Network Working Group
Request for Comments: 1875
Category: Informational

N. Berge
Norwegian Computing Center

December 1995

UNINETT PCA Policy Statements

Status of this Memo

This memo provides information for the Internet community. This memo does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Table of Contents

1. Introduction....2
2. PCA Identity....2
3. UNINETT - a brief overview....2
4. PCA Scope....2
4.1 The certification tree....3
4.2 Use of Registration Authorities (RAs)....3
5. PCA Security & Privacy....3
5.1 Security requirements imposed on the PCA....3
5.2 Security requirements imposed on CAs....4
5.3 Security requirements imposed on RAs....4
5.4 Measures taken to protect the privacy of any information collected in the course of certifying CAs and (for CAs) users....4
6. Certification Policy....5
6.1 Policy and procedures when certifying CAs....5
6.2 Policy and procedures when certifying RAs....5
6.3 Policy and procedures when certifying users....5
6.4 Validity interval for issued certificates....6
6.5 The CAs right to a DN and procedures to resolve DN conflicts....6
6.6 The users right to a DN and procedures to resolve DN conflicts....6
7. Certificate Management....7
8. CRL Management....7
9. Naming Conventions....8
10. Business Issues....9
10.1 Legal agreement concerning CAs....9
10.2 Legal agreement concerning RAs....9
10.3 Fees....9
11. Other....9
11.1 Distribution of software needed by CAs, RAs and users....9
12. Security Considerations....9

13. References.....10
14. Author's Address.....10

1. Introduction

This document provides information about policy statements submitted by the UNINETT Policy Certification Authority (UNINETT PCA).

It's purpose is to provide information to members of the Internet community who wish to evaluate the trust they can place in a certification path that includes a certificate issued by the UNINETT PCA, or to set up a CA to be certified by the UNINETT PCA.

2. PCA Identity

Distinguished Name (DN): C=no, O=uninett, OU=pca

The UNINETT PCA will be run by:
Norwegian Computing Center
Gaustadallien 23
P.O.Box 114 Blindern,
N-0314 Oslo, Norway

Contact person:
Nils Harald Berge
Email: Nils.Harald.Berge@nr.no
Tel.: (+47) 22 85 25 00
Fax : (+47) 22 69 76 60

Duration: This policy is valid from Oct 1, 1995 to Jan 1, 1998

Info about this PCA is available at: http://www.uninett.no/pca/

3. UNINETT - a brief overview

UNINETT is a Limited Company (AS) operating the Norwegian network for academics and research. It is incorporated under Norwegian law, and it's company number is 968100211.

More information is available from the UNINETT web server at: http://www.uninett.no/

4. PCA Scope

The scope of the UNINETT PCA is determined by UNINETT Policy. It will chiefly certify CAs to run on behalf of legal entities such as schools and companies.

4.1 The certification tree

The certification tree beneath the UNINETT PCA comprise three distinct entities: Certification Authorities (CAs), Registration Authorities (RAs) and users. CAs are described in the PEM documents [1,2,3,4]. An explanation of RAs is given bellow.

There will be one CA, with possible sublevel CAs, per UNINETT member organization. The CA may be run by the organization itself, or by the organization running the PCA for organizations who do not want to take on the responsibility themselves.

4.2 Use of Registration Authorities (RAs)

Since the CA may be located far away from the users, local authorities are needed for physical identification/authentication of users. For security reasons, and to avoid an unnecessary large number of CAs, these authorities are not allowed to issue certificates.

A registration authority (RA) is an ordinary user, appointed by an organization or an organizational unit and trusted by a CA, serving as a point of contact for persons who want to register as users, i.e. to have a certificate issued. In order to avoid faked requests for certification, users must send their self-signed certificate to an appropriate RA, and then physically visit the RA with proof of identity. The RA will forward the self-signed certificate to the CA in a message signed by the RA, if the user is properly authenticated.

For bulk certification (see 5.3) the RA must physically verify the identity of the user before giving out the password for access to the users private key.

A CA may appoint as many RAs as it wish. The only difference between certifying an RA and an ordinary user is that the RA (a person) must sign an agreement with the certifying CA, stating the obligation to adhere to the agreed procedures.

5. PCA Security & Privacy

5.1 Security requirements imposed on the PCA

- The PCA will have its private key stored on a smartcard.

- The PCA will be run on a dedicated workstation with no network connection. The workstation will be physically secured.

- Exchanging data between the PCA workstation and the rest of the world will be done by using tapes or floppy discs.

- The PCA RSA key pair will have a length of 1024 bits.

- Backups from the PCA workstation must be stored in at least one off site location. Backups must be physically secured

5.2 Security requirements imposed on CAs that are to be certified

- A CA must be run on a dedicated workstation with no network connection. The workstation must be physically secured.

- Exchanging data between the CA workstation and the rest of the world must be done by using tapes or floppy discs.

- The CA RSA key pair must have a minimum length of 1024 bits.

A security requirements document concerning CAs will be made available online, and expected to be obeyed.

5.3 Security requirements imposed on RAs that are to be certified

- RAs must use a work station, with remote login disabled. Use of X-terminal, terminal emulator etc. with processes running on a remote machine is strictly prohibited.

- The RA RSA key pair must have a minimum length of 512 bits.

A security requirements document concerning RAs will be made available online, and expected to be obeyed.

5.4 Measures taken to protect the privacy of any information collected in the course of certifying CAs and (for CAs) users.

CAs will not collect any security relevant information about users. In those cases when CAs generate keys (and certificates) on behalf of users, all information pertaining the users private key will be securely deleted after it has been received by the user. CAs will always generate their own key pairs, thus no security relevant information will be collected by the PCA.

All archived material concerning DNs for users will be stored on the CA workstations, which are physically protected and does not have any network connections.

6. Certification Policy

6.1 Policy and procedures when certifying CAs

In order to be certified, a CA must sign an agreement with the UNINETT PCA stating the obligation to adhere to the agreed procedures.

The persons responsible for running the CA will be evaluated by the UNINETT PCA, in order to determine whether they exhibit the necessary qualifications and have access to the resources needed in order to run the CA securely.

The CA must submit its self signed certificate to the UNINETT PCA.

6.2 Policy and procedures when certifying RAs

The organization or organizational unit is responsible for appointing RA persons, typically 1-3 persons per organization/unit. The person representing the RA must sign an agreement with the certifying CA, stating the obligation to adhere to the agreed procedures in order to be certified.

The person representing the RA will be evaluated by the certifying CA, in order to determine whether he/she exhibits the necessary qualifications and has access to the resources needed to run the RA securely.

The RA must submit its self signed certificate to the certifying CA. In the absence of RAs, or equivalent, the validity of the certification request (i.e. the identity of the requestor) must be verified by "out of band" means. These means will vary from case to case, depending on physical distance, prior knowledge etc.

6.3 Policy and procedures when certifying users

There are two ways in which a user can be certified:

- individual certification, or
- bulk certification

When applying individual certification, a user will generate his own key pair, and his own self-signed certificate. The certification procedure follows the PEM documents [1,2,3,4], with the exception that the certification request will be sent to an RA. The user must then visit the RA with proof of identity

Bulk certification of users will typically be done when it is desirable to certify many users belonging to the same organization. An example could be the certification of students at the beginning of a semester, or initial certification of all employees belonging to a company. When bulk certifying users, the CA will generate the users' key pairs and certificates. A user's key pair together with the certificate will be DES-encrypted and sent electronically to the user. The pass phrase to generate the DES-key can be collected at the local RA, given proof of identity. The pass phrase can also be sent by certified surface mail.

When bulk certifying users the CA or RA shall not access or store any of the users' private information.

A person's identity is verified by:

- driver's licence
- passport
- bank card (Norwegian)

CA and RA need not be separate entities. A CA may verify the identity of users directly, following the procedures described above.

6.4 Validity interval for issued certificates

Validity interval for user and RA certificates is maximum 2 years from date of issue.

There is in principle no special requirements regarding validity intervals for CA certificates, though it is recommended not to issue certificates for more than a 10 year period.

6.5 The CAs right to a DN and procedures to resolve DN conflicts

CAs will preferably use DNs reflecting the organizational scope under which they certify users (see also "Naming conventions"). The certifying entity must ensure, with the aid of X.500 as disambiguation tool, the uniqueness of a DN.

6.6 The user's right to a DN and procedures to resolve DN conflicts

It is the certifying CA who will determine a user's DN and ensure, with the aid of X.500 as disambiguation tool, the uniqueness of a DN. Users will preferably use DNs reflecting the organization to which they belong, and their full name (see also "Naming conventions").

7. Certificate management

UNINETTs X.500 service will be used when storing certificates belonging to users within UNINETT member organizations. Other users may also use the X.500 service if available. All certificates issued will be maintained in a local database by the certifying entity in addition to the X.500 directory. If a CA does not have access to the X.500 service, all issued certificates must be mailed to the UNINETT PCA who will make the X.500 entries on behalf of the CA.

Certificates can be requested in two ways, either directly from the X.500 directory, or by querying a mail-responder service maintained by the UNINETT PCA.

Details on how certificates are mailed, and how to use the mail-responder service can be found at the following WWW site: http://www.uninett.no/pca/

8. CRL Management

Certificate Revocation Lists (CRLs) must be issued at least once a month, on a specified date, by CAs. The UNINETT X.500 service will be used to publish CRLs. If a CA does not have access to the X.500 service the CRL must be mailed to the UNINETT PCA who will make the X.500 entries on behalf of the CA.

CRLs can be requested in two ways, either directly from the X.500 directory, or by querying a mail-responder service maintained by the UNINETT PCA.

Details on how CRLs are mailed, and how to use the mail-responder service can be found at the following WWW site:

http://www.uninett.no/pca/

The UNINETT PCA will continually update the CRL with revoked CA certificates.

There is no automatic distribution service of CRLs. Therefore users will have to pull CRLs from the X.500 or the mail-responder. Black lists are currently not supported. Appropriate news groups and information services will be used to announce the issuance of new CRLs.

9. Naming Conventions

Naming conventions for CAs:

CAs' DNs will follow the conventions adopted by their organization. Organizations who do not have any preferences in this matter should use the following scheme:

C=<country>, O=<organization> [, OU=<organizational-unit>]

Country is the country code, e.g. all Norwegian organizations have C=no. Organization is the organization represented by the CA (e.g. the scope for which the CA certify users). Organizational-unit is optional, reflecting a unit within a large organization for cases in which the organization has more than one CA. Example: the CA responsible for certifying UNINETT employees will be assigned the following DN: C=no, O=uninett

Naming conventions for users:

Users' DNs will follow the conventions adopted by their organization. Organizations who do not have any preferences in this matter should use the following scheme:

C=<country>, O=<organization>, [OU=<organizational-unit>,]
CN=<personal name>

Personal name will be a unique name for the user with respect to the organization to which the user belongs. An organization's CA is responsible for ensuring that all certified users have a distinct personal name. Usually personal name will be the user's full name. Use of OU is optional. Example if Per Olsen is an employee of UNINETT he will be assigned the following DN: C=no, O=uninett, CN=Per Olsen.

The choice of which users to certify as belonging to the organization is made by the CA, not by the PCA.

10. Business Issues

10.1 Legal agreements concerning CAs

If a CA wishes to be certified by the UNINETT PCA, the CA will have to sign a legal agreement with the UNINETT PCA. The legal agreement can be obtained by contacting the UNINETT PCA.

10.2 Legal agreements concerning RAs

If an RA wishes to be certified by a CA, a person representing the RA will have to sign a legal agreement with the CA. The legal agreement can be obtained from the appropriate CA, or directly from the UNINETT PCA. Each CA will locally decide whether the RA is to be certified.

10.3 Fees

The UNINETT PCA reserves the right to charge fees. The fee structure will be determined by UNINETT policy.

11. Other

11.1 Distribution of software needed by CAs, RAs and users

The software needed is based on the SecuDE-package from GMD Darmstadt, and is available without fee for non-commercial purposes. All software distributions should include a signature from the UNINETT PCA to verify its integrity. Users, CAs, and RAs are expected to verify such signatures immediately after installation.

12. Security Considerations

Security issues are discussed throughout this memo.

13. References

[1] Linn, J., "Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures", RFC 1421, IAB IRTF PSRG, IETF PEM WG, February 1993.

[2] Kent, S., "Privacy Enhancement for Internet Electronic Mail: Part II: Certificate-Based Key Management", RFC 1422, IAB IRTF PSRG, IETF PEM, BBN, February 1993.

[3] Balenson, D., "Privacy Enhancement for Internet Electronic Mail: Part III: Algorithms, Modes, and Identifiers", RFC 1423, IAB IRTF PSRG, IETF PEM WG, TIS, February 1993.

[4] Kaliski, B., "Privacy Enhancement for Internet Electronic Mail: Part IV: Key Certification and Related Services", RFC 1424, RSA Laboratories, February 1993.

14. Author’s Address

Nils Harald Berge
Norwegian Computing Center
Gaustadallien 23
P.O.Box 114 Blindern,
N-0314 Oslo, Norway

Phone: (+47) 22 85 25 00
Fax : (+47) 22 69 76 60
EMail: Nils.Harald.Berge@nr.no