IBM IDENTITY MIXER

Authentication without identification

IBM Identity Mixer is a cryptographic protocol suite for privacy-preserving authentication and transfer of certified attributes. It allows for user authentication without collecting any personal data. Thus, no personal data is received that needs to be protected, managed, and treated according to complex legal regulations. Nevertheless, service providers can rest assured that their access restrictions are fully satisfied.

IDENTITY SECURITY AND PRIVACY FOR ELECTRONIC USER AUTHENTICATION

Your personal identity data was worth several hundred dollars on the black market 10 years ago. Today, it's worth pocket change. Why? Because it's easier to steal this information than ever before.

As more pieces of our lives go online, we regularly have to authenticate ourselves for service providers, including social media tools and e-commerce sites. Today, identity authentication is realized by mirroring the paper-based processes in the electronic realm, but this often exposes an excessive amount of personal information. For example, when you show your driver's license to prove your age, you also unintentionally share your address.

PROTECTING PERSONAL INFORMATION IN THE PAPER AGE

Because electronic information is much harder to control and protect than information on paper, this praxis erodes our privacy and puts us at risk. Indeed, the flow of information in today's electronic networks is virtually impossible to follow and assess. Thus, it is important that data is always protected and kept secret and that disclosure is minimized whenever possible.

Consider this fictional transaction: Alice, a movie buff, wants to stream the classic film "Alice in Wonderland" from BestMovies, an online movie service. Before it will stream the movie, BestMovies requires proof that Alice satisfies the necessary access control rules, i.e., that Alice has bought a subscription and is older than 12 years of age.

In the paper-based world, the clerk at BestMovies would tell Alice what proof is required, and Alice would present her BestMovies subscription card and her driver's license or some other government-issued ID. The clerk would verify the two documents for authenticity and specifically check Alice's birthdate. While the clerk would see all of her information, he would most likely forget shortly thereafter, assuming he views hundreds of similar documents every day. Thus, Alice's privacy and information security is retained.

MOVING TOWARD DIGITAL SOLUTIONS

The same doesn't hold true in the digital world. Like Neil Armstrong's footprints on the lunar surface, the information will not be forgotten, but rather stored — most likely in the cloud, which is often poorly protected.

Unfortunately, the naïve transposition of the paper-based world approach is exactly what is typically done: The identity providers issue a credential to the users containing their attributes. Then, when authenticating with the credential, the user has no choice but to transmit the full set of credentials to the provider no matter what data is being requested. Apart from revealing more information than often necessary, users can be tracked across different service providers because of the uniqueness of their certificates. Some popular examples of such technologies that follow this approach include X.509 client certificates as well as existing government eID solutions.

The second approach that is often employed requires the identity provider to be online and involved in all of its users' authentication transactions. While the issuer can certify only those attributes that are explicitly required (which is good for

privacy), there's a privacy bottleneck in the system that can track all its users' transactions. From a security point of view, this approach is not ideal: The identity provider needs to be highly available but also highly protected from cybercriminals, which are contradictory requirements.

Neither of these approaches is completely satisfactory from a privacy and security point of view because they both require users to reveal more information than necessary. To solve this, the team at IBM Research – Zurich developed Identity Mixer. Identity Mixer uses advanced, provably secure cryptographic algorithms to authenticate users while providing only the minimally necessary information, without revealing any collateral and unintended data, to simultaneously achieve both privacy and security.

HOW IDENTITY MIXER WORKS

In its simplest form, Identity Mixer works similar to traditional attribute-based credentials with a few crucial differences. Each user has a single secret key but can have multiple public keys that correspond to it. In a way, this secret key is the user's secret identity, and users can derive as many public identities from it as necessary. For example, Alice could use one identity for BestMovies and another to pay her taxes online. Each transaction gets a different public key, leaving no privacy breadcrumbs.

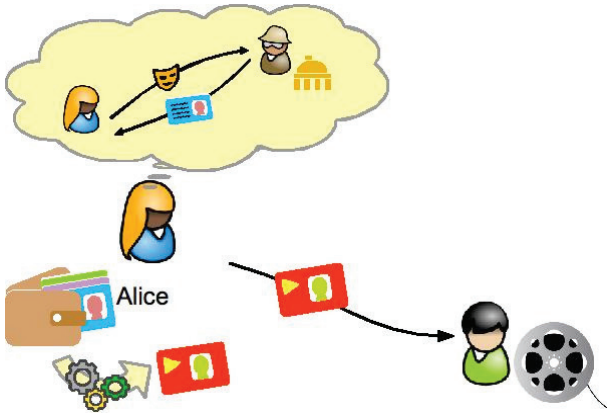
Alice can get a certified attribute-credential such as an eID, a driver's license or a membership card by sending one of her public keys to the issuer of the desired credential. The issuer will then sign that public key along with Alice's attributes, which vouches for and sends the resulting credential back to Alice. Alice stores the received credential in her digital wallet, which can run on her mobile phone, computer, another preferred device, or via a cloud-based wallet. This process is conceptually identical to one of the X.509 attribute certificates, except Identity Mixer uses different, privacy-protecting cryptographic algorithms.

When Alice is requested to authenticate to a service — let's say she wants to stream "Alice in Wonderland" from BestMovies again — the service provider will send her a presentation policy stating the information needed to proceed. In the example, the presentation policy would state BestMovies requires Alice to prove that she's older than 12 according to government-issued credentials and that she possesses a valid subscription credential from BestMovies. This is the second difference to traditional approaches, where users are typically asked to identify themselves in order for the service provider to evaluate whether the user satisfies the access control policy.

Now, having received the presentation policy, Alice's digital wallet will offer her a choice of which credentials she can use to satisfy it, or the wallet will point out which credentials she is missing. After Alice has selected the necessary credentials, her wallet will use a cryptographic algorithm to transform her credentials into a presentation token, which she can then send to BestMovies, the verifier.

This transformation is the third and probably most important difference to the traditional approaches. The presentation token consists only of the information that Alice needs and is willing to reveal instead of the full set of attributes contained in her credentials. Thus, the presentation token would just contain the attributes "User is older than 12 according to a credential issued by the government" and "User possesses a subscription credential from BestMovies with a non-expired validity date." The presentation token validates with the public verification key. Then the verifier can check the validity of the token using the issuer's verification key with the cryptographic verification algorithm and learn only the information about Alice that was specified in the presentation policy — nothing more.

Want to give Identity Mixer a spin? You only need a Web browser to test the ultimate tool for both privacy protection and security.



IDENTITY MIXER AS A SERVICE

Identity Mixer is available as an experimental service on the IBM Bluemix cloud development platform. This allows application developers to integrate authentication with Identity Mixer in a way as simple as with openID.

Alternatively to Bluemix, application developers can use the open source distribution of Identity Mixer.

MORE INFORMATION

Identity Mixer offers many more extended features than the ones explained above, including exclusive pseudonyms, multicredential tokens and designated inspectors. Learn more about the privacy-preserving characteristics and data-minimizing strategies implemented on Identity Mixer's website.

Project Website: www.zurich.ibm.com/idemix

Demo: idemixdemo.mybluemix.net

Bluemix: console.ng.bluemix.net/catalog/ibm-identity-mixer

Open Source: github.com/p2abcengine/p2abcengine

Contact: idemix@zurich.ibm.com

For more information:
www.zurich.ibm.com/idemix

IBM®