Decision taken by
the Federal Government
regarding
security in electronic legal and commercial transactions involving the federal administration

on 16 January 2002

I.
Decision

With the aim of

- acting with legally binding effect, and
- safeguarding baseline IT security,

in respect of legal and commercial transactions with its partners where the underlying means of facilitating these transactions is electronic (citizens, businesses, administrations), the Federal Government wishes to implement security measures that are deemed necessary and appropriate for the respective application or use. This extends to confidentiality (protection from unauthorised access), integrity (protection from manipulation), authenticity (protection from persons claiming false identities / origins) and availability (protection from the failure of IT systems) of communications.

In order to promote the straightforwardness of electronic legal and commercial transactions, uniform standards are to be used.

The measures comprise

- the application-based nationwide use of electronic signatures based on qualified certificates that provide a basis for the "BundOnline2005" e-government initiative,
- the nationwide use of IT baseline security for electronic communications at workstations, unless measures have been taken to guarantee a higher level of security, and
- safeguarding maximum economic efficiency by ensuring public authorities have adequate, applications-based security and equipment on the basis of uniform standards, in particular ISIS-MTT (Industrial Signature Interoperability Specification (MailTrusT).)

1.
Communications between the federal administration and its communications partners

The federal administration will provide security measures for e-government in its own applications and in doing so will take the security requirements of its communications partners into consideration.

In order to do so, it will

1.1. affix an electronic signature based on qualified certificates to documents if this is deemed necessary or appropriate by virtue of formal requirements (legal validity) or applications,

1.2. make it possible to check e-mails by allocating a sender ID, encrypting them in order to safeguard integrity and authenticity on the basis of well-known systems, once the addressee presents his or her certificate bearing their public signature key,

1.3. provide authentication and encryption mechanisms in respect of online transaction services in order to confirm the identity of persons signing electronically and to protect confidentiality and

1.4. implement standard security measures in order to safeguard the availability of its applications.

The federal administration will ensure that it provides its communications partners with verification software used to check the legal validity, integrity and authenticity of the federal administration’s communications free of charge.

2.
Communications with the administration

The communications partners of the federal administration will be required to provide sufficiently secure, user-friendly and cost-effective systems for their communications with the federal administration. The Federal Government has defined this requirement. In doing so, it will be at the discretion of the communications partners within the scope of legal requirements what means they employ to ensure communications are secure.

The federal administration will

2.1. accept electronic signatures and sender codes of its communications partners used to check the legal validity, integrity and authenticity of documents, provided they safeguard sufficient applications-based security and the electronic document transmitted can be processed by the respective authorities,

2.2. provide its certificates bearing the public signature keys for encrypting e-mails (in order to safeguard confidentiality) and

2.3. encrypt the data of its communication partners in online transactions.

II.
Reasons and explanations on implementation

1.
General information

The decision is intended in particular to promote legally binding and secure electronic legal and commercial transactions (e-government) between the federal administration and its partners (citizens, businesses, administrations):

- By using electronic signatures based on a qualified certificate in the administration and with its communications partners, it will be possible to ascertain the legal validity of signed electronic documents in respect of applications, thereby enhancing the conclusive force of a wide range of other documents.

- IT basic protection in e-commerce (confidentiality, integrity, authenticity) shall be safeguarded in particular by the issuing of certificates used to secure e-mail transactions and online transactions.

- The creation of suitable general conditions, in particular, the widespread use of uniform standards and the elimination of technical, administrative and any other barriers is intended to foster the straightforwardness of electronic legal and commercial transactions.

Security measures are an important prerequisite for implementing the BundOnline 2005 programme within the scope of which all online-capable services of the federal administration are to be made available on the Internet by 2005. The Federal Government will take the necessary steps to implement signature and encryption systems in the administration of the implementation plan. Signatures, authentication and encryption will have to be integrated into numerous applications, including systems used to process forms and procedures.

Against the backdrop of the current threat situation in the aftermath of the suicide attacks of 11 September 2001, it would also appear to be appropriate to ensure the comprehensive security of electronic legal and commercial transactions.

The standard of applications-based, adequate security will ensure greatest possible economic efficiency.

2.
Legal framework

With the amended version of the Digital Signature Act (Signaturgesetz) and new legislation to adapt formal requirements rendering certified, digital signatures equivalent to handwritten signatures under private law and public law, the Federal Government is seeking to gain support for the widespread use of electronic signatures.

a) Signature Act and Signature Ordinance

Germany took on a leading role by international standards when it adopted the Digital Signature Act in 1997. The Act provided important impetus for Directive 1999/93/EC of 13. December 1999 providing a Community framework for electronic signatures (hereinafter referred to as *Directive*).
The new "Act governing the Framework of Digital Signatures" (Signaturgesetz – SigG)" of 16 May 2001 (Federal Law Gazette I p. 876) entered into force on 22 May 2001, the Signature Ordinance of 16 November 2001 (Federal Law Gazette I p. 3074) entered into force on 22 November 2001. The amended legal provisions implement the Directive, taking the evaluation results of the Digital Signature Act of 1997 into account at the same time.

b) Recognition of the electronic form in private and public law

The Act on the Adjustment of Formal Requirements under Private Law and other Requirements to be met by modern Legal Transactions (Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr) of 13 July 2001 (Federal Law Gazette I p. 1542) entered into force on 1 August 2001, creating the basis for the introduction of the electronic form in private law. The new provision set forth in Article 126a of the German Civil Code, recognises electronic signatures as an alternative to handwritten signatures.

The 3rd Act amending Administrative Regulations adopted by the Federal Government (3. Gesetz zur Änderung verwaltungsverfahrensrechtlicher Vorschriften des Bundes) (Administrative Procedure Act, Social Code, Book X and the Fiscal Code) is currently in the pipeline. They are intended to facilitate the legal validity of e-commerce in administrative procedure to the greatest possible extent. Comparable regulations are to be issued in the administrative procedure laws of the Federal Länder.

These laws stipulate that the written form can be replaced by electronic signatures based on qualified certificates. All forms of electronic communications can continue being used for applications that do not have any formal requirements.

3.
Implementation in the federal administration

a) Communications between the federal administration and its communications partners

Re 1.1. of the decision:
The federal administration shall affix digital signatures based on qualified certificates to documents, if this is deemed necessary or appropriate due to formal requirements (legal validity) or for an application.

Electronic signatures that are based on qualified certificates will be used nationwide for e-government applications requiring the written form. The technical prerequisites have been created, with a high level of security being provided on the basis of chipcards re-

flecting the state of the art. While the BundOnline 2005 initiative is being implemented, the officials involved will be provided with chipcard-based cryptographic keys and relevant certificates. Their workstations will be equipped with the necessary infrastructure, in particular chipcard reading devices. This means certified signatures will be implemented in relevant e-government applications. As a rule, a **document**, i.e. a file will be signed (and, if necessary, be sent as an attachment to an e-mail).

Certificates and facilities for signatures based on a qualified certificate will be procured on the market. Software that, if necessary, supports the various standards will generally be provided for the verification of signed documents.

The Federal Government welcomes that certification-service-providers will provide signature products and services on the basis of voluntary accreditation schemes that have been proven to meet high requirements placed on signatures and the certificate on which they are based, particularly with regard to

- their permanent review and
- their technical and administrative security

and at the same time guaranteeing their interoperability. A decision whether electronic signature based on qualified certificates with service provider accreditation will be taken based on the relevant applications.

Re 1.2. of the decision:
The federal administration will allocate a sender code to e-mails in order to safeguard their integrity and authenticity and encrypt them on the basis of widely- known systems in order to safeguard their confidentiality if the addressee gives access to his or her certificate bearing a public signature key.

E-mail is of paramount importance for e-government due to its nationwide availability. There are applications that do not have any specific formal requirements, such as informal or form-free administrative transactions that can be handled by e-mail . At the same time, e-mail is a transport medium for signed documents. That is why IT security measures need to be taken (baseline protection).

The aim is to introduce security systems for e-mail (confidentiality, integrity and authenticity) in the federal administration nationwide by the end of 2003, starting on the basis of MailTrusT V.2 (MTT) standards, with the aim of converting to ISIS-MTT by the end of 2003. The cryptographic keys can be provided on the basis of software or chipcards. The authorities decide which basis is to be used depending on market developments (standards, prices) and demand (introduction of digital official identification documents, increased electronic implementation of applications that have specific formal requirements), safeguarding economic efficiency. Any such decisions can be taken once the certificates have expired, usually three years after review, based on the experience gained and on recent trends. Software is generally provided for the verification of securely transmitted e-mails.

The federal administration encrypts e-mails being sent to its communications partners using S/MIME, provided it has access to their public signature keys using X.509v3 certificates. Other standards will be supported, as required.

Re 1.3. of the decision:
The federal administration will provide authentication and encryption mechanisms for secure identification purposes and for safeguarding confidentiality in respect of online transaction services.

As a rule, many e-government applications are provided as web-based, online transaction services between a public authority's server and the communication partner's client. As such, authentication and encryption are implemented by the respective server based on applications.

Re 1.4. of the decision:
The federal administration will implement standard security measures in order to safeguard the availability of its applications.

In addition to specific IT basic measures for safeguarding communications, standard security measures will be taken, if necessary, in accordance with the IT Basic Security Manual.

b) Communications with the federal administration

Re 2.1. of the decision:
The federal administration will accept electronic signatures and sender IDs of its communications partners in order to check the legal validity, integrity and authenticity provided that they safeguard sufficient applications-based security and that the electronic document transmitted is suitable for processing by the relevant authorities.

The federal authorities shall provide software that will facilitate the verification of signatures according to different standards.

Re 2.2. of the decision:
The federal administration will provide its certificates bearing the public signature key used to encrypt e-mail (protection of confidentiality).

In order to support as many encryption programmes as possible, the federal administration will provide the public signature keys using X.509v3 certificates so that communications partners can send e-mails encrypted with S/MIME.

c) Accompanying measures

(1) Security culture

The Federal Government is fostering the development of a "security culture". Both citizens and public officials are called up to become accustomed to the new terms and procedures, to comprehend their purpose and to learn how to use them correctly.

(2) Interoperability

Standards will be required for communications using digital signatures and encryption between communication partners who have heterogeneous facilities, which

- safeguard interoperability between the various software and hardware products (horizontal interoperability) and
- safeguard interoperability between advanced and qualified signatures (vertical interoperability).

In order to foster efficient use amongst the public authorities of the Federal Government, workstations are to be equipped with an interoperable technical solution that facilitates all types of electronic communication between the federal administration and its communications partners.

The Industrial Signature Interoperability Specification (ISIS) provides for secure processes between the bodies of a certification infrastructure. Standard MailTrusT V2 (MTT) including relevant software products (horizontal interoperability) are available on the market for the secure, interoperable exchange of e-mails.

The Federal Government welcomes the activities undertaken by industry (“Trust Centre“ task force of the Trust Centre Operator T7 e. V. and the “MailTrusT“ task force of the association of manufacturers and users TeleTrusT Deutschland e. V.) for the introduction of the uniform “ISIS-MTT“ interoperability standard. The first specifications have already been presented. The Federal Government supports this work in order to ensure that ISIS-MTT can be used in applications as soon as possible. ISIS-MTT is based on the global S/MIME and X.509V3 standards and facilitates the introduction of a wide range of products which can be used for various platforms and applications, if necessary, after supplementing specifications for attribute certificates and document signatures.

The federal administration anticipates that the interoperability standard ISIS-MTT will establish itself quickly on the market and that suitable products based on the ISIS-MITT standard will be available for the respective applications. Once this has been established, it will make comprehensive use of ISIS-MTT in its invitations to tender.

The Federal Government supports the harmonisation and interoperability of electronic signatures called for by the Federal Government within the Single European Market as well as the creation of secure and reliable systems at global level that meet market requirements.

(3) Certification infrastructures (PKI)

Under the Digital Signature Act, the Regulatory Authority for Telecommunications and Posts is responsible for certifying the public signature keys of accredited certification-service-providers. It is also responsible for supervising all providers of certificates for qualified electronic signatures.

In order to safeguard communications security based on basic IT protective measures (e-mail security in particular) in public administrations in Germany, the administrative PKI was established. It ensures that security and interoperability standards are adhered to, for so-called technical signatures too (server-to-server communications). Following a decision taken by the Co-operation Committee ADP Federal Government/Federal Länder/local government, the Federal Länder and local authorities have also been involved in the administrative PKI. This creates a basis for basic IT protection aimed at safeguarding communications of the public administration in Germany.

The Federal Government fosters the development of certification infrastructures (Public Key Infrastructure - PKI) for signatures, authentication and encryption with the aim of giving participants access to certificates and making it easy to check certificates.

All private certification-service-providers will be able to issue certificates that meet the respective requirements within the complementary certification infrastructure that will be required for the time being because of the various tasks that need to be performed. This means public authorities will be able to obtain certificates for qualified signatures , safeguarding the communications security of **one** certification agency in the market.

The concept of having a Bridge Certification Authority (Bridge-CA), an initiative launched by industry and public authorities to link various certification infrastructures, will facilitate communications beyond administrative and corporate frontiers. Alongside the Digital Signature Act and the availability of interoperable products, this is an important step towards creating a national and international, interoperable certification and security infrastructure and towards the success of electronic legal and commercial transactions.

The directory service provided in the Berlin-Bonn Information Network (IVBB) will be expanded to encompass a directory of all public officials in order to facilitate the exchange of e-mails between administrative authorities. It will be linked to the directories of the Federal Länder and local government.

(4) Organisation

Applications used for signatures, authentication and encryption will be incorporated into the organisational processes of all public authorities, in particular

- the role of the registration agency that establishes the identity of public officials and verifies their identity to the certification agency looking after public officials in respect of security issues,
- the IT administration that installs, tests and operates the programmes and, if necessary, the chipcard reading devices and looks after the public officials regarding IT queries and
- the necessary training.

Certification services (Trust Centre services) for qualified, electronic signatures and communications security will be procured on the market, as a rule. The certification-service-providers ensure that security and interoperability requirements are met. They

also issue certificates in directories to facilitate communications with participants within their own and other certification infrastructures.

(5) Providing basic components

The Federal Ministry of the Interior (BMI) is looking into the need for a “virtual postal agency“. The aim is to establish the legal and actual possibility of taking over tasks in electronic legal and business transactions, in particular, looking into the tasks associated with encryption and decoding, signature checking and forming, virus checking, filing and time stamping. These tasks could be supported centrally by a “virtual postal agency“ for a public authority, at the same time supporting the standards used by the communications partners. To this end, the Federal Ministry of the Interior will make use of the experience gained with the MEDIA@Komm approach “Online Services Computer Interface (OSCI)“ for online transactions based on electronic signatures. If necessary, the Federal Ministry of the Interior will provide the federal authorities with a virtual postal agency.

The Federal Ministry of the Interior will provide the communications partners of the federal administration with verification software that is used to check the legal validity, integrity and authenticity of the federal administration’s communications.

The Federal Ministry of the Interior will provide information on individual topics with a view to introducing electronic signatures, authentication and encryption devices to the federal administration

4.
Costs

The introduction of digital signatures and encryption will incur introduction costs (hard- and software) and current costs (maintenance, certification-provider-services). These non-recurrent and annual costs and the costs incurred by the development and maintenance of basic components (verification software) will be provided centrally and decentrally in accordance with the decision taken by the Federal Cabinet regarding the implementation scheme for the BundOnline 2005 e-government initiative of 14 November 2001.

The following costs are estimated to be incurred in addition to the funds already earmarked for pilot projects at the individual public authorities:

- *Installing the relevant equipment in what has been estimated to be around 20,000 workstations of the immediate federal administration during the initial phase as a priority task, at which electronic signatures based on qualified certificates will be required to configure e-government applications: approx. €60 , per annum approximately. €20 – €40 per workstation,*

- *Providing around 200,000 workstations with e-mail security products at the non-recurrent cost of around €10 and a further €10 per annum for workstation programmes ("plug-ins") and services provided by certification-service-providers,*

- *Creating the general organisational conditions at public authorities, in particular, the establishment of registration agencies and introduction expenses of approx. €30,000 per public authority,*

- *Installing chipcard reading devices on other PCs within the framework of procurement on a rota basis at the cost of approx. €15 per PC,*

- *Personnel costs for 1 staff member (higher intermediate service) per 1,000 public officials in addition to personnel expenditure incurred during the introduction phase,*

- *Training costs.*

The total costs incurred by the introduction of signature, authentication and encryption systems for electronic legal and commercial transactions are outlined in the total sum of the financial estimate in accordance with the BundOnline 2005 implementation scheme.

The capital expenditure is juxtaposed with enhanced security and the promotion of business. It is anticipated that by organising processes more efficiently, for instance, by using qualified, electronic signatures, by making greater use of e-mail and by processing files more efficiently by introducing e-government applications within the BundOnline 2005 government initiative, significant use will be made of rationalisation and savings potential.

The costs incurred today, for instance, for chipcard reading devices and certification-provider-services are likely to drop considerably as a result of the widespread introduction of relevant systems.

5.
Co-operation, publicity work

From the Federal Government's perspective, digital signatures can only be introduced successfully if industry is involved in every aspect. The Federal Government is therefore giving manufacturers and associations the opportunity to engage in comprehensive co-operation.

A task force involving several ministries under the leadership of the Federal Ministry of the Interior and the Federal Ministry of Economics will co-ordinate the next steps that need to be taken by the Federal Government and in doing so, will co-operate closely with the Federal Länder and communes as well as with other users, manufacturers and associations.

The Federal Government will support the introduction of electronic signatures by launching an extensive publicity campaign.