

DFN - PCA
The World Wide Web Policy

Certification guidelines for the PCA project

As of 1 April 1999

Version: 1.0 (FINAL VERSION)

DFN-PCA
Stefan Kelm
Britta Liedtke
Universität Hamburg
Fachbereich Informatik
Vogt-Kölln-Straße 30
22527 Hamburg

Contents

1 Introduction

2 Identity of the PCA

3 Sphere of responsibility of the PCA

- 3.1 Legal significance
- 3.2 The DFN certification hierarchy
- 3.3 Registration authorities (RAs)

4 Security of the PCA equipment

- 4.1 Security requirements for the DFN-PCA
- 4.2 Security requirements for CAs
- 4.3 Security requirements for RAs
- 4.4 Security requirements for end users

5 Certification rules

- 5.1 Rules for the certification of CAs
- 5.2 Rules for the certification of RAs
- 5.3 Rules for the certification of end users
- 5.4 Rules for the cross certification of two PCAs/CAs

6 Management of certificates

7 Revocation of certificates

8 Rules for naming

- 8.1 Choice of a name for CAs
- 8.2 Choice of a name for RAs and end users

9 Miscellaneous

DFN - PCA: The World Wide Web Policy

Preliminary remarks

This is Version 1.0 of the World Wide Web Policy of the DFN-PCA. This version is valid until 31 December 2000 and follows the low-level policy version 1.2 of the DFN-PCA.

1. Introduction

This document contains the certification guidelines (the so-called "policy" or "certification practice statement", CPS) of the top-level certification authority of the *Verein zur Förderung eines Deutschen Forschungsnetzes e. V.* (DFN-PCA - Association for the Promotion of a German Research Network).

The statements made in this document are binding for the work of the DFN-PCA and of the CAs certified by the DFN-PCA, unless they contradict legal regulations. The DFN-PCA exclusively issues certificates according to the guidelines of this policy. In order to permit international cooperation with other CAs, an English translation is herewith published; at all events, however, the German version, as amended, shall prevail.

2 Identity of the PCA

Address

DFN-PCA

Universität Hamburg

FB Informatik - RZ

Vogt-Kölln-Str. 30

D - 22527 Hamburg

Telephone: +49 40 - 428 83 2262

Fax: +49 40 - 428 83 2241

E-mail addresses

certify@pca.dfn.de (for questions concerning certification)
dfnpca@pca.dfn.de (for general inquiries to the DFN-PCA)
s=dfnpca;ou=pca;p=dfn;a=d400;c=de (X.400)

Information services of the DFN-PCA

FTP server : <ftp://ftp.pca.dfn.de/pub/pca/>
WWW server: <http://www.pca.dfn.de/dfnpca/>

Validity of this document

1 April 1999 to 31 December 2000

Version of this document

1.0

3 Scope of the PCA

The DFN-PCA's sphere of responsibility comprises all member institutions of the DFN Association, i.e. primarily natural as well as legal persons under public or private law from science and research. Other organizations and users can be certified upon request.

The DFN-PCA will exclusively issue certificates for CAs and not for end users. The DFN-PCA will additionally offer the services of one or more subordinate CAs so as to be able to issue certificates for end users whose organizations do not yet operate CAs of their own.

This policy supports especially the X.509v3 certificate format used in current standard browsers for different applications (SSL and S/MIME or code signing).

3.1 Legal significance

A certification by the DFN-PCA (or subordinate CAs) does not entail any legal significance; there is no legal claim to have a certificate issued by the DFN-PCA or subordinate CAs. Especially the general legal relevance of digital signatures is currently unclear. The purpose of a DFN-wide public key infrastructure is the creation of the technical prerequisites for secure electronic communications. In particular, the DFN Association, the University of Hamburg as well as the DFN-PCA's project staff do not assume any form of warranty. All tasks are performed by the project staff to the best of their knowledge and belief.

The requirements for technical components and procedures for certification underlying this policy do not currently conform to the Digital Signature Act.

3.2 The DFN certification hierarchy

The certification hierarchy below the DFN-PCA consists of three different units (certificate holders):

- certification authorities (CAs)
- registration authorities (RAs, see 3.3)
- end users:
 - WWW servers
 - users (client certificates for SSL, S/MIME, code signing)

The international linkage of the DFN certification hierarchy to other hierarchies can be achieved by mutual certification (cross certification, see section 5.4) of the DFN-PCA with other PCAs or incorporation of the DFN-PCA in European certification hierarchies.

CAs operating below the DFN-PCA on their part have the opportunity of establishing links of their own to certification authorities and infrastructures of organizations not

members of the DFN Association by cross certification with other CAs (see section 5.4).

The public key of the DFN-PCA is contained in a self-signed certificate (root certificate) issued by the DFN-PCA. All users of the infrastructure receive this root certificate in the course of their own certification and can thus verify the authenticity and validity of all certificates issued below the DFN-PCA level.

Anonymous or pseudonymous certificates can be issued for users, but not for CAs if they can be identified as such.

3.3 Registration authorities (RAs)

All CAs have the possibility of nominating trustworthy registration authorities (RAs) for the local verification (registration) of the identity and authenticity of individual end users. RAs may only be used for the registration and verification of end users, but not of CAs.

An RA is a user certified in the usual manner by a CA, in order to undertake on behalf of its CA the verification of other end users prior to their certification by the CA.

An RA may neither generate asymmetric key pairs for other users nor can it issue or revoke certificates itself. After having verified the identity of the end user in a suitable manner (see chapter 5), the RA passes the certificate signing request (CSR) of an end user on to the CA. The registered data may be transmitted by personal delivery to the CA or by electronic communication. In order to preclude any misuse, every electronic transmission to the CA must be digitally signed by the RA.

In those cases in which the key generation is not performed by the end user himself, the RA only passes the end user's identity information on to the CA. If a CA receives an end user's certificate signing request from a trustworthy RA, it always has to verify the validity of the RA signature if the registered data were transmitted electronically.

The new certificate issued by the CA is then transmitted to both the RA and the end user.

Each CA can nominate any number of persons as RAs. The CA can request the signature of an agreement which binds the RA to certain guidelines fixed by the CA. In particular, the RA should comply with the security requirements according to section 4.3. Each CA should publish these guidelines together with a list of all RAs it has nominated.

4. Security of the PCA equipment

Due to the participation in a public key infrastructure, specific requirements with respect to the security of the hard- and software used, on the one hand, and to the reliable handling of cryptographic keys, on the other hand, will arise for all users. The requirements for the DFN-PCA and the CAs are naturally higher since the misuse of a PCA/CA key would withdraw trustworthiness from all subordinate certificates.

4.1 Security requirements for the DFN-PCA

The following demands are made on the DFN-PCA:

- For the services of the DFN-PCA a dedicated computer is used which has no connection to a computer network. Certificates are exclusively generated off line on the dedicated computer.
- Any data exchange with networked computers will be performed by the DFN-PCA's staff using external data carriers (e.g. floppy disk or magnetic tape); data processing is not automated. All media containing keys are stored in a safe location if they are not in use.
- Secret keys of the DFN-PCA for the generation of digital signatures are exclusively generated and used by the staff on the dedicated computer and

stored on external peripherals (e.g. smart card, removable hard disk, floppy disk) as far as this is supported by hard- and software. Access to these peripherals is protected by nontrivial passwords (minimum length: 8 characters) or PINs which are only known to the project staff and are never stored as plain text or sent through unprotected network connections. The peripherals are not used on other computers.

- Secret PCA signature keys are exclusively used to sign CA keys and certificate revocation lists (CRLs) or to issue cross certificates. Secret signature keys are not used for any standard communications; the DFN-PCA therefore uses different asymmetric key pairs for signing and decoding.
- Asymmetric key pairs of the DFN-PCA for the generation of signatures have a minimum length of 2048 bits RSA (or a comparable level).
- The integrity of all relevant data and programs on DFN-PCA computers is regularly verified with the aid of cryptographic applications. Furthermore, all data are treated confidentially by the project staff; all legal data protection regulations in force are complied with.
- A data backup is performed for all relevant (electronic) DFN-PCA data at regular short intervals; the respective data carriers are stored at an external site. This data backup is based on a suitable backup concept for the DFN-PCA which, in particular, is intended to permit long storage times for certificates and CRLs.

4.2 Security requirements for CAs

The following demands are made on all certified CAs below the DFN-PCA:

- For the services of the CA a computer must be used which is adequately protected against misuse. Unauthorized access to the CA computer and to any possibly stored key data must be prevented by the use of suitable hard- and software. In particular, it is recommended that a computer without any network

connection should be used and physically protected.

- Secret CA keys for the generation of digital signatures must be adequately protected against misuse by unauthorized persons and must not be disclosed. Responsibility is with the CA administrators who are urged to use external peripherals (e.g. smart card, removable hard disk, floppy disk) for protecting the secret CA keys. Access to these secret CA keys must in any case be protected by nontrivial passwords (minimum length: 8 characters) or PINs which may only be known to the CA administrators and must never be filed as plain text or sent through unprotected network connections. The external peripherals must not be used on other computers.
- The secret CA signature keys may be exclusively used to sign CA or end user keys and certificate revocation lists (CRLs) or to issue cross certificates. The secret signature key must not be used for any standard communication.
- Each CA must in principle generate its own asymmetric key pairs; no key generation is performed by the DFN-CA or other CAs.
- Asymmetric CA key pairs for the generation of signatures must have a minimum length of 1024 bits RSA (or a comparable level); however, considerably longer key lengths are recommended.
- In those cases where a CA generates asymmetric key pairs for the end users, the CA must perform this on the dedicated CA computer. Furthermore, it must be ensured that all copies of the end user's secret key are definitely deleted on the part of the CA after certification and handing the key over to the end user. The CA must in no case store, deposit or disclose to third parties secret keys or parts of the end user's secret key after handing over the keys. The process of deleting a secret key must be documented in a suitable manner.
- All data produced in connection with a certification must be treated confidentially by the CA staff. The legal data protection regulations applicable to the CA must be complied with.

The security requirements for CAs described in this section are equally valid for CAs directly operated by the DFN-PCA staff and certified by the DFN-PCA. However, these CAs never generate asymmetric key pairs for other end users.

4.3 Security requirements for RAs

The following demands are made on the RAs instituted by a CA:

- For the services of the RAs a computer must be used which is adequately protected against misuse. Unauthorized access to the RA computer and any possibly stored keys must be prevented.
- Secret keys of the RAs for the generation of digital signatures must be adequately protected against misuse by unauthorized persons and may not be disclosed. If no smart cards or other peripherals are used for the storage of secret keys, access to secret keys must be protected by nontrivial passwords (minimum length: 8 characters) or PINs. Neither the optional peripheral nor a password or PIN may be passed on to other persons. Password and PIN must never be stored as plain text or sent through unprotected network connections.
- Asymmetric key pairs of the RAs for the generation of signatures must have a minimum length of 1024 bits RSA (or a comparable level).
- Further requirements may be stipulated by the CA responsible for the RAs.

4.4 Security requirements for end users

The end user's secret key must be adequately protected against misuse by unauthorized persons and may not be disclosed; each end user is himself responsible for this.

If no external peripheral (e.g. floppy disk) is used for storing the secret key, access to an end user's secret key should be protected by setting a nontrivial password (minimum length: 8 characters) or a PIN. Neither the optional peripheral nor the password or PIN may be disclosed to other persons. Password or PIN must never be stored as plain text or sent through unprotected network connections.

Security requirements for users (SSL, S/MIME, code signing)

Users in terms of this policy are individual persons.

- A user's asymmetric key pair must have a minimum length of 512 bits RSA (or a comparable level). The choice of longer key lengths is urgently recommended and depends on technical availability.
- The user must protect access to his secret key by setting a nontrivial password provided that the application used supports this.
- The directory or files in which the cryptographic keys are stored by the application must be protected by the user against unauthorized misuse as far as possible. This can be achieved, for example, by setting specific rights of access provided that this is supported by the operating system used. The storage of cryptographic keys on external data carriers (e.g. floppy disk) is urgently recommended.

Security requirements for WWW servers

- The asymmetric key pair for WWW servers must have a minimum length of 1024 bits RSA (or a comparable level).
- Since the secret key is normally unlocked for the first time when starting the WWW server (e.g. by entering a nontrivial password), the server computer with the corresponding files and directories must be protected by suitable (also physical) measures against misuse. This should be achieved, in particular, by setting appropriate rights of access. Storage of the cryptographic keys on external data carriers (e.g. floppy disk) is urgently recommended.

5 Certification rules

This section describes technical and organizational guidelines and procedures to be observed prior to a certification of CAs or end users.

CAs as well as end users are given distinguished names whose correct choice is of particular significance. The choice of these names is described in section 8.

In order to identify illegal certificate signing requests, the certifying authority (CA or PCA) must convince itself of the identity of the key holder requesting certification in a suitable manner by technical and organizational measures prior to each certification. In this connection, the CA can also demand a proof of possession of the corresponding secret key from the key holder prior to a certification. This may be done, for example, by exchanging digitally signed messages.

The registration process is only possible by personal contact - or in individual exceptional cases by phoning back personally well-known persons - prior to certification. If a CA employs RAs, the latter are responsible for identity checking, but the CA can nevertheless assume responsibility. In no case, however, may certificate signing requests be processed automatically.

Certificates are exclusively granted if the public key to be certified has the minimum length defined in section 4 and the certifying authority has duly convinced itself of the key holder's identity and the possession of the correct asymmetric key pair. The new certificate issued is transmitted to the certificate holder immediately after certification, for example, by e-mail or through a URL. The certificate holder is urged to immediately verify the correctness of his own certificate and of the higher-level CA certificates.

Each certificate must contain a serial number assigned by the certifying CA, and each CA must ensure in the certification process that no serial number has been assigned several times.

As a rule, certificates are not automatically extended by the issuing CA; applications for re-certification must be filed with the corresponding CA, if necessary.

Certificate extensions

X.509v3 certificates are characterized by the fact that each certificate may contain arbitrary extensions (certificate extensions). Moreover, each extension can be flagged as particularly significant by setting a particular bit (critical flag).

Certificate extensions are included in the certificate by the respective CA during certification; however, extensions can also be proposed in the certificate signing request (CSR).

Each CA should make known all extensions it has supported. In particular, a CA can limit the application of an issued certificate to certain functions (e.g. the signing of objects such as Java applets) by such extensions. CAs are urgently recommended to generate only certificates according to X.509v3 and to support widely used standard extensions (cf. X.509v3, PKIX, Netscape).

If a CA receives a certificate signing request with unknown certificate extensions, it should not issue a certificate.

5.1 Rules for the certification of CAs

CAs wishing to be certified by the DFN-PCA will sign an agreement with the DFN-PCA prior to certification. This agreement contains a declaration that the guidelines of this policy are accepted and the policy will be complied with during operation of a user's own CA. In particular, the CA administrators must comply with the security requirements according to section 4.2.

A person responsible for CA operation is entitled to sign this agreement. This authorization can be verified by the DFN-PCA prior to issuing a certificate.

The DFN-PCA reserves the right to verify CAs for their suitability as well as the existence of the technical prerequisites on site.

A CA generates its own asymmetric key pair and subsequently transmits the certificate signing request (CSR) to the DFN-PCA. This certificate signing request should be signed digitally for reasons of protection; the certifying CA must verify the digital signature prior to certification. The CSR can be transmitted to the CA by e-mail or by the exchange of a data carrier.

Prior to the certification of a CA, a staff member of the DFN-PCA verifies the CA administrator's identity, the affiliation of the CA administrator to the respective institution and, if necessary, its existence. This verification always requires a personal meeting between a CA administrator and a member of the DFN-PCA staff. For the process of verification it is necessary to present an identity card/passport or a comparable document.

The establishment of organization-wide sub-CA hierarchies is the responsibility of the top-level CA of a respective organization. For subordinate sub-CAs the rules of this section apply analogously. Any guidelines going beyond this policy may be defined, if required, by this CA in its own policy.

Certificates for CAs have a maximum validity of two years.

5.2 Rules for the certification of RAs

An RA certificate does not differ from a usual user certificate. For the certification of RAs, therefore, see the following section.

5.3 Rules for the certification of end users

End users wishing to be certified will first generate a personal asymmetric key pair and subsequently transmit the certificate signing request (CSR) to the RA or CA in charge. This certificate signing request should be signed digitally for reasons of protection; the certifying CA must verify the digital signature prior to certification. Where appropriate, the end user's asymmetric key pair can also be generated by the CA which must absolutely comply with the security requirements described in section 4.2.

Irrespective of the deployment of an RA, the end user must present himself personally to enable the CA (or RA) to verify his identity and the correct allocation of the information specified in the certificate to this end user (and, where applicable, the allocation of the identity to an alias). For the verification process it is necessary to present an identity card/passport or a comparable document. If the verification is made by an RA, the latter will pass the certificate signing request (CSR) received from the end user on to the competent CA (cf. section 3.3.).

Certificates for end users have a maximum validity of twelve months.

Additional rules for the certification of WWW servers

In addition to the above-described certification rules for end users, specific guidelines are valid for the certification of WWW servers not allocated to an individual but to a computer (name).

If WWW servers are to be certified, an administrator of this server must transmit the certificate signing request (CSR) to the certifying authority. The latter must verify in a suitable manner the unambiguity of the following information:

- affiliation of the server to a specific organization
- identity of the organization
- identity of the server administrator

5.4 Rules for the cross certification of two PCAs/CAs

To permit linkage to other certification hierarchies there is the possibility of cross certification with other CAs both for CAs and for the PCA. The process does not differ for PCAs and CAs.

Prior to a cross certification, the responsible CA administrators must make themselves familiar with the certification guidelines of the other CA. The process of cross certification means that the other CA's policy was known at the time of certification and that its current guidelines are accepted, but not that these guidelines must be in agreement with a CA's own policy. Cross certification thus always relates to a CA's currently valid policy; if this is changed fundamentally, a new cross certification is necessary.

The cross certification of a CA does not differ organizationally from the certification of an end user. A CA's public key or certificate is transmitted to the other CA by e-mail or by the exchange of a data carrier. Subsequently, the identities must be mutually verified to exclude illegal certificate signing requests. This process must take place at a personal meeting of the CA administrators.

After certification, the CA publishes the cross certificate issued which contains the public key of the other CA. A cross certificate should not be valid for a longer period than the regular certificate of the cross-certified CA.

6. Management of certificates

All users of the DFN certification hierarchies basically agree to the publication of their certificate. It is possible, however, to individually object to a publication in applying for a certificate.

Each CA (incl. the DFN-PCA) is responsible for the publication [hier bin ich nicht sicher was im Deutschen Text 'Bereitstellung' bedeuten soll. D. Erwin] of all certificates issued by that CA including both the CA's own and the higher-level CA certificates. New certificates and CLRs issued by a CA (see section 7) must be published within a reasonable period of time (normally within one working day).

For the provision of certificates each CA must establish information services (directories) whose task is to distribute certificates and CRLs. Suitable for this purpose are in particular WWW, FTP, e-mail, LDAP and X.500 servers whose data must be adequately protected against misuse. Such information services may be operated by the CA's partner institutions; in exceptional cases, the DFN-PCA will publish a CA's certificates and CRLs upon request.

7. Revocation of certificates

Each CA (incl. the DFN-PCA) can revoke certificates issued by it at any time prior to the expiry of validity without specifying explicit reasons. Causes for the revocation of a certification may be, for example, the discovery of improper actions by a CA administrator or failure to comply with individual guidelines of this policy. Other reasons may be a staff member leaving an institution or a change of name.

Each certificate holder can request the authority which has certified his public key to revoke a certificate issued for him without giving reasons. The CA concerned must comply with this request within a reasonable period of time as soon as it has convinced itself by taking suitable steps that the request has been made or authorized by the certificate holder himself. If a CA's own secret key is known to have

been misused or compromised, each user should immediately notify the certifying authority and initiate the revocation of his own certificate.

Certificates can only be revoked by the issuing authority. All revoked certificates are published by the responsible CA in a certificate revocation list (CRL) which must be made available to all users. This CRL contains the date of CRL issue (e.g. in the form of a time stamp) and is digitally signed by the CA. Revoked certificates remain in the CRL until the original validity period has been exceeded. Those certificates whose publication has been objected to during certification are also published in a CRL.

Certificates once revoked cannot be renewed or extended. However, each user basically has the possibility of applying for a new certificate.

Immediately after starting its own operation, each CA must issue a new (empty) CRL. Subsequently, new CRLs must be issued at regular intervals (e.g. monthly), even if no further certificates have been revoked by the CA in the meantime. It is recommended that old CRLs should be archived to enable verification of the validity of certificates even at a later date.

The DFN-PCA will publish a CRL at least once a month.

For the provision of CRLs, the CA must establish information services (directories) whose task is to distribute certificates and CRLs (cf. section 6). Since many software products at present only insufficiently support the processing of CRLs, each CA is urged to inform its certificate holders accordingly and, if possible, to implement solutions of its own for CRL distribution.

8 Rules for naming

All certificate holders are assigned a distinguished name (DN) to be used upon issuance of a certificate for a user as his subject name. A DN contains a sequence of uniquely identifying name attributes by which all the users of a hierarchy can be

referenced; unusual special characters (e.g. umlauts) within this name should not be used for reasons of interoperability.

The DNs of all certificate holders below the DFN-PCA level contain the attribute C=DE. Prior to certification, the correctness and unambiguity of the specified name is verified by the CA; no name may be assigned several times.

The name of each certificate holder should follow the scheme below:

```
C=DE,  
O=organization,  
[OU=<department>],  
[CN=<distinguished name>],  
[EMAIL=<e-mail address>]
```

Deviations from this scheme are only possible after prior agreement with the DFN-PCA.

Alternative names may be adopted in the certificate, if required, by certificate extensions. In this case, the certifying CA must verify the contents of these extensions for correctness prior to certification.

8.1. Choice of a name for CAs

Each CA directly certified by the DFN-PCA chooses its own name, which should directly reflect the affiliation to an organization.

The organization name ("O=") contains the name of the institution which is represented by the CA. One or more organizational units (departments, "OU=") may be specified; optionally, further attributes (e.g. "L=") can be included in the name.

A CA's valid e-mail address should be specified; the attribute "CN=" is optional for CAs but should be used for reasons of interoperability.

Each CA is responsible for the correct choice of name of the CAs and end users certified by it.

8.2 Choice of a name for RAs and end users

The choice of distinguished end user names is primarily governed by the guidelines of the certifying CA. RAs are subject to the same rules for naming as users.

The attribute "CN=" is obligatory for all end users and occurs precisely once. It contains the complete name of the user.

It is recommended to adopt a valid e-mail address via the attribute "EMAIL="; optionally, further attributes (e.g. "L=") can be included in the name.

If a name occurs several times within one organization, it is the CA's task to choose distinguished names by suitable name additions. The competent CA is furthermore responsible for checking the affiliation of the user to the institution concerned and for ensuring that all certified users have different names.

Additional rules for WWW servers

Certificates for WWW servers must contain a distinguished host name in the "CN=" attribute. This attribute must not contain wildcards nor any numerical IP addresses.

The optional attribute "EMAIL=" should contain a valid e-mail address, for example, that of the server administrator.

9 Miscellaneous

This document was drawn up in a DFN project at the University of Hamburg. No liability is assumed for the correctness, completeness or applicability of the information contained and the measures proposed. Furthermore, no liability can be assumed for possible damage arising from making use of the DFN-PCA services. The responsibility for using the above-described procedures and programs lies solely with the persons carrying out the installation.

The DFN-PCA reserves the right not to fulfil certificate signing requests. Furthermore, no guarantee can be assumed for the availability of the PCA services. On account of the status as a research project, there is at present no possibility of offering the DFN-PCA services on a 24-hour basis.

Documentation and data protection

All activities within the framework of this policy will be documented as far as technically feasible. All CAs and RAs must treat the data arising in certification as confidential and comply with the respective data protection guidelines.

All certificate holders agree to the storage and processing of their data arising in certification by the certifying authority.

Agreements between PCA and CA

A CA administrator wishing to be certified by the DFN-PCA must sign by hand an agreement with the DFN-PCA. This agreement primarily contains a declaration on compliance with the guidelines of this policy and can be obtained from the DFN-PCA.

Agreements between CA and RA

A CA may demand the signing of an agreement which binds the RA to specific guidelines. This agreement must be signed by hand by the person acting as the RA; it can be obtained from the competent CA.

Declaration by the users

All users of the DFN hierarchy must sign a declaration by hand prior to certification, informing them about their rights and duties and about the risks and dangers in the employment of public key systems. This declaration which, in individual cases, can also be faxed by the users to the certifying CA is kept by the certifying authority and primarily contains the agreement to the guidelines of this policy and possibly a declaration indicating which party generated the asymmetric key pair to be certified.

Fees

The DFN-PCA reserves the right to impose fees for certain services. Each certified CA on its part has the possibility of imposing fees for certain services.

References

DFN-PCA: Low-Level Policy, Version 1.2, 1 January 1999

RFC 1422: S. Kent: Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management, February 1993

X.509: ITU-T Recommendation X.509 (1997 E): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997

PKIX: Public Key Infrastructure (X.509), Working Group of the Internet Engineering Task Force (IETF), 1999

Abbreviations

CA: Certification Authority

CPS: Certification Practice Statement

CRL: Certificate Revocation List

CSR: Certificate Signing Request

DFN: Verein zur Förderung eines Deutschen Forschungsnetzes e.V.

DN: Distinguished Name (X.500 Name)

FTP: File Transfer Protocol

ID: Identifier

ITU: International Telecommunication Union

LDAP: Lightweight Directory Access Protocol

PCA: Policy Certification Authority

PIN: Personal Identification Number

RA: Registration Authority

RFC: Request for Comment

RSA: Rivest, Shamir, Adleman (developers of the RSA algorithm)

S/MIME: Secure/Multipurpose Internet Mail Extensions

SSL: Secure Sockets Layer

WIN: Wissenschaftsnetz (Science Network)