Practical Experiences implementing a Scheme for Digital Signature

Panel-Chair:
K. J. KEUS, Bundesamt für Sicherheit in der Informationstechnik (BSI/GISA), Germany
keus@bsi.de

Panelists:
Dr. O.E. Liebetrau, Bundesamt für Sicherheit in der Informationstechnik, Germany, Lbt@bsi.de
Dr. H.R. Baader, debis IT-Security Services, Germany, hr-baader@itsec-debis.de
Dr. E.-H. Gruschwitz, TUEV Information Technology GmbH, Germany,
E.Gruschwitz@tuvit.cubis.de
P. Mertes, Deutsche Telekom AG, Germany, Paul.Mertes@telekom.de

Abstract

This panel deals with the practical experiences installing and driving a digital signature scheme. Currently Germany has defined and implemented a bill in respect to establish uniform economic conditions for the various applications of electronic information and confirmation services, parts tailored for the application of digital signatures. The involved parties of the scheme present their practical experiences based on the implementation and the application of the German approach.

A general overview over the structure of the German digital signature scheme is given by the representative of the German government (BSI/GISA). Based on a short presentation of the bill, the related ordinance and the transformation into detail requirements expressed in a handbook, published by BSI, he will address the aim and the focus of the law and the underlying intentions, expressed in the dual approach by the binding of governmental and commercial oriented private parties to one common commercial oriented scheme. The general requirements and conditions are presented in respect to the national legal aspects and the problem dealing with international recognition of certificates will be touched.

The representative of the Certification Authority (CA) will present the first experiences installing and offering a scheme in conformity with the requirements defined by the law and the ordinance from his special view. He will talk about the commercial issues of a digital signature scheme and will give first impressions from his view, dealing with problems such as the responsibilities for the CA and its liability problems. The different services offered by a German CA will be addressed. A distinction will be made between such services as the Registration Service by a Registration Authority (RA), the Key-Generation, the Issuing of the Certificate, the Issuing of Smart Cards, the Directory Service, the Certification Revocation List Service (CRL), the Time Stamp Service. The mandatory services will be separated from the voluntary ones and such services which should be excluded for a German CA.

The requirements for the technical infrastructure including the requirements for the technical components, the requirements dealing with organizational, procedural and technical issues expressed in a Security Policy (SP) of a CA and the evaluation / certification of all these issues will be presented by accredited and licensed CLEFS (commercial licensed evaluation facility). The representatives address the detail requirements for the components itself and will talk about the requirements for its underlying ITSEC evaluation / certification of the components and products for digital signature. They will present the experiences dealing with their evaluation / certification activities of the security policy of a CA.

The German digital Signature Bill: practical and technical Implications

Dr. O.E. Liebetrau, Bundesamt für Sicherheit in der Informationstechnik, Bonn, Germany

A general overview over the German digital signature scheme will be given. Based on a presentation of the bill and its underlying intentions as well as the more detailed security requirements as expressed in the related ordinance the transformation of these requirements to safeguard catalogues will be addressed.
Those cover security measures for the organizational structure of certification authorities, for technical components used for key generation, key storage and signature generation and verification, and sound mathematical principles.
Further the general (technical, policy, legal) problem of international recognition of certificates will be touched.

A Certification Authority's Position and Statement

P. Mertes, Deutsche Telekom AG, Siegen, Germany

As for the overall content of the German Digital Signature Act (GDSA), Deutsche Telekom very much supports the Act in its present form. The GDSA offers a framework supporting secure on-line transactions which in turn is necessary to further foster the implementation of electronic commerce in a legally recognized environment. Digital Signatures in principle make it possible to the recipient of on-line data to determine the origin of the data (identity) and to verify whether these data have been altered (integrity). Not only from a legal point of view, these advantages are vanishing away if the infrastructure used for digital signatures is focussing more on minimal security standards than on ensuring a satisfactory proof of the aforementioned key issues 'identity' and 'integrity'. Nevertheless, a Digital Signature Act should not prohibit the use of digital signatures generated and managed in a less secure framework. Instead, a Digital Signature Act should use an enabling approach, offering a framework with maximum security standards open to everybody, not touching other possible public key infrastructures. It is then up to the market as well as to the judges and legislators to decide which system meets there needs best. This is a truly market driven approach and this is the GDSA approach.

Evaluation and Confirmation of Products and Security Concepts: Requirements, Problems and Solutions:

Evaluation and confirmation of smart cards for digital signatures - special facets in the debis spectrum of SigG/V-specific services

Dr. H. R. Baader, debis IT-Security Services, Bonn, Germany

After a short presentation of the company 's (debis) organizational embedding into the Daimler-Benz group and of the portfolio of services conformable with SigG/V a survey of prerequisites for the technical infrastructure is given - deducible from the synoptic approach of SigG/V (consideration not only of juridical aspects). These prerequisites comprise confirmed technical components with specific evaluated security properties as well as licensed evaluation and confirmation facilities with regard to such components eminently represented by smart cards.
Task and work of the debis evaluation and confirmation facilities for components are exemplified for a (general) SigG/V-conformable smart card comprising hard-, software and especially

cryptographic features. The focal activities concern the fulfillment of the specific requirements addressed explicitly (on "E4 high" evaluation level according to the ITSEC which is comparable to EAL 5 of the CC). The essential smart card functionalities - the security of which, i.e. their trustworthiness with respect to development, implementation and operational aspects must be investigated and confirmed in this context - are the asymmetric key generation (if applicable), the storage of the (generated or loaded) private key without any read-out possibility and the generation of a digital signature string.

Examination and Confirmation Bodies in the German Digital Signature Act

Dr. Ernst-Hermann Gruschwitz, TÜV Information Technology GmbH, Essen, Germany

The German Digital Signature Act installs certification authorities as trust centers, that issue signature keys for the purpose of signing digital data to natural persons acting as individuals or in representation of their companies. These trust centers confirm the assignment of a public signature key to a natural person by means of a digital certificate. The certification authority (trust center) also upon request affixes a time stamp to a digital document.

To guarantee the reliability and the secure operation of a certification authority the German Digital Signature Act requests the implementation of a security concept that is checked and confirmed by a recognized body.

For handling the processes of generation and storage of signature keys, the presentation of data to be signed, the verification of signed data and the management of signature key certificates technical components with safeguards have to be used. These technical components shall be adequately tested against standards and their compliance with the requirements has to be confirmed by a recognized body.

In this presentation the requirements of the German Digital Signature Act that have to be fulfilled by a certification authority are shown with regard to the confirmation process. The security concept and the confirmed technical components to be used by the certification authority are described.

Over and above that the operation of such an examination and confirmation body and the interdependence between the competent authority, these recognized bodies and the certification authorities is discussed.

Panel Chair:

K. J. KEUS,
Bundesamt für Sicherheit in der Informationstechnik
P.o.box: 200363
D-53133 BONN
Phone / Fax: +49 228 9582-141 , -455
Email: keus@bsi.de

Panelists:

Dr. O.E. Liebetrau,
Bundesamt für Sicherheit in der Informationstechnik
P.o.box: 200363,
D-53133 BONN, Germany
Phone / Fax: +49 228 9582-646 , -750
Email: lbt@bsi.de

Dr. H.R. Baader,
debis IT-Security Services
Rabinstr. 8
D-53111 BONN, Germany,
Phone / Fax: +49 228 9841-118 , -598
Email: hr-baader@itsec-debis.de

Dr. E.-H. Gruschwitz,
TUEV Information Technology GmbH,
Im Teelbruch 122
D- 45219 Essen/Kettwig, Germany,
Phone / Fax: +49 201 825-5110, -2464
Email: E.Gruschwitz@tuvit.cubis.de

P. Mertes,
Deutsche Telekom AG,
Produktbereich TELESEC
P.o.Box 1465
D-57238 Nethpen, Germany,
Phone / Fax: +49 271 708-1610, - 1625
Email: Paul.Mertes@telekom.de