a solution

To protect from such a privacy risk in practice, we propose a mechanism, which would be built on top of the existing architecture framework of Privacy-ABCs. This would involve establishing separate, independent and trusted entity, which would *certify presentation policies* of Verifiers. This relates to the increase of technical trustworthiness of the systems using Privacy-ABCs and a better transparency in general.

For a similar purpose, the new German eID scheme [22] was designed and equipped with a special security mechanism (TA - Terminal Authentication), which protects the data (credential attributes) in the card from being read from an unauthorized terminal (i.e. at the Verifier). In particular, some of the attributes which are considered to be more sensitive are restricted to a number of authorised parties only, e.g. biometric data, such as photo or fingerprints, are denied to all entities, except for "sovereign authorities", such as law enforcement agencies during border control. In consequence, the terminal needs to explicitly show that it is authorized to read the specific data (attributes) by showing a particular certificate [22]. At a more abstract level, the purpose of using this mechanism is similar, namely to prevent the Verifiers from reading unnecessary attributes from the user's credential by having certified read authorizations for specific authorized Verifiers. Although Privacy-ABCs can also be applied in additional scenarios besides eIDs, the principles of the architecture design can be similarly applied in any other scenario where such a protection mechanism is desired.

What entity would be most suitable for certifying such presentation policies in practice certainly depends on the application scenario. As an example, in the case of the German eID card, a government institution, the Issuing Office for Certificates (*Vergabestelle für Berechtigungszertifikate* (VfB), which is part of the Federal Office of Administration, (in German: *Bundesverwaltungsamt* (BVA)), is set up and made responsible for the authorization certificates to the service providers. In order to be able to read the eIDs, the service provider would have to submit evidence on the reason why access to specific personal data is necessary for the execution of the service [23]. A certificate issued by the Issuing Office enables the service provider to access the card for basic operations, such as age verification (without reading the birthdate), but may also specify fields of personal data (attributes) that the Service Provider is authorized to access.

To summarize, it is important to avoid scenarios, which could enable Verifiers or other entities to get access to data, which would violate privacy features of attribute-based credential technologies, namely selective disclosure or unlinkability of (otherwise unlinkable) Privacy-ABC tokens. This is also in line with the EU Directive on privacy and electronic communications [2], which demands service providers to "*limit the amount of personal data necessary to a strict minimum",* and the EU Data protection directive, which requires that "*the data must be adequate, relevant and not excessive in relation to the purposes for which they are processed*" [3].

This is not a typical standardization action per-se, but it can prove to be a de-facto standard in certain areas of everyday life, particularly in cases that require a stronger protection of citizens' privacy. In addition to this, one could also create practical standards for most-commonly used presentation policies. These could potentially ease the adoption of Privacy-ABC technologies if some of the most commonly used types of proofs are standardized, such as, e.g. having standard presentation policies for showing that a person is of a certain age.

There are certainly other ways to achieve similar goals, such as reputation-based mechanisms, where Users or some other entity could review different Verifiers in terms of appropriateness of their presentation policies. Nevertheless, the main point is to make clear the possibility of having additional mechanisms in place to assure the protection of the promised privacy for the Users. Finally, having the infrastructure support these privacy assurance mechanisms would hopefully increase the trust on the technology, and ensure that the promised privacy features are well preserved.

5 Other related projects in standardization and Outlook

Chapters 2 and 3 highlight the most relevant standardization projects suitable for the architecture of Privacy-ABC technologies. However, there are a number of other projects of relevance within ISO/IEC JTC 1/SC 27/ WG5, which will be presented in this chapter. In addition, we also present a concrete effort for a new study period on privacy-enhancing identity management using Privacy-ABC technologies, which takes the form of a joint work within WG2 and WG5. Finally, we give an overview of other prospects and an outlook of other parts of the architecture that have a potential for standardization.

5.1 Further relevant standards within ISO/IEC JTC 1/SC 27/WG 5

In WG 5 of ISO/IEC JTC 1/SC 27, there are three more projects of relevance:

- ISO/IEC 29191: Information technology – Security techniques – Requirements for partially anonymous, partially unlinkable authentication [13] is very closely related to the architecture of Privacy-ABC technologies, as it particularly focuses on related technologies, namely anonymous credentials and group signatures. Despite the differences in the approach, we have contributed with comments to the previous draft of this standard, and considered it to be highly relevant, as its covers ABC systems to some advanced degree; it also encompasses another cryptographic technology known as group signatures[5].
- ISO/IEC 29115: Information technology – Security techniques – Entity authentication assurance [14] delivers a metric for four levels of authentication assurance. How Privacy-ABCs relate to such authentication levels might be an interesting subject for further research, since ISO/IEC 29115 follows a traditional approach, usually matching real entities (often individuals). How this would relate to the architecture of Privacy-ABC technologies is a subject that reaches beyond technological questions, but relates to requirements design, privacy (by design) and ultimately legal frameworks, often requiring real person authentication, where this may not necessarily be the best option considering freedom and individual self-determination. ABC4Trust contributed to the previous drafts of this standard in a similar way to ISO/IEC 24760-2 by distinguishing between the concept of credential and presentation tokens, namely on the fact that the User can transform the credential in a new form before presenting it to the Relying Party.
- ISO/IEC 29146: Information technology – Security techniques – A framework for access management [15] provides a framework for the definition of Access Management and the secure management of the process to access information. It is aimed to supplement ISO/IEC 24760 (see above) by describing the relevant services for access management. The project was at a Working Draft stage at the initial relevancy study time for ABC4Trust, currently having made to a Committee Draft. It was thus not considered to be a good candidate to concentrate ABC4Trust resources on. Also, the scope is slightly off topic for the core of ABC4Trust.

[5] These can actually be seen as a special case of our Privacy-ABCs where the signing key is a credential with one uniquely identifying attribute, and the signature is a presentation token for the signed message and inspection on the unique attribute.

5.2 New Study Period based on Privacy-ABC technologies

In April 2014, ISO/IEC JTC 1/SC 27/WG 2 and WG 5 launched a joint study period on "A privacy-respecting identity management scheme using attribute-based credentials". The study period had been initiated by the Swiss National Body and has so far resulted in multiple National Body contributions.

During the course of the study period, Switzerland has made two extensive contributions, namely one targeted at the WG 2 aspects and one at the WG 5 aspects. The contribution related to WG 5 comprises the terminology and main features of Privacy-ABC technologies. The contribution related to WG 2 includes a description of the parties involved in a Privacy-ABC system, the technical details behind issuing and presentation of credentials, and aspects of credential revocation. Both of these contributions were based on the architecture for Privacy-ABC technologies [10].

On the one hand, the contribution related to WG 5 essentially extends the ones that have been made by the ABC4Trust project to the ISO/IEC 24760-3, as discussed in Section 2.3. It has been intended as a starting point for further discussions on and elaboration of Privacy-ABC technologies. On the other hand, the contribution related to WG 2 presented a subset of the cryptographic protocols defined in the ABC4Trust architecture [10] at a reduced complexity level to be fit for standardization. Also, the protocol subset has been selected in such a way that it can serve for eID cards based on Privacy-ABC technologies. A related standardization project in this regard is the ISO/IEC 19286 initiative in SC 17/WG 4, which, among other things, standardizes Privacy-ABCs for chip cards.

On top of that, the French National Body has made a contribution related to protocols for privacy-respecting identity management based on traditional cryptography and possible involvement of third parties in authentication transactions. The Mexican National Body has also made a contribution in which it reinforced many of the goals of the Joint Study Period. Overall, the current discussions within WG 2 and WG 5 have been positive towards continuing work related to the Joint Study Period, which has been formally extended and awaits further input from National Bodies.

5.3 Other prospects and outlook

There are, of course, numerous Identity Management Implementations and elements thereof, such as X.509 [16], OAuth [17], OpenID [17,18] with SAML, supplemented by Access Control languages such as XACML [19], and trust frameworks, such as WS-Trust [20]. As shown in the architecture of Privacy-ABC technologies [10], most of these could be integrated with the ABC4Trust architecture. In the case of trust frameworks, for instance, there is already specific work available for integrating Privacy-ABC technology into trust frameworks [21], namely Microsoft's U-Prove into WS-Trust.

Future work may consider standardizing the XML-formats developed in D2.2 [10], potentially within OASIS or W3C. Also concrete cryptographic schemes may be worth the effort, potentially within ISO/IEC JTC 1/SC 27/WG 2. Both of these approaches are discussed in a bit more detail in Deliverable D8.13 "Reference Implementation for Standardization V2".

6 References

[1] ABC4Trust Consortium: ABC4Trust – Project description. Available at https://abc4trust.eu/download/ABC4Trust-Project-Description.pdf. Last accessed on November 3rd, 2014.

[2] European Commision: Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications); Official Journal of the European Communities, 2002.

[3] European Commision: Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; Official Journal of the European Communities, vol. 23, p. 31, 1995.

[4] T. Weichert: Datenschutzzertifizierung - Vorteile für Unternehmen; in ITK-Kompendium 2010: Expertenwissen, Trends und Lösungen in der Informations- und Kommunikationstechnologie, M. Neudörffer, ed. Frankfurt am Main: FAZ-Institut, 2009, pp. 274-279.

[5] European Commission: Proposal for a regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 2012.

[6] T. Christiansen and M. Dobbels: Implementing and Delegated Acts after Lisbon-Towards the Parliamentarisation of Policy-Implementation? Paper for Presentation; in Decision-Making in the European Union Before and After Lisbon, Leiden, 2011.

[7] ISO/IEC: ISO/IEC 24760-1:2011 – Information technology – Security techniques – A framework for identity management – Part 1: Terminology and concepts, 2011. Freely available via http://standards.iso.org/ittf/PubliclyAvailableStandards/index.html.

[8] ISO/IEC JTC 1: Text for ISO/IEC FDIS 24760-2 – Information technology – Security techniques – A framework for identity management – Part 2: Reference architecture and requirements, 2014.

[9] ISO/IEC JTC 1/SC 27: ISO/IEC 24760-3 (2nd CD): Information technology – Security techniques – A framework for identity management – Part 3: Practice, 2014.

[10] A. Sabouri (ed.): D2.2 Architecture for Attribute-based Credential Technologies – Final Version, 2014.

[11] ISO/IEC: ISO/IEC 29100:2011 – Information technology – Security techniques – Privacy framework, 2011.

[12] ISO/IEC: ISO/IEC 29101:2013 – Information technology – Security techniques – Privacy architecture framework, 2013.

[13] ISO/IEC: ISO/IEC 29191:2012 – Information technology – Security techniques – Requirements for partially anonymous, partially unlinkable authentication, 2012.

[14] ISO/IEC: ISO/IEC 29115:2013 – Information technology – Security techniques – Entity authentication assurance, 2013.

[15] ISO/IEC JTC 1/SC 27: ISO/IEC CD 29146 – Information technology – Security techniques – A framework for access management, 2014.

[16] ITU-T: X.509: Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks, International Telecommunications Union, 2008.

[17] Internet Engineering Task Force: OAuth Web Resource Authorization Profiles, 2010.

[18] OpenID: OpenID Authentication 2.0, 2007.

[19] T. Moses (ed.): eXtensible Access Control Markup Language (XACML) Version 2.0 (OASIS Standard), 2005.

[20] A. Nadalin et al. (eds.): WS-Trust 1.4, OASIS, 2009.

[21] C. Paquin: U-Trust WS-Trust Profile V1.0, Microsoft, 2011.

[22] Federal Office for Information Security (BSI): Innovations for an eID Architecture in Germany, September 2010. Available at http://www.personalausweisportal.de/SharedDocs/Downloads/EN/Flyers-and-Brochures/Broschuere_BSI_innovations_eID_architecture.html?nn=3610692. Last accessed on November 3rd, 2014.

[23] Marian Margraf: Federal Ministry of Interior. The New German ID Card.