ABC4Trust

Attribute-based Credentials for Trust

The EC-funded project Attribute-based Credentials for Trust (ABC4Trust) deepened the understanding in attribute-based credentials as an identity management technology. The project enabled their efficient and effective deployment in practice and fostered their federation in different domains.

Project Description

Almost all applications and services based on computer systems require some authentication of participants to establish trust relations. Given the weakness of simple authentication methods like password-based authentication, multiple alternate techniques have been developed to provide a higher degree of security. Cryptographic certificates are one known example of this. Although such certificates offer sufficient security for many purposes, they cannot be regarded as privacy-friendly.

Any usage of such a certificate may expose a lot of identity information of the holder to the party requesting the authentication, but there are various scenarios where the user of such certificates unnecessarily reveals more information than needed. For example, if proof is required that the user is of a given age or student of a university, neither the identity nor the exact birth date needs to be known to the other party. Revealing more information than is necessary not only harms the privacy of the users, but also increases the risk of information abuse, like identity fraud, and enables linkability of the usages. Furthermore, processing more data than is necessary violates the principles established within the EU Data Protection Directive 95/46/EC.

ABC4Trust addresses the federation and "interchangeability" of technologies that support trustworthy, privacy-preserving Attribute-based Credentials (Privacy-ABCs). Privacy-ABCs allow holders to reveal and prove just the minimal information required by the application, without disclosing their complete identity. Additionally, their holder can transform them into a presentation token providing only a subset of attribute values stored in the original credential while preserving a valid signature. Thus these credentials foster a trustworthy and at the same time privacy-protecting solution for the information society.

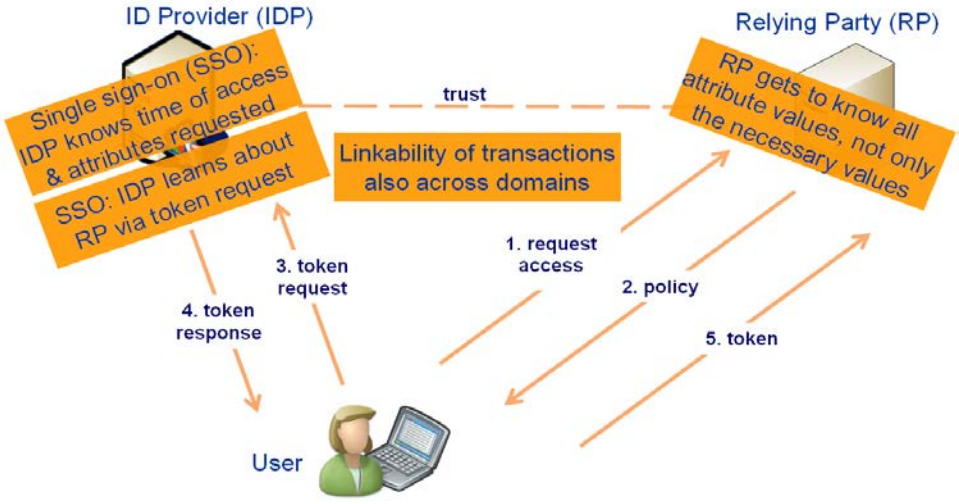

Figure 1: "Privacy issues of classical authentication and single sign-on

Project Objectives

The objectives of ABC4Trust were:

- To define a common, unified architecture for Privacy-ABC systems to allow comparing their respective features and combining them on common platforms; and
- To deliver open reference implementation of selected Privacy-ABC systems by deploying them in the project's pilots to support provably accredited members of restricted communities in order to either interact with one another or evaluate their courses.

The results of the project will enable stakeholders to better understand privacy-preserving ABC technologies and to compare the relative merits of different technologies in different scenarios. ABC4Trust conducted trials deploying attribute-based credentials at a Greek university and a Swedish secondary school. For this, ABC4Trust deployed the pre-existing ABC technologies by IBM (Identity Mixer) and Microsoft (U-Prove).

Privacy Risks of Existing Federated Identity Management Architectures

Using certificates in typical federated identity management (IdM) architectures poses several risks to the user's privacy (see Figure 1). Classical certificates, as they are commonly used within X.509 architectures, cannot be changed without invalidating the issuer's signature. This makes it impossible to strip off unnecessary personal information before presentation and forces users to reveal more data than is actually needed for the respective purpose.

Some federated IdM architectures, such as single sign-on (SSO), require a communication of the user with the ID provider (IDP) as part of each authentication. This unintentionally reveals profiles of communication habits.

Whenever the token request also contains information about the relying party (RP), interest profiles of the user can be aggregated. Even worse, from a privacy perspective, are setups where the RP directly communicates with the IDP, like payment systems with real-time account balance verification.

ABC4Trust Pilots

ABC4Trust conducted the following pilot trials:

Protecting the privacy of children in a school environment in Sweden involved pseudonymous community access and social networking for pupils. This trial dealt with online communication between pupils, parents and school personnel. The system provided safe, yet verifiable means for the exchange of sensitive personal information where pupils were able to seek advice from pedagogical staff inter alia on intimate questions related to physical, psychological or social situations without revealing their true identity. They were also able to more freely communicate in Restricted Areas where various levels of access could be granted, for example, only to pupils of a certain age, grade and/or sex are allowed to join. This part of the trial benefited from the advantages of the Privacy-ABC technology by allowing anonymous proofs of attribute values.

Course Evaluation within Universities was the second trial of the project. It comprised the provision of credentials to the students of a Greek university that certified a number of attributes to the students, like: year of study, major, attended lectures, etc. Eligible students were able to anonymously provide feedback regarding

courses and teachers they had during a semester by using proper credentials.

By taking into account the collection of criteria and the implementation of necessary infrastructure the evaluation of these pilots provided a clear proof of concept of both the unified attribute-based credentials approach as well as the reference architecture with feedback for enhancements.

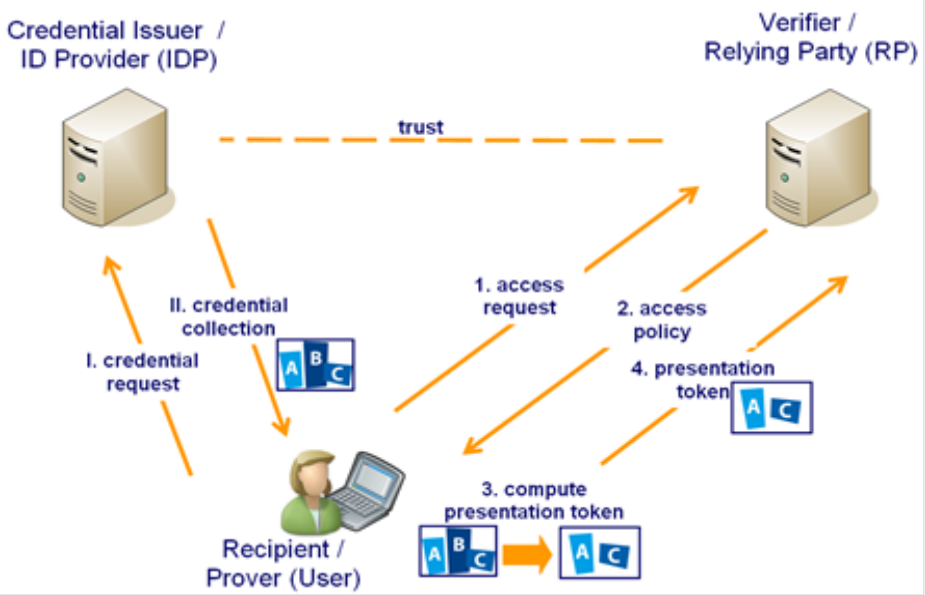

Figure 2:
"Workflow of an authentication deploying Attribute-based Credentials"

Privacy Potential of Attribute-based Credentials

Due to their design, Privacy-ABCs and the underlying cryptographic mechanisms are designated for building privacy-enhancing technologies. The aforementioned ABC4Trust pilots utilised the technology for authentication by Privacy-ABCs.

The operation of Privacy-ABCs illustrated below demonstrates the potential for privacy-enhancing authentication. Privacy-ABC technology eliminates the risks identified in classical IdM infrastructures while preserving the advantages of federated IdM architectures. Figure 2 illustrates the parties and processes involved within a typical authentication deploying Privacy-ABCs.

Parties in a basic ABC infrastructure

The IDP issues the credentials which attest attribute values of the user; this is why the IDP is referred to as "issuer" within the Privacy-ABC setup. Usually this requires that the user is known to the IDP and that the IDP is able to acknowledge certain attribute values of the user. A university acting as an IDP could, for example, confirm that a given user is member of the university or studies a particular discipline on a given level such as student or PhD candidate.

The user is the entity that receives the credential from the IDP to prove certain attribute values towards the RP. When applying Privacy-ABC terminology, the user holds the roles of a "recipient (of credentials)" and a "prover (of a claim)".

The user can use those certificates to obtain resources from the RP. The RP takes the role of a "verifier" and gets a presentation token that allows it to verify whether its policy is satisfied by the user. The presentation token, in the Privacy-ABC context, is a transformed credential that reveals only as much information as necessary.

Workflow of a Privacy-ABC Authentication

Foremost, credentials need to be obtained from the IDP by a request (I) and the subsequent collection of the credentials (II). This step needs to be done only once. Collected credentials are stored and managed on the client side under control of the user. Consequently, the IDP may be offline or unreachable for one or both parties during subsequent authentication processes.

Whenever the user wants to access a restricted resource residing with a RP, she will request access to this resource (1). The server of the RP answers by providing the access policy for the requested resource (2). Such a policy might refer to any attribute, like the user's name, being of a certain age, member of a university, etc. The client aids the user by computing a presentation token satisfying the access policy (3). This step may include stripping off personal data not required by the policy. The resulting presentation token is then presented towards the RP for cryptographic verification of the claimed attribute values (4).

Project reference:
257782

Project duration:
November 2010 – February 2015

Partners:
12 partners from industry, academia, research centres and data protection authorities

Costs:
€ 13.59 Million (€ 8.85 Million EU funded)

Funding:
The ABC4Trust project receives research funding from the European Union's Seventh Framework Programme under grant agreement n° 257782 as part of the "ICT Trust and Security Research" theme.

Project coordination:
Prof. Dr. Kai Rannenberg
Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt am Main
Grüneburgplatz 1
60629 Frankfurt am Main
Germany
contact@abc4trust.eu

Contact:
Marit Hansen
t: +49 431 988 1214
f: +49 431 988 1223
press@abc4trust.eu

Version and date of publication:
Version 2.1, January 2015

Want more info?
www.abc4trust.eu

SEVENTH FRAMEWORK PROGRAMME

ABC4TRUST