# *D2.3 Benchmarking Criteria*

*Fatbardh Veseli, Jesus Luna, Hamza Ghani, Tsvetoslava Vateva-Gurova, Harald Zwingelberg, Katalin Storf, Felix Bieker, Daniel Deibler, Marit Hansen*

*Editor:* *Fatbardh Veseli (Goethe University Frankfurt)*
*Reviewer:* *Gregory Neven (IBM Research – Zurich)*
*Identifier:* *D2.3*
*Type:* *Deliverable*
*Version:* *1.05*
*Date:* *18/06/2014*[1]
*Status:* *Final*
*Class:* *Public*

Abstract

This document is an outcome of the ABC4Trust project, mainly as a contribution from "Work Package 2 – Architecture", but in close collaboration with project partners from different work packages. The document presents an extensive set of criteria for benchmarking privacy-enhancing attribute-based credential (Privacy-ABC) technologies. It is organised in five main dimensions, namely into efficiency, functionality, security assurance, legal data protection aspects, and economic viability. For each of these dimensions there are a number of individual aspects, which have been considered most relevant for benchmarking, out of which benchmarking criteria tailored for those dimensions have been identified. The individual criteria follow the approach of the lifecycle of Privacy-ABCs, starting from credential issuance to presentation, inspection, and revocation of Privacy-ABCs. This document can serve as a framework for benchmarking Privacy-ABC technologies, and can be used to provide a more insightful overview on the differences between different such technologies, which should lead to a better-informed decision on the most suitable choice among different Privacy-ABC technologies.

[1] This version (1.0.5) dates 22 December 2014 and presents a minor update to the previous version 1.0. This update fixes a previously misplaced sentence in Section 3.1.2.1.

*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 Solutions and Networks | NSN | Germany |
| 9. | Research Academic Computer Technology Institute | CTI | Greece |
| 10. | Söderhamn Kommun | SK | Sweden |
| 11. | Technische Universität Darmstadt | TUD | Germany |
| 12. | Unabhängiges Landeszentrum für Datenschutz | ULD | Germany |

# List of Contributors

| Chapter | Author(s) |
|---|---|
| Executive Summary | Fatbardh Veseli (GUF) |
| Chapter 1 - Introduction | Fatbardh Veseli (GUF), Jesus Luna, Hamza Ghani, Tsvetoslava Vateva-Gurova (TUD), Felix Bieker (ULD), Daniel Deibler (ULD), Marit Hansen (ULD) |
| Chapter 2 - ABC4Trust architecture overview | Fatbardh Veseli (GUF) |
| Chapter 3 – Efficiency | Fatbardh Veseli (GUF) |
| Chapter 4 - Functionality | Fatbardh Veseli (GUF) |
| Chapter 5 – Security Assurance | Jesus Luna (TUD), Hamza Ghani (TUD), Tsvetoslava Vateva-Gurova (TUD) |
| Chapter 6 – Legal data protection aspects | Harald Zwingelberg (ULD), Katalin Storf (ULD), Felix Bieker (ULD), Daniel Deibler (ULD), Marit Hansen (ULD) |
| Chapter 7 – Economic Viability | Fatbardh Veseli (GUF) |
| Chapter 8 – Summary of the criteria | Fatbardh Veseli (GUF), Daniel Deibler (ULD) |

# Executive Summary

This deliverable presents an extensive set of criteria, which can be used for benchmarking different Privacy-ABC technologies. Benchmarks based on these criteria should help designers and vendors of Privacy-ABC technologies to improve the different aspects of Privacy-ABC technologies, but also be used to compare different Privacy-ABCs against such benchmarks. It should be useful for a variety of audiences, such as system designers and architects, application developers, data protection officers and other parties interested in the technology to understand the main differences between different realisations of Privacy-ABC technologies. In turn, this should thus help them make the decision in selecting the instantiation of Privacy-ABC technologies that best suit application requirements.

The document starts by defining the goal of its existence and specifying the target technologies, which the presented criteria apply to, as well as the organisation of the document and the logic behind the structure of the criteria. The second chapter of the document provides a short summary of the concepts and features of Privacy-ABCs, and the main architecture entities and their interactions, briefly describing the lifecycle of Privacy-ABCs, making it easier for the reader to continue through the rest of the document.

The upcoming chapters are aligned according to the same lifecycle of the Privacy-ABCs (starting with *issuance, presentation, inspection,* and *revocation*), each enumerating a comprehensive set of benchmarking criteria along five main dimensions: *efficiency, functionality, security assurance, legal data protection aspects*, and *economic viability*. Furthermore, the deliverable provides a summarised version of the work in a form of guidance on how to use these criteria in order to compare different Privacy-ABC technologies based on their benchmarks.

Finally, the goal of this deliverable is to bring a list of criteria, which can be used to benchmark Privacy-ABC technologies in practice. However, the results of practical benchmarks of existing Privacy-ABC technologies, such as Microsoft's U-Prove or IBM's Idemix, are not presented here. Practical benchmarks on these technologies have been performed in ABC4Trust and they will instead be presented in a separate deliverable, namely in the upcoming deliverable D3.1 "Scientific comparison of ABC protocols – Part II Practical Comparison" [D3.1P2].

# Table of Contents

# Index of Figures

# Index of Tables

# 1. Introduction

The goal of this deliverable is to present a comprehensive set of benchmarking criteria, which can be used to objectively compare different privacy-preserving attribute-based credential technologies (Privacy-ABC) technologies. The contributed criteria consist of a set of metrics, both quantitative and qualitative, that can be applied to compare the Privacy-ABC technologies used within ABC4Trust, but can also be used to compare other Privacy-ABC technologies outside ABC4Trust. The foundation for these benchmarking criteria is deliverable D2.1 "Architecture for Attribute-based Credentials V1" [D2.1], where the main concepts and features of Privacy-ABCs have been defined.

This document is intended for different audiences. On the one hand, Privacy-ABC technology adopters (deploying application using Privacy-ABCs) and system architects can use these criteria both to elicit their requirements, and compare how the herein presented Privacy-ABC technologies actually fulfil those requirements. On the other hand, developers of other (potential) Privacy-ABC technologies (e.g., researchers and cryptographers) can use it to benchmark their proprietary Privacy-ABC technology with respect to those used in ABC4Trust, whereas system architects can use these criteria to be able to know which potential factors to consider when designing new systems that use Privacy-ABCs.

This document is organized in the following way: the rest of this chapter presents in further detail the methodological approach followed to build the set of metrics comprising our benchmarking criteria. Chapter 2 reviews the base concepts and features of Privacy-ABC systems, in order to provide readers with a self-contained document. Then, Chapters 3 - 7 present the actual benchmarking criteria for each of the major benchmarking dimensions, starting from efficiency in Chapter 3, functionality-related criteria in Chapter 4, security assurance-related criteria in Chapter 5, criteria related to legal data protection aspects in Chapter 6, and economic viability criteria in Chapter 7. Finally, the deliverable presents in the last chapter a summarized version of the criteria in a minimalistic view in tabular form (Chapter 8).

## 1.1 Privacy-ABC technologies and the scope of this document

This document describes the most important criteria that should be taken into account for benchmarking different Privacy-ABC technologies. The criteria are meant to be generic enough to apply not only to the implementations in ABC4Trust, such as Microsoft's U-Prove or IBM's Idemix, but also to other Privacy-ABC technologies that may exist now or emerge in the future. Other application specific criteria, which are not unique for Privacy-ABCs, are out of the scope of this document.

Technologies based on privacy-preserving attribute-based credentials (Privacy-ABCs) support privacy features, such as *selective disclosure of attributes (attribute hiding)*, *untraceability*, *unlinkability*, and *pseudonymity*, A short summary of the main privacy properties of Privacy-ABCs together with their description is provided in Table 1.1, whereas a more detailed description of the properties of Privacy-ABC technologies and related notions is presented in Chapter 2.

Furthermore, the formal security properties of Privacy-ABCs are defined in the work of Work Package 3, and will be published in another deliverable from Work Package 3, namely D3.1 "Scientific comparison of ABC Protocols – Part 1" [D3.1P1], which is to be consulted for this purpose.

**Table 1.1 - Privacy notions of Privacy-ABC technologies**

| Property | Description |
|---|---|
| *Selective disclosure of attributes* or *attribute hiding* | Refers to the feature of these Privacy-ABCs that makes it possible for the User to hide (certain) attribute values from the Verifier during the presentation, while disclosing only a subset of the attributes. |
| *Untraceability* | A feature of Privacy-ABCs, whereby an Issuer colluding with (several) Verifier(s) should not be able to link the issuance of a credential to a derived presentation token. Also referred to as "issuance-presentation non-linkability" |
| *Unlinkability* | Refers to the fact that a Verifier (or several of them) should not be able to link different presentation tokens derived from the same credential. Also referred to as "multiple presentation non-linkability". |
| *Pseudonymity* | Refers to the property of Privacy-ABCs, which enables Users to create different pseudonyms, and use the desired one for different contexts or applications. The different types of pseudonyms are briefly described in Chapter 2. |

## 1.2 The comparison criteria at a glance

The metrics comprising the comparison criteria presented in this document were developed with the aim to benchmark Privacy-ABC technologies and do not take into account the details related to their deployment and operation in specific contexts. These metrics were hierarchically classified in two different dimensions:

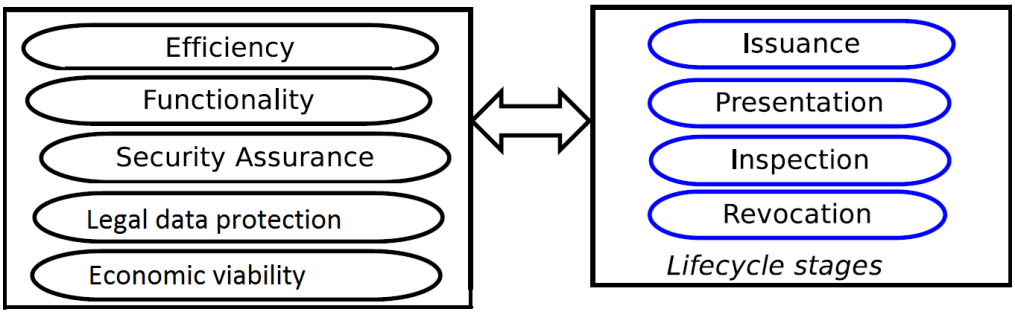


**Figure 1.1 - Organisational structure of the benchmarking criteria (adopted from [VesVat14])**

- The first dimension of the benchmarking criteria consists of five main aspects, namely the *efficiency*, *functionality*, *security assurance*, *economic viability*, and *legal data protection aspects*, as shown on the left side of Figure 1.1. The explanation of the idea behind each of these categories will be presented in Section 1.3, whereas these sections are part of every top-level category (each one is a sections in each chapter).
- The second dimension goes deeper into identifying granular criteria related to the aspects from the first dimension. In doing so, we follow the approach of the lifecycle of Privacy-ABCs, which starts with *issuance*, and continues with *presentation, inspection, and revocation*, as shown on the right side of Figure 1.1. A more detailed description of these stages is presented in Section 2.3.

To facilitate reading of the criteria from different dimensions, we have defined a template that is presented in Table 1.2, together with the attributes, such as name of the criterion, the unique identifier (ID), status, the intended audience, etc., and a brief explanation of each attribute.

**Table 1.2 - Template used to define the metrics comprising the benchmarking criteria**

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | The name of the metric |
| **ID** | Short name or abbreviation |
| **Status** | Possible states: Draft, Ready for Review, Reviewed, Final. |
| **Audience** | Choice of *End-User, System Architect, Developer, Other* |
| **Description** | A general description of the metric |
| **Implementation evidence** | List of controls that validate the implementation of the metric. Implementation evidence is used to calculate the metric, as indirect indicators that validate that the activity is performed, and as causation factors that may point to the causes of unsatisfactory results for a specific metric. |
| **Visualization** | The kind of visualization technique e.g., tables, time-series charts, etc. |
| **Units of Measure/ Comments** | Units of measure (only for quantitative metrics). Optionally, this field can be also used to add further comments with respect to the measured result e.g., describing in more detail the mechanisms used to protect a credential's confidentiality. |
| **Numeric range** | The range of numeric values expected for the metric expressed as an interval e.g., (1,100), (128, 256, 512, 1024)<br>Applies only to quantitative metrics. |
| **How to Calculate** | A general description of how to calculate the metric plus a formula or cross reference, if possible. |

The next section presents in further detail the concepts and rationale behind each one of the top-level categories in the comparison criteria.

## 1.3 The five aspects of benchmarking

The benchmarking criteria presented in this document consist of the main benchmarking aspects shown in and explained in the rest of this section, namely the dimension of *efficiency*, *functionality*, *security assurance*, *legal data protection aspects*, and *economic viability*.

### 1.3.1 Efficiency

Different Privacy-ABC technologies may be built using different cryptographic building blocks, such as Zero-Knowledge Proofs, Commitment and Signature Schemes, etc. Furthermore, they may be practically implemented using different development environments, such as Java RE or .Net Framework, or can target different running environments, i.e. tailored for particular operating systems, In any case, an important benchmark for different Privacy-ABC technologies is their efficiency. For

this purpose, we have developed a set of refined criteria, which aim at benchmarking performance efficiency of Privacy-ABC technologies at different lifecycles of the Privacy-ABCs: setup of the system and entities, issuance of credentials and their presentation, but also the (computational and communication) cost of revocation and inspection.

The performance criteria usually comprise the quantitative metrics and they mainly aim to compare the operational cost both from a theoretical viewpoint and a practical one. Both of these types of criteria consider the *computational efficiency* for performing such an operation (the number of mathematical operations, the number of building blocks, etc. used for the given metric), as well as the *communication efficiency* (the size of data exchanged between parties) for performing such operations. On top of that, we also define a number of *storage efficiency* criteria, which are important for evaluating the storage requirements for each entity, especially for the User.

For the theoretical computational efficiency, the benchmarking deals with the number of operations for performing a certain operation, e.g. presentation. In this sense, it is important to recognize the building blocks used (at each entity) for performing such a presentation, the efficiency of the underlying steps for performing such an operation. For the communication efficiency, it is important to know the size of messages exchanged between the parties during a given operation, which also depends, among other things, on the security level applied, e.g. during issuance or presentation.

The practical benchmark (for both computational and communication metrics) should clearly state, among other things, the test-bed where the execution takes place, and the security level used during certain operations.

### 1.3.2 Functionality

The functional criteria are mostly qualitative and they aim at benchmarking a given Privacy-ABC technology from their support for different functional features, which are defined in D2.1 [D2.1]. Most of the general privacy-related concepts and features of Privacy-ABCs are studied in the functional sections of each chapter.

Having in mind the Privacy-ABC-focus of the criteria, the functional criteria also identify additional characteristics which may be important for the adopters of the technology, but which are not necessarily straightforward to understand. In this regard, we also included additional criteria for comparing certain functional Privacy-ABC-specific features, which may have an impact on the architecture of an application or pose additional requirements for the entities. Furthermore, here go also other operational features, such as scalability and known limitations of different Privacy-ABC technologies.

### 1.3.3 Security Assurance

The security assurance metrics aim to assess the security offered by some particular Privacy-ABC technology. This group of metrics was mainly developed taking into account the properties presented in Section 1.1.

Where applicable, the security assurance metrics were also derived from the results of the quantitative threat modelling methodology (QTMM) [LKS12] applied in both Deliverable 6.2 [D6.2] and Deliverable 7.2 [D7.2]. In essence the QTMM considered a real-world scenario that used Privacy-ABC technology (i.e., the ABC4Trust pilots), then elicited a set of security mechanisms able to mitigate the specific risks associated with Privacy-ABCs. The security assurance metrics contained in these benchmarking criteria are precisely in charge of quantitatively assessing the effectiveness of the elicited security mechanisms, but only taking into account the technology-specific ones.

Unlike e.g., performance metrics, a number of the security assurance metrics presented in this document cannot be directly mapped to a quantitative value (e.g., a numeric security level measured in bits). Therefore, just as in the case of the functional metrics (cf. Section 1.3.2), our security assurance metrics consider qualitative criteria, which can result in comparable results. That is the case of a comparable assumption under which a scheme is provably secure e.g., where RSA is stronger than factoring. Such qualitative measurements also aim to provide users of this criterion with the information required to objectively compare side-by-side two or more Privacy-ABC technologies (cf. Chapter 8). However, still there might be specific cases for which the assumptions are not comparable (e.g., discrete logarithm and factoring assumptions for a provably secure scheme).

### 1.3.4 Legal Data Protection Aspects

Privacy-ABCs are a new way to approach privacy issues, thereby significantly improving the current state of the art concerning best practice solutions that follow privacy and data protection principles. Such principles are defined in the European Data Protection Framework (among others in the Directive 95/46/EC) and in general world-wide discussed privacy principles (among others the OECD Guidelines on the Protection of Privacy and Trans-border Flows of Personal Data [OECD13] and ISO/IEC 29100 Privacy Framework [ISO11]). In the ABC4Trust project we take into account those privacy principles, but for discussing legal compliance, we apply European data protection law, or, whenever appropriate, e.g. for the pilots, national data protection regulations. For discussing benchmarking criteria, we refrain from detailed legal compliance criteria, but describe them on a more abstract level structured according to protection goals as explained below.

In the following, the most relevant privacy benefits generally provided by the deployment of attribute-based credentials are listed:

- For many use cases, the current state of the art for authentication processes perform the desired functionality, but mostly come along with a full identification of the User. In this context, Privacy-ABCs enable a minimisation of personal data being disclosed thus enabling Relying Parties (Verifiers) to adhere to the principle of data minimisation. For the exchange of opinions, an anonymous and unauthenticated forum can create a sphere for Users to express themselves free of fear from identification and repression. Likewise, the right to inform oneself by access to information available under some access restrictions such as licenses granted to a municipality or for members of a university can be made possible by anonymous access to those websites verifying only the necessary membership attribute.
- Privacy-ABCs allow verifying certain attributes such as age, place of residence or being a student without revealing any additional information such as the detailed birth date. They enable various functionalities for data minimisation, such as the verification that the same entity was acting on a previous occasion without collecting further identifying information (contextual authentication). This can be achieved, e.g. by assigning a cookie or sharing a secret, such as username and password. Moreover, Privacy-ABCs go further by not relying on a shared secret, but being cryptographically bound to the credential issued by the Issuer. This way, the necessary access token cannot be easily passed on to someone else without risking impersonation at any Verifier that accepts the same credential. Therefore, Privacy-ABCs provide an additional reason for Verifiers to trust this authentication without giving away any more information. Conditional identification: Privacy-ABCs support the inspection feature, allowing the identification of a User who authenticated herself towards the system using a pseudonym. The authentication is done in the same way as described before. However, there is also an encrypted part added to the token containing identifying information, which the Verifier cannot access in clear text. Rather, a third entity, the Inspector, can decrypt the information if certain predefined and communicated conditions (inspection grounds) are met. Therefore, the real identity of the User can be established

("inspected") under certain, clearly defined conditions. As a consequence, the complete inspectable token has to be categorised as personal data since it entails attributes about a person that is identifiable. The identifiability of the User results from the addition of the encrypted (identifying) information. Nonetheless, the encrypted identifying information will only be sent to the Verifier with prior consent of the User, ensuring the transparency of the process for the User right from the start.

- Identified use: It is also possible to configure policies in such a way that verified attributes allow a direct identification and linkage to a specific person, e.g. the real name, matriculation number or other unique identifier. However, this possibility of linking to the user is made transparent prior to submitting her personal data. By enabling this, Privacy-ABCs may be used in a deployment for eID solutions as well – offering all that is necessary for a trustworthy eID but offering all the privacy-preserving options in addition.

Generally, a concrete legal evaluation needs to be done based on specific use cases rather than on an abstract architecture or the underlying technology. However, a first abstract evaluation provides some insight already. For weighing the interests of all roles within an ABC-architecture, also the following elements of the concrete use case must be taken into account, such as the type of data processed in particular when special categories of data are concerned (medical data, race, ethnic origin, religious beliefs, trade union membership or sex life, etc.), but also in the context in which the personal data will be processed or might appear must be considered.

Recent research in the area of privacy from a legal, sociological and technological perspective has shown that the traditional protection goals of confidentiality, integrity, and availability should be extended by specific privacy-related protection goals [RosPfi09].

The classic protection goals, well established in the sphere of information security, are:

⇒ *Confidentiality*, preventing unauthorised access to information or systems concerned,

⇒ *Integrity*, meaning that information or systems cannot be altered undetected,

⇒ *Availability*, meaning that information or systems are available timely and reliable when needed.

These requirements are usually formulated and understood in a way as to meet the demands of technical and organisational systems both in abstract overview and in a comprehensible form of sufficiently concrete measures. But these protection goals do not cover all aspects needed. Therefore, three additional complementary protection goals have been proposed. Further the view on all six goals must be broadened, including not only the protection of the organisation's assets, but also the privacy of users and the rights of other involved parties such as supervisory bodies thus strengthening the data subject's perspective on data processing (see [RosPfi09], [RosBoc11] and applied specifically to eID solutions by [ZwiHan12]).

In the field of information security, additional properties worth aiming for have been included in the legal parts, namely *authenticity*, *accountability*, *non-repudiation* and *reliability*. In the bigger view including the privacy aspects as proposed these additional properties can be understood as subsets of the six major goals, e.g. as part of integrity (authenticity, non-repudiation, accountability) or availability (reliability).

The specific privacy protection goals are:

⇒ *Transparency*, ensuring that all privacy-relevant data processing, including the legal, technical and organizational setting, can be understood and reconstructed,

⇒ *Intervenability*, ensuring that the parties involved in any privacy-relevant data processing, including the individual whose personal data is processed, have the possibility to intervene,

where necessary. The objective is to offer corrective measures and counterbalances in processes. [ZwiHan2012]

⇒ *Unlinkability*, ensuring that privacy-relevant data cannot be linked across privacy domains or used for a different purpose than originally intended.

Overall, the – security and privacy – protection goals form a system, which has been visually illustrated in Figure 1.2 below. The combination of a star and the hexagon shall illustrate the rather complex relations between the different protection goals. While at a first glance the correlation between certain goals might seem fairly contradictory, such as integrity vs. intervenability or confidentiality vs. transparency, their relationship should rather be understood as dependent instead of exclusive. When applying the protection goals they have to be weighted and balanced in a risk analysis on a case-by case basis to determine to which extent, on which layer, and by which means the respective protection goal can be implemented into the process of IT-systems.[RosBoc2010] The goal of this risk analysis and balancing act should always be the implementation of all goals to the greatest possible extent. This means that the assessment should aim towards a full functionality (‘positive sum, not zero sum’) and a possible reconcilement of all interests. [RosBoc2011]

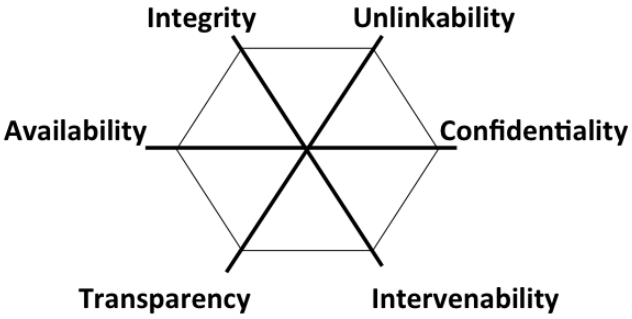


**Figure 1.2 - System of protection goals covering IT security and privacy as proposed by [RosPfi09]**

## 1.3.5 Economic Viability

The economic viability criteria aim at showing how to calculate the cost for applying a certain Privacy-ABC scheme to a certain application or scenario. This section gives examples on how to combine the main Privacy-ABC technology factors (including efficiency and functionality differences) with potentially given combinations of hardware and software environment to assume the cost for such an implementation. It also identifies some potential economic initiative to provide certain services for the other entities, such as running the services around revocation, or inspection.

# 2. ABC4Trust architecture overview

Identification and definition of the main concepts and features of privacy-enhancing attribute-based credentials has been an initial contribution of ABC4Trust towards a unified architecture for these technologies. The architecture of Privacy-ABC technologies [D2.1] presents in separate chapters the concepts and features of these technologies in an abstract way, with which not only existing, but also emerging Privacy-ABC technologies can be described. In this regard, the curious reader can find the extensive list of these features in Chapter 2 "Features and Concepts of Privacy-ABCs" of [D2.1]. However, this chapter will bring an overview of these concepts and features in a condensed form, in order to have a self-contained deliverable.

## 2.1 Architecture Entities

The ABC4Trust architecture identifies several architecture entities, which interact with each other during certain lifecycle moments of Privacy-ABCs. Figure 2.1 shows the complete list of the recognized entities, whose roles and interests differ from one another. Some entities, such as the User, the Issuer, and the Verifier are mandatory, while other entities, such as the Revocation Authority and the Inspector are optional. Furthermore, the Revocation Authority presented in the figure reflects the current setting in ABC4Trust, but other schemes are also possible to be integrated in the architecture and in the lifecycle of Privacy-ABCs. The entities should be seen as representations of different functions in the lifecycle of Privacy-ABCs.

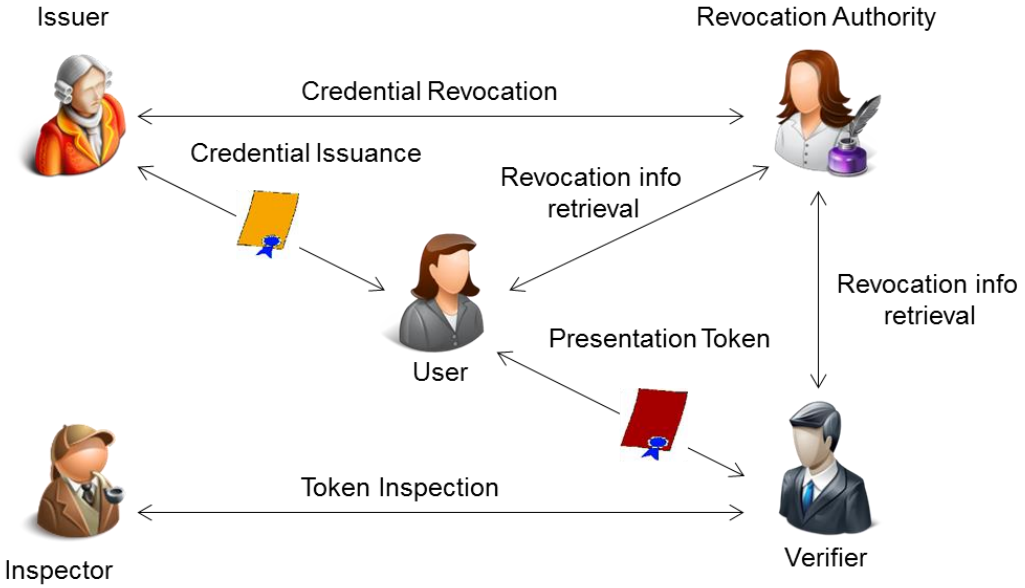


**Figure 2.1 - The main architecture entities and their interactions**

The central entity in the architecture is the *User*, whose interest is to have privacy-preserving access to services, which may be offered by different Service Providers, which in the ABC4Trust architecture are known as *Verifiers*. The Verifier may ask the User to present a (cryptographic) proof about certain claims of the User, or even make her reveal certain attribute values about her identity. A Verifier, also known in the literature as a Relying Party, trusts certain *Issuers*, which are entities that certify certain attributes about the Users. A Revocation Authority's role is to revoke users' credentials and maintain

the list of valid (invalid) credentials in the system, while the Inspector is a trusted entity, which has the technical capabilities to, when specific priori specified conditions are met, "de-anonymise" a conditionally anonymous transaction of a user. Note however, that the user is informed at the time of authentication about the possibility of *inspection* if those conditions are fulfilled, whereby her consent is necessary and the possibility is made transparent on her user interface.

While certain roles can be performed by a single entity, some of them must be kept separate. For instance, an Issuer can also act as a Verifier or a Revocation Authority, but a Verifier and an Inspector must not collide into a single entity.

## 2.2 Basic concepts

A *credential* is a cryptographic container of attributes about certain identity information about the User, signed and vouched for by a trusted authority. A credential may contain different types of attributes, such as name, birth date, or other information. A credential may be bound to a "secret key", "knowledge" of which may need to be shown before it can be used.

Besides credentials, a User may also own (create) different number and types of *pseudonyms*, which may be used to create certain degree of linkability. In this regard, we have to distinguish between three different types of pseudonyms:

- A *verifiable pseudonym* allows the User to re-authenticate under the same pseudonym by proving the knowledge of the User secret, which it is generated from. This type of pseudonym is mostly useful in log-in scenarios as a replacement for a username and password scheme.
- A *certified pseudonym* is a verifiable pseudonym, but it is bound to the same secret as a previously issued credential. A User may own a different number of such credentials, which are untraceable between them, but different uses of the same pseudonym are of course linkable.
- Finally, the Verifier can also prevent a User from creating more than one pseudonym for a given "scope". This is achieved by *scope-exclusive pseudonyms*, which are useful in scenarios when the Verifier needs to control Users from accessing a single resource with more than one pseudonym, for instance, in online voting.

## 2.3 Lifecycle of Privacy-ABCs

During its lifetime, a Privacy-ABC can be summarized in the following steps: issuance, presentation, revocation, and inspection. The issuance and the presentation are two crucial steps for any system that adopts these Privacy-ABC technologies, while revocation and inspection are optional features, which may be desired to be present, depending on the application that uses these technologies.

### 2.3.1 Issuance

The lifecycle of a credential starts with the Issuance, which is an interactive protocol, possibly separated into multiple steps of communication, between the User and the Issuer, in the end of which the Issuer issues a (signed) credential to the User, thereby vouching for the correctness of information contained in it.

Issuance also comes with additional types:

- Normal issuance or *issuance from scratch* is the simplest form of issuance, where all attribute values of the issued credential are known to the Issuer. The User only requests credential issuance and the process continues until the User has received them.
- *Advanced issuance with carry-over attributes,* which has the additional feature that the User certain attribute values of a user's credential may be "re-issued" in a new credential without the Issuer necessarily having them revealed to the Issuer during this process. In this case, the User already possesses certain credentials and wants to merely *carry those values over* into the new credential. This type of issuance involved additional protocol steps between the User and the Issuer, during which the User shows that she knows certain secret about her attribute values.
- There is also a third option of issuance, which is also considered to fall into the category of advanced issuance, where the attribute values are chosen by the User. This type of issuance is called issuance with *carry-over self-claimed* attributes.

In the end of all the types of issuances, the User will receive the necessary (cryptographic) material to generate her final credentials. During the advanced issuance, neither the carried-over attribute values nor the secret key of the User are visible to the Issuer. Furthermore, the issuance can also involve a *jointly-random* issuance, during which both the User and the Verifier contribute with their input to the final value of the attribute in the newly-issued credential.

### 2.3.2 Presentation

The presentation phase occurs when a User wants to access a resource at the Verifier side. In this case, the Verifier responds to the User by sending a presentation policy, which describes what proofs must the User present, and what information from her credential(s) the User must reveal (if any). The User may then check which of her combination of credentials fulfils the policy and use them to generate the response - a *presentation token*, which is sent *(presented)* to a Verifier.

Thus, a presentation token may reveal information about the User (reveal attribute values), but also *prove* certain facts about some other attributes (while hiding the values), such as proving that her birth date is earlier than a given day, or that two attribute values from different credentials are the same, etc. As explained earlier, presentation tokens generated from Privacy-ABCs are untraceable and they may also be unlinkable, if desired.

During a presentation, the User may also need to prove not only that she possessed certain attribute values, but also that the credentials certifying those attributes have not been revoked. On the other hand, the Verifier is able to verify the validity of the presentation tokens both from the policy fulfilment point of view, but also validate the validity of the credentials with regards to the revocation information.

### 2.3.3 Inspection

*Attribute-hiding, unlinkability* and *untraceability* may in general be desired privacy features a system should have, but there are also certain cases, when they can lead to misuse. In those cases, it may be desired that there is an optional feature, which enables "de-anonymisation" of anonymous presentation tokens, i.e. identifying the user who generated the presentation token, providing a particular aspect of accountability should specific (misuse) conditions be met. This feature is called *inspection* and it is under the responsibility of the dedicated entity called "Inspector". The fact that a certain presentation token is inspectable is specified in the inspection grounds, which is made transparent to the User in the presentation policy. The presentation policy also defined the inspection grounds, under which such a potential inspection may take place.

The Inspector should provide its service having two specific goals (interests) in mind:

1. Fairness towards the User - the Inspector should be trusted by the Users not to abuse its authority - for instance, it should be trusted not to perform inspection of presentation token, unless a particular condition clearly defined a-priori from the eligible inspection grounds is met; and
2. Fairness towards the Verifier – the Inspector should be trusted by the Verifier to inspect a presentation token whenever the inspection grounds are met.

The inspection grounds must be clearly defined in advance and be transparent to the User. The User must be aware of the fact that, in case the inspection grounds hold, the presentation token it presents to the Verifier may be subject to potential later inspection.

### 2.3.4 Revocation

A User may lose possession of her credentials, may want to change certain information from her credentials, violate the usage policy of her credentials or misuse them in other forms, which may be clearly described, depending on the scenario. In those cases, it is necessary for the system to be able to *revoke* certain credentials (users), thus invalidating those credentials and disabling their possible use in the future.

A Revocation Authority is a specialised entity, which maintains such revocation lists and disseminates the latest revocation information to the other parties (namely, to the Users and Verifiers, but possibly also to Issuers). Every credential contains a unique identifying number, which is used for revocation – the *revocation handle*, which should never be disclosed to any Verifier.

Depending on which entity initiates the revocation process and the scope of revocation, we can distinguish between *Issuer-driven* and *Verifier-driven* revocation. In the former, the Issuer asks the Revocation Authority to completely revoke the validity of certain credentials and this type of revocation is "global" in scope, in which case no Verifier will accept such credentials. The Verifier-driven revocation is initiated by the Verifier and has a local impact: the revocation effect will only impact the Verifier initiating such revocation, and the credentials can be used with other Verifiers.

## 2.4 Key Binding

Different user credentials/pseudonyms can be bound to a certain secret during the issuance or presentation. Each credential issued may contain a secret key as part of the cryptographic information related to it, which only the User is supposed to know, but also different credentials can be bound to the same secret key. This feature is known as *key-binding* and is used to prevent different credential misuse scenarios, such as credential pooling, where different users in possession of different credentials get together to combine their credentials to get access to certain services, which they should individually not be able to. Therefore, Issuers can issue new credentials or pseudonyms and bind them to (the secret key of) existing credentials of the User, while also Verifiers can impose in the presentation policy that the credentials used for presentation should all be bound to the same secret.

# 3. Efficiency

Privacy-ABC technologies are meant to serve as building blocks of privacy-friendly identity management systems, which are building blocks of many electronic services. Besides fulfilling security requirements of the service where they are used, an identity management system must perform efficiently in order to be acceptable and used by users. From this point of view, it is important that the Privacy-ABC technologies can be compared in terms of their efficiency, in order to be able to assess their potential overhead on the performance of the applications where they are used, which can be early indicators on the acceptance of the technology by the users.

In this regard, we consider three main dimensions of efficiency, namely *the computational, communication* efficiency, and *storage* efficiency.

## 3.1 Computational Efficiency

Computational or time efficiency of an algorithm measures the time required to perform the operations defined under a certain algorithm. In the case of Privacy-ABC technologies, computational efficiency can vary, depending on the building blocks used and the chosen feature of operation. In most of the cases, the operations involve different types of cryptographic operations, which may be relatively complex in terms of computations. In general, computational efficiency is important to measure in order to be able to assess which Privacy-ABC technology requires less computing resources and time in order to perform a given operation.

Typically, the computational efficiency represents the amount of time to process a certain operation on a given algorithm. Typically, the computational efficiency depends on the size of the input data of the algorithm. In the case of the Privacy-ABC technologies, the input size is typically the size of the key used for the cryptographic operations, but other input factors can also influence the efficiency many computations, such as the number of shown/hidden attributes or the number of credentials proved during presentation. Usually one distinguishes between theoretical efficiency and empirical (practical) one. In a theoretical model, the efficiency is represented in mathematical terms, and the execution environment is abstracted away, ignoring the overhead of the practical implementation factors, such as development and execution environment, as well as hardware performance in different platforms, but only defines the mathematical properties which the algorithm relies on and the computational complexity of those. The measurement unit in the theoretical model is the number of *basic* or *dominant operations,* which typically include basic arithmetic operations (addition, subtraction, multiplication, division, and exponentiations), comparisons and logical operators (negation, disjunction, and conjunction). In the empirical model, the computational efficiency analysis defines an execution and development environment, and is measured in time units (usually milliseconds) needed to perform different operations.

In the case of the Privacy-ABC technologies, we take into account the different lifecycles of the Privacy-ABCs and define benchmarking criteria for assessing the efficiency of different operations used for different features during the issuance, presentation, inspection, and revocation. The following sections present a set of efficiency-related criteria tailored for each of the stages in the lifecycle of the Privacy-ABCs, starting from issuance, presentation, inspection, and revocation.

### 3.1.1 Issuance

Issuance is the first step in the credential lifecycle that involves the interaction of the User (assuming that the setup of the system has been done a-priori). Issuance is in general thought of as a necessary step in order for the User to get her credential(s) (and the necessary information related to them). In the context of computational efficiency related to the issuance stage of the Privacy-ABCs, one can identify criteria for the different types of issuance (simple and advanced issuance forms), but also the choice of platform where different operations are executed (computers, or smart cards). The following tables present individual such criteria and identify a number of factors that could impact the final efficiency benchmarks.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Computational Efficiency for Issuance from Scratch |
| **ID** | Eff-Iss1 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | This criterion is used to measure the computational efficiency each entity is expected to handle for the issuance from scratch. The metric should take into account the following issuance cases:<br>-issuance of different of credentials with different number of attributes<br>-different security levels, and<br>In the best case, show the cryptographic building blocks used in this operation and the participation of each block in the efficiency of the overall operation (in percentage or individual weight). This excludes test with revocation, unless it is inseparable part of the Privacy-ABC technology (unlike in ABC4Trust). |
| **Implementation evidence** | For the theoretical benchmark, the specification of the complexity of the given Privacy-ABC system and its building blocks from the research papers, whereas for the practical part, the sensors in the code of the given implementation. |
| **Visualization** | Tabular and/or diagram |
| **Units of Measure** | The theoretical computational efficiency is expressed in the number of arithmetic operations, while the practical one in time units. For the practical test, the testbed must be clearly defined. |
| **Numeric range** | n/a |
| **How to Calculate** | Issue different credentials with different number of attributes and compare their efficiency. Test the same with different security level. |

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Computational efficiency for Advanced Issuance and Credential Update |
| **ID** | Eff-Iss2 |
| **Status** | Final |
| **Audience** | Developer, Designer |
| **Description** | If the Privacy-ABC in question supports the advances issuance features, this criterion deals with the computational efficiency for the Issuer and the User for (the supported types of issuance from) the following:<br>- issuance with carry-over attributes,<br>- jointly random issuance,<br>- issuance with self-claimed carry over attributes, and |

| | |
|---|---|
| | - credential update.<br><br>The first three issuance features are defined in [D2.1], whereas credential update refers to a particular feature, which would enable a user to get an already issued credential update with new values for certain attributes.<br><br>Each of the above factors (if supported) must be tested under different security levels to see how the efficiency changes accordingly. The benchmark should take into account the number of attributes being carried over/self-claimed, as well as the number of credentials involved.<br><br>In the best case, show the cryptographic building blocks used in this operation and the participation of each block in the efficiency of the overall operation. |
| **Implementation evidence** | For the theoretical benchmark, the specification of the complexity of the given Privacy-ABC system and its building blocks from the research papers, whereas for the practical part, the sensors in the code of the given implementation. |
| **Visualization** | Tabular and/or diagram |
| **Units of Measure** | As with other performance measurements, this one has also practical and theoretical measurement at different security levels and different number of attributes:<br><br>-For the practical measurement, the unit of measurement is expressed in time units (milliseconds)<br><br>-For the theoretical measurement, the number of basic arithmetic operations to perform the crypto computation during update. |
| **Numeric range** | n/a |
| **How to Calculate** | Test all the supported types of issuance from the list above and compare their efficiency. |

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Benchmarking Issuance time on smart cards |
| **ID** | Eff-Iss3 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | This metric aims at providing some figures on specific smart card implementations of certain issuance operations. The metric must define which operations are carried on the card versus those performed on a computer. This should give a clear idea of how expensive certain operations are when run on certain smart card.<br><br>The types of scenarios to be tested are similar as in Eff-Iss1 and Eff-Iss2, with the only difference being the use of hardware smart card instead. In the simple issuance, the only card-related operation is probably the storage of the credential in the card, while on the advanced issuance key-binding operations has to be done on the card. However, the benchmark should clearly distinguish between the operations performed on the smart card, i.e. whether only the key-binding feature is done on the card, or whether additional proofs (presentation tokens) are computed on the smart card.<br><br>Note that this experiment needs only practical benchmarks, as the theoretical complexity is the same as in Iss-E1 and Eff-Iss2.. However, it may be useful to show the complexity of the operations done on the smart card even for the theoretical benchmark separately, in order to give an impression of which building blocks can be outsourced in other devices and what the expected overhead would be. |
| **Implementation evidence** | For the theoretical benchmark, the specification of the complexity of the given Privacy-ABC system and its building blocks from the research papers, whereas for the practical part, the sensors in the code of the given implementation. |
| **Visualization** | Tabular and/or diagram |
| **Units of Measure** | Time units (seconds) |
| **Numeric range** | n/a |
| **How to Calculate** | This metric can be split: one involves only storing the credential in the card; one is with the key-binding operation being performed on the card; the other one can deal with additional operations performed on the card during the issuance, which must be clearly specified. |

### 3.1.2 Presentation

Presentation is the most commonly used stage in the lifecycle of Privacy-ABCs and the one that mostly impacts the User. It is therefore a focal element in choosing a Privacy-ABC technology, since different such technologies may provide different efficiency results or support different functionalities, but also come with different security assumptions.

For the computational efficiency, similar to the presentation stage, it is important to identify different cases, where efficiency would differ, both in terms of different features used during the presentation, but also considering the platform where the computations are being done (computers and smart cards). Clearly, for the benchmarks involving smart cards, one should clearly describe which features are implemented on the card versus those implemented (performed) on the computer, which would certainly make a difference in a potential comparison of the respective efficiencies.

Computational efficiency can be done theoretically and practically, as for the issuance phase, and as for the other phases in the lifecycle. The crucial difference in the case of presentation is that the presentation is separated in two main parts: the operations done on the User side (*proving*) in order to generate a presentation token for a given presentation policy, and the efficiency on the Verifier's side (*verification*) to verify the received presentation token. This way, the network delay for transporting the presentation token from the User to the Verifier is abstracted away from the benchmarks, providing a fairer benchmark in the isolation of the transportation efficiency, which can vary, but is irrelevant from the choice of the Privacy-ABC technology.

Each of these domains will be presented into their own section. Note, however, that these cases should not include the additional (computational efficiency) overhead of revocation or inspection, which are presented in their respective sections in this chapter.

#### 3.1.2.1 Proving

As described above, we separate the presentation session in two main parts: the part of the computations on the User side (proving) to generate the presentation token, and the part of the computation on the Verifier's side (verification).

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Computational Efficiency for Proving (Possession of) Credentials |
| **ID** | Eff-P1 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | This criterion is used to measure the computational efficiency for the User when generating a presentation token. The metric should take into consideration the following different cases (policies):<br>- Presentations using one credential and the impact of the number of hidden attributes<br>- Presentation tokens from a combination of different credentials<br>- Presentation with pseudonyms and key binding;<br>- Presentations using predicates;<br>- Presentations under different security levels;<br>The objective is to find out how does the efficiency of computations required for generating a presentation token depends on the different scenarios described above. Note that in this case only the hidden attributes are taken into account. However, the metric could also show the computational efficiency of showing (revealing) attributes. Note also that the results should compare the performance at different security levels.<br>In the best case, show the cryptographic building blocks used in this operation and the participation of each |

| | |
|---|---|
| | block in the efficiency of the overall operation (in percentage or individual weight). |
| **Implementation evidence** | For the theoretical part, the efficiency results should be based on the scientific specification of the Privacy-ABC scheme used for the presentation and its building blocks, whereas for the practical part, the sensors in the code for the implemented Privacy-ABC technology. |
| **Visualization** | Tabular and/or diagram |
| **Units of Measure** | For the theoretical measurement, the measurement unit is the number of arithmetic operations required for creating a presentation token of a certain type, while for the practical measurement, the measurement is expressed in time units. |
| **Numeric range** | n/a |
| **How to Calculate** | The measurement aims at measuring the time to perform the cryptographic operations on the User side. |

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Benchmarking Computational Efficiency for Proving on smart cards |
| **ID** | Eff-P2 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | This criterion is used to measure the computational efficiency a User/Verifier is expected to handle when generating/verifying a given presentation token when the smart card is involved, which is a more precise performance benchmark, since smart card platforms are less complex, making comparisons between their architectures/capabilities more straightforward than, e.g. coputers.<br><br>The measurement should provide performance figures for different presentations and specify which operations have been carried on the card versus those operated on a different platform, for instance, on a computer. At least the key-binding is performed on the smart card, and possibly other cases when the card performs additional operations, which clearly must be specified.<br><br>The results should give a clear idea of how expensive certain operations are when run on smart cards. |
| **Implementation evidence** | |
| **Visualization** | Tabular and/or diagram |
| **Units of Measure** | This is a practical benchmark and therefore the measurement is expressed in time units. |
| **Numeric range** | n/a |
| **How to Calculate** | The time difference between a similar presentation on a computer compared to the one involving a hardware smart card is what should be measured. |

#### 3.1.2.2 Verification

Verification is the second part of the presentation protocol, during which it is the efficiency of the computations on the Verifier's side that is evaluated. For the verification, the benchmarks must take the same scenarios as defined for presentation (see 3.1.2.1) and measure the efficiency of completing the verification process for each of the given presentation scenarios on the Verifier side.

### 3.1.3 Inspection

Inspection is a feature of Privacy-ABCs, whereby an external trusted entity could, under a-priori defined and clearly described misuse cases, identify the hidden attribute values in a normally non-linkable and non-traceable presentation token. This needs to be described in the presentation policy and made transparent to the User.

If a presentation policy states that certain attributes are conditionally inspectable (under those strict cases), then there is an additional cost for the User and the Verifier during presentation. How much this affects the presentation, may depend on the precise cryptographic scheme used for inspection.

The following two sections define benchmarking criteria for efficiency aspects related to inspection, namely the impact on the other entities and the inspection process itself.

#### 3.1.3.1 Impact on other entities/credential lifecycles

Having inspection enabled may have an impact on the other steps in the lifecycle of Privacy-ABCs, most notably on the presentation. This affects mostly the User, who needs to perform additional steps in order to have the presentation token inspection-enabled, e.g. by encrypting the content with the public key of the Inspector, which results in decreased efficiency for presentation. An impact on verifying the presentation token with inspection enabled may also be noticed at the efficiency benchmarks for the Verifiers.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Computational overhead on the User during presentation |
| **ID** | Eff-Ins1 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | Presentation of inspectable attributes in a presentation token is an additional workload and performance overhead on the User, because of the verifiable encryption used in this scenario: the user has to do an additional step, which includes encrypting the attributes in a way that the Verifier can verify they are indeed the same as the ones proved in the presentation token and that they are encrypted using the public key of the Inspector.<br>How much this affects the presentation efficiency is the main focus of this criterion. This metric should compare a representative range of different presentations and show its dependence on the following parameters:<br>- types and number of inspectable attributes;<br>- number of credentials:<br>- security levels and inspector's public key sizes; and<br>- the number of inspectors; |
| **Implementation evidence** | The scientific description of the inspection building blocks (theoretical parts), or the implementation of the given inspection scheme (practical part). |
| **Visualization** | Tables |
| **Units of Measure** | The comparison is twofold and therefore has two different units of measurement: the theoretical one will be measured in the number of operations performed for the inspection at the User side, while the practical one will be measured in time units at a well-defined testbed. |
| **Numeric Range** | n/a |
| **How to Calculate** | The calculation can take the difference of the computational efficiency of presentation for the same scenarios with and without inspection in a presentation. The difference should be the inspection overhead. |

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Computational overhead on the Verifier during verification |
| **ID** | Eff-Ins2 |
| **Status** | Final |
| **Audience** | Developer, System Architect |

| | |
|---|---|
| **Description** | Inspection may also have an impact on the verification of the presentation tokens. The Verifier needs to perform an additional step to check whether the "inspectable part" of the presentation token indeed contains the same values as the ones proved in the presentation token and that the Inspector can inspect them.<br>How much this affects the verification efficiency is the main focus of this criterion. It should compare a representative range of different:<br>- types and number of attributes;<br>- number of credentials:<br>- security levels and inspector's public key sizes. |
| **Implementation evidence** | The scientific description of the inspection building blocks (theoretical parts), or the implementation of the given inspection scheme (practical part). |
| **Visualization** | Tables |
| **Units of Measure** | The comparison is twofold and therefore has two different units of measurement: the theoretical one will be measured in the number of operations performed for the inspection at the Verifier side, while the practical one will be measured in time units. For the latter, the testbed must be clearly defined. |
| **Numeric Range** | n/a |
| **How to Calculate** | The calculation can take the difference of the computational efficiency for verification for the same scenarios with and without inspection in a presentation. |

### 3.1.3.2 The inspection process

Apart from the impact of the inspection on the computational efficiency of presentation, it may also be of interest to recognize how efficiently the inspection can be done at the Inspector's site. This may depend on a number of factors, which are described in the table below.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Computational efficiency for inspection (Inspector) |
| **ID** | Eff-Ins3 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | This criterion is used to measure the scheme computational efficiency for the Inspector for performing inspection on a single attribute and the cost (overhead) for inspecting additional attributes from a presentation token. The measurement must take into account a number of parameters: the number of credentials used in the inspectable token, the number of attributes and the types of the attributes to be inspected, at varying security levels. For the practical measurement, the figures should show the testbed where the measurement was taken (hardware/software configuration, scenarios, etc.). |
| **Implementation evidence** | The scientific description of the inspection building blocks (theoretical parts), or the implementation of the given inspection scheme (practical part). |
| **Visualization** | Tables |
| **Units of Measure** | -Time units (seconds) for the practical measurement<br>-Number of (computationally-expensive) mathematical operations for inspection |
| **Numeric Range** | n/a |
| **How to Calculate** | Given different security levels and testbeds, the measurement should clearly show the varying figures for each of the scenarios. Theoretical efficiency of the cryptographic operations for inspection under varying security assumptions, number and types of inspectable attributes, as well as practical measurement on a given testbed. |

### 3.1.4 Revocation

Revocation is an important feature of Privacy-ABCs for many reasons. For one, it is a special challenge to have a revocation scheme that fulfils all the requirements for efficiency, functionality and privacy, due to the unlinkability requirements of presentation (presentation privacy). Thus, no unique identifier of a credential should be revealed to the Verifier (as this would violate the privacy of presentation principle). Therefore, different schemes have been developed to enable support revocation of Privacy-ABCs in a number of different strategies, resulting in different impacts on the other stages of the lifecycle of Privacy-ABCs, but also on the functionalities supported and other practical limitations, which the criteria in the following sections should better clarify.

For instance, a revocation method may have a negative impact on the efficiency of presentation by imposing additional efforts on either the User or the Verifier in order to show that a Privacy-ABC is not revoked without revealing its unique identifier (the revocation handle), besides proving that they fulfil the requirements of the presentation policy in terms of showing that they possess certain type of credential. On top of that, a choice of the revocation scheme may have impacts on the information flow during the different stages of the Privacy-ABCs, resulting in an architecture impact. All of these aspects are reflected in the following criteria presented in the tables below, especially the impact of revocation on the User and on the Verifier.

#### 3.1.4.1 Impact on the User

Similar to inspection, also revocation, depending on the revocation scheme chosen and modalities of the implementation, may have an impact on the efficiency of the presentation for the User and/or on the Verifier. During presentation, the User may need to, in addition to proving possession of the necessary credentials as required by the presentation policy of the Verifier, also prove that the credentials used in the presentation are not revoked. This may directly impact the efficiency of presentation for the User, or the entity which bears the effort for doing such a proof.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Computational overhead on the User for proving the non-revoked status of a credential |
| **ID** | Eff-R1 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | Depending on the revocation scheme, the User may need to fetch the latest revocation information from the Revocation Authority (or any entity to which the Revocation Authority delegates the task of disseminating revocation information). How computationally efficient this is remains to be answered by this metric.<br>The factors that may impact the efficiency include:<br>- the number of revocable credentials in the system<br>- the number of revoked credentials (ratio of revoked to unrevoked)<br>- the frequency of revocation check for the Verifier, namely the period between two different revocation information checks for the Verifier;<br>- the security level used, and<br>- the number of revocable credentials used in presentation.<br>The benchmarks should test this under different scenarios to find the impact of the above factors on presentation. |
| **Implementation evidence** | |
| **Visualization** | Tables or charts |

| | |
|---|---|
| **Units of Measure** | Mathematical complexity (theoretical) or time (practical) |
| **Numeric range** | |
| **How to Calculate** | Compare the efficiency of proving when no revocation check is done with this one. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Computational overhead on the Issuer during issuance |
| **ID** | Eff-R2 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | Depending on the implementation of a specific revocation scheme, the Issuer may need to contact the Revocation Authority during the issuance of a credential in order to obtain the revocation handle for it. The computational complexity for this step (the interaction between the Issuer and the Revocation Authority) as well as the size of the data exchanged between the two entities is an additional criterion, which should be clarified. This may be dependent, and therefore varying the results for different security levels used in this communication. |
| **Implementation evidence** | The description of the implementation of the given scheme. |
| **Visualization** | Tables or charts |
| **Units of Measure** | For the practical part, the unit of measurement is the time to perform the interaction.. |
| **Numeric range** | |
| **How to Calculate** | Calculate, at varying security levels, the amount of revocation-related data the User needs to fetch from the Revocation Authority at different scenarios (different frequencies of update, different ratios of revoked/unrevoked users, etc.) |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Computational and communication overhead for updating non-revocation evidence |
| **ID** | Eff-R3 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | Except for proving the non-revocation, the User may also need to fetch updated version of the revocation information from the Revocation Authority, and then compute the new value of the local witness before proving the non-revocation of the credential(s). Both the computational and communication efficiency in this case are important to benchmark. |
| **Implementation evidence** | Published scientific description/specification of the revocation scheme used (theoretical part), as well as the implementation of that scheme (practical part). |
| **Visualization** | Tables or charts |
| **Units of Measure** | For the computational complexity, the time to perform the interaction, while for the communication complexity the unit should be the data size (bytes). |
| **Numeric range** | |
| **How to Calculate** | Calculate, at varying security levels, the amount of revocation-related data the User needs to fetch from the Revocation Authority at different scenarios (different frequencies of update, different ratios of revoked/unrevoked users, etc.). |

### 3.1.4.2 Impact on the Verifier

Revocation schemes may spare the User from the additional (computational) cost of proving non-revocation by shifting this task to the Verifier. Furthermore, independent of that, any scheme may have some additional overhead on the Verifier on the verification of the presentation tokens which contain revocable credentials (for checking non-revocation).

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Computational overhead on the Verifier for Verifying the validity of credentials |
| **ID** | Eff-R4 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | Same as for the User, this should also test the computational efficiency for the Verifier. This only deals with the difference in performing the local verification of the presented token. This assumes that the version of the revocation information is the latest and only local verification has to take place. |
| **Implementation evidence** | |
| **Visualization** | Graph |
| **Units of Measure** | Data size units (Bytes) |
| **Numeric range** | |
| **How to Calculate** | Compare the efficiency of verification of the presentation token when revocation is implemented as compared to when there is no revocation. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Computational overhead on the Verifier for fetching the latest revocation information and updating local version |
| **ID** | Eff-R5 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | The Verifier must, besides checking that a presentation token is cryptographically valid and fulfils the conditions to access the protected resource(s), also check for the validity of the credentials used in such a presentation token against the latest revocation information. In this case, what we care about is the revocation information provided centrally by the Revocation Authority (or any other entity distributing such information on behalf of the Revocation Authority) – the Issuer-driven revocation.<br><br>In this sense, this benchmarking criterion aims at identifying the computational overhead for the Verifier during the verification of the validity of the credentials used in the presentation token. This may depend on a variety of parameters, depending on the revocation scheme, but this metric must take into account at least the following:<br><br>-total number of users<br><br>-the ratio of revoked to unrevoked credentials<br><br>-frequency of revocation<br><br>-frequency of revocation information update (for the Verifier)<br><br>-the number of revoked users since the last update, and<br><br>-different security levels. |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocations scheme. Implementation of the same and testing with different scenarios. |
| **Visualization** | Table or Chart |

| | |
|---|---|
| **Units of Measure** | Time units (practical test);<br>Mathematical efficiency (the number of expensive operations for the theoretical test). |
| **Numeric range** | |
| **How to Calculate** | The test must perform both theoretical and practical test with varying input parameters from the list above. An option is to check the performance difference between the verification of "similar presentation tokens" from revocable with other non-revocable credentials. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Computational Overhead on the Verifier for the Verifier-driven Revocation |
| **ID** | Eff-R6 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | If the Verifier-driven revocation is supported, it may be interesting to see how the verification of the validity of revocation information about the presented token is impacted in this case.<br>In this sense, this benchmarking criterion aims at identifying the computational overhead for the Verifier during the verification of the validity of the credentials used in the presentation token. This may depend on a variety of parameters, depending on the revocation scheme, but this metric must take into account at least the following:<br>-different security levels<br>-number and type of revoked attributes,<br>- number of users in the system,<br>-if applicable, also the parameters used for the Issuer-driven revocation |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocations scheme. Implementation of the same and testing with different scenarios. |
| **Visualization** | Table or Chart |
| **Units of Measure** | Time units (practical test);<br>Mathematical efficiency (the number of expensive operations for the theoretical test). |
| **Numeric range** | |
| **How to Calculate** | The test must perform both theoretical and practical test with varying input parameters from the list above. An option is to check the performance difference between the verification of "similar presentation tokens" from revocable with other non-revocable credentials. |

### 3.1.4.3 Efficiency of the actual revocation process

Finally, besides the impact the revocation has on other stages of the Privacy-ABCs, it is interesting to also benchmark the actual computational efficiency for doing the actual revocation by the Revocation Authority. On an input a revocation handle, which is a unique attribute in a revocable credential, the Revocation Authority can revoked a credential and update the list of revoked credentials in its database, which should later be synchronised with Verifiers.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Computational efficiency for Processing Revocation Requests (Revocation Authority) |
| **ID** | Eff-R14 |
| **Status** | Final |
| **Audience** | System Architect |

| | |
|---|---|
| **Description** | This metric is used to measure the computational efficiency the Revocation Authority is supposed to handle in order to be able to process a single revocation request. It includes the period from receiving the revocation request until credential in question is revoked. This metric must take into account an expected (average, normal) revocation requests rate in a certain period of time, as well as predict extreme cases, when a maximum number of requests for revocation is made. It does *not* include the computational requirement for disseminating the revocation information to the parties (Verifiers, Users). |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocations cheme. Implementation of the same and testing with different scenarios. |
| **Visualization** | Tables or Charts |
| **Units of Measure** | Time units for the practical tests; the number of basic arithmetic operations for the theoretical test. |
| **Numeric range** | |
| **How to Calculate** | The benchmarking test must be both theoretical and practical. For the theoretical test, the metric must provide number of arithmetic operations required for revoking a credential and updating the repository of (in)valid credentials, while for the practical one the time it takes to process a revocation request (in this case, the testbed must be clearly defined). The test must be made on single and batch revocations, and the performance compared at different security levels. |

## 3.2 Communication Efficiency

Communication efficiency describes a number of criteria, which focus on identifying the size of the data that are produced by the Privacy-ABC technologies under a different set of incoming parameters, such as input data size, the Privacy-ABC feature used, and so on. The structure of this chapter is similar to the one of computational efficiency, starting from the issuance, presentation, inspection, and revocation, but the unit of measurement for these benchmarking criteria is expressed in data units (Bytes) rather than time units.

### 3.2.1 Issuance

Similar to the computational efficiency, a number of factors can influence the communication efficiency for issuance. The tables below present a number of criteria, including the main impacting factors, that should be considered when assessing the communication efficiency for issuance.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Communication Efficiency for Issuance from scratch |
| **ID** | Eff-Iss4 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | This criterion is used to measure the communication size each entity is expected during the issuance protocol. The metric should take into account the following issuance cases:<br>-issuance of credentials with a different number of attributes, and<br>-different security levels,<br>The metric must identify, for each of the above, the following:<br>-the number of messages exchanged between the Issuer and the User (if applicable, also with other parties)<br>-the size of the messages each party is handling at each protocol step<br>-a summary with the overall communication efficiency with the sum of all message sizes from all steps<br>The goal is to see how the size of the communication data changes for every entity, based on the above parameters and identify the requirements for data transfer capabilities for the central entities. |
| **Implementation** | For the theoretical benchmark, the specification of the given Privacy-ABC system and its building blocks from |

| | |
|---|---|
| **evidence** | the research papers, whereas for the practical part, the sensors in the code of the given implementation. |
| **Visualization** | Tabular and/or diagram |
| **Units of Measure** | For the theoretical part, the number and size of group elements transmitted, whereas for the practical part, the unit of measurements must be expressed in bytes. |
| **Numeric range** | n/a |
| **How to Calculate** | Measure the issuance messages exchanged during the interactive issuance protocol between the User and the Issuer. Test with different security levels. |

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Communication Efficiency for Issuance using hardware key binding – smart cards |
| **ID** | Eff-Iss5 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | This metric measures the communication size between a computer terminal and a smart card, when issuance of a credential involves the key-binding operation, which is done on the card.<br>In this case, the metric must define which types of data are exchanged between the terminal and the card, and measure how this traffic size grows with varying:<br>-issuance types (different types and number of attributes)<br>- types of operations done on the card; and<br>- different security levels; |
| **Implementation evidence** | For the theoretical benchmark, the specification of the given Privacy-ABC system and its building blocks from the research papers, whereas for the practical part, the sensors in the code of the given implementation. |
| **Visualization** | Tabular and/or diagram |
| **Units of Measure** | For the theoretical part, the number and size of group elements transmitted, whereas for the practical part, the unit of measurements must be expressed in bytes. |
| **Numeric range** | n/a |
| **How to Calculate** | Show different figures for each type of metric separately or on a cumulative table. Retest with a different security level. |

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Communication Efficiency for advanced Issuance and Credential Update |
| **ID** | Eff-Iss6 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | This criterion is used to measure the communication size each entity is expected during the advanced issuance protocol. The metric should take into account the following issuance cases:<br>-different types of advanced issuance (carry-over, jointly-random, self-claimed carry-over, credential update)<br>-issuance of different types of credentials (different types and number of attributes)<br>-different security levels<br>Moreover, the metric must identify, for each of the above, the following:<br>-the number of messages exchanged between the Issuer and the User (if applicable, also with other parties)<br>-the size of the messages each party is handling at each protocol step |

| | |
|---|---|
| | -a summary with the overall communication efficiency with the sum of all message sizes from all steps<br>The goal is to see how the size of the communication data changes for every entity, based on the above parameters and identify the requirements for data transfer capabilities for the central entities. |
| **Implementation evidence** | For the theoretical benchmark, the specification of the given Privacy-ABC system and its building blocks from the research papers, whereas for the practical part, the sensors in the code of the given implementation. |
| **Visualization** | Tabular and/or diagram |
| **Units of Measure** | For the theoretical part, the number and size of group elements transmitted, whereas for the practical part, the unit of measurements must be expressed in bytes. |
| **Numeric range** | n/a |
| **How to Calculate** | Show different figures for each type of issuance separately. |

### 3.2.2 Presentation

Compared to the computational efficiency criteria, here we focus on the communication efficiency – the amount of traffic each party is expected to handle in different scenarios of presentation. For this purpose, the same criteria as in 3.1.2 should be used here for benchmarked, with the main difference being the focus – measuring the size and number of the messages exchanged between the User and the Verifier during the presentation phase. For the theoretical part, the communication efficiency should show the number and size of the group elements transmitted during the different presentations, while the practical benchmark measures the same in bytes.

### 3.2.3 Revocation

The main communication efficiency aspects for revocation include the overhead on the operations on the other entities, which rely on the revocation information of the Revocation Authority, as well as the efficiency for disseminating the latest revocation information to the Users.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Communication Overhead due to revocation on the Issuer during Issuance |
| **ID** | Eff-R7 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | At certain schemes, a communication between the Issuer and the Revocation Authority must take place at a certain step of the issuance protocol. If this is the case with the given revocation scheme, this criterion must then measure the communication overhead for this message exchange between the Issuer and the Revocation Authority (for instance, if the Issuer needs to retrieve a revocation handle from the RA, which is to be issued in the new credential).<br>Measuring this for a single such request at different security levels can give estimation about other important communication measures, such as average/peak loads. |
| **Implementation evidence** | The implementation of the given Privacy-ABC system. |
| **Visualization** | Table |
| **Units of Measure** | Data size units (Bytes) |
| **Numeric range** | |
| **How to Calculate** | Calculate the size of data exchanged for this purpose at different security levels. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Communication Overhead on the Verifier when fetching updates |
| **ID** | Eff-R8 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | The Verifier must be able to fetch the "latest" revocation information either automatically or at certain time frames. The amount of traffic (data) varies and depends on the revocation scheme and probably on other parameters, such as number of users in the system, number of revoked credentials, ratio of revoked to unrevoked credentials, frequency of revocation information update, security level, and so on.<br>All these parameters must be taken into account and the results of the measurement should clearly show the relation between these and the communication overhead on the Verifier. |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocations scheme. Implementation of the same and testing with different scenarios. |
| **Visualization** | |
| **Units of Measure** | Data size units (Bytes) |
| **Numeric range** | |
| **How to Calculate** | Calculate the size of data exchanged for this purpose at different security levels. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Communication efficiency for dissemination of non-revocation evidence to the User |
| **ID** | Eff-R10 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | Similar to the Verifier, the User may also need to fetch the latest revocation information from the Revocation Authority (or any entity to which the Revocation Authority delegates the task of disseminating revocation information). This benchmarks is used to measure the communication efficiency per dissemination of the revocation information from the Revocation Authority to the Users, in case of personalised non-revocation evidence disseminated from the Revocation Authority for each User (for each credential). The communication size may vary depending on the revocation scheme, but also on a number of factors, such as:<br>- the number of users in the system,<br>- the type of listing (black- vs. whitelisting)<br>- the number of updates per revoked credential per User/Verifier, and<br>- the size of each update message.<br>Knowing these figures, one can predict the amount of traffic the Revocation Authority is expected to handle on average as well as at peak times, if they can be distinguished, in order to help prepare for the required capacities to handle them. |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocations cheme. Implementation of the same and testing with different scenarios. |
| **Visualization** | Tables or Charts |
| **Units of Measure** | Bytes |
| **Numeric range** | |
| **How to Calculate** | Calculate the amount of traffic the Revocation Authority receives/sends during each revocation. |

## 3.3 Storage Efficiency

Storage efficiency is an important factor for benchmarking Privacy-ABC technologies, especially when the user storage device has limited storage capacity, particularly in the case of smart cards. A storage-inefficient Privacy-ABC technology might impact the suitability of different smart card platforms for a given scenario.

### 3.3.1 User's permanent storage

Different Privacy-ABC technologies may require the User to store different amounts of data, starting from the credentials, pseudonyms, and other related data to them. The goal here is to benchmark the efficiency of storage by listing the types of data each technology requires and the amount. This may be important for evaluating the suitability of storing these data on smart cards or other low-memory devices.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Storage efficiency for the credentials and pseudonyms |
| **ID** | Eff-Iss7 |
| **Status** | Final |
| **Audience** | Technology adopters, developers, system architects, smart card developers |
| **Description** | This criterion aims at measuring the size of the credential-relevant data the User needs to store on her side at the end of the issuance. This may be important when the storage of the credential is done on a device with limited storage (i.e. smart cards).<br>It includes the size of the credential or the credential material for the User, excluding revocation-related information. The size may change and has to be tested against the following cases:<br>• varying number of attributes in a credential,<br>• different types of issuance; and<br>• varying security levels. |
| **Implementation evidence** | For the theoretical benchmark, the specification of the given Privacy-ABC system and its building blocks from the research papers, whereas for the practical part, the sensors in the code of the given implementation. |
| **Visualization** | Tabular and/or diagram |
| **Units of Measure** | Data units (Bytes) |
| **Numeric range** | n/a |
| **How to Calculate** | Measure the size of the credentials and pseudonyms under different scenarios, different number of attributes, security levels. |

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Storage efficiency for the system and issuer parameters |
| **ID** | Eff-Iss8 |
| **Status** | Final |
| **Audience** | Technology adopters, developers, system architects, smart card developers |
| **Description** | This criterion aims at measuring the size of the system-wide data that need to be stored for each entity, most importantly at the User side, but also at the other entities, wherever applicable.<br>Depending on the security level, this metric must test (under varying security levels) the size of the: |

| | |
|---|---|
| | • System parameters, and<br>• Issuer parameters,<br>• Revocation Authority parameters, and<br>• Inspector keys.<br>The size of the above data may be impacted by a number of factors, but the most commonly relevant factor is the choice of the key size to be used for all entities, which has a direct relation to the security level provided. |
| **Implementation evidence** | For the theoretical benchmark, the specification of the given Privacy-ABC system and its building blocks from the research papers, whereas for the practical part, the sensors in the code of the given implementation. |
| **Visualization** | Tabular and/or diagram |
| **Units of Measure** | Data units (Bytes) |
| **Numeric range** | n/a |
| **How to Calculate** | Check the size of the issuer parameters and other system parameters that need to be stored on the User side (card or computer), depending on the given security level. |

### 3.3.2 Impact of revocation on the storage efficiency

Revocation may have an impact on the storage efficiency for different entities. On the User, it may impose storage of additional revocation-related information, which needs to be stored besides the credentials. On the Verifier, it may similarly impose additional storage of revocation-related information, which may need to be updated periodically. Finally, the Revocation Authority itself must store a list of revoked credentials or a mapping of such a list to a common value (such as an accumulator). For different choices of revocation technologies, the storage efficiency impact may be different. The following tables reflect a list of criteria aimed at these particularities, which may not be straightforward, but may play an important role on the choice of the revocation strategy.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Storage overhead of the revocation-related information on the User and Verifier |
| **ID** | Eff-R11 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | The User may need to store, besides her credential(s), the cryptographic evidence related to the revocation information of her credentials. This includes the particular revocation-related information that the User needs to store besides the credentials rather than the public values of the revocation database published at the Revocation Authority. Depending on the storage capacities of the device where the User stored these data, it may be an important factor to decide on the type of revocation and other configuration parameters, since the size of the user's revocation information may vary depending on different factors.<br>This benchmark requires to list the types of revocation-related data this entity stores, the sizes of each of these data elements and how, if at all, the repository size changes over time, depending on:<br>-the number of Users, Verifiers, Issuers and Revocation Authorities in the system;<br>-the number of revocable credentials the User possesses;<br>-the security level.<br>The objective of this metric is to find out the appropriate storage requirements for the revocation-related information for the User, but also the Verifier. |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocations cheme. Implementation of the same and testing with different scenarios. |
| **Visualization** | For each of the stored data, a list with a description of their purpose and their confidentiality (access control) is to |

| | |
|---|---|
| | be provided. The reader should understand which data are user-specific and which are publicly available. |
| **Units of Measure** | Bytes |
| **How to Calculate** | Compare the size of revocable to non-revocable credentials. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Storage requirements for the Revocation Authority |
| **ID** | Eff-R13 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | The Revocation Authority, or whichever entity maintains the latest revocation information on its behalf, may need to maintain a publicly available repository with the latest revocation information.<br>This metric requires to list the types of revocation-related data this entity stores, the sizes of each of these data elements and how, if at all, the repository size changes over time, depending on<br>-the number of Users, Verifiers and Issuers in the system,<br>-the security level, and<br>-any information the Revocation Authority keeps for logging purposes (history and such).<br>The objective of this metric is to find out the appropriate storage requirements for the revocation-related information for the Verifier. |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocations cheme. Implementation of the same and testing with different scenarios. |
| **Visualization** | For each of the stored data, a list with a description of their purpose and their confidentiality (access control) is to be provided. The reader should understand which data are user-specific and which are publicly available. |
| **Units of Measure** | Bytes |

# 4. Functionality

Apart from efficiency, another important dimension for comparing different Privacy-ABC technologies is their support for different functionalities, which consist mostly of different features of Privacy-ABCs, but also different factors that impact the architecture of deployment of Privacy-ABCs in different applications, making it less user-friendly, and to identify not obvious limitations of Privacy-ABC technologies. This chapter identifies a number of functionality criteria for benchmarking Privacy-ABC technologies organised following the stages in the lifecycle of the Privacy-ABCs, starting from issuance, presentation, inspection, and revocation. Some of the criteria are designed to have a simple binary answer in terms of support for a given feature, but some other ones may require additional explanation on what impacts or limitations of a given Privacy-ABC technology may be on supporting a certain feature on the users or the information flow (architecture) between the entities (namely User, Verifier, Issuer, Revocation Authority, and Inspector).

## 4.1 Issuance

Functional criteria aim at distinguishing between Privacy-ABC technologies that support certain features from those that don't. In addition, the list also aims at identifying other impacts of deploying Privacy-ABC schemes in practice for the other entities, especially for the Users.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Supported types of issuance |
| **ID** | Fun-Iss1 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | A basic criterion to distinguish different types of Privacy-ABC technologies is their support for the different kinds of issuance from the following list:<br>- Issuance from scratch<br>- Advanced issuance of carry-over attributes<br>- Issuance of self-claimed carry-over attributes<br>- Issuance of attribute values created jointly-random<br>- Issuance of key-bound credentials |
| **Implementation evidence** | Check against the specification of the given Privacy-ABC system and the underlying building blocks used. Test in the implementation of the system. |
| **Visualization** | Tabular |
| **Units of Measure** | Yes/No |
| **Numeric range** | n/a |
| **How to Calculate** | On a matrix-like table, the metric should show for each of the above-mentioned issuance-related features, whether or not the Privacy-ABC system supports them and any necessary additional information to clarify the criteria. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Support for Credential Update |
| **ID** | Fun-Iss2 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | This criterion is used to tell whether the Privacy-ABC in question supports update, rather than re-issuance, of certain attribute values from existing credentials.<br>This criterion may be important in certain occasions, where there are dynamic attribute values in a credential. |
| **Implementation evidence** | Check against the specification of the given Privacy-ABC system and the underlying building blocks used. Test in the implementation of the system. |
| **Visualization** | Tabular |
| **Units of Measure** | Yes/No |
| **Numeric range** | |
| **How to Calculate** | List and describe how the technology supports these features and briefly explain how the technology handles these. |

## 4.2 Presentation

Functional criteria relevant for the presentation deal mostly with the support from a given Privacy-ABC technology for certain Privacy-ABC features, which different applications may require. Therefore, the following criteria in this section aim at distinguishing the differences in supporting these features.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Privacy features for the User |
| **ID** | Fun-P1 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | A basic criterion to distinguish different types of Privacy-ABC technologies is their support for the different kinds of Privacy-ABC features. This criterion lists and explains the supported features from the following list:<br>-Unlinkability<br>-Untraceability-Selective disclosure<br>-Anonymous comparison over attributes (predicates over attributes) |
| **Implementation evidence** | For the theoretical part, the technology specification of the Privacy-ABC system and its building blocks from the public reports or scientific papers, whereas for the practical part, the implementation of the given system. |
| **Visualization** | Tabular |
| **Units of Measure** | Yes/No |
| **Numeric range** | n/a |
| **How to Calculate** | On a matrix-like table, the metric should show for each of the above-mentioned presentation-related features, whether or not the Privacy-ABC system supports them and any necessary additional information. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Supported Predicate functions over attributes |
| **ID** | Fun-P2 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | An additional advantage of certain ABC technologies is that they allow a User to not only reveal a minimal subset of her attribute values, but even more: she can perform different predicates over the values of her attributes, providing additional layer of privacy (anonymity) for the User.<br>The aim is to find out whether logical tests can be made to User's attribute values, without requiring their disclosure, thus generating a more privacy-friendly, anonymous proof.<br>The following list should be taken as a reference:<br>- boolean operations of equality /non-equality of strings, integers, booleans, times, dates;<br>- range proofs (whether a given value lies in a given number range-interval);<br>- equal-one-of proofs (whether a given attribute value matches one of the other values in a group of values);<br>- value comparison (greater than, smaller than);<br>- arithmetic operations: addition, multiplication; and<br>- whether these operations can be performed to compare attributes with constants, attributes with attributes, or both. |
| **Implementation evidence** | The specification of the papers describing the privacy-ABC system or its building blocks (theoretical part), as well as the reference implementation (the code) of the same (practical part). |
| **Visualization** | Tabular |
| **Units of Measure** | Yes/No |
| **How to Calculate** | Compare the supported predicates from the list, if any. If necessary, add explanations on the details. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Controllable "spending" of credentials |
| **ID** | Fun-P3 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | This criterion is used to tell whether a certain Privacy-ABC supports such a feature that they allow users to "spend" their credential a limited number of times. After that, the usage of the credential would be impossible. This may be desired in certain scenarios, where we want the users to be able to perform a certain action only a limited number of times. In this case, the users anonymity should not be violated, but the usage beyond a certain number of times should simply be prevented. |
| **Implementation evidence** | The specification of the papers describing the privacy-ABC system or its building blocks (theoretical part), as well as the reference implementation (the code) of the same (practical part). |
| **Visualization** | Tabular |
| **Units of Measure** | Yes/No and an explanation. |
| **Numeric range** | |
| **How to Calculate** | State whether this feature is supported or not, explain the details of how it works (if supported) and what its limitations/consequences are. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Supported types of pseudonyms |
| **ID** | Fun-P4 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | This criterion is used to tell whether the Privacy-ABC in question supports the following types of pseudonyms, as defined in the ABC4Trust architecture:<br>*-verifiable pseudonyms*<br>*-certified pseudonyms, and*<br>*-scope exclusive pseudonyms*,<br>together with an explanation of each. |
| **Implementation evidence** | The specification of the papers describing the privacy-ABC system or its building blocks (theoretical part), as well as its implementation (practical part). |
| **Visualization** | Tabular |
| **Units of Measure** | Yes/No |
| **Numeric range** | |
| **How to Calculate** | List and describe how the technology supports these features (description is optional). |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Support for Key Binding |
| **ID** | Fun-P5 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | The metric should define whether the Privacy-ABC scheme supports key-binding as an additional feature. Key binding binds a set of credentials/pseudonyms to a certain key, preventing users to combine different credentials (from different users, which should be bound to different keys) in a presentation (during presentation or issuance). |
| **Implementation evidence** | The specification of the papers describing the privacy-ABC system or its building blocks (theoretical part), as well as its implementation (practical part). |
| **Visualization** | Tabular |
| **Units of Measure** | Yes/No |
| **Numeric range** | |
| **How to Calculate** | Simply state whether this feature is supported or not. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Combination of different credentials in presentation |
| **ID** | Fun-P6 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | A User may own more than one credential. Moreover, some of these credentials may be issued by different issuers, which may also be different entities (e.g. a student may possess a bank card credential and a student credential). This criterion is used to specify whether the Privacy-ABC in question allows the user to present a |

| | |
|---|---|
| | proof out of a:<br>- Combination of different credentials from the different Issuers (different Issuer entities)<br>- Combination of different credentials from the same Issuer only (the same Issuer entity) |
| **Implementation evidence** | The specification of the papers describing the privacy-ABC system or its building blocks (theoretical part), as well as its implementation (practical part). |
| **Visualization** | Table |
| **Units of Measure** | Yes/No |
| **Numeric range** | |
| **How to Calculate** | State, for the two above-mentioned criteria, whether the Privacy-ABC in question supports such presentations. |

## 4.3 Inspection

Inspection is certainly one of the features which may be important in certain scenarios because of the possibility to enable a conditional accountability in otherwise pseudonymous presentations of the User. The most important functionality criterion for inspection is the identification of the actual support for inspection, and the possibility to enable different inspection-related risk mitigation features.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Support for inspection and inspection features |
| **ID** | Fun-Ins1 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | This criterion is simply to check whether the given Privacy-ABC technology gives support for inspection or not. In case inspection is supported, then it should also clarify whether users can chose between different Inspectors, in order to give her the freedom to select the inspector she likes. Furthermore, the benchmark should also clarify whether a number of inspectors can be chosen in a multi-party computation fashion, where each can "inspect" part of the presentation tokens, but none would be able to individually do the complete inspection. In addition, it should clarify whether arbitrary attribute values can be encrypted to the inspector, or whether only a specific identifier of the user can be recovered. |
| **Implementation evidence** | The scientific description of the inspection building blocks (theoretical parts), or the implementation of the given inspection scheme (practical part). |
| **Visualization** | Tables |
| **Units of Measure** | Yes/no |

## 4.4 Revocation

The revocation section provides an extensive list of benchmarking criteria in terms of functionality, as this feature deserves a special attention. The first part identifies a number of criteria related to the technology support for different features related to revocation, which may be particularly applicable or challenging for Privacy-ABCs, whereas the second part discusses certain benchmarking criteria that deal with the dissemination of revocation information from the Revocation Authority to the other entities, namely to Users and Verifiers.

### 4.4.1 Support for different features and architectural implications

The criteria in the following tables present different architectural implications of having revocation may impose on the other entities, particularly on the User and the Verifier (on presentation).

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Connectivity requirements for the Revocation Authority |
| **ID** | Fun-R1 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | The revocation mechanism should clarify which, if any, of the parties may need to be online during presentation, in order to check the validity of the presentation tokens against the latest revocation information. In this regard, this criterion should clarify the two following:<br><br>-*Requirement for contacting the RA during presentation (User)* - This criterion has a strong connection with the revocation scheme, but has a direct impact on presentation process. Its requirement for the Revocation Authority to be connected with the User (online) during each presentation has a negative impact on the (computational and network) efficiency of the presentation overall, and the overall process of generating the presentation token.<br><br>-*Verifier's Active Connectivity with the Revocation Authority* - This criterion has a strong connection with the revocation scheme, but has a direct impact on verification of user's claims. Depending on the scheme, the Verifier is supposed to contact the Revocation Authority after every revocation to get the latest version of revocation-related information.<br><br>-*Issuer's connectivity with the Revocation Authority* – the metric must identify the steps (lifecycle moments) when the Issuer needs to contact the Revocation Authority, except for revocation. This may be, for instance, a step during the issuance of the credentials. |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocations cheme. Implementation of the same and testing of the given functionalities. |
| **Visualization** | Table |
| **Units of Measure** | Yes/No |
| **Numeric range** | |
| **How to Calculate** | State if the above conditions stand and explain briefly the details of this part of the architecture. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Support for Issuer- and Verifier-driven revocation |
| **ID** | Fun-R2 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | The issue of "who initiates a revocation process" is solved differently in different schemes, as well as who can revoke.<br><br>In this criterion, the comparison should tell whether the specific revocation scheme allows Issuer-driven revocation.<br>Similarly, the comparison should tell whether the scheme allows for Verifier-driven revocation, if applicable.<br><br>The criterion should compare the two types of revocation against the revocation mechanism in question and give details on whether they are supported by the scheme. If yes, then some basic information how that type of revocation is handled would be complementary. |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocation scheme. Implementation of the same and testing of the supported types of revocation. |
| **Visualization** | Tabular |

| | |
|---|---|
| **Units of Measure** | Yes/No and how. What does the Issuer know from credentials and what does it need from which party. Similarly for the Verifier-driven revocation. |
| **Numeric range** | |
| **How to Calculate** | Show for each type of revocation whether it is supported and some basic details on how this works. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Support for immediate revocation |
| **ID** | Fun-R3 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | It is, in many cases, important that the revocation mechanism allows immediate revocation of credentials. The EU directive on Electronic Signatures requires, among other things, *"…the operation of a prompt and secure directory and a secure and immediate revocation service*" [EC93].<br><br>This functional criterion has to classify schemes based on their support for immediate credential revocation. While this tends to be a difficult task for many revocation schemes, some schemes do not support revocation of credentials before their expiration time. It is nevertheless an important criterion both from a functional point of view, but also as a legal requirement, at least in the European Union's legislation. |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocation scheme. Implementation of the same and testing with different scenarios. |
| **Visualization** | |
| **Units of Measure** | Yes/No |
| **Numeric range** | |
| **How to Calculate** | Explain if this is supported and how. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Scheme distribution |
| **ID** | Fun-R4 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | Issues related to managing the revocation scheme, i.e. whether the scheme supports the distribution of the Revocation Authority into several sub-entities, and whether it allows the "outsourcing" of part of their work, such as dissemination of revocation information.<br><br>Plus, related to risk management, whether the scheme can be distributed to increase the reliability, but also improve performance during high-peak requests. While some cryptographic schemes used for revocation may allow such a distributive revocation service, others may be limited to being performed by a particular (dedicated) server. |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocation scheme. Implementation of the same and testing with different scenarios. |
| **Visualization** | Text |
| **Units of Measure** | Yes/No |
| **Numeric range** | |
| **How to Calculate** | Explain whether the scheme allows for such a distribution and what measures are in place to ensure the basic security and privacy features in that case. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Supported privacy features |
| **ID** | Fun-R5 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | Different Privacy-ABC systems support different privacy features for the User. This metric deals should identify the list of features the Privacy-ABC in question supports from the following:<br><br>- *Backwards unlinkability after revocation* – in some schemes, the different user presentation tokens can be linked together after the revocation. This criterion should explain how this is handled in the given revocation scheme.<br><br>- *Revocation information update-presentation unlinkability* – the revocation scheme must provide protection against the potential linkability of presentation tokens in case the Revocation Authority and the Verifier cooperate, so the update of revocation information from the Revocation Authority and the presentation of the revocation information to the Verifier.<br><br>- *Anonymous update of non-revocation status of own credentials* – this relates to the fact of whether the User is identified during the update of the revocation information about her credentials.<br><br>-*Protection of user (credential) identifiers in the revocation information* – In certain cases, such as online gambling applications, knowing that a certain person is revoked may be personally sensitive information. Therefore, it is important to distinguish between revocation mechanisms that disclose identifiers of the revoked users in the publicly available revocation information. |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocation scheme and its implementation. |
| **Visualization** | Table with a detailed description of how these features are supported (and if they are supported at all). |
| **Units of Measure** | Yes/No and possibly an explanation of how the mechanism supports it. |
| **How to Calculate** | For each of the given features, the criterion must show which specific mechanism is in place to provide those features, if they are present. Otherwise, it should state if certain features are not supported. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Compatibility and integration |
| **ID** | Fun-R6 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | Each revocation schemes has its own cryptographic blocks, upon which is it built, which may cause limitations on its compatibility with certain (versions of) anonymous credential systems, but also its combination with other revocation mechanisms (in case an application needs to combine them).<br><br>In this regard, this criterion must clarify the following:<br><br>- *Compatibility of the revocation scheme with different Privacy-ABC systems* – the given revocation scheme should be checked for applicability to the existing Privacy-ABC systems (U-Prove, Idemix, etc.).<br><br>-*Coexistence with other revocation schemes* – this is probably not technology-specific, but in case there is a limitation such that the scheme cannot be integrated in an application in combination with other schemes (such as, for instance, accumulators in combination with credential update), this should be clarified. |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocation scheme and its implementation. |
| **Visualization** | Tabular |
| **How to Calculate** | List the (versions of) applicable Privacy-ABC technologies, with which the revocation scheme could be integrated. List the revocation mechanisms, which the given revocation mechanism is (not) compatible with or can (not) coexist with. |

### 4.4.2 Dissemination of Revocation Information

The following criteria focus more on aspects related to the dissemination of revocation information to the other entities, namely Users and Verifiers.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Frequency of User's contact with the Revocation Authority |
| **ID** | Fun-R7 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | This criterion has multilateral effects and relations: it depends on the revocation scheme, but has an impact on the performance of the presentation and can be regarded both as functional and performance characteristic. The issue we are looking for here is to identify the cases when the User needs to update her credentials' (non-) revocation information, i.e. during each presentation, on regular time periods, depending on other "external" events to the User (such as after a revocation taking place at the Revocation Authority), after credential validity expiration date, after certain "threshold" is reached (which is decided by the Verifier), etc.<br><br>The aim it to identify how frequently the user needs to contact the Revocation Authority in practice and assess its possible impact on the presentation. This metric, together with the computational and communication efficiency metrics, may be combined to show the real burden on the User the revocation imposes. |
| **Implementation evidence** | Scientific papers describing the building blocks and the Privacy-ABC system using the given revocation scheme and its implementation. |
| **Visualization** | A detailed description on the cases when the User may need to update the revocation-related information about her credential(s). |
| **Units of Measure** | Number of updates in relation to the number of revoked credentials. |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Personalisation (personalised vs. public nature )of the non-revocation evidence (User) |
| **ID** | Fun-R8 |
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | The User may need to fetch personalised non-revocation evidence (witness update) from the Revocation Authority, depending on the revocation scheme. In other cases, the User may download the public value of the revocation information, which is the same for all Users, and compute her witness locally. This may be an important factor to compare different revocation schemes for different purposes, i.e. get revocation information from other Users, in case the Revocation Authority is not available, but may also have other privacy implications.<br><br>This criterion should clarify which approach a given revocation scheme implements. |
| **Visualization** | Tabular |
| **Units of Measure** | Public/Personalised |
| **How to Calculate** | List the different types of data each party downloads and their confidentiality class (public or confidential). |

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Frequency of dissemination of the latest revocation information from the Revocation Authority to the Verifier |
| **ID** | Fun-R9 |

| | |
|---|---|
| **Status** | Final |
| **Audience** | System Architect |
| **Description** | Similar to the User, the Verifier may also need the latest revocation information from the Revocation Authority, in order to be able to verify that the credentials the User has used for the presentation token are indeed valid.<br>This metric should simply state the cases when such a revocation information update takes place: after every update, after a threshold of updates of revocation information at the Revocation Authority repository, or perhaps never. |
| **Implementation evidence** | |
| **Visualization** | A detailed description of the cases when the Verifier needs to fetch new revocation information from the Verifier, if applicable. |

# 5. Security Assurance

From security assurance perspective we consider metrics that are relevant for the complete lifecycle of the Privacy ABC technologies e.g., metrics considering the underlying security proofs and assumptions, as well as security assurance metrics that are specific for a particular lifecycle's step such as "Access to Revocation Handles".

## 5.1 Security of the basic schemes

In order to enable the security assurance-based benchmarking Privacy-ABC technologies we have to consider the security proofs for the basic scheme used in the respective Privacy-ABC technology. The underlying security proofs and assumptions are relevant for the complete lifecycle of Privacy-ABC. It should be taken into account whether implementation is made with security reductions or not. It should be stated whether security proofs are given and under which assumptions.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Security proofs and assumptions of the basic schemes. |
| **ID** | All-Sec1 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | Qualitative metric that lists the underlying security proofs and assumptions.<br>Survey Question: Are the security criteria (cf. Section 1.3.3) of the basic scheme either (i) information theoretic, (ii) computational or (iii) without security reduction/proof (e.g., a lot of U-Prove security)? If "computational", please specify the hardness assumptions. |
| **Units of Measure** | For each security criterion should be described the underlying security proofs and assumptions. |

## 5.2 Inspection

Inspection is an optional feature of Privacy-ABCs, but it has to be assured that the Inspector performs inspection only in cases when predefined conditions are met, as specified in the inspection grounds. Although the Inspector is considered a trusted entity, additional measures can be taken to prevent misuse of the inspection capability. The proposed security assurance metric aims at providing information about how authority misuse is prevented from the person in charge of inspection.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Technical Preventive measures against authority misuse |
| **ID** | Ins-Sec1 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | This is a security measure to prevent authority misuse from the person in charge of inspection. In order to avoid this kind of power misuse, the technology can support respective measures to be implemented, such as key sharing, where k out of n key must come together in order to be able to inspect, but there may also be additional types of protection mechanisms for this purpose. |

| | |
|---|---|
| **Implementation evidence** | |
| **Visualization** | Text or list |
| **Comments** | List the mechanisms used to prevent against authority misuse. |
| **Numeric Range** | n/a |
| **How to Calculate** | List the supported preventive measures. |

## 5.3 Revocation

For the revocation we propose the usage of the security assurance criterion: "Mechanisms used by the Privacy-ABC technology to guarantee the integrity and authenticity of the Revocation Information", "Support in case of compromised end-user's Private Key's" and "Access to Revocation Handles".

### 5.3.1 Protection of Revocation Information

This criteria, as the name suggests, is mostly concerned with the mechanisms the respective technology provides to guarantee particularly the integrity and authenticity of the Revocation Information.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Mechanisms used by the Privacy-ABC technology to guarantee the integrity and authenticity of the Revocation Information |
| **ID** | Rev-Sec1 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | Qualitative metric that specifies the mechanisms used to protect the integrity and authenticity of the Revocation Information.<br>Survey Question: Which mechanisms have been implemented by the Privacy-ABC technology to protect the Revocation Information's integrity and authenticity? |
| **Implementation evidence** | |
| **Visualization** | Text or list |
| **Units of Measure** | List of implemented integrity/authenticity mechanisms, adding a comment if necessary |
| **Numeric range** | n/a |
| **How to calculate** | List the supported preventive measures. |

### 5.3.2 Revocation process

This benchmarking criterion aims to estimate the process that can be triggered in case of a compromised end-user's private key or the support the technology can provide in such cases.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Support in case of compromised end-user's Private Key's |
| **ID** | Rev-Sec2 |

| | |
|---|---|
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | Qualitative metric that describes what happens if end-user's private key has been compromised.<br>Survey Question: Is there a process (i) to request the automatic revocation of all the credentials bound to a specific end-user's Private Key or (ii) to block all the pseudonyms generated from that Private Key for future authentication? |
| **Implementation evidence** | |
| **Visualization** | Text or list |
| **Units of Measure** | Not defined, No (both are not supported), One of them is supported, Yes (both are supported) |
| **Numeric range** | n/a |
| **How to Calculate** | List the supported methods. |

### 5.3.3 Revocation Handles

The "access to revocation handles" security assurance criterion aims at assessing the access level to revocation handles that is possible. The revocation handles are a particular attribute in a Privacy-ABC, which is used to revoke a credential by the Revocation Authority.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Access to Revocation Handles |
| **ID** | Rev-Sec4 |
| **Status** | Final |
| **Audience** | Developer, System Architect |
| **Description** | Qualitative criterion that describes the access level to Revocation Handles.<br>Survey Question: Which of the following access restrictions apply to revocation handles:<br>• Public or private,<br>• Learnt by RA or by Verifier only. |
| **Implementation evidence** | |
| **Visualization** | Text or list |
| **Units of Measure** | Describe the access restrictions that apply to revocation handles. |
| **Numeric range** | n/a |
| **How to Calculate** | List the supported access levels. |

# 6. Legal Data Protection Aspects

The subsequent chapter will look at each step of the lifecycle of a Privacy-ABC system from a privacy protection point of view. Therefore, each step will be examined under each of the six before mentioned protection goals (see 1.3.4). As a result certain requirements for each step will be outlined.

However, for several reasons only observing these requirements will not automatically guarantee a complete legal compliance with the applicable data protection laws. First of all, it has to be borne in mind that the protection goals are not legal obligations per se, even though they are generally well established and based on the fundamental rights to privacy and data protection. Nonetheless, since some of the goals are contradictory, each transformation into law has to strike its own balance. Therefore, different laws might come to a different balance and place more emphasis on one goal rather than another. Secondly, to establish the following requirements it was not only relied upon the six protection goals, but also on the European Data Protection Directive (Directive 95/46/EC, in the following: DPD) [EC95], which sets the frame of data protection in the European Union. The DPD itself, however, only stipulates the minimum requirements of European Law. Consequently, European member states were free – and even encouraged – to achieve a higher level of data protection when transforming the directive into national law. Therefore, the applicable national law may include further obligations. Moreover, the European privacy laws are in a stage of transition. Since the beginning of 2012 the European Union has tried to unify data protection by adopting a General Data Protection Regulation, which would replace not only the DPD but also the national data protection laws. Nonetheless, even though there are no major changes expected in regards to the area of the protection goals, it is not possible to ascertain which new requirements will be introduced until the new regulation is finally ratified.

Therefore, this chapter can only serve as a starting point for a legal evaluation of a specific use case and outline general considerations about the protection goals in each step of the system. These sections are not able to outline the specific legal requirements of each national law nor is it yet possible to elaborate on the exact requirements of the envisaged General Data Protection Regulation.

## 6.1 Issuance

For all types of issuance within an ABC technology mentioned above (see 2.3.1) many requirements depend on the particularities and threats of the given scenario. From the privacy point of view and with regard to the above-mentioned privacy protection goals (see 1.3.4), the following remarks have to be taken into account.

### 6.1.1 Confidentiality

In general all personal data must be kept confidential and processed in accordance with the Data Protection Directive [EC95], the national privacy laws and the purposes stipulated in an informed consent. This applies to all entities processing personal data in Privacy-ABC settings. This has to be guaranteed on the Issuer's side by using appropriate techniques that refer to applicable information security standards, e.g. limiting access or encryption of stored personal data.

On the User side the system must provide mechanisms allowing the User to keep her personal data confidential. This more or less lies in the hands of the User, but she needs to be able to implement requirements (e.g. encrypted file formats for credentials, etc.).

The communication of personal data between User and Issuer should also generally be secured, e.g. by encryption, but this is not specific to Privacy-ABCs but must be considered good practice in general.

### 6.1.2 Integrity

With regard to integrity, during the issuance of a credential, it has to be guaranteed that the User obtains a certificate with correct information and also that the Issuer gets the correct information from the User. It is to prevent that the User gets credentials with another entities' information allowing impersonating this entity. Therefore, the User has to authenticate herself towards the Issuer. The requirements for this identification towards the Issuer determine, together with the security of the underlying ABC-technology, the authentication level and consequently influence the reliability of the issued credential. While the authentication level itself is not directly linked to the ABC-technology it should be possible to express the necessary authentication level somehow showing the Verifier how the User had been identified.

However, it may be noted that use cases exist that do not require that the user identifies towards the Issuer but rather verifies only one or several attributes. In these cases the level of the verification may be interesting for Verifiers.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Indication of the authentication method used by the Issuer |
| **ID** | Leg-Iss1 |
| **Status** | Final |
| **Audience** | Issuers, Verifiers, Users |
| **Description** | Survey Question:<br>Is it possible to connect information on the authentication to issued credentials allowing Verifiers to reliably verify this? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

With specific regard to Privacy-ABCs the underlying cryptographic solutions must prevent that any third party may issue valid credentials falsely indicating the Issuer as issuing entity. Such a forged credential must rather be identifiable as a forgery with the means provided to Verifiers. Likewise it must not be possible to alter attribute values within a validly issued credential without these changes being detectable by a Verifier and invalidating the credential.

### 6.1.3 Availability

The system for issuing a credential has to be sufficiently available. Depending on the requirements and importance of the application relying on the authentication with Privacy-ABCs, the User must be able to obtain a credential within a defined timeframe. Users should be able to solve minor problems (e.g. change of PIN on a smartcard token) themselves.

### 6.1.4 Transparency

The User and the Issuer need to be clearly and in an understandable way informed about all privacy-relevant data processing including the legal, technical and organizational settings. Documentation and information required for informed consent in the sense of Art. 2 DPD [EC95] have to be guaranteed.

Furthermore, there needs to be a documentation of the given consent (e.g. by a signed consent form or a protocol of digitally given consent).

Nevertheless, both the Issuer and the User have to be informed about all steps of the credential issuance scenario, including e.g. a privacy policy.

Furthermore, in case of delegation, it has to be clearly visible if one entity is acting on behalf of another. (Art. 10, 17 DPD [EC95])

### 6.1.5 Intervenability

Issuer and User need to have, already during the issuance process but also afterwards, the opportunity to intervene in all privacy-relevant data processing. While on the Users' side this means mostly that there has to be an effective way of exercising one's data subject rights, in particular to erase one's data or withdraw one's consent, the Issuer also has to be able to overrule automated decisions or stop a running process to limit possible harm. Moreover, intervenability also includes the right to lodge a claim or raise a dispute to achieve a satisfying remedy. Nevertheless, in the context of issuance, the ability to correct incorrect attributes in a credential is of upmost importance for both sides.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Intervenability during/after the process of issuance of credential |
| **ID** | Leg-Iss2 |
| **Status** | Final |
| **Audience** | Users, Issuers |
| **Description** | Survey Question:<br>Is it possible for the User as well as for the Issuer to intervene/correct incorrect issuance of a credential, e.g. if a User receives some credential with incorrect attribute values (wrong spelling, or other cases)? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

### 6.1.6 Unlinkability

Credentials have to be issued in a way that they do not allow linking between presentations unless this is an effect of the personal data verified or necessary for a particular scenario. In detail the protection goal of 'unlinkability' means, in the context of credential issuance, that one is unlinkable of issuance and presentation, even if the Issuer and the Verifier, or even multiple Verifiers cooperate. Likewise two presentation tokens used in relation to different Verifiers must not allow linkage. Linking here refers to certain transactions with those credentials rather than linkage of the credentials themselves.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Linking or tracking by Issuer or Verifier on basis of extended knowledge |
| **ID** | Leg-Iss3 |
| **Status** | Final |
| **Audience** | Issuers, Verifiers, Users |
| **Description** | Survey Questions:<br>Is it possible for an issuer who has retained all information available for the issuance process (legal or not) to |

| | |
|---|---|
| | identify a User who authenticates only with not-identifying attributes such as age or place of living?<br>Is it possible to link different issuance processes from the same User?<br>Is it possible that different Verifiers collaborate to link different uses of the same credential? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

Furthermore, the advance collection of credentials that can be managed locally by the User without the need to contact a central entity should be allowed.

Within the issuance process, only necessary personal data should be processed and retained by the Issuer. Personal data that is not necessary any more has to be deleted by the Issuer.

In case the issuance may occur towards an anonymous user, lower communication layers need to be secured by other means, e.g. mix-cascades to hide IP-addresses as Privacy-ABCs to prevent linkability on the application level.

## 6.2 Presentation

During the presentation and verification phase for ABC-Technologies, the following has to be taken into account with regard to the above-mentioned privacy protection goals (see Section 1.3.4).

### 6.2.1 Confidentiality

In general, all personal data must be kept confidential. This has to be guaranteed on the Verifier's side by using appropriate techniques that refer to applicable information security standards, e.g. limiting access or encryption of stored personal data, especially user attributes.

Within a Privacy-ABC technology, sufficient security for the storing and processing of personal data has to be ensured on the Verifier´s side. This assumes secure communication channels (e.g. SSL), as well as secure storage and processing of personal data (e.g. encryption) for the Verifier are in place.

For Verifiers in an inspection-enabled system this is true for the stored tokens. Even if the information, verifiable by the Verifier, only contains non-identifying attributes, due to the encrypted inspectable section the whole token must be treated as personal data and hence the storage of tokens must comply with data protection requirements. This holds even more for the presentation tokens containing revealed attributes from users, which need to be protected from any misuse.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Confidentiality of attributes |
| **ID** | Leg-P1 |
| **Status** | Final |
| **Audience** | Users, Verifiers |
| **Description** | Survey Question:<br>Is it possible for the Verifier to get more information from the presentation token than intentionally presented by the User? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

### 6.2.2 Integrity

Within the ABC system, it has to be prevented, that a User can authenticate himself with false data. Therefore appropriate cryptographic needs to be used, such as signatures to prevent creation of forged

presentation tokens. Users can only prove the attribute values contained within the credential. Consequently it also has to be guaranteed that only correct presentation tokens are derived from the source credential. Therefore, it has to be prevented that the User can alter the attributes while obtaining a presentation token as well as that the system includes attribute values into the token, which do not exist in the credential.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Fraud prevention |
| **ID** | Leg-P2 |
| **Status** | Final |
| **Audience** | Users |
| **Description** | Survey Questions:<br>Can the user also prove other attribute values contained within the credential?<br>Is authentication with false data possible? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

### 6.2.3 Availability

Besides the technical hardware that should be available for the presentation and verifying process in particular the availability of the presentation policy of the Verifier gains importance during the presentation phase. Only if the User is able to see the presentation policy beforehand she is able to determine if she can authenticate towards the Verifier. Consequently the policy should be disclosed to the User as soon as possible.

On the User side, the necessary hardware (for example card readers) has to be available. Furthermore, the User has to possess credentials that verify the necessary attributes so that she is able to create a presentation token matching the presentation policy. Last but not least, it is advisable to provide the User with a possibility to test the validity of her credential. However, this issue is closely connected with the revocation process and will therefore be discussed in the relevant section.

### 6.2.4 Transparency

For the presentation and verification process, necessary information for an informed consent needs to be provided for the User and the Verifier. Especially the Verifier and its representative (if any) have to inform clearly about which data needs to be processed for which purposes within the particular ABC-Technology, as required by Art. 10 DPD [EC95]. Regarding the presentation token, the User needs to be informed about storage and deletion of all personal data. This is basically done by a detailed privacy policy containing a description of the purposes for which the personal data will be processed.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Information about the purpose, the stored attributes and the retention period of the data processing |
| **ID** | Leg-P3 |
| **Status** | Final |
| **Audience** | Users |

| | |
|---|---|
| **Description** | Survey Question:<br>Is the User provided with clear and understandable information regarding the purpose, the stored attributes and the retention period of the data processing? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

### 6.2.5 Intervenability

Intervenability in the presentation phase should not be reduced to the possibility of the User to abstain from using a service, because she does not agree with the presentation policy. Consequently, the User should be able to complain about or initiate a review of the presentation policy. This possibility should be provided by the Verifier itself or the respective data protection authority.

### 6.2.6 Unlinkability

In the context of the token presentation, the protection goal of "unlinkability" can mostly be specified as "multiple-presentation-unlinkability", where a Verifier is not able to link different presentation tokens of the User.

To avoid linkability, tokens used in different transactions of the Verifier should in general be unlinkable unless they share equal attributes identifying the User or intentionally contain equal pseudonyms. As Privacy-ABCs are deployed to enhance privacy, Verifiers should also abstain from deploying other methods of linking transactions or persons, e.g. cookies.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Linking of different presentation tokens |
| **ID** | Leg-P4 |
| **Status** | Final |
| **Audience** | Verifiers |
| **Description** | Survey Questions:<br>Is the Verifier able to link different information of the User?<br>Are any tracking mechanisms, such as cookies, used for linking? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

Within a Privacy-ABC technology, the principle of data minimisation has to be complied with during the presentation phase by only collecting those attributes necessary for the specified purposes on the Verifier's side. Furthermore, a limitation of the storage period is necessary and needs to be defined within the privacy policy. The immediate deletion of non-inspectable presentation tokens after the end of a transaction is preferable, since it is not only in compliance with the principle of data minimisation but also reduces the possibilities of linking different interactions of the User.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Limitation of storage period |
| **ID** | Leg-P5 |
| **Status** | Final |
| **Audience** | Verifiers |
| **Description** | Survey Questions:<br>Is the retention period limited with respect to presentation tokens?<br>Is the immediate deletion of non-inspectable presentation tokens implemented after the end of the transaction? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

## 6.3 Inspection

In the context of Privacy-ABCs, inspection is the retrospective identification of the User in a case where an inspection ground is triggered. As the identification of a User affects her privacy, this feature has to comply with the privacy protection goals in order to not undermine User rights (Art. 10 et seqq. DPD [EC95]).

### 6.3.1 Confidentiality

In general, all personal data must be kept confidential. This has to be guaranteed on the Inspector's side by using appropriate techniques that refer to applicable information security standards, e.g. limiting access or encryption of stored personal data. In particular the Inspector's secret key allowing to decrypt the inspectable sections of the presentation tokens must be well guarded.

As in all systems processing or storing personal data, the data contained in a presentation token may usually contain personally identifying information and thus should therefore be securely processed and stored.

For Verifiers in an inspection-enabled system this is particularly true for the stored tokens. Even if the information verifiable by the Verifier only contains non-identifying attributes, due to the encrypted inspectable section the whole token must be treated as personal data and hence the storage of tokens must comply with the data protection requirements. Furthermore, it has to be ensured that the Verifier is not able to see the inspectable attributes or decrypt the encrypted section of the token without the involvement of the Inspector. On the Inspectors side, the inspected attributes and any related information must be processed in accordance with the Data Protection Directive[EC95] and appropriate means should be implemented to avoid any potential misuse of authority or accidental loss of personal data. This may be accomplished by deploying appropriate techniques that refer to applicable information security standards, e.g. use smart cards, limiting access to systems and/or encryption of stored personal data. Moreover, it has to be ensured that the identity of the User is only disclosed if an inspection ground is fulfilled. Therefore, a viable inspection process has to be in place that includes the obligation for the Inspection requester to provide adequate evidence of the fulfillment of an inspection ground.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Confidentiality of the inspectable part of the presentation token |
| **ID** | Leg-Ins1 |
| **Status** | Final |
| **Audience** | Issuers, Verifiers, Users |
| **Description** | Survey Questions:<br>Is it impossible for any third party, other than the Inspector, to see the inspectable attributes?<br>Is it impossible for any third party, other than the Inspector, to decrypt the encrypted section of the inspectable token without the involvement of the Inspector? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

### 6.3.2 Integrity

With regard to integrity, the Verifier, trusting to have obtained appropriate data about the user in case an inspection ground is given, should be able to verify that the correct information is indeed contained within the encrypted part of the presentation token. Furthermore it must not be possible for the user to forge some different attribute-value into the presentation token than issued for the particular attribute in the credential. While the technology does not necessarily need to totally prevent this to happen such an attempt must at least be detectable.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Verification that the inspectable part of the presentation tokens contains the required data |
| **ID** | Leg-Ins2 |
| **Status** | Final |
| **Audience** | Issuers, Verifiers, Users |
| **Description** | Survey Question:<br>Is it possible for a Verifier to check whether the attributes are correct, e.g. by having the Inspector validate them? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

### 6.3.3 Availability

The process set up for inspection of a presentation token has to be sufficiently available. Depending on the requirements and importance of the use case relying on the authentication with Privacy-ABCs, the Verifier must be able to obtain the information within a defined timeframe. The process of contacting and involving the Inspector should therefore be tailored to the necessities of the use case but also to the sensitivity of the information obtained by the Inspection. The Inspector must be available and be allocated sufficient resources to verify the inspection grounds in a timely manner.

### 6.3.4 Transparency

The User needs to be informed clearly and accessibly about any privacy-relevant data processing including the legal, technical capabilities and organizational settings of the inspection process. Documentation and information required for informed consent in the sense of Art. 2 DPD [EC95] has to be available.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | User information on inspection process |
| **ID** | Leg-Ins3 |
| **Status** | Final |
| **Audience** | Issuers, Verifiers, Inspectors, Users |
| **Description** | Survey Questions:<br>Is the User informed about the clearly defined inspection process, including the accessible inspection grounds? Is there a system to notify the User of the fact that an inspection occurred, if this is not legally prohibited, e.g. by a gag order?<br>Are all the steps in the inspection process logged to allow review? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

### 6.3.5 Intervenability

Users need to have the opportunity to intervene in any privacy-relevant data processing with regard to the process of inspection. This addresses inter alia the data subjects' rights to rectification and deletion and withdrawal of consent. Depending on the use case, this may be possible to accomplish with cryptographic means, but also on an organisational level, e.g. hearing of the User by the Inspector after inspection but prior to the release of information to the Verifier. Furthermore, the right to intervene is governed by the normal rules of law. While the organisation (Verifier) would be entitled to retain the identifying information under a normal system set up (storing clear text data right from the start), the User may rather not demand deletion of inspectable tokens after a withdrawal of consent.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Definition and balance of the inspection process |
| **ID** | Leg-Ins4 |
| **Status** | Final |
| **Audience** | Issuers, Verifiers, Inspectors, Users |
| **Description** | Survey Questions:<br>Is there a predefined inspection process, with clear attributions of roles and competences? Is it procedurally guaranteed that no other than the predefined inspection grounds are assessed?<br>Is it ensured that rights of the Inspection Requester and the User are weighed against each other?<br>Is it ensured that Inspection Requesters cannot blackmail Users through the repeated misuse of the report function? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

### 6.3.6 Unlinkability

While inspection in many use cases aims at identifying a User and thus on linking a particular occurrence to a specific person, the mere existence of an inspectable token must not allow linkability. Thus inspectable presentation tokens derived from a single credential must not be linkable among each other, among inspectable tokens presented towards another Verifier or become linkable if the Verifier and the Inspector act collusively. These criteria refine the unlinkability criteria for inspectable tokens.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Identification by Verifier on basis of extended knowledge |
| **ID** | Leg-Ins5 |
| **Status** | Final |
| **Audience** | Issuers, Verifiers, Users |
| **Description** | Survey Questions:<br>Is it possible for a Verifier having a series of inspectable presentation tokens derived from a single credential to identify the relation among the tokens unless the inspection part of the token is decrypted by the inspector?<br>Is it possible for several Verifiers acting collusively and having possession of a series of inspectable presentation tokens derived from a single credential to identify the relation among the tokens unless the inspection part of the token is decrypted by the inspector?<br>Is it possible for Verifiers acting collusively with the Issuer of a source credential on basis of the possession of a series if inspectable presentation tokens derived from a single credential to identify the relation among the tokens unless the inspection part of the token is decrypted by the inspector? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

## 6.4 Revocation

Within a system deploying Privacy-ABC technology, revocation means the act of withdrawing the validity of a previously issued credential. Revocation is performed by a dedicated Revocation Authority, which could be the Issuer, the Verifier, or an independent third entity. Which Revocation Authorities must be taken into account can be specified by the Issuer in the issuer parameters (Issuer-driven revocation) or by the Verifier in the presentation policy (Verifier-driven revocation).[2] As this terminates the possibility to use the service, these measures must be assessed with regard to the privacy protection goals.

### 6.4.1 Confidentiality

It has to be ensured that the User's communication with the Revocation Authority employs secure channels. If revocation is caused by the cancellation of the contract between User and Issuer, the Issuer with regard to the principle of purpose binding, must securely delete the respective personal data that has been kept during the legal relationship unless retention of the personal data is required. Adequate and secure methods for deletion have to be used (e.g. overwriting). Furthermore, the general process in

[2] See glossary of deliverable D5.1 [D5.1]: https://abc4trust.eu/index.php/pub/119-d5-1-scenario-definition-for-both-pilots.

case of the termination of the business relation has to be defined in detail and should also be part of the contractual relationship.

### 6.4.2 Integrity

It has to be ensured that in case of revocation of a credential, it should not be possible to be used for authentication purposes anymore without the Verifier at least getting to know that the credential has been revoked. Even if the credential has been revoked, the User must still be able to read its contents. Also the use in relation to Verifiers should still be possible to e.g. allow verifying that the owner of a replacement credential is identical to the owner of the revoked credential. Only the parties entitled to request or to start a revocation must be able to trigger the revocation process.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Use of revoked credential |
| **ID** | Leg-R1 |
| **Status** | Final |
| **Audience** | Users, Issuers, Revocation Authorities |
| **Description** | Survey Questions:<br>Is secure authentication provided to ensure that the correct User's attributes are revoked?<br>Can revoked credentials still be used for authentication purposes (generate presentation tokens out of revoked credentials)?<br>If so, will the Verifier learn about the revocation, if it follows the procedures necessary for Issuer-driven revocation? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

### 6.4.3 Availability

It needs to be ensured that the Revocation Authority is sufficiently available and can respond in a timely manner. This must be the case for cases of revocation, as well as un-revocation, i.e. instances when a wrongful revocation has occurred or the reason for the revocation ceases to exist. Due to the severe consequences of revocation for the User, there has to be a clearly defined revocation process at hand.

### 6.4.4 Transparency

The key point here is documentation. A clear process for the revocation of credentials as well as retention or deletion periods and a process for the deletion of personal data have to be defined within the terms and conditions and while setting up the process of deploying Privacy-ABCs. All parties involved have to know how they can trigger the revocation process. Especially the User should be provided with detailed information.

A further form of documentation, such as secure logging, must be in place for keeping records of every – even temporary – revocation of credentials and changes in the revocation information. Thus, the Revocation Authority can be deterred from attempting to identify a User by abusing the revocation process and thereby breaking the anonymity of the Privacy-ABCs. While it is technically possible that a Revocation Authority finds out about a specific interaction of a User by briefly pretending that a

particular target credential has been revoked and waiting for a failed presentation of the target credential, the documentation requirement would, at least, make the abuse detectable. Furthermore, documentation should contain processes for re-issuance of certificates in case of lost credentials.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Documentation |
| **ID** | Leg-R2 |
| **Status** | Final |
| **Audience** | Users, Issuers, Revocation Authorities |
| **Description** | Survey Questions:<br>Can Users see on the user interface, whether a credential has been revoked?<br>Are Users informed about revocation policy?<br>Are retention periods made known to the User?<br>Is a process for deletion of especially personal data made known to the User?<br>Are processes for re-issuance of certificates in case of lost credentials defined?<br>Is the revocation process itself documented? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

### 6.4.5 Intervenability

Revocation of a credential is a means to support intervenability. For a system using Privacy-ABCs, it is necessary to define who is allowed to demand a revocation (Revocation Requestor). This does not necessarily need to be the same person that actually triggers the technical process of listing a credential as revoked. Besides the Issuer, it will usually be the User who is running the risk of impersonation and consequently should be entitled to demand revocation. Therefore, as already mentioned within the transparency section, a clear revocation process for all parties concerned has to be established.

This revocation process may also govern the deletion of personal data. E.g. if the reason for the revocation is the termination of the underlying legal relationship with the User, the process to check necessity for further processing of personal data must be triggered and unnecessary personal data must be deleted or otherwise blocked. Additionally, the processes for re-issuance and un-revocation have to be accessible to the User.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Documentation |
| **ID** | Leg-R3 |
| **Status** | Final |
| **Audience** | Users, Issuers, Revocation Authorities |
| **Description** | Survey Questions:<br>Can Users initiate the revocation process?<br>Are processes for re-issuance of certificates in case of lost credentials and for un-revocation defined? |
| **Units of Measure** | Yes, no or "to be accomplished with extensions" |

### 6.4.6 Unlinkability

Also within the revocation of a credential, linkability of credentials or personal data has to be prevented. Therefore unique identifiers should not be used to list revoked credentials or at least must not allow linkability among presentation tokens. The revocation of a credential of a User should not have any effect to any valid credential of this User.

The revocation process must in particular also not require that the Revocation Authority is contacted every time, when a presentation token is used, to ascertain if a particular credential is revoked or not. Otherwise the Revocation Authority would gain information on all occurrences and the respective Verifiers at which a credential is being used. Therefore, the Privacy-ABC system of a user should by default perform proactive updates of the required non-revocation evidence at regular intervals and only allow the User to change the default setting to contacting the revocation authority only shortly prior to presenting a credential for the necessary data. Similar safeguards should be implemented on the Verifiers side. A Verifier has to be prevented from identifying a User by linking changes in the provided revocation information to failed presentation attempts.

| Attribute | Attribute Definition |
|---|---|
| **Summary** | |
| **Name** | Deletion |
| **ID** | Leg-R4 |
| **Status** | Final |
| **Audience** | Issuers, Revocation Authorities |
| **Description** | Survey Question:<br>Are adequate and secure methods of deletion possible (e.g. overwriting)? |
| **Units of Measure** | Yes, no or “to be accomplished with extensions” |

# 7. Economic Viability

Economic viability criteria identify the most important factors that may impact the choice of a certain Privacy-ABC technology or a combination of the platform for different aspects of Privacy-ABC technologies as enablers of the privacy-enhancing identity management schemes. They are also organised following the lifecycle of Privacy-ABCs.

## 7.1 Issuance

In the case of issuance, the economic viability criteria are mostly concerned with predicting (economic/financial) factors from the issuance process that could influence the choice of a given Privacy-ABC technology. The main focus here is to help parties deploying the technology (adopters) to make the best choice between given Privacy-ABC technologies, and to choose the most suitable combination of the hardware/software platform that fulfils the operational requirements/functionalities. The following table summarizes the most important factors that impact the choice of the Privacy-ABC technology on a given application scenario.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Cost of running own issuance service |
| **ID** | Ecn-Iss1 |
| **Status** | Draft |
| **Audience** | System Architects, Technology adopters |
| **Description** | A number of different factors may impact the choice of economically more viable technology, among the most relevant ones being:<br>• The expected (privacy, security) benefits by deploying a certain Privacy-ABC technology, supported functionalities<br>• Costs for the hardware for the Users (storage related, i.e. smart cards and smart card readers, mobile phones, etc.)<br>• Cost for setting up a dedicated Issuer service (server setup and maintenance)<br>• Licensing differences between different available Privacy-ABC technologies (e.g. open source with modification rights, or not)<br>• Development costs for integration into the application<br>• Cost for outsourcing the service<br>• Technical support costs<br>• Cost of identity vetting, i.e., checking that attribute values issued to users are correct.<br>Taking these factors into account, one could estimate certain differences in economic viability for different technologies, and decide on the model of deploying an issuance service, such as in-house, or outsourced. |
| **Visualization** | n/a |
| **Units of Measure** | Monetary value. |
| **Numeric range** | n/a |
| **How to Calculate** | Compare the given benefits and the expected costs for deploying different privacy-ABC technologies, and different available options for deployment. |

Besides calculating the cost for different operations related to the issuance, one can also investigate the opportunity that can be given by running an Issuer (issuance service) for other entities in a given market. In this case, the different economic models could be used to compare what the revenue stream for such a service would be, and compare it with the costs given for putting it in operation.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Economic incentive to serve as Issuer |
| **ID** | Ecn-Iss2 |
| **Status** | Draft |
| **Audience** | CEOs, Higher Management |
| **Description** | Running an issuance service is serving as a trusted identity service provider for other entities. In practice, such an entity can be a private or public service, whose credentials would be trusted by other services. In such an ecosystem, one would need to account for a number of different factors that could influence the economic viability to offer such a service. Among these, the most relevant factors include:<br>- The hardware cost for running the issuance service<br>- Development costs for integrating it into the desired ecosystem/applications<br>- The revenue model to be applied (e.g. charge per-issuance, or similar)<br>- Assessment of the potential use of the issuance services (trends, frequency of issuances over time)<br>- The potential licensing costs for using protected intellectual property from vendors of the Privacy-ABC technology<br>- Costs for user's dedicated devices, if applicable<br>- Potential costs for certification/standardisation necessary<br>- Liability costs for identity-related services |
| **Visualization** | n/a |
| **Units of Measure** | Monetary value. |
| **Numeric range** | n/a |
| **How to Calculate** | Take all the above parameters into account, and evaluate the economic viability for running a dedicated issuance. |

## 7.2 Presentation

Similarly to the issuance stage, the benchmarking criteria related to the presentation phase aim at identifying the most important factors related to presentation that is more suitable in economic terms.

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Relevant criteria for benchmarking presentation economic viability |
| **ID** | Ecn-P1 |
| **Status** | Final |
| **Audience** | System Architects, Technology adopters |
| **Description** | A number of different factors may impact the choice of economically more viable technology wrt to presentation, among the most relevant ones being:<br>• Necessary Privacy-ABC features to be used during presentation, i.e. key binding, predicates, inspection, revocation, etc.<br>• Economic costs (personnel, overhead, hardware, etc.) for providing and maintaining the Verifier services |

| | |
|---|---|
| | • Licensing issues from vendors of Privacy-ABC technologies<br>• The number of users and the IT skills of the users;<br>• Technical support for users;<br>• In case revocation is required, potential costs involved for verifying revocation information<br>• If inspection is needed, the potential costs of using the inspection feature<br>• The computational device of the users<br>• Types of personal data to be disclosed in presentation policies and potential liability issues resulting from such data.<br>Taking these factors into account, one could estimate certain differences in economic viability for different technologies, based on their requirements for each of the above factors. |
| **How to Calculate** | The technology adopters have to decide on the best compromise for their choice between the given costs and the requirements. |

## 7.3 Inspection

If inspection is needed, one needs to take into account the costs associated with running an Inspector entity. On top of that, running such a service can also be based on a dedicated revenue model, such as charging per-inspection, or applying contracts with running flat-rate payments over periods (in case such a service is intended to be served for profit by private companies).

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Relevant criteria for benchmarking inspection economic viability |
| **ID** | Ecn-Ins1 |
| **Status** | Final |
| **Audience** | System Architects, Technology adopters |
| **Description** | A number of different factors may impact the choice of economically more viable technology, among the most relevant ones being:<br>• Cost of running and maintaining an “Inspector” entity in-house compared to outsourcing<br>• Expected revenue model for running an inspector service (e.g. charge per issuance, or flat monthly rate for Verifiers)<br>• Eventual cost of inspection by the Inspection (e.g. per inspection cost), in case externally provided<br>• Communication costs (communication size, number of interactive protocol steps) per transaction (inspection token)<br>• Licensing issues for using the cryptographic libraries required for inspection<br>• Organisational costs (personnel, overhead, etc.) for setting up the inspection functionality<br>• Organisational costs for verifying that the inspection grounds have been meet<br>• The number of inspectors<br>• Number of Verifiers involved and expected trend of Verifiers<br>• Estimated frequency of performing inspection<br>• Liability and insurance costs<br>• Costs for mitigating different security risks of misuse (by persons acting as inspectors)<br>• Reputation benefits and costs in cases of misuse<br>Taking these factors into account, one could estimate certain differences in economic viability for different technologies, based on their requirements for each of the above factors. |

## 7.4 Revocation

Revocation service is a potential feature, which can be profitable in case of a good revenue model analysis. For Verifiers it is important to recognize which credentials are revocable and which are not, and this can be a service, which Verifiers could be willing to pay for. On top of that, depending on the revocation design, such a service could also be interesting for Issuers, who may need some interaction with the Revocation Authority when issuing credentials (e.g. assigning a unique credential identifier, i.e. a revocation handle, to enable credential revocation).

| Attribute | Value |
|---|---|
| **Summary** | |
| **Name** | Relevant criteria for benchmarking economic viability of the revocation mechanism |
| **ID** | Ecn-R1 |
| **Status** | Final |
| **Audience** | System Architects, Technology adopters |
| **Description** | A number of different factors may impact the choice of economically more viable technology/mechanism for revocation, among the most relevant ones being:<br>• The costs of implementing a certain revocation scheme<br>• Revenue stream (charging model for Verifiers and Issuers, potentially also Users) for providing revocation-related services<br>• Cost of running and maintaining a "Revocation Authority" service, including the cost of implementing the right security features<br>• Potential costs of required certification<br>• The number of users in the system, number of Issuers, and Verifiers<br>• Frequency of the non-revocation proof and non-revocation verification<br>• Expected frequency of revocation<br>• Liability costs and costs for legal compliance<br>• Potential reputation costs and benefits from providing the service<br>Taking these factors into account, one could estimate certain differences in economic viability for different technologies, based on their requirements for each of the above factors. On top of that, one can assess what revenue model suits best for a particular scenario, e.g. whether to charge per-revocation, per-revocation-check, or apply other flat-rate models, as well as the parties which would be supplying such revenue streams (Issuers, Verifiers, and/or Users) |
| **Visualization** | n/a |
| **Units of Measure** | Monetary value |
| **Numeric range** | n/a |
| **How to Calculate** | Compare the costs |

# 8. Summary of the criteria

The previous chapters have defined a number of different criteria for benchmarking Privacy-ABC technologies. They present a numerous collection of individual criteria from different dimensions, as earlier described. In this section, the reader is presented with a minimalistic overview of a selection of the most relevant criteria from the five different dimensions, namely *efficiency, functionality, security assurance, economic viability, and legal data protection aspects*, along the lifecycle of Privacy-ABCs, similar to before. This is presented in Table 8.1, which also enables the reader to see how a combination of different dimensions can be reflected against one another, and read a minimal set of benchmarking criteria, giving a higher-level overview of the previous piece of the work in the other chapters.

This is not meant as a replacement or complement to the individual criteria provided in earlier chapters, but rather as a higher-level overview of the criteria. Interested readers can then browse from one section (column) from the table into the respective chapter in the deliverable, which follows a similar organisational structure.

**Table 8.1 - An accumulated representation of a summary of the main benchmarking criteria**

| Dimension / Stage | **Efficiency** | **Functionality** | **Security assurance** | **Economic viability** | **Legal data protection** |
|---|---|---|---|---|---|
| **Issuance** | -Computational, communication and storage efficiency (CCSE[3]) based on the issuance types used[4];<br>-Potential impact of revocation on the CCSE of issuance;<br>-Impact of the key length (security assurance level) on the CCSE of issuance;<br>-Storage efficiency for user's credentials and pseudonyms;<br>-Storage efficiency for the static system-wide crypto parameters;<br>-Storage efficiency for the User of the public keys of other entities;<br>-Cryptographic key size. | -Supported types of advanced issuance features, such as *carry-over of attributes*, *same key binding*, jointly random issuance of attribute values;<br>-Issuance of revocable vs. non-revocable credentials;<br>-Support for credential update. | -Security assumptions and level of security assurance for the chosen Privacy-ABC features;<br>-Security assurance level (chosen key length) for the cryptographic operations;<br>-Measures to assure the adequate identity assurance level for issuance of credentials;<br>-Security of communication channel along the lifecycle of Privacy-ABCs, to preserve both security and privacy features. | -Costs for technical solution of running and maintaining an Issuer;<br>-Costs related to intellectual property (implemented cryptographic libraries used as building blocks);<br>-Revenue model for providing issuance service (pro-issuance, flat-rate);<br>-Reputation gain by acting as a trusted identity service provider. | -Correctness of verified attributes in credentials;<br>-Detectability of forged or altered credentials;<br>-Provision of clear and understandable information about the issuance process;<br>-Sufficiency of information, provided before giving informed consent;<br>-Possibilities to intervene during the issuance process;<br>-Prevention of linking of interactions with one credentials as well as with different credentials of the same user;<br>-Processing of the least amount of personal data possible;<br>-Deletion of unnecessary data. |

[3] The different efficiency types of Computational, Communication, and Storage Efficiency are abbreviated as CCSE.

[4] See respective Functionality column for the different types of issuance.

| | | | | | |
|---|---|---|---|---|---|
| **Presentation** | -CCE[5] for of presentation (proving and verification) for the given presentation features[6] used;<br><br>-Overhead of inspection and revocation on the CCE of presentation;<br><br>-Number of inspectable attributes, number of credentials and pseudonyms to be proven;<br><br>-Use of smart cards and the choice of platform, both soft- and hardware;<br><br>-Chosen security assurance level (cryptographic key size). | -Presentation features supported by the Privacy-ABC technology, such as *key binding*;<br><br>-Support for *predicate proofs* and the *types of predicates supported*;<br><br>-Support for multiple-show unlinkability;<br><br>-Use of dynamic vs. static presentation policies;<br><br>-Support for offline presentation for the User;<br><br>-Potential deployability in smart cards. | -Security assumptions for the given level of the security assurance on the building blocks providing the chosen privacy features;<br><br>-Security assurance on the combination of different building blocks;<br><br>-Security assurance level on the combination of the Privacy-ABC technology, and processing and storage platform (smart card vs. smart phone). | -Costs for technical solution of running and maintaining a Verifier;<br><br>-Costs related to intellectual property (implemented crypto libraries used as building blocks);<br><br>-Potential costs for using services of the Inspector and the Revocation Authority;<br><br>-Cost savings by not processing sensitive identity information about users and avoiding liability issues related to it;<br><br>-Reputation gain by providing a privacy-friendly authentication to the services for the users. | -Guarantees to ensure confidentiality of communication and data storage;<br><br>-Prevention of misuse of personal data;<br><br>-Sufficiency of information provided in the presentation policy (about the purpose of the processing and the processing itself);<br><br>-Prevention of linking different presentation tokens of the same user/credential;<br><br>-Renouncement of tracking mechanisms, such as cookies;<br><br>-Limitation of data storage periods. |

[5] The different efficiency types of Computational and Communication Efficiency are abbreviated as CCE.
[6] See the respective „Functionality“ column for the features.

| | | | | | |
|---|---|---|---|---|---|
| **Inspection** | -CCE of the inspection process;<br>-The number of inspectors, and the platform where the inspection takes place;<br>-Cryptographic key size. | -Support of inspection and inspection type;<br>-Information flow for inspection;<br>-Number of inspectable attributes;<br>-Possibility of the choice of the Inspector by the User. | -Availability of multi-party computation for inspection;<br>-Imposing of *k* out of *n* inspection keys for inspection;<br>-Level of security assurance of the inspection scheme. | -Cost of running and maintaining (technically) the service of Inspector;<br>-Revenue model for inspection;<br>-Reputation gain by acting as a trusted third entity for inspection. | -Security of stored data, in particular of the inspector's secret key;<br>-Correctness of information entailed in the encrypted part of the token;<br>-Possibility to detect forged or altered information:<br>-Sufficiency of the information concerning inspection provided in the consent form;<br>-Enabling of data subjects' right despite the potential of inspection;<br>-Confidentiality of the inspectable part of the presentation token. |
| **Revocation** | -CCE of the revocation process itself and the inherent design of the revocation scheme;<br>-Distribution of the scheme to different entities;<br>-Scalability of the scheme;<br>-Effort distribution between entities;<br>-Information flow between the Revocation Authority and other entities;<br>-Cryptographic key size; | -Type of revocation supported: Issuer (global) vs. Verifier (local) revocation;<br>-Support for user key- vs. attribute revocation;<br>-Protection of user's privacy when proving non-revocation;<br>-Possibility for offline non-revocation proof for the User; | -(Non/) Personalisation of revocation information;<br>-Assurance on the correctness of the revocation information;<br>-Security assumptions / level of security assurance of the revocation scheme;<br>- Security assurance aggregation of Privacy-ABC features related to revocation. | -Cost of running and maintaining a Revocation Authority Service;<br>-Revenue model for providing with revocation-related services (pay-per-revocation, pay-per-non-revocation proof, etc.);<br>-Reputation for acting as a trusted third party for providing revocation services;<br>-Liability and other costs related to providing revocation service;<br>-Costs for the intellectual property issues with the use and/or modification of the chosen Privacy-ABC technology. | -Effectiveness of the revocation process;<br>-Provision of information regarding revocation policy, - process, - result;<br>-Documentation of the respective processes;<br>-Provision of processes for 're-issuance' and 'un-revocation';<br>-Relinquishment of unique identifiers for revoked credentials;<br>-Prevention of abuse of the revocation process. |

# 9. References


[D2.1] Jan Camenisch, Ioannis Krontiris, Anja Lehmann, Gregory Neven, Christian Paquin and Harald Zwingelberg. *D2.1 Architecture for Attribute-based Credential Technologies*, 2011 https://abc4trust.eu/index.php/pub/107-d21architecturev1 (Project deliverable).

[D3.1P1] Jan Camenisch, Stephan Krenn, Anja Lehmann, Gert Læssøe Mikkelsen, Gregory Neven, Michael Østergaard Pedersen. *D3.1 Scientific Comparison of ABC Protocols - Part I – Formal Treatment of Privacy-Enhancing Credential Systems* (Project deliverable), 2014.

[D3.1P2] Fatbardh Veseli, Ahmad Sabouri, Tsvetoslava Vateva- Gurova, Michael Østergaard Pedersen, Jesus Luna. *D3.1 Scientific comparison of ABC protocols – Part II: Practical comparison*, 2014.

[D5.1] Souheil Bcheri, Norbert Götze, Vasiliki Liagkou, Apostolis Pyrgelis, Christoforos Raptopoulos, Yannis Stamatiou, Katalin Storf, Peder Wängmark, and Harald Zwingelberg. *D5.1 Scenario Definition for both Pilots*, 2012. https://abc4trust.eu/index.php/pub/119-d5-1-scenario-definition-for-both-pilots (Project deliverable).

[D6.2] Joerg Abendroth, Souheil Bcheri, Kasper Damgaard, Hamza Ghani, Jesus Luna, Gert Læssøe Mikkelsen, Maxim Moneta, Monika Orski, Neeraj Suri and Harald Zwingelberg. *D6.2 Necessary hardware and software package for the school pilot deployment*, 2013 (In Press).

[D7.2] Kasper Damgaard, Hamza Ghani, Norbert Goetze, Anja Lehmann, Vasiliki Liagkou, Jesus Luna, Gert Læssøe Mikkelsen, Apostolos Pyrgelis, Yannis Stamatiou. *D7.2 Necessary hardware and software package for the student pilot deployment*, 2013 (In Press).

[EC93] Directive 1999/93/ of the European Parliament and the Council on a Community framework for electronic signatures", 1999. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:1999L0093:20081211:EN:PDF.

[EC95] 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. Available online at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

[H3.1P1] Jan Camenisch, Maria Dubovitskaya, Stephan Krenn, Anja Lehmann, Gert Læssøe Mikkelsen, Gregory Neven, Lan Nguyen, Michael Østergaard. "H3.1: Scientific Comparison of ABC Protocols. Part I: Definitions and Cryptographic Building Blocks", October 2013. Project heartbeat (confidential).

[LGS12] Jesus Luna, Hamza Ghani and Neeraj Suri,"Quantitative Assessment of Cloud Security Level Agreements: A Case Study" In Proc. of the International Conference on Security and Cryptography. 2012.

[LGS12b] Jesus Luna, Robert Langenbergand Neeraj Suri, “Benchmarking Cloud Security Level Agreements Using Quantitative Policy Trees” In Proc. of the ACM Cloud Computing Security Workshop. 2012.

[LKS12] J. Luna, I. Krontiris and N. Suri, “Privacy-by-Design Based on Quantitative Threat Modeling” In Proc. of the IEEE International Conference on Risks and Security of Internet and Systems. 2012.

[RosBoc11] Martin Rost, Kirsten Bock, "Privacy By Design und die Neuen Schutzziele – Grundsätze, Ziele und Anforderungen" in Datenschutz und Datensicherheit (DuD) Vol. 35, No. 1, 30–35, 2011, Available online: http://link.springer.com/article/10.1007/s11623-011-0009-y.

[RosPfi09] Martin Rost, Andreas Pfitzmann, "Datenschutz-Schutzziele – revisited", in *Datenschutz und Datensicherheit (DuD*), Vol. 33, No. 12, 353– 358 (2009). Available online: http://link.springer.com/article/10.1007%2Fs11623-009-0072-9.

[ZwiHan12] Harald Zwingelberg, Marit Hansen. Privacy Protection Goals and Their Implications for eID Systems. In *Privacy and Identity Management for Life* – 7th IFIP WG 9.2, 9.6/11.7, 11.4, 11.6 International Summer School Trento, Italy, September 2011. Revised Selected Papers", Springer Boston, 2012. Available online at: http://link.springer.com/chapter/10.1007/978-3-642-31668-5_19.

[VesVat14] Fatbardh Veseli, Tsvetoslava Vateva-Gurova, Ioannis Krontiris, Kai Rannenberg, Neeraj Suri: *Towards a Framework for Benchmarking Privacy-ABC Technologies*. In Cuppens-Boulahia, N., Cuppens, F., Jajodia, S., Abou El Kalam, A., Sans, T., eds.: ICT Systems Security and Privacy Protection. Volume 428 of IFIP Advances in Information and Communication Technology. Springer Berlin Heidelberg (2014) 197–204.

[WP29] Article 29 Data Protection Working Party; *Statement of the Working Party on current discussions regarding the data protection reform package*, Brussels, 27/02/2013.

[RosBoc2010] Rost, Martin/Bock, Kirsten: Privacy by Protection Goals, EuroPriSe Fact Sheet (2010).