60

Development of an European-wide Citizen Javacard to Support Administrative Processes by the Use of the Electronic Signature and the Biometric Fingerprint Sensor

A case study of legal implications

Markus Wenderoth and Dennis Wörmann
Zuendel & Partner Unternehmensberatung, Bochum, Germany

Abstract: This paper describes the results of the project "Facilitating Administrative Services for Mobile Europeans (FASME), which aims to develop a Javacard prototype, i.e. a chip card on the basis of the Java programming language which is not platform dependent. The Javacard will allow for specific administrative tasks such as the registration and de-registration of addresses and reregistering motor vehicles to be safely and flexibly carried out throughout Europe.

1. INTRODUCTION

The abbreviation FASME stands for the project entitled "Facilitating Administrative Services for Mobile Europeans", i.e. supporting individual EU citizens in dealing with administrative processes within Europe. The project, which in all is to run for a period of 18 months, was started on 1 January 2000. Within the framework of the FASME project a Javacard prototype will be developed, a chip card on the basis of the Java programming language which is not platform dependent, that will allow for specific administrative tasks such as the registration and de-registration of addresses and reregistering motor vehicles to be safely and flexibly carried out throughout Europe. Furthermore, the prototype provides individual assistance within the framework of services (meta applications) for the initial period following a move within the European member states.

By using the FASME Javacard prototype, visits to the authorities regarding administrative matters by individual EU citizens such as registering and deregistering an address and reregistering motor vehicles can be organised in a more efficient manner.

The FASME Java Card is especially equipped with a biometric fingerprint sensor and an e-Signature. By using these two components administrative processes in the public sector for each EU citizen and the municipalities should be legally secure.

2. BIOMETRIC FINGERPRINT PROCEDURE

The FASME Javacard is equipped with a fingerprint sensor that is integrated in the card. This fingerprint sensor carries out and ensures for the safety of the verification or the identity of the EU citizen in carrying out the administrative processes on the basis of the minutia[79] comparison procedure. Furthermore the fingerprint sensor is used as an access security mechanism for the electronic signature.

2.1 Practical procedure

The detailed procedure of the identity analysis by way of the biometric fingerprint is carried out in the following steps:

1. Placing the FASME Javacard in the terminal reading device. The internal error counter on the Javacard, which also serves the purpose of limiting the number of possible unsuccessful analysis attempts, increases by the value one.
2. Reading the fingerprint of the card user by way of the fingerprint sensor and transmitting the read data to the Java chip on the card.
3. Comparison of the read fingerprint of the card user with the fingerprint sample (reference value) of the card owner (verification) stored on the card via the chip processor (Java VirtualMachine). The verification is based on an examination of minutia pairs.
4. In the event that the two fingerprint data records are identical, the card is approved for usage and a specific data transaction made possible that is supported by the Javacard. As only one single transaction is possible, a new fingerprint analysis shall be required for each transaction. In the case of a successful fingerprint analysis the error counter will be reset to zero.
5. If the two fingerprint data records are not identical, the error counter within the card increases by the value one. If the error counter reaches a predetermined valid, the card will be (temporarily) blocked for all further usage. In such a case the blockage lifted by an authorised administrative official.

[79] Sample of dermal ridges on the fingertip; Data Protection and Data security, 06/2000 p.328

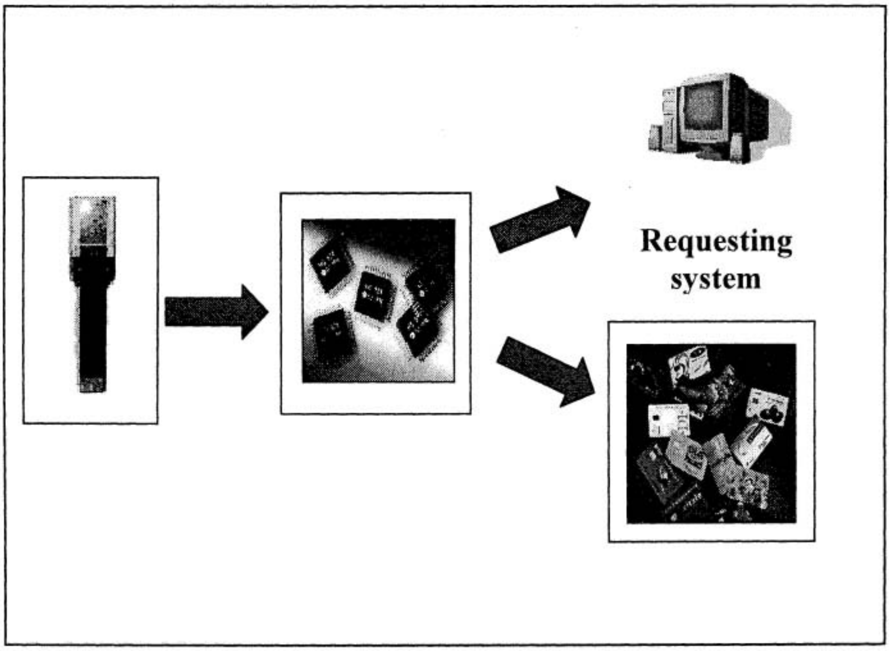

Figure 6. Minutia comparison procedure

2.2 Legal implications

The practical procedure described above warrants a comprehensive legal appraisal on the basis of the following criteria.

2.2.1 Constitutional requirements within the EU member states

The constitutions in the EU member states stress in strong terms the protection of human dignity and thus make the principle the uppermost value of the respective constitution.

If the use of biometric procedures were to constitute a violation of the dignity of man, the state authorities would, on the one hand, be prohibited from using these procedures. On the other hand agreements under civil law that provided for the use of such procedures which violated man's dignity would also be inadmissible. The state would be under obligation to intervene to put an end to the situation in violation of the constitution. With regard to the use of biometric procedures the initial question law should be put as to whether certain restrictions or parameters are contained in the constitution. The particular explosive nature of biometric procedures arises in this respect from two aspects: on the one hand identification procedures are directly linked to physical features of the affected person. On the other, physical characteristics are thus instrumentalised for certain purposes.

If an individual is forced to use his/her body in a certain manner, such action may be discussed as a vulgarisation from a subject to an object.

Whether individual procedures place the dignity of man in jeopardy in a non-uniform market depends, above all, on the features with which it works and in which manner the biometric data of the user is requested. The dignity of man is particularly endangered if an individual has no opportunity to control, at a given time, his/her biometric data that is being recorded[80]. Then, he/she would be more in danger of being vulgarised to a mere object. Therefore, such procedures are worthy of preference which calls for an active participation of the affected person, for example the signature verification. The violation of dignity may, however, also arise from the excessive information content which can occur in some procedures.

In general a distinction between the use of biometry in the public and private sector is to be made. The private sector is not taken into consideration in this examination.

In the public sector it is worthwhile making a distinction between two different areas of application of biometric identification procedures:

- Global applications in which a considerable group of the population is placed under obligation to achieve an administrative purpose in participating in a procedure. The American examples demonstrate that such procedures are frequently used to prevent unauthorised use with regard to the receipt of state services.
- The separate application in a public institution to bring about certain security objectives. The access security mechanisms should be given consideration in this respect. However, authentication via a system as regards the authorship of certain decrees is also possible.

Because of the explosive nature of the legal foundations of these procedures, which arise from the proximity described above to the dignity of man that is separately protected by the constitution, it would, moreover, appear to be necessary to provide for the global application by way of a special, area-specific legal foundation.

2.2.2 Legal admissibility of biometric procedures

The Directive 1999/93 pertaining to the Community outline conditions for electronic signatures expressly leaves open the technology that is to be used which, in particular, is expressed in the reason for consideration (8): "The rapid technological development and the global character of the Internet call for a concept which provides an open-minded approach towards technologies and services in the field of electronic authentication."

[80] E.g. facial recognition at greater distances, analysis of the chemical composition of body odour

Furthermore, according to the opinions held by technicians, the signature composition data defined in Article 2, no. 4 also allows for the use of biometry.

In addition, according to Annex III, 1.c) of the Directive, a guarantee must be provided in the case of the so-called secure signature composition data that "the lawful user's signature composition data used for the compilation of the signature is capable of being reliably protected from use by others."

2.2.3 Legal and data protection law implications

By using biometric fingerprint sensor the increased protection for the so-called sensitive data listed in Article 8, Section 1 of the EU data protection directive[81] could be, above all, of interest. This includes information pertaining to the racial and ethical origin, political opinions, religious or philosophical convictions, union membership, health or sexual activities. The processing of such data is only permitted subject to restricted preconditions. The fingerprint can, for example, provide indications of a certain racial or ethical affiliation. However, this merely applies to the biometric raw data that has not yet been prepared for the purpose of identification. In contrast, the templates, with which the actual identification process operates, do not constitute any sensitive data because a direct conclusion as regards the full biometric entry information (for example on the fingerprint) cannot be drawn on the basis of such templates. The increased preconditions in accordance with Article 8 of the Directive follow on, however, from the processing, but not only from the storage. In accordance with Article 2, letter b) of the Directive, even the collation of data is regarded as processing. The collating of biometric raw data by the system constitutes a record within the meaning of this Directive. Accordingly, an excessive information content in the case of the collation of biometric raw data can be sufficient to make the procedure, or at least the respective procedural part, subject to the special protection of sensitive data in accordance with Article 8 of the Directive. This can only be avoided if no excessive amounts of sensitive information arise in the respective procedures.

Due to the fact that the biometric data is personal data, it is necessary, therefore, that the following requirements are ensured via the fingerprint sensor and the like integrated in the FASME JavaCard[82]:

- It must not be possible to deduce the personal identity of a user from the biometric data
- Biometric things may not be used as personal reference numbers
- Data storage and transport must be secure

[81] Directive 95/46/EC of the European Parliament and Council dated 24 October 1995

[82] Compare in detail Weichert, CuR 6/97, p. 369 et seq. and Data Protection and Data Security 3/1999, p. 128 et seq.

- With regard to the estimation of the necessary level of protection, the question of how permanent the link is between the biometric data and the person should be taken into consideration
- The user must be aware of the possibility of a check

2.3 Legal appraisal of the applied biometric procedure (fingerprint sensor) of the FASME Javacard

The special technical design of the FASME Javacard allows for the data processing of the read fingerprint data, i.e. it is possible to match the stored reference data (submitted fingerprint sample) on the card. In this respect the match is carried out via the chip's central processor, the Central Processing Unit (CPU).

Instead of a central storage of reference data, which would call for the necessity of a higher level of legal data protection, the FASME Javacard only stores reference data of the respective card owner. Thus the decentralised storage of reference data is within the dominion of the respective user.

The aforementioned reasons allow an assurance to be given as regards the aspect of the security of data storage and data transport.

Because merely a few characteristics (minutia) of the fingerprint are processed during the application of the fingerprint sensor, a reproduction of the entire fingerprint and thus a conclusion as to the personal identity of a respective user are excluded. This means the amount of used minutia is not greater than that which is required for the recognition (principle of avoiding the creation of unnecessary data and the effective usage of data). Therefore, the usage of the biometric data as a reference to a person is excluded.

In the case of processing the supported processes the system provides an express request to submit the personal fingerprint prior to the analysis of each fingerprint. In this respect it is incumbent upon the respective user to either approve of or discontinue the process.

As a result of the active co-operation by the user same is aware of a possible verification at all times.

The intended integration of the biometric fingerprint sensor in the FASME Javacard ensures that there is a reliable protection, which is not achieved by way of the PIN and password, because biometric procedures provide considerably better protection as regards access to the signature key on the basis of the aforementioned reasons.

It should be noted that the biometric fingerprint procedure used in the FASME project satisfies the highest legal data protection requirements.

Finally it should be noted, that the global use of an european-wide citizencard for administrative processes requires an explicit european-wide legal basis. The opportunities of biometry should, in particular in view of the discussed legal effects of electronic signatures, be used within the different legal systems in Europe.

3. APPLICATION OF THE ELECTRONIC SIGNATURE

It is envisaged that the electronic signature be initially used with the support of the FASME Javacard in the case of data transfer processes in public administration for the process of changing an address and registering a motor vehicle.

It is envisaged that as a result of this EU citizens will, in the future, be able to make use of public sector services which ensure that security objectives are reached, such as:

- The authenticity of a sender
- The coding / deciphering of the content
- The integrity / genuineness of the data content

The binding nature of the documents and explanations.

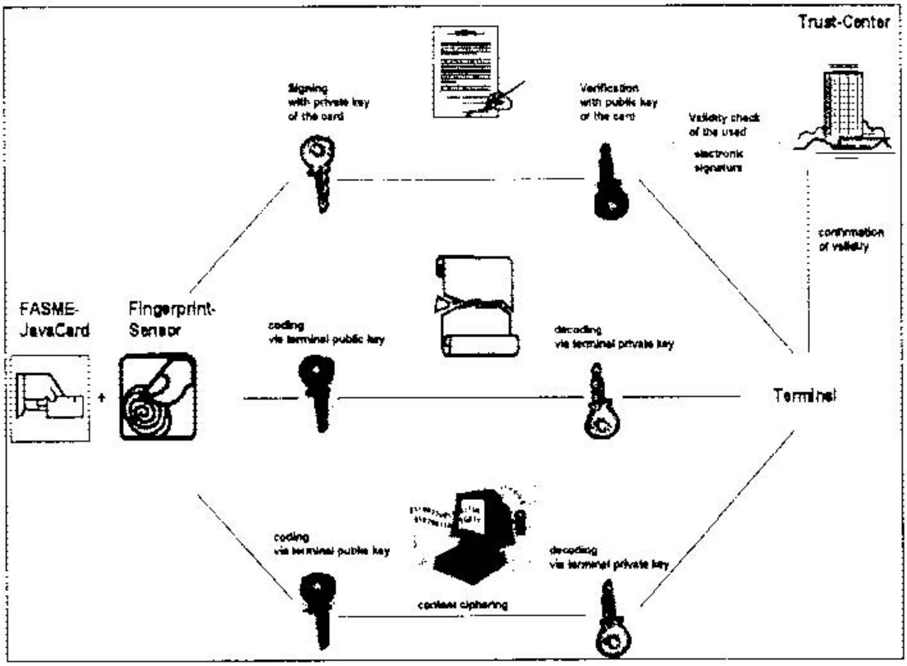

Figure 2. Signature procedure

3.1 Practical procedure

The following outline conditions are created with regard to the application of the electronic signature so as to ensure that the stated security aspects are followed:

- Each FASME-Javacard is allocated a unique asymmetrical key-pair. This key pair is made up of one private key and one public key. The allocation of the key pairs is carried out within the framework of the certification of the FASME Javacard via a state-recognised certification service provider.
- The private key serves the purpose of signing a data record that is to be forwarded so as to guarantee the authenticity of the owner of the private key, and thus the sender.
- Furthermore, the private key is used to decipher / decode a received and coded data record and to authenticate / verify the genuineness of the content of a received data record.
- The public key serves the purpose of coding / ciphering data records which are sent to the key owner and to verify the authenticity of the identity of the sender (by way of his/her public key). To this end the public key must initially be made known to the sender (coding) or the addressee (authenticity).

The detailed procedure of the application of the electronic signature is explained below on the basis of a data transfer from the FASME Javacard to a terminal at an official institution:

1. The FASME Javacard contains the relevant data which is required for the terminal at an official institution to handle a specific process.
2. For the secure transmission of the relevant data - avoiding inspection by unauthorised persons / guaranteeing the genuineness (authenticity) - the information is ciphered / coded by way of the terminal public key.
3. To sign the data record and thus guarantee the clear identity (authenticity) of the sender, the information is coded / ciphered by way of the private key of the FASME Javacard. The creation of the electronic signature is sparked via a legitimisation on the card by way of the provision of a fingerprint of the respective card user.
4. The actual data transfer takes place.
5. Once the data transfer has been concluded, the decoding / deciphering of the received data takes place by way of the terminal private key. The verification of the integrity of the transferred data takes place via the calculation of a proof total (hash value) by way of the terminal private key and the match with a test value calculated prior to the data transfer. Even the smallest change in content of the transferred data record brings about a deviation between these test values.
6. Securing of the authenticity of the sender is carried out by verifying the signature with the sender's public key. In this respect the party providing the guarantee is a state-recognised certification authority (a so-called Trust Centre).

3.2 EU Directive 1999/93/EC

Electronic communication and electronic business transactions call for "qualified electronic signatures" and appropriate authentication services for data. Diverging regulations pertaining to the legal recognition of qualified electronic signatures and the accreditation of certification service providers in the member states can pose a serious obstacle to electronic communication and electronic business transactions. In contrast, clear Community outline conditions for qualified electronic signatures strengthen the trust and general acceptance regarding new technologies. After more than one year of continuous discussions an agreement has been reached in Europe regarding a Directive for electronic signatures. It came into force on 19.01.2000 in Brussels via the European Parliament and the Council of the European Union.

The Directive should be conceived such that, above all, different legislation in the member states be avoided. Therefore, the Directive not only provides for the definition of a legal but also an organisational framework.

The objective of the Directive of creating the application of electronic signatures in a largely uniform legal framework within the European Union will be largely achieved.

The framework is sufficiently flexible so as not to exclude any future technological developments.

In accordance with Article 13 - Implementation, the Directive must be implemented in national law in all EU states within the next 18 months, at the latest by 19 July 2001.

3.3 Legal appraisal of the FASME signature procedure

After more than one year of ongoing discussions an agreement has been reached in Europe regarding a Directive for electronic signatures. Next year will see the implementation of the Directive in the member states of the EU. It is envisaged that the Directive be designed such that above all different forms of legislation be avoided in the member states. Therefore, the Directive does not provide for just a legal framework, it also offers an organisational framework.

In the case of the implementation of the Directive primary importance should be attached to the aspect of harmonisation. The states should not create any new terms[83] following the approach towards harmonisation of the EU Directive. The terms used in the Directive have not been selected optionally because they do not comply with the nomenclature defined by the standardisation committee.

However, a new introduction of - even contradictory - terms in the national legislature would result in widespread confusion among the population and companies. It is worthy of note that the member states may make the application of signatures in the public sector dependent on additional requirements[84]. In this respect it is hoped that for the EU member states no additional legal requirements are created that would hamper the trans-border services for citizens.

[83] Data Protection and Data Security, edition 02/2000, p. 88

[84] Artikel 3 Absatz 7 EU Directive 1999/93/EC

3.3.1 Qualified signature

In order to do justice to the statutory requirements regarding the application of the FASME JavCard in the area of public administration for the processes involving a change of address and registering a motor vehicle, a qualified electronic signature is used which satisfies the preconditions of Article 2, no. 2 a) to d) of the EU Directive 1999/93.

The qualified electronic signature used in the FASME JavaCard is, in each case, solely allocated to the lawful owner of the card, by whom it can be created, because only the right user can use the card to sign by way of the biometric components. Accordingly, the qualified electronic signature thus created allows for a definite identification of the FASME JavaCard used to sign and in addition an identification of the signing user as a result of the uniqueness quality of the key pairs. Because all the components used for the creation of the qualified electronic signature (key pairs, numeric processing unit, fingerprint sensor) are to be found directly on the card, and are thus directly within the user's dominion, the signing party can keep them under his/her sole control. By creating a hash value via the signature within the framework of the coding, it is possible to recognise subsequent changes made to the data.

3.3.2 Secure signature composition units

The secure signature composition units that are required to create a qualified electronic signature are determined in greater detail in Annex III of the Directive 1999/93. The utilisation of special signature composition units is guaranteed within the framework of the FASME project on the basis of the techniques and procedures described below:

The signature composition data used to create the signature are cryptoalgorithms in accordance with the parameters of the interoperability specifications which are to be issued by way of the Trust Centre that complies with the requirements. This ensures that the used data is unique. The secrecy of the data and the prevention of unauthorised usage are guaranteed by the method of construction and the functions of the used chip card.

The modern signature procedure and the used cryptoalgorithms (RSA[85]) allow the user to inspect the data that is to be signed. They do not change the content of the data but, however, prevent the signature composition data from being deduced and prevent signature forgery.

The cryptographical requirements regarding the used hash functions and signature algorithms to create a key are satisfied by the FASME JavaCard. It is presumed that the hash function SHA-1 and the cryptoalgorithms in accordance with

[85] Rivest, Shamir und Adleman Krypthoalgorithmen

the RSA procedure be used within the framework of the project to create signatures, and for coding and decoding.

3.3.3 Certificates

In order to satisfy the requirements pertaining to the qualified signature, the signature used in the FASME project must be based on a qualified certificate. In accordance with Article 2 of the definition no. 9 of the Directive, the term "certificate" describes an electronic certification with which signature testing data of a person are allocated and with which the identity of this person is confirmed. A "qualified certificate" is a certificate that satisfies the requirements of Annex I and which is made available by a certification service provider which does justice to the requirements set out in Annex II. The Directive and the Europe-wide legislation have not yet stipulated any definite certification format. However, it solely pursues the objective of creating outline conditions for qualified electronic signatures with high security requirements.

A utilisation of the version X.509v3, which has presented itself as the general format for certificates, is planned within the framework of the FASME project, that would allow an european-wide usage. It is noticed that different efforts are in progress to norms of certificates harmonise european-wide.

4. TRUST CENTRE

Finding solutions to two problems is of crucial importance to the security of data transmission in open networks. On the one hand it must be ensured that unauthorised access is not possible so as to prevent manipulation of the transferred data. On the other it must be clearly determinable that transferred data actually originates from an authorised sender. Like an "electronic notary" the Trust Centre creates and "authenticates" the signature key and thus creates a trusted foundation for qualified electronic signature procedures in the case of the electronic transmission of data. The Trust centre must satisfy the stringent legal requirements to as to ensure that the electronic signing of information is legally binding and secure.

If it is determined within a public key infrastructure that a certain public electronic key belongs to a certain person or institution, a trusted and independent third party must have previously verified the allocation. Subsequently, this third party can vouch for the identity of the key owner. This trusted third party is the Trust Centre. Following the identification of a person, for example by way of the presentation of a personal identity card, the Trust Centre establishes by means of a qualified certificate that a certain electronic key belongs to the appropriate certificate owner. The qualified certificates are, in turn, kept ready in a secure, electronic directory which is accessible at all times so that a third party can determine the validity and the authenticity of the owner.

As it is envisaged that an qualified electronic signature that is required to be legally binding be used to deal with administrative processes via the FASME JavaCard (change of address / motor vehicle registration), co-operation with a Trust Centre is inevitable. For the FASME project this means that the administrative authority must have access to the aforementioned electronic directory when verifying the electronic documents that are completed and signed by the citizen so that the authority can determine the validity of the qualified certificate and the authenticity of the EU citizen.

A "certification service provider" in accordance with Article 2 of the definition no. 11 of the EU Directive 1999/93 is an office or a legal or natural person who issues certificates or provides other services in conjunction with electronic signatures.

A certification service provider is a certification service provider who complies the preconditons of Annex II of the Directive.

The directive allows the member states and the suppliers of certification services plenty of room for manoeuvre as regards the establishment of different infrastructures for electronic signatures.

In accordance with Article 2, Section 1, the member states may not make the provision of certification services dependent upon a prior agreement. However, certification service providers who satisfy the requirements of Annex II are subject to a monitoring system that is to be set up in each member state if they offer qualified certificates publicly. The monitoring system may either be publicly or privately organised.

In addition, the member states are not prevented from establishing a voluntary accreditation system to achieve greater security. It is questionable as to who would require still greater security. But this hypothetical question aside, it is possible for the member states to establish own voluntary accreditation systems which place different requirements on security. The Directive text does not state whether the system must build on that what has already been defined or whether requirements may be formulated which extend beyond the four annexes[86] . At the present time it would appear that as a result very different systems may occur in the individual sates. To increase harmonisation the EU Commission can publish reference figures of secure products which can be used for the composition of qualified signatures[87].

In view of the planned EU-wide application of the FASME JavaCard it remains to be seen whether the individual member states make these Trust Centres subject to additional statutory requirements during the course of introducing accredited certification service providers.

[86] Data protection and data security, edition 02/200, p. 88

[87] See also article 3, Section 5 of the Directive 1999/93/EC

It is hoped that the states do not make any new form requirements or regulations so as to justify the higher security level for a voluntary accreditation system.

5. CONCLUSION

On the basis of the biometric fingerprint procedure that is used, a level of protection is achieved which complies with the highest legal data protection requirements as regards processing person-related data.

The requirement of a special legal basis will be deemed given with regard to the EU-wide application of the FASME JavaCard in which the biometric fingerprint sensor is used in the field of public administration.

Within the framework of the FASME project a so-called advanced or qualified electronic signature is to be used that is based on a qualified certificate pursuant to the preconditions of Annex I. This must satisfy the preconditions of the EU Directive 1999/93, Article 2, no. 2 a) to d). Secure signature composition units that do justice to the requirements of Annex III of the Directive 1999/93 are required to create such an advanced or qualified electronic signature. As a result of the components used within the framework of the project (JavaCard, etc.) it is possible to ensure that the requirements regarding secure signature composition units are adhered to.

As a result of the intended utilisation of the hash function SHA-1 and the signature algorithm based on the RSA procedure, it is possible to ensure that the interoperability of the signature procedure will function as required.

It is envisaged that the signature used in the FASME project be based on the standard version X.509v3, which has presented itself as a general format for certificates, because a certain certificate format has neither been stipulated Europe-wide nor by national legislation in the member states.

With regard to the EU-wide application of the FASME JavaCard in the public sector it would be necessary to install a certification service provider who at least satisfies requirements of Annex II of the Directive 1999/93. First of all it remains to be seen how the individual member states implement the special preconditions of Annex II into national law. In this respect a harmonisation of the infrastructure for the Europe-wide application of the advanced or qualified electronic signature is of the greatest importance. Beyond this it is hoped that the EU member states do not make the certification service providers in the public sector subject to additional statutory requirements.

In the author's opinion it would be desirable that the member states implement uniform provisions of law pertaining to the parity of treatment of the qualified electronic signature with hand-written documents, in particular in the field of public administration, because a pioneering role is attributed to public sector administration.

6. REFERENCES

Kruse, Peuckert (1995): Chipkarte und Sicherheit; in: Datenschutz und Datensicherheit, Nr. 3, 1995

Probst, T. (2000): Biometrie und SmartCards, in: Datenschutz und Datensicherheit, Nr. 6, 2000

Weichert, CuR 6/97, p. 369 et seq. and Data Protection and Data Security 3/1999, p. 128 et seq.

Wirtz, B. (1999): Biometrische Verfahren, in: Datenschutz und Datensicherheit, Nr. 3, 1999

Directive 95/46/EC of the European Parliament and Council dated 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

Directive 1999/93/EC OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 13 December 1999 on a Community framework for electronic signatures pertaining to community outline conditions for electronic signature dated 19.01.2000.

Data Protection and Data Security, edition 02/2000, p. 88

Fox, D. (1997): Wohlmacher, P., Chipkarten - Nutzen und Leid; in: Datenschutz und Datensicherheit, Nr. 5, 1997

German Federal Office for Security in Communications Technology dated 6.08.2000