AUTHENTICATION BEYOND BASIC ATTRIBUTES (ABBA)

Roland M. van Rijswijk-Deij
SURFnet, Radboudburcht 273, 3511 CK, Utrecht, The Netherlands
e-mail: roland.vanrijswijk@surfnet.nl

Joost van Dijk
SURFnet, Radboudburcht 273, 3511 CK, Utrecht, The Netherlands
e-mail: joost.vandijk@surfnet.nl

Author affiliations

SURFnet bv

Keywords

Smart Cards, Attribute-based Authentication, Identity, Security, Cryptography

Abstract

The NREN community has been building and championing the federated identity management ecosystem for the past decade. This has led to great advances in online identity. Indeed, the model is so successful that it is seeing broad adoption in both enterprise environments as well as in the consumer identity landscape. Cloud service providers increasingly offer federated authentication by default rather than on request from existing federations.

Two of the cornerstones of federated identity are the concepts of attributes and attribute release. When a user is authenticated at his or her identity provider the IdP not only affirms successful authentication but also releases attributes about the user, such as, for instance, their full name, their affiliation and their e-mail address. This gives service providers the opportunity to base their authorisation decisions on a rich set of information about the user. Attribute release is strictly regulated by the policies governing identity federations. Most federations herald the principle of minimal disclosure, only releasing those attributes required by the service provider to be able to make authorisation decisions about the user. This protects user privacy. In some cases, federations go one step further and require users to give consent before their attributes are released.

Up until now, attribute-based authentication has been mostly limited to online identity federations. It has also been mostly limited to static attributes describing the user, stored at their identity provider. There are a number of movements in the academic arena that want to take attribute-based authentication further, expanding its use to, for example, offline scenarios like public transport ticketing. We are interested in keeping up to date with these developments as they may prove to be relevant for our constituency. To that end, we are participating in a project that aims to expand attribute-based authentication to the world of NFC-capable smart cards. The main driver for this project is to come up with privacy-friendly alternatives to, for instance, the Dutch Public Transport Chip Card ("OV chipkaart"). SURFnet's participation in this project is in the context of a project we call "Authentication Beyond Basic Attributes". This project looks at cutting edge technologies that take the attribute model beyond what is currently done in identity federations.

In this project, we collaborate with the Radboud University in Nijmegen and TNO (Netherlands Organisation for Applied Scientific Research) in Groningen and are helping them pilot a technology they call "IRMA", which stands for "I Reveal My Attributes" [1]. IRMA strives to offer a fast implementation of privacy-friendly and secure attribute-based authentication technologies on an NFC-capable smart card. Their solution is based on two technologies, one from IBM, called Idemix [2], and one from Microsoft called U-Prove [3]. Both technologies work in a similar fashion and have the following key properties:

- Use of (non-identifying) attributes is untraceable
- Integrity, authenticity, confidentiality and non-transferability of attributes is guaranteed
- Attributes are only stored locally, on the smart card and are under the user's control
- The user is in control; he/she voluntarily selects and loads attributes onto the card

To achieve these properties the technologies rely on novel cryptographic techniques such as blind signatures and zero-knowledge proofs. The most important concept in IRMA is that of credentials. Credentials form a set of coherent attributes released by a single issuer. The structure of a credential is shown in Figure 1.

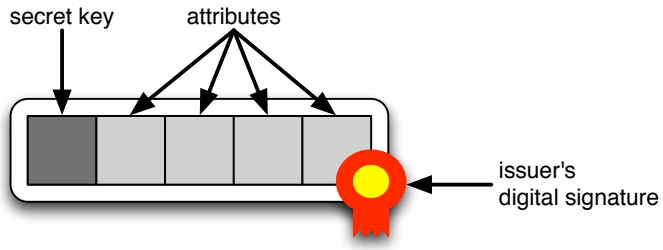

Figure 1 - IRMA credential

As the figure shows, a credentials consists of 3 key elements:

- A secret key that is used to ensure that credentials are non-transferable (cannot be copied from the card)
- The attributes associated with the credential
- A digital signature by the issuer of the credential, vouching for the authenticity of the attributes

Examples of credentials are:

- An address credential, containing attributes for the country, city, street + number and postal code of the card holder
- An age verification credential, containing attributes that certify that the user is, e.g., over 16, over 18, over 21 and under 30.

Any subset of attributes from a credential can be released upon approval by the user (this is a called "selective disclosure"). Also, attributes from multiple credentials can be released simultaneously, for instance, the "country" attribute from the first example above could be combined with the "over 18" attribute from the other example to create a privacy-friendly "wietpas"[1] under the condition that the country is "NL".

Two more important properties of the IRMA card are *issuer-unlinkability* (the issuer of a credential cannot track *where*, *when* and *which* attributes were released by a user) and *multi-show-unlinkability* (service providers cannot collude to build a profile on the user by comparing attributes released by the user to trace them).

We are currently (Fall of 2012) working on a pilot of this technology, where students of a research master track in Digital Security (called the Kerckhoffs' Master) are issued a smart card with the IRMA application installed. The smart card is issued with a base credential on it with attributes from our identity federation (SURFconext) and the students can obtain additional attributes from, for example, the Kerckhoffs' Master program to indicate that they are a student of said program. The physical smart card body will not contain any identifying information other than a photo printed on the front to prove that the person using the card is the legitimate owner when the card is used in an offline scenario (see Figure 2 below for an example of what the card looks like).

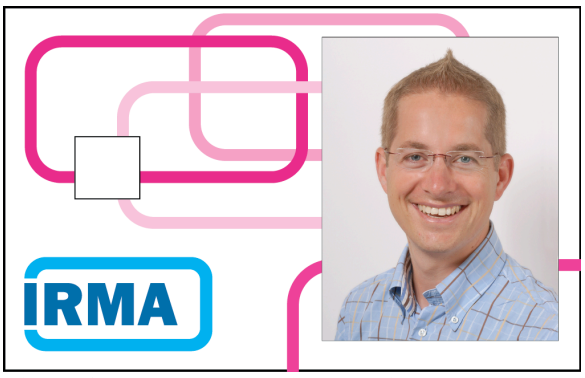

Figure 2 - Example IRMA card with user photo printed on the front

[1] The "wietpas" is an ID that allows Dutch citizens over 18 to legally purchase soft drugs from the infamous "Coffee Shops"

In the pilot project students are encouraged to use the card both in online as well as offline scenarios, for example:

- Getting coffee at a reduced price at some of the teaching locations
- Free printing for students of the Kerckhoffs' Master at the Radboud University
- Access control to a number of online resources such as a portal for grading teacher performance for courses

The goal of the pilot project is not to come up with and test an exhaustive list of use cases, rather, we want to stimulate use of the technology so we can find out how it performs in real life. The use cases above have thus been specifically tailored to stimulate students to use the card, preferably on a daily basis.

At TNC 2013 we would like to present the results of the pilot project, going into what we learned about using this kind of technology in a real-life environment. We will also bring a live demonstration to TNC to show attendees how this technology works. In addition to presenting we will also bring a poster to give attendees the opportunity to interact with us and experience a demo of the technology outside of the track sessions.

References

[1] Jacobs, B., "IRMA – I Reveal My Attributes", Radboud University Nijmegen, August 2012, https://www.irmacard.org/?page_id=48

[2] Camenisch, J. and Lysyanskaya, A., "Idemix, Identity Mixer", IBM Zürich, http://www.zurich.ibm.com/idemix/details.html

[3] Brands, S., "U-Prove, End-to-End Trust", Microsoft Research, February 2011, http://www.microsoft.com/mscorp/twc/endtoendtrust/vision/uprove.aspx

[4] FP7, "ABC4Trust – Attribute-based Credentials for Trust", 2011, https://abc4trust.eu

Acknowledgements

The authors would like to express their gratitude to Bart Jacobs and Jaap-Henk Hoepman of the Digital Security research group at Radboud University Nijmegen for inviting SURFnet to participate in this project, and to the IRMA team with participants from the Radboud University Nijmegen, TNO and SIDN for the spirited collaboration in this project. We would also like to thank MULTOS Corporation for their patience in helping us figure out what smart cards were best suited for use in the project.

Author Biographies

Roland van Rijswijk works as Technical Product Manager for SURFnet and is responsible for innovation projects involving identity, trust and Internet security. Roland participates in the ABBA/IRMA project on behalf of SURFnet because he believes this is one of the possible roads to future mechanisms for electronic identities. Roland obtained a Master of Science degree in Computer Science from the University of Twente (2001), after which he worked in software development for Philips, Advanced Encryption Technology (AET) and InTraffic. His expertise is in the application of high-end cryptography. Roland joined SURFnet in 2008.

Joost van Dijk is Technical Product Manager of the SURFfederatie. As such, he is responsible for innovation projects in the area of Identity Management and Identity Federations. He graduated in Computer Science from Utrecht University (1995), after which he continued research at the department's Center for Software Technology. After leaving Utrecht University in 1997, he worked as a researcher at the Software Engineering Research Center (SERC), as an independent consultant for various companies, as a part-time lecturer at the Leiden Institute of Advanced Computer Science (LIACS) and as an instructor at TUNIX Internet Security & Training.