Mobile Devices to the Identity Rescue

Gergely Alpár[⋆1,2] and Maarten H. Everts[⋆⋆2]

[1] Institute for Computing and Information Sciences
Radboud University Nijmegen, The Netherlands.
gergely@cs.ru.nl
[2] TNO, The Netherlands.
maarten.everts@tno.nl

Abstract Identity management is defined as the set of processes related to identity and access information for the whole identity life cycle in a system. In the open internet users need new methods for identity management that supply reliable authentication and sufficient user control. Currently applied methods often lack a proper level of security (*e.g.*, passwords) and privacy (*e.g.*, diverse processing of personal data).
A personal smart card and a personal smart phone can communicate using near-field communication (NFC). This allows users to apply their smart phone as a personal semi-trusted smart-card reader. For applications such as authentication, this `Trusted Couple` can then be used in a secure and intuitive way, like a remote card reader. As attribute-based credentials (ABCs) can efficiently be implemented on tamper-resistant smart cards with the current technology, we can achieve a more privacy-friendly and more flexible way of not only authentication but also role-based access control or management of personal information. In this paper we describe how a `Trusted Couple` can solve security, privacy, and usability problems in identity management.

Keywords: attribute-based credential, smart card, NFC, mobile phone, identity management

1 Introduction

Identity management in our digital society is non-trivial. The traditional way of organisations to provision and manage identities is mostly not applicable across multiple domains and on the internet. There is currently no clear solution for users to manage their identities when carrying out transactions with different entities in a secure, privacy-friendly, and user-friendly manner [13,14,2]. As a result, typically service providers themselves manage all personal data about their customers now; however, this may not be desirable. The current practice of identity silos raises several problems for the data controller (i.e., the service provider, in this case):

[⋆] Partly supported by the research program Sentinels as project ‘Mobile IDM’ (10522). Sentinels is being financed by Technology Foundation STW, the Netherlands Organisation for Scientific Research (NWO), and the Dutch Ministry of Economic Affairs.

[⋆⋆] Supported by the THeCS project as part of the Dutch national program COMMIT.

- Liability: in terms of data protection regulation;
- Economic: in terms of costs of authentication, authorisation, and keeping data up-to-date;
- Security: in terms of technical and procedural data protection, and prevention of phishing;

as well as for the users:

- Usability: in terms of the management of appropriate passwords and the use of many different authentication methods at various service providers;
- Privacy: in relation to the fact that personal data is processed by different companies in an opaque manner.

Practical solutions, with increasing adoption, exist in the form of network-based (centralised) identity management (e.g., SAML, OpenID). In such systems verifiers acquire identity information about users directly from the identity providers. Thus, this requires identity providers to be constantly online, resulting in security and privacy risk.

In contrast, attribute-based credentials (ABCs) [3,6,7,8,9] solve many of the identity-management problems without the need for the identity provider to be online at all times as it is not involved when a user interacts with a service provider. However, despite the promising properties of ABCs, building a practical system based on ABCs poses additional challenges in finding the appropriate trust models together with practical and intuitive user interaction.

Technological advances can support a transition towards user centricity in identity management [4]. The number of people owning NFC-enabled (see Section 2.3) smart phones[3] with internet access is increasing. Having a trusted smart card with a contactless communication interface, users can use their mobile phones as a smart-card reader to facilitate communication between the card and potentially remote verifiers (service providers). In this paper we argue that two personal devices, a tamper-resistant smart card that holds ABCs and an NFC-enabled smart phone, can constitute the proper user-controlled platform for authentication, for exchange of user attributes between identity providers and verifiers, and for managing personal digital information.

Our contribution is threefold. First, in Section 2 we describe a mechanism that enables a mobile phone to establish a channel with a web server that facilitates communication between a smart card and an authentication service. The process is simple and intuitive, moreover, it requires a user's explicit control over data release. Second, as this mechanism can host attribute-based credential technology, constituting a `Trusted Couple`, we study its possible, diverse applications. It supports not only secure and privacy-friendly authentication, but also personal attribute management and credential issuance. Third, recognising the strength of the setup, we show how ABCs and the `Trusted Couple`

[3] Smart phone brands that deliver NFC-enabled devices include Acer, Asus, BlackBerry, HTC, LG, Motorola, Nokia, Samsung, Sony, Vertu. `http://www.nfcworld.com/nfc-phones-list/`, accessed on March 14th, 2013.

can solve general identity management problems. These contributions bridge the gap between cryptography (theory, implementation) and deployment.

The rest of the paper is organised as follows. First, in Section 2 we give conceptual and technical background for attributes, ABCs, and the required wireless technologies. Second, having these tools, we can define a `Trusted Couple` in Section 3.1 and describe applications in Section 3.2; this includes authentication through a channel that enables remote card reading. Next, Section 4 gives an account of solutions for identity management problems. Finally, Section 5 concludes the paper with technical alternatives for the `Trusted Couple` and possible further research directions.

2 Preliminaries

Attribute-based credentials can be stored and deployed using mobile devices, and they motivate the introduction of a `Trusted Couple`. In this section the necessary underlying concepts and technologies (attributes, ABCs, NFC, and QR-codes) are discussed.

2.1 Attributes

An *attribute* in the context of this paper is a property or a qualification that holds for an individual. An *identity* of an individual within a scope can be considered as a set of his attributes. An attribute can be *identifying* or *non-identifying.* A name, a social security number, or a bank account number is identifying and, in fact, they are often used as identifiers. Non-identifying attributes can be the name of a city of residence or the boolean variable ‘over 18’, though in some specific scopes these attributes may be identifying.

A simple identity management model comprises three participants: an identity provider (or issuer), a service provider (or verifier), and a user. Although on an abstract level general identity management and ABC systems can be explained similarly (see Figure 1–(1)), the message flow in the latter case is quite different. Unlike in other conventional identity management in which the identity provider has a central position, the user is in the centre of the communication. A user can receive (a) certified attributes from issuers, and later show (b) the relevant ones to service providers (SPs) in order to authenticate—and eventually, to access some service or resource. The SP has to rely on the IdP that the attributes are true for the user; this trust assumption is the relation denoted by (c). We note that in conventional identity management the identity provider takes part of the actual authentication/authorisation process and it exchanges data with the service provider on channel (c).

2.2 Attribute-Based Credentials

An attribute-based credential [6,7,9] (ABC) is a cryptographic container of some attributes signed by an issuer who is entrusted with the task of attesting to and signing the credential. A name, a gender, and a date of birth are examples of attributes in an 'identity' credential, possibly issued by a governmental organisation. Further examples include (1) a 'loyalty' credential issued by an airline company consisting of a customer identifier, the current number of loyalty points, and a loyalty level attribute, or (2) an 'employee' credential consisting of a photo, an employee code, and some access right attributes issued by an employer.

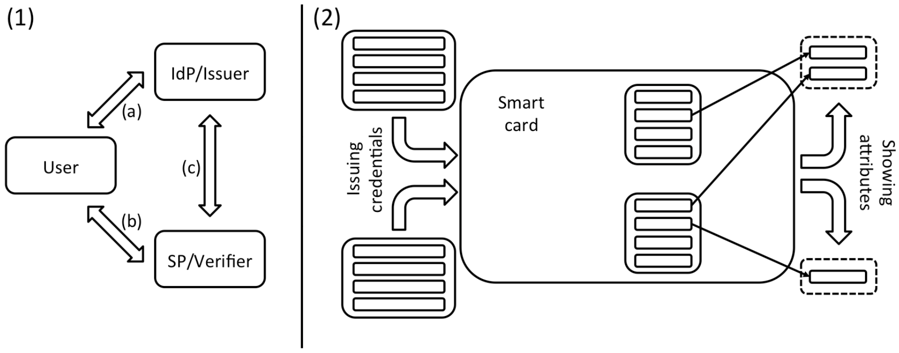

Figure 1. (1) The general model of identity management. (2) An abstract view of attribute-based credentials on a smart card and selective disclosure of attributes.

Within the IRMA project[4] a secure ABC belonging to an individual is bound to a smart card which is, in turn, bound to its owner. Therefore, a credential or an attribute cannot be modified or transferred to a different user. Also, unlike in the physical world, attributes in a particular credential can be shown independently of each other using a so-called *selective disclosure* protocol; see Figure 1–(2). The processes of issuing credentials and showing attributes can be separated not only in time and place, but also in terms of cryptographic protocols: Issuer unlinkability and multi-show unlinkability make issuing and showing instances computationally unrelated by the underlying cryptographic techniques. The user-controlled communication operates as follows. After appropriate authentication and data verification (which may include attributes from the card), an issuer can issue a credential to a user's smart card. Later the card owner can show attributes from credentials on her card for authentication purposes to a service provider. Only relevant attributes (determined by some policy mechanism) needs to be revealed in this process.

[4] The IRMA technology is a pilot project and a proof of concept employing an efficient card implementation of Idemix attribute-based credentials [20]. IRMA stands for 'I Reveal My Attributes'; further information can be found on its web site: `https://www.irmacard.org/`. The current study is also based on the experiences in the IRMA project.

2.3 NFC and QR Codes

Two additional technologies are required to create a Trusted Couple from a phone and a smart card: NFC and QR codes.

Near-field-communication (NFC) is an extension of radio-frequency identification (RFID) and it provides a broader range of functionalities; see technical details and references in [1]. Applications using NFC in mobile devices include data exchange and payment. Several recent research projects propose to use NFC-enabled phones as card readers. While Alpár et al. [1] already consider the use of cards with ABCs, their primary focus is online banking. Morgner et al. [15] use an NFC-enabled mobile phone as a traditional card reader connecting it to a PC by a USB cable. Both papers argue that these devices are increasingly available; this is also in line with recent forecasts[5].

A QR code is a two-dimensional barcode that encodes text in a way that is easily scanned by machines; in particular using a camera included in most mobile phones. QR codes can be efficiently generated, making them available in applications with for instance ad hoc URLs. We note that unlike most of the technologies enabling communication between devices, scanning a QR code requires an intentional action from the user. This is particularly important in a world where wireless networks are ubiquitous. Furthermore, as shown in Section 3.2, a QR code enables easy connection from a browser session on a PC to a smart card (using a mobile phone) without problems related to firewall protection or mobile device discovery.

3 The Trusted Couple

We state that by combining a smart card and a mobile phone (Trusted Couple), the use of ABCs can become practical. To illustrate this, we describe three applications. But first, we specify what this Trusted Couple entails.

3.1 A smart card and a mobile phone

A Trusted Couple is defined as the combination of a smart card and a mobile phone that meet the following requirements.

- *Contactless smart card.* A smart card is assumed to be tamper resistant, so it cannot be cloned and secret values cannot be extracted from it. Furthermore, a smart card carries a working implementation of attribute-based credentials. It is possible to issue ABCs on the card and selectively disclose attributes from these credentials. A card holder is required to enter her PIN during a credential verification protocol. Finally, a card has a contactless interface that enables it to communicate with the phone.

[5] According to NFC World and API Research, 400 million NFC-enabled mobile devices are predicted to be delivered in 2013 and nearly 2 billion such devices are expected to be shipped in 2017. [21]

- *NFC-enabled mobile phone.* Using its NFC-interface, a phone can communicate with the smart card. In most applications, the phone is also required to have internet access to communicate with a remote server and to have a camera to scan QR codes. (In fact, this device does not need to be a phone, it can also be for example a tablet with Wi-Fi internet connection.) A phone is semi-trusted: it is assumed not to leak the PIN and attribute information. Note, however, that even if this information leaks, it does not enable a potential attacker to produce proofs about the attributes. In particular, an attacker needs a smart card to perform a full-fledged attack, which renders large-scale and remote attacks infeasible.

In summary, a phone acts here as a semi-trusted reader for the trusted smart card that helps in communicating both with the card owner and other entities (verifiers, issuers) in the identity management scope.

3.2 Running the `Trusted Couple` in Practice

Assuming the security and privacy properties of the attribute-based credential technology and their proper implementation (*e.g.*, [16,19,20]), we can design new applications using the `Trusted Couple`.

Authentication Depending on the set of attributes that is disclosed in a verification protocol, we can distinguish two types. On the one hand, an identifying set of attributes provides a new, secure, and user-friendly way of authentication. For instance, a social network site or a governmental administration webpage can use the method as an alternative to logging in using a username and a password. On the other hand, non-identifying sets of attributes basically generalise the notion of role-based access control in a privacy-friendly manner. Attributes can carry general and specific information about the identity of a user and the relation between a user and her context.

Figure 2 shows an overview of such an authentication process, in which an NFC-enabled mobile phone becomes a *remote card reader* that is trusted by the user. The user visits (1) a webpage of a service provider (SP) that requires authentication. The SP's webpage presents a QR code (2). The user scans it (3) using her mobile phone. The QR code contains a URL that binds the browser's session to the phone. The mobile phone sends a request to that URL (4) to start a selective disclosure protocol and subsequently, receives the commands from the SP (5) to be sent to the smart card. The mobile phone asks the user to enter her PIN on the phone, and sends the commands to the smart card (6) through NFC. The smart card evaluates the request and verifies the PIN. The responses (in essence a fresh zero-knowledge proof about the attribute(s)) of the smart card (7) to the commands are then sent back to the SP (8) by the phone. Based on these responses the SP can decide whether or not the user should be given access to the resource. This is finally relayed back to the browser session on the PC (9) and in case of a successful authentication, the user is allowed to proceed to the service.

The use of a QR-code in this process not only binds the browser's session to the phone, it also requires a deliberate user action. Together with the application of the smart card, these conducts give the user a sense of control.

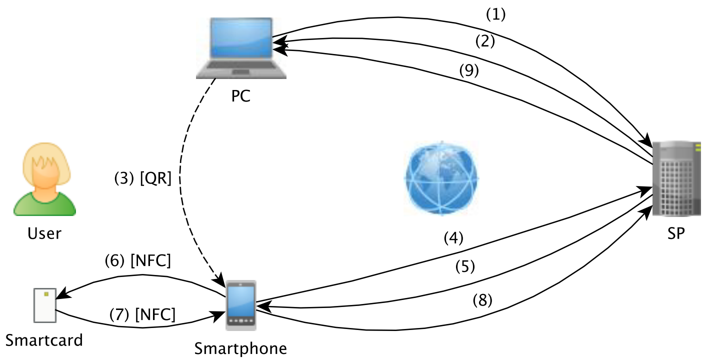

Figure 2. Online authentication with the `Trusted Couple`.

Credential issuance The verification process above can also be followed by a credential-issuing protocol in which case the SP is an issuer. We note that if the authentication is non-identifying, such a credential issuing process is in accord with the original notion of anonymous credentials [11,8].

To motivate anonymous use cases, we give an example. Consider the following privacy-friendly on-line shopping procedure. A user, already having an 'age' credential with the attribute 'over 16' and a 'student card' credential with the attribute 'university student', can buy an age-restricted 'festival ticket' credential with a student discount. Within the same secure session (not described, only assumed here), a verification procedure is extended with a subsequent issuance of a new credential. The resulting ticket credential may consist of the following attributes: serial number, beer coupon, start date, end date. The serial number makes sure that a ticket at the venue cannot be used more than once.

Card and Attribute Management A smart card is trusted, but its content is usually not visible for its owner. However, because of the flexibility and variability of attribute-based identity management, it is desirable for a user to see what credentials she owns or when those credentials expire. Additionally, a user may also want to verify log entries on a smart card showing all credential issuance and verification events.

A `Trusted Couple` enables the owner to see the whole content of the card on the display of the phone. This application assists the management (*e.g.*, read, delete) of personal information and the possibility of checking a posteriori the use of a personal card.

4 To the Rescue in the Identity Crisis

According to [2], the current identity management practice, having a large number of unsolved problems, is an identity crisis. Similar concerns are presented in [10,13,12,14,18]. This section describes how a `Trusted Couple` can solve fundamental identity management problems.

By means of a `Trusted Couple`, attribute-based identity management is becoming practical which helps to realise the benefits of ABCs.

- First of all, the verification process of attributes does not *include the identity provider*; thus, security and privacy functionalities improve because (1) the IdP is not a *single point of failure*; (2) the IdP does not *know all user transactions*. As a result, no *surveillance* can be conducted based on such data records.
- Secondly, *phishing*, a major problem in online security in which users reveal secret authentication information to malicious parties, can efficiently be prevented. As authentication in our system relies on zero-knowledge proofs about secret keys and attributes residing on a tamper-resistant smart card, there is no efficient large-scale phishing possible. Also, as cards are assumed to be unclonable, *card owners have control over activities* of their cards. This also means that *identity fraud* becomes much harder.
- Thirdly, ABCs provide un*linkability across scopes*. In particular, showing credentials cannot be linked to their issuance protocols or other showing instances. This prevents tracing users, turning a system into *mass surveillance*, or construct combined profiles about them.
- Next, selective disclosure, a major functionality of ABCs, allows for revealing a minimally required amount of personal information during transactions. Furthermore, the attribute management is mainly carried out at the user's device, which is the lowest level and the most direct way in an identity system. Therefore, we achieve *proportionality* and *subsidiarity*. This is also in accordance with the European principle of data minimisation (Directive 1995/46/EC).
- Lastly, as attributes can express not only identifiers and roles but also such abstract concepts as *membership* and *ownership*, attribute-based identity management can achieve the new *paradigm of "is (s)he entitled?" to access a resource instead of "who?" accesses it.*

Not only do the benefits of attribute-based credentials become available, but also an important principle can be fulfilled. Having the `Trusted Couple`, the system achieves the law of *location independence*, defined in [2] as

> *The identity system must allow a user to create, manage, and use his identity independently of his current location and current device in use.*

First, users are not bound to one specific, static computer when they access different services. Even a potentially untrusted public PC can be suitable for users to log in to a system using their `Trusted Couple` as the authentication process does not require the transfer of secret information. Moreover, such a PC does not need any special hardware or software components, or additional drivers. In particular, smartcard readers are still not very common. Second, users do not have to involve their identity providers or any special infrastructure thereof when signing in to services.

In summary, ABCs provide security for verifiers and privacy for the card owner while the `Trusted Couple` provides independence for users from particular computers, systems, or identity providers.

5 Conclusion

In this paper we described how a `Trusted Couple` (a trusted smart card and a semi-trusted mobile phone) can help solving challenges in the current identity crisis. As smart cards become increasingly powerful, ABCs are expected to be available in many more applications. At the same time, more and more mobile phones are equipped with NFC chips. The ubiquity of these technologies makes the described setup and the applications truly practical and user friendly. As a result, processing of personal data and authorisation on the internet and in a broader context may become more secure and more privacy friendly.

Technological Variations We briefly enumerate some possible alternatives and extensions to a `Trusted Couple`. (1) A *card reader* is an obvious alternative to a phone. However, it provides only a limited set of functionalities compared to a smart phone [15] and it entails an additional tool for users to carry. (2) As an improvement, the relation between the card and the phone can be reinforced by *binding* the devices within a `Trusted Couple`. This requires an additional shared secret key between the phone and the card. (3) Mobile devices are expected to provide *trusted states* in the near future; see ARM's TrustZone[6] and Intel's TXT[7]. Mobile phones in such a trusted state, being verifiably malware-free, can be used as a reliable PIN pad. (4) Besides a mobile phone's trusted state, phones may provide *reliable functionalities for storage and cryptographic operations*. Thus, they can act like a smart card. However, two problems then arise: (a) What can create the link between the phone's trusted and untrusted states? (b) How does the trust assumption change if the `Trusted Couple` merges into one device? Bichsel et al. [5] propose two protocols in this setup but in a different model: In their proposal, the local PC is more trusted and both directions of the zero-knowledge proofs are conveyed by QR codes. (5) Another trend is that *smart cards may be soon equipped with a display and a keyboard*[8]. Since smart

[6] `http://www.arm.com/products/processors/technologies/trustzone.php`

[7] `http://software.intel.com/en-us/articles/intel-trusted-execution-technology`

[8] `http://www.nidsecurity.com/microsite/mastercard/`

cards are not yet expected to have other communication interfaces (*e.g.*, camera, any internet access), it is not clear how they can be applied in online scenarios. And again, merging the device that carries ABCs and the device that provides user-interaction changes trust assumptions.

Further Research Other directions in research and development include *more direct and user-friendly control* when personal information is exposed. A system of verifier certificates and a posteriori log monitoring are possible using the current IRMA technology [3,20], but an intuitive selection of revealed attributes in particular applications is not yet provided to the user. The IRMA technology provides ways to separate different personas (*e.g.*, citizen, social web, financial, academic, etc.) of the same user by arranging credentials in different sets on a card or by applying multiple cards. After a proper analysis, the question raised by [2] *"How many identities should a user have?"* could also be answered.

Finally, future research also can explore how trust assumptions modify the flow of procedures in applications. First, emerging technologies can *change the* `Trusted Couple` *model* as described above. Second, phones can *enforce and control policies* in a more powerful way than a card (of much more limited resources) can. Third, a mobile phone, communicating with its environment, could decide about *in what mode it operates depending on its context* (*e.g.*, it behaves differently in a bank or at home than in the street). Using this feature, a phone can act adaptively when assisting ABC verification proofs. The latter two questions closely relate to contextual integrity and thus, they can contribute to even further improve privacy [17].

References

1. Gergely Alpár, Lejla Batina, and Roel Verdult. Using NFC Phones for Proving Credentials. In Jens B. Schmitt, editor, *MMB & DFT 2012*, LNCS 7201, pages 317–330. Springer, 2012.
2. Gergely Alpár, Jaap-Henk Hoepman, and Johanneke Siljee. The Identity Crisis. Security, Privacy and Usability Issues in Identity Management. *Journal of Information System Security*, 8(3), 2013.
3. Gergely Alpár and Bart Jacobs. Credential Design in Attribute-Based Identity Management. In Ronald Leenes, editor, *TILTing Perspectives*, 2013.
4. Abhilasha Bhargav-Spantzel, Jan Camenisch, Thomas Gross, and Dieter Sommer. User centricity: a taxonomy and open issues. *Journal of Computer Security*, 15(5):493–527, 2007.
5. Patrik Bichsel, Jan Camenisch, Bart Decker, Jorn Lapon, Vincent Naessens, and Dieter Sommer. Data-minimizing authentication goes mobile. In Bart Decker and DavidW. Chadwick, editors, *Communications and Multimedia Security*, volume 7394 of *Lecture Notes in Computer Science*, pages 55–71. Springer Berlin Heidelberg, 2012.
6. Stefan A. Brands. *Rethinking Public Key Infrastructures and Digital Certificates: Building in Privacy.* MIT Press, Cambridge, MA, USA, 2000.

7. Jan Camenisch, Ioannis Krontiris, Anja Lehmann, Gregory Neven, Christian Paquin, Kai Rannenberg, and Harald Zwingelberg. D2.1 Architecture for Attribute-based Credential Technologies. Technical report, ABC4Trust, 2011.
8. Jan Camenisch and Anna Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In *Advances in Cryptology – Eurocrypt 2001*, pages 93–118. Springer-Verlag, May 2001.
9. Jan Camenisch and Anna Lysyanskaya. A Signature Scheme with Efficient Protocols. In Stelvio Cimato, Giuseppe Persiano, and Clemente Galdi, editors, *Security in Communication Networks*, volume 2576 of *LNCS*, pages 268–289. Springer Berlin / Heidelberg, 2003.
10. Kim Cameron. Laws of identity. `http://www.identityblog.com/stories/2004/12/09/thelaws.html`, may 2005.
11. David Chaum. Security without identification: transaction systems to make big brother obsolete. *Communications of the ACM*, 28:1030–1044, October 1985.
12. Rachna Dhamija and Lisa Dusseault. The seven flaws of identity management: Usability and security challenges. *IEEE Security & Privacy*, 6(2):24–29, 2008.
13. Audun Jøsang, Muhammed Al Zomai, and Suriadi Suriadi. Usability and privacy in identity management architectures. In *Proceedings of the fifth Australasian symposium on ACSW frontiers-Volume 68*, pages 143–152. Australian Computer Society, Inc., 2007.
14. Eve Maler and Drummond Reed. The Venn of Identity: Options and Issues in Federated Identity Management. *IEEE Security & Privacy*, 6(2):16–23, 2008.
15. Frank Morgner, Dominik Oepen, Wolf Müller, and Jens-Peter Redlich. Mobile Smart Card Reader Using NFC-Enabled Smartphones. In Andreas U. Schmidt, Giovanni Russello, Ioannis Krontiris, and Shiguo Lian, editors, *Security and Privacy in Mobile Information and Communication Systems (MobiSec)*, volume 107 of *LNICST*, pages 24–37. Springer, 2012.
16. Wojciech Mostowski and Pim Vullers. Efficient U-Prove implementation for anonymous credentials on smart cards. In George Kesidis and Haining Wang, editors, *Security and Privacy in Communication Networks – SecureComm 2011*, volume 96 of *LNICST*, pages 243–260. Springer-Verlag, 2011.
17. H. Nissenbaum. Privacy as Contextual Integrity. *Washington Law Review*, 79(1):119–158., February 2004.
18. Andreas Pfitzmann and Katrin Borcea-Pfitzmann. Lifelong privacy – privacy and identity management for life. In *Privacy and Identity Management for Life, 5th IFIP/PrimeLife, International Summer School*, pages 1–17. Springer, 2010.
19. IBM Research Zürich Security Team. Specification of the Identity Mixer cryptographic library, version 2.3.4. Technical report, IBM Research, Zürich, February 2012.
20. Pim Vullers and Gergely Alpár. Efficient Selective Disclosure on Smart Cards Using Idemix. In Simone Fischer-Hübner, Elisabeth de Leeuw, and Chris Mitchell, editors, *Policies and Research in Identity Management (IDMAN)*, IFIP AICT 396, pages 53–67. Springer, 2013.
21. NFC World. Forecast (last accessed: September 10, 2013). `http://www.nfcworld.com/technology/forecast/`.