ABC4Trust

ABC4Trust Architecture for Privacy-ABCs

The EC-funded project Attribute-based Credentials for Trust (ABC4Trust) has specified an architecture and a reference implementation for working with privacy-enhanced attribute-based credentials (Privacy-ABCs).

Overview

The user first obtains credentials, certified attribute-value pairs, from an issuer who vouches for the correctness of the certified attributes. The user can subsequently authenticate towards a verifier by sending a presentation token, which is derived from her credentials. A single presentation token can selectively reveal attribute values from one or more credentials. It can also prove that a given predicate holds, without revealing the full attributes' values. E.g., that the date of birth is before January 1st, 1994, or that the name on the user's credit card matches that on her driver's license.

For an easy integration of Privacy-ABCs in various applications and systems, we consider a mechanism-independent ABC Engine layer on top of the core Cryptographic Engines. This ABC Engine layer contains all the mechanism-agnostic components of a Privacy-ABC system.

Basic Concepts

The main entities are users, issuers and verifiers, optional entities are inspectors and revocation authorities:

The user is collecting credentials from various issuers and controlling which information from which credentials is presented to which verifiers.

The issuer issues credentials to users, thereby vouching for the correctness of the information contained in the credential with respect to the user to whom the credential is issued. Each issuer generates a secret issuance key and publishes the issuer parameters that include the corresponding public verification key.

The verifier protects access to a resource or service that it offers by imposing restrictions on the credentials that users must own and on the information from these credentials that users must present to access the service.

The revocation authority (optional) is responsible for revoking issued credentials, so these credentials can no longer be used to generate a presentation token.

The inspector (optional) is a trusted authority who can de-anonymize presentation tokens under specific circumstances.

A credential contains attribute-value pairs, certified by the issuer. A user can generate a presentation token containing a subset of the certified attributes. Upon receipt of a presentation token from a user, a verifier checks whether the presentation token is valid w.r.t. the relevant issuers' public keys. If the verification succeeds, the verifier can rest assured that the corresponding issuers vouch for the attributes contained in the presentation token.

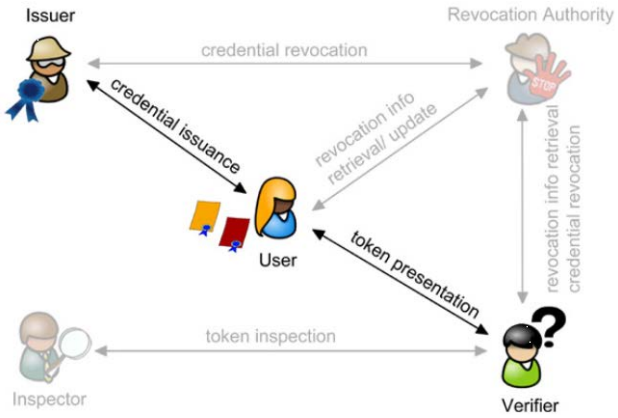

Figure 1: *Overview of the entities involved.*

A secure realization of a Privacy-ABC system must guarantee that

1) users can only generate a valid presentation token if they were indeed issued the corresponding credentials, and

2) the presentation tokens do not reveal any further information about users other than the attributes contained in them.

Point 2) comprises *unlinkability* and *untraceability* of tokens. *Unlinkability* means that different tokens derived from the same credential cannot be linked together. Untraceability covers the issuance process and requires that an issuer cannot link a given token to a particular issuance session and user. Both properties only hold with respect to the identifiability due to the disclosed attributes.

Pseudonyms

In traditional public-key cryptography, users generate a private/public key pair that can be used to authenticate the users. In a Privacy-ABC system, however, users may generate as many public keys as they wish from a previously generated secret key. These public keys are called pseudonyms. Pseudonyms are cryptographically unlinkable, meaning that given two different pseudonyms, one cannot tell whether they were generated from the same or from different secret keys. By generating different pseudonyms users can thus be known under different unlinkable pseudonyms to different sites, yet use the same secret key to authenticate to all of them.

A secret key can be generated by a piece of trusted hardware (e.g., a smart card) that stores the key and uses it in computations (e.g., to generate pseudonyms), but never reveals the key. The key is thereby bound to the hardware, such that the hardware must be present to use the key

There are situations where the possibility to generate several unlinkable pseudonyms is undesirable. E.g., in an online opinion poll, users should not be able to bias the result by entering multiple votes under different pseudonyms. In such situations, the verifier can request a special pseudonym called a scope-exclusive pseudonym, that is unique for the user's secret key and a given scope string. Scope-exclusive pseudonyms for different scope strings remain unlinkable.

Credentials and Key Binding

A credential is a certified container of attributes issued by an issuer to a user. An attribute is described by the attribute type that determines the semantics of the attribute (e.g., first name) and the attribute value that determines its contents (e.g., "John"). By issuing a credential, the issuer vouches for the correctness of the contained attributes with respect to the user.

Optionally, a credential can be bound to a user's secret key, i.e., it cannot be used without the secret key. We call this key binding. It is somewhat analogous to traditional public-key certificates, where the certificate contains the CA's signature on the user's public key, but unlike traditional public-key certificates, a Privacy-ABC is not bound to a unique public key: it is only bound to a unique secret key. A user can derive pseudonyms from this secret key and (optionally) show that they were derived from the same secret key that underlies the credential. As with pseudonyms credentials can also be bound to a trusted physical device, such as a smart card.

Presentations

In a typical token presentation interaction, the user first requests access to a protected resource, upon which the verifier sends a presentation policy that describes which credentials the user must present and which information from these credentials must be revealed to obtain access. The user ABC Engine then checks whether it has the necessary credentials, and if so, generates a presentation token containing the appropriate cryptographic evidence.

ABC4Trust Architecture for Privacy-ABCs

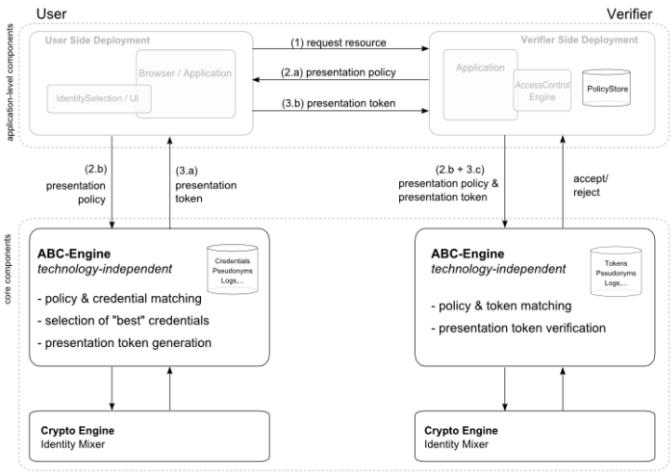

Figure: 2: *Presentation*

Upon receiving the presentation token, the verifier checks that the cryptographic evidence is valid for the presented token and checks that this token satisfies the presentation policy. If both tests succeed, it grants access to the resource. The sequence of a token presentation interaction is illustrated in figure 2 above.

Presentation tokens only reveal the attributes explicitly requested by the presentation policy – all other attributes in the credentials remain hidden. Moreover, presentation tokens are cryptographically unlinkable and untraceable (no collusion of issuers and verifiers can tell whether two presentation tokens were generated by the same or by different users, or correlate a presentation token to the issuance of the underlying credentials).

Rather than requesting and revealing full attribute values, presentation policies and tokens can request and reveal predicates over attributes. E.g., a token could reveal that the name on the user's credit card matches that on her driver's license, without revealing the name, or a token could reveal that the user's date of birth is before January 1st, 1994, without revealing her exact date of birth.

When the presentation policy requires a key-bound credential, the derived presentation token always contains an implicit proof of knowledge of the underlying secret key. Thus, the verifier can be sure that the rightful owner of the credential was involved in the creation of the presentation token. When the secret key of the user is a device key, i.e., a key that is kept on a trusted device and cannot be extracted from the device, then the proof of knowledge of the key is performed on the device and included in the generation of the presentation token. Accordingly, for credentials that are key-bound to a physical device it is impossible to create a presentation token without the device.

Issuance

In the simplest setting, an issuer knows all attribute values to be issued. Credential issuance is a multi-round interactive protocol between the issuer and the user, at the end of which the user obtains a new credential. Prior to the issuance, the issuer may have obtained and verified all attribute values through an out-of-band process. The sequence of a credential issuance interaction is illustrated in figure 3 above.

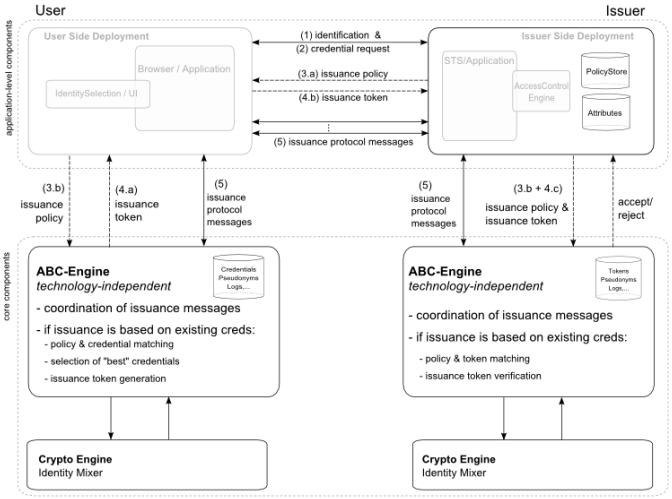

Figure 3: *Issuance*

Privacy-ABCs also support advanced issuance features in which attributes are blindly "carried over" from existing credentials, without the issuer becoming privy to their values. Similarly, the issuer can blindly issue a user's self-claimed attribute values (i.e., not certified by an existing credential), carry over the secret key to which a credential is bound, or assign a uniformly random value to an attribute such that the issuer cannot see it and the user cannot bias it. Advanced issuance is an interactive protocol between the user and the issuer. In the first move, the issuer provides the user with an issuance policy that consists of a presentation policy specifying which pseudonyms and/or existing credentials the user must present and of a credential template specifying which attributes or secret keys of the newly issued credential will be generated at random or carried over from credentials or pseudonyms in the presentation policy. In response, the user sends an issuance token containing a presentation token that satisfies the issuance policy. Then the cryptographic issuance protocol is executed.

ABC4Trust at a glance

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

Press contact:

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

Version and date of publication:

Version 1.0, January 2015

Want more info?

www.abc4trust.eu/

SEVENTH FRAMEWORK PROGRAMME

ABC4TRUST