Towards a Framework for Benchmarking Privacy-ABC Technologies

Fatbardh Veseli, Tsvetoslava Vateva-Gurova, Ioannis Krontiris, Kai Rannenberg, Neeraj Suri

Towards a Framework for Benchmarking Privacy-ABC Technologies*

Fatbardh Veseli[1], Tsvetoslava Vateva-Gurova[2], Ioannis Krontiris[1], Kai Rannenberg[1], and Neeraj Suri[2]

[1] Chair of M-Business & Multilateral Security, Goethe University Frankfurt, Germany
firstname.lastname@m-chair.de
[2] Department of Computer Science, Technische Universität Darmstadt, Germany
lastname@deeds.informatik.tu-darmstadt.de

Abstract. Technologies based on attribute-based credentials (Privacy-ABC) enable identity management systems that require minimal disclosure of personal information and provide unlinkability of user's transactions. However, underlying characteristics of and differences between Privacy-ABC technologies are currently not well understood. In this paper, we present our efforts in defining a framework for benchmarking Privacy-ABC technologies, and identifying an extensive set of benchmarking criteria and factors impacting such benchmarks. In addition, we identify important challenges in the adoption of Privacy-ABC technologies, indicating directions for future research.

1 Introduction

In the digital world, users are often required to authenticate towards service providers in order to use their services. In many interactions with different service providers, users must disclose personally identifying information in order to use these services, resulting in the loss of control over such information, and a direct impact on their privacy. Privacy-enhancing attribute-based credentials (Privacy-ABCs) enable an identity management system that takes into consideration both the privacy interests of the User, and the security requirements of the Service Providers. They eliminate the need for an active participation of the identity service provider during the authentication of the user, and enable minimal disclosure of personal information for authentication purposes. However, despite existence of implementations of such technologies, such as Microsoft's U-Prove [1] or IBM's Idemix [2], there are additional challenges towards their wider adoption in practice, one of which is the lack of understanding of their differences.

Privacy-ABC technologies are mainly investigated as part of anonymous credential systems. As the underlying technology relies heavily on cryptographic

* The research leading to these results has received funding from the European Communitys Seventh Framework Programme (FP7/2007-2013) under Grant Agreement no. 257782 for the project Attribute-based Credentials for Trust (ABC4Trust).

primitives [3,4], much of the work has been focused on individual aspects, such as efficiency [3,5,6,7,8,9], or support for additional features [10,11]. In addition, there are a number of proposed mechanisms for revocation of anonymous credentials, which also need to be benchmarked. An analysis on revocation schemes for PKI is presented in [12], but it does not take into account the specific aspects of Privacy-ABCs (e.g. privacy features). In this regard, tradeoffs between revocation schemes for anonymous credentials have been analysed in [13,8,9]. From a methodological perspective, elicitation of benchmarking criteria in general is studied also in other areas, e.g. on benchmarking security [14,15,16], although not particularly focusing on Privacy-ABC technologies. However, there is no comprehensive work on benchmarking Privacy-ABC technologies with a broader perspective covering a wider range of aspects.

In this paper, we provide results of an ongoing work towards a framework for benchmarking Privacy-ABC technologies, identifying an extensive set of criteria covering main aspects of Privacy-ABC technologies. We organise these criteria into four main dimensions and identify relevant factors that could influence the benchmarks. We base our work on the unified architecture, concepts and features of Privacy-ABCs [17,18], and build on both the relevant literature on these technologies, as well as experiences during the deployment of these technologies in real-world pilots [19]. Besides for benchmarking Privacy-ABC technologies, this work can also be used as an indicator to the specific challenges and important considerations in their deployment in real life applications.

This paper is organized as follows. First we briefly introduce Privacy-ABC technologies. Then we present the proposed framework for benchmarking these technologies, describing also typical factors that may influence benchmarks. Finally, we conclude the paper with a summary of our results, and a discussion on the potential utility of this work, and give future research directions.

2 Privacy-ABCs - Overview of Features and Concepts

This section gives a very brief introduction on the Privacy-ABC technologies. The interested reader is referred to [18,17], where a comprehensive description of these technologies is provided. Privacy-ABC technologies address the privacy implications of existing identity management schemes, by supporting *selective disclosure* of identity information, and enabling *unlinkability* of user's transactions. Through Privacy-ABCs users can be authenticated without being identified due to the anonymous zero-knowledge proofs support.

The architecture of Privacy-ABCs [18] recognizes the entities: User, Issuer, Verifier, Revocation Authority and Inspector. The *User* is a central entity mainly interacting with the *Issuer* to get Privacy-ABC in an issuance protocol, and with the *Verifier* when accessing services. A Verifier accepts verifiable proofs by the User in forms of *presentation tokens*, and trusts the proofs generated by the credentials of the User, which are issued by the Issuer. Following the Privacy-ABCs architecture [18] and the interactions between the entities [17], we

consider the following stages in the lifecycle of Privacy-ABCs, namely *issuance, presentation, inspection*, and *revocation*.

Issuance. During this initial stage of the lifecycle, an Issuer issues a credential to the User. Privacy-ABC technologies support different forms of issuance, also more "advanced" ones e.g., reflecting the relation of a new credential to an existing one. Examples are "carrying-over attributes" or "key binding".

Presentation. In a presentation protocol the User can prove the possession of credentials and disclose certain information to the Verifier using Privacy-ABC. The Verifier sends a *presentation policy* to the User, specifying the type of proof the User must present. This may include proof of possession of a certain type of credential, disclosure of a subset of attributes, proof of not being revoked, etc., which the User presents in the form of a *presentation token* to the Verifier. Finally, the Verifier can verify the validity of the presented proof.

Inspection. In scenarios where an identity management system aims at conditionally "anonymous" transactions with conditional accountability, Privacy-ABCs support the optional feature of *inspection*, which enables revocation of anonymity in exceptional cases, and is performed by a trusted entity, the Inspector. The fact that a particular presentation token may potentially be subject to inspection in the future should be clearly explained to the User in the presentation policy, along with a strict description of the potential reasons that require inspection to take place.

Revocation. Revocation is the last stage in the lifecycle of Privacy-ABCs, invalidating the credential(s). It is a crucial component of an identitiy management system. The reasons for revocation might be scenario-specific, but revocation is considered normally in cases of misuse, lost or compromised credentials or their storage medium, etc. Responsible for revocation is the Revocation Authority, which maintains the list of (in)valid credentials, and disseminates the latest information on this list to the other entities.

3 Benchmarking Criteria and Impact Factors

We have organised the extensive set of identified benchmarking criteria into four main subsets: *Functionality, Efficiency, Security Assurance,* and *Practical Viability*. Each of these subsets represent a separate benchmarking dimension and contains a list of criteria, organised following the lifecycle of Privacy-ABCs, as presented in Figure 1. Furthermore, we identify typical impact factors for the benchmarks related to given criteria, following a user-centered approach.

3.1 Functionality

The functionality criteria are mostly qualitative and they aim at benchmarking different Privacy-ABC technologies based on their native support for different features, as well as on the additional factors that could be valuable in practice. Table 1 summarizes the list of criteria which could be used for functionality benchmarking, organised following the Privacy-ABC lifecycle approach.

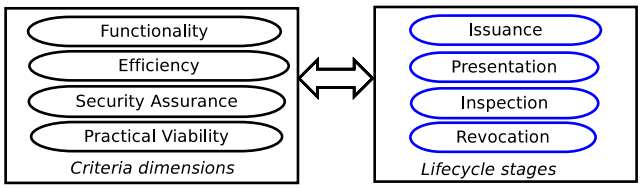

Fig. 1. The organisational structure of the benchmarking criteria

Support for the advanced privacy features of the *issuance* phase, such as "key binding", or "attribute carry-over" (blindly, from another credential), or *presentation* features, such as pseudonymity, (types of) predicates, inspection, or non-revocation proof, provide basic criteria for benchmarking functionality aspects of different Privacy-ABC technologies. For *inspection* it is important to recognize whether the technology provides certain features that would minimise the potential for authority abuse by an Inspector, such as four-eyes principle or requiring k out of n inspectors to be present for inspection. Finally, as *revocation* is usually a challenging aspect of Privacy-ABCs, the support for immediate revocation is a key benchmarking criterion, whereas additional advantage is gained if a revocation scheme enables revocation of the secret key instead of a credential attribute (for instance, to revoke all credentials based on a given key at once).

3.2 Efficiency

Privacy-ABC technologies can be built using different cryptographic building blocks, such as signature schemes, encryption, zero-knowledge proofs, commitments, and revocation schemes. Efficiency has been identified as an important factor for Privacy-ABCs already in previous research [3,5,6,7,8,9,11], as it directly affects the performance of the applications using these technologies, which is a crucial factor for their wider acceptance. In our work, we identify a set of criteria for benchmarking the efficiency, which are mostly quantitative, and organise them in three main aspects, namely into *computational, communication* and *storage* efficiency criteria.

Computational efficiency is expressed in time units (in seconds) required to perform a given operation, whereas **communication efficiency** deals with

Table 1. Functionality benchmarking criteria

Stage	**Functionality Criteria**
Issuance	-Supported advanced issuance features
Presentation	-Unlinkability of multiple presentations
	-Supported advanced presentation features
Inspection	-Support for multi-party inspection
Revocation	-Support for immediate revocation
	-Key- vs. attribute revocation

Table 2. Efficiency benchmarking criteria

Stage	Criteria	Impact Factors
Issuance	-CCE of issuance	-Number of attributes -Use of "advanced" issuance features
Presentation	-CCE of presentation	-Number of credentials proven -Use of advanced presentation features
Inspection	-Overhead on presentation	-Number of inspectable attributes
Revocation	-Overhead on presentation	-Number of revocable credentials
All stages		-Security level (key size)

the data sizes exchanged during different operations. Both efficiency metrics depend on the underlying cryptographic operation that are performed. Table 2 presents the main criteria for benchmarking different Privacy-ABCs on these two metrics, and the most important factors, which influence both of these efficiency aspects along the lifecycle of Privacy-ABCs. The use of advanced features during the *issuance* and *presentation*, such as key binding or (type of) predicates, should impact both efficiency figures, as they incurr additional crypto operations. However, the actual impact on on different Privacy-ABC technologies may vary. On top of that, a significant overhead on the presentation efficiency can be the use of *inspection*, which may also vary depending on the number of inspectable attributes. Finally, *revocation* has a similar overhead on presentation, which may depend on the type of revocation scheme used. Finally, the security level, which corresponds to the cryptographic key length used, has a direct impact on the efficiency of presentation.

Storage efficiency is important, as storage requirements can have impact on the choice of storage medium for the user. Besides the Privacy-ABCs, a number of other information might need to be stored in practice, such as revocation-related information to credentials, pseudonyms, and other static information about other entities (public key of the issuer, revocation authority, inspector). Hence, it is important to benchmark the different storage requirements of different Privacy-ABC technologies, and the factors impacting it.

3.3 Security Assurance

To be able to assess the security assurance provided by a specific Privacy-ABC technology, we propose the usage of security assurance criteria for the different stages of the lifecycle of Privacy-ABCs. The aim of these criteria is to assess the effectiveness of the technology-specific security assurance mechanisms in order to evaluate how the security requirements are met by the respective Privacy-ABC technology. Table 3 presents the security assurance benchmarking criteria we are proposing. As can be seen from the table, security assumptions and security proofs are involved in all the stages of the lifecycle and have to be taken into account. It has to be considered whether the security proofs and assumptions of the issuance protocol and the presentation token, as well as the security proofs and assumptions of the inspection-related and revocation-related mechanisms

Table 3. Security assurance benchmarking criteria

Stage	Criteria
Inspection	-Preventive measures against authority misuse
Revocation	-Mechanisms to guaraantee the authenticity and integrity of RI -Access to the Revocation Handles
All stages	-Security proofs and assumptions

are information theoretic, computational or without security reduction. In case they are computational, the hardness assumptions have to be described. In each of the lifecycle's stages the underlying security proofs and assumptions have to be listed.

In addition, means to assess the security of the conventional mechanisms, which are specifically applied and customized to enhance the security assurance of Privacy-ABCs (e.g. access control mechanisms for the Revocation Information), are necessary; therefore security assurance benchmarks for these mechanisms are to be considered. With regard to Inspection, the security assurance for preventing authority misuse by the person in charge of inspection has to be investigated. It has to be assessed whether the technology supports measures for preventing this, e.g. by applying key sharing mechanisms, where k out of n keys must be combined in order to be able to conduct inspection. Additional security assurance criteria are needed also for the Revocation. The guarantees the the Privacy-ABC technology provides for the protection of integrity and authenticity of the Revocation Information have to be studied and the applied protection mechanisms need to be specified. Moreover, the access restrictions to the Revocation Handles that are posed through the technology have to be analyzed. The different possibilites, e.g. public vs. private access and whether the Revocation Handles are learnt only by the Verfier or also by the Revocation Authority have to be studied.

3.4 Practical Viability

Practical viability benchmarking deals with a group of criteria that may inhibit or enable adoption of Privacy-ABC technologies in the ever-more mobile world. These criteria are listed in Table 4 and relate to the workarounds in overcoming potential lack of support for certain Privacy-ABC features, limiting restrictions on the deployment platforms, or challenges in maintaining privacy in potentially unforeseen application requirements.

Table 4. Benchmarking criteria for practical viability

Stage	Practical Viability Criteria
Issuance	-Reissuance of linkable credentials
Presentation	-Feasibility of smart card deployment
Revocation	-Offline non-revocation proof

Reissuance of linkable credentials. Certain Privacy-ABC technologies do not provide multiple presentations unlinkability. In case this feature is required, a workaround could be to use Privacy-ABCs only one time, requiring re-issuance of such credentials (before every presentation). In order to overcome potential privacy implications, it is possible to automate the process of issuance by issuing a batch of such credentials at once. However, this approach has not only storage implications for the User, but also the usability impact for the fact that the User needs to engage in additional issuance instances with the Issuer (which also may require the User needs to be online).

Feasibility of smart card deployment. Many scenarios where Privacy-ABCs could be deployed, such as new e-IDs or e-tickets, could benefit from the use of smart cards. Except for storing Privacy-ABCs, it may be useful to be able to perform presentation proofs in the card, which can be challenging, considering the computing power of current smart cards. In addition to that, as smart cards are offline devices, Privacy-ABC technologies must enable offline presentations. This factor is important for the wider acceptance and usability of the Privacy-ABC technologies in such scenarios, as also recognized in the the efforts to efficiently implement them on smart cards [5,6,7,13].

Offline non-revocation proof. Proving non-revocation comes challenging for Privacy-ABCs, as this needs to be done without losing privacy. Schemes that support immediate revocation rely on accumulators [11,9], and this typically involves some overhead on the presentation, who needs to provide an additional proof of not being revoked. This makes the presentation less efficient (longer), but also requires periodical connectivity of the User with the Revocation Authority during the presentation in order to refresh the "evidence" that her credentials are not revoked, limiting the deployability of these technologies on devices with network capabilitiy (making them infeasible such as smart cards). A number of studies in this area show the different overhead distribution of revocation (non-revocation proof) on the presentation [13,8], whereas the importance of non-interactive schemes is obviously acknowledged [9].

4 Conclusion

Privacy-ABC technologies enable user-centric, privacy-preserving identity management. This paper summarizes ongoing work in providing a framework for benchmarking Privacy-ABC technologies, enabling a transparent identification of their differences in terms of functionality, efficiency, security assurance, and practical viability. It identifies a number of challenges in the adoption of these technologies in practice, which can also be used to identify open research directions. Next steps in completing the proposed framework include identifying additional factors that could influence the benchmarks and performing actual benchmarks to evaluate the actual impact of these factors on different Privacy-ABC technologies.

References

1. Paquin, C. and Zaverucha, G.: U-prove Cryptographic Specification v1.1 (Revision 2). Technical report, Microsoft Corporation (2013)
2. Bichsel, P., Binding, C., Camenisch, J., Gro, T., Heydt-Benjamin, T., Sommer, D., Zaverucha, G.: Cryptographic Protocols of the Identity Mixer Library. Technical Report RZ 3730 (99740), IBM Research GmbH (2008)
3. Camenisch, J. and Lysyanskaya, A.: A Signature Scheme with Efficient Protocols. In: Proceedings of the 3rd International Conference on Security in Communication Networks, Springer (2003) 268–289
4. Brands, S. A.: Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press (2000)
5. Vullers, P. and Alpar, G.: Efficient Selective Disclosure on Smart Cards Using Idemix. In: IDMAN. Volume 396. Springer (2013) 53–67
6. Mostowski, W. and Vullers, P.: Efficient U-Prove Implementation for Anonymous Credentials on Smart Cards. In: SecureComm. Volume 96. Springer (2011) 243–260
7. Schnorr, C.P.: Efficient signature generation by smart cards. Journal of Cryptology **4** (1991) 161–174
8. Lapon, J., Kohlweiss, M., Decker, B., Naessens, V.: Performance Analysis of Accumulator-Based Revocation Mechanisms. In: SEC. Volume 330. Springer (2010) 289–301
9. Camenisch, J. and Lysyanskaya, A.: Dynamic Accumulators and Application to Efficient Revocation of Anonymous Credentials. In: Advances in Cryptology, Springer (2002) 61–76
10. Belenkiy, M., Chase, M., Kohlweiss, M., Lysyanskaya, A.: P-signatures and Noninteractive Anonymous Credentials. In: Theory of Cryptography. Volume 4948. Springer (2008) 356–374
11. Li, J., Li, N., Xue, R.: Universal accumulators with efficient nonmembership proofs. In: ACNS, Springer (2007)
12. Aarnes, A., Just, M., Knapskog, S., Lloyd, S., Meijer, H.: Selecting Revocation Solutions for PKI (2000)
13. Lapon, J., Kohlweiss, M., Decker, B., Naessens, V.: Analysis of Revocation Strategies for Anonymous Idemix Credentials. In: Communications and Multimedia Security. Volume 7025. Springer (2011) 3–17
14. Luna, J., Langenberg, R., Suri, N.: Benchmarking Cloud Security Level Agreements Using Quantitative Policy Trees. In: CCSW, ACM (2012) 103–112
15. Luna, J., Ghani, H., Vateva, T., Suri, N.: Quantitative Assessment of Cloud Security Level Agreements: A Case Study. In: SECRYPT, SciTePress (2012) 64–73
16. Parrend, P., Frenot, S.: Security benchmarks of OSGi platforms: toward Hardened OSGi. Softw., Pract. Exper. **39**(5) (2009) 471–499
17. Camenisch, J., Dubovitskaya, M., Lehmann, A., Neven, G., Paquin, C., Preiss, F.: Concepts and Languages for Privacy-Preserving Attribute-Based Authentication. In: IDMAN. Volume 396. Springer (2013) 34–52
18. Camenisch, J., Krontiris, I., Lehmann, A., Neven, G., Paquin, C., Rannenberg, K., Zwingelberg, H.: D2.1 Architecture for Attribute-based Credential Technologies - Version 1. *ABC4TRUST* - Deliverable to the European Commision (2011) https://abc4trust.eu/index.php/pub.
19. ABC4Trust: Abc4trust pilots. https://abc4trust.eu/index.php/home/pilots/. Last accessed on 14.12.13.