Attribute-based Credentials for Trust (ABC4Trust)

Ahmad Sabouri, Ioannis Krontiris, and 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.net
https://www.abc4trust.eu

The rapid growth of communication infrastructures and enterprise software solutions has caused electronic services to penetrate into our everyday life. So it is not far from reality that many personal and trust-sensitive transactions happen online. In this regard, one of the biggest challenges to deal with will be proper user authentication and access control, as strong authentication and authorization techniques used nowadays are double-edged swords: while they can protect service providers by offering a satisfactory level of resilience against unauthorized accesses, most of these technologies have the drawback of threatening the clients' privacy.

As an example, X.509 certificates, which are one of the most common strong authentication mechanisms, contain a list of attributes of users attested and digitally signed by a trusted issuer in the domain. The static representation of these certificates makes it possible to trace users' online activities and link their various transactions . Furthermore, due to the nature of these certificates, the signature cannot be verified if a single modification occurs in the issued certificates. As a result, there is no choice for the users other than revealing all the attested attributes in their transactions even though some of them are not needed. Online techniques like SAML, OpenID, or WS-Federation can overcome this problem and offer selective disclosure of attributes, but they still suffer from other privacy breaches such as enabling the respective identity service provider to track the user's online transactions.

Privacy Preserving Attribute-Based Credentials (Privacy-ABCs) are elegant techniques to cope with these problems. They can 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. However, inspite of the powerful features Privacy-ABCs provide, the diversity of the cryptographic schemes used in different existing implementations has so far hindered a satisfactory level of adoption.

The EC funded project Attribute-based Credentials for Trust (ABC4Trust) aims to bring all the common features of the existing Privacy-ABC technologies together under the same hood and provide a framework abstracted from the concrete cryptographic realization of the modules underneath. This gives software developers the flexibility to build Privacy-ABC enabled systems without

any concern about what cryptographic schemes will be employed at the bottom layer. As a direct result, the service providers are free to choose from those concrete cryptographic libraries that implement the ABC4Trust required interfaces, and plug them into their software solutions. This helps to avoid a lock-in with a specific technology, as the threat of a lock-in reduces the trust into an infrastructure.

The interchangeability of Privacy-ABC techniques in ABC4Trust framework is the outcome of its layered architecture design. Figure 1 depicts a cropped view of the high level ABC4Trust architecture where two of the main actors, namely User and Verifier, interact in a typical service request scenario. The core of the architecture is called ABCE (ABC Engine) layer; it provides the necessary APIs to the application layer residing on the top and utilizes the interfaces offered by the bottom layer called CE (Crypto Engine). To complete the picture an XML-based language framework has been designed so that ABCE peers from different entities of the system, e.g. the User and the Verifier, can communicate in a technology-agnostic manner. Putting all the pieces together, the application layer follows the corresponding steps defined in the protocol specification [1], calls the appropriate ABCE APIs, and exchanges the given messages with the other parties. Further down in the layers, upon receiving an API call, the ABCE performs technology-agnostic operations, such as matching the given access policy with the user's credentials, interacting with the user in case it is needed, and invoking crypto APIs from the CE in order to accomplish cryptographic operations. Finally the bottom layer CE is where the different realizations of Privacy-ABC technologies appear and provide their implementations for the required features.

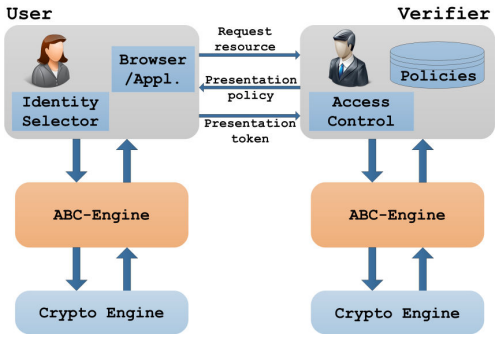

Fig. 1. ABC4Trust layerd architecture, User-Verifier interaction

References

1. Ioannis Krontiris (ed.), *D2.1 Architecture for Attribute-based Credential Technologies Version 1,*Available at ABC4Trust project website.