Identity Deployment and Management in Wireless Mesh Networks

Leonardo A. Martucci[1], Albin Zuccato[2] and Simone Fischer-Hübner[1]

[1] Karlstads University, Department of Computer Science
{leonardo.martucci, simone.fischer-huebner}@kau.se
[2] TeliaSonera, R&D Informations Security
albin.zuccato@teliasonera.com

Abstract. This paper introduces the problem of combining security and privacy-friendly provisioning in wireless mesh network environments. We present a set of non-functional requirements for a privacy-friendly identity management (IdM) system suitable for wireless mesh networks and derive another set of security and privacy properties for digital identifiers to be used in such networks. Later, we compare two existing identifiers, anonymous attribute certificates and anonymous credentials, and verify if any of those conforms to our set of defined properties. A business model and some business cases are presented to support and justify the need for a privacy-friendly IdM system not only from the security and privacy perspective, but also from a business-enabler perspective.

1 Introduction

Mesh networking is an elegant and affordable technical solution for extending the range and the provisioning of services that are deployed in an infrastructured network behind an wireless access point, such as a private network or even the Internet. The extension of the radio range of access points is achieved using nodes called wireless relays. Wireless relays can be mobile or stationary, and usually belong to telecommunication service provides (TSP). Ad hoc routing protocols are used when the wireless relays are mobile, especially if mobile clients can operate as intermediary nodes to forward packets from users that are located beyond the radio range of a wireless access point or a wireless relay. Therefore, a mobile client can also operate as wireless relay to other clients.

In Figure 1, we illustrate a wireless mesh network scenario. There are many research problems shown in this figure. In this paper we focus the technical and economical problems arising from the presented scenario. We divided those problems into three areas:

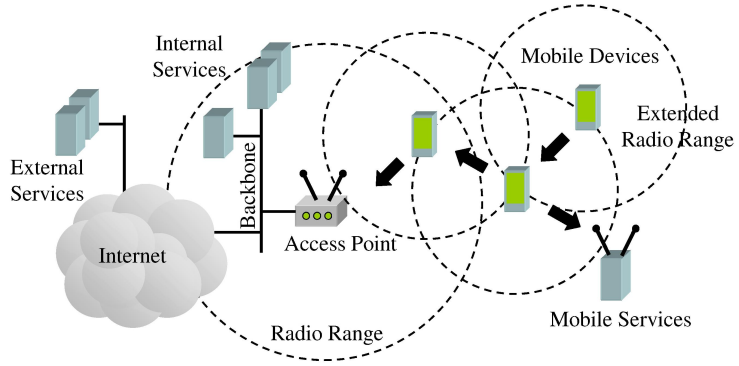

Fig. 1. A wireless mesh network with one gateway connected to the backbone of the telecommunication / service provider and also to the Internet, and one wireless relay connecting 3 nodes through a mobile ad hoc network. Services are provided directly from the provider's backbone, from the Internet and also from the mobile network.

- performance aspects regarding hybrid ad hoc routing, QoS, transport layers, power-efficiency, and roaming between relays for instance[1]. In this paper we do not deal with performance aspects;
- the security and privacy aspects, especially on the problems of identity management, user untraceability against other network participants and other privacy and security problems arising from lack of identification or Sybil attacks [8]. The security and privacy aspects are the main focus of this work;
- the economic and business problems involved, especially regarding the business models and business cases involved and how to stimulate and reward the cooperation among mobile nodes. In this paper we present a business model and some business cases regarding services that may be deployed by a TSP.

The organization of the paper is as follows. Section 2 sets the objective of this paper and stresses the importance of selecting proper identifiers when the provisioning of privacy is one of the goals of a TSP. In Section 3 we present the security threats in a wireless mesh network scenario, the trivial solution and the implications to users' privacy. Section 4 presents the basic structure of an identity management system, the privacy rights of each entity and the requirements for the deployment of digital identifiers in a wireless mesh scenario. Section 5 discusses the available techniques to issue anonymous identifiers, while Section 6 presents the business model of the system. Finally, Section 7 concludes the paper.

[1] The IEEE 802.11 task group S is currently working on the standardization for wireless mesh network based on the IEEE 802.11 standard [10].

2 Digital Identifiers and Privacy

User privacy could be largely improved simply by distributing non-revocable anonymous credentials to end-users. However, for the TSP point of view, complete anonymous access to the network is usually undesirable for several reasons, such as: billing, impossibility of identifying malicious insiders (i. e., subscribed users misbehaving in the network into an impossible problem) and, in a wireless mesh network scenario, it is hard to reward subscribers collaborating into the network (e. g., for actions such forwarding packets from other users in the mobile ad hoc network).

The TSP needs to identify its subscribers for the purposes of billing and network security, nevertheless it is also a goal of the TSP to protect its users against privacy abuses coming from malicious insiders and outsiders i. e. user anonymity against other network users, but not towards the TSP. Revocable anonymous identifiers are a possible solution for protecting the TSP's customers privacy in a wireless mesh network scenario.

The goal of this work is the specification of these revocable identifiers that allows the identification of users by the TSP, but not does not permit a user to uniquely identify another network user. Therefore, the TSP is able to deploy security services (e. g., authentication, authorization, access control, accounting) to protect the network against malicious users and attacks, such as a Sybil attack, and provide user privacy simultaneously. We describe the system requirements, suggest an adequate solution and evaluate its advantages and disadvantages.

The first step for the provisioning of anonymity towards other network users is to distribute untraceable identifiers to the network subscribers. Despite the property of being anonymous apparently contradicts the possession and disclosure of a unique identifier to other parties, this is not true for deploying privacy in network environments where users may join or leave as they wish, such as a wireless network. Unique identification is a requirement for the provisioning anonymity. Without protection against identity-based attacks, the network may be compromised by Sybil attacks[2] [8]. The need for unique identification for the provisioning of anonymity in wireless network environments is referred as the identity-anonymity paradox [12].

Therefore, the TSP has to distribute network identifiers that will be used for the provisioning of anonymity against other network users[3]. Preferably, those identifiers should also allow pseudonimity. Pseudonyms are valuable for the

[2] A Sybil attack occurs when a malicious user influences the network by controlling multiple logical identifiers from a single physical device. The distribution of identifiers (by a trusted third party) that guarantee the one-to-one relationship between logical identifiers and network devices can prevent Sybil attacks.

[3] In this paper we assume that the data link and IP addresses also change when the electronic identifier changes. We disregard other forms of electronic stalking using physical or application layer information.

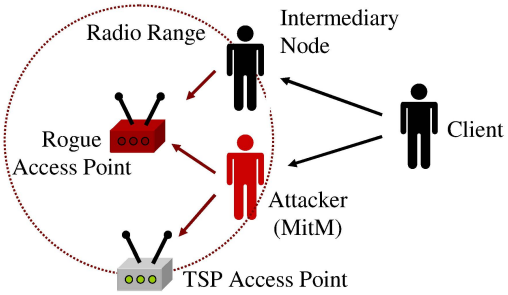

Fig. 2. Possible threats related to impersonation and man-in-the-middle (MitM) attacks in wireless mesh networks. In the figure, a client has her data being forwarded either by a honest intermediary node to a rogue access point or by an attacker towards a rogue access point or to an authentic access point that belongs to the TSP.

provisioning of personalized network services, especially when those services are provided by third party service providers.

The Pfitzmann and Hansen terminology [13] is followed in this paper for following terms: anonymity, unlinkability and pseudonimity. The term untraceability is used to describe the property of a subject to be protected against electronic stalking (i. e., tracking) by an (omnipresent) attacker eavesdropping the wireless network.

3 Security Threats, the Trivial Solution and Privacy

The threats involved in this scenario include privacy and network security threats. Network security threats include impersonation and man-in-the-middle attacks, as depicted in Figure 2. In an ad hoc network, the total absence of identification may lead to a Sybil attack [8], since honest users are not able to detect that the relationship between logical identifiers (e. g., IP addresses) and physical devices is actually one to one. In the absence of trustable identification, network security services, such as authentication, authorization and access control, cannot be guaranteed, and those security threats can affect the network performance and functionality, leading to denial of services attacks that deny the usage of the network by honest users [12].

Preventing the security threats described could be trivially achieved with the deployment of a Certification Authority (CA) and authentication servers (AS) on the TSP side (using two-way authentication), distribution of X.509 public key certificates [11], mutual authentication and end-to-end secure channels between network entities. Users and servers would then be able to univocally identify other network entities and verify the authenticity of their communication partners. There are many details involved even within this trivial solution, such as: decisions regarding the end-to-end secure communication protocol suite between users and servers, and users and users; the authentication protocols and

data link security between wireless relays and access points; the use of on upper layer encryption, such as VPN connections, for users' transactions; and the security properties of the ad hoc routing algorithms (to be used in the extended radio range).

However, the presented solution does not address the privacy threats. Privacy threats include profiling, monitoring and stalking of devices using the provided identifiers as source of information[4]. X.509 public key digital certificates are not privacy-friendly since it is possible to track users using the serial number information of those certificates. Data link and network layer information (i. e., $\{MAC, IP\}$ pairs) could be used as privacy-friendly identifiers because they can be changed regularly [9], but this information cannot provide trustable identification [12] and makes the system vulnerable to Sybil attacks. Thus, the usage of privacy-friendly certificate-like identification, issued by a Trusted Third Party (TTSP), is a solution for both privacy and security threats in a wireless mesh network scenario.

4 Identities and Identity Management System

The identity management (IdM) system in the wireless mesh network scenario follows the general three type categorization for IdM [1]: *account management*, *profiling* and *management of own identities*. The account management – for authentication, authorization and accounting (AAA) purposes – is done by the TSP. The management of own identities is performed by each network user, who is able control her partial identities using an IdM tool. Profiling is done by the service providers (SP), especially for the purpose of service customization and / or customer relationship management. Therefore, identifiers are used in different ways in a wireless mesh network.

A privacy-friendly wireless mesh network must offer the following non-functional requirements for users and other parties during the life-cycle of a user's identifier[5] into the system:

a) users may remain anonymous against other users.
b) users may choose to be anonymous against a SP, or to be able to reuse pseudonyms. Pseudonyms may be used to obtain personalized services and are usually associated to the disclosure of a user's partial identity.
c) privacy-friendly does not only mean the TSP protecting the users' identity and identifiers, but also that users have control over their personal information and can share it if they wish so.

[4] Some threats related to physical and routing layer attacks are not going to be considered in the scope of this paper. Such threats include network jamming and radio device tracking using radio fingerprints and signal to noise (S/N) ratio techniques.

[5] The life-cycle of a user's identifier starts when the identifier is created by the IdM system, eventually hosted by the TSP, and ends when the identifier expires, is revoked by the IdM system or deleted by the user.

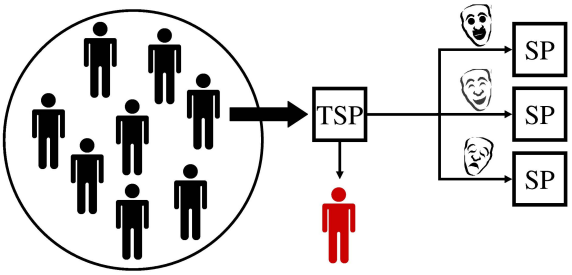

Fig. 3. Users are anonymous among their peers and at the same time are uniquely identified by the TSP and may have different identities towards different SP.

d) TSP can identify users and eventually revoke their identifiers, thus these identifiers cannot be used any longer, and also disclose user anonymity if necessary[6].
e) TSP must be fair and trusted regarding the disclosure of identities, and the rules for doing so must be well-defined and well-described. The TSP duties and rights on handling personal data are regulated according to the legislation regarding data protection[7].
f) SP may retain and process (anonymized) users' related information according to the applicable legislation.

Thus, a user has many identifiers: a single identifier towards the TSP, one or more pseudonyms towards different SP, and one-time identifiers (transaction pseudonyms) towards other users. Figure 3 provides an illustration of the multiple identifiers described in this paragraph. The security and privacy properties for digital identifiers in a wireless mesh network scenario are:

i) Identifiers must be unique. This is needed to guarantee the 1-to-1 relationship between logical identifiers and physical devices, especially in the extended radio range of the wireless mesh network. Uniqueness is needed for preventing Sybil attacks [8] in the wireless mesh network.
ii) Identifiers must be anonymous against all other entities, except the TSP. This is required for the provisioning of user untraceability against other network entities (e. g., other mobile users, SP).
iii) Re-identification of anonymous identifiers must be supported. The TSP shall be able to identify users and eventually revoke users' identifiers to disclose their anonymity and prevent them to be used any longer.
iv) It must be possible to authenticate peer devices without the interference of the TSP's AS (running in the TSP's AAA servers). This is needed for

[6] The disclosure of user anonymity is needed for pinpointing malicious users and for the provisioning of some network security services, such as authentication, authorization and accounting (AAA) for instance.
[7] In Europe, this includes the Data Protection Directive 95/46/EC and the Directive 2002/58/EC on privacy electronic communications.

supporting mobile ad hoc services or peer-to-peer (P2P) applications that can be provided without the support of the TSP's telecommunication infrastructure.

A simplified network topology depicting the basic infrastructure and services supported or connected to the TSP is shown in Figure 4.

5 Anonymous Credentials in a Wireless Mesh Network

The usage of either anonymous attribute certificates (ATC) [2] or anonymous credentials [4, 5, 6] is recommended since they might provide untraceability to the user if used correctly. Untraceability is provided by preventing unauthorized identification of network clients by distinguishing multiple appearances of a given node into the wireless mesh network. Thus, each appearance of a user in the network must be unlinkable to a previous appearance. The set of potential attackers include other (colluding) nodes in the mobile ad hoc network or a SP.

ATC are based on zero-knowledge (ZK) proofs of knowledge[8] and are structured as a composition of a group certificate and an X.509 attribute certificate [11]. There are mechanisms associated with ATC that allow users' identities to be disclosed, traced or revoked by an identity escrow [2]. ATC do not offer guarantees to the 1-1 relationship between identifiers and devices (item "*i*" – Section 4) since there are no means to prevent or detect ATC sharing.

Anonymous credentials can be constructed using either blind signatures or ZK proofs. Anonymous credentials based on ZK proofs can, beyond providing anonymity, be used multiple times (multiple show) [6], be revocable [3] and can be built to detect sharing of credentials, as shown in [4]. Therefore, anonymous credentials have the potential to fulfill all the basic security and privacy requirements for identifiers in a wireless mesh scenario presented in Section 4.

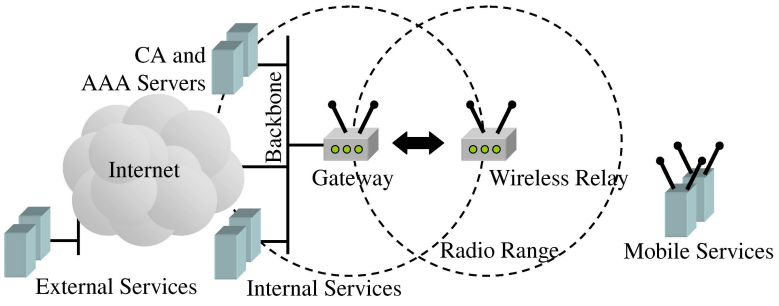

Fig. 4. The basic infrastructure provided by the TSP includes the wireless mesh network, CA and AAA servers and other internal and external services.

[8] ZK proofs of knowledge are interactive proofs in which the verifier learns nothing besides the fact that the statement that is proven is true [14, 7].

6 Business Model for Privacy-Friendly IdM

To discuss a business model for a privacy-friendly IdM system we have to clarify the general conditions in which such a model need to exist. The TSP's key assets are the following three: (*i*) its customers, (*ii*) its technical infrastructure, and (*iii*) its technical competence. For the further discussion the first two are of significance.

The customer is a utterly important asset for the TSP. To maintain customers' loyalty and trust significant resources are required from the TSP (i. e., customer relationship management). The TSP aims to protect and strengthen its customer relationships and is reluctant to put it at risk. A SP must not receive enough "identifying" information that allows it to deal with the TSP's customers directly. Customer satisfaction decreases with inappropriate handling of personal information. The TSP is interested to act in a privacy-friendly way, so that the customer is satisfied and do not consider to move to another TSP.

The second important factor is the network infrastructure (i. e., networking hardware). The TSP has to invest heavily into infrastructure to provide a broader range of services to more customers. Wireless mesh networks are a way to reach more customers (by extending the network range) without infrastructure investments. A drawback is that wireless mesh networks imply that the TSP loses the control over part of the network. From a security point of view, this loss of control requires that the operator (*a*) do its uttermost to maintain security by investing into security mechanisms and (*b*) informing the customer about the risk.

A customer's identity can be divided in partial identities that enable the customer and the TSP to use only a subset of the personal information for the purpose at hand. Partial identities can be far better tailored to the purpose of the SP and the TSP does not risk to lose control of its customer's identities. By deploying an IdM system the TSP allows its customers to control their partial identities. Moreover, an IdM is an value-added service that increases the market attractiveness of the TSP to keep and attract more customers, and also offers new business opportunities (e. g., the customer pays for the service, 3^{rd} parties pay for obtained information), which allow the creation of new income sources. The dilemma with market attractiveness effects is that they fade out over time as the competitors adapt them as well. This means they are very beneficiary in the beginning but are not reliable as income source. The business opportunities on the other hand allow to generate new income sources and we shall discuss some of them as business cases for privacy-friendly IdM. These business cases, which are presented in the following sections, are also viable requirement sources for the subsequent solution.

6.1 Business Case - IdM for Wireless Mesh Networks

Wireless mesh networking allows more customer to use the TSP network. This creates revenue from more user subscriptions (i. e., more customers are in range for using the service) and service usage (i. e., data traffic in the TSP network).

It is crucial that the parties are identifiable to guarantee some network security functions and also for billing / compensation payments and rewarding. The use of persistent identifiers can affect the privacy and risk the customers' privacy. Therefore, an IdM must be able to provide privacy-friendly identifiers that can be used to fulfill the requirements presented in Section 4.

6.2 Business Case - Distributed IdM Service

In this business case we assume that an operator charges for its IdM service. It is possible to charge different parties (e. g. the identity owner, active identity verifier) for the IdM activities that they consume. To be able to do that the IdM system has to support identity creation and validation activities. In addition value adding management functions (e. g. policy management for automatic identity use) should be provided to the user.

6.3 Business Case - Provide an IdM Infrastructure to 3^{rd} Parties

Many projects (e. g. smart home) would like to use the identity of the user to customize the service they offer. This implies that each service would need to collect and maintain identity information of the user which it does not need most of the time. The costs and risk involved with that can be omitted with a 3^{rd} party IdM. The operators role in this business case is to provide an IdM infrastructure that only delivers the personal information necessary for the service and encapsulates so that it is not linked to the identity. The difference to the business case above is that the operator not only provides a service via its own infrastructure but opens the infrastructure for others to provide their services upon it.

For instance, in an automobile example, starting a car engine should only be allowed upon the availability of a valid driver's license. The preferences for the adjustment of a car seat could be set using another identifier. And in the case of an accident it should still be possible to retrieve the driver's and passengers' identities and medical information (i. e. sensitive personal information). Naturally, the automobile could also hold this information – but it would need to collect, protect, maintain and communicate it. If the same information could be stored somewhere else and provided only as partial identity containing the purpose related information (e. g. the driver's licence, seat adjustment preferences) the automobile would not need any sophisticated IdM mechanisms. In addition, in an emergency situation, meaningful identification information would be obtained not from the vehicle but from the personal IdM system.

Our idea is to have a communication device in possession of the individual as an identity broker which delivers the right kind of information to the party which needs it at the moment. The broker would not need to have all identity information accessible at all time. In fact we imagine an online and offline capability where predictable identity information is stored locally (offline) in a protected form (e. g. credentials) and additional credentials, which are protected

and partial for the new purpose, received on demand (online) from an online repository – maybe by a mesh network. The offline capability can also come handy in a mesh scenario because we cannot assume that a central connection is available at all time (e. g. when the end node in Figure 1 takes contact with the intermediate node the intermediate does not have online connection either but both must be able to identify each other).

6.4 Business Case - Customer Goodwill by Privacy Activities

Internal studies indicate that customers expect their operator to respect privacy. Engaging in an IdM platform would be a clear sign to the market that a TSP cares about its customers' privacy. Therefore the investment may deliver returns also in this segment and therefore provides a business case there.

7 Summary and Future Work

In this paper we introduced the problem of combining security and privacy-friendly identifiers in wireless mesh networks. We presented six non-functional requirements for users and other parties (TSP, SP) during the life-cycle of a user's identifier in a privacy-friendly wireless mesh network environment. From those requirements we derived four security and privacy requirements for digital identifiers in these environments. We compared two existing solutions for anonymous identifiers, anonymous attribute certificates and anonymous credentials, and concluded that anonymous credentials fulfill the imposed requirements: the provisioning of anonymity, uniqueness, revocability and independence of a central authentication server.

We also presented a business model that justifies the economic need of anonymous identifiers and wireless mesh network from a telecommunication provider viewpoint. We support our business model with two business cases.

A multiple-show, revocable, anonymous credential system, with credential sharing detection, derived from the periodic n-times spendable e-token scheme [4] is a work-in-progress initiated within the EU FIDIS Project[9]. As a future work, we plan the development of a prototype which will provide a proof-of-concept implementation of the selected scheme.

Acknowledgements

This research was partially funded by the European Network of Excellence Future of Identity in the Information Society (FIDIS), under the 6^{th} Framework Program for Research and Technological Development within the Information Society Technologies (IST) priority. The authors also thank the reviewers that helped to improve this paper with insightful comments.

[9] See http://www.fidis.net

References

1. M. Bauer, M. Meints, and M. Hansen. D3.1: Structured Overview on Prototypes and Concepts of Identity Management Systems. Technical report, FIDIS – Future of Identity in the Information Society, 15 Sep 2005.
2. V. Benjumea, J. Lopez, and J. M. Troya. Anonymous Attribute Certificates based on Traceable Signatures. *Internet Research: Electronic Networking Applications and Policy. Special Issue on Privacy and Anonymity in the Digital Era: Theory, Technologies and Practice*, 16(2):120–139, 2006.
3. J. Camenisch. Efficient Private Credential Systems and Applications: Cryptography for Privacy – Credential$^+$ Systems. 3^{rd} FIDIS Doctoral Consortium Event, Stockholm, Sweden, 9–13 Aug 2006.
4. J. Camenisch, S. Hohenberger, M. Kohlweiss, A. Lysyanskaya, and M. Meyerovich. How to Win the Clone Wars: Efficient Periodic n-Times Anonymous Authentication. In *Proceedings of the 13th ACM Conference on Computer and Communications Security (CCS 2006)*, 30 Oct–3 Nov 2006.
5. J. Camenisch and A. Lysyanskaya. An Efficient System for Non-transferable Anonymous Credentials with Optional Anonymity Revocation. In *Proceedings of the International Conference on the Theory and Application of Cryptographic Techniques (EUROCRYPT 2001)*, volume 2045 of *Lecture Notes in Computer Science*, pages 93–118. Springer, 2001.
6. J. Camenisch and A. Lysyanskaya. A Signature Scheme with Efficient Protocols. In *Security in Communication Networks: Third International Conference (SCN 2002)*, volume 2576/2003 of *Lecture Notes in Computer Science, LNCS 2576*, pages 268–289, Amalfi, Italy, 12–13 Sep 2002. Springer.
7. J. Camenisch and M. Stadler. Proof systems for general statements about discrete logarithms. Technical Report TR 260, Institute for Theoretical Computer Science, ETH Zürich, Mar 1997.
8. J. R. Douceur. The Sybil Attack. In P. Druschel, F. Kaashoek, and A. Rowstron, editors, *Peer-to-Peer Systems: Proceedings of the 1^{st} International Peer-to-Peer Systems Workshop (IPTPS)*, volume 2429, pages 251–260. Springer-Verlag, 7–8 Mar 2002.
9. M. Gruteser and D. Grunwald. Enhancing Location Privacy in Wireless LAN Through Disposable Interface Identifiers: A Quantitative Analysis. In P. Kermani, editor, *Proceedings of the 1^{st} ACM International Workshop on Wireless Mobile Applications and Services on WLAN Hotspots (WMASH 2003)*, 19 Sep 2003.
10. Mar 2007. See `http://www.ieee802.org/11/Reports/tgs_update.htm`.
11. ITU-T Recommendation X.509, The Directory: public-key and attribute certificate frameworks. Recommendation X.509 - International Telecommunications Union, The International Telegraph and Telephone Consultative Committee, Data Communication Networks: Open Systems Interconnection (OSI); Security, Structure and Applications, Aug 2005.
12. L. A. Martucci. The Identity Anonymity Paradox: on the Relationship between Identification, Anonymity and Security in Mobile Ad Hoc Networks, Licentiate Thesis, Karlstad University Studies 2006:36, September 2006.
13. A. Pfitzmann and M. Hansen. Anonymity, Unlinkability, Undetectability, Unobservability, Pseudonymity, and Identity Management - A Consolidated Proposal for Terminology v0.30, 26 Nov 2007. See `http://dud.inf.tu-dresden.de/literatur/`.

14. C. P. Schnorr. Efficient signature generation for smart cards. *Journal of Cryptology*, 4(3):239–252, 1991.