Trust Relationships in Privacy-ABCs' Ecosystems

Ahmad Sabouri, Ioannis Krontiris, Kai Rannenberg

Goethe University Frankfurt, Deutsche Telekom Chair of Mobile Business & Multilateral Security,
Grueneburgplatz 1, 60323 Frankfurt, Germany
{ahmad.sabouri, ioannis.krontiris, kai.rannenberg}@m-chair.de

Abstract.— Privacy Preserving Attribute-based Credentials (Privacy-ABCs) are elegant techniques to offer strong authentication and a high level of security to the service providers, while users' privacy is preserved. Users can obtain certified attributes in the form of Privacy-ABCs, and later derive unlinkable tokens that only reveal the necessary subset of information needed by the service providers. Therefore, Privacy-ABCs open a new way towards privacy-friendly identity management systems. In this regards, considerable effort has been made to analyse Privacy-ABCs , design a generic architecture model, and verify it in pilot environments within the ABC4Trust EU project. However, before the technology adopters try to deploy such an architecture, they would need to have a clear understanding of the required trust relationships.

In this paper, we focus on identifying the trust relationships between the involved entities in Privacy-ABCs' ecosystems and provide a concrete answer to "*who needs to trust whom on what?*" In summary, nineteen trust relationships were identified, from which three of them considered to be generic trust in the correctness of the design, implementation and initialization of the crypto algorithms and the protocols. Moreover, our findings show that only six of the identified trust relationships are extra requirements compared with the case of passport documents as an example for traditional certificates.

Keywords: Privacy Preserving Attribute-based Credentials, Trust Relationships

1 Introduction

Trust is a critical component of any identity system. Several incidents in the past have demonstrated the existence of possible harm that can arise from misuse of people's personal information. Giving credible and provable reassurances to people is required to build trust and make people feel secure to use the electronic services offered by companies or governments on-line.

Indeed, organizations that have built trust relationships to exchange digital identity information in a safe manner preserve the integrity and confidentiality of the user's personal information. However, when it comes to privacy, typical identity management systems fail to provide these strong reassurances. For example, in these systems, the so-called "Identity Provider" is able to trace and

link all communications and transactions of the users and compile dossiers for each individual about his or her habits, behaviour, movements, preferences, characteristics, and so on. There are also many scenarios where the use of certificates unnecessarily reveals the identity of their holder, for instance scenarios where a service platform only needs to verify the age of a user but not his/her actual identity.

Strong cryptographic protocols can be used to increase trust, by not letting such privacy violations be technically possible. Over the past years, a number of technologies have been developed to build Privacy Preserving Attribute-based Credentials (Privacy-ABCs) in a way that they can be trusted, like normal cryptographic certificates, while at the same time they protect the privacy of their holder. Such Privacy-ABCs are issued just like ordinary cryptographic credentials (e.g., X.509 credentials) using a digital secret signature key. However, Privacy-ABCs allow their holder to transform them into a new token, in such a way that the privacy of the user is protected.

As prominent instantiations of such Privacy-ABC technologies one could mention Microsoft's U-Prove [2] and IBM's Idemix [3]. Both of these systems are studied in depth by the EU project ABC4Trust [1], where their differences are abstracted away to build a common architecture for Privacy-ABCs and tested in real-world, large-scale user trials. A privacy-threat analysis that we performed on the implementation of one of the pilot scenarios [4], we showed that indeed the use of Privacy-ABCs has helped mitigate many serious threats to user's privacy. However, some risks still remain, which are not addressed by Privacy-ABCs, requiring some degree of trust between the involved entities.

In this work, we focus on identifying the trust relationships between the involved entities in Privacy-ABCs' ecosystems and provide a concrete answer to "*who needs to trust whom on what?*". The rest of the paper is organized as follows: In Section 2, we elaborate on the definition of *Trust*, which we considered in this paper. Section 3 provides a brief overview of the related work in the area of identity management and trust relationships. Later in Section 4, we introduce the entities involved in the life-cycle of Privacy-ABCs and their interactions. Section 5 describes the required trust relationships from the perspective of each entity introduced in Section 4. Then, in Section 6, we compare the complexity of the systems based on Privacy-ABCs with the traditional systems in terms of the required trust relationships. In the end, we conclude the discussion in Section 7.

2 The Concept of Trust

A wide variety of definitions of trust exist in the bibliography [5][6]. A comprehensive study of the concept has been presented in the work by McKnight and Chervany [7], where the authors provide a classification system for different aspects of trust. In their work, they define trust intention as *"the extent to which one party is willing to depend on the other party in a given situation with a feeling of relative security, even though negative consequences are possible."* [7]

Their definition embodies (a) the prospect of negative consequences in case the trusted party does not behave as expected, (b) the dependence on the trusted party, (c) the feeling of security and the (d) situation-specific nature of trust. So, trust intention shows the willingness to trust a given party in a given context, and implies that the trusting entity has made a decision about the various risks of allowing this trust.

3 Related Work

Jøsang et al. [8] analyse some of the trust requirements in several existing identity management models. They consider the federated identity management model, as well as the isolated or the centralized identity management model and they focus on the trust requirements of the users in the service and identity service providers, but also between the identity service providers and service providers. However, this work does not cover the case of identity management based on Privacy-ABCs.

Delessy et al. [9] define the Circle of Trust pattern, which represents a federation of service providers that share trust relationships. The focus of their work however lays more on the architectural and behavioural aspects, rather than on the trust requirements which must be met to establish a relationship between two entities.

Later, Kylau et al. [10] concentrated explicitly on the federated identity management model and identify possible trust patterns and the associated trust requirements based on a risk analysis. The authors extend their scenarios by considering also scenarios with multiple federations.

To the best of our knowledge, there is no work that discusses systematically the trust relationships in identity management systems that incorporate Privacy-ABCs. However, some steps have been done in systematisation of threat analysis in such schemes, by the establishments of a quantitative threat modelling methodology that can be used to identify privacy-related risks on Privacy-ABC systems [4]. We perform our trust relationship analysis based on the risks identified by applying this methodology.

4 Privacy Preserving Attribute-based Credentials' Life-Cycle

Figure 1 shows the entities that are involved during the life-cycle of Privacy-ABCs [11]. The core entities are the User, the Issuer and the Verifier, while the Revocation Authority and the Inspector are optional entities. The User interacts with the Issuer and gets credentials, which later presents to the Verifiers in order to access their services. The User has the control of which information from which credentials she presents to which Verifier. The human User is represented by her UserAgent, a software component running either on a local device (e.g., on the User's computer or mobile phone) or remotely on a trusted cloud service. In

addition, the User may also possess special hardware tokens, like smart cards, to which credentials can be bound to improve security.

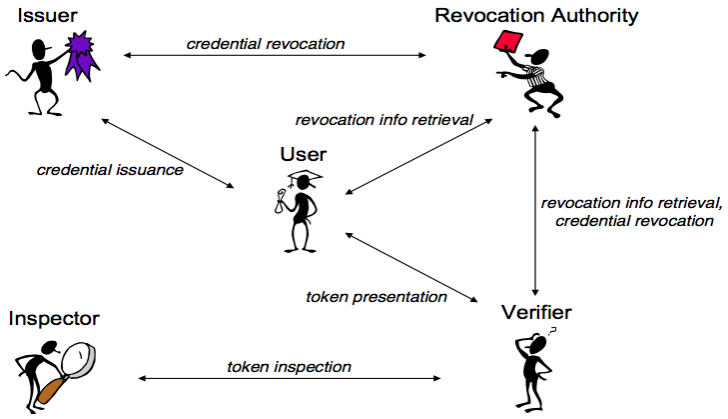

Fig. 1. Entities and relations in the Privacy-ABC's architecture [11]

A Verifier is posing restrictions for the access to the resources and services that it offers. These restrictions are described in a presentation policy and specify which credentials Users must own and which attributes from these credentials they must present in order to access the service. The User generates from her credentials a presentation token, which corresponds to the Verifier's presentation policy and contains the required information and the supporting cryptographic evidence.

The Revocation Authority is responsible for revoking issued credentials. Both the User and the Verifier must obtain the most recent revocation information from the Revocation Authority to generate presentation tokens and respectively, verify them. The Inspector is an entity who can de-anonymize presentation tokens under specific circumstances. To make use of this feature, the Verifier must specify in the presentation policy the conditions, i.e., which Inspector should be able to recover which attribute(s) and under which circumstances. The User is informed about the de-anonymization options at the time that the presentation token is generated and she has to be involved actively to make this possible. In an actual deployment, some of the above roles may actually be fulfilled by the same entity or split among many. For example, an Issuer can at the same time play the role of Revocation Authority and/or Inspector, or an Issuer could later also be the Verifier of tokens derived from credentials that it issued [11].

5 Trust Relationships

In order to provide a comprehensible overview of the trust relationships, we describe the trust requirements from each entity's perspective. Therefore, whoever

likes to realise one of the roles in the Privacy-ABCs' ecosystem could easily refer to that entity and learn about the necessary trust relationships that need to be established. Figure 2 depicts an overview of the identified trust relationships between the involved parties. On the bottom of Figure 2, the general trust requirements by all the parties are demonstrated.

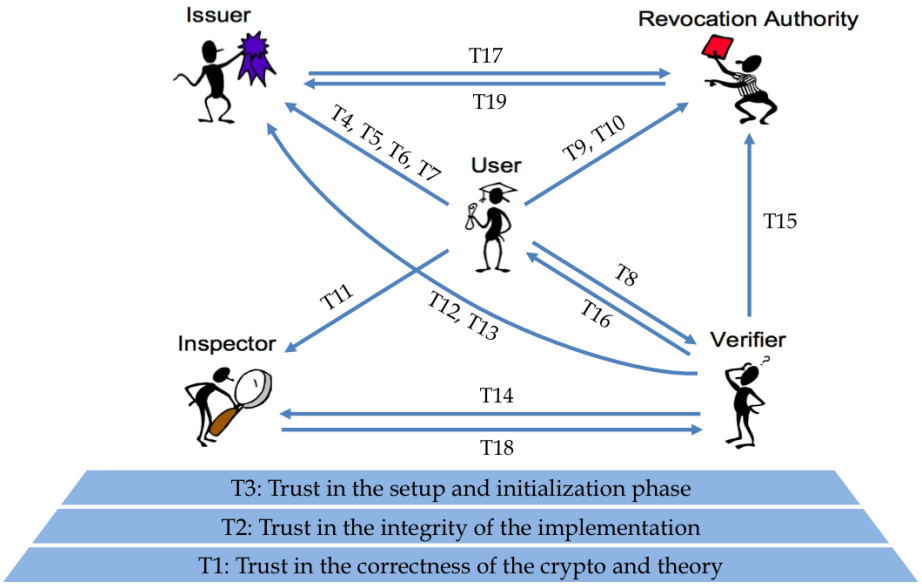

Fig. 2. Visualization of the trust relationships

5.1 Assumptions

Before delving into the trust relationships, it is important to elaborate on the assumptions that are required for Privacy-ABCs to work. Privacy-ABCs are not effective in cases where tracking and profiling methods that work based on network level identifiers such as IP addresses or the ones in the lower levels. Therefore, in order to benefit from the full set of features offered by Privacy-ABCs, the underlying infrastructure must be privacy-friendly as well. The recommendation for the users would be to employ network anonymizer tools to cope with this issue.

Another important assumption concerns the verifiers' enthusiasm for collecting data. Theoretically, greedy verifiers have the chance to demand for any kind of information they are interested in and avoid offering the service if the user is not willing to disclose this information. Therefore, the assumption is that the verifiers reduce the amount of requested information to the minimum level possible either by regulation or any other mechanism in place.

5.2 Trust by all the parties

Independent from their roles, all the involved parties need to consider a set of fundamental trust assumptions that relates to design, implementation and setup of the underlying technologies. The most fundamental trust assumption by all the involved parties concerns the theory behind the actual technologies utilized underneath. Everybody needs to accept that in case of a proper implementation and deployment, the cryptographic protocols will offer the functionalities and the features that they claim.

T1. *All the involved parties need to put trust in the correctness of the underlying cryptographic protocols.*

Even a protocol that is formally proven to be privacy preserving does not operate appropriately when the implementation is flawed. Consequently, the realization of the corresponding cryptographic protocol and the related components must be trustworthy. For example, the Users need to trust the implementation of the so-called UserAgent and the smart card application meaning that they must rely on the assertion that the provided hardware and software components do not misbehave in any way and under any circumstances, which might jeopardise the User's privacy.

T2. *All the involved parties need to put trust in the trustworthiness of the implemented platform and the integrity of the defined operations on each party.*

A correct implementation of privacy preserving technologies cannot be trustworthy when the initialization phase has been compromised. For example, some cryptographic parameters need to be generated in a certain way in order to guaranty the privacy preserving features of a given technology. A diversion in the initialization process might introduce vulnerabilities to the future operation of the users.

T3. *All the involved parties need to put trust in the trustworthiness of the system setup and the initialization process.*

5.3 Users' Perspective

In typical scenarios, verifiers grant access to some services based on the credentials that the users hold. A malicious issuer can trouble a user and cause denial of service by not providing credible credentials in time or deliberately embedding invalid information in the credentials. For example, in case of a voting scenario, the issuer of ballots can block some specific group of users with fake technical failures of the issuance service.

T4. *The users need to put trust in the issuers delivering accurate and correct credentials in a timely manner.*

When designing a credential, the issuer must heed that the structure of the attributes and the credential will not impair the principle of minimal disclosure. For example, embracing name and birth date in another attribute such as registration ID is not an appropriate decision since presenting the latter to any verifier results in undesirable disclosure of data.

T5. *The users need to trust that the issuers design the credentials in an appropriate manner, so that the credential content does not introduce any privacy risk itself.*

Similar to any other electronic certification system, dishonest issuers have the possibility to block a user from accessing a service without any legitimate reason by revoking her credentials. Therefore the users have to trust that the issuer has no interest in disrupting users activities and will not take any action in this regard as long as the terms of agreement are respected.

T6. *The users need to trust that the issuers do not take any action to block the use of credentials as long as the user complies with the agreements.*

It is conceivable that a user loses control over her credentials and therefore contacts the issuer requesting for revocation of that credentials. If the issuer delays processing the user's request the lost or stolen credentials can be misused to harm the owner.

T7. *The users need to trust that the issuers will promptly react and inform the revocation authorities when the users claim losing control over their credentials.*

One of the possible authentication levels using Privacy-ABCs is based on a so-called *scope-exclusive pseudonym* where the verifier is able to impact the generation of pseudonyms by the users and limit the number of partial identities that a user can obtain in a specific context. For example, in case of an online course evaluation system, the students should not be able to appear under different identities and submit multiple feedbacks even though they are accessing the system pseudonymously. In this case, the verifier imposes a specific *scope* to the pseudonym generation process so that every time a user tries to access the system, it has no choice other than showing up with the same pseudonym as the previous time in this context. In this situations a dishonest verifier can try to unveil the identity of a user in a pseudonymous context or correlate actives by imposing the "same" scope identifier in generation of pseudonyms in another context where the users are known to the system.

T8. *The users need to trust that the verifiers do not misbehave in defining policies in order to cross-link different domains of activities.*

If a revocation process exists in the deployment model the user needs to trust on the correct and reliable performance of the revocation authority. Delivering illegitimate information or hindrance to provide genuine data can disrupt granting user access to her desired services.

T9. *The users need to trust that the revocation authorities perform honestly and do not take any step towards blocking a user without legitimate grounds.*

Depending on the revocation mechanism, the user might need to show up with her identifier to the revocation authority in order to obtain the non-revocation evidence of her credentials for an upcoming transaction. If the revocation authority and the verifier collude, they might try to correlate the access timestamps and therefore discover the identity of the user who requested a service.

T10. *The users need to trust that the revocation authorities do not take any step towards collusion with the verifiers in order to profile the users.*

Embedding encrypted identifying information within an authentication token for inspection purposes makes the users dependent of the trustworthiness of the inspector. As soon as the token is submitted to the verifier, the inspector is able to lift the anonymity of the user and disclose her identity. Therefore the role of inspector must be taken by an entity that a user has established trust relationship with.

T11. *The users need to trust that the inspectors do not disclose their identities without making sure that the inspection grounds hold.*

5.4 Verifiers' Perspective

Provisioning of the users in the ecosystem is one of the major points where the verifiers have to trust the issuers to precisely check upon the attributes that they are attesting. The verifiers rely on the information that is certified by the issuers for the authentication phase so the issuers assumed to be trustful.

T12. *The verifiers need to trust that the issuers are diligent and meticulous when evaluating and attesting the users' attributes.*

When a user loses her credibility, it is the issuer's responsibility to take the appropriate action in order to block the further use of the respective credentials. Therefore, the verifiers rely on the issuers to immediately request revocation of the user's credentials when a user is not entitled anymore.

T13. *The verifiers need to trust that the issuers will promptly react to inform the revocation authorities when a credential loses its validity.*

In an authentication scenario where inspection is enabled, the only party who is able to identify a misbehaving user is the inspector. The verifier is not able to deal with the case if the inspector does not to cooperate. Therefore, similar to trust relationship T11 by the users, the verifiers dependent of the fairness and honesty of the inspector.

T14. *The verifiers need to trust that the inspectors fulfil their commitments and will investigate the reported cases fairly and deliver the identifiable information in case of verified circumstances.*

The validity of credentials without expiration information is checked through the information that the verifier acquires from the revocation authority. A compromised revocation authority can deliver outdated or illegitimate information to enable a user to get access to resources even with revoked credentials. Therefore the revocation authority needs to be a trusted entity from the verifiers' perspective.

T15. *The verifiers need to trust that the revocation authorities perform honestly and deliver the latest genuine information to the verifiers.*

Often user credentials are designed for individual use, and sharing is not allowed., Even though security measures such as hardware tokens can be employed to support this policy limit the usage of the credentials to the owners, the users can still share the tokens and let others benefit from services that they are not normally eligible for. The verifiers have no choice than trusting the users and the infrastructure on this matter.

T16. *The verifiers need to trust that the users do not share their credentials with the others, if this would be against the policy.*

5.5 Issuers' Perspective

As mentioned earlier T13, the issuer is responsible to take the appropriate steps to block further use of a credential when it loses its validity. The issuer has to initiates the revocation process with the revocation authority and trust that the revocation authority promptly reacts to it in order to disseminate the revocation status of the credential. A compromised revocation authority can delay or ignore this process to let the user benefit from existing services.

T17. *The Issuers need to trust that the revocation authorities perform honestly and react to the revocation requests promptly and without any delay.*

5.6 Inspectors' Perspective

In order to have a fair inspection process, the inspection grounds must be precisely and clearly communicated to the users in advance. In case of an inspection request, the inspector has to rely on the verifier that the users had been informed about these conditions properly.

T18. *The Inspector need to trust that the verifier has properly informed the users about the actual circumstances that entitle the verifier for de-anonymisation of the users.*

5.7 Revocation Authorities' Perspective

Revocation authorities are in charge of delivering up-to-date information about the credentials' revocation status to the users and the verifiers. However, they are not in a position to decide whether a credential must be revoked or not, without receiving revocation requests from the issuers. Therefore, their correct operations depends on the diligent performance of the issuers.

T19. *In order to provide reliable service, the revocation authorities need to trust that the issuers deliver legitimate and timely information of the revoked credentials.*

6 Added Complexity

In order to better illustrate the added complexity compared to the traditional authentication schemes without Privacy-ABCs, we analysed the case of passport documents to find out about the overhead for enhancing privacy in terms of trust relationships. In our analysis, we exclude the first three trust relationships (T1, T2, and T3) since they concern the theoretical and operational correctness of the crypto and the protocols.

From the rest, T11, T14 and T18 do not exist in the case of passport documents, as there is no *Inspector* role involved. Interestingly, there are only three more trust relationships that do not hold for passport documents and all of them are from the users' perspective. T5, T8 and T10 focus on the problem of privacy and profiling, thus they are not applicable for passports. Investigating the remaining 10 trust relationships, we concluded that all of them are valid for the passport document scenarios. As a result, the added complexity due to the privacy requirements is 6 trust relationships out of 16.

7 Conclusion

Privacy-ABCs are powerful techniques to cope with security and privacy requirements at the same time. Extensive research has been conducted to understand Privacy-ABCs and bring them into practice[12][13][1]. In order to deploy Privacy-ABCs in real application scenarios, a clear understanding of the trust relationships between the involved entities is unavoidable. In this work, we investigated the questions of "*who needs to trust whom on what?*" and introduced the necessary trust relationships between the architectural entities of the Privacy-ABCs' ecosystems. However, a particular application might potentially introduce further trust dependencies, and therefore, the proposed list might get extended.

In summary, nineteen trust relationships were identified, from which three of them considered to be generic trust in the correctness of the design, implementation and initialization of the crypto algorithms and the protocols. Furthermore, it turned out that the credential "Issuer" is the entity that has to be trusted the most and the "User" is the one who is putting the most trust in the others' correct performance. Comparing the trust relationships to the case of passport documents, as an example for traditional certificates, we identified six of them to be the additional requirements introduced by Privacy-ABCs.

8 Acknowledgements

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

References

1. "Attribute-based Crednetials for Trust (ABC4Trust) EU Project," https://abc4trust.eu/.
2. "Microsoft U-Prove," http://www.microsoft.com/uprove.
3. "Identity Mixer," http://idemix.wordpress.com/.
4. J. Luna, N. Suri, and I. Krontiris, "Privacy-by-design based on quantitative threat modeling," in *Risk and Security of Internet and Systems (CRiSIS), 2012 7th International Conference on*. IEEE, 2012, pp. 1–8.
5. R. Hardin, *Trust and trustworthiness*. Russell Sage Foundation, 2004, vol. 4.
6. K. O'Hara, *Trust: From Socrates to Spin*. Icon Books Ltd, 2004.
7. D. H. Mcknight and N. L. Chervany, "The meanings of trust," Tech. Rep., 1996.
8. A. Josang and S. L. Presti, "Analysing the relationship between risk and trust," in *Second International Conference on Trust Management (iTrust 2004)*, C. Jensen, S. Poslad, and T. Dimitrakos, Eds., vol. LNCS 2. Springer, 2004, pp. 135–145, event Dates: March 29 - April 1st 2004. [Online]. Available: http://eprints.soton.ac.uk/258769/
9. N. Delessy, E. B. Fernandez, and M. M. Larrondo-Petrie, "A pattern language for identity management," in *Proceedings of the International Multi-Conference on Computing in the Global Information Technology*, ser. ICCGI '07. Washington, DC, USA: IEEE Computer Society, 2007, pp. 31–. [Online]. Available: http://dx.doi.org/10.1109/ICCGI.2007.5
10. U. Kylau, I. Thomas, M. Menzel, and C. Meinel, "Trust requirements in identity federation topologies," in *Proceedings of the 2009 International Conference on Advanced Information Networking and Applications*, ser. AINA '09. Washington, DC, USA: IEEE Computer Society, 2009, pp. 137–145. [Online]. Available: http://dx.doi.org/10.1109/AINA.2009.80
11. "D2.1 Architecture for Attribute-based Credential Technologies Version 1," https://abc4trust.eu/download/ABC4Trust-D2.1-Architecture-V1.pdf.
12. "PRIME - Privacy and Identity Management for Europe," https://www.prime-project.eu/.
13. "PrimeLife EU Project," http://primelife.ercim.eu/.