1 Biometric Authentication and Multilateral Security

Gerrit Bleumer

AT&T Labs-Research, Shannon Laboratory, Florham Park, NJ

Abstract:

We are currently facing industrial societies turning rapidly into information societies. Computer systems that were previously separated and dedicated to specific tasks become a more and more integrated global information system. The driving force is competition of service providers of all kinds and perhaps the most visible indicator is the convergence of telephone, cell phone and satellite networks, TV cable networks and the Internet. This global system provides a multitude of services and at the same time controls access to services, resources and funds. In order to enforce access authorizations effectively, and also to overcome the notorious disadvantages of passwords and PINs, which need to be memorized, it will become common practice to recognize human individuals biometrically. Biometric technology is already available and will soon be cheap enough to be applied on a large-scale basis. If this leads to an uncontrolled proliferation of biometric data, then not only the privacy of individuals is at serious risk, but democracies as such are so. It may sound paradoxical, but biometric recognition is possible, without individuals giving away their personal biometric data to any device under the control of a verifying organization or corporation. We draft a cryptographic solution based on recent research results. This work focuses less on the biometric techniques themselves, but rather on how the resulting biometric data is handled in the authentication process.

Subject descriptor codes:

Communications networks (D04), Computer architecture (D05), Encryption (D07), Human computer interaction (D10), Remote sensing (D30),

Market application codes:

Biosensors (A05), Data/information security (D07), Mobile communications/cellular radio (D25), System security (D30)

1.1 Introduction

More and more biometric technology is getting employed in order to detect and recognize individuals. Criminal investigation and intelligence are still the dominant areas of application, but it is becoming commonplace in the commercial sector and in the public. For example, scarce and/or valuable resources in everyday life are increasingly protected by video controls.

Governments enforce their immigration laws by taking fingerprints of certain people entering their countries. Companies, hospitals and organizations protect the entrances

of their buildings, interior rooms, computers and safes by fingerprint readers. Some companies keep track of working hours by automatically recognizing incoming and outgoing employees. Banks monitor their tellers and ATMs in order to defeat theft and credit card fraud. Car manufacturers are developing biometrically protected door locks and ignition locks in order to discourage theft and keep minors from driving. Drivers are getting video monitored when passing road tollbooths, bridges or tunnels.

More sophisticated biometric technology will soon lead to non-transferable membership cards, passports, driver's licenses, season tickets or election ballots.

Biometric technology tends to cost more than password or token-based systems, because the hardware required to sense and analyze biometric patterns is more complicated. However, biometrics provide a very high level of security because the authentication is directly related to a unique physiological or behavioral characteristic of the individual, which is more difficult to counterfeit. Recent technological advances have also helped to reduce the cost of biometrics. Moreover, biometric technology can be easier and more convenient to use than password or token-based systems. Biometric samples cannot be forgotten or lost, and they need not (and cannot) be changed on a regular basis.

According to Frost & Sullivan the worldwide revenues for biometric systems in 1998 were about US$ 113 million. This amount breaks down into the following application areas: Physical access control (52.8%), law enforcement (12.9%), healthcare (10.2%) banking (8.3%), immigration (4.9%), computer security (4.1%), welfare (4.1%) and telecommunications (2.7%) [23].

In principle, biometric samples can be used more or less reliably to recognize individuals quickly, anywhere, and at any time throughout their entire life. So the technology opens the possibility to link all the political, economic and social roles and behaviors of an individual. How someone behaves as a customer, patient, car driver, member of the armed forces or as a tenant may have consequences on his treatment as an insurance policy holder, bank account owner, employee, or seeker of employment and vice versa.

If biometric technology gets deployed on a large scale basis and thus individuals cannot prevent the proliferation of their personal biometric data unless facing serious disadvantages in everyday life, then automatic biometric recognition becomes the default; avoiding it will require criminal activity [13, 14, 20].

Another risk of biometric technology is that personal biometric data could be interpreted in medical terms and therefore may reveal certain medical diagnoses. Some methods of obtaining biometric data may even harm individuals. For example, taking blood samples may cause infection with debilitating diseases. The higher these risks are, the more *invasive* or *intrusive* the biometric method is called. Some governments and international organizations already acknowledge and address the risks of intrusive biometric methods by specific legislation. See for example the Convention 108 of the Council of Europe for the Protection of Individuals with regard to Automatic Proc-

essing of Personal Data [16] and the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data [24].

We give an overview of how current biometric technology works and then draft a new cryptographic solution for personal credentials. Our solution combines the security of biometrics with strong data protection. In previous work, it has been shown how personal credentials can be used to implement drivers' licenses [7] or to invoice and remunerate medical expenses in a health care system [6].

1.2 Biometric Authentication

The purpose of user *authentication* is to determine whether or not a user at hand has a required privilege, such as an access right. Every user first needs to be enrolled in the system by providing some unique individual *pattern* or *characteristic* which is then digitized and stored by the system as a (binary) *template* for the respective user. In the simplest case, the pattern is a keyed-in password, digitization is obsolete and the template is the password in clear, compressed or encrypted form. During each authentication later on,

1. the user first reproduces the pattern and lets the system sense it (*sensing*).
2. The system then compares the actual pattern with the templates in order to recognize the user (*recognition*).
3. Finally, the system determines whether the recognized user is assigned the required credential(s) (*authorization*).

If the patterns are biometric samples, then we speak of *biometric recognition* and *authentication.* In principle there are two types of recognition. The most frequent case is (biometric) *verification*. During the enrollment process, users are assigned some index such as a username or PIN, and their biometric templates are stored together with these indexes. In order to be recognized, users provide their index and their actual pattern, while the system verifies that the actual pattern matches the template stored for the provided index. The other case is (biometric) *identification.* During the enrollment process, users only leave their biometric templates. Whenever an actual pattern is presented to the system, it looks-up the best matching templates. This is how AFIS (Automated Fingerprint Identification Systems) work, which are used to automate the identification of culprits for crimes where a fingerprint has been left behind.

For biometric recognition, unique physiological or behavioral characteristics are used. Common characteristics include the following [1]:

Fingerprints are the recognized worldwide standard for identifying individuals; they are unique (even for identical twins) and non-transferable. Reliable and mature fingerprint readers are available off-the-shelf. About 30.4% of the worldwide revenue in biometric systems in 1998 is due to fingerprint technology [23].

Hand geometry looks at the three-dimensional size and shape of the hand. The results of over ninety measurements, including length, width, thickness and surface areas are converted into a nine-byte template. A new technique checks the vein pattern at the back of the hand. About 35.3% of the worldwide revenue in biometric systems (1998) is due to hand geometry technology [23].

Voice patterns still have problems that have not been solved satisfactorily. If the voice pattern depends on a single static phrase, it is very easy to masquerade by using a tape recorder. At the other extreme, text independent voice patterns require longer phrases, which in turn increases the time needed for recognition. The most promising trade-off may be voice patterns that depend on text that is chosen from a specified and large enough pool of phrases [18]. Other problems are background noise, effects of colds and other voice changes. About 21.4% of the worldwide revenue in biometric systems (1998) is due to voice recognition technology [23].

Vein patterns on the eye's retina are known as one of the most unique characteristics owned by humans. This pattern is not genetically determined, but is randomly developed by each individual. It is one of the most stable characteristics in the life of a person. Only extreme wounds can alter the retina pattern. A typical retinal template is 40 byte long and a scan takes 1.5s. This and each of the following technologies contribute to the worldwide revenues in biometric systems (1998) by less than 5%.

Optical or thermal face patterns are the ideal characteristics in terms of intrusiveness and user acceptance. However, the ways in which the appearance of the face of the same person may change are so many that most recognition systems are only in research state and have never performed well enough for actual use.

Physiological characteristics like fingerprints, hand geometry etc. are usually called *static* because they cannot be altered deliberately. Behavioristic characteristics like voice patterns, typing patterns and written signatures are called *dynamic* although they may contain a (small) physiological component.

The performance and quality of a given biometric recognition method is stated in terms of the following criteria:

1. *false acceptance rate* (FAR),
2. *false rejection rate* (FRR),
3. processing time (time to reproduce a pattern and to match it with a template)
4. size of templates (short templates are important for smart card based solutions)
5. vulnerability to fraud (authorized individuals may or may not collaborate in fraud.)
6. acceptability (social acceptability, intrusiveness, discrimination of minorities)
7. long-term stability (period over which a biometric pattern remains stable)

The interpretation of FAR, FRR and processing time is not easy, because they are inherently related [18]. In practical systems, the rate of false acceptances can be decreased at the expense of a higher rate of false rejections and vice versa. Also repeat-

ing the number of scans of the biometric pattern can decrease both rates. That of course reduces the time to recognize. More information about available products can be found on the homepage of the Biometrics Consortium [5].

1.2.1 System Architectures

From now on, we consider distributed *biometric verification architectures* with a number of access points where users from a given population can be biometrically verified and optionally be authenticated to have a required privilege. In the latter case we call them *biometric authentication architectures*. The standard solution is an *online architecture* where one or more *verification servers* run a (distributed) database of biometric templates and make it available to each access point by means of wired or wireless networks. For each verification the access points need to contact the verification servers. In order to match the actual biometric pattern to a template, the access point can send the actual pattern to a verification server and wait for a response (*push-model*). Alternatively, it can request one or more templates from a verification server to make the match itself (*pull-model*). Software applications can use these services through a BioAPI™, which is currently under development by the BioAPI™ consortium [4].

If the access points have enough storage and computing capacity and the database of templates does not need to be updated too frequently, then the templates can be stored right at the access points. This results in an *offline architecture* because the access points can recognize individuals without connecting to any verification servers online [16].

1.2.2 Security and Acceptability

Sensing static patterns like blood samples, retina or iris scans, fingerprints, or DNA samples tends to be more intrusive than sensing dynamic patterns, and therefore the latter is more acceptable to the general public. Sensing dynamic patterns, however, usually leads to higher false acceptance and rejection rates because dynamic patterns cannot be produced as accurately as static ones, in particular so in case of illness, stress, intoxication or other environmental influences. Another problem is that dynamic patterns can be counterfeited to a certain extent.

Fingerprint readers are currently the most mature and most widely deployed devices for biometric recognition in part because they have a long history in criminal investigation. For example, the Touchsafe II Fingerprint Identity Verification Terminals by Identix achieves FAR < .001% and FRR < 2% at 2s per recognition. Besides there are devices to distinguish live fingers from dead fingers or latex gloves. The long tradition in criminal investigation, however, stigmatizes fingerprint scanners and makes them less acceptable in many civil areas. There are off-the-shelf products that produce the templates in a data format incompatible to that used by law enforcement. But it is unclear how much effort is necessary to convert the format of a commercial product with sufficient accuracy into a format used in law enforcement.

In terms of privacy protection, online verification architectures pose a much bigger threat of surveillance than traditional paper based systems where persons identify themselves by means of passports, badges, etc, with imprinted photographs. The problem with online verification architectures is that the verification servers can gather enough information in order to compile the histories of users with respect to certain activities. For example, road tollbooths can be used to compile moving profiles; computer login data and cookie information can be used to compile detailed profiles of interest and behavior of each member enrolled in a system. This is already becoming reality in online marketing (e.g. www.doubleclick.com). Offline verification architectures are less threatening per se, but they bear the potential for large-scale surveillance because the separate access points can of course be connected at some later time. So in terms of privacy protection, the problem is not so much, which biometric characteristics are used for verification, but rather who is in control of the biometric templates and the actual biometric data resulting from the numerous verifications every day.

1.3 Personal Assistants and Observers

From now on, we consider an offline authentication architecture, where each individual holds a personal mobile device (*assistant*) that is capable of biometrically verifying its holder. In order to prevent individuals from counterfeiting, the biometric sensor is embedded into a tamper resistant security module [14, 25] (*observer*) inside of each assistant. Whenever an assistant communicates with an access point, it needs the help of its observer, but the communication protocols are designed such that the assistant can effectively prevent its observer from leaking unintended information to the access point, or receive unintended information from there. All the observer does is to authenticate legitimate transactions of its assistant, which may or may not require a biometric verification of the actual holder. In this offline authentication architecture, the access points are effectively split into two pieces, a machine (*verifier*) controlled by the verifying organization, and an observer controlled by the respective user seeking access. The two pieces are physically and logically separated by the user's assistant, which hosts the respective observer and provides the communication interface to the verifier. This way, each user keeps her biometric templates and all her actual biometric data under her exclusive control. Users cannot inspect their observers, but they can effectively prevent their observers from leaking any information to the outside world. No proliferation of personal biometric data can occur, unless observers are lost or stolen. The general concept of a personal assistant hosting a tamper resistant security module has been introduced by Chaum and Pedersen as the wallet-with-observer architecture [14, 13].

Candidates for assistants are cell phones, organizers, palm pilots or computer cards, i.e., the next generation of smart cards, which can have a biometric sensor implanted. An overview of existing and upcoming personal devices is found in [15, editor: include reference to the reachability manager in this volume]. Assistants must have their own power supply and user interface in order to be independent of the verifiers.

Assistants must be capable to communicate with verifiers, for example, by wireless or infrared connections. Observers are preferably implemented by chips that integrate a biometric sensor and a digital signature functionality. Single chip solutions of biometric sensors already exist. See for example AuthenTec's FingerLoc™ system [2]. Cell phones with integrated biometric identification are under development by a consortium of GEMPlus (France), ARM (UK) and Nokia (Finland) sponsored by the European Union through their project ESPRIT-CASCADE [10].

Each observer comes from the manufacturer with a built in secret signing key (*native key*) and a corresponding registered public verification key. Before an observer can be used, it needs to be personalized with a biometric template of its legitimate holder. During this irreversible process, the holder's biometric template is created and stored inside the observer. From then on, the observer can biometrically verify its actual holder.

Offline identification by assistants with observers keeps personal biometric data under the control of their holders unless observers are lost or stolen. Even in this case, adversaries learn only one biometric template at a time, not hundreds or thousands as in the case of verification servers broken into. The most interesting potential of offline verification by assistants is the possibility of anonymous, even untraceable, transactions that require biometric verification or authentication. For example, showing a driver's license could be done anonymously, if the assistant guarantees that the person showing the driver's license to an automatic road check point is indeed the owner of the driver's license. Nothing must be revealed about the driver except that he has a valid license. Drivers licenses may even be shown in an untraceable way. That is if two cars pass an automated road check point, the system need not even be able to find out if it is the same driver. In principle, an online verification system cannot support untraceable biometric verification or authentication, because verification servers can link each individual's transactions by its index and biometric template.

1.4 Untraceable Biometric Credentials

The third step of user authentication is to look up if the verified user holds the authorization or credential that is required by the application, for example, a valid driver's license. Only then is the user successfully authenticated. In online and offline authentication architectures, the database of credentials, i.e., who has what privileges, can be implemented in the same database as the biometric templates. Furthermore, if users choose pseudonyms as their indexes, then they can be authenticated anonymously, i.e. without revealing their real identity. Alternatively users might keep their own credentials locally in their assistants in an unforgeable way. The advantages are twofold: It is more natural for users to keep their credentials under their own control, and users can be authenticated not only in an anonymous but also in an untraceable way.

We are now going to sketch an efficient cryptographic solution for untraceable personal credentials. Our principals are the issuers, the holders and the verifiers of cre-

dentials. Holders are equipped with assistants each hosting an observer into which a biometric sensor is implanted. The basic idea underlying the following solution is that holders show their credentials in an untraceable way by using one-time pseudonyms. We consider three basic transactions:

- A credential holder introduces herself to an issuer under a chosen pseudonym.
- An issuer issues a credential to a holder under a pseudonym introduced to him.
- A holder shows a credential to a verifier using a new pseudonym.

During each of these transactions, the holder's assistant interacts with the machine of the respective issuer or verifier. Pseudonyms for which credentials are issued and shown are called *source pseudonyms* and *target pseudonyms*, respectively.

The following solution makes use of two cryptographic building blocks, namely interactive *proofs of knowledge* [3] and *blind signatures* [11, 12]. Conceptually, they are applied as follows. Credentials tie an authorization to a user identifier (real name, pseudonym, etc.) in a publicly verifiable way. Here, they are implemented by digital signatures given for pseudonyms. A pseudonym represents a credential holder, and a public verification key represents an authorization also called the *type* of a credential. For example, if there are 3 types of club members, then the issuer provides signatures with respect to 3 different verification keys. Special blind signature schemes allow to obtain a signature for a source pseudonym with respect to a given public key and to transform it into a signature for a target pseudonym with respect to the same and only the same verification key. This way, the holder can produce many different and unlinkable representations of the same credential, which allows her to show a credential many times without revealing that all the shows have resulted from the same holder. Next, the pseudonyms of a user need to be tied to her biometric template in a way that is enforceable by the observer in her assistant. We therefore introduce pseudonym "witnesses", which are secrets that unlock a pseudonym in the following sense.[1] For each pseudonym there is at least one witness. In order to use a pseudonym, users have to prove knowledge of a matching witness. This is done by an interactive proof of knowledge that does not disclose the prover's witness to the verifier. Pseudonym witnesses are split into two shares, one chosen and held privately by the user's assistant, and the other by its observer. Finally, the observer participates in proving knowledge of its share of a pseudonym witness only if it verifies its holder successfully. Any transfer of credentials among individuals is thus prevented unless observers are broken.

Now we sketch the three transactions in some more detail. A technical cryptographic description in found in [7] and an implementation of the special blind signature scheme is found in [8].

[1] The term "witness" is established in the cryptographic literature for proofs of knowledge.

1.4.1 Introducing Source Pseudonyms

Assistant and observer together form a new source pseudonym ψ for the user. Each of them independently chooses one respective witness share *a* and *b*. Together, they hold the complete witness $z = (a, b)$ without learning each other's shares. Finally, they compute the source pseudonym ψ for the witness *z*. Then the user introduces herself to an issuer by submitting the source pseudonym ψ and attaching a valid native signature from its observer. The observer produces this signature by its native key, which assures the issuer that a registered observer co-operates in the introduction of a pseudonym. Finally, the assistant asks its observer to co-operate in proving knowledge of the witness *z* for ψ. The observer verifies the actual user biometrically and, if successful, co-operates in the proof of knowledge (Figure 1). The issuer registers the new source pseudonym as successfully introduced. When showing this credential later on, the assistant needs to ask its observer to re-use its witness share *b*.

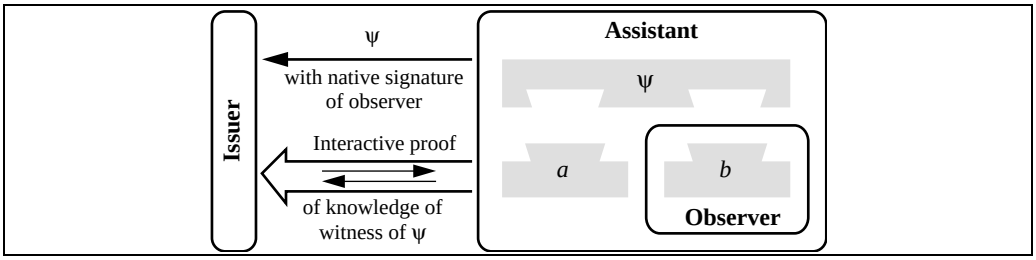

Figure 1: Introducing a source pseudonym

1.4.2 Issuing Credentials

The user connects her assistant either directly or remotely to the issuer's machine. She then asks for a certain type of credential for the source pseudonym ψ introduced earlier. The issuer provides a credential of the requested type for the suggested source pseudonym. The blind signature protocol enables the assistant to compute a signature σ' for a new intermediate pseudonym ψ' without the issuer learning any of the two. At the same time, the assistant is able to update its witness share to a', so that the two shares (a', b) make up a witness of the intermediate pseudonym ψ' (Figure 2). A user can request several credentials from the same issuer for the same or different source pseudonyms.

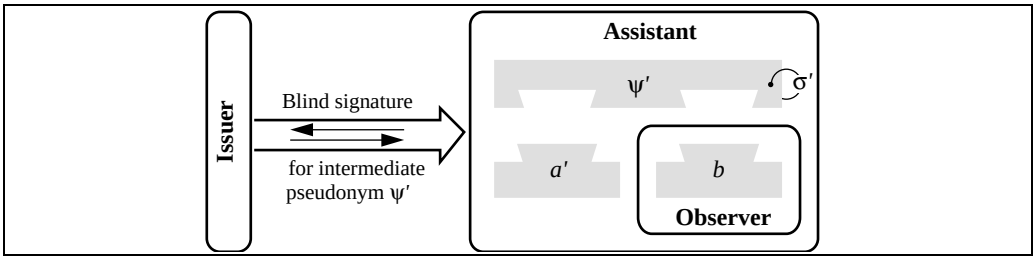

Figure 2: Issuing a credential

1.4.3 Using Credentials

The user connects her assistant either directly or remotely to the verifier's machine. For each show, the assistant transforms its intermediate pseudonym and signature into a target pseudonym ψ'' and signature σ''. Again, this transformation allows the assistant to update its witness share to a'', so that the two shares (a'', b) make up a witness of the target pseudonym ψ'' (Figure 3). Next, the assistant asks its observer to co-operate in proving knowledge of a witness for the target pseudonym. Here, the assistant asks its observer to use the same witness share *b* as during the issuing of the credential. The observer co-operates only if it now verifies the actual holder successfully. Otherwise, the verifier is not convinced and rejects access.

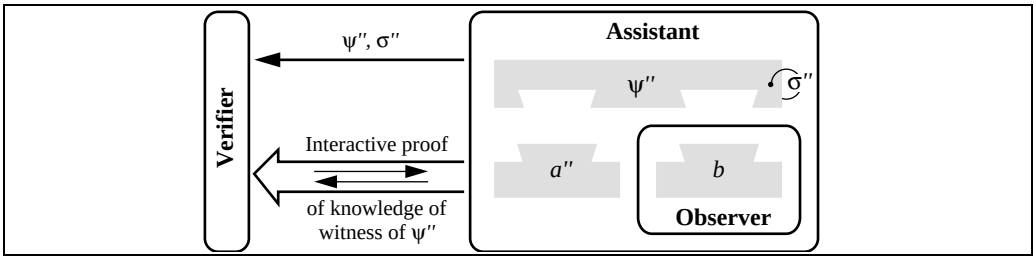

Figure 3: Showing a credential

1.4.4 Interdependent Credentials

In real life, users often get issued a new credential if they have previously presented another credential and in addition pass a certain test. In case of the driver's license, it is usually required to present some document of identification and a medical report. Upon passing a written test and/or a driving test, a driver's license is issued. The document of identity, the medical report and the driver's license can all be regarded as personal credentials and in real life, many other examples of personal credentials exist and much more complex interdependencies occur. It appears that not many pseudonyms need to be introduced in advance. For example, the driver's license can be issued for the pseudonym for which the medical exam is shown. In other words, target pseudonyms of one credential can be re-used as source pseudonyms of another. Not only is this more efficient because it saves the explicit introduction of a new pseudonym, but rather is it vital to sustain untraceability. Note that every time a user introduces a new pseudonym explicitly (Section 1.4.1), its observer provides a signa-

ture with respect to its native key. Since each native key is unique and specific to one observer, all explicitly introduced pseudonyms are linkable by the respective issuers. In general, a user is better off to re-use target pseudonyms which have been introduced implicitly by showing other credentials (Section 1.4.3).

1.5 Security

In mathematical terms, the transformation of source pseudonyms into intermediate pseudonyms is the same as the transformation of intermediate pseudonyms into target pseudonyms (including the respective signatures). If the assistant performs the transformation correctly and uses unbiased coins as a source of randomness in the protocol, each possible pseudonym and signature is equally likely to result from any given pseudonym and signature. Hence, source-, intermediate- and target pseudonyms are mutually unlinkable. So the assistant may show the same credential arbitrarily often without releasing more tracing information to the verifiers than what the type of this credential tells them anyway. For example, if a certain type of credential has been issued only once, then all shows of this type are easily linkable.

In order to prevent users from loaning their credentials to others, the assistants must not be able to transform a given intermediate pseudonym and signature into a target pseudonym and signature, so that the assistant knows a complete witness for the target pseudonym. This would allow the user to bypass her observer, thereby also bypassing the biometric verification. The credential would be freely transferable to anyone. An efficient way to enforce this requirement is to employ a restrictive blind signature scheme. Such schemes guarantee that valid signatures can only be obtained for pseudonyms that are correctly transformed. It is then left to the relation of witnesses and pseudonyms to ensure that if an observer holds one witness share b of the source pseudonym, then it is feasible to find a witness of the intermediate pseudonym only if the observer's witness share b is known. Non-transforming restrictive blind signatures have been introduced by Brands [9], who built on work of Chaum and Pedersen [14]. These signature schemes allow elegant and efficient implementations of offline electronic cash with double spender detection. A transforming restrictive blind signature scheme, which is required for untraceable credentials as sketched above, was developed by the author [8].

What happens if an attacker breaks one or more observers? In the above solution, at most all credentials that have been issued using the broken observer(s) become transferable and can then be shown by anyone. However, the credentials of honest users are not affected, and the attacker is not enabled to create new credentials.

1.6 Conclusion

Personal devices like cell phones, organizers, palm pilots, and others bear the potential to integrate various functionalities at a unified and convenient user interface. This is already apparent in devices by Qualcomm and Nokia, which combine the functionalities of a cell phone, pager, e-mail client, calendar and organizer. Personal devices

have an even bigger potential to increase the ease of biometric user verification for different services offered by various providers and at the same time enforce a level of personal data protection that could not be achieved by previous solutions. The importance of personal assistants for personal and multilateral security has been demonstrated in other work of the Daimler-Benz Kolleg [editor: could perhaps include one or two references here; preferably in one of these 3 volumes.]

A solution is sketched how personal devices can be used in order to verify users biometrically, while their anonymity is maintained. A further solution is sketched for untraceable personal credentials using assistants that host security modules. Only non-transferability relies on the assumption that the security modules are tamper resistant, but unforgeability and untraceability hold without such an assumption. This distinguishes the new solution from a previous proposal by Chaum and Pedersen [8] where both unforgeability and non-transferability depend on tamper resistant observers.

The new solution is applicable to many areas where personal membership is an issue. Holding a health insurance policy is one example. The whole billing process revolving around invoicing and remunerating medical expenses in a health care system can be designed based on patient held assistants [6].

All cryptographic building blocks used in this implementation are efficiently computable, can be employed in small personal devices and can be combined with any biometric recognition technology.

1.7 Bibliography

[1] AND Identification B.V.: Comparison of Biometric Identification Methods; http://www.and.nl/id/products/biometri/biometri.html.
[2] AuthenTec Inc.: http://www.semi.harris.com.
[3] Mihir Bellare, Oded Goldreich: On Defining Proofs of Knowledge; Crypto '92, LNCS 740, Springer Verlag, Berlin 1993, 390-420.
[4] The BioAPI Consortium: http://www.bioapi.org/bioapi.htm.
[5] The Biometrics Consortium: http://www.biometrics.org/.
[6] Gerrit Bleumer, Matthias Schunter: Digital Patient Assistants: privacy vs cost in compulsory health insurance; Health Informatics Journal 4/3-4 (1998) 138-156.
[7] Gerrit Bleumer: Biometric yet Privacy Protecting Person Authentication; Information Hiding Workshop '98, LNCS 1525, Springer-Verlag, Berlin 1998, 101-112.
[8] Gerrit Bleumer: Many-Time Restrictive Blind Signatures; AT&T Technical Report 98.38.2; http://www.research.att.com/library/trs/
[9] Stefan Brands: Untraceable Off-line Cash in Wallet with Observers; Crypto '93, LNCS 773, Springer-Verlag, Berlin 1994, 302-318.
[10] ESPRIT-CASCADE: Chip Architecture for Smart CArds and portable intelligent DEvices; http://www.dice.ucl.ac.be/crypto/cascade/
[11] David Chaum: Blind Signature System; Crypto '83, Plenum Press, New York 1984, 153.
[12] David Chaum: Security without Identification: Transaction Systems to make Big Brother Obsolete; Communications of the ACM 28/10 (1985) 1030-1044.
[13] David Chaum: Achieving Electronic Privacy; Scientific American (August 1992) 96-101.
[14] David Chaum, Torben Pryds Pedersen: Wallet Databases with Observers. Crypto '92, LNCS 740, Springer Verlag, Berlin 1993, 89-105.
[15] Richard Comerford: Pocket Computers ignite OS Battle; IEEE Spectrum 35/5 (1998), 43-48.
[16] Coucil of Europe: Convention for the protection of individuals with regard to automatic processing of personal data; http://www.coe.fr/eng/legaltxt/108e.htm.

[17] George I. Davida, Yair Frankel, Brian J. Matt, B. J. On Enabling Secure Applications Through Off-Line Biometric Identification; IEEE Symposium on Security and Privacy, IEEE Press 1998, 148-159.
[18] Sadaoki Furui, Aaron Rosenberg: Speaker Verification; in Vijay K Madisetti, Douglas B. Williams (eds.): The Digital Signal Processing Handbook; CRC-Press 1998.
[19] Identix Inc.: http://www.identix.com.
[20] Constance Loizos: Biometrics – The identification that you'll never leave home without; Red Herring, 9/98, 22-24. http://www.cnnfn.com/digitaljam/redherring/9808/26/redherring_biometrics/
[21] Benjamin Miller: Vital signs of identity; IEEE spectrum 31/2 (1994) 22-30.
[22] Klaus Müller, Axel Pfau: Biometrische Verfahren zur Verifikation der Personenidentität; DuD 16/7 (1992) 346-352.
[23] Emma Newham, Calum Bunney, Carolan Mearns: The Biometrics Report; SJB Services, Langport UK 1998; http://www.sjb.co.uk.
[24] OECD: Guidelines on the Protection of Privacy and Transborder Flows of Personal Data; http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM.
[25] Andreas Pfitzmann, Birgit Pfitzmann, Matthias Schunter, Michael Waidner: Trusting Mobile User Devices and Security Modules; Computer 30/2 (1997) 61-68.