Usability of Biometrics in Relation to Electronic Signatures

EU Study 502533/8

Version 1.0

September 12th 2000

GMD – German National Research Center for Information Technology
Institute for Secure Telecooperation (SIT)

Dirk Scheuermann
Scarlet Schwiderski-Grosche
Bruno Struif

The version 1.0 is based on the final report for commenting (July 12th 2000) and reflects the comments sent to the authors during the commenting period from July 12th until September 12th 2000.

Contact Addresses:

GMD – German National Research Center for Information Technology
Institute for Secure Telecooperation (SIT)

GMD Forschungszentrum Informationstechnik GmbH
Institut für Sichere Telekooperation (SIT)

Rheinstraße 75
D-64295 Darmstadt

Fax: +49-6151-869-224

Dr. Dirk Scheuermann
Tel. +49-6151-869-289
e-mail: scheuerm@darmstadt.gmd.de

Dr. Scarlet Schwiderski-Grosche
Tel. +49-6151-869-709
e-mail: schwider@darmstadt.gmd.de

Dipl.-Ing. Bruno Struif
Tel. +49-6151-869-206
e-mail: struif@darmstadt.gmd.de

Table of Contents

1 SCOPE 6

2 REFERENCES 6

3 DEFINITIONS AND ABBREVIATIONS 8

3.1 DEFINITIONS 9
3.2 ABBREVIATIONS 10

4 SIGNATURE CREATION SYSTEMS AND SECURE SIGNATURE CREATION DEVICES 11

4.1 SIGNATURE CREATION SYSTEMS 11
4.2 SECURE SIGNATURE CREATION DEVICES 13
4.3 SSCDS AND SIGNER AUTHENTICATION 15
4.4 SMARTCARD TECHNOLOGY 18

5 BIOMETRIC METHODS AND CHARACTERISTICS 19

5.1 CLASSIFICATION OF BIOMETRIC METHODS FROM THE USER'S AND BIOMETRIC VIEWPOINT 19
5.1.1 Static Methods 19
5.1.2 Dynamic Methods 20
5.2 BIOMETRIC METHODS IN USE 20
5.2.1 Fingerprint 20
5.2.2 Facial Features 23
5.2.3 Hand Geometry Measurement 24
5.2.4 Iris Feature 25
5.2.5 Retina Identification 27
5.2.6 Vein Recognition 28
5.2.7 Signature Dynamics 28
5.2.8 Speaker Recognition 29
5.2.9 Keystroke Dynamics 30
5.3 BIOMETRIC METHODS UNDER DEVELOPMENT OR OF LESS RELEVANCE IN THIS CONTEXT 30
5.3.1 Ultrasound Finger Identification 31
5.3.2 Facial Thermogram – Infrared Identification 31
5.3.3 Palmprint 31
5.3.4 Gait Recognition 31
5.3.5 Body Odour Measurements 32
5.3.6 Ear Shape Recognition 32
5.3.7 DNA-based Identification 32
5.4 UNIMODAL, MULTIMODAL AND COMBINED BIOMETRICS 32
5.5 SUITABILITY OF BIOMETRIC METHODS FOR ELECTRONIC SIGNATURES 33

6 KNOWLEDGE-BASED VERSUS BIOMETRIC AUTHENTICATION 36

6.1 ADVANTAGES OF BIOMETRIC FEATURES 36
6.2 PUBLIC STATIC BIOMETRIC DATA 37
6.3 PREPROCESSING OF BIOMETRIC DATA 37
6.4 NO EXACT DATA MATCH 37

7 SSCDS AND BIOMETRICS 38

7.1 CLASSIFICATION OF BIOMETRIC METHODS FROM THE VIEWPOINT OF A SIGNATURE DEVICE 38
7.1.1 Static Biometric Methods 38
7.1.2 Dynamic Biometric Methods 38
7.2 SMARTCARD USAGE AND BIOMETRICS – STATE OF THE ART 38
7.3 SPECIFICATION OF PROCESSES IN CONNECTION WITH SMARTCARDS 39
7.3.1 Enrollment 39
7.3.2 Verification 42

8 PROTECTION OF TRANSMITTED BIOMETRIC DATA 43

8.1 DATA TRANSMISSION MODES 44
8.1.1 Transmitting Plain Text Data 44

8.1.2 Protecting Data with a Scramble Function *44*
8.1.3 Authentic Data Transmission with Cryptographic Checksum *45*
8.1.4 Encrypted Data Transmission *45*
8.2 KEY MANAGEMENT 46
8.2.1 Key Management for Symmetric Algorithms *47*
8.2.2 Key Management for Public Key Methods *48*
8.2.3 Separate Protection of Raw Data and Extracted Data *48*
8.2.4 Crypto Sensors *50*
8.3 DISTRIBUTION OF BIOMETRIC FUNCTIONS AMONG SYSTEM COMPONENTS 50
8.3.1 Crypto Sensor in Data Terminal, Matching in SSCD *51*
8.3.2 SSCD with Biometric Sensor, Feature Extraction and Feature Matching *52*

9 BIOMETRIC PRODUCTS AND COMPONENTS 52

9.1 FINGERPRINT SENSORS 53
9.1.1 Optical Fingerprint Sensors *53*
9.1.2 Ultrasound Fingerprint Sensors *54*
9.1.3 Chip-Based Fingerprint Sensors *54*
9.1.4 Summary *57*
9.1.5 Integrated Sensors *57*
9.2 FACE RECOGNITION SYSTEMS 60
9.3 HAND GEOMETRY DEVICES 62
9.4 IRIS RECOGNITION SYSTEMS 63
9.5 RETINAL RECOGNITION SYSTEMS 64
9.6 DYNAMIC SIGNATURE VERIFICATION SYSTEMS 65
9.7 SPEAKER RECOGNITION SYSTEMS 66
9.8 KEYSTROKE DYNAMICS SYSTEMS 67
9.9 MULTIMODAL BIOMETRIC SYSTEMS 67

10 STANDARDS AND SPECIFICATIONS 67

10.1 ISO/IEC 7816 AND THE NEW WORK ITEM ON BIOMETRICS 67
10.2 ANSI/NIST STANDARD FOR CODING BIOMETRIC DATA 68
10.3 CRYPTO STANDARDS PKCS#11 AND PKCS#15 70
10.3.1 PKCS#15: Cryptographic Token Information Syntax Standard *70*
10.3.2 PKCS#11: Cryptographic Token Interface Standard *71*
10.4 BIOAPI 73
10.5 QUALIFIED CERTIFICATE PROFILE 74
10.6 COMMON BIOMETRIC EXCHANGE FILE FORMAT (CBEFF) 75
10.7 STANDARDISATION OF BIOMETRIC ALGORITHMS AND DATA FORMATS 75

11 ELECTRONIC SIGNATURES AND BIOMETRICS IN APPLICATION SECTIONS 75

11.1 CONSTRAINTS AND GENERAL ASPECTS 75
11.2 HOMEBANKING 76
11.3 E-COMMERCE 76
11.4 HEALTH CARE 77
11.5 OFFICE ENVIRONMENT 77

12 QUALITY AND EVALUATION CRITERIA FOR PRODUCTS AND ALGORITHMS 77

12.1 STRENGTH IN COMPARISON TO PIN MECHANISM 77
12.2 DISCRIMINATORY POWER REGARDING FAR AND FRR 78
12.3 MODELS OF DISTRIBUTION FUNCTIONS FOR FAR AND FRR 79
12.4 PROBABILISTIC ESTIMATION OF ERROR RATES 80
12.5 TEST SUITES AND DATA BASES 80
12.5.1 Live Tests and Offline Tests *80*
12.5.2 Significance of Test Persons *81*
12.5.3 Neutral and Objective Test Scenarios *81*
12.6 CLASSIFICATION OF FORGERY ATTEMPTS 81
12.6.1 Random Forgeries vs. Trained Forgeries *81*
12.6.2 Attack Levels for Trained Forgeries *82*
12.6.3 Defrauding vs. Circumventing the Sensor *82*

13 LEGAL ASPECTS 82

13.1 CURRENT REGULATIONS ON EUROPEAN LEVEL 82
13.2 CURRENT REGULATIONS ON NATIONAL LEVEL 83
13.3 DATA PRIVACY 83

14 OUTLOOK AND OPEN PROBLEMS 84

1 Scope

In the last decade(s), many investigations have been made in the field of biometrical authentication, i.e. verification or identification of a person by using biometrical features. Many biometrical methods have been developed to an extent, where products are available and used already in many application areas.
In the field of electronic signatures, after many years of stagnation a breakthrough is now expected. The legal situation has changed dramatically with the EU directive for electronic signatures and issued legal regulations on the national level of many countries in Europe and outside Europe. In several countries, the Public Key Infrastructure (PKI) has already reached a stage where Certificate Service Providers are able to produce Qualified Certificates and to offer directory and time stamp services. The smartcard technology as the most important and prominent representative of technologies for secure signature creation devices (SSCDs) has already shown for years that it is capable to execute signature algorithms and to provide storage for certificates.
However, the creation of an electronic signature is a security function which has to be protected against unauthorised use. The usual way for the signer authentication is a knowledge based mechanism, i.e. the presentation of a Personal Identification Number (PIN) or a password. However, the question is to clarify, whether and which biometrical authentication mechanisms are suitable to be applied as addition or alternative to knowledge-based authentication mechanisms in the context of electronic signatures, what is the state of the art in this field and where are problems to be solved. This study concentrates on the following subjects:

- SSCDs and their use in connection with biometrics.
- Different biometric methods and their suitability for electronic signatures.
- Secure data transmission from the biometric sensor to the SSCD.
- Existing standards for biometrics and electronic signatures
- Legal aspects for the use of biometrics in connection with electronic signatures.

For background information, the study also deals with some general aspects of biometrics as the confrontation of biometric authentication versus knowledge based authentication and general criteria for the testing and evaluation of biometric products and algorithms.
In addition, some existing biometric products are described and images of some specific example products are displayed for illustration purpose. The study has no intentions to evaluate specific products or to represent the interests of specific manufacturers. A complete listing of all existing biometric products in the world is outside the scope of the study.

2 References

For this study, the following standards, specifications and publications are of special relevance:

[AGV2000] AgV (German Consortium of Consumers): Statement to Law about Principles for Electronic Signatures – Discussion Submission 07. April 13th 2000.

[ANSI/NIST93] ANSI/NIST-CSL 1-1993:
Data Format for the Interchange of Fingerprint Information. Nov. 1993.

[ANSI/NIST97] ANSI/NIST –ITL 1a-1997:
Data Format for the Interchange of Fingerprint, Facial & SMT Information. April 1997.

[Beut95] Albrecht Beutelspacher, Jörg Schwenk, Klaus-Dieter Wolfenstetter:
Moderne Verfahren der Kryptographie: Von RSA zu Zero-Knowledge. Vieweg Verlag Braunschweig 1995.

[BioAPI] BioAPI Specification Version 1.00, The BioAPI Consortium, [http://www.bioapi.org], March 2000.

[Bur99] Burge, M. and Burger, W., Ear Biometrics, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.273-286.

[BWT2000] BWT (German Ministery for Business and Technology): Law on Framework Conditions for Electronic Signatures – Vertices for a Law Concept. April 2000.

[Cab2000] Concept of a Law on Framework Conditions for Electronic Signatures. – German Cabinet's decision, Aug 16th 2000.

[Cam99] Campbell, J.P., Speaker Recognition, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.165-190.

[Dau94] Daugman, J., United States Patent No. 5,291,560 (issued in March 1994). Biometric Personal Identification System Based on Iris Analysis, Washington DC: U.S. Government Printing Office, 1994.

[Dau99] Daugman, J., Recognizing Persons by their Iris Patterns, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.103-121.

[EESSI99] EESSI: Final Report of the EESSI Expert Team.
July 20th 1999.

[EU99] Directive 1999/93/EC of the European Parliament and of the Council of Dec. 13th 1999 on a Community Framework for Electronic Signatures. Jan. 19th 2000.

[Hil99] Hill, R.B., Retina Identification, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.123-141.

[HJ99] Hong, L and Jain, A, Multimodal biometrics, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.327-344.

[IBG] International Biometric Group, http://www.biometricgroup.com .

[IUKDG97] IUKDG (German Act on Information and Communication Services). June 13th 1997.

[JBP99] Jain, A, Bolle, R., Pankanti, S., Introduction to biometrics, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.1-42.

[Lec94] Leclerc, F. and Plamondon, R., Automatic Signature Verification: The State of the Art – 1989-1993, Int. Journal of Pattern Recognition and Artificial Intelligence, Vol. 8, No. 3 (1994), pp. 643-660.

[Meh93] B. M. Mehtre: Fingerprint Image Analysis for Automatic Identification.
Machine Visions and Applications V.6, 1993 (124-139).

[Mil94] Miller, B., Vital Signs of Identity, IEEE Spectrum, pp. 22-30, 1994.

[Nal99] Nalwa, V.S., Automatic On-Line Signature Verification, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.143-164..

[Neg2000] Negin, M. et. al., An Iris Biometric System for Public and Personal Use, COMPUTER, 2000, Vol. 33, No. 2, pp. 70-75.

[NIST/ITL99] NIST/ITL: „Common Biometric Exchange File Format“ (1999)
[http://www.nist.gov/itl/div895/isis/cbeff]

[Nix99] Nixon, M.S. and Carter, J.N., Automatic Gait Recognition, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp. 231-250.

[O'Gor99] O'Gorman, L., Fingerprint Verification, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.43-64.

[Oba99] Obaidat, M.S., Keystroke Dynamics Based Authentication, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.213-230.

[Per99] Persaud, K.C., Lee. D.-H., Byun, H.-G., Objective Odour Mesurements, in: Jain, A., Bolle,R., Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.251-272.

[PKCS#11] PKCS#11 v2.10: Cryptographic Token Interface Standard, RSA Laboratories, [http://www.rsasecurity.com/rsalabs/pkcs], December 1999.

[PKCS#15] PKCS#15 v1.1: Cryptographic Token Information Syntax Standard, RSA Laboratories, [http://www.rsasecurity.com/rsalabs/pkcs] May 2000.

[PKIX-QC] PKIX Working Group: Internet X.509 Public Key Infrastructure – Qualified Certificates Profile. http://search.ietf.org/internet-drafts/draft-ietf-pkix-qc-03.txt (Internet Draft valid from Feb. 2000 to Aug. 2000.)

[Pro99] Prokoski, F.J., Riedel, R.B.: Infrared Identification of Faces and Body Parts, in: Jain,A., Bolle,R.,Pankanti, S.: Biometrics: Pers. Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.191-212.

[Rat96] Nalini K. Ratha, Kalle Karu, Shaoyun Chen and Anil K. Jain: A Real-time Matching System for Large Fingerprint Databases. IEEE Transactions on PAMI 1996.

[Rud99] Rudin, N., Inman, K., Stolovitzky, G., Rigoutsos, I., DNA-Based Identification, in: Jain, A., Bolle, R., Pankanti, S.: Biometrics: Pers. Identification in Networked Society, Kluwer Acad. Publishers, 1999, pp.287-310.

[Scheu99] Dirk Scheuermann, Bruno Struif: SmartCards und Biometrie – Grundlagen der Kodierung und des Vergleiches von Fingerabdruckdaten. Card Forum, May 1999, pp 41-48. (German journal on smartcard technology.)

[SF99] Struif, Bruno
ISO/IEC 7816-.x - Biometric Authentication, Proceedings GMD-SmartCard Workshop 2000, Darmstadt, 8. Feb. 2000.

[TTT98] TeleTrusT e.V.: Kriterienkatalog zur Bewertung der Vergleichbarkeit biometrischer Verfahren. August 1998.
(German paper on criteria for evaluation of biometric methods, to be available in English soon; see http://www.teletrust.de.)

[Way99] James L. Wayman: Technical Testing and Evaluation of Biometric Identification Devices, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.345-368.

[Wen99] Weng, J. and Swets, D.L., Face Recognition, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.65-86.

[Wi2000] B. Wirtz: Security and Chip Card ICs.
Proceedings of Smart Card 2000.

[Zun99] Zunkel, R.L., Hand Geometry Based Verification, in: Jain, A., Bolle, R. and Pankanti, S.: Biometrics: Personal Identification in Networked Society, Kluwer Academic Publishers, 1999, pp.87-101.

3 Definitions and Abbreviations

3.1 Definitions

For this study the following definitions apply:

Enrollment
The process of capturing and storing the biometric data for registering a user is called *enrollment*. The enrollment process may contain the repetition of data capturing in case of bad quality or the capture of several samples to choose the best or calculate an optimised sample.

Equal Error Rate (EER)
If the tolerance limit for biometric data to match for a successful verification is chosen, such that the values of false acceptance rate) and false rejection rate (see definitions below)are equal, this common value is called the *equal error rate*.

False Acceptance Rate (FAR)
The *false acceptance rate* is the success probability for a defrauder of a biometric system to be falsely recognised as the legally registered user. Low tolerance limits for the biometric data to match lead to a very low FAR value, but to higher values for FRR (see def. below).

False Rejection Rate (FRR)
The *false rejection rate* is the probability for the legally registered user to be falsely rejected by the biometric system when presenting his biometric feature. High tolerance limits for the biometric data to match lead to a very low FRR value, but to higher values for FAR.

Identification
Identification means determining the identity of a user presenting his biometric feature. For this purpose, a database of several biometric data samples is searched, and the user is identified as the owner of the biometric data with the best match to the actually presented data. For this reason, the process of identification is also called a "one-to-many-comparison" or "1:N-comparison" (in contrast to the process of verification (see def.) where only one biometric comparison is performed).

Reference Data
The enrolled biometric data of a user to be later recognised during a verification or identification process are called *reference data*.

Resetting Code
If the value of the retry counter (see def.) has been set to zero and the verification method is blocked, the method may be activated again by the use of a resetting code. This resetting code sets the value of the retry counter back to its initial value.

Retry Counter
To prevent an attacker from getting access to the system by trying to present a biometric feature an arbitrary number of times, a retry counter is used. This allows only a limited number of false trials. From a predetermined initial value, the retry counter is decremented by one for each failed verification; in case of successful verification, it is set back to the initial value. If the value of the retry counter is zero, the verification method is blocked.

Secure Signature Creation Device (SSCD)
A signature creation device fulfilling the requirements in Annex III of the EU directive for electronic signature [EU99].

Signature Creation System (SCS)
A system within the signature creation environment that uses an SSCD to create a qualified electronic signature to data to be signed (ie. the signer´s document and signature attributes).

Verification
Verification means testing if a user is really the person he/she claims to be. The presented data is compared against the previously stored reference data; in case of a match within the specified tolerance limit, the verification is successful. In contrast to the process of identification (see def.), only one biometric comparison is performed. For this reason, the process of verification is also called a "one-to-one-comparison".

Verification Data
The biometric data of a user actually presented during a verification process (which are compared against the previously stored reference data) is called *verification data.*

3.2 Abbreviations

In this study, the following abbreviations are used:

AFIS	Automated Fingerprint Identification System
API	Application Programming Interface
ASV	Automatic Speaker Verification
ATM	Automatic Teller Machine
BS	Biometric Sensor
BT	Biometric Template
CC	Cryptographic Checksum
CG	Cryptogram
CCD	Charge Coupled Device
CRC	Cyclic Redundancy Check
CS	Crypto Sensor
DS	Digital Signature
EER	Equal Error Rate
ESD	Electro Static Discharge
FAR	False Acceptance Rate
FEU	Feature Extraction Unit
FRR	False Rejection Rate
IFD	Interface Device
IK	Individual Key
IRID	Infrared Identification
MK	Master Key
PC	Personal Computer
PCMCIA	Personal Computer Memory Card International Association
PDA	Personal Data Assistent
PIN	Personal Identification Number
PKCS	Public Key Crypto Standard
POS	Point-Of-Sale
PrK	Private Key
PuK	Public Key
PST	Public Signature Terminal
RI	Retina Identification

RND	Random Number
SCS	Signature Creation System
SIM	Subscriber Identification Module
SK	Secret Key for a symmetrical algorithm
SSCD	Secure Signature Creation Device
UART	Universal Asynchronous Receiver Transmitter
USB	Universal Serial Bus
WS	Workstation

4 Signature Creation Systems and Secure Signature Creation Devices

4.1 Signature Creation Systems

- Electronic signatures are produced at signature creation systems (SCS) using secure signature creation devices (SSCDs).

Such a signature creation system may be

- under signer´s control and used at home, in the office or mobile at any place or
- under service provider´s control (e.g. a Public Signature Terminal at an airport or a banking terminal).

An SCS has trusted SCS components and application specific SCS components, as Fig. 1 shows. The trusted components are mandatory if not marked otherwise and relevant for every SCS. The application specific components are application context dependend, i.e. their presence, construction and functionality is application specific.

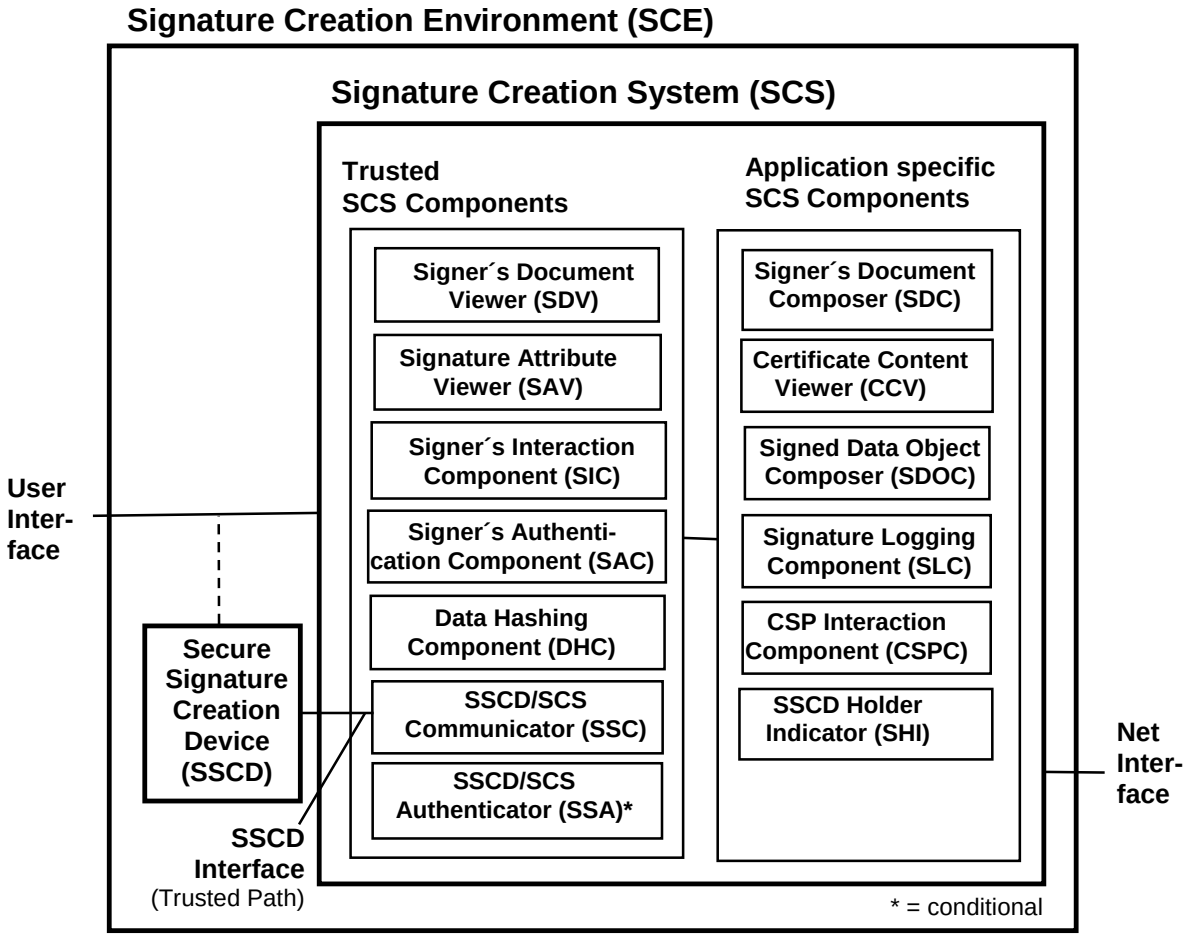

Fig. 1 : Components of a Signature Creation Systems (SCS)

The quality "trusted component" can be achieved either by organisational means or appropriate technical means.

Of special relevance for this study is the Signer´s Authentication Component and the conditional SSCD/SCS Authenticator:

- Signer´s Authentication Component (e.g. card terminal with PIN pad and biometric sensor unit) shall be a trusted SCS component which is used for presenting knowledge based signer´s authentication data (PIN or password) and/or biometric features and preparation of the signer´s authentication data (SAD) in such a way that they can be compared with stored SAD in the SSCD
- SSCD/SCS Authenticator shall be a trusted SCS component which establishes a trusted path between SSCD and SCS (component only relevant for SCS under control of service providers *and* where the trusted path cannot be established by organisational means)

In any case, a trusted path between a signature creation system and a secure signature creation device (e.g. smartcard) is required.
A concrete representation of an SCS is called a signature creation application. One or more signature creation applications may be present in the same physical unit and share possibly some SCS components.

Typical physical units where signature creation applications may be present, are

- PCs in all variants (workstations, laptops, ...) and
- Public Customer Service Terminals (internet terminals, ...),

but also (in the near future or already in use)

- Palmtops,
- PDAs and
- mobile phones.

4.2 Secure Signature Creation Devices

A Secure Signature Creation Device (SSCD) is a signature creation device that is considered to be secure enough for creating Advanced Electronic Signatures by applying the Signature Creation Data of the signer (i.e. its private key) and that meets the requirements of Annex III of the EU directive.

Typical SSCDs are

- smartcards (see Fig. 2)
- SIMs (Subscriber Identification Modules (see Fig. 3) and
- USB tokens (see Fig. 4)

but also

- PCMCIA tokens (see Fig. 5)and
- crypto boxes (see Fig. 6 and Fig. 7).

Fig. 2: Example of SSCD of type smartcard [German physician identity card]

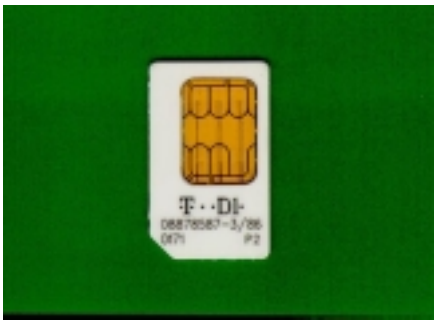

Fig. 3: Example of SSCD of type SIM [GSM card, where an electronic signature function may be added]

Fig. 4: Example of SSCD of type USB crypto token [CRYPTO IDENTITY token of Eutron Europe, Netherlands]

Fig. 5: Example of SSCD of type PCMCIA token [Fortezza Crypto Card of Spyrus, real cover was not available]

Fig. 6: Example of SSCD of type crypto box to be placed inside a system unit [IBM 4758 PCI Crypto Coprocessor]

Fig. 7: Example of SSCD of type crypto box to be inserted into a 5 ¼ " slot [Cipher Box by Giesecke & Devrient]

4.3 SSCDs and Signer Authentication

The EU directive for electronic signatures [EU99] requires that an "advanced electronic signature shall be uniquely linked to the signatory" (see Fig. 8).

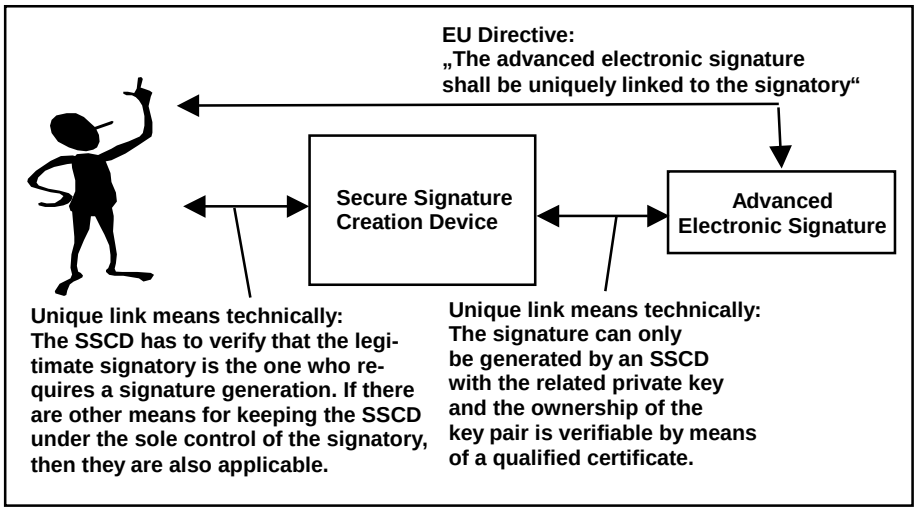

Fig. 8: Linkage of electronic signature to signatory

NOTE - In [EU99] the term "signatory" is used, whereas in this study for brevity the term "signer" is preferred.

Unique link means with respect to the signer authentication prior to each or only the first signature creation during a session:

- for knowledge-based mechanisms the SSCD has to verify that the presented PIN or password is identical with the reference data stored in the SSCD
- for biometric mechanisms, the SSCD has to compare the biometric verification data derived from the live presented biometric feature with the biometric reference data stored in the SSCD and to verify whether the probability is high enough to ensure that the person presenting the biometric feature is the legitimate user.

The comparison of biometric verification data with biometric reference data requires as minimum that the matching algorithm has to be performed in the SSCD; this is necessary, because the SSCD must verify the legitimate owner of the signature creation data, i.e. the SSCD has to check, when the private key for signature creation shall be used, whether the "security conditions" for the usage of this function are fullfilled. Due to the configuration of the SSCD and the security policy of the application provider, the SSCD requires only once a signer authentication and is then open for the creation of several electronic signatures or requires each time a signer authentication as shown in Fig. 9.

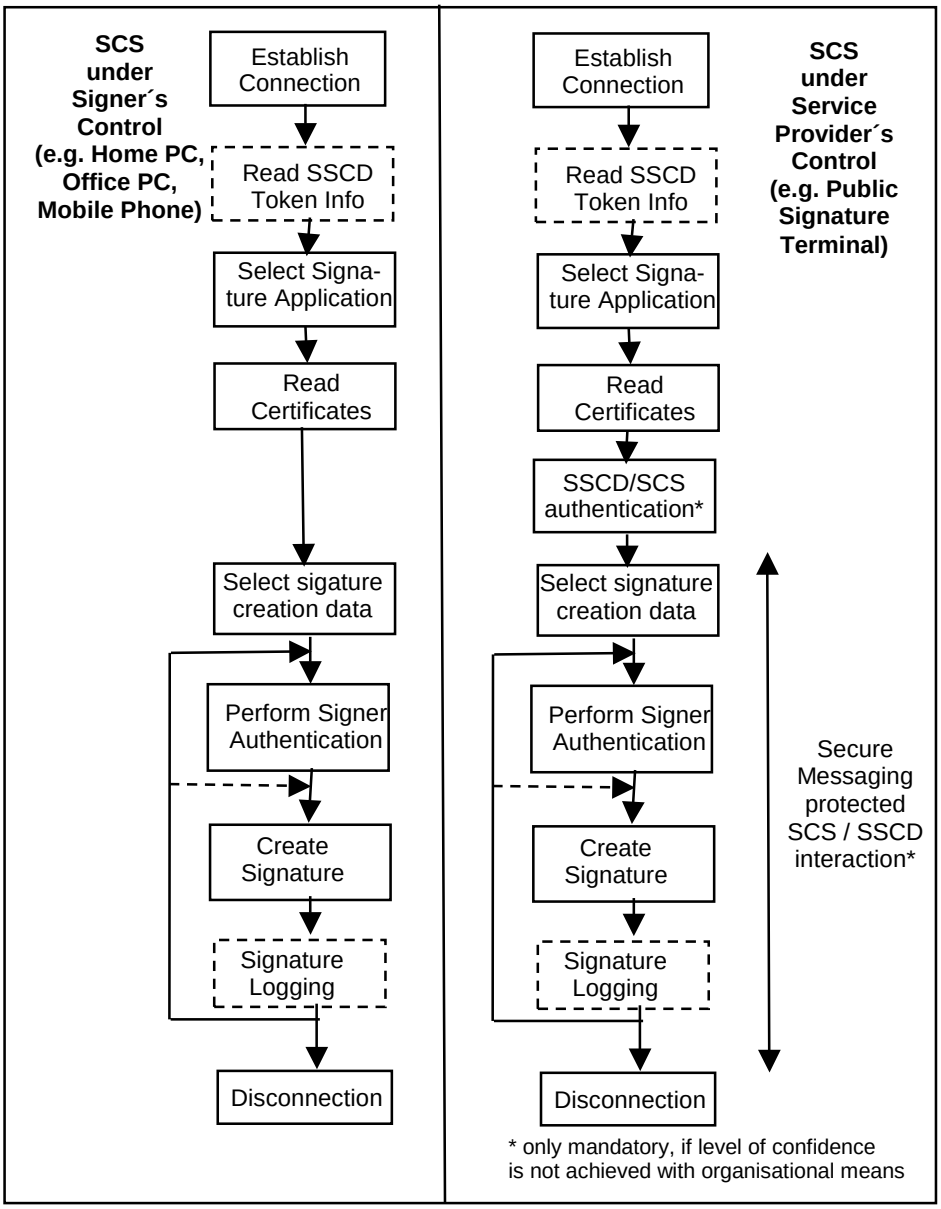

Fig. 9: Typical interaction sequences betwen SCS and SSCD

Since the raw data are in most cases voluminous, many biometric methods apply feature extraction

- to mimimise the data size for the verification data and the reference data and
- to speed up the verification process.

The usual way is therefore, that the biometric verification data consists only of the encoded features as Fig. 10 shows.

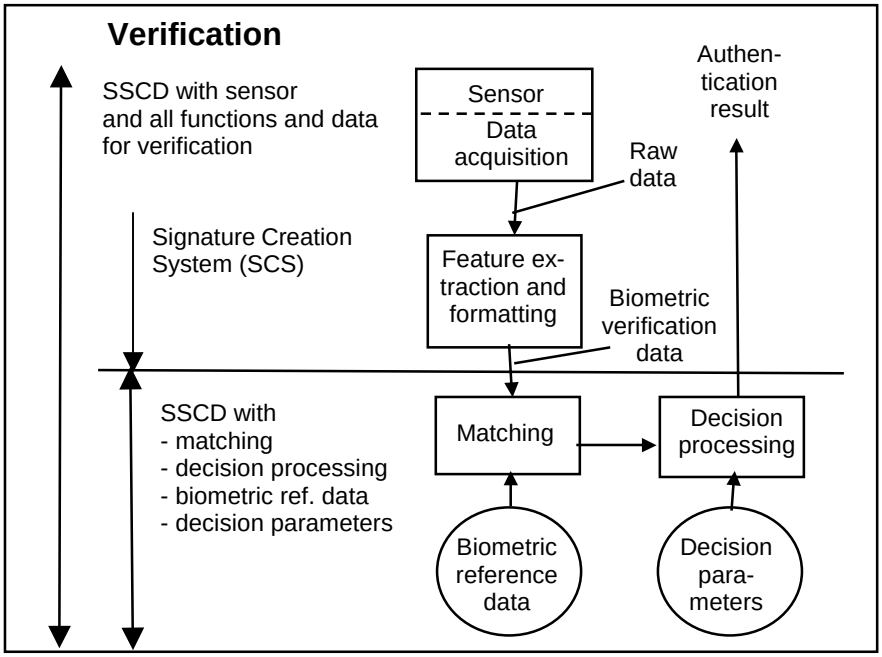

Fig. 10: Possibilities for worksharing between SCS and SSCD

In special cases, depending on

- the SSCD technology and
- the biometric system

it might be possible that also the biometric sensor and the feature extraction is performed inside the SSCD.

4.4 Smartcard Technology

Since the smartcard as a portable SSCD plays an important role for the creation of electronic signatures, the status of the technology shall be outlined. Smartcards currently in use with signature algorithm function have usually

- 8 - 16 bit CPU
- 16 - 64 kByte ROM
- 256 - 2048 Byte RAM
- 4 - 48 kByte EEPROM.

The technology makes rapid progress. New chips are announced which have even more CPU power and extended memory (see Fig. 11).

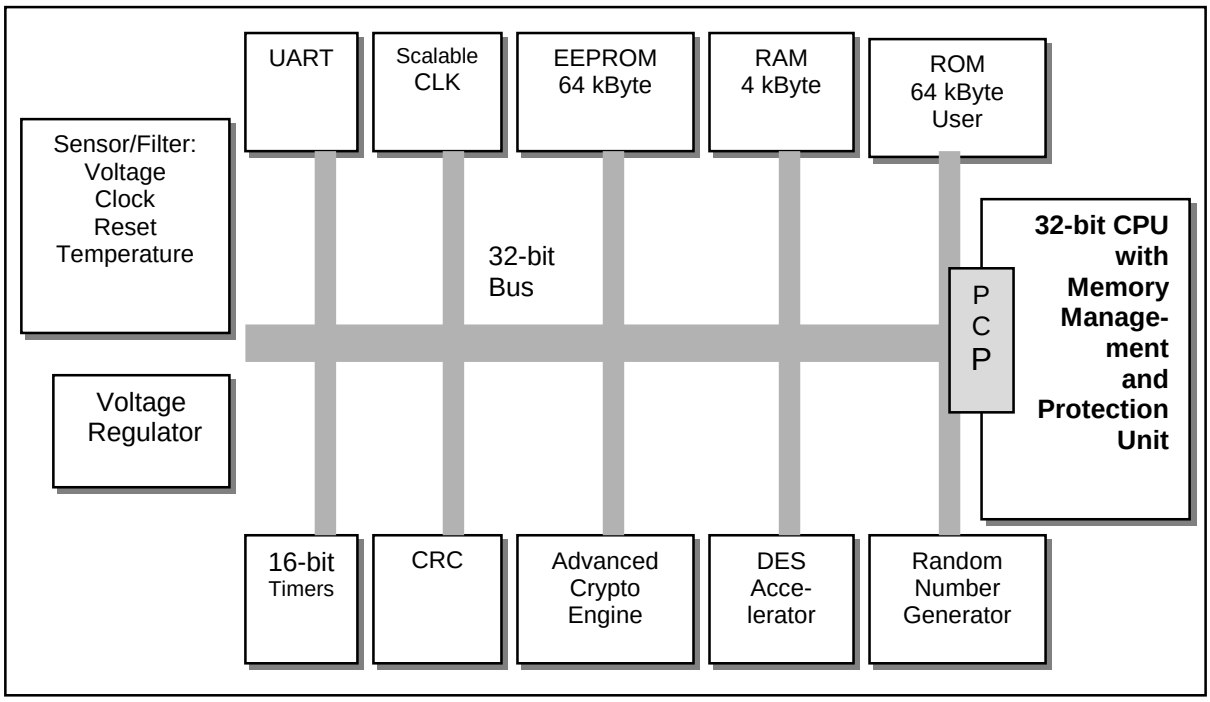

Fig. 11: Block diagram and technical data of a smartcard chip to be issued in 2001 (example)

With these technical capabilities the smartcard technology is or becomes strong enough to support already a variety of biometric methods.

5 Biometric Methods and Characteristics

5.1 Classification of Biometric Methods from the User's and Biometric Viewpoint

5.1.1 Static Methods

For some biometric methods, the user has to present one fixed unchangeable feature; this feature is always present, independent of any special action of the user. From the user's viewpoint, such biometric features where no action is required to present them are called *static biometric features*, i.e. the biometric recognition method is called a *static method.*
Examples of static biometric methods are:

- Fingerprint
- Facial Features
- Hand Geometry Measurement
- Iris Feature
- Retina Identification
- Vein Recognition

These static methods provide the advantage that the user does not have to keep in mind anything like a password in order to be able to present the biometric feature. The disadvantage consists in the fact that there is no or only very limited choice for enrolling different samples or changing the reference data.

5.1.2 Dynamic Methods

Biometric features that are only present in connection with a certain action of the user are called *dynamic features*, i.e. the biometric recognition methods are called *dynamic methods*. (They are also called *behavioural characteristics* since the user is recognised by his/her behaviour.) Using different actions, a dynamic feature can be presented in many different ways that all lead to different biometric data. For a verification or identification process, the user has to repeat the same action as for the enrollment process. Examples of dynamic biometric methods are:

- Speaker Recognition
- Signature Dynamics
- Keystroke Dynamics

Dynamic methods make it easy to enroll different samples or to change reference data. The possible disadvantage is that the user has to keep in mind the required action for presenting the biometric feature, e.g. a certain word or sentence to write, type or speak.

5.2 Biometric Methods in Use

5.2.1 Fingerprint

Fingerprints represent the oldest method of personal identification, its history going back as far as at least 6000 BC. Since 1896, fingerprints have been used for criminal identification. Today, *automated fingerprint identification systems (AFIS)*, used in either forensic or civil applications, represent the most extensive application of biometric identification.

A fingerprint consists of *ridges* (lines across fingerprints) and *valleys* (spaces between ridges). The pattern of the ridges and valleys is unique for each individual. There are two approaches to fingerprint matching: *minutia matching* and *global pattern matching*. The first approach analyses ridge endings and ridge bifurcations, whereas the second approach represents a more macroscopic approach, considering the flow of ridges in terms of, for example, arches, loops, and whorls.

Fingerprints can be used either for verification (one-to-one matching) or for identification (one-to-many matching). In either case, the matching process consists of the following steps [O'Gor99]:

1. Image capture
2. Noise reduction
3. Image enhancement
4. Feature extraction
5. Matching

There are different methods for performing these steps, depending on (often proprietary) algorithms for minutia matching or global pattern matching. The following description outlines the matching process using a minutia-based verification approach.

1. Image capture
   The image area ranges from 0.5 square inches to 1.25 square inches, with an image

resolution of 250 dots per inch to 625 dots per inch.

2. Noise reduction
   Noise occurs due to dirty, cut, scarred, creased, dry, wet or worn finger tips. The aim of this step is to eliminate noise and enhance the ridges. This can be done by applying a *matched filter*, a filter based on the local orientation of the ridges. Everything "in line" with the filter is enhanced, everything oriented differently is eliminated.

3. Image enhancement
   This step consists of binarisation and thinning. The information carried by the enhanced image is binary: ridges against background. Binarisation transforms the input/grayscale image into a binary image. Thinning reduces the width of the ridges down to a single pixel. Binarisation facilitates processing, thinning facilitates the detection of ridge endings and bifurcations.

4. Feature extraction
   Feature extraction means the detection of fingerprint minutiae. Ridge endings are found at termination points of thin lines; ridge bifurcations are found at the junctions of three lines. This step also involves the reduction of extraneous minutiae, which originate, for example, from a noisy input image. The result of feature extraction is the *minutia template*, which includes between 10 and 100 minutiae.

5. Matching
   In the case of verification, the minutia template of the claimant is compared to that of the enrollee. Typically, neighbourhoods of nearby minutiae are compared for similarity. If a comparison indicates only minor differences, the neighbourhoods are said to match. These comparisons are performed for all combinations of neighbourhoods and if a sufficient number of matching neighbourhoods is found, the fingerprints are said to match. Please note that fingerprints will rarely match exactly, due to the noisy input image and the elastic nature of the skin. A *match score* between 0 and 1 (or 10 and 100) indicates the extend of similarities found. The match score can be adjusted by the end-user.
   In the case of identification, the fingerprints stored in the database are categorised by pattern type. A comparison of the pattern types of the input fingerprint and the database of fingerprints eliminates the majority of non-matching fingerprints. The rest of the fingerprints are compared to the input fingerprint using the minutia-based verification described above.

Fig. 12: FP_processing (Sequence of fingerprint processing steps: a) original, b) orientation, c) binarised, d) thinned, e) minutiae, f) minutia graph).

Fig. 12 presents the sequence of fingerprint processing steps.

The *recognition rate*, which is determined by the false acceptance rate (FAR) and false rejection rate (FRR, see def.), measures the utility of a fingerprint system for a particular application.
The enrollment process is crucial for obtaining a high recognition rate, since verification (identification) depends greatly on the enrollment template. Hence, special effort is applied for obtaining the highest-quality input image. For example, a fingerprint may be captured multiple times and the best taken or some combination of each taken as the enrolled fingerprint.

The recognition rate can be enhanced by using not just one, but two or more fingers. However, this will also increase recognition time.
Special care must be taken to prevent fraud, e.g. applying artificial fingerprints or dead fingers. *Anti-spoofing deterrents* are designed to detect fraud by measuring skin temperature, resistance, or capacitance.

A fingerprint template requires approximately 500 bytes of memory storage.

5.2.2 Facial Features

As opposed to some other biometric methods, face recognition is an established method of human identification. This and the fact that cameras can be considered as standard computer equipment with numerous application areas (not just as a biometric sensor) makes face recognition play a superior role in biometric identification.

The environment of a face recognition system has an important impact on the face recognition process. In a *controlled environment*, frontal and profile photographs of human faces are taken, complete with a uniform background and identical poses among the participants. These face images are commonly called *mug shots*. Mug shots are then normalised in terms of the size and position of the face. Face recognition algorithms which are based on such *canonical face images* have been successfully developed [Wen99]. In an *uncontrolled environment*, face recognition is much more complicated. There may be none, one, or several faces in an image, with varying lighting conditions; faces may appear at different scales, positions and orientations; facial expressions may differ, as do facial hair, make-up and glasses. In such uncontrolled environments, *face detection* and *face localisation* are two steps that must be performed first to yield canonical face images.

There are numerous face recognition algorithms: traditional algorithms are based on *manually defining features*, whereas *automatically deriving features* are used today. Manually defining features means that geometry-dependent features of the face are defined by humans, such as the distance between eye corners, mouth extremities, nostrils and chin top. However, face recognition algorithms based on this approach are not satisfactory in terms of their reliability, because the number of features measurable is small and their accuracy questionable. Algorithms regarding automatically deriving features, also called *holistic algorithms*, are based on neural networks, template matching, or Eigenfaces.

Besides the advantages of face recognition stated above, namely the convenience of using cameras as biometric sensors and the acceptability by the public, there is the advantage that face recognition is fast and discrete (hidden cameras). However, there are several disadvantages:

- The face varies due to aging, make-up, hair, glasses etc.
- It is almost impossible to recognise the faces of identical twins.
- Uncontrolled environments cause problems, for example, due to extreme lighting conditions.
- In order to prevent false acceptance, it is important to protect the system against fraud using e.g. photos, masks, video.

A face template requires about 3-4 kBytes of memory storage

5.2.3 Hand Geometry Measurement

The idea of using body measurements for identifying people arose in ancient Egypt. The first mechanical hand geometry readers were then developed in the late 1960's, with electronic devices following in the mid-1980's. Today, hand geometry reading is an established method of human identification, especially in access control applications.

Each human hand is unique. Measurements like finger length, width, thickness, curvatures and their relative location distinguish one individual from another. Modern hand geometry readers use a charge coupled device (CCD) camera and infrared light emitting diodes (LEDs) with mirrors and reflectors to capture black and white images of the human hand. Two images are taken, one from the top and one from the side. This method is called *orthographic scanning*. Fig. 13 shows a model of the human hand with typical hand geometry measurements [Zun99, p.89].

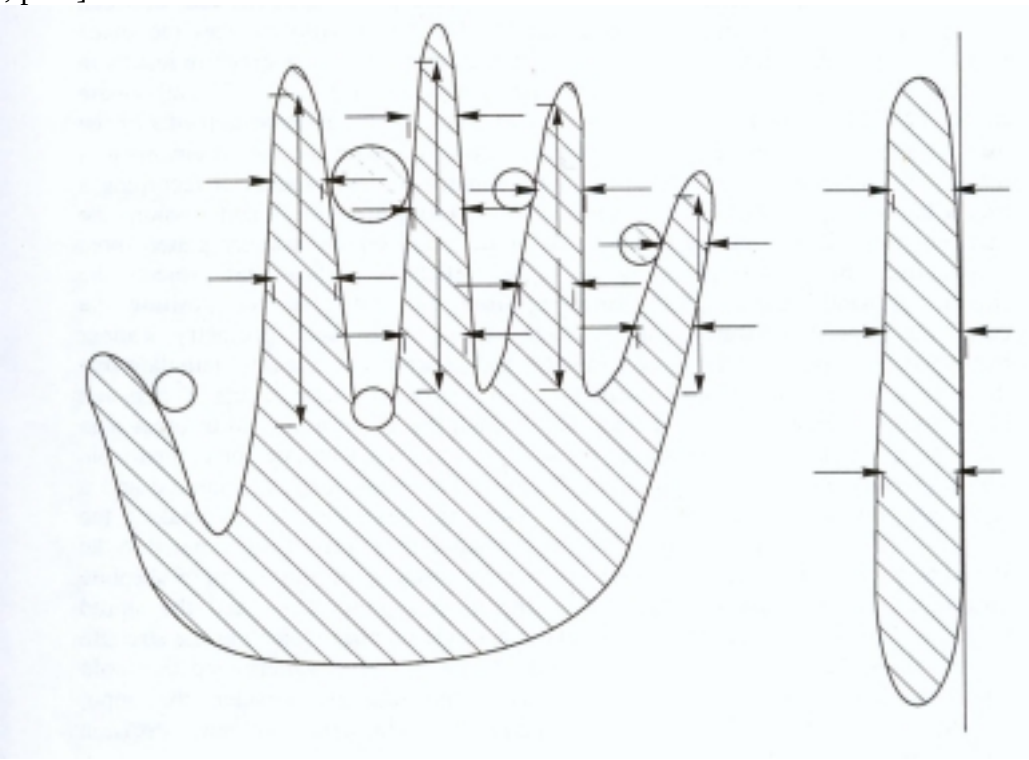

Fig. 13: Typical hand geometry measurements

Fig. 14 represents a model of hand scanner optics. The optical path, that is, the distance between camera and platen measures about 28cm. The optical path can be reduced by half by employing a mirror. This architecture implies that a typical hand geometry scanner is about 22cm square by 25cm high. The platen, which is a highly reflective surface, is equipped with a number of pins to guide the position of the human hand. The scanner takes in the order of 100 measurements of the human hand.

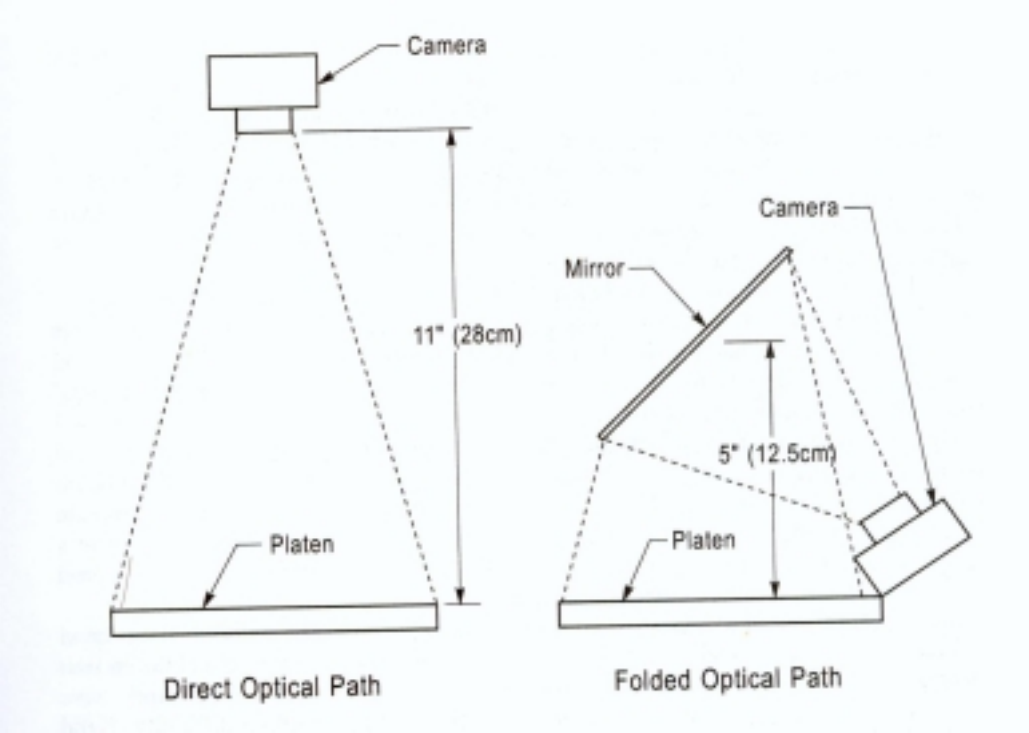

Fig. 14 :Hand scanner optics

During enrollment, several images of the human hand (usually 3) are taken. A mathematical average is calculated by the hand geometry scanner and the reference template is generated and stored. During verification, a single image of the human hand is taken and compared with the stored template. The comparison may involve the accumulation of absolute differences in the individual measurements of the reference template and the input data. The comparison yields a single number indicating the strength of the similarity (score) or their difference (distance).

Hand geometry templates are used for verifying a person's identity. However, templates are not sufficient for identification since they cannot be reversely engineered. Hence, hand geometry is suitable for verification but not for identification.

Using a hand geometry reader requires training and experience. For example, different platen heights (e.g. for sitting or standing persons) affect the hand shape and can cause false rejection. Hence, a hand placement training is recommended before enrollment.

A hand geometry template requires about 20 bytes of memory storage.

5.2.4 Iris Feature

The iris is composed of elastic connective tissue, the so-called *trabecular meshwork*. It consists of pectinate ligaments adhering into a tangled mesh revealing striations, ciliary processes, crypts, rings, furrows, a corona, sometimes freckles, vasculature, and other features [Dau99]. Although the colour of the iris changes during the first year of life, the trabecular meshwork itself is stable throughout the lifespan. The pattern of the iris reveals about 266 independent degrees-of-freedom of textural variation across individuals. This makes the iris an exceptionally accurate biometric. Hence [Neg2000],

- The iris reveals an extremely data-rich physical structure
- The property of *genetic independence* means that no two eyes are the same, not even for the same person or for identical twins.
- The iris pattern is stable throughout the lifespan.
- The iris is physically protected by the cornea that does not inhibit external viewability.
- The pattern of the iris can be encoded from distances of up to one meter.

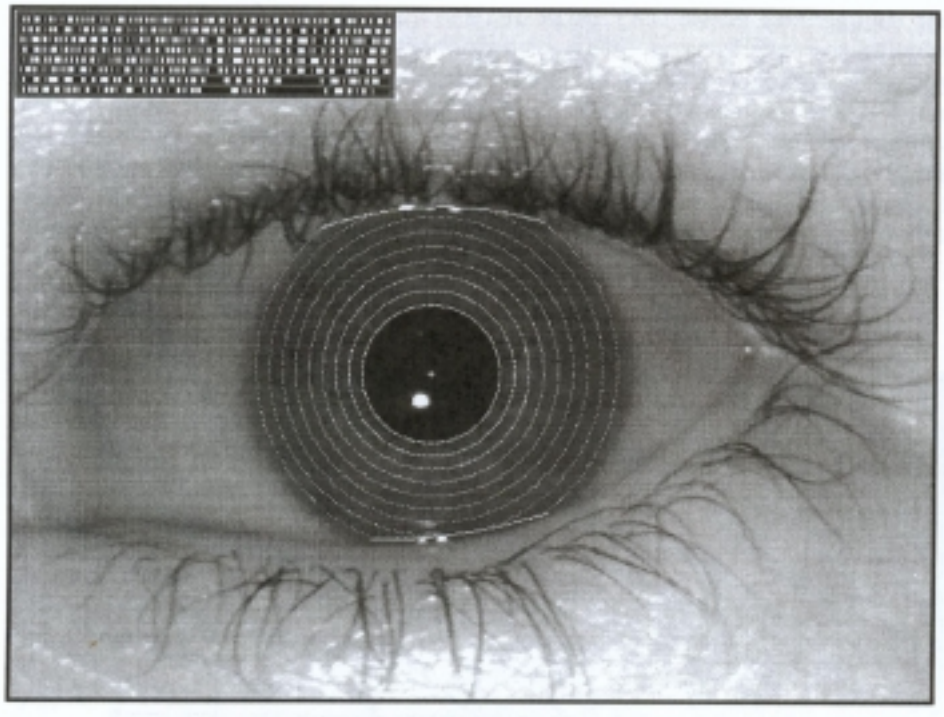

Fig. 15: Isolation of an iris for encoding, and its resulting iris code

John Daugman of Cambridge University, England, developed an efficient algorithm for converting an iris image into numerical code, the *iris code* (see Fig. 15). The iris code, which requires 256 bytes of memory storage, allows for efficient comparison of irises by calculating their *Hamming distance*. The Hamming distance is defined to be the fraction of mismatched bits between two iris codes; for two identical images of an iris the HD is 0, for two different irises the HD is about 0.5, and for two different images of the same iris, the HD ranges from approximately 0.05 to 0.1. A HD threshold of 0.342 results in a FRR and FAR of 1 in 1.2 million. This extremely low error rate makes the iris an ideal biometric for large-database identification applications with high security demands. All current commercially available systems for iris recognition are based on the algorithms of John Daugman, by software licence of the executable binary code [Dau94].

There are several methods for detecting fraud. One could imagine that a photograph, a video tape or a fake iris printed onto a contact lens could be used to fool the iris recognition system. One countermeasure is the monitoring of the pupil. Even in the absence of illumination changes, there is a small oscillation called a *hippus*. In the presence of illumination changes, the pupil reacts with constriction and dilation accordingly within a certain time period. Moreover, it is possible to monitor reflections from the moist cornea of the living eye.

Different setups for iris recognition systems are possible [Neg2000]:

- Public-use systems:
  For example for ATMs. Such systems require minimal user cooperation and training. The system automatically locates the user's eye, computes an iris code, and validates it through comparison with the enrolled iris code. The systems requires about 2.5 seconds for the full recognition process.
- Personal-use systems:
  The user manually positions the camera three to four inches in front of the eye. This process requires the user to align the camera and the eye.

5.2.5 Retina Identification

In 1935, Drs. C. Simon and I. Goldstein discovered the uniqueness of the retinal vascular pattern; every eye has a totally unique pattern of blood vessels.

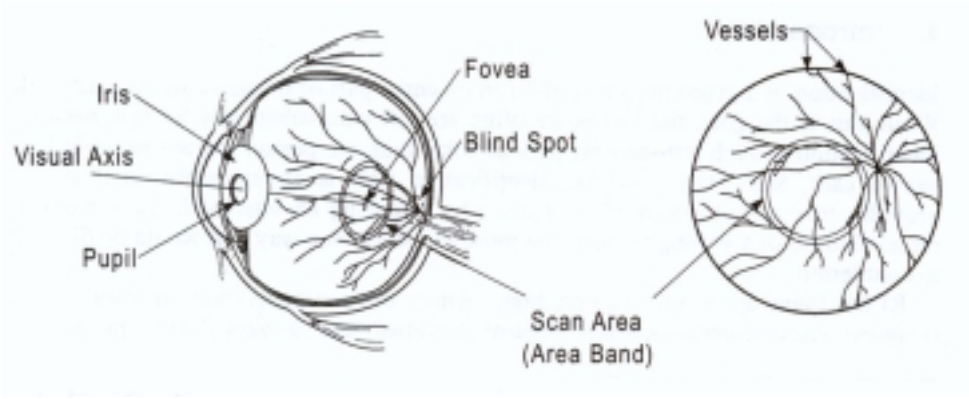

Fig. 16: Retina: Eye and scan circle (area band)

The retina is located on the back inside of the eyeball. Blood reaches the retina through vessels that come from the optic nerve. Just behind the retina is a matting of vessels called the choroidal vasculature (see Fig. 16) [Hil99]. For retina identification (RI), the retina is illuminated using infrared light. Since the retina is transparent to this wavelength of light, the choroidal vasculature reflects the light and the returned information is captured by the RI camera and evaluated by the computing subsystem. Only an annular region of retina, called the *scan circle*, is captured which represents the smallest possible region of visible retina (corresponding to the worst case of very small eye pupils).

There are a number of properties which make retina identification a highly accurate and secure biometric identification method:

- *Genetic independence,* that is, the fact that no two eyes are the same is true for retina identification as well as for iris recognition.
- The retinal vascular pattern is stable throughout the lifespan.
- Because of its internal location, the retina is protected from variations caused by the external environment.

However, there are a number of problems regarding RI:

- Difficult usage
  The subject must be aligned with the RI camera and fixated on its target. Eyeglasses must be removed. Because of that, people with severe astigmatism may have problems

fixating on the target. The distance between subject and camera must not exceed a certain limit (e.g. 12 inches). Usage of RI, especially for enrollment is difficult and requires the assistance of an enroller.

- Perceived health threat
  Although this fear is unfounded, many people think that RI can hurt the retina.
- High sensor cost
  Although prices are dropping, the camera equipment puts a lower limit on the cost of the system which will always be more expensive than e.g. fingerprint or speaker recognition.

A retina template requires approximately 40 bytes of memory storage.

5.2.6 Vein Recognition

Vein biometric systems record subcutaneous infrared absorption patterns. Veins and other subcutaneous features present large, robust, stable and largely hidden patterns. Subcutaneous features can be conveniently imaged within the wrist, palm, and dorsal surfaces of the hand. The technology can be applied to small personal biometric systems, e.g. Biowatches and Biokeys and to generic biometric applications including intelligent door handles, door locks etc. [VBHP].

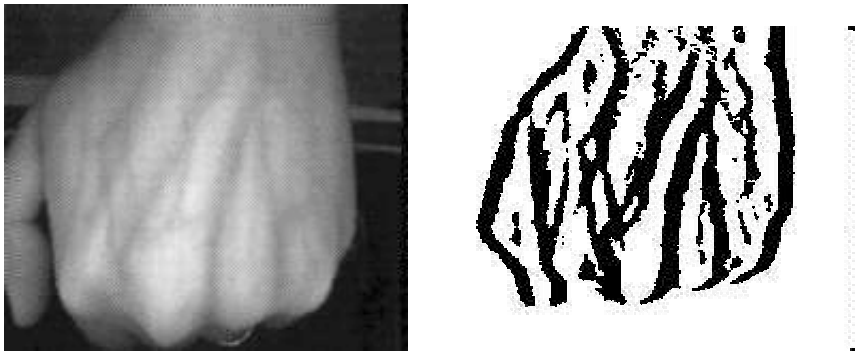

Fig. 17: Grey-scale and binarised vein images

Fig. 17 shows a grey-scale infrared vein image and a binarised vein pattern template.

5.2.7 Signature Dynamics

The style of handwriting is unique to each person and handwritten signatures on paper have been used from time immemorial as a means of authentication. Automatic signature verification aims at the computer-based verification of signatures. There are two approaches to signature verification: *static* and *dynamic*. Static signature verification, also called *off-line signature verificatio*n, aims at the analysis of the static image of the signature while dynamic or *on-line signature verification* evaluates the action of signing itself, in terms of total time taken, or the average or root-mean-square speed, acceleration, force, and pressure [Nal99].

Static signature verification which is needed for the automated verification of cheque signatures and signatures on official documents poses many problems regarding the achieved error rates FAR and FRR. Approaches to static signature verification are numerous and are based on e.g. similarity measurement, base heuristic, dynamic programming or neural networks.

In dynamic signature verification, the choice of signals that can be processed is fairly large (the x and y coordinates of a pen tip as a function of time, speed, acceleration, pressure, etc.) [Lec94] and therefore, the signal acquisition process is important to the whole verification process. Special equipment is used to support the acquisition step, for example, an instrumented pen or a digitised graphics tablet (see Clause 9.6). There are numerous approaches to dynamic signature verification based on e.g. comparison techniques (regional correlation, elastic matching, and tree matching), segmentation or neural networks.

Signature verification is one of the least accurate biometrics; the matching process is difficult and the user can easily change his signature to generate a false rejection. However, an inherent advantage of signature verification is that the signature has been established as an acceptable form of personal identification method and can be transparently incorporated into the existing business processes requiring signatures. An advantage of dynamic signature verification is that it is impossible for an impostor to obtain the dynamics information from a written signature.

5.2.8 Speaker Recognition

Speaker recognition [authentication | verification], also called talker or voice recognition [authentication | verification], involves the use of a microphone to verify a person's claimed identity from his voice. This technique is suitable for identification as well as for recognition, that is, when there is no a priori identity claim [Cam99].

Automatic speaker verification (ASV) systems represent the most natural and economical methods of biometric authentication of an individual. The ubiquitous telephone network and microphones being integrated in computers, the cost of an ASV system might only correspond to the cost of the software for the recognition system.

There are *text-dependent* and *text-independent systems* for speaker recognition: in text-dependent recognition, the phrase is known to the system and it can be fixed, or not fixed and prompted (visually or orally). In text-independent recognition, the phrase is arbitrary. The latter is generally more difficult to implement.

An ASV system works as follows: prior to a verification session, the user must enroll into the system. During this enrollment, voice models are generated and stored (possibly on a smart card) for use in later verification sessions. There is a tradeoff between the recognition accuracy and the duration of speech during the enrollment-session and the number of enrollment sessions. For verification, text-dependent ASV systems prompt specific phrases to the user, who speaks the corresponding words into a microphone. In addition to his voice, ambient room noise and delayed versions of his voice enter the microphone via reflective acoustic surfaces. The speech signal is analysed by the verification system that makes the decision to accept or reject the user's authentication. In some cases, the verification system requests additional input before making a decision.

Generally, people accept a speech based biometric system. However, ASV systems are sensitive to a number of factors [Cam99]:

- Misspoken or misread prompted phrases
- Extreme emotional state
- Time varying (intra- or intersession) microphone placement

- Poor or inconsistent room acoustics (e.g. multipath and noise)
- Channel mismatch (e.g. using different microphones for enrollment and verification)
- Sickness (e.g. head colds)
- Aging

Still, ASV systems can achieve an equal error rate of 0.5%. This, together with the fact that speaker verification works with a microphone or a regular telephone handset makes this a very popular biometric method.

A voice recognition template requires about 1000 bytes of memory storage.

5.2.9 Keystroke Dynamics

The same neuro-physiological factors that make written signatures unique are exhibited in an individual's typing pattern. Keystroke dynamics analyses the way a user types at a terminal by monitoring the keyboard inputs thousands of times a second, and aims to identify users based on specific habitual typing rhythm patterns [Mil94]. Computer users can be authenticated by analysing keystroke latencies (that is, elapsed time between keystrokes), hold times, finger placement and applied pressure on the keys [Oba99]. Keystroke dynamics is a behavioural/dynamic biometric.

A computer user types for a while, pauses to collect thoughts and ideas, pauses again to take a rest, continues typing, and so forth. There are two models describing the interactions between user and computer system, the *keystroke-level model* and the *hold times model*. The keystroke-level model measures the inter-character time intervals as the user types a known sequence of characters (for example, the user's login string), whereas the hold times model measures the time durations between the moment every key button is hit to the moment it is released to authenticate computer users. Evaluation algorithms are based on traditional pattern recognition techniques and neural network paradigms correspondingly. Hold times are more effective than interkey times, but the best performance can be achieved by using both time measurements.

Keystroke dynamics is a very economical biometrics because it does not involve the acquisition of extra hardware. Instead, it uses the computer keyboard. Another advantage of this biometric method is its non-intrusiveness meaning that it will be accepted by a large number of users. However, keystroke dynamics is a very new technology and not yet ready for the application in high security environments. Open problems include how to deal with typographical errors, the permanence of this behavioural biometric (the characteristic should not change over time), its uniqueness (no two persons should be the same) and universality (each person should have it).

5.3 Biometric Methods under Development or of Less Relevance in this Context

In this clause, a number of biometric methods which are either under development or which are less relevant for electronic signatures will be described briefly:

- Skin and epithel structure – ultrasound finger identification
- Facial thermogram – infrared identification (IRID)
- Palmprint
- Gait recognition

- Odour measurements
- Ear shape recognition
- DNA-based identification

5.3.1 Ultrasound Finger Identification

With the aid of ultrasound technique, it is possible to recognise the surface of a fingerprint as well as the structure of the skin and epithels. These features are much harder to forge than ordinary fingerprint images.

5.3.2 Facial Thermogram – Infrared Identification

IRID uses cameras in the infrared spectrum to take *facial (or body) thermograms*. The thermal patterns seen by an infrared camera derive primarily from the pattern of blood vessels under the skin which transport warm blood throughout the body [Pro99]. The recognition algorithms for IRID correspond to those used for face recognition. The main advantages of IRID are that it is completely passive, it can be performed from a distance, and it yields very reliable recognition results. However, sensor cost is quite high.

5.3.3 Palmprint

So far, two approaches to hand identification have been reviewed: fingerprint and hand geometry. Palmprint represents a third possibility which is still under development [ShZh98]. There is rich and useful information in a palmprint:

- Geometry features (such as width, length, and area)
- Principal-line features (location and form of life, heart, and head line)
- Wrinkle features
- Delta-point features (centre of a delta-like region in a palmprint)
- Minutiae features (ridges of a palmprint)

The main advantage of palmprint is that it works well in the presence of noise in the palmprint image, because the main features (geometry, principal-line and wrinkle) can be obtained from a low-resolution image. More effective features, such as delta points and minutiae can be gained when both the resolution and the quality of the palmprint image are high.

5.3.4 Gait Recognition

Biometric studies on *gait recognition* have emerged recently [Nix99], with a strong relation to other subjects, including medical studies, psychology, human body modelling and motion tracking. Using gait recognition, people are recognised by the way they walk. Essentially, computer vision techniques are used to derive a gait signature from a sequence of images. The main advantage of gait recognition is that it requires no contact. However, there may be problems regarding the recognition of e.g. drunken, pregnant, or ill people. On the whole, this approach requires further investigation.

5.3.5 Body Odour Measurements

Automated methods for *odour measurement* are required in various application areas. For example, industrial processes and agricultural operations produce odours, but also malodours and chemically toxic substances that need to be monitored and controlled [Per99]. The idea of using odour measurements as biometric method originates in the observation that body odour has a genetic influence and can be used to distinguish identical twins from unrelated people. Although the odour profile of the human body is affected by habits such as the use of perfumes, or diet and medication, it can still be used for recognition. Please note that trained dogs are able to distinguish between persons on the basis of odour. Electronic nose systems are being developed as intelligent chemical array sensor systems. However, their use for biometric authentication does not seem to be realistic in the near future.

5.3.6 Ear Shape Recognition

The ear reveals a unique structure that can be used as an effective biometric for passive identification (does not need direct interaction). Its features are both reliable and robust. Cameras can be used to capture an image of the ear which is then processed in terms of e.g. Iannarelli's System (taking 12 measurements of the ear) or the ear biometric graph model [Bur99]. Ear biometrics is a novel approach which seems to have a promising future. However, there are problems regarding ears covered by hair, hats etc. or ears that cannot be revealed for religious reasons.

5.3.7 DNA-based Identification

Genetic traits, displayed at their most fundamental level in DNA (deoxyribonucleic acid), provide an excellent tool for both species and individual identification [Rud99]; there are many applications for *DNA profiling*, including medical science, environmental science, historical research, and forensic science. However, since DNA typing is a slow, labour intensive and difficult to automate process, the application of DNA profiling as biometric method is a long-term vision.

5.4 Unimodal, Multimodal and Combined Biometrics

A biometric system which uses only a single biometric characteristic is called a *unimodal biometric system*, whereas a biometric system which uses multiple biometric characteristics is called a *multimodal biometric system* [HJ99].
If in the same verification process several biometric characteristics are involved, e.g. face and voice recognition, then it is called a *combined biometric* system.
Signature application systems will be usually multimodal biometric systems for reasons which are outlined in clause 11.1.
The use of combined biometric methods for verification cannot improve the verification speed, but only the verification accuracy. It may be more robust to fraudulent technologies, because it is more difficult to forge multiple biometric characteristics. However, a verification process with combined biometrics takes more time and is well suitable e.g. for login control, but considered as less suitable in the electronic signature context not only with respect to time consumption, but also with respect to the increased complexity for the matching algorithm to be placed in the SSCD.

5.5 Suitability of Biometric Methods for Electronic Signatures

Evaluating the different biometric methods regarding their suitability for electronic signatures involves a number of important factors. The following *biometric requirements* represent some general requirements for the evaluation of biometric methods [JBP99].

- Universality
  each person should have the characteristic
- Uniqueness
  no two persons should be the same in terms of the characteristic
- Permanence
  the characteristic should neither change nor could be altered
- Collectability
  the characteristic can be measured quantitatively
- Performance
  achievable identification accuracy, speed, and robustness, the resource requirements to achieve the desired identification accuracy and speed, as well as operational or environmental factors that affect the identification accuracy and speed
- Acceptability
  the extend to which people are willing to accept a biometric method in their daily lives
- Forgery Resistance
  reflects the security of the system against being fooled by fraudulent methods (In [JBP99], the term "circumvention" is used instead.)

Each biometric method reviewed above has its own advantages and disadvantages. Tab. 1 provides a comparison regarding the seven requirements of biometric methods introduced earlier [JBP99].

Biometrics	**Universality**	**Unique-ness**	**Permanence**	**Collectability**	**Perfor-mance**	**Acceptability**	**Forgery Resistance**
Fingerprint	medium	high	high	medium	high	medium	high
Face	high	low	medium	high	low	high	low
Hand Geometry	medium	medium	medium	high	medium	medium	medium
Iris	high	high	high	medium	high	low	high
Retina	high	high	medium	low	high	low	high
Signature Dynamics	low	low	low	high	low	high	low
Speaker Recog-nition	medium	low	low	medium	low	high	low
Keystrokes	low	low	low	medium	low	medium	medium
Hand Vein	medium	medium	medium	medium	medium	medium	high
Facial Thermogram	high	high	low	high	medium	high	high

Tab. 1 : Comparison of biometric methods regarding general biometric requirements according to [JBP99]

In addition, there are a number of particular requirements for the evaluation of biometric methods in relation to electronic signatures:

- Cost
  regarding the hardware (sensor) and software required for every user

- Usability
  Ease of use regarding the signature tool (software and hardware); disruption of the user
- Maintenance
  required concerning the operation of the sensor over a longer period of time

Biometrics	Cost	Usability	Maintenance
Fingerprint	medium	easy	medium to high
Face	medium	difficult	medium
Hand Geometry	high	medium	medium
Iris	high	easy	medium
Retina	high	difficult	medium
Signature Dynamics	medium	easy	medium
Speaker Recognition	low	easy	low
Keystrokes	low	medium	low
Hand Vein	medium	easy	medium
FacialThermogram	medium	difficult	medium
NOTE - This table does not take into account, whether the related method and a concrete realisation meets the strength of function required to be usable as signer´s authentication method.			

Tab. 2: Comparison of biometric methods regarding particular requirements for electronic signature applications according to the author's view

Tab. 2 presents the comparison of biometric methods regarding particular requirements for electronic signature applications. The cost is low for those biometrics not requiring special hardware, and high for hand geometry, retina, and iris which require expensive optical equipment. The usability is difficult for all biometric methods which require interactive user handling, that is, the user has to focus his face, iris or retina into a corresponding frame which is usually presented on the computer screen, and easy for all biometric methods which do not need any feedback (e.g. putting finger on sensor, typing a word, or speaking a phrase). Hand geometry is of medium difficulty, since it requires a specific training. Maintenance is low for biometric methods not requiring specific hardware (speaker recognition and keystroke dynamics). Fingerprint has been assessed as requiring medium to high maintenance, although this statement has to be refined. The optical sensors that handle dry finger problems use a silicone coating that tends to wear quickly. Silicon sensors where the user touches the chip can all suffer from electro-static discharge (ESD) and fragility issues since the silicon is exposed directly to the user. Some fingerprint sensors, however, are quite durable. The other biometric methods introduced use a digitising tablet or electronic pen (signature dynamics) or optical equipment and require medium maintenance.

Environment Biometrics	Home / Office (PC / WS / Laptop)	Mobile (any Place) (Mobile Phone / PDA / Laptop)	Public Environment (Banking Terminal / Payment Terminal / Internet Terminal)
Fingerprint	yes	yes	yes
Face	yes	yes (condit. for mob. phone)	yes
Hand Geometry	yes	no (impractical)	less suitable (impractical)
Iris	yes	no (impractical)	yes
Retinal Scan	less suitable	no (impractical)	no (impractical, vandalism)
Signature Dynamics	yes	less suitable (impractical)	less suitable (impractical; vandalism problem, if special pen)
Speaker Recognition	yes	yes	no (environmental noise)
Keystrokes	yes	no (yes for laptop)	no (lack of unique keyboards)
Hand Vein	yes	no (impractical)	less suitable (impractical)
Facial Thermogram	yes	no (impractical)	yes
NOTE - This table does not take into account, whether the related method and a concrete realisation meets the strength of function required to be usable as signer´s authentication method.			

Tab. 3: Comparison of biometric methods regarding suitability in different signature application environments according to the author's view

Another important factor for the evaluation of biometric methods in relation to electronic signatures is the application environment (see Tab. 3). All methods are suitable in a controlled home/office environment, whereas methods requiring a bulky, fragile sensor are unsuitable in a mobile environment. Signature devices in public environments, such as public signature terminals and bank terminals, have to be evaluated more from the durability/fragility viewpoint; in such environment it is best to apply a passive biometric method (no direct interaction of user required) or a biometric method whose corresponding sensor is robust.
Finally, the frequency of signatures has an influence on choosing a corresponding method since a biometric user authentication is required for each individual electronic signature. In an environment where electronic signatures are applied frequently (like e.g. a banking or a legal application), there are different demands than in an environment where electronic signatures are applied occasionally only; for environments with frequently applied signatures, only those biometric methods with are fast and which require minimal user interaction can be used (see Tab. 4). Please note that the last tables represent our own assessment of the different biometric methods regarding cost, usability, maintenance, corresponding signature environment and signature frequency. It is not based on practical experience (since there are no SSCD products with biometrics yet), but on our own estimation and literature sources corresponding to the different biometric products.

Biometrics	Suitability for many subsequent verifications
Fingerprint	good, simple use
Face Recognition	good
Hand Geometry	medium / less practical
Iris	medium / less practical
Retinal Scan	less practical
Signature Dynamics	good; strong analogy between electronic and handwritten signature
Speaker Recognition	medium
Keystrokes	less practical; similiar to, but more expendable than PIN presentation
Hand Vein	medium / less practical
Facial Thermogram	good
NOTE - This table does not take into account, whether the related method and a concrete realisation meets the strength of function required to be usable as signer´s authentication method.	

Tab. 4: Comparison of biometric methods regarding suitability for many subsequent verifications (verification prior to each signature) according to the author's view

The above considerations represent an evaluation of biometric methods in terms of specific requirements in an electronic signature environment. From the discussion, it is obvious that there is not one ideal biometric method. All biometric methods have advantages and disadvantages correspondingly. However, some biometric methods are more suitable than others for electronic signature applications. From our point of view, the most important factors in an electronic signature environment are

1. Security of biometric method (universality, uniqueness, permanence, collectability, performance, circumvention, strength of mechanism)
2. Acceptability by the user
3. Cost
4. Usability - ease of use
5. Market maturity - state of development

One biometric method that performs well in all the above categories is fingerprint; it is also the biometric method supported by the majority of biometric products. Other biometric methods that seem suitable are face recognition and signature dynamics. However, before one or multiple biometric methods can be chosen for a specific electronic signature application, a detailed evaluation of the application environment and constraints needs to be performed.

6 Knowledge-based versus biometric Authentication

6.1 Advantages of Biometric Features

Biometric authentication methods have the general advantage over knowledge-based methods that it is not possible to give the biometric feature to someone else (neither intentionally nor unintentionally). A password can be given to another person such that he/she can use it in the same way as the legal owner, but a biometric feature can be used in a natural way by the legal owner only.

In this sense, a biometric feature is really bound to a person and not only related to a person. These arguments are valid for static as well as for dynamic biometric features.
Static biometric features have the additional advantage that they cannot be lost or forgotten. You can always loose a key or forget a password, but a static dynamic feature is always present with the person.
Of course, this argument is not valid for dynamic biometric features that require a certain action to be presented. It may happen that the user forgets which exact action to perform (e.g. the word or sentence to speak for voice recognition or to write for Writing Dynamics Recognition.)

6.2 Public Static Biometric Data

Care must be taken to the fact that some static biometric data are publicly available. While knowledge-based authentication systems depend on the fact that the PIN or password is kept secret, this cannot be demanded for all biometric authentication systems using static features. You have to keep in mind that it is always possible to get a facial image from a camera or other sources or fingerprint images from glasses; these data could be digitised and fed into a biometric system, pretending to be captured by the biometric sensor.
For this reason, the security of a biometric authentication system may not depend on keeping the verification or reference data secret; it is rather necessary that the data are transported from the biometric sensor to the verification or identification process authentically, i.e. the process is able to recognise that the data were really live captured by the sensor.

6.3 Preprocessing of Biometric Data

Whereas a PIN or password, after typing in, is directly passed to the verification process or stored as reference data, this is not the case for biometric data. Biometric raw data captured by the biometric sensor (as for example complete grey scale images of faces or fingerprints) are far too large for direct processing or being stored in a smartcard. A preprocessing is required where characteristic features are extracted out of the raw data; this step may also contain some normalisation functions for eliminating disturbances.
This step of feature extraction means an additional necessary calculation step between data capture and data comparison which is not present for PIN or password authentication schemes and which therefore makes biometric authentication schemes more complicated.

6.4 No Exact Data Match

It must be observed that even the extracted biometric data are always different, even for the same user. This means that an exact match between verification data and reference data can never be demanded for a positive verification result. Due to this fact, the feature matching algorithm itself is also much more complicated than a simple comparison of PINs or passwords; under certain defined mathematical criteria, a comparison value between verification data and reference data has to be calculated, and the verification is considered successful if the comparison value lies within a specified non-zero tolerance limit.
The tolerance limit depends on the desired values for the error rates: If a high tolerance is given, less legal users will be falsely rejected by the system (i.e. a lower False Rejection Rate), but on the other hand the success probability for a defrauder, i.e. the False Acceptance Rate, will be higher. In contrast, a lower tolerance limit will lead to a higher FRR and a lower FAR.

7 SSCDs and Biometrics

7.1 Classification of Biometric Methods from the Viewpoint of a Signature Device

From the viewpoint of the signature device (e.g. a smartcard), the classification of biometric methods into static and dynamic methods is different from the classification from the user's viewpoint. The relevant classification parameter does not consist in the general possibility for the user to choose between different reference data; it depends on whether the signature device precribes the use of a certain sample by a challenge during each authentication process.

7.1.1 Static Biometric Methods

A biometric method is static from the viewpoint of the signature device if the signature device does not send a challenge to the user to prompt for a special sample of biometric data. Once the authentication process is activated by the user, one fixed sample of reference data is determined to be matched against the actually presented verification data.
This may also be the case, if the biometric method is dynamic from the user's viewpoint. If several different samples are enrolled and may be used for the authentication process, the user makes the decision which one to use.

7.1.2 Dynamic Biometric Methods

A biometric method is dynamic from the viewpoint of the signature device if the user is prompted for a certain action i.e. for presenting a certain biometric sample from the signature device during the authentication process. At the beginning, the user sends a challenge request to the signature device, and the signature device answers with a challenge.
The precondition for such a dynamic method is the presence of several enrolled samples. With the challenge, the signature device (and not the user) makes the decision which sample to use.
The use of this challenge, unforeseeable for the user, helps to prevent replay attacks; verification data captured during an authentication process (e.g. a recording of a spoken sentence for voice recognition) will be useless for a defrauder since he may be prompted for quite different data.

7.2 Smartcard Usage and Biometrics – State of the Art

For biometric applications, smartcards are currently used to store the biometric reference data only. For the verification process taking place in the service system, the data (usually encrypted) have to be read out again. This way is acceptable, if the service to be protected is provided by the service system (e.g. a cash dispenser has to verify that the legitimate user requires the money).
In the case of the creation of an electronic signature the situation is different: As already pointed out in clause 4.3, the SSCD has to provide the secured service, i.e. the signature computation. Therefore, the SSCD has to know, that the person requesting the signature creation is the legitimate SSCD holder.
Currently, the industry as well as research institutes try to implement on-card matching algorithms. Veridicom succeeded in providing an on-card matching algorithm for fingerprint veri-

fication, which has been implemented by Veridicom, Giesecke&Devrient and Gemplus. Also GMD has developed an on-card matching algorithm for fingerprint, named FipSec. The implementations show that the integration of such algorithms is possible, but performance needs to be improved. In addition, there are open problems with respect to securing the verification data (see clause 8).
Besides of the fingerprint algorithm, other methods have been already implemented (e.g. voice recognition).

7.3 Specification of Processes in Connection with SmartCards

7.3.1 Enrollment

During the enrollment phase, the biometric data template must be put into the SSCD. If a smartcard is the verifying entity, i.e. the verification is performed in the card, these data are put into a key file (similar to files already used for storing PINs or cryptographic keys).
The main part of this template is the data object Bio Data which contains the biometric reference data. Beside the Bio Data object, the key file will also contain the following data objects (see Fig. 18):

- Retry Counter for the Bio Data with actual value, initial value and additional security attributes
- Tolerance Limits for successful verification
- Key Reference to address the key file.

The additional security attributes stored with the retry counter will decide

- if the reference data can be changed after initialisation
- if the verification method can be disabled (such that access to the security application is possible without authentication)

As an optional addition, there may be a resetting code to set the retry counter for the Bio Data back to the initial value if the biometric verification method is blocked. In the same way as to the Bio Data, there also belongs a retry counter with initial value to the resetting code.
In general, the retry counters and initial values will consist of 1 byte each; the additional security parameters will be coded together in one byte. The resetting code will have the length of a usual PIN, e.g. 8 byte.

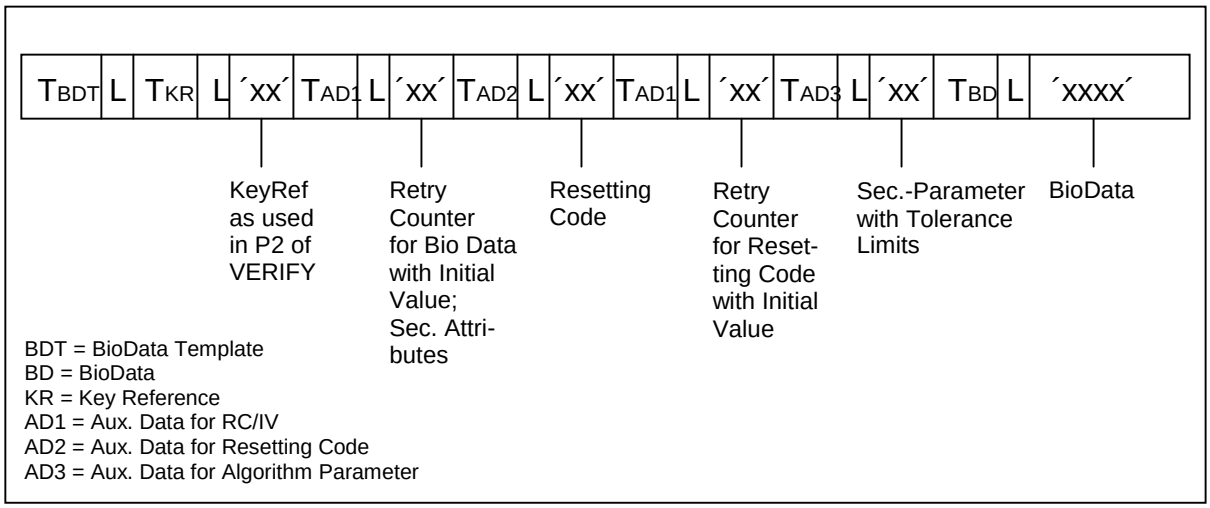

Fig. 18: Contents of a key file for biometric data (example)

The tolerance limits and the initial values for the retry counters are key attributes and must be determined by the security policy of the application to be protected (i.e. the signature application). The key file must be created during the phase of personalising the smartcard.
Once created, this key file will not allow any external read or write access. All the data contained in the key file can only be used or modified by the commands for verification, changement of reference data or resetting the retry counter.
The biometric data can be stored in the key file either during personalisation, if the enrollment has already taken place, or later, when the smartcard is delivered to the user, e.g. at a bank counter. In the following, an example is outlined, where the enrollment is made when delivering the smartcard to the user.

For this example, it is assumed, that the card

- is totally personalised except the storing of the biometric reference data and the related biometric info template (this includes also the presence of a biometric record in the key file with the related attributes for the biometric reference data, i.e. retry counter with initial value, resetting code with retry counter and initial value, flags for enabling/disabling verification requirement and changeability, ...)
- supports knowledge-based authentication besides biometric authentication.

Before the reference data can be delivered to the card, the security status for this operation has to be set. In this example, the user types in his password. With the CHANGE REFERENCE DATA command, the empty reference data are replaced by the user´s reference data computed in the enrollment process.

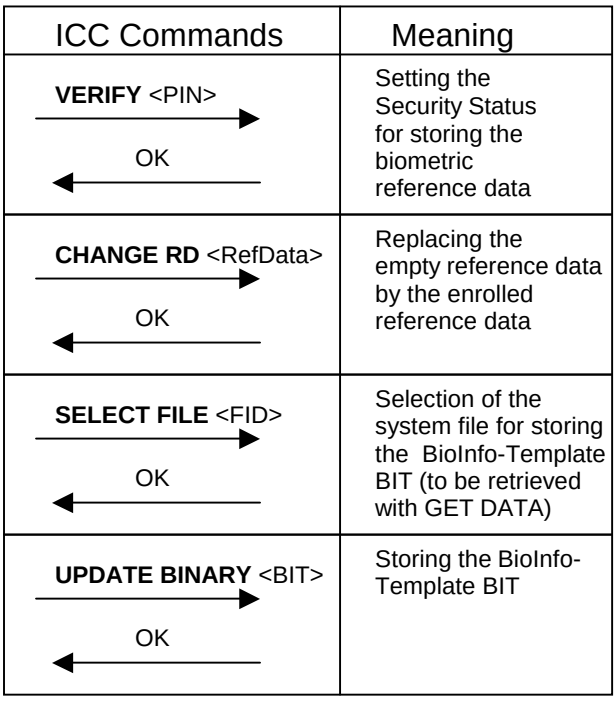

Fig. 19: Commands for enrollment (example)

After the biometric reference data have been stored (the process may be repeated, if reference data of a second biometric instance, e.g. a second finger, shall be stored), the biometric info template BIT has to be stored, which is needed by the IFD in a verification process.

The biometric info template BIT provides in the given example the following information:

- the OID of the biometric algorithm present in the card
- algorithm parameter relevant for the IFD (e.g. resolution of the reference data, which are also valid for the verification data)
- the biometric instance enrolled (e.g. right thumb)
- the key reference for addressing the biometric reference data
- discretionary data, if any
- repetition of the last 3 items, if a second biometric instance is enrolled

Fig. 20 shows the BIT and its DOs.

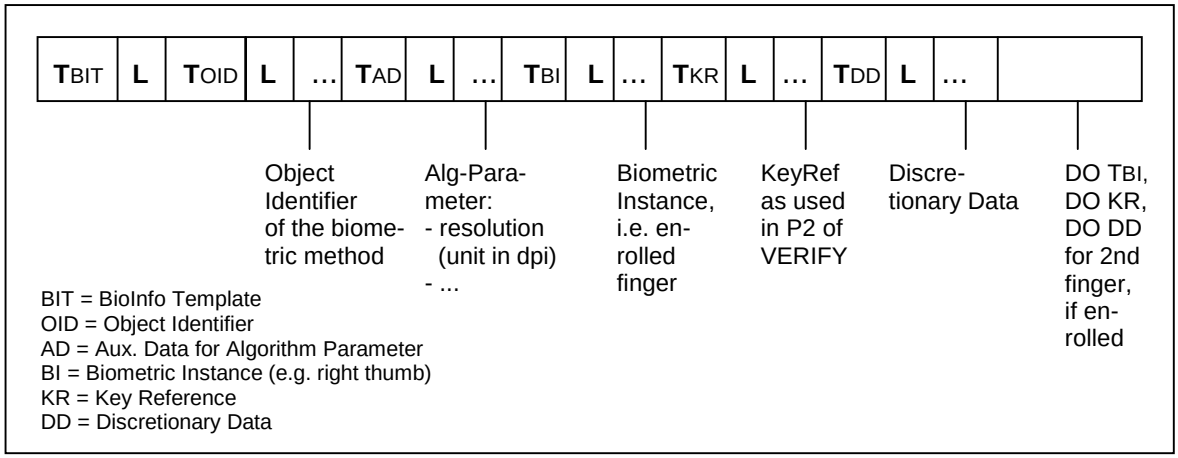

Fig. 20: BioInfo Template (example)

7.3.2 Verification

The signer authentication has to be performed before the signature creation can be invoked. In the following example it is assumed, that the smartcard is inserted e.g. in a public customer service terminal (e.g. internet terminal, bank automat). This service system does not know, whether the smartcard presented

- belongs to a user which applies biometrics
- has a biometric algorithm supported by the service system
- which biometric instance is enrolled for which it should prompt
- which value the related key reference has
- which resolution the sensor of the enrollment system has had for the computation of the verification data

Therefore, after the card application has been selected, the verification process is initiated with GET DATA to retrieve the BioInfo Template BIT. If the service system and the presented card fits together and the user has presented the related biometric feature, the verification data have to be computed and delivered to the card by using the VERIFY command (see Fig. 21).

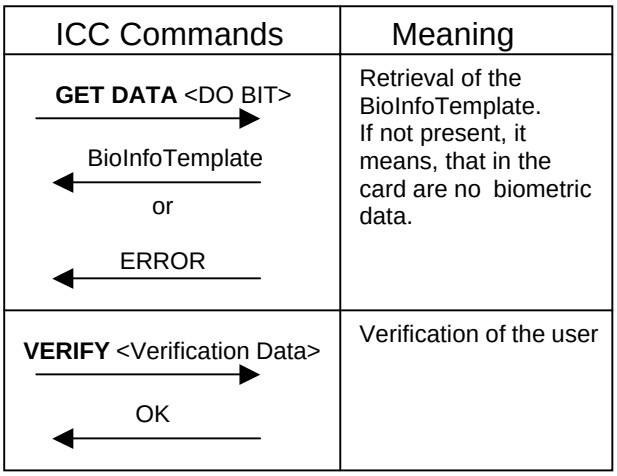

Fig. 21: Commands for verification with a static biometric method (example)

In the case that a dynamic biometric method is used, then instead of the VERIFY command

- a GET CHALLENGE command is sent to retrieve the challenge to which the user has to react, followed by
- an EXTERNAL AUTHENTICATE command for delivering the verification data.

Verification data considered as "public" (e.g. fingerprints, face, ear shape) need cryptographic protection, when sent to the smartcard, or in general, to the SSCD. Attacks and countermeasures are outlined in the subsequent clause.

8 Protection of Transmitted Biometric Data

Independent of the location where the electronic signature operation is performed (locally in the smartcard or in a remote environment), any secure biometric recognition system must be able to withstand the following attacks:

- Spying out biometric data (e.g. fingerprint from glass or facial image from camera), digitising it (to the same format as from the biometric sensor) and inserting it into the biometric authentication system
- Capturing the electronic verification data from a verification process and inserting it into the system again (replay attack)

In a security environment with a signature device verifying the biometric data, these attacks can be used to present verification data to the signature device pretending to be live captured by the sensor from the legal owner of the signature key. As already mentioned in clause 6.2, biometric verification or reference data cannot be generally considered as secret data, i.e. the security of the biometric system cannot depend on the protection of the reference data against being read out.
Therefore, the biometric verification data must be transported from the biometric sensor to the signature device (i.e. the verifying entity) authentically, such that the signature device can verify that the data were really live captured by the biometric sensor. This condition must be satisfied if the use of biometrics for digital signatures shall provide real security and not only convenience in connection with PIN authentication.

8.1 Data Transmission Modes

In general, there are the following modes of transmitting biometric data from the biometric sensor to the receiving entity (for data preprocessing or verification identification resp.) which provide different levels of security.
If the signature takes place in a remote environment and the smartcard is used as a device to store the reference data, the same considerations as those for the transfer of the verification data will also be necessary for the transfer of the reference data from the smartcard to the signature device.

8.1.1 Transmitting Plain Text Data

For most of the biometric systems currently available, the biometric data are sent in plain text without any additives. This is the lowest level of security. The receiving entity is unable to distinguish data live captured by the sensor from data inserted into the system by a defrauder (see Fig. 22).

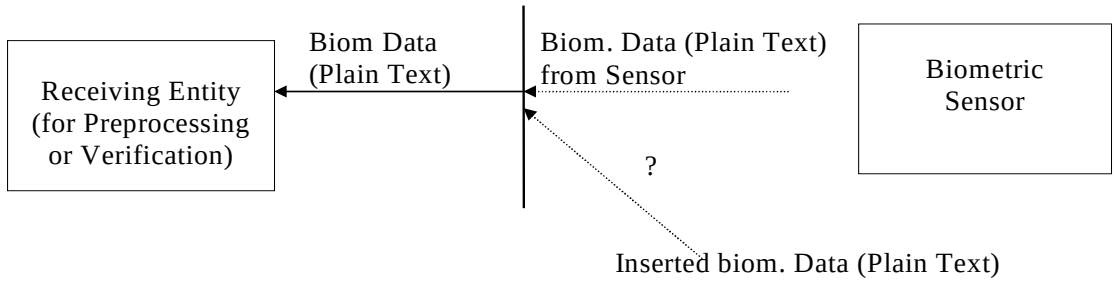

Fig. 22: Transmission of biometric data without any protection

The security of the biometric verification is then based on the assumption that an attacker is neither able to directly forge the biometric sensor nor to insert any data into the system in any other way. This transmission mode guarantees the integrity of the biometric verification data only if biometric sensor and receiving entity are integrated into one unit such that it is physically impossible to access the data transmission line from outside.

8.1.2 Protecting Data with a Scramble Function

A first enhancement of security against the simple plain text transmission can be reached with the aid of scrambling technique if the use of cryptographic functions (with possibly time consuming calculations and complicated key management) is not desired.
The measured biometric data MD or their hash value H will be mixed ("scrambled") by a scramble function in such a way that they are useless for an outsider. This scrambled data (SD) are transmitted from the biometric sensor to the receiving entity where the original data MD are restored.
To really avoid replay attacks, one string SD may be valid only one time even if the same data MD are used again. For this purpose, the receiving entity will first send a random number RND which is also used for the scrambling function (see Fig. 23).

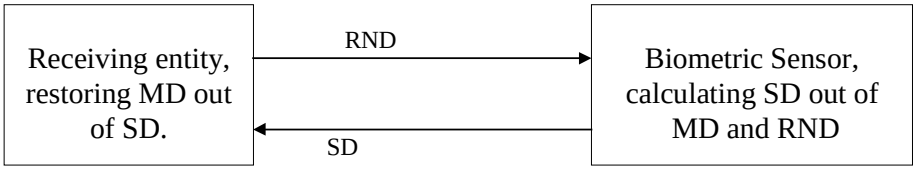

Fig. 23: Calculation and transmission of scrambled data

8.1.3 Authentic Data Transmission with Cryptographic Checksum

A much higher security level is provided if the biometric data are transmitted in plaintext but with an attached cryptographic checksum. For this purpose, the biometric sensor and the receiving entity both have to be equipped with a cryptographic coprocessor. The sensor calculates the cryptographic checksum, and the receiving entity verifies that the checksum is valid for the transmitted data.
The calculation of the cryptographic checksum can be done either by an asymmetric (public key) method together with a cryptographic hash function (i.e. a digital signature) or by a symmetric method (i.e. a MAC function).
For avoiding replay attacks by using the verification data with the cryptographic checksum once more, it is important that the checksum is always different for each verification process, even with identical verification data. This can be accomplished either by using a random number as additional input for calculating the cryptographic checksum (CC, see Fig. 24) or by generating a new key for each verification process.

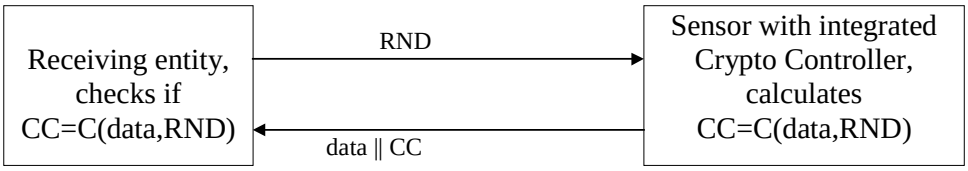

Fig. 24: Authentic data transfer with cryptographic checksum and random number

With this mode of data transfer, the receiving entity can verify the integrity of the biometric data. An attacker, having access to the data transmission line, can get the verification data in plain text, but has no chance to use them for forging the system.

8.1.4 Encrypted Data Transmission

In addition to protecting the biometric data with a cryptographic checksum, it is also possible to transmit the data in encrypted form. The sensor will calculate the cryptogram (CG) of the data and afterwards calculate a cryptographic checksum out of the cryptogram. The receiving entity will decrypt it again and verify the validity of the checksum for the cryptogram. A random number as additional input for the CC-calculation can be used in the same way as before to guarantee different checksums for identical cryptograms (see Fig. 25).
Even if a symmetric method is used where a valid cryptogram can only be calculated with the aid of the secret key owned by the sensor, the encryption cannot replace the use of a cryptographic checksum. If a block cipher method like DES is used, a cryptogram can be manipulated by cutting off blocks and is still valid afterwards; the receiving entity would not be able

to detect this manipulation. Therefore, the additional use of the cryptographic checksum as in 8.1.3 is still necessary to guarantee the integrity of the biometric data.
For performance reasons, only symmetric algorithms can be used to encrypt the biometric data (which may contain several hundred bytes or even kilo bytes). Encrypting and decrypting the biometric data with an asymmetric (public key) algorithm would lead to very high calculation times during the verification process (especially for smartcards) which are unacceptable for the user of a signature application.

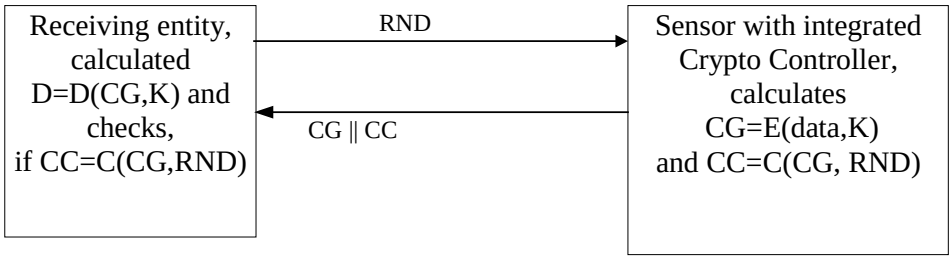

Fig. 25: Transmission of biometric data as a cryptogram with cryptographic checksum using a random number

This transmission mode of biometric data guarantees that an attacker can neither insert any biometric data into the biometric system nor get biometric data in digitised form out of the system.
The method of encrypted transfer of biometric data should be considered as an optional additive to give the user of a signature application a better feeling of safety. For sure, it can be considered as an enhancement of safety if biometric data are not directly available to an attacker in electronic form. And, in addition, there is a general high desire for protection of such personal data in electronic form even though the content may be public.
However, the encryption of biometric data should not be considered as a mandatory part of a secure biometric verification system for the following reasons:

1. As already mentioned earlier, static biometric data often have to be considered as publicly available data; the security of a biometric system cannot depend on keeping the data secret.
2. The additional need for encryption keys beside the keys needed for calculating the cryptographic checksum makes the key management much more complicated (see the following clause).

Systems should be designed to be open for the possible integration of encrypted data transfer as soon as strong cryptographic devices are available. They should then finally be offered with and without this additional feature, depending on the security policies of the application provider and the need for security in the respective environment.

8.2 Key Management

If the transfer of biometric data shall be protected cryptographically, a central problem is caused by the necessary key management. All relevant system components (biometric sensor, feature extraction unit, signature device and, if separate, reference data storing device) must perform the necessary functions like generating and exchanging the keys and storing them protected against external read or write access or other unauthorised use.

8.2.1 Key Management for Symmetric Algorithms

For symmetric algorithms, both corresponding instances use the same secret key which must be agreed in some secure way. There are two general methods for generating and exchanging the key:

- *Key Agreement:* Building a key out of part secrets on both sides without direct exchange of the key (e.g. with the aid of a Diffie-Hellman protocol, as described in Chp. 3 of [Beut95]).
- *Key Exchange:* Generating a key on one side and transferring it to the other instance in a secret way (e.g. encrypted with a public key method).

In general, the use of symmetric cryptographic algorithms means that every pair of users exchanging data (in this case the biometric sensor and the receiving entity) needs a separate secret key. This represents a problem since different sensors have to work together with different entities for preprocessing or verifying the biometric data, and the sensor will not be able to store a separate key for every possible receiving entity. A possible solution to this problem is the use of a master key and different individual serial numbers to calculate individual keys out of the master key. On one side, the master key (MK) is stored; on the other side, the individual key (IK) together with the individual serial number (ISN) is stored.
For each authentication process, the entity holding the MK receives an ISN from the other side to calculate the corresponding IK. This is no problem, since the ISN for its own is no secret.
The decision whether to equip the biometric sensor with a master key or an individual key will depend on the location where the biometric data shall be processed. In case of a central verifying entity (i.e. a remote signature device), this verifying entity will get a master key, and each individual sensor will be assigned an individual key (see Fig. 26).

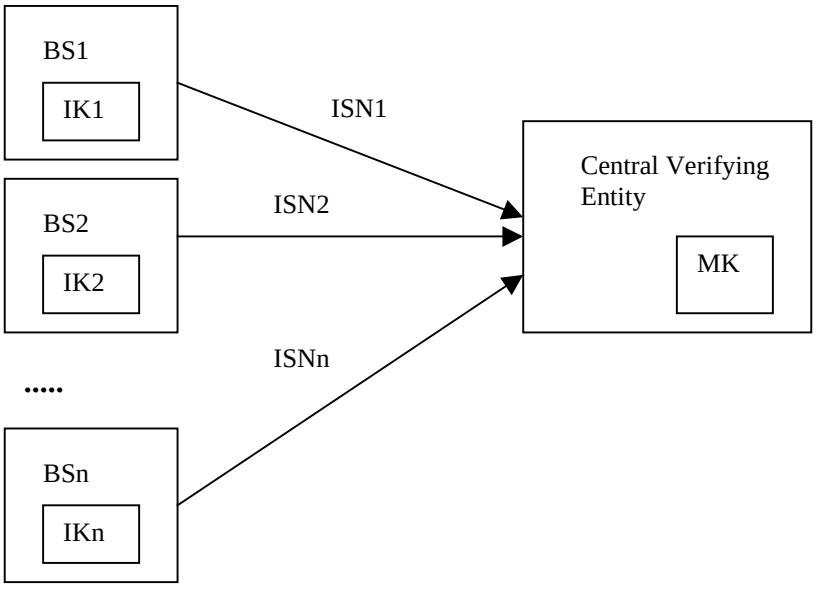

Fig. 26: Central Verifying Entity with master key (MK) and several biometric sensors (BS) with individual keys

If, in contrast, the signature (i.e. the verification of the biometric data) is performed locally on an SSCD, this SSCD will not be assigned a master key. In this case, the master key will be assigned to the sensor, and each SSCD will get an individual key (see Fig. 27).

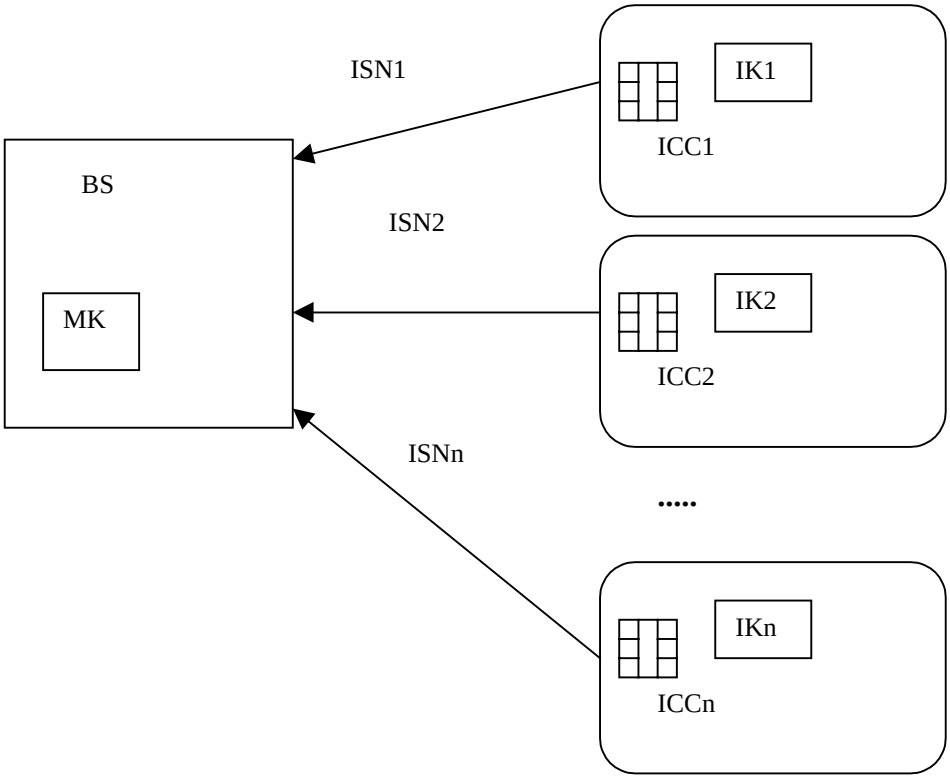

Fig. 27: Biometric Sensor with Master Key and different smartcards with individual keys

8.2.2 Key Management for Public Key Methods

For asymmetric algorithms, there is not the problem of securely exchanging secret keys. A pair of a private key (PrK) and a public key (PuK) is generated, and the public key can be delivered to anyone willing to use it. Instead, there is the problem that a public key must be certified; the certificate must ensure that the public key belongs to a certain user, in this case the biometric sensor.
Even though for symmetric algorithms there exists the solution with the use of master keys, it is strongly recommended to use an asymmetric method for calculating cryptographic checksums of biometric data. This makes it possible to uniquely assign a certified key to each biometric sensor.
This concept represents a further application of biometrics in connection with electronic signatures: Since biometric data may be public and could origin from any unknown source, the advanced electronic signature of the biometric sensor proves the origin and integrity of the data. The certified signature key is bound to the biometric sensor in the same way as otherwise to a natural person.

8.2.3 Separate Protection of Raw Data and Extracted Data

It must be observed that there are two different data streams on the way from the biometric sensor to the verifying entity that have to be protected separately: The transmission of the biometric raw data from the sensor to the feature extraction (preprocessing) unit and the

transmission of the extracted data from the feature extraction unit (FEU) to the verifying entity.
A secure cryptographic algorithm has the general property to invert each second output bit (statistically) if one input bit is inverted. This means that there is no mathematical relation between checksum (cryptogram resp.) of raw data and extracted data . The feature extraction unit needs all the cryptographic functions (generating and storing keys, calculating checksums, delivering and verifying random numbers), too.
There are two different possibilities:
Two separate keys can be agreed, one between sensor and FEU, and another one between FEU and verifying entity. For symmetric algorithms, this is the only way to avoid the exchange of any secret keys. When using symmetric algorithms, two different keys SK1 and SK2 could be generated by key agreement (see Fig. 28). For public key methods, the biometric sensor would generate a key pair and deliver the public key PuK1 to the FEU, and the FEU would generate a second key pair and deliver the public key PuK2 to the verifying entity as indicated in Fig. 29.

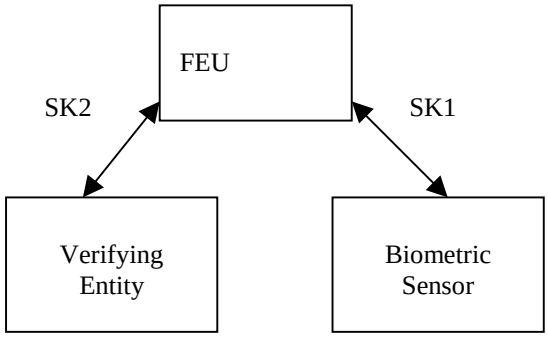

Fig. 28: Generating two different secret keys for a symmetric algorithm by key agreement

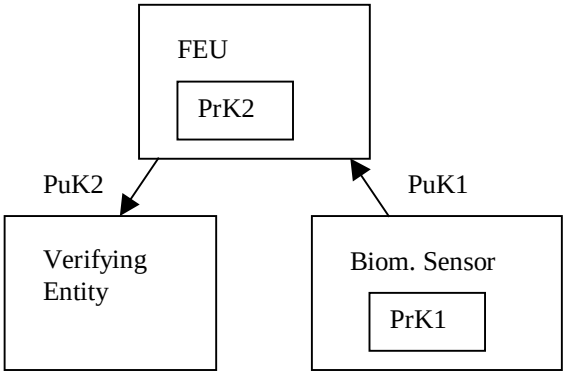

Fig. 29: Use of two different public keys for biometric sensor and FEU

The other possibility is to generate only one key that is used by the biometric sensor and the FEU to authenticate or encrypt the biometric data. In this case, the transmission of at least one secret key cannot be avoided when symmetric algorithms are used: The secret key SK has to be agreed e.g. between sensor and verifying entity and must then be securely transmitted (e.g. encrypted with a public key) to the FEU (see Fig. 30).
For asymmetric algorithms, the private key can be agreed between biometric sensor and FEU, and the corresponding public key can then be sent to the verifying entity as indicated in Fig. 31. If the mathematical design of the public key algorithms allows the construction of a usable

private key by an appropriate key agreement method like the Diffie-Hellman Protocol, biometric sensor and FEU can use the same private key without the need of exchanging it.

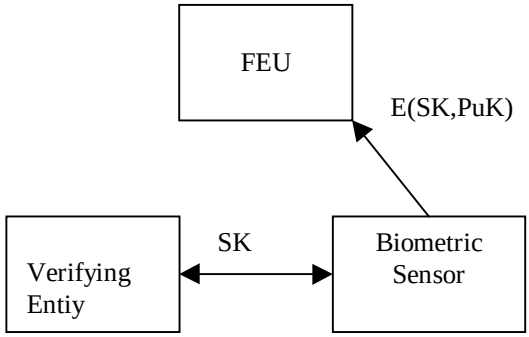

Fig. 30: Agreement of a common secret key for a symmetric algorithm with encrypted transfer to the FEU

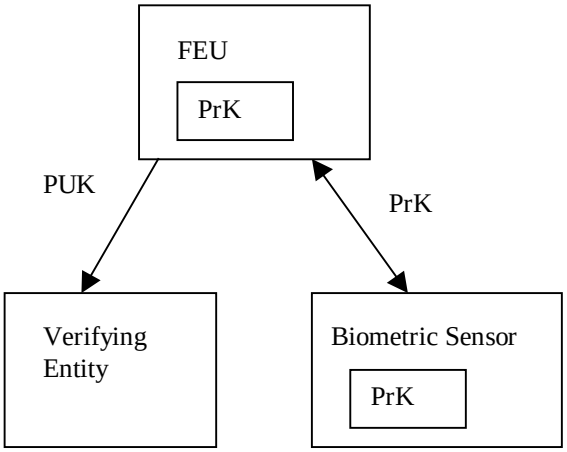

Fig. 31: Agreement of a common private key for an asymmetric algorithm with transfer of the public key to the verifying entity

8.2.4 Crypto Sensors

The need for applying cryptography to the biometric data two times is a very bad property of a signature system to be protected with biometric authentication. For this reason, it is very desirable to think about biometric systems where the sensor and the FEU are integrated into one device, such that no special protection of the raw data is required. Due to security risks and problems with the key management if symmetric algorithms are applied, the use of public key algorithm for securing the data is recommended.

8.3 Distribution of Biometric Functions among System Components

From the viewpoint of the software, a biometric recognition system has three major components: Data Capturing (from the sensor), Feature Extraction (Preprocessing) and Feature Matching. A biometric system with several peripheral devices (like smartcards, USB tokens or smartcard readers) can have many different configurations under the aspect where these different functions are realised. In general, the biometric sensor is directly handled by

the data capturing function, i.e. the result of this function consists of the biometric raw data delivered by the sensor.
Now, the security of the biometric system also strongly depends on its configuration, i.e. where the feature extraction and the feature matching takes place.
From these three functions, the feature extraction is the most time and computing power consuming. It may be easy to integrate a biometric sensor into some sorts of SSCDs which are also able to perform the feature matching; but these devices may not be able to perform the complicated steps necessary for calculating the characteristic biometric features out of the biometric raw data.
On the other hand, it makes no sense to implement a biometric sensor into an SSCD, even if it also contains the unit for feature matching, as long as the biometric raw data have to be read out again and be transported to an external FEU. This gives no chance to realise the concept of the crypto sensor where no special authentication of the biometric raw data is required.
In this point, the actual development state of many existing products (like the Cherry keyboard with integrated fingerprint sensor delivering the grey scale image to the PC over the parallel port) is very unsatisfactory.
For this reason, the guideline of distributing the biometric functions is to always implement the biometric sensor into an environment which allows the implementation of the feature extraction algorithm, too. The system configuration must always allow to realise the concept of the crypto sensor as soon as such devices are available.
For this reason, there are only two reasonable system configurations for an SSCD protected by biometric authentication: Either an SSCD with integrated feature matching and an external crypto sensor containing the FEU or the complete realisation of the biometric process (data capturing, feature extraction and feature matching) inside the SSCD.

8.3.1 Crypto Sensor in Data Terminal, Matching in SSCD

If the SSCD is unable to perform the feature extraction, it is desirable to perform the feature matching in the SSCD, but to implement the complete crypto sensor into the data terminal.
The SSCD will send a random number RND to the crypto sensor in the data terminal, and the crypto sensor will compute the digital signature DS out of the biometric template (the reference data) and the random number. The SSCD must verify the certificate of the crypto sensor (see Fig. 32). In order to enable the use of smartcards, the certificate must be a CV- (card verifiable) certificate.

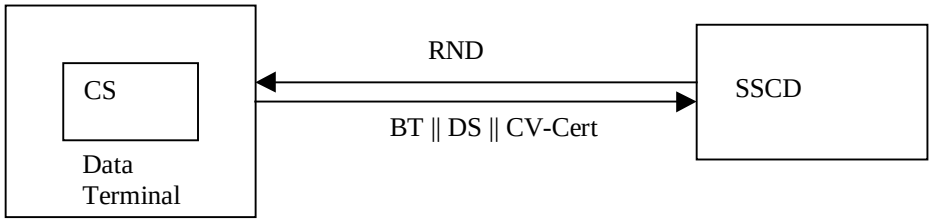

Fig. 32: Crypto sensor in data terminal, signature application with feature matching in SSCD

As long as the process of feature extraction cannot be implemented into an SSCD, this configuration provides the highest possible security. It is applicable to all sorts of SSCDs decribed in clause 4.1.

8.3.2 SSCD with Biometric Sensor, Feature Extraction and Feature Matching

The highest level of security for signature applications in local devices can be reached if the complete biometric process (data capturing, feature extraction and feature matching) can be realised inside the SSCD.
For this configuration, distinctions must be made depending on the sort of SSCD. For smartcards, it is still necessary to use a crypto sensor in order to guarantee the integrity of the biometric data since the transmission line from the biometric sensor, the FEU resp. is vulnerable to a replay attack.However, no verification of the sensor certificate is required for each authentication process since always the same crypto sensor and the same SSCD is used; instead, the public key of the crypto sensor will be stored ont the card. Fig. 33 shows the system configuration with a smartcard.

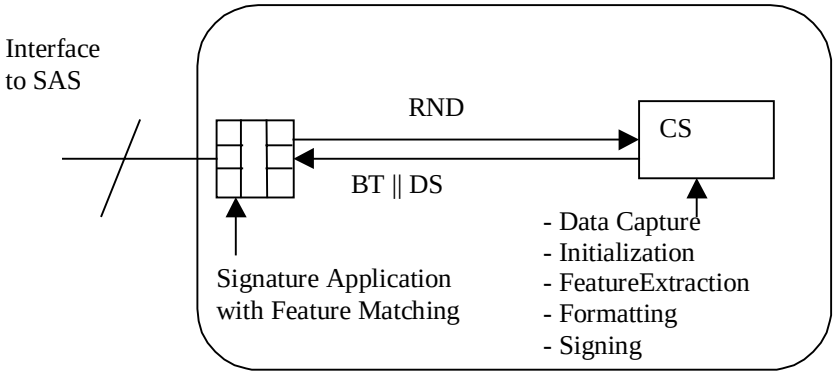

Fig. 33: Signature smartcard with integrated crypto sensor and feature matching

No crypto sensor is necessary if a tamper proof SSCD like a crypto box or a PCMCIA card is used; such security devices allow no physical access to internal data transmission lines without making the whole device unusable. In this case, a simple biometric sensor is enough (see Fig. 34). Inside a tamper proof SSCD, it is irrelevant whether the FEU is realised as a separate unit or integrated into the sensor.

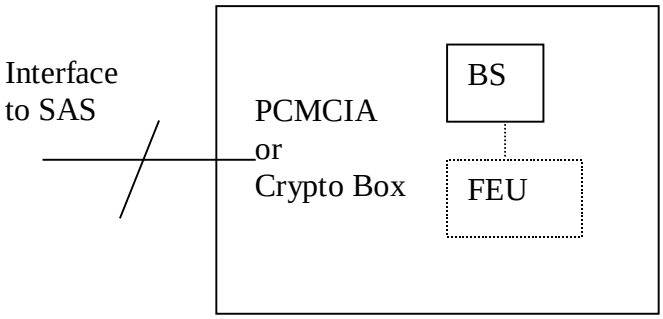

Fig. 34: Biometric Sensor, Feature Extraction and Feature Matching in Tamper Proof SSCD

The problem of realising this configuration is the high computing power needed for the process of feature extraction. The actual development state of SSCDs does not allow an implementation of the feature extraction.

9 Biometric Products and Components

9.1 Fingerprint Sensors

Fingerprint is the most popular biometric technology, and fingerprint biometric systems dominate the market for biometric identification and verification. The following clauses describe the three types of fingerprint sensors, namely optical, ultrasound and chip-based. After a short summary we will review some standard off-the-shelf fingerprint sensors integrated into a PC or mobile environment.

9.1.1 Optical Fingerprint Sensors

Systems of this kind represent the oldest and most mature category. One or more fingers are placed against a platen (usually made of glass, often with a soft coating) and an image is taken using an optical device [IBG]. Fingerprint sensors are all essentially the same size and will eventually be the same price. The only differentiators are image area, resolution, and accompanying software. The sensors that handle dry finger problems use a silicone coating that tends to wear quickly. These sensors will not get much smaller in the future due to the required optical path length or induced optical distortion from wide angle lenses .

Products: There are numerous manufacturers of optical fingerprint systems, including

- American Biometric Company [http://www.abio.com]
- Biometric Access Corp. (BAC) [http://www.biometricaccess.com]
- CrossMatch Technologies [http://www.crossmatch.net]
- Digital Persona [http://www.digitalpersona.com]
- Identicator [http://www.identicator.com]
- Identix [http://www.identix.com]
- Kinetic Sciences [http://www.kinetic.ba.ca]
- Mitsubishi [http://www.mitsubishi.com]
- Mytec [http://www.mytec.com]
- Polaroid [http://www.polaroid.com]
- SAC Technologies [http://www.sacman.com]
- SAF-LINK [http://www.saflink.com]
- SecuGen [http://www.secugen.com]
- Sony [http://www.sony.com]

Fig. 35 shows a typical stand-alone optical sensor.

Fig. 35: Example of optical sensor [Fingerprint Identification Unit FIU-001/500 by Sony]

9.1.2 Ultrasound Fingerprint Sensors

Instead of light, this type of sensor uses ultrasound for capturing fingerprint images. The main advantage of this technology is that it is unaffected by the dirt, grease, moisture, etc., typically found on fingers in real world unattended applications. Hence, the systems achieve a superior image quality in comparison to optical scanners leading to reduced error rates FAR and FRR. However, operating temperatures are 10° to 32°C which limits its use to indoor applications.

Products, for example:

- UltraScan [http://www.ultra-scan.com] is the only vendor of ultrasonic fingerprint systems, offering a range of products for one-finger, two-finger and high resolution scanning.

9.1.3 Chip-Based Fingerprint Sensors

The following clauses describe technologies regarding chip-based fingerprint sensors.

9.1.3.1 Capacitive Sensor Chips

Capacitive or silicon fingerprint sensors represent the largest fraction of chip-based fingerprint sensors. When a finger contacts the sensor surface, the capacitance at each pixel in an approximately 300x300 array (depending on the manufacturer) is measured. Differences in the capacitance values across the array correspond to the ridges, valleys, and pores that characterise a unique fingerprint. The image of the fingerprint is then transformed into a digital signal and passed to the recognition algorithms.

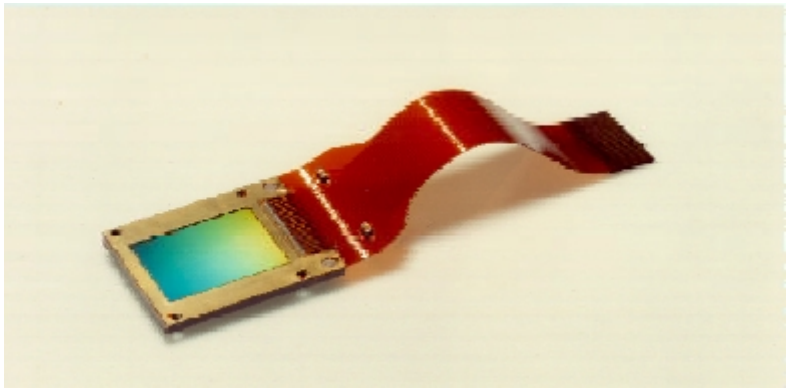

Fig. 36: Example of capacitive sensor [FingerTIP™ by Infineon]

Products, for example:

- Infineon [http://www.infineon.com], formerly Siemens Semiconductors: FingerTIP™ with a resolution of 513 dpi and 224x288 pixels (see Fig. 36).
- Sony [http://www.sony.com]: Puppy FIU-700 with a resolution of 317 dpi and 128x192 pixels
- STMicroelectronics [http://www.st.com]: TouchChip™ with a resolution of 500 dpi and 384x256 pixels
- Veridicom [http://www.veridicom.com]: FPS110 with a resolution of 500 dpi and 300x300 pixels

9.1.3.2 E-Field Technology

This new technology by AuthenTec claims to provide the ability to acquire fingerprints previously unreadable by other sensors. It reads the sub-surface of the skin, not being affected by skin surface issues such as dry, worn, or dirty skin.

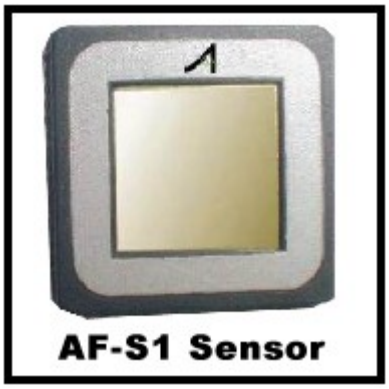

Fig. 37: E-Field Sensor AF-S1 by Authentec

Products, for example:

- AuthenTec [http://www.authentec.com]: the sensor AF-S1 (and the complete system FingerLoc™) with a resolution of 250 pixels per inch (Fig. 37).

9.1.3.3 Electro-Optical Sensor Chips

Who?Vision developed this technology which enables the TactileSense™ polymer to generate an image of the fingerprint patterns, without the need for a light source. Tactile-Sense™ transforms the ridges, loops and whorls of a fingerprint into an optical image pattern. This pattern is captured as an image by a custom designed sensor, then transformed from an optical image into digital code. The TactileSense™ polymer consists of several layers. First, an insulating layer protects the inner layers of the sensor from contaminates. The inner layers are comprised of a black-coat layer, a transparent conductive layer that supplies current, a light-emitting layer that acts as the illuminator and a base layer that allows TactileSense™ to adhere to another surface device. The sensor will be manufactured by Philips in a process that brings TactileSense™ together with flat panel display technology. This results in a slim profile (less than 1/8" thick), low-cost fingerprint sensor that can be integrated into displays on notebook computers, cell phones, handheld systems and other devices. The general architecture of the sensor is shown in Fig. 38, the sensor components in Fig. 39.
Another electro-optical sensor (with a CCD chip) is produced by the German company DELSY (previously P&P Security Systems). According to DELSY, the sensor is very robust due to a complete fibreglass wrapping.

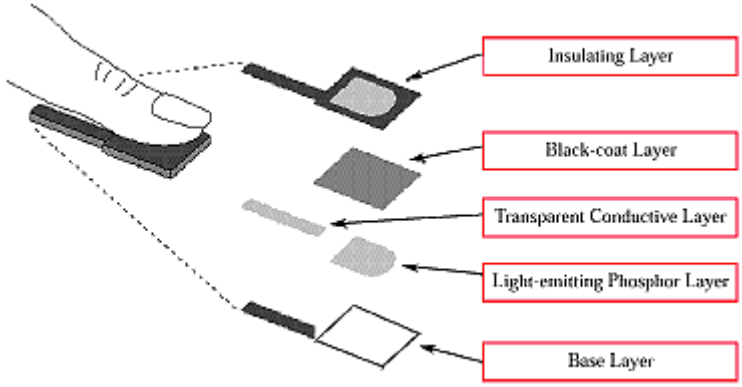

Fig. 38: Architecture of electro-optical sensor chip [TactileSense™ by Who?Vision]

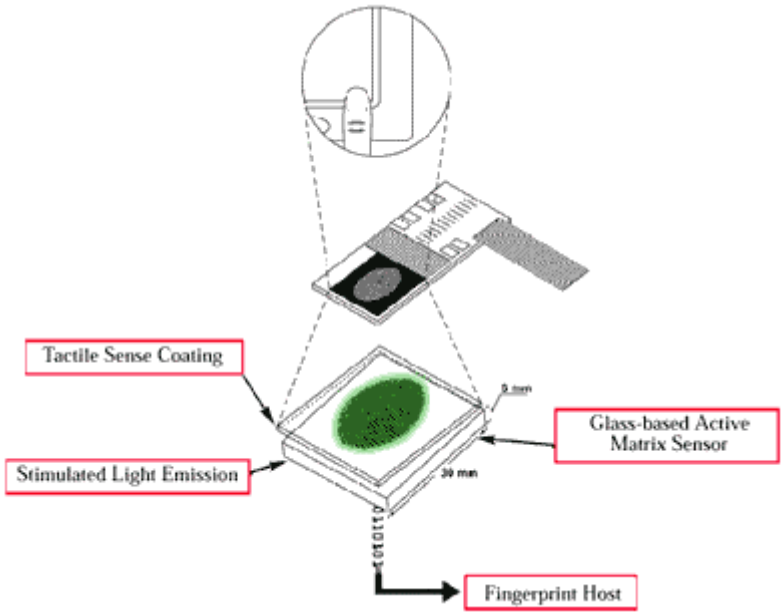

Fig. 39: Components of electro-optical sensor chip [TactileSense™ by Who?Vision]

Products, for example:

- DELSY [http://www.delsy.de]: CCD chip.

- Who?Vision [http://www.whovision.com]: US company producing TactileSense™ polymer

9.1.3.4 Thermal Sensor Chips

TCS Thomson (a subsidiary of Thomson-CSF') has developed this technology which images a user's finger in real-time through direct contact with the silicon sensor. No optics or light source are required as the finger's own heat produces all that is necessary to capture an image. A new method for imaging the entire finger is applied by 'sweeping' it across the silicon sensor. The FingerChip™ captures several images, and proprietary software then reconstructs those images into a full fingerprint. With this scanning technique, the FingerChip™ actually images fingerprints 10-20 times larger than its surface.

Products, for example:

- TCS Thomson [http://www.tcs.thomson-csf.com]: FingerChip™

The German company BERGDATA [http://www.bergdata.com] has developed software for the FingerChip™ sensor (which can be used for other sensor chips, too) and distributes a complete system with software and security applications.
In spring 2000, TCS Thomson has been taken over by the American Company ATMEL for 60% (with a further option to take over the last 40 %, too). TCS Thomson now appears under the name ATMEL/Grenoble [http://www.atmel-grenoble.com].

9.1.4 Summary

There are three different kinds of fingerprint sensors: optical, ultrasound, and chip-based. Choosing a specific sensor depends on the application and the environment. Optical sensors are quite durable but are affected by the dirt, grease, moisture, etc. typically found on fingers in real world unattended applications. Ultrasound fingerprint sensors tackle exactly this problem, they read the sub-surface of the skin. However, their use is restricted to indoor applications since the operating temperature ranges from 10° to 32°C. Chip-based sensors use different technologies, i.e. capacitive, e-field, electro-optical, and thermal. Usually, these sensors can all suffer from electro-static discharge (ESD) and fragility issues since the silicon is exposed directly to the user. However, for example the CCD chip of DELSY is meant to be very robust due to a complete fibreglass wrapping. Generally, due to their small size, chip-based sensors can be integrated into displays on notebook computers, mobile phones, handheld systems and other devices. Some of those devices are introduced in the next clause.

9.1.5 Integrated Sensors

9.1.5.1 Sensor in PC Environment

For a PC environment, there are many different possibilities where the biometric sensor can be placed. The simplest form (which you usually get when ordering an SDK or Evalutation Kit) is a sensor as a standalone device to be connected with the PC over serial port, parallel port or USB.

For security applications like electronic signatures, it is more convenient to integrate the sensor directly into a peripheral device like a PC mouse, a keyboard or a smart card reader. This can be accomplished easily with fingerprint sensors which is one reason why fingerprint recognition is a very important biometric recognition method in connection with electronic signatures. Numerous products with fingerprint sensors integrated into PC peripheral devices have already been developed.
Cherry developed a keyboard with an integrated fingerprint sensor and a smart card reader (see Fig. 40). The optical sensor of Identicator is used.

Fig. 40: Cherry smartcard reading keyboard with integrated fingerprint sensor serie G 81-12000

For other fingerprint sensors, there also exist solutions with an integrated smartcard reader, like BioMouse™ of American Biometric Company (see Fig. 41) or a smartcard reader with the electro-optical sensor TactileSense (see Fig. 42).

Fig. 41: BioMouse™ plus integrated fingerprint scanner and smartcard reader by American Biometric Company

Fig. 42: Standalone appliance with TactileSense™ sensor and smartcard reader

Moreover, Fig. 43 presents the VeriTouch vr-3 (U) Biometric Smartcard Terminal, incorporating Universal Serial Bus (USB) smartcard reader and Infineon Technologies' FingerTIP™ sensor.

Fig. 43: VeriTouch smartcard terminal with integrated Infineon sensor

9.1.5.2 Biometric Sensor in Mobile Equipment

For security applications like electronic signatures, there is also the need to use biometric sensors in a mobile environment, like mobile phone or laptop. Again, the most suitable kind of sensor for this application is the fingerprint sensor, and products have already been developed.
The electro-optical sensor TactileSense™ has already been integrated into a standard laptop (see Fig. 44).

Fig. 44: Standard laptop with integrated TactileSense™ sensor

Another interesting configuration is the integration of a fingerprint sensor into a PCMCIA-based PC card to be used for laptops. This has been performed by Identix (see Fig. 45) and Fujitsu (see Fig. 46).

Fig. 45: Identix BioTouch PC-card fingerprint reader

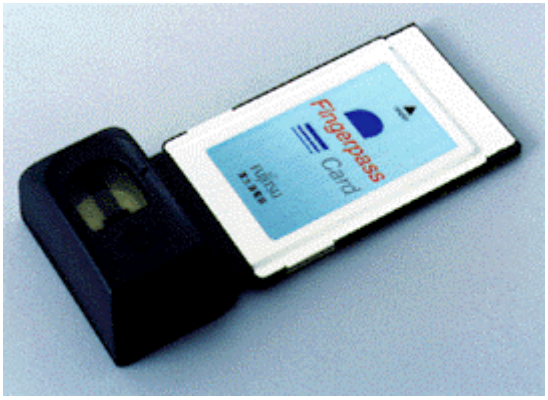

Fig. 46: Fujitsu PCMCIA PC-card based Fingerprint Recognition Device (FPI-550)

9.2 Face Recognition Systems

Common to all face recognition products is that they work with standard off-the-shelf camera equipment. This makes face recognition a cost effective solution.

Miros, now a division of eTrue.com [http://www.etrue.com] provides software solutions in face and finger recognition for physical access control, surveillance and computer access. Miros technology has evolved from eigenface to local feature analysis to neural network technology. Products include TrueFace Engine, a core software module for locating, verifying and/or identifying people's faces, TrueFace ID, a complete solution for identifying a person's face in a database of people's faces from either a surveillance video or image files, and TrueFace Network, a network software solution that allows secure logon to network servers using face and/or finger verification (see Fig. 47).

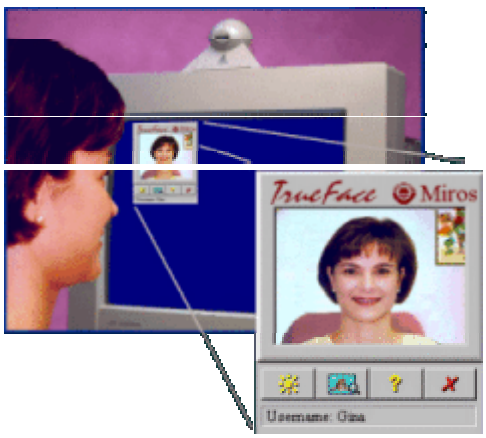

Fig. 47: Example of face recognition system with feed back over the PC monitor [Miros TrueFace Engine]

Viisage Technology [http://www.viisage.com] specialises on facial recognition, but also aims at combining facial recognition software with other biometrics such as iris, voice, signature and fingerprint technology as well as with existing identification card systems. Using a sophisticated algorithm based on Principle Component Analysis (PCA) developed at the Massachusetts Institute Technology's Media Lab, the Company's software translates the characteristics of a face into a unique set of numbers, which is referred to as the eigenface.

Viisage's products include FaceFINDER™ for identity surveillance, FacePASS™ for access control applications, FacePIN™ for point of sale applications, and FaceNET™ for electronic and mobile commerce.
Visionics [http://www.visionics.com] provides face recognition solutions based on Local Feature Analysis (LFA). Visionics' FaceIt product line offers the toolkits SDKs FaceIt® ActiveX for authentication from live video, FaceIt® DBCom for large scale database search applications, and the FaceIt® Library. Moreover, there are the applications FaceIt® DB, a stand alone search engine, FaceIt® Surveillance, an intelligent agent in CCTV control centers, and FaceIt® NT/PC for desktop logon and security.
Biometric Access Corporation [http://www.biometricaccess.com] offers BAC One-on-One Facial Recognition, including a desktop camera and corresponding software. Focussing is made easy using this system, because a person has to look into the mirror (=reflective surface of camera) only (see Fig. 48). BAC also provides a fingerprint reader (BAC SecureTouch) and corresponding software.
The German company Dermalog Identification Systems [http://www.dermalog.de] sells Face-ID.
The German security company plettac electronic security GmbH [www.plettac-electronics.de] provides facial recognition technology both toend-users and system integrators; their system FaceVACS provides feedback to the user by control signals (see Fig. 49). FaceVACS-Logon is a product that secures access to computer systems (for logon and screen-unlock) via standard webcams. An SDK using the BioAPI standard will be available by the end of 2000.

Fig. 48: Example of face recognition system with feedback over a mirror [One-on-One™ by BAC]

Fig. 49: Example of a face recognition system with control signals [FaceVACS by plettac electronics]

9.3 Hand Geometry Devices

Due to their size (22cm square by 25cm high), hand geometry scanners are not suitable for desktop or laptop applications. Instead, they are typically deployed in access control applications.

Products, for example:

- Dermalog Identification Systems [http://www.dermalog.de]: HandID
- Recognition Systems [http://www.recogsys.com]: HandPunch®, HandKey® and HandNet® (see Fig. 50).
- BioMet Partners [http://www.biomet.ch] produces two-finger recognition devices (see Fig. 51).

Fig. 50: Example of hand geometry device [Recognition Systems HandNet® access control systems]

Fig. 51: Example of two-finger geometry device [BioMet Partners FingerFoto finger geometry biometric OEM camera]

9.4 Iris Recognition Systems

Iris recognition technology involves the use of a camera to capture an image of the iris, the coloured portion of the eye. There are two types of iris recognition systems: active and passive. In the active system, the user must adjust the camera by moving forward or backward a few inches in order to bring the iris into focus. Further, the user must be within 6-12 inches of the camera. This requires substantial supervision and instruction. The passive system incorporates a set of cameras to automatically locate the user's face and eye, therefore removing the need to manually focus the camera. The latter system is much easier to use.

Products, for example:

- IrisScan [http://www.irisscan.com] sells active iris recognition systems (see Fig. 52).
- Sensar [http://www.sensar.com] (see Fig. 53) and
- LG Corporate Institute of Technology [http://www.lgcit.com] sell passive iris recognition systems.
- Dermalog Identification Systems [http://www.dermalog.de]: Iris-ID

Fig. 52: Example of active iris recognition system [Iris recognition device of IrisScan]

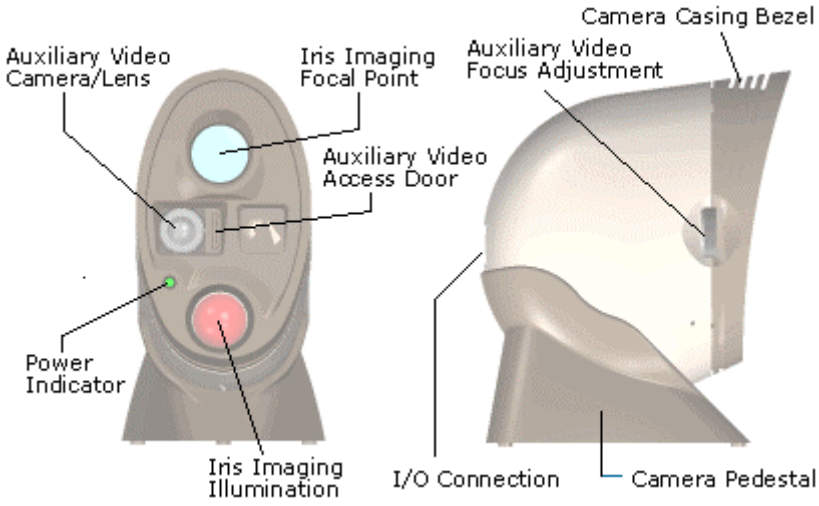

Fig. 53: Example of passive iris recognition system [Sensar...Secure®Cam model C2 camera]

9.5 Retinal Recognition Systems

Eyedentify [http://www.eyedentify.com] is the only producer of retinal recognition systems. Fig. 54 presents their latest product Icam 2001 Positive Identification System.

Fig. 54: Example of retina recogntion system [Eydentify's retinal recognition system Icam 2001]

9.6 Dynamic Signature Verification Systems

For dynamic signature verification, there is the distinction between the capturing device and the verification software. The capturing device can be either a digitising tablet or an electronic pen. Fig. 55 shows the digitising tablet of Hesy [http://www.hesy.de]. Other vendors of digitising tablets or electronic pens include Wacom [http://wacom.com], Interlink [http://www.interlinkelec.com] and Topaz [http://www.topazsystems.com].
Fig. 56 presents SMARTpen™ “BiAS” (Biometric Authentication System) by LCI Technology Group [http://www.smartpen.net] which includes sensors for measuring pressure and tilt, as well as a computer processor for managing the operation of the pen, supervising data sampling and encryption, and preparing radio transmission.

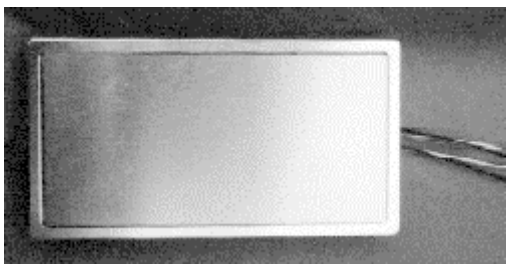

Fig. 55: Example of digitising tablet [Hesy]

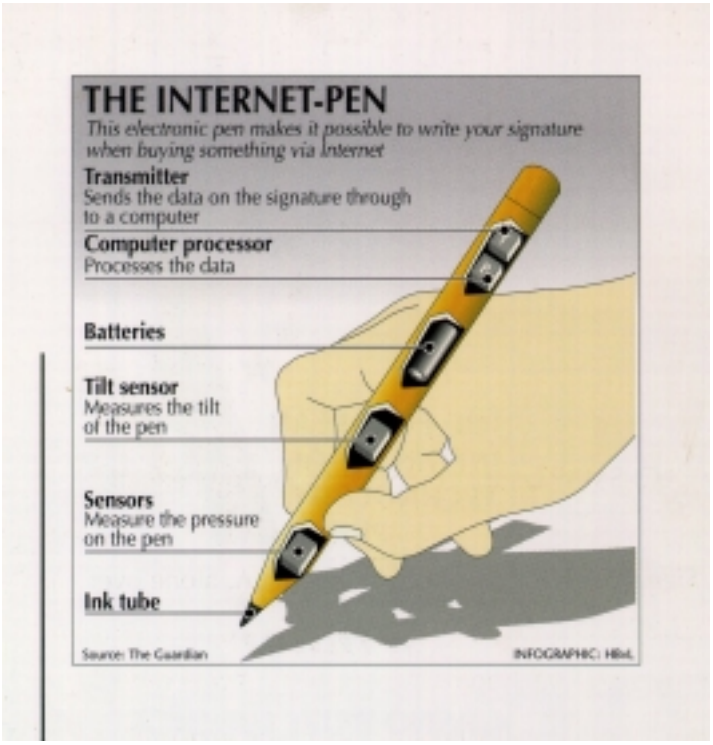

Fig. 56: Example of electronic pen [LCI-SmartPen ™]

There are several vendors of dynamic signature verification software, for example

- Communication Intelligence Corporation (CIC) [http://www.cic.com]
- Cyber-SIGN [http://www.cybersign.com]
- Dermalog Identification Systems [http://www.dermalog.de]: Sign-ID
- PenOp [http://www.penop.com]
- Quintet [http://www.quintetusa.com]
- SOFTPRO [http://www.softpro.de]: SignPlus [http://www.signplus.com] (product range also includes systems for static signature verification and electronic signature capture)

9.7 Speaker Recognition Systems

Speaker recognition systems work with microphones or with regular telephone handsets. There are a number of vendors of speaker recognition software.

Products, for example:

- Dermalog Identification Systems [http://www.dermalog.de]: Voice-ID
- ITT and Buytel™ [http://www.buytel.com]: Phonekey SM (using the telephone), WebkeySM (using the WWW) and NetkeySM (using the Internet)
- Keyware Technologies [http://www.keyware.com]: VoiceGuardian® (Microphony SDK, Telephony SDK)
- Nuance [http://www.nuance.com]: Nuance Verifier 2.0™
- OTG The Ottawa Telephony Group [http://www.otg.ca]: SecurPBX® Voice Verification
- T-NETIX [http://www.t-netix.com] : SpeakEZ Voice Print Speaker Verification
- VeriVoice [http://www.verivoice.com]: VeriVoice Security Lock

9.8 Keystroke Dynamics Systems

Keystroke dynamics utilises standard keyboards or keypads. No extra hardware is required. Since keystroke dynamics is a very new technology, there are not a lot of vendors yet. Netnanny [http://www.netnanny.com] has developed BioPassword® for NT Server Logon security, and as a SDK to allow engineers to incorporate the technology into any environment where keypads and passwords are used and laptop/desktop security, where the technology can be woven directly into the BIOS to deter machine theft and unauthorised boot-ups.

9.9 Multimodal Biometric Systems

In clause 9.2, we have already introduced two vendors of multimodal biometric systems: Miros and Viisage Technology, both producing facial recognition systems combined with fingerprint biometric systems. Viisage Technology also offers facial recognition systems combined with iris, voice, and signature technology.

Products, for example:

- Dermalog Identification Systems [http://www.dermalog.de]: the Dermalog system includes a wide range of biometric products namely, Finger-ID, Face-ID, Hand-ID, Iris-ID, Sign-ID, and Voice-ID which can be combined. Dermalog AFIS (Automatic Fingerprint Identification System) is the core product of the company.
- DCS Dialog Communication Systems [http://www.bioid.com]: BioID Technology for recognition by means of face, voice, and lip-movement while speaking. This system is a multimodal biometric security solution for small office networks, the home office, and for notebook computers.
- SAC Technologies [http://www.sacman.com]: layered biometrics systems consisting of fingerprint identification, voice verification, and facial recognition
- SAFLink Corporation [http://www.saflink.com]: SAF2000 Enterprise Network Suite Components including Finger BSP (Biometric Service Provider), Voice BSP, and Facial BSP modules
- Miros: see above
- Viisage: see above

10 Standards and Specifications

10.1 ISO/IEC 7816 and the New Work Item on Biometrics

On the ISO level (WG4 of ISO/IEC JTC1/SC17), a new standard with respect to biometrics is under development: "Personal verification through biometric methods in integrated circuit(s) cards". This standard will become either an own part of the famous ISO/IEC 7816 standards for smartcards or an amendment to "ISO/IEC 7816-4: Interindustry commands for interchange". The current Working Draft (WD) consists of 3 sections:

- the main part, in which extensions to the commands VERIFY, GET CHALLENGE and EXTERNAL AUTHENTICATE together with the biometrics related data objects BDT and BIT are specified
- annex A (informative), which provides information about biometric authentication processes and
- annex B (informative), which contains examples for enrollment and verification.

This standard is of high importance for smartcards with on-card matching and thus for smartcards with signature creation function. It is expected, that in autumn 2000 the WD will be submitted as Committee Draft for voting. The examples presented in clause 7.3.1 and 7.3.2 are in line with the ISO standard under development.

10.2 ANSI/NIST Standard for Coding Biometric Data

The American National Standards Institute Inc. (ANSI) and the National Institute for Standards and Technology (NIST) have developed standards for formats of the following biometric data:

- Facial images
- Fingerprint images (greyscale and binary, low and high resolution)
- Fingerprint minutiae.

The standard for facial images is also applicable to scar, mark or tattoo images.
The existing ANSI/NIST standard does not specify any feature matching algorithms for fingerprint or facial image recognition.
Very interesting for the closer specification of biometric authentication processes is the standard for fingerprint minutiae, the extracted features from fingerprint images. The standard contains a lot of optional information and provides much freedom for some user defined coding. The standards for fingerprints was established 1993 (see [ANSI/NIST93]), additions for facial images were made 1997 (see [ANSI/NIST97]).
For all types of biometric data mentioned above (fingerprint images, fingerprint minutiae, facial images), certain types of records are defined. As closer described in [ANIS/NIST93], each record consists of several information fields with specified field numbers which are again divided into subfields and information units.
A fingerprint minutiae record consists of the following fields where the fields 1 to 4 are all mandatory:

Field 1: Record Length (LEN)
The LEN-Field of variable length contains the total byte length of the whole minutiae record, including all information fields and delimiters.

Field 2: Image Designation Character (IDC)
The IDC-field has a length of two byte. It contains an identification number of the minutiae coded in this record. Records containing minutiae data of the same fingerprint shall be assigned the same IDC number.

Field 3: Impression Type (IMP)
The IMP field contains 1 byte with 8 possible values (binary coding from 0 to 7). It specifies the method by which the corresponding fingerprint was captured (live scanned, using a photo, rolling the finger etc.).

Field 4: Minutiae Format (FMT)
This one byte field with two possible values decides whether the further coding of the minutiae is done by the standard defined in the following fields ("S") or by a user defined coding ("U"). In case of FMT="U", the following fields (no. 5 to 12) may be not present.
If one of the following fields is called "mandatory", this is always under the assumption that FMT="S".

Field 5: Originating Fingerprint System (OFR)
This mandatory field contains closer information about the fingerprint system and the minutiae extraction method used to capture the data. A mandatory part of the OFR field contains the name of the fingerprint system and a one byte information field to which degree manual coding of the fingerprint was performed. An additional optional subfield consists of a two byte long "subsystem designator" to closer describe the system environment.

Field 6: Finger Position (FPG)

The FPG field is also mandatory and contains one byte to describe which finger from which hand was used. It has 11 possible values (binary coding from 0 to 10) where the value 0 means that the position of the finger at the hand is unknown.

Field 7: Fingerprint Pattern Classification (FPC)
The mandatory FPC field performs the classification of the fingerprint (arch, loop, whorl etc.) and contains two information units: The first information unit decides whether a prescribed standard table (value "T") or a user defined coding (value "U") is used. The second information unit contains the coding of the classification. The values of the standard table have a length of two byte.

Field 8: Core Positions (CRP)
If the fingerprint contains core points, the optional CRP field can be used to describe their locations. It contains the location coordinates x and y of the core points, each of them coded as a 4-digit decimal number in 4 bytes with values from 0 to 5000. The length unit is 0.01 mm.

Field 9: Delta Positions (DLT)
In the same way as the CRP field for the core points, the optional DLT field can be used to describe the locations of the delta points contained in the fingerprint.

Field 10: Number of Minutiae (MIN)
The mandatory MIN field contains one byte with the number of minutiae contained in the fingerprint.

Field 11: Minutiae Ridge Count Indicator (RDG)
The mandatory one byte RDG field contains the information whether the minutiae record contains ridge count information (number of ridges between two minutiae). If ridge count information is present, the value is "1", otherwise "0".

Field 12: Minutiae and Ridge Count Data (MRC)
The mandatory MRC field is the central part of the minutiae record and contains the intrinsic information about the minutiae. Each minutia is coded with one subfield, and each of these subfields contains several information units.
The following information units are mandatory:
- Specification of a minutia index number
- Location coordinates x and y (coded in the same way as for the optional fields CRP and DLT)
- Tangential angle θ of the ridge in the minutia point (coded in three byte as a 3-digit decimal number between 0 and 359, angle unit 1°)

In addition to this mandatory information, the following optional information may be present:
- Quality and reliability of the coded minutia (one or two byte): If the minutia was encoded manually, the value is "0". A value of "1" means that no reliability information is present, and the values "2" to "63" represent different levels of reliability where "2" is the highest level.
- Minutia type: "A" for ridge ending, "B" for ridge bifurcation, "C" for composed type (crossing or trifurcation) and "D" for unknown type.
- Ridge Count Information (if RDG=1): Index and ridge count distance of all minutiae to be considered for this minutia.

It is visible from many publications (e.g. [Meh93], [Rat96]) that the informations (x,y,θ) about the location and the angle of a minutia, which are mandatory for the ANSI/NIST standard, are very frequently used in some way for existing fingerprint recognition systems (see also [Scheu99]).
However, no vendor or manufacturer of a fingerprint system is currently known as using this standard. For most manufacturers, the exact coding of minutiae is handled as an intellectual property to be kept secret. On the other hand, there are no standards about image resolutions (dpi) of fingerprint sensors although the ANSI/NIST standard suggests that a resolution of 500 dpi provides enough security. This has the result that developers of fingerprint recognition software designed for a special sensor prefer to use the number of pixels as a distance measure instead of a meter-based length unit.
For storing fingerprint minutiae in smartcards or other small cryptographic tokens, this standard needs to be modified since it is highly redundant and therefore wastes a lot of

memory. All the fields and subfields are separated by delimiters each of them needing at least one byte. In addition, the content of many information fields is not really needed for the process of feature matching.
Each minutiae inside the MRC field needs at least 15 bytes, and the other information fields of the minutiae record need at least another 77 byte.

10.3 Crypto Standards PKCS#11 and PKCS#15

PKCS (Public-Key Cryptography Standard) are specifications produced by RSA Laboratories in cooperation with secure systems developers worldwide for the purpose of accelerating the deployment of public-key cryptography. There are two standards, namely PKCS#11 [PKCS#11] and PKCS#15 [PKCS#15], which are relevant for this study. Further information on PKCS can be found under [http://www.rsasecurity.com/rsalabs/pkcs].

10.3.1 PKCS#15: Cryptographic Token Information Syntax Standard

PKCS#15 specifies a file and directory format for storing security-related information on cryptographic tokens such as smartcards and other types of SSCDs. The main objectives of PKCS#15 are:

- Enable interoperability among components running on various platforms (platform neutral)
- Enable applications to take advantage of products and components from multiple manufacturers (vendor neutral)
- Enable the use of advances in technology without rewriting application-level software (application neutral)
- Maintain consistency with existing, related standards while expanding upon them only when necessary and practical.

PKCS#15 provides means to describe the existence and the use of objects, e.g. the objects in an SSCD, as shown in Fig. 57.

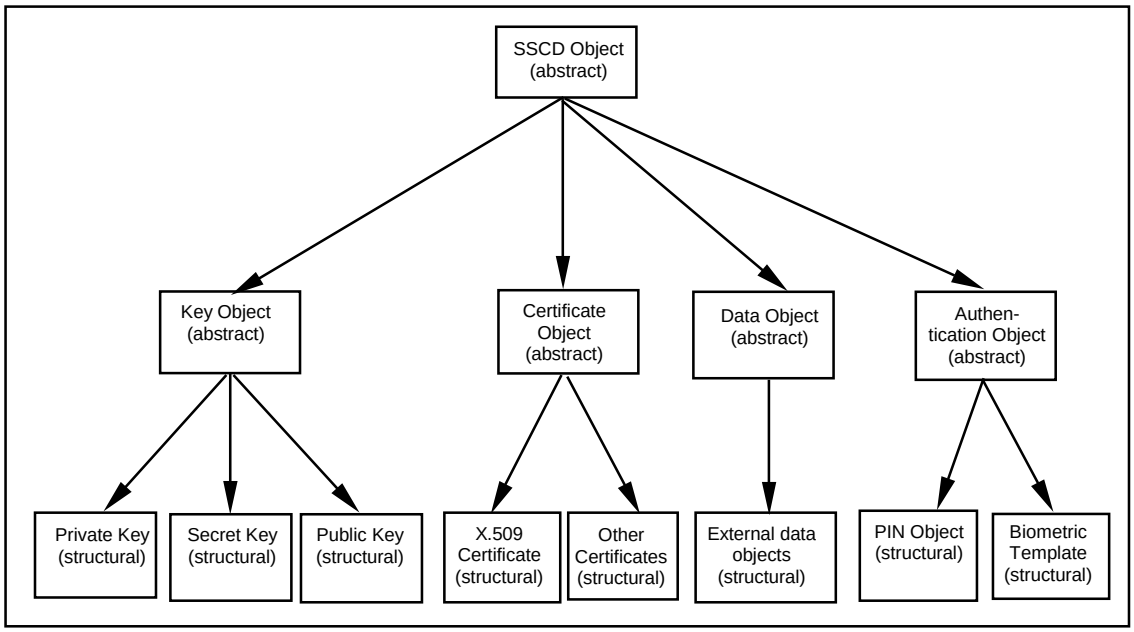

Fig. 57: PKCS#15 and SSCD objects

User authentication objects are among the objects which can be described with PKCS#15. Authentication objects are either PINs or passwords, or biometric templates.Thus, it can be expressed in the information to be retrieved by the SCS that the use of the private key for signature creation requires the successful presentation of e.g. the left or right thumb of the legitimate SSCD user.

10.3.2 PKCS#11: Cryptographic Token Interface Standard

PKCS#11 specifies an application programming interface (API), called *Cryptoki*, to devices which hold cryptographic information and perform cryptographic functions [PKCS#11]. Cryptoki was intended from the beginning to be an interface between applications and all kinds of portable cryptographic devices, such as those based on smartcards, PCMCIA cards, and smart diskettes.
The main objectives of Cryptoki are

- Technology independence
  Cryptoki abstracts the details of the devices and presents to the application a common model of the cryptographic device, called a *cryptographic token*.
- Resource sharing
  A single cryptographic device should be shared between more than one application. In addition, an application should be able to interface to more than one cryptographic device at a given time.

Cryptoki provides an interface to one or more cryptographic devices through a number of *slots*. A slot corresponds to a physical reader or other device interface and may contain a cryptographic device, called a *token*. A cryptographic device can perform some cryptographic operations, following a certain command set; these command sets are typically passed

through standard device drivers, for instance PCMCIA card services or socket devices. Cryptoki makes each cryptographic device look logically like every other device, regardless of the implementation technology. Thus, the application need not interface directly to the device drivers. The Cryptoki API consists of a number of functions, spanning slot and token management and object management, as well as cryptographic functions.

Cryptoki is likely to be implemented as a library supporting the functions in the interface, and applications will be linked to the library. The kinds of devices and capabilities supported will depend on the particular Cryptoki library.

In order to use or view the private objects of a token, a user must be authenticated to the token by a PIN or some other token-dependent method, e.g biometrics. In addition to this *standard login mechanism*, Cryptoki allows an application to specify that a private key should be protected by a *secondary authentication mechanism.* Secondary authentication is intended for the creation of electronic signatures, in order to achieve a high level of security regarding the authenticity of the signer.

Currently, PKCS#11 supports the PIN mechanism:

- The application can call the function C_InitPIN passing the PIN value as parameter for initialising the normal user's PIN. The user is authenticated by the application calling C_Login with the corresponding PIN parameter.
- Instead of passing the user's PIN as a parameter of C_InitPIN and C_Login, the application passes NULL_PTR. This means that the token has a *protected authentication path*, indicating that there is some way for the user to be authenticated to the token without having the application send a PIN through the Cryptoki library. For example, the user could enter the PIN on a PINpad on the token itself, or on the slot device.

Future versions of PKCS#11 will also support biometric authentication.

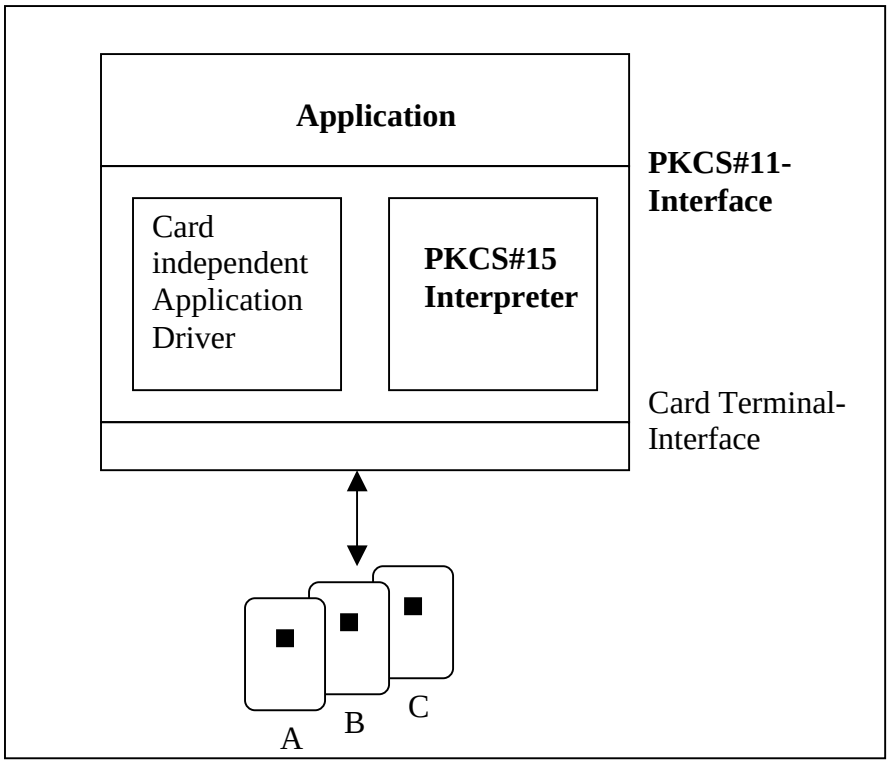

Fig. 58: Model of an application using PKCS#11 and PKCS#15 (example)

10.4 BioAPI

The BioAPI Consortium was founded in April 1998 in order to develop a widely available and widely accepted API that will serve for various biometric technologies [BioAPI]. In March 1999, the Human Authentication API (HA-API) merged their activities with the Bio-API Consortium. The following goals are defined in [BioAPI]:

Implementation of the BioAPI will enable:

- Rapid development of applications employing biometrics
- Flexible deployment of biometrics across platforms and operating systems
- Improved ability to exploit price performance advances in biometrics
- Enhanced implementation of multiple biometric alternatives (fingerprint, voice, face, iris, etc.)

The BioAPI will enable these business benefits by providing:

- Simple application interfaces
- Standard modular access to biometric functions, algorithms, and devices
- Secured and robust biometric data management and storage
- Standard methods of differentiating biometric data and device types
- Support for biometric identification in distributed computing environments

Implementation of BioAPI will provide value to:

- Industry security administrators
- System integrators and value added resellers
- Application developers
- End users of biometric technologies

The BioAPI (see Fig. 59) is intended to provide a high-level generic biometric authentication model, suited for any form of biometric technology. It covers the basic functions of Enrollment, Verification, and Identification, and includes a database interface to allow a biometric service provider (BSP) to manage the Identification population for optimum performance. It also provides primitives which allow the application to manage the capture of samples on a client, and the Enrollment, Verification, and Identification on a server. The goal is to hide the unique aspects of individual biometric technologies, and particular vendor implementations, products, and devices, while providing a high-level abstraction that can be used within a number of potential software applications. The BioAPI is designed for use by application developers and biometric technology providers.

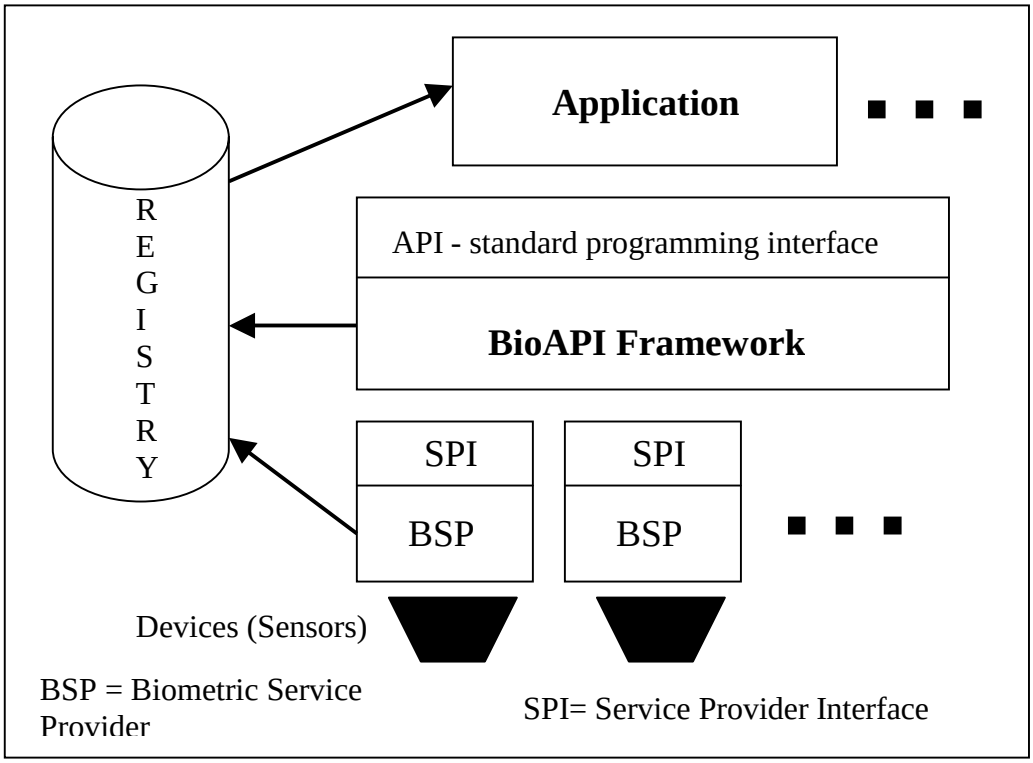

Fig. 59: BioAPI – Basic Structure

One drawback of the current version of BioAPI is that it does not define any security requirements for biometric applications and service providers. Moreover, the current BioAPI version does not consider the special scenario relevant to biometrics and on-card matching, which is relevant for SSCDs. Therfore, only parts of the BioAPI model can be applied for enrollment systems and signature application systems interacting with SSCDs.

For further information please refer to [BioAPI]; an overview is also presented in [Wi2000].

10.5 Qualified Certificate Profile

The PKIX-Working Group (Public Key Infrastructure for X.509) of IETF (Internet Engineering Task Force) is working on standards for qualified certificates for PKIX. It is proposed to use biometric data as an addition to the certificate.
The proposed certificate profile neither plans to store the complete biometric data with the certificate nor defines standards for the format of the data. Instead, the certificate shall contain

a hash value calculated out of the biometric data. In addition, a pointer shall be present to identify the source where the corresponding data can be found.
(Please note that the hash value can always be valid for one single sample only that must be stored somewhere; different samples of the same individual will always deliver slightly different binary data with completely different hash values!)
For further information on the proposed qualified certificate profile please refer to [PKIX-QC].
As already mentioned in the introduction, this concept represents a new application of biometrics in connection with electronic signatures. Biometric data is used to connect a signature certificate to its owner more closely.

10.6 Common Biometric Exchange File Format (CBEFF)

The Common Biometric Exchange File Format has been worked out by NIST/ITL and the Biometric Consortium [NIST/ITL99] (see also [Wi2000]). The specification will enable interoperability of biometric based application programs and systems from different vendors. A common biometric file format as defined in [NIST/ITL99] may consist of a header that contains information such as file length and biometric types, followed by a block of data in unspecified format that can pertain to one of any biometric template types and any other required biometric metadata. The specification intends to accomodate any biometric technology. The standard is usable also for smartcards and other kind of tokens, if the biomteric reference data have to be delivered to the service system, in which the matching is performed. The standard does not take into account the special scenario, where on-card matching is required. It is planned, to enhance the CBEFF standard in this direction.

10.7 Standardisation of Biometric Algorithms and Data Formats

As already mentioned earlier, biometric algorithms are intellectual property at the moment. Especially

- the exact kind of feature,
- the way, feature extraction is performed,
- the way of encoding the biometric templates

is kept secret. This situation originates from the fact that biometrics have been applied mainly in closed environments, so that no interoperability was required.

11 Electronic Signatures and Biometrics in Application Sections

11.1 Constraints and General Aspects

Biometric methods are not suitable or applicable to any signer in the following cases:

- rejection due to personal reasons
- cultural incompatibility (e.g. hidden face, hidden ears)
- absence of the respective biometrical feature
- insufficient characteristics of the respective biometric feature
- abnormal characteristics of the respective biometric feature.

Therefore, any signer should have a choice to decide

- whether he wants biometric authentication and
- which method he would like to apply

beside of the possibility to present a PIN (seeFig. 60).

At a public signature terminal, the knowledge based method shall always be supported in addition to one or more biometric authentication methods (multimodal signature application systems).

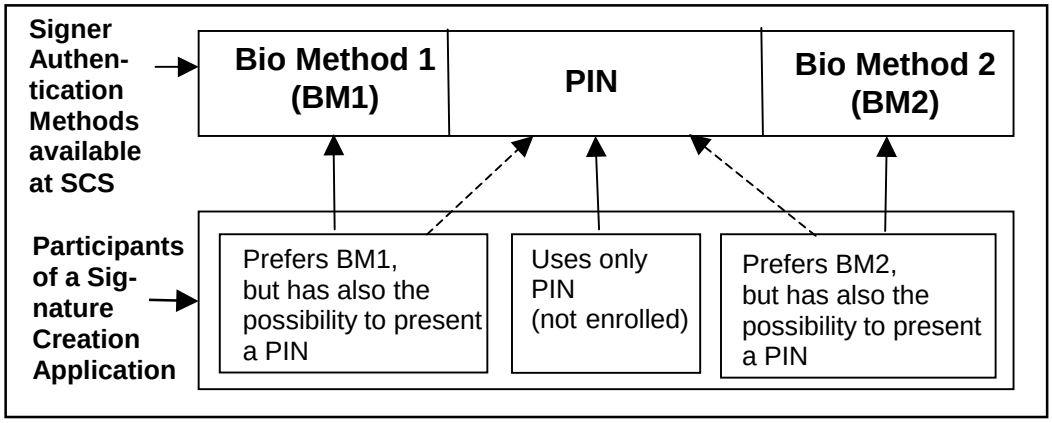

Fig. 60: Grouping of participants of a signature application with respect to applied authentication methods (example)

In a signature creation environment, where a 1-to-1-relationship between signer and the SCS exists, an authentication method should be used that is appropriate to the signer.

11.2 Homebanking

Homebanking is an example for an application in a private PC environment. The banking transactions might need digital signatures to be completed. The legal user of the banking account proves his/her identity with the digital signature.
In this case, the biometric authentication provides the unique link between user and banking account. When using passwords to activate the signature function, one possible danger could consist of underage children looking at their parents typing in the password; afterwards, they could be able to perform banking transactions under the name of their parents. This danger can be avoided if the digital signature is enabled after successful biometric authentication only.

11.3 E-Commerce

Applications of E-Commerce where goods are ordered and paid electronically can be provided in a private PC environment as well as at a public service terminal.
If a private PC environment is used, the situation is very similiar to homebanking: If biometric authentication is used for enabling the signature to confirm the order, underage children can be prevented from doing financial transactions under the name of their parents.

11.4 Health Care

Many possible applications of electronic signatures are provided in the field of health care. One important application is the signing of electronic prescriptions in a medical doctor's surgery. In this case, the feature matching, if it shall be performed inside a smartcard, will be implemented into the Health Professional Card, the special sort of signature card for this application.
The generation of signed electronic prescriptions is an example for an application where a lot of signatures have to be generated during one day. The need for typing in a PIN for each individual signature will not find a high level of user acceptance among the medical doctors.
Here, the combination of PIN and biometric authentication, as currently required by the German Signature Establishment, can already provide more convenience: When entering the surgery in the morning, the doctor only needs to type in the PIN once to start the electronic prescription application. Afterwards, the system may stay in this state all day, and biometric authentication is used for each individual signature.

11.5 Office Environment

In an office environment where e-mails are signed, the situation is similar to the medical doctor's surgery: Many documents have to be signed on one day.
With the combination of knowledge-based and biometric authentication, it is possible to activate the e-mail application by typing in a PIN once a day and then to use biometric authentication for signing each individual e-mail.

12 Quality and Evaluation Criteria for Products and Algorithms

There are still a lot of problems around the quality features of biometric products and algorithms:

- strength of mechanism (e.g. in comparison to the PIN mechanism)
- testing, test suites and biometric databases
- evaluation and embedding in protection profiles
- comparison of products with the same biometric method and with different biometric methods

Many manufacturers express the quality by indicating the values for FAR and FRR. However, the values as such are not sufficient if it is not exactly specified how they have been measured.

12.1 Strength in Comparison to PIN Mechanism

The final goal of the development of biometric authentication systems is to get an alternative to the previously used PIN mechanism.
For security applications, it is usual to use a 4-digit PIN (e.g. for a cash dispenser). This means that the mechanism of biometric authentication must provide at least the same strength as that of using a 4-digit PIN.
If you disregard, for simplicity, the fact that not all 4-digit numbers represent a valid PIN, there are 10000 possible PIN values, i.e. the probability for guessing the correct PIN is 1/10000. This means that a biometric authentication system must have an FAR value of 1/10000 (for one trial) in order to provide the same security as a PIN mechanism with a 4-digit PIN.

12.2 Discriminatory Power regarding FAR and FRR

For all biometric recognition methods, there is the dilemma of the right choice for the tolerance limit for a correct match: On the one hand, the legal user of a security application like an electronic signature shall not be rejected (i.e. a low FRR value is desired), on the other hand, defrauders have to be prevented from getting unauthorised access (i.e. the FAR value must not be too high, too).
It depends on the individual application, whether the minimisation of FAR or that of FRR has higher priority. For a customers service application, a low FRR value will have the priority since the customer would not accept the usage of a system rejecting the legal user. For security applications in a company, it is more important to really prevent any unauthorised access, i.e. the tolerance limit will be lower in order to minimise the FAR value.
One quality measure of a biometric product or algorithm will consist in the discriminatory power of the biometric feature, i.e. how far it is possible to make a reasonable separation of accepted and rejected data samples.
The EER value is one parameter that gives some information about the discriminatory power. However, this information alone is not sufficient; closer information can be obtained by looking how fast the two error rates are increasing when moving the tolerance limit away from the EER point.
For this purpose, you consider a fixed value Δ and look at the size of the zone where FAR and FRR are both below EER+Δ. Fig. 61 shows the two curves for FAR and FRR with the crossover point at the EER value (see also [TTT98]). The area *A* between the horizontal line for EER+Δ and the two curves represents the measurement for the discriminatory power: A large area means a high, a small area means a low discriminatory power.

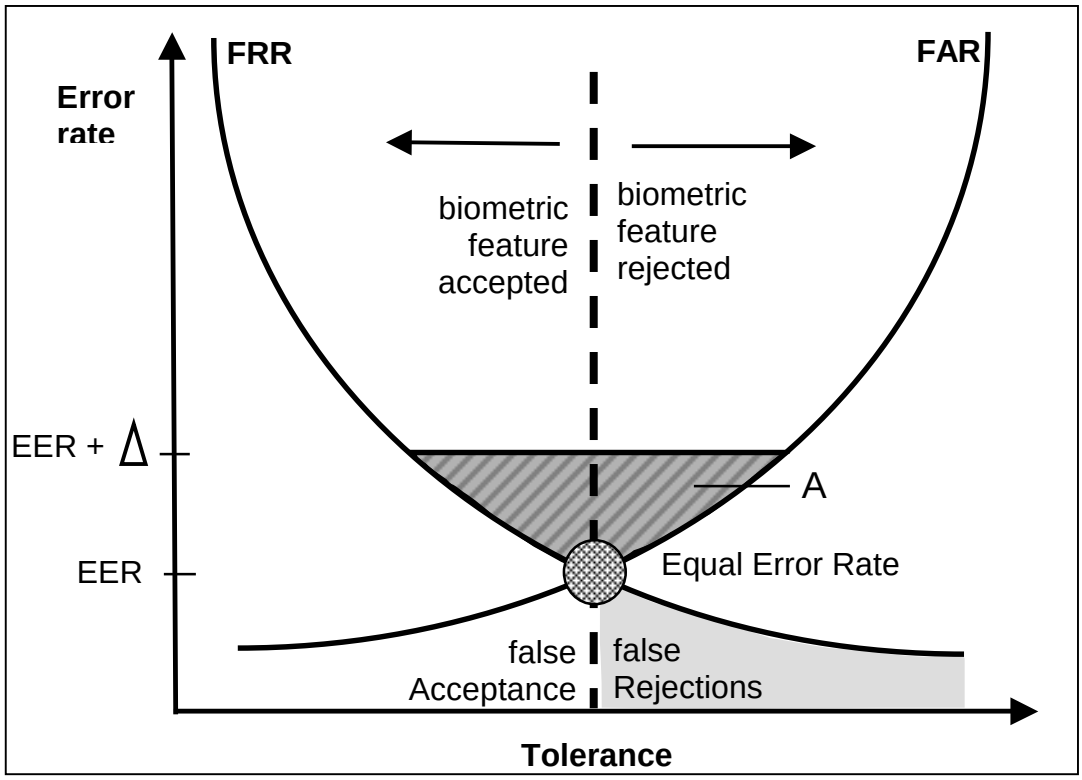

Fig. 61: Discriminatory Power Measurement with FAR and FRR

The formula for calculating *A* can be expressed in the following way:

Let $t_0 \leq t_1 \leq t_2$ be the corresponding values for the tolerance limit for which $FRR(t_0)=EER+\Delta$, $FAR(t_1)= FRR(t_1)=EER$ and $FAR(t_2)=EER+\Delta$.
Then, if the functions for the curves for FAR and FRR are known, there is

$$A = (EER + \Delta) \cdot (t_2 - t_0) - \int_{t_0}^{t_1} FRR(t)dt - \int_{t_1}^{t_2} FAR(t)dt .$$

This simplified model considers only the case of a scalar (one-dimensional) distance between verification data and reference data and a corresponding one-dimensional tolerance limit; this may be handled e.g. by calculating a vector norm of a difference vector. Of course, not all feature matching algorithms may be handled in this simple way; it may be necessary to consider several different tolerance limits for several features or to fulfil a chain of such conditions for a successful verification (e.g. a minimum number of fingerprint minutiae where each of them has to match within specified tolerance limits).

12.3 Models of Distribution Functions for FAR and FRR

The model presented in clause 12.2 is useless as long as the curves for FAR and FRR are unknown. Before being able to calculate any error rates dependent on tolerance limits, you first need statistical distribution functions for the considered biometric features.
Setting up these distribution functions is a difficult task since the biometric features depend on many influence parameters that are difficult to capture by simple formulas. The situation is even more complicated for a model of the FAR function since this requires a distribution function for the biometric features of any unknown defrauder.
In general, it will be necessary to set up a distribution function where the final decision parameters will depend on each individual genuine user or impostor. In order to get universal values for FAR and FRR, a cumulative value out of the individual values obtained from several test persons has to be determined.
An approach to this problem is described in [Way99] where two distance values for a biometric user template are defined: A so called "genuine distance" and an "impostor distance". This model makes the following assumptions:
One biometric sample of a user h is represented as a feature vector X_h, consisting of J components x_{hj} (j=1,...,J).
A template (i.e. the reference data) of a user h consists of an average vector $\overline{X_h}$ of M different samples X_h^i (i=1,...,M), i.e. $\overline{x_{hj}} = \frac{1}{M} \sum_{i=1}^{M} x_{hj}^i$.
Now, for an additional sample X_h^{M+1} of the user h (which can be considered as actual verification data) the genuine distance for the user h is defined as $d_{hh} = \left\| \overline{X_h} - X_h^{M+1} \right\| = \left\| \Delta_{hh} \right\|$.
With the same metrics, the impostor distance for a user $k \neq h$ with a sample vector X_k is defined as $d_{hk} = \left\| \overline{X_h} - X_k \right\| = \left\| \Delta_{hk} \right\|$.
For the distance measure, any ordinary vector norm (like the euklidean distance) can be used; a weighted vector norm provides the flexibility to consider the varying importance of different features.
Now, during a verification or identification process, two data samples X and Y will be considered as identical if the distance $d=||X-Y||$ is below a certain tolerance limit t.
From the probability distributions for the different features x_j of the users h and k, the probability density functions f_{gen} and f_{imp} for the genuine distance and the impostor distance have to be derived. Then, the error rates with dependence of the tolerance limit t can be calculated in the following way:

$$FAR(t) = \int_{o}^{t} f_{imp}(\tau)d\tau$$

$$FRR(t) = \int_{t}^{\infty} f_{gen}(\tau)d\tau$$

As mentioned at the beginning, each genuine user, pair of genuine user and impostor resp., will have different curves for the error rates. In practice, it will be necessary to calculate the different genuine and impostor distances over a large data base of different users.

12.4 Probabilistic Estimation of Error Rates

As obvious from the previous clause, it is very difficult to get exact values for the error rates. But these values are also not relevant for practical purposes. It is more important to know that the error rates, their distances to the desired values resp. are below a certain limit with a high probability. For this purpose, the error rates are again modelled as random variables whose distributions have to be measured over a large number of test persons. For presenting statements in this direction, you need the following parameters:

- The value r for the desired error rate
- The maximal distance δ to the desired error rate
- The security level τ for which the real error rate is not greater than $h+\delta$ with a probability of at least $1-\tau$.

For simplicity, the error rates are supposed to be normally distributed. Under this assumption, there is a formula stating how many tests have to be performed in order to prove a security level with the parameters mentioned above; this is also discussed in [TTT98]. The number n_τ of necessary tests depends on the parameters in the following way:

$n_\tau=(Z_\tau/\delta)^2 r(1-r)$,

where Z_τ is the $(1-\tau)$-quantil of the standard normal distribution, i.e. for any standard normal distributed random variable Z there is $P(Z> Z_\tau)=\tau$.
If the distributions of the error rates really turn out to be unsuitable for an approximation with the normal distribution, a higher amount of work has to be done to get a reasonable approximation with another probability distribution function.
However, it makes no sense to try to make estimations with the Chebycheff Inequality which makes use of mean value and standard derivation only. This rough estimation is unsuitable for practical purposes since it includes the possible presence of many theoretic and unrealistic distribution functions (e.g. only two possible values with a probability of 50 % each) that will surely not apply to biometric features and error rates. The number of tests theoretically necessary for proving security with the Chebycheff Inequality would be infeasibly large.

12.5 Test Suites and Data Bases

For practical verification test or identification tests, different aspects have to be considered such that their results give reasonable estimations for the error rates.

12.5.1 Live Tests and Offline Tests

Two general sorts of tests have to be distinguished, namely

- Live (online) tests where the test persons present their biometric features each time
- Offline-tests with databases.

Live tests have the advantage that each individual test represents the real situation of a real user. For offline tests, many biometric data samples have to be collected from each test person in advance; afterwards, the verification or identification tests are performed by matching different samples from the data base against each other. The advantage of offline tests consists in the possibility of performing much more different matching tests without the assistance of the test persons.

12.5.2 Significance of Test Persons

For the significance of the tests, it is very important that the test persons represent a large population consisting of many different sorts of people, and not a special circle of persons. Persons from different occupation groups (scientists, hand workers etc.) and with different ages have to be taken.
It is also necessary to consider the different conditions for presenting biometric data at different times. Therefore, the data have to be captured over a longer time period at different day times.
These arguments are valid for live tests as well as for capturing data for a data base to be used for offline tests.

12.5.3 Neutral and Objective Test Scenarios

For test scenarios, it is also important that they are not influenced by the individual interest of any manufacturer. Of course, the test methods have to be adapted to the individual biometric method. However, the following points have to be observed:

- One unique test scenario has to be prescribed for all products using the same biometric method
- Tests must be performed not by the manufacturer or vendor himself, but by a trusted third party not representing the interests of special products or manufacturers.

12.6 Classification of Forgery Attempts

In general, the FAR will be measured by forgery tests: Verification data are presented by a non-owner of the previously stored reference data, and the cases will be count which falsely result in a successful verification or identification.
It must be observed that there are many different ways of classifying forgery attempts. An FAR value stated afterwards can only be significant if it is clear by which sort of attack it has been measured.

12.6.1 Random Forgeries vs. Trained Forgeries

The first general distinction has to be made between the following two sorts of forgeries:

- Random Forgeries: The original data of another user is presented to the system in a natural way; no special effort is taken to manipulate the system.
- Trained Forgeries: Impostor's data are presented in a special way with the intention to be similiar to the original data.

In practice, an FAR value measured by random forgeries only represents the ability of a biometric algorithm to distinguish the biometric data of different users. For evaluating a product with respect to the security against attacks, the FAR has to be measured with trained forgeries.
With offline tests using simple comparisons of different data out of a data base, only random forgeries can be simulated. If is possible to calculate appropriate modifications of the data contained in the data base, offline tests may also be used to simulate trained forgeries.

12.6.2 Attack Levels for Trained Forgeries

For attacking a system by trained forgeries, different attack levels have to be considered concerning the expenditure and the necessary knowledge about the system for the impostor. As stated in [TTT98], the German Agency for Secure Information Technology (BSI) uses the following classification:

- Low expenditure: No special knowledge about the system, low time exposure.
- Medium expenditure: Some special, but publicly available system knowledge, time exposure of some hours or days.
- High expenditure: Very special insider knowledge about the system, time exposure of several weeks.

12.6.3 Defrauding vs. Circumventing the Sensor

From the physical point of view, the two following sorts of attacks have to be distinguished:

- Defrauding the biometric sensor directly by a dummy.
- Circumvention of the sensor by inserting electronic data pretending the origin from the sensor (spying out or replay attack).

This shows that a biometric system contains different components that must be evaluated with the aid of different forgery tests: The resistance against direct defraud of the sensor is a quality criterion for the sensor itself whereas the resistance against replay attacks is a quality criterion concerning the secure data transfer from the biometric sensor to the verification unit (i.e. the SSCD).

13 Legal Aspects

When protecting an electronic signature application with biometrics, the different existing laws and establishments on electronic signatures have to be observed first. There are some regulations on European level as well as some national signature laws in the individual European countries.

13.1 Current Regulations on European Level

The current directive of the European Parliament does not put any specific restrictions on using biometrics for digital signatures. It only says that signature creation devices must ensure that signature creation data "can be reliably protected by the legitimate signer against the use of others" ([EU99], Annex III). Nothing is said how this protection has to be done exactly, i.e. with knowledge based or biometric authentication.

13.2 Current Regulations on National Level

Existing national regulations in the field of electronic signatures have to be adapted to the European regulations within a timespan of 2 years. As example for the national situation with respect to electronic signature and biometrics, the situation in Germany will be outlined.
In 1997, the German Information and Communication Services Act ([IUKDG97]) with the Digital Signature Act and the corresponding Digital Signature Ordinance was founded. In contrast to the European directive, the German Signature Ordinance is very restrictive. It states that biometric authentication can be used in addition to knowledge-based authentication to protect electronic signatures. This currently allows only a combined system of biometrics and PIN authentication, but no complete replacement of the PIN by biometric authentication.
In practice, this means that the advantage of biometrics currently does not consist of security reasons but of convenience reasons only. A signature system might e.g. be configured in this way that the application has to be started once by typing in a PIN, and that biometric authentication is used for each individual signature afterwards. This just avoids the need for typing in a PIN for each signature; however, the security of a signature system following the German Signature Ordinance still depends on the fact that the user needs to know a PIN in order to activate the application.

The German Ministry for Business and Technology has recently worked out an amendment of the German Signature Law [BWT2000], which, in the mean time, has been decided by the German Cabinet, too [Cab2000]. This new law, a law on "Framework Conditions for Electronic Signatures" shall come into effect at the beginning of 2001. The major point of the renewed law is the adaption to European principles on electronic signatures.
The plans of changing the signature law with regard to realisation of European guidelines has recently been commented and welcomed by the German Consortium of Consumers "AGV - Arbeitsgemeinschaft der Verbraucherverbände e.V.", see [AGV2000]). In these comments, it is also recommended to change the corresponding Signature Ordinance. One important point is the possibility to also use biometrics as an alternative to knowledge based authentication. This would give biometric methods a higher relevance than before where it could only be used in addition to PIN authentication. By this way, the role of biometric authentication could be raised from pure convenience reasons to a real security tool.
However, AGV also points out that the signer authentication component shall be embedded into a trusted system environment.
Now, after the decision of the new law on electronic signatures, an amending law of the German Signature Ordinance is in progress, too.

13.3 Data Privacy

Biometric data belong to the personal data and as such they are subject of data privacy. Since in this context the verification data are stored only in the SSCD, no problems are seen with respect to data privacy regulations. For the case that an application provider sees a lack of data privacy in the transportation of the verification data to the SSCD, encrypted data transfer should be available as an optional addition as described in clause 8.1.4.
If the SCS is under control of the signer, the encryption of biometric data is optional.

If an SCS is under control of a service provider and the level of confidence for signature creation cannot be achieved by organisational means, then the user's verification data (PIN, password, biometric data) shall be transmitted to the SSCD in authentic and encrypted form.

14 Outlook and open Problems

The use of biometric authentication in the context of electronic signatures would have many benefits. It is obvious that some methods are more suitable than others. Among the favourite candidates for this context will be

- fingerprint
- face recognition
- signature dynamics,

whereby great differences may occur with respect to the type of SCS (PC, laptop, mobile phone, PST, ...) and the usage environment (home, office, mobile, public).

"In principle", the biometric technology is mature enough to be applied in this context. Also, the technology from the viewpoint of a secure signature creation device, especially from that of smartcards, is ready or will be ready soon for performing matching algorithms of different kind in the SSCD. However, there are still considerable problems:

- the resistance against attacks and fakes is in some solutions not sufficient

- in many cases, the overall performance should be improved

- to date, no crypto sensor units with feature extraction are available for methods where biometric verification data needs to be secured by means of symmetric or asymmetric crypto algorithms

- the reliability of some solutions seems not to be sufficient

- the realisation of smartcards with sensor (e.g. flexibel fingerprint sensor), feature extraction and feature matching remains still a great challenge

- there are no standardised algorithms to ensure interoperability, what is essential for this context (aspects of second sources for SSCDs, usage of different sensor types for the same biometrical method, different SCS manufacturers, ...)

- standards in various fields related to this subject (BioAPI, CBEFF, ISO/IEC 7816, ...) are either not yet finished or do not take into account the special scenario, where the comparison of verification data and reference data is performed in the SSCD

- there is less experience in evaluation, testing, determination of strength of function and comparison of biometric solutions, so that potential application providers hesitate to rely on certain solutions.

Therefore, the combination of biometric methods and electronic signatures remains a challenge for the industry, research institutes and standardisation bodies. Also the pricing for

biometric solutions should be "reasonable" since this factor has also big impact on market relevance of products.