Attribute-based Authentication and Signatures in Practice

Bart Jacobs
Institute for Computing and Information Science, Radboud University, Toernooiveld 212, 6525 EC Nijmegen, The Netherlands
E-mail: bart@cs.ru.nl, web: http://www.cs.ru.nl/~bart

Joost van Dijk
SURFnet, Moreelsepark 48, 3511 EP, Utrecht, The Netherlands
E-mail: joost.vandijk@surfnet.nl

Sietse Ringers
Institute for Computing and Information Science, Radboud University, Toernooiveld 212, 6525 EC Nijmegen, The Netherlands
E-mail: sringers@cs.ru.nl, web: https://sietseringers.net

Author affiliations
Radboud University, SURFnet bv, Privacy by Design Foundation[1]

Keywords
Attribute-based Authentication, Attribute-based Signatures, Identity, Security, Privacy, Cryptography

Abstract

For the past decade the NREN community has been building and championing (federated) identity management ecosystems based on attributes. This has led to great advances in online identity. At TNC 2013 our colleague Roland van Rijswijk-Deij has given a presentation[2] about decentralised attribute-based identity management using the IRMA system. Since then many developments have taken place, including:

1. IRMA has moved from an academic research environment at Radboud University to an independent (non-profit) foundation, called *Privacy by Design*; the foundation is now responsible for further development of the technology and for its deployment.

2. Back in 2013 an IRMA implementation was available on a smart card. Since then the emphasis has shifted entirely to smart phone implementations.

3. IRMA has been designed initially for attribute-based authentication, but very recently its ecosystem has been extended with attribute-based electronic signatures.

4. The foundation has established connections with (currently) two identity federations, namely SURFconext and iDIN; the latter is operated by the banks in the Netherlands and can be used by anyone with access to internet banking. The foundation is expected to join eduGAIN as a Service Provider before the end of 2017.

The proposed TNC 2018 presentation will elaborate on these developments. They will be described in some more detail below.

[1] See https://privacybydesign.foundation/en/
[2] See https://tnc2013.terena.org/core/presentation/5

Ad 1. Move to the Privacy by Design foundation

Since 2008 the IRMA project has been running within the Digital Security group at Radboud University, with both internal and external funding. It has resulted not only in many scientific publications[3] but has also led to two prototype implementations: one on a MULTOS smart card, and one on the Android platform. Throughout the years IRMA matured to such a form that it was ready to leave the academic environment. For this purpose the non-profit foundation *Privacy by Design* was founded in the fall of 2016, by two of the current authors (BJ en SR). The broad aim of the foundation is to develop and deploy privacy-friendly open source technology. This is a task that goes beyond the normal research and teaching activities of a university since it involves operating infrastructure and establishing operational relations with various societal organisations in identity management. The main role of the foundation so far is setting up and running the IRMA infrastructure and guiding its further practical development.

In setting up decentralised attribute-based identity management there is a chicken-and-egg problem where both *issuance* and *verification* of attributes must be possible. The foundation concentrates on issuance. It is now issuing various attributes from various sources, including:[4]

- Name, address, date-of-birth from bank registers via iDIN;
- Name, e-mail, affiliation, role from SURFconext, and soon the wider NREN community through eduGAIN;
- E-mail and mobile phone numbers via verification codes;
- Attributes of health professional from the Dutch national register BIG.

Ad 2. Smart phone implementation

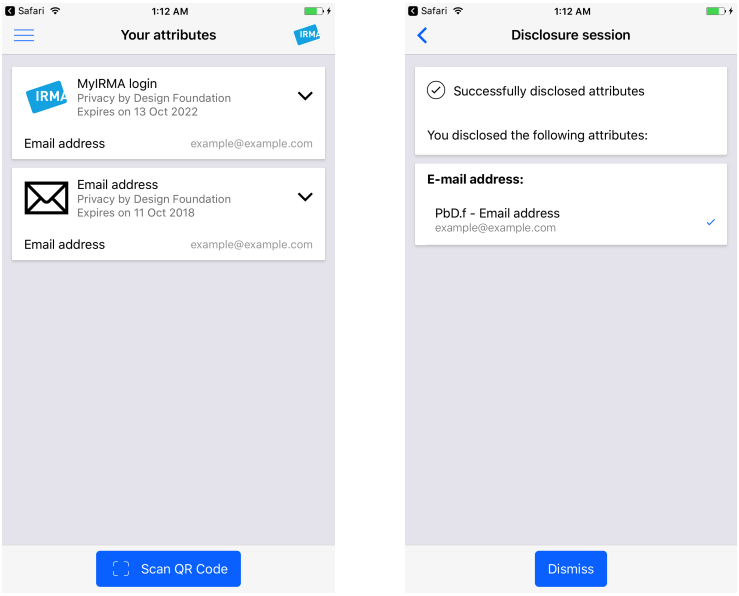
The cryptographic basis of IRMA is Idemix [3], developed at IBM Zürich. It uses zero-knowledge proofs, for maximal privacy protection. Such proofs are computationally non-trivial and thus their efficient implementation on a smart cards (in 2013) was quite an accomplishment [4]. The smart card implementation was chosen because IRMA's security relies on the protection of a personal private key. At each demonstration of the smart card implementation, people were asking: can you also do this on a smart phone?

Securely storing a private cryptographic key on a smart phone is a delicate matter. The IRMA team developed its own multiparty computation protocol, using homomorphic encryption, to store part of the private key on the server of the foundation. This "central" part of the key is needed for each attribute disclosure, but the protocol works in such a way that the foundation cannot see which attributes are disclosed and to whom. This protocol is up and running since early 2017, see also [2].

The foundation has developed a new implementation of the IRMA app, both for Android and iOS, with a common code-base in the programming language Go, with graphical interface in React Native. The pictures below give some impression.

[3] Collected at `https://privacybydesign.foundation/publications/`

[4] See `https://privacybydesign.foundation/issuance/` for the an overview of the current situation



Ad 3. Attribute signatures

Whereas attribute-based authentication is relatively well-known, attribute-based signatures are not [1]. It offers to include a number of attributes of the signer in an electronic signature. Any verifier of the signed document can then check that the signer is a person for which the included attributes hold. Obvious attributes to include are your name, or address, but possibly also your profession, like medical doctor together with your medical registration number.

These attribute-based signatures offer enormous new possibilities, for instance for citizens to sign their request to the authorities with their citizen registration number. Or electronic bills can be turned into cheques by signing them with your bank account number as attribute.

Experiments with attribute-based signatures are ungoing via a "signature request" application. It can be used to generate a signature request, consisting of a text and a list of attributes. Such a request can be sent as a special email attachment to the signer. Upon clicking on this attachment on the signer's phone, the IRMA app is opened and the text is displayed. When the signer agrees, and possesses the required attributes, the signature is generated on the phone after a correct PIN entry. Copies of the result are then returned to the requester, and also stored locally on the phone. Experiments have been carried out to verify such IRMA signatures via an Adobe plugin.

Ad 4. Connections with federations

Ideally, in the IRMA ecosystem, organisations like banks, governments, telecom / network providers, and (web)shops issue their own attributes to users of IRMA, like bank account numbers, address, date of birth, nationality, e-mail address, mobile phone number, loyalty member numbers, coupons, etc. In the current start-up phase of IRMA, these organisations cannot be expected to do this immediately. For the time being, the foundation has taken up this issuance role, in the following way: it collects relevant (personal) attributes at these sources, and issues them itself, in signed form, to the user. This is currently operational for the higher education (NREN) community in the Netherlands via SURFconext, and also for the banking sector via its own authentication system iDIN. The SURFconext link is now being

extended with strong 'step-up' authentication, where IRMA is used as a second factor.

By joining eduGAIN as a service provider, the foundation is aiming to extend its service to the NREN community. This is particularly interesting for international collaboration scenario's, as IRMA provides an alternative to federated login by decoupling attribute providers from attribute consumers in a privacy-enhancing manner, mixing and matching attributes obtained from multiple sources, thus bringing end-users back in control of their attributes.

References

[1] G. Alpár, F. van den Broek, B. Hampiholi, and B. Jacobs. Towards practical attribute-based signatures. In R.S. CHakraborty, P. Schwabe, and J. Solworth, editors, *Proceedings of the Fifth Int. Conf. on Security, Privacy, and Applied Cryptography Engineering (SPACE 2015)*, number 9354 in Lect. Notes Comp. Sci., pages 310–328. Springer, Berlin, 2015.

[2] G. Alpár, F. van den Broek, B. Hampiholi, B. Jacobs, W. Lueks, and S. Ringers. IRMA: practical, decentralized and privacy-friendly identity management using smartphones. In *10th Workshop on Hot Topics in Privacy Enhancing Technologies (HotPETs 2017)*, 2017.

[3] J. Camenisch and E. van Herreweghen. Design and implementation of the Idemix anonymous credential system. In *CCS'02: Proceedings of the 9th ACM conference on Computer and communications security*, pages 21–30. ACM, 2002.

[4] P. Vullers and G. Alpár. Efficient selective disclosure on smart cards using Idemix. In S. Fischer-Hübner, E. de Leeuw, and C. Mitchell, editors, *Policies and Research in Identity Management: Third IFIP WG 11.6 Working Conference*, volume 396 of *IFIP Adv. in Inf. and Comm. Techn.*, pages 53–67. Springer, 2013.

Author biographies

Bart Jacobs is a professor of computer security at the Radboud University Nijmegen. With his research group he has worked over the last decade on a number of scientifically and societally relevant security topics such as chipcards (eg. in passports and transport), electronic voting, smart metering, road pricing and privacy. Recently he is also involved in privacy and security in medical research via the PEP project (`pep.cs.ru.nl`); it provides the infrastructure for a large Parkinson study with Radboudumc and Verily. Jacobs is a member of the Academia Europaea, of the National Cyber Security Council, and he heads the advisory board of the digital rights organisation Bits of Freedom. He is co-founder and chairs the board of the Privacy by Design foundation.

Joost van Dijk is a Technical Product Manager at SURFnet. He is responsible for the SURFconext identity federation platform and works on innovation projects in the area of Identity Management and Identity Federation. 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.

Sietse Ringers studied Mathematical Physics in Amsterdam and obtained his computer science PhD in 2016 in the area of identity management and cryptography from the University of Groningen. He is involved in the design and development of various privacy-enhancing technologies, such as a privacy-friendly attribute-based credential scheme and of IRMA. He is co-founder and board member of the Privacy by Design foundation.