A Trusted Biometric System

Liqun Chen, Siani Pearson, Athanasios Vamvakas
Trusted E-Services Laboratory
HP Laboratories Bristol

HPL-2002-185
July 15th , 2002*

E-mail: {Liqun_Chen, Siani_Pearson}@hp.com

trusted computing platform, trusted biometric system, biometrics-based user authentication

This technical report describes a method for biometric identification based user authentication in distributed environments, which makes use of Trusted Platforms combined with Smart Cards and Trusted Biometric Readers for providing a trusted biometric system. With this authentication method, a user can establish a trust relationship with a Biometric Reader (via integrity checking), and the user can trust that the system (incorporating both reader and platform) will not disclose his or her sensitive biometric information to any unauthorized entity. Such an approach can be applied, regardless of the type of Biometric Reader. It provides an alternative to integrating biometric capture with Smart Cards, for example by providing a Biometric Reader actually on a Smart Card.

* Internal Accession Date Only
Approved for External Publication

A Trusted Biometric System

Liqun Chen, Siani Pearson and Athanasios Vamvakas
Hewlett-Packard Laboratories, Bristol
Filton Road, Stoke Gifford, Bristol, BS34 8QZ, the UK
{Liqun_Chen, Siani_Pearson}@hp.com

Abstract

This technical report describes a method for biometric identification based user authentication in distributed environments, which makes use of Trusted Platforms combined with Smart Cards and Trusted Biometric Readers for providing a trusted biometric system. With this authentication method, a user can establish a trust relationship with a Biometric Reader (via integrity checking), and the user can trust that the system (incorporating both reader and platform) will not disclose his or her sensitive biometric information to any unauthorized entity. Such an approach can be applied, regardless of the type of Biometric Reader. It provides an alternative to integrating biometric capture with Smart Cards, for example by providing a Biometric Reader actually on a Smart Card.

1 INTRODUCTION

Biometric technology has been used in many applications to increase the security of password-based identity. Unfortunately, biometrics has its own drawbacks. Unlike a password, a user's biometric information, such as face, fingerprint, hand, iris etc is unchangeable.

A good biometric system must ensure that (1) the biometric information comes from a live person at the time of verification, and (2) the biometric information matches the master biometric data on file. However, a big threat for biometric authentication is still compromise of a user's biometric information [Woo97]. The reason is that many platforms and biometric systems are used without their untrustworthiness being detected. If an impostor is able to access a user's biometric information, he or she can then replay this information to a matching algorithm used for user authentication, and be accepted as a valid user, given that the matching algorithm is not able to recognize the origin of the biometric information. The reason this has become a big issue is because more and more users need to access unfamiliar computing platforms, i.e., open computer platforms, such as airport terminals and cafe terminals, with Biometric Readers.

Beyond this, we try to address two issues: first, how a user can always trust that he or she is using a good biometric system, in particular if the system includes an open platform which he or she has never known; second, in many real-life applications, a user wants to retain privacy when accessing a service with biometric authentication, which means that he or she would not like any unauthorised entity to know that he or she is accessing, or has accessed, the service.

Based on these two issues, in this document we first discuss a few possible threats and requirements, and then provide a solution for both biometric system integrity and biometric data protection. This solution makes use of an extension of TCPA technology; and it ensures that an unauthorised entity is not able to access sensitive biometric information during biometric authentication. Our solution shows that a hardware-based tamper-resistant trusted chain can meet the needs of providing a trusted biometric system. This trusted chain consists of Trusted Platforms (TPs), Trusted Biometric Readers (TBRs) and Smart Cards (SCs). Each of these three apparatuses can bring benefits in this system, and by combining them a much more secure solution can be achieved.

2 EXISTING BIOMETRIC AUTHENTICATION TECHNOLOGY

The following two procedures are generally used for identification verification by biometric systems:

1. **enrolment.** The system captures *Biometric Code* (BC) (an individual's biometric information) as a sort of registration template.
2. **matching.** *Biometric Data* (BD) (recently captured biometric information) is compared to the BC, to decide whether or not it matches.

The format of BC and BD will differ according to the biometric techniques used, which range from fingerprint and hand geometry to voice, retina, face and behavioral characteristics (see for example [DaFrMa98], [IEEE00], [JaRoPr98], [Rat99], and [Way98]).

This document does not focus on any particular biometric technique, and we are concerned with protection of biometric information and checking integrity of the whole system based on a typical user authentication model, as follows. This biometric authentication model, for the purpose of letting a valid user access a computing platform, involves three entities: a Smart Card (SC) holding the user's BC, a Biometric Reader (BR) collecting the user's BD and the accessed computing platform running the matching process. This model is different from the existing biometrics with smart cards technology, such as [BoRe95] and [Sei86], because it combines user authentication with integrity checking of the platform and Biometric Reader.

3 POSSIBLE THREATS

The following are a number of possible threats regarding biometric data protection and system integrity. These threats have been addressed in [ChPeVa00].

T1. *Interception of communications between the SC and the platform.* If the BC is sent in clear text or protected weakly, an eavesdropper could obtain the BC by listening in on communications between the SC and platform. This is a particular problem if the SC communicates with the platform over public networks, because the platform is not located locally to the user.

T2. *Interception of communications between the platform and the BR.* If the BD is sent in clear text or protected weakly with mere scrambling on the line, an eavesdropper could obtain the BD by monitoring communications between the BR and platform. Again, this is a particular problem if public networks are involved in the communications.

T3. *Malicious BRs*. A malicious BR is able to record the BD of a user, and a malicious BR is able to send a fake BD of a user.

T4. *Malicious platforms*. A malicious platform can obtain both the BC and BD of a user, and of course a malicious platform can give a fake result of the user authentication.

4 SECURITY REQUIREMENTS

We now list general requirements for providing a trusted biometric system, based on our analysis above. Again, these requirements have been addressed in [ChPeVa00].

S1. Neither BCs nor BDs should be transmitted in an unprotected manner between the SC and the platform or between the BR and the platform (addressing threats T1 and T2).

S2. The BD should be protected by tamper-resistant hardware in the BR (addressing threat T3).

S3. The BC and BD should be protected by tamper-resistant hardware in the platform (addressing threat T4).

S4. Before the user gives his or her BC and BD, the integrity of both the platform and the BR should be checked (addressing threats T3 and T4).

5 A SOLUTION - TRUSTED BIOMETRIC SYSTEM

In this section we describe a solution for providing a trusted biometric system. Within this solution, we try to avoid transmission, process and storage of users' BCs and BDs on any mistrusted environment, including the public interface, the computing platform and the biometric reader without integrity checking.

5.1 Outline and Extension of TCPA Technology

TCPA [TCPA02] is an industry alliance formed in October 1999 focused on raising the level of "trustworthiness" of a computing platform, to allow sensitive transactions to take place. TCPA focuses on platform identity and integrity metrics to prove trust. Trusted Computing Platforms get their name from the fact that they enable trust in a platform for some particular purpose. They use a behavioural definition of trust: *an entity can be trusted if it always behaves in the expected manner for the intended purpose*. A Trusted Computing Platform (TCP) is a normal open computer platform that has been modified to maintain privacy [TCPA011]. It provides protection against theft and misuse of secrets held on the platform. It also provides a mechanism for the platform to prove its identity while maintaining anonymity, and a mechanism for a platform to show that it is executing the expected software. For further details of these mechanisms see the latest TCPA specification [TCPA012].

Each TCP has at least one Trusted Platform Module (TPM) that contains a processor and supports for some standard security functions, such as calculating keys, hashes and signatures. However, it differs from a cryptographic co-processor by providing several additional mechanisms, including platform integrity checks, platform identity, and protected storage. It has been designed to do all this at minimal cost, to promote wide deployment.

A TCP supports a secure mechanism for remote integrity checking of the TCP via examination of the hardware BIOS, master boot record and operating system, and supply on demand of authenticated information about the TCP's integrity. A challenger checks the appropriateness of the measurement processes, and compares the supplied results of measurements (called 'integrity metrics') with the expected values (whether these values were provided by the platform itself, already known to the challenger, or retrieved from a third party). The challenger can decide whether to trust the platform or not for the intended purpose based on his/her policies, the identity and integrity information and the authorities vouching for this information.

A method is provided for storage of data that prevents access to it if the software environment of the platform is altered: secure off-TPM storage is provided whereby the TPM can encrypt data or keys (decryptable only via use of a root storage key private to the TPM) and store these on the local platform. Applications can digitally sign data that will be sent to other parties, via the TPM - this functionality is provided to the local OS once the TPM is satisfied with the integrity measured during the boot process. The TPM must therefore trust the OS not to provide this functionality to applications running on other platforms.

For the purposes of this document, we extend TCPA technology to introduce a Trusted Biometric Reader (TBR), which following market trends acts as an independent machine. The TBR may be a trusted platform and have a TPM, but this is not necessarily the case – it may be only a certified component of the whole TCP. When the TBR connects with the TCP, its identity and integrity can be checked and recorded by the TCP.

A SC can verify the correctness of integrity checking of both the platform and the TBR. Furthermore, the SC is able to show a user the result of integrity checking, for example by displaying a special image or value known only to the user. Technology about Smart Cards with a trusted user interface of the TCP is referred to in [BaChChPePr002].

5.2 Our Solution

We now propose a solution that uses a combination of a Smart Card (SC), a Trusted Biometric Reader (TBR) and a TCP to establish a trusted relationship amongst the user, BR and platform. The TCP must have means of storing a version of biometric comparison software. Either the biometric comparison software is stored within the TPM, or a version signed with a trusted third party's (normally the software issuer's) private key is stored within the platform, and the third party's public key certificate is verifiable to the TPM. This function is not required by TCPA specification v1.1: to achieve it, we need to extend the standard TPM by adding an authentication function, e.g., to be able to verify a digital signature based on its public-key certificate and a biometric matching function; and optionally to add some trusted software that can work with the standard TPM. In the remaining part of this report, for simplicity, we use "TPM" to stand for such an extended TPM or the standard TPM with such trusted software. In this case, the computing platform is programmed so that, upon booting of the platform: the biometric comparison software is integrity checked with reference to the signed version and the public key certificate; and if the integrity check fails, the biometric comparison software is prevented from being loaded. If the integrity check fails, it may be arranged that the complete platform integrity check fails.

Suppose that a user's BC is stored in a SC and is transferred into to the TPM during the authentication procedure. Alternatively, the BC could be centralized and stored (for example in the TPM) in order to be controlled by administrators more easily. In the later case, the SC will still be used for integrity checking purpose.

In certain environments a BR is potentially untrustworthy, and so there is an option for the TPM to require authentication of the BR, and preferably additional integrity checks. Preferably, the SC is able to check the integrity of both the platform and also the BR (via the TPM). It can do this by interrogating the TPM as to the status of its platform integrity, and the stored value of the BR integrity as part of an authentication protocol, and only continuing with the protocol if it is satisfied on both counts.

This solution is based on a combination of PKI techniques and symmetric cryptographic techniques. Optionally, a trusted Certification Authority (CA) issues certificates corresponding to public and private key pairs associated with the TPM and SC, and possibly the BR. Each end user has a smart card equipped with an asymmetric key pair for signature and verification. The TPM has two asymmetric key pairs respectively for signature-verification and encryption-decryption. The BR optionally has an asymmetric key pair for signature and verification.

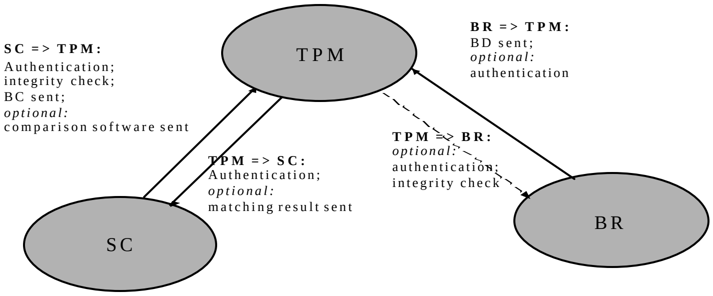

Figure 1 Transactions between TPM, SC and BR

Figure 1 illustrates a diagram representing the transactions between TPM, SC and BR. Upon sign-on using the SC, there is mutual authentication between the TPM and the SC and if necessary certificates are exchanged, with the SC checking that the integrity of the TPM is satisfactory before proceeding further. This can also be combined with an integrity check by the TPM on the BR. The BC is transferred from SC to TPM, encrypted with a symmetric session key set up for this purpose. Optionally, comparison software is also sent from the SC to the TPM. Optionally, the TPM authenticates the BR and/or BR authenticates to TPM and certificates are exchanged. This procedure is optional because the BR may only have integrity check-related information or a serial number and not the cryptographic functionality needed for authentication purposes. The SC and BR have no direct communication link in general, so do not authenticate directly.

The SC is able to show the user that it is happy with the result of platform and BR integrity checking. After being convinced of this, the user gives the BR his/her BD (by touching a fingerprint sensor, or the equivalent in other biometric methods). The BD is then sent from BR to TPM, encrypted with a symmetric session key set up for this purpose. The TPM then makes a comparison between the BC and BD to see to what degree they match. It can then report its findings to the user directly via the display, or to the SC, signed using the TPM's private signing key. Reporting findings to the SC could be useful if it is desired that the SC should release certain secret information only when it has been determined that the user is the valid owner of the SC.

In summary, based on this solution a biometric authentication can be carried out as follows:

- There is mutual authentication between the platform (TCP) and the SC, and optionally also with the BR. The SC verifies the integrity of the platform and BR. The integrity checking ensures that the TPM has a good record of the platform and BR's state (i.e. composition and environment).
- The SC shows the user that the TPM authentication and the platform and BR integrity checking have been successful (using the methods discussed in [BaChChPePr002]).
- The TPM authenticates the SC identity and obtains the BC from the SC.
- The BR takes the BD and transfers it to the TPM in a secure manner.
- The TPM compares the BD and the BC by using a biometric algorithm. Only if they match according to a previously defined threshold will the TPM allow the user to log into the platform or to access appropriate services. (The threshold is dependent upon the type of biometrics and application involved.)

The solution described has the following advantages, in that all security requirements S1- S4 are addressed, as follows:

S1. *Transmission of BCs and BDs in a protected manner.* These are always transmitted in an encrypted form. The symmetric keys used to do this are set up using protocols between the SC, platform and BR, as described further in [PeChVa00].

S2. *Protection of BD in the BR.* In this case, the BR is made into a trusted platform, and contains a TPM, which protects the BD.

S3. *Protection of BC and BD in the platform.* In the platform, the BC and BD are protected by the TPM by being located within it or protected via the TCPA protected storage mechanisms, and probably only released in a proper trusted state and they are never disclosed to any unauthorized entity.

S4. *Integrity checking the platform and the BR before BC and BD are released.* The accessed platform is not given either the BC or BD until the integrity of both the platform and the BR is checked by the SC. Similarly, the BR is not given the BD until the user is convinced about the correctness of both the platform and BR integrity checking.

6 A MECHANISM FOR AUTHENTICATION WITH DATA PROTECTION

In this section we describe a mechanism, which can be used to implement the solution described in the above section.

6.1 Requirements and Notations

This mechanism is based on a combination of asymmetric cryptographic techniques, symmetric cryptographic techniques and biometric algorithms. The following cryptographic functions are required.

- *A private key signature function S*. We use $S_X(m)$ to denote a private key signature on a data element *m* signed with a private signature key of the entity *X* (*X* = {*SC*, *TPM*, *TBR*}).
- *A public key encipherment function E*. We use $E_X(m)$ to denote public key encipherment of data *m* using the public encryption key of the entity *X* (*X* = {*TPM*}).
- *A symmetric encipherment function E'*. We use $E'_K(m)$ to denote the encrypted output given input data *m* and key *K*. If necessary, the encipherment algorithms used by the two pairs: SC/TPM, and TBR/TPM, can be distinct; we have assumed that a single algorithm is used to simplify the presentation.

The following keys need to be in place:

- The TPM needs to generate a *public key/private key pair for the public key encipherment algorithm*. The SC and TBR must have a reliable copy of the TPM's public encipherment key.
- The TPM, SC and TBR need each to generate *a private key/public key pair for the private key signature algorithm*. Both the SC and TBR must have a reliable copy of the TPM's public verification key; and the TPM must have reliable copies of the SC's and TBR's public verification key.

In addition the SC, TPM and TBR must be able to generate non-repeating nonces; the SC and TBR must be able to generate session keys; the TPM must be able to generate integrity metrics of the platform and selected components; and the SC must be able to verify the integrity metrics (referred to in [BaChChPePr001] and [BaChChPePr002]).

In the specification of protocols of the mechanism described in the next subsection, the following notations will be used:

- $N_{n\text{-}X}$ – a nonce issued by the entity *X* (*X* = {*SC*, *TPM*, *TBR*}) with a number *n*;
- D_n – a data element;
- SK_n – a shared session key used for protecting transmission of BD and BC.
- m_1,m_2 – a concatenation of two data elements m_1 and m_2;
- $S_X(m)$ – a signature on a data element *m* signed with a private signature key of the entity *X* (*X* = {*SC*, *TPM*, *TBR*});
- $E_X(m)$ – a data element *m* encrypted via an asymmetric algorithm by using the public encryption key of the entity *X* (*X* = {*TPM*});
- $E'_K(m)$ – a data element *m* encrypted via a symmetric algorithm by using the key *K*;
- *A ? B: m* – a data element *m* is transferred from entity *A* (*A* = {*SC*, *TPM*, *TBR*}) to entity *B* (*B* = {*SC*, *TPM*, *TBR*}).

6.2 The Protocols

The mechanism includes four protocols as follows.

6.2.1 Mutual authentication between the SC and TPM and transfer of BC from SC to TPM

The following protocol (partly) conforms to Key Transport Mechanism 5, specified in Clause 7.5 of ISO/IEC 11770-3 [ISO 11770-3]. The main point at which the protocol significantly diverges from the standard is that the SC must check the integrity provided by the TPM before replying to message M2.

M1. SC → TPM: $N_{1\text{-}SC}$, SC, D_1
M2. TPM → SC: $N_{2\text{-}TPM}$, $S_{TPM}(N_{1\text{-}SC}, N_{2\text{-}TPM}, SC, D_3), D_2$
M3. SC → TPM: $E_{TPM}(SK_1, SC, D_4)$, $E'_{SK_1}(N_{1\text{-}SC}, N_{2\text{-}TPM}, BC, D_5)$,
$S_{SC}(N_{1\text{-}SC}, N_{2\text{-}TPM}, TPM, E_{TPM}(SK_1, SC, D_4), D_6)$

The protocol procedure is as follows: if at any point a check fails, then the protocol is aborted.

- The SC generates and stores a nonce $N_{1\text{-}SC}$. The SC then sends the TPM an authentication request M1 with the nonce, its identity, SC, and the integrity checking request D_1.
- On receipt of M1, the TPM generates and stores a nonce $N_{2\text{-}TPM}$. The TPM then signs the integrity metric D_3 required with the two nonces $N_{1\text{-}SC}$ and $N_{2\text{-}TPM}$ and the SC's identity, and distributes them in M2. If necessary, D_2 can be certificates of the verification keys for the integrity checking purpose.
- On receipt of M2, the SC verifies the signature and checks the integrity metric. The SC then checks that the nonce it contains is correct. The SC then generates a session key SK_1 for use by the TPM and itself, and distributes the session key and BC in M3.
- On receipt of M3, the TPM retrieves the session key, verifies the signature and checks that the nonce it contains is correct. The TPM then stores the BC.

6.2.2 Mutual authentication between TBR and TPM and establishment of a session key

With the same message flows as the above protocol, the TPM and TBR can authenticate to each other and then transfer the BD from the TBR to the TPM. If required, the user must get the information issued by the SC that the SC is satisfied with the result of the TPM authentication and the TP and TBR integrity checking. One possible solution is referred to in [BaChChPePr002].

Here is a brief description of the protocol.

M1. TBR ? TPM: $N_{3\text{-}TBR}$, D_7
M2. TPM ? TBR: $N_{4\text{-}TPM}$, D_8, $S_{TPM}(N_{3\text{-}TBR}, N_{4\text{-}TPM}, TBR, D_9)$
M3. TBR ? TPM: $E_{TPM}(SK_2)$, D_{10} ,
$S_{TBR}(N_{3\text{-}TBR}, N_{4\text{-}TPM}, TPM, E_{TPM}(SK_2), D_{11})$

The TPM and TBR must authenticate each other to avoid non-valid biometric readers replacing the genuine ones, collecting the BD and transferring it to an impostor. Also transfer of data from the TBR to a non - valid TPM will be avoided. The TPM must be able to tell the user that the TBR is a valid one and he can put his finger on it or allow other biometric information to be taken with security. The reason why we need to authenticate the TBR (and not assume that one specific is attached to the PC) is because of the nature of distributed environments. It may be desirable that the TBR and the user are not physically present where the TPM is (e.g. public client platforms at airports or coffee clubs).

If this stage is not carried out, the establishment of a key that is to be used for encryption of the biometric data needs to be incorporated into the protocol shown for the following stage, i.e. where the biometric data is sent from TBR to TPM.

6.5.3 Biometric data is sent from TBR to TPM

M1. TPM ?   TBR: $N_{5\text{-}TPM}$, D_{12}

M2. TBR ?   TPM: $N_{6\text{-}TBR}$, D_{13}, E'_{SK2} ($N_{5\text{-}TPM}$, $N_{6\text{-}TBR}$, TBR, TPM, BD, D_{14})

After receiving the BC and BD, the TPM verifies the validation of the BD by using a biometric algorithm.

6.5.4 TPM sends SC the result of the biometric match (optional)

M1. SC ?   TPM: $N_{7\text{-}SC}$, D_{15}

M2. TPM ?   SC: S_{TPM} ($N_{7\text{-}SC}$, SC, *match_result*, D_{16}), D_{17}

One-way authentication is included within this stage.

The mechanism described here has the following advantages over biometric authentication:

1. The accessed TP is not given either the BC or BD until the integrity of both the TP and TBR is checked by the SC;
2. The TBR is not given the BD until the user is convinced about the correctness of both the TP and TBR integrity checking;
3. In the TP, the BD and BC are located in the TPM (which has hardware-based protected storage) or protected with the TPM protected storage function and they are never disclosed to any unauthorized entity.

7 CONCLUSIONS

In conclusion, although it is true that in many applications, biometric data is not secret, in many other applications for privacy and trust reasons biometric data is sensitive and we may need to protect it.

By using Trusted Computing Platform technology that includes a combination of a Trusted Computing Platform, a Smart Card and a Trusted Biometric Reader, as described in this document, secure transmission of biometric information and integrity checking of the biometric system are achieved. The data is not disclosed either during transmission or within accessed equipment, including both the computing platform and the Biometric Reader. This solution, furthermore, allows a user to verify that he or she is using a good biometric system.

ACKNOWLEDGEMENT

We would like to thank Boris Balacheff, David Chan, David Plaquin, and Graeme Proudler for their support and help.

References

[BaChChPePr001] B. Balacheff, D. Chan, L. Chen, S. Pearson, and G. Proudler. How can you trust a computing platform? In *the Proceedings of Information Security Solutions Europe Conference (ISSE 2000)*, Barcelona, Spain, 27-29 September 2000.

[BaChChPePr002] B. Balacheff, D. Chan, L. Chen, S. Pearson, and G. Proudler. Securing smartcard intelligent adjuncts using trusted computing platform technology. In *the Proceedings of IEIF Fourth Smart Card Research and Advanced Application Conference (CARDIS 2000)*, pp 177-195, Bristol, UK, 20-22 September 2000.

[BoRe95] E. Bovelandar and R.L. van Renesse. Smart cards and biometrics: an overview. In *the Proceedings of the 12th World Conference on Computer Security, Audit and Control*, 1995.

[ChPeVa00] L. Chen, S. Pearson, and A. Vamvakas. On Enhancing Biometric Authentication with Data Protection. In *the Proceedings of the Fourth International Conference on Knowledge-Based Intelligent Engineering Systems & Allied Technologies*, pp 249-252, IEEE, 2000.

[DaFrMa98] G. I. Davida, Y. Frankel and B. J. Matt. On Enabling Secure Applications Through Off-line Biometric Identification. In *the Proceedings of 1998 IEEE Symposium on Security and Privacy*, pp 148-157, 1998.

[IEEE00] Special Issue on Biometrics, *Computer*, Vol 33, No 2, IEEE, February 2000.

[ISO 11770-3] ISO/IEC DIS 11770-3. Information technology – Security techniques – Key management – Part 3: Mechanisms using asymmetric techniques. International Organization for Standardization, 29 July 1997.

[JaRoPr98] A.K. Jain, A. Ross and S. Prabhakar. Biometrics-based web access. MSU Technical Report TR98-33, 1998.

[PeChVa00] S. Pearson, L. Chen and A. Vamvakas. On Enhancing User Authentication with Biometric Data Protection by Smart Card and other Trusted Hardware. *Gemplus Developers Conference*, 2000.

[Rat99] N.K. Ratha et al.. A biometrics-based secure authentication system. In *the Proceedings of IEEE Workshop on Automatic Identification Advanced Technologies*, pp 70-73, 1999.

[Sei86] S. Seidman. Biometrics and smart cards combine to offer high security. *Journal of Nuclear Materials Management*, vol 15, pp 143-145, INMM Annual Meeting, 1986.

[TCPA011] TCPA. TCPA Design Philosophies and Concepts, Version 1.0, 2001. Available at www.trustedcomputing.org.

[TCPA012] TCPA. TCPA Main Specification, Version 1.1, 2001. Available at http://www.trustedcomputing.org.

[TCPA02] TCPA. Trusted Computing Platform Alliance, founded October 11, 1999. Available at www.trustedcomputing.org.

[Way98] J.L. Wayman. A generalized biometric identification system model. In *the Proceedings of the 31st Asilomar Conference on Signals, Systems and Computers*, pp 291-295, 1998.

[Woo97] J.D. Woodward. Biometrics: Privacy's Foe or Privacy's Friend? In *the Proceedings of the IEEE, Special Issue on Automated Biometrics*, Vol. 85, No. 9, p.1480, 1997.