Towards Practical Attribute-Based Identity Management: The IRMA Trajectory

Gergely Alpár and Bart Jacobs

Institute for Computing and Information Sciences (iCIS),
Radboud University Nijmegen, The Netherlands

Abstract. IRMA is an abbreviation for "I Reveal My Attributes", and at the same time it is the name of a project run by the Digital Security group of the University of Nijmegen and its partners to get attribute-based identity management up and running. This hands-on approach forces us to elaborate many unexplored issues, leading to a better understanding of attributes and their possibilities and challenges.

Cryptographic techniques that enable secure and privacy-friendly attribute-based authentication have been around for more than a decade, see [3,5,6,8]. But what is new is that the latest generation of smart cards is powerful enough to perform the required (non-trivial) cryptographic operations in an adequately efficient manner [9]. Hence only now we see efforts to actually deploy attributes in practice, like the IRMA project[1] at Nijmegen. Two other pilot projects should be mentioned, both of which are carried out by the EU-sponsored ABC4Trust consortium [4]. The Swedish pilot [2] gives anonymous access for elementary school pupils to on-line resources (*e.g.*, chat room), while the Greek pilot [1] enables university students to evaluate lectures anonymously. In both cases eligibility and privacy are of primary importance. Although the IRMA pilot uses the same underlying technology, the objective of our research is more general as we investigate a *broad variety* of attributes and applications. The associated kind of challenges does not appear in these ABC4Trust pilots since each focusses on a single context.

This document gives a brief overview of some of the more salient aspects of the IRMA project.

First of all, attributes are used in a very broad sense as describing some property of a person. This property may be anonymous (non-identifying), such as your gender, or whether or not you are over 18, but in the IRMA context it may also identify you, for example when the attribute is your bank account or social security number. While the underlying technology provides full unlinkability, the attribute values may provide linkability. This usage of identifying attributes may go against the original intention that attributes should be anonymous, but extending their interpretation to (partial) identification greatly extends the application scenarios. For instance, we foresee registration and status attributes for medical personnel (giving access to medical files), for employees (giving access

[1] See `www.irmacard.org` for up-to-date information and developments.

S. Fischer-Hübner et al.(Eds.): IDMAN 2013, IFIP AICT 396, pp. 1–3, 2013.

to premises, networks, and PCs), and for customers (giving benefits, and online access to their purchase/bonus history). Additionally, attributes may be used for a micro medical dossier, with essential (emergency) information.

Second, the IRMA project uses a smart card implementation [9] based on the Idemix technology [7]. However, the essential feature involved is selective disclosure of only a limited number (possibly only one) attributes, while hiding all other attributes. This focus on the core of the credential technology—using zero knowledge proofs—means that the system allows high level interfaces, beneath which other implementations, such as U-Prove, can also be employed. As a simplified view of the technology and the concepts, we may say that "credentials are issued and attributes are shown". Thus, at this stage, only a small part of the power of Idemix is actually used on IRMA cards. Future upgrades may involve more functionality.

Next, the extensive use of all kinds of attributes within IRMA leads to *dependencies* between these attributes: attribute X can only be issued after attribute Y has been verified. As an example, before you can receive an attribute stating what your bank account or mobile phone number is, you need to authenticate properly. This authentication may involve a mixture of already issued attributes on your IRMA card (like your name and date of birth) and out-of-band communication (like a one-time SMS code). These dependencies lead to a tree structure for attributes. An interesting question then arises: what should be the "root" attributes that do not depend on any other attributes on the card. It turns out that this question has deep implications for the "identity fabric" in our society. For instance, one can image that your Facebook identifier is issued as an attribute, so that you can use your IRMA card as Facebook login. But should this Facebook attribute be root, or not? If it is a root, it cannot depend on any other attributes, and must be issued purely via out-of-band authentication. But if it is not a root, it will typically depend on your name and date of birth attributes; in that case one can no longer have a pseudonym Facebook account, enforcing Facebook's real name policy.

Finally, who should decide about such delicate issues? We foresee an independent, non-profit foundation that runs the IRMA scheme and sets such policy issues. Also, this foundation should do the certificate management that regulates access to the card, both for issuing and verification of credentials. Within the IRMA project there is close coordination with both public and private parties to openly discuss such issues. Ongoing work involves a (experimental) connection between existing government identity management infrastructures and IRMA cards, for the issuing of credentials based on government data.

The use of a wide variety of attributes leads to a new activity that we label as "credential design". It involves the organisation of individual attributes in signed containers (credentials), with dependencies between them. In the IRMA set-up a credential contains at most four (related) attributes, such as first name, family name, full names, initials. Our experience so far leads to the following principles of credential design.

1. Attributes in one credential form a coherent set.
2. Each attribute in one credential falls under the responsibiility of a single most authoritative issuer.
3. Attribute duplication (same content, multiple issuers) should be avoided.
4. Verifiers should only be able to read a limited, predefined set of attributes.
5. Credential dependencies should be public.
6. An independent non-profit scheme manager should decide about such dependencies.

References

1. Abendroth, J., Liagkou, V., Pyrgelis, A., Raptopoulos, C., Sabouri, A., Schlehahn, E., Stamatiou, Y., Zwingelberg, H.: D7.1 Application Description for Students. Technical report, ABC4Trust (2012)
2. Bcheri, S., Goetze, N., Orski, M., Zwingelberg, H.: D6.1 Application Description for the School Deployment. Technical report, ABC4Trust (2012)
3. Brands, S.A.: Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy. MIT Press, Cambridge (2000)
4. Camenisch, J., Krontiris, I., Lehmann, A., Neven, G., Paquin, C., Rannenberg, K., Zwingelberg, H.: D2.1 Architecture for Attribute-based Credential Technologies. Technical report, ABC4Trust (2011)
5. Camenisch, J., Lysyanskaya, A.: An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In: Pfitzmann, B. (ed.) EUROCRYPT 2001. LNCS, vol. 2045, pp. 93–118. Springer, Heidelberg (2001)
6. Camenisch, J., Lysyanskaya, A.: A Signature Scheme with Efficient Protocols. In: Cimato, S., Galdi, C., Persiano, G. (eds.) SCN 2002. LNCS, vol. 2576, pp. 268–289. Springer, Heidelberg (2003)
7. IBM Research Zürich Security Team. Specification of the Identity Mixer cryptographic library, version 2.3.4. Technical report. IBM Research, Zürich (February 2012)
8. Verheul, E.R.: Self-Blindable Credential Certificates from the Weil Pairing. In: Boyd, C. (ed.) ASIACRYPT 2001. LNCS, vol. 2248, pp. 533–551. Springer, Heidelberg (2001)
9. Vullers, P., Alpár, G.: Efficient Selective Disclosure on Smart Cards Using Idemix. In: Fischer-Hübner, S., de Leeuw, E., Mitchell, C. (eds.) IDMAN 2013. IFIP AICT, vol. 396, pp. 53–67. Springer, Heidelberg (2013)