# Privacy-preserving identities for a safer, more trusted internet

Microsoft Corporation, November 5th 2010.

## The problem

Business and government services are increasingly being migrated online to improve convenience and reduce the cost of conducting these services in person. Migrating high-value transactions online require, however, high-level of identity assurance. The challenge is to create a system offering the richness of real-world credentials we carry in our pockets, while preserving the same level of security and privacy we enjoy when using them.

Username and passwords are ubiquitous online and are therefore difficult to replace, but provide low-levels of security and do not offer the capabilities required to encode identity information about users. Public Key Infrastructure (PKI) certificates are well-known and provide high-levels of security, but don't scale internet-wide and do not provide an adequate level of privacy.

Identity federation is fast becoming the prevailing mechanism to exchange identity information online. Many federation protocols and frameworks are being proposed to solve these identity problems; the most popular being WS-Federation, SAML, Information Cards, OpenID, OAuth, etc. Many challenges exist to provide an adequate level of security, privacy, scalability when using these. Indeed:

- **Security**. Relying on one or a small set of identity providers to authenticate users has security implications. First, the value of the identity credential increases because of its reusability; phishing and hijacking attacks therefore become more problematic. Second, insiders at the identity providers have the power to access users' accounts without their knowledge.
- **Privacy**. Identity providers gain a lot of visibility on the users' activities; either in real-time by observing what information is sent to whom, or later by comparing notes with relying parties. In contrast, this level of traceability is not present today when we use real-life credentials.
- **Scalability**. Depending on an identity provider to provide identity information for all transactions in real-time increases the fault-tolerance requirements and makes these parties interesting targets of denial of service attacks.

## Minimal disclosure technologies

A class of technologies, called "Minimal Disclosure Technologies"[1] is being developed to address these difficult challenges. They have a 25-year history in academia, starting from the work of David Chaum and Stefan Brands, and are still being actively researched today (in particular by Microsoft Research [1]). Minimal disclosure technologies are a building block providing unique security, privacy, and scalability benefits that can improve the abovementioned identity systems.

Minimal disclosure "tokens" are a type of credentials, similar to federation token (such as SAML) and PKI certificates (such as X.509), but providing better privacy.

- First, the presentation of a minimal disclosure token is "unlinkable" to its issuance, meaning that nothing in the token's construct inescapably identifies the user presenting it. In particular, a token's cryptographic materials (public key and issuer signatures) are transformed by the user at token

[1] Synonyms encountered in the literature include anonymous, private, and attribute-based credentials.

issuance to break the linkages that otherwise would otherwise be present. In contrast, conventional X.509 certificates and SAML assertions contain many “correlation handles” that allow observers to build a profile of a user’s activities.

- Second, a user has more flexibility when presenting a minimal disclosure token. Conventional tokens can only be presented in their entirety. Minimal disclosure tokens allow the user to present the “minimal” information required for a specific transaction. For example, if a token encodes a user’s name, address and date-of-birth; then a user could chose to only present its country of residence to access a website, without disclosing anything else. Typically, “hiding” the other attributes would prevent the relying party to verify the integrity of the credential, but the cryptography behind minimal disclosure technologies allows this counter-intuitive property. Even more advanced “proofs” are possible; for example, a user could prove that she is over-21 without disclosing her birth date, or prove that her name does not appear on a blacklist without identifying herself.

Microsoft recently released the U-Prove minimal disclosure technology [2] to great acclaims.[2] Microsoft sees this technology as an important piece of the puzzle to create a safer and more trusted identity system for the internet; built with privacy by design. Identity protocols need to be supported by a rich ecosystem in order to be successful; to this end, Microsoft released the U-Prove specifications under the Open Specification Promise [3] allowing anyone to implement and freely use the technology, and donated two Software Development Kits to the open-source community [4]. Microsoft also released a Community Technology Preview (CTP) that demonstrates how the U-Prove technology can be used in real identity systems by integrating into Microsoft identity platform consisting of Active Directory Federation Services 2.0 (ADFS), the Windows Identity Foundation (WIF), and Windows CardSpace 2.0.

## The road ahead

Minimal disclosure technologies are emerging from research labs, and are now mature enough to be adopted by the industry. Like any new technology, especially cryptographic technology with counter-intuitive properties, a lot of effort is needed to educate the various stakeholders to demonstrate the value and practicality of these technologies, and to dispel the false perception that accountability and privacy goals are irreconcilable.

Microsoft recently partnered with Franhaufer Fokus on two projects relating to the German eID card: the first project demonstrates how a student identity can be used in a privacy-protecting manner to fill-out a survey and access online materials [5]; the second project illustrates how the privacy and security requirements of an e-Participation (poll) scenario can be met with U-Prove [6].

Microsoft firmly believes in the value of the minimal disclosure technologies, and pursues the development of the U-Prove technology. Microsoft would be happy to share its experience at the IAB Internet Privacy Workshop, and discuss with other participants the need of these technologies for safer, more trusted identities on the internet that protect the privacy of the users.

## References

[1] http://research.microsoft.com/en-us/projects/creds/

[2] http://www.microsoft.com/u-prove

[2] Microsoft received the International Association of Privacy Professionals (IAPP) Privacy Innovation Awards last September, and European Identity Award in the "Best Innovation" category from Kuppinger Cole & Partners in May [7].

[3] http://www.microsoft.com/interop/osp/default.mspx

[4] C# version: http://code.msdn.microsoft.com/uprovesdkcsharp
Java version: http://code.msdn.microsoft.com/uprovesdkjava

[5] http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/uprove.aspx

[6] http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/eid.aspx

[7] http://blogs.technet.com/b/identity/archive/2010/09/30/microsoft-receives-the-privacy-innovation-award-for-technology-2010.aspx