ABC4Trust
c/o Marit Hansen
Unabhängiges Landeszentrum für Datenschutz
Holstenstraße 98
24103 Kiel, Germany
press@abc4trust.eu

Press release

ABC4Trust project publishes source code of privacy-enhancing authentication solution

Online services can use the code to protect customer's data and reduce exposure to liabilities in case of personal data breaches

"Privacy is an integral part of human dignity and personal freedom", as Vice-President of the European Commission Viviane Reding stressed at a speech regarding the proposal for a Data Protection Regulation. Personal data breaches cause major liability risks and loss of reputation for businesses and may impact the life of the compromised person in a long term. Protection of personal data is served best by taking data protection aspects into account right from the planning phase. The draft for a General Data Protection Regulation demands privacy by design and privacy by default when developing new processes. This is taken into account by the EU-funded project "Attribute-based Credentials for Trust" (ABC4Trust) that is piloting cryptographic solutions to authenticate persons in a privacy-preserving way with selective disclosure of attributes in authentication processes.

Appropriate privacy-enhancing technologies (PET) as developed in the ABC4Trust project allow secure authentication while only revealing the data essential for the requested service and no longer require verifying every detail of a user's identity. Reducing data in this early state may aid businesses to comply with these principles by avoiding unnecessary data processing, and citizens gain more privacy. To assist online services in implementing such technologies, the ABC4Trust project has published the source code of the first version of its solution.

Electronic identity solutions are based on attributes about a person with the respective attribute value like the person’s name or date of birth. Classic electronic identification does not allow presentation of selected attributes without invalidating the issuer’s signature and thus risking a rejection. Advanced and privacy-preserving solutions support selective disclosure of attributes: the service provider can only learn those pieces of information that are necessary for the given purpose while the signature verifying the correctness of the information remains intact. The privacy-enhancing attribute-based credentials (Privacy-ABCs) deployed in the ABC4Trust project’s pilots support the above-mentioned attribute selection.

The use of Privacy-ABCs has now become accessible for a broader audience, as the ABC4Trust project has released the first iteration of the Attribute-based Credential Engine (ABCE) implementation. The ABCE allows owners and implementers of online services to leverage the potential of Privacy-ABCs to protect customer’s data and reduce exposure to liabilities in case of personal data breaches.

The first iteration of the ABCE consists of a number of core components and a user interface needed to implement a Privacy-ABC system. The release includes source code and documentation on how to setup and integrate the ABCE and can be found on the ABC4Trust website: https://abc4trust.eu/index.php/source. The components deal with issuing, verifying, inspecting, and revoking privacy-preserving attribute-based credentials, as well as handling the required user interaction. ABC4Trust has developed two applications that are currently deployed and being used by users in two pilot trials; one in Söderhamn, Sweden and the other in Patras, Greece.

Building on the basic components fully functioning support for Privacy-ABCs can be implemented in a given system. The ABCE is provided with adapters for storing keys on smart cards and a very generic user interface. Additional customization will be required regarding the storage of keys and credentials along with the user interaction.

All parts of the ABCE are released under the Apache License 2.0 license. However, the cryptographic engines underlying the ABCE are not currently a part of the ABCE, and must be downloaded separately. The cryptographic engines are IBM Identity Mixer (Version 2.4 or later) and Microsoft U-Prove. The U-Prove binary can be downloaded from https://microsoft.com/u-prove. The IBM Identity Mixer can be downloaded from https://abc4trust.eu/idemix.