

UNICORE-CA (U-CA) Policy

Certification Guidelines for UNICORE

As of 2000-11-27
Version: 0.9
Validity: 2001-01-01 to 2001-06-30
Author: Dr. Ernst Bötsch
Leibniz Computer Centre (LRZ)
of the Bavarian Academy
of Sciences

Contents

1 Introduction

2 Identity of the U-CA

3 Scope of the U-CA

3.1 Legal significance

3.2 The UNICORE certification hierarchy

3.3 UNICORE registration authorities (U-RAs)

4 Security of the U-CA equipment

4.1 Security requirements for the U-CA

4.1 Security requirements for U-RAs

4.1 Security requirements for end entities

5 Certification rules

5.1 Rules for the certification of end entities

6 Management of certificates

7 Revocation of certificates

8 Rules for naming

8.1 Choice of a name for U-RAs and end entities

9 Miscellaneous

10 References

11 Abbreviations

12 Change History

Preliminary remarks

This is Version 0.9 of the policy for the UNICORE Certification Authority (U-CA). This version is valid until 2001-06-30 and largely follows the "World Wide Web Policy" of the DFN-PCA (see [KeLie]).

1. Introduction

This document contains the certification guidelines (the so-called "policy" or "certification practice statement", CPS) of the certification authority of the UNICORE project.

The statements made in this document are binding for the work of the U-CA, unless they contradict legal regulations. The U-CA exclusively issues certificates according to the guidelines of this policy. For work under the UNICORE project, an English translation is herewith published; at all events, however, the German version, as amended, shall prevail.

2. Identity of the U-CA

Postal address: Leibniz-Rechenzentrum (LRZ)
der Bayerischen Akademie der Wissenschaften
UNICORE-CA
Barer Straße 21
D-80333 München
Telephone: +49 89 / 289-2 88 31
Fax: +49 89 / 2809460

E-mail address: unicore-ca@lrz-muenchen.de

Information services: WWW server: <http://unicore-ca.lrz-muenchen.de/>

Validity of this document: 2000-12-01 to 2001-06-30

Version of this document: 0.9

3. Scope of the U-CA

The U-CA's sphere of responsibility comprises all organizations / institutions participating in the UNICORE collaboration, i.e. primarily natural as well as legal persons under public or private law from science and research.

The U-CA exclusively issues the following certificates:

- certificates for UNICORE users

- certificates for gateways and network job supervisors (NJSs) of the UNICORE sites
- certificates for code signing for the developers of the UNICORE software

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

3.1. Legal significance

A certification by the U-CA does not entail any legal significance; there is no legal claim to having a certificate issued by the U-CA. Especially the general legal relevance of digital signatures is currently unclear. The purpose of a UNICORE-wide public key infrastructure (PKI) is the creation of the technical prerequisites for secure access to the UNICORE resources.

In particular, the UNICORE project, the Leibniz Computer Centre of the Bavarian Academy of Sciences (LRZ), the U-CA staff as well as the staff members of the UNICORE registration authorities (U-RAs) do not assume any form of warranty. All tasks are performed by the PKI staff to the best of their knowledge and belief. Moreover, no liability or warranty under the Digital Signature Act will be assumed.

3.2. The UNICORE certification hierarchy

The UNICORE-PKI consists of the following levels:

- **DFN Policy Certification Authority (DFN-PCA):**

The U-CA is incorporated in the DFN certification hierarchy (see [DFN-PCA]). In the event of any conflicts with the DFN-PCA policy (see [KeLie]), attempts will be made to adapt the U-CA policy in order to maintain the incorporation of the U-CA in the DFN certification hierarchy.

The DFN-PCA issues the root certificate of the DFN certification hierarchy.

- **U-CA:**

- The public key of the U-CA root certificate is contained in a certificate issued by the DFN-PCA.

The root certificate serves exclusively for signing the actual "certifier certificates".

- Each U-CA staff member receives a personal certifier certificate which is exclusively used for signing the remaining certificates or certificate revocation lists (CRLs).

- UNICORE registration authorities (U-RAs, see 3.3)

- The **end entities** are composed of the following groups:

- users (client certificates for SSL)
- gateways and NJSs of the UNICORE sites
- developers of UNICORE software (client certificates for code signing)

All subscribers to the infrastructure receive the DFN-PCA root certificate and the U-CA certificates in the course of their own certification and can thus verify the authenticity and validity of all certificates issued below the U-CA level.

The U-CA does not certify any sub-CAs. Cross certification with other (P)CAs is not planned for the time being.

Anonymous or pseudonymous certificates are not issued. The U-CA generates no asymmetric key pairs for end entities.

3.3. UNICORE registration authorities (U-RAs)

The UNICORE registration authorities (U-RAs) are trustworthy persons who verify (register) the identity and authenticity of individual end entities on site on behalf of and for the support of the U-CA, before these end entities are certified by the U-CA. The UNICORE project nominates such U-RAs.

A U-RA may neither generate asymmetric key pairs for end entities nor can it issue certificates itself; a U-RA can, however, initiate the revocation of certificates.

The certificate signing request (CSR) of the end entity is recorded via a corresponding WWW interface.

The U-RA verifies the following in a suitable manner (see section 5.):

- the validity of the proof of identity
- the identity of the end entity
- all data in the user agreement (see the "user form" in [Böt]), which can be checked using the proof of identity presented
- the end entity's signature in the user form

The U-RA confirms the verification performed by countersigning the user form. It then passes this *original user form* on to the U-CA (e.g. by handing it over personally or sending it by post). The U-RA is recommended to keep a second original safe on site.

The *registered data* (CSR etc.) may only be transmitted in one of the following ways:

- personal delivery
- combined procedure in which *all* of the following four conditions must be *simultaneously* fulfilled:

- The U-RA has released the data (protected by identification/password and SSL) in the PKI management system (WWW interface).
- The U-RA has sent the user form to the U-CA by post, courier etc.
- The U-CA has checked the U-RA's signature in the user form received with the aid of a signature list.
- The U-CA has convinced itself by phoning back that the U-RA has really dispatched the user form and initiated certification.

If these four conditions are simultaneously fulfilled, the DFN-PCA accepts this procedure as equivalent to a personal delivery (see [KeLie] section 3.3).

- Electronic transmission where the data must, however, be digitally signed to preclude misuse.
In this case, the U-CA must always verify the correctness of the U-RA signature.

The new certificate issued by the U-CA is subsequently made available both to the U-RA and to the end entity.

The UNICORE project may nominate any number of persons as U-RAs. These persons must each sign an agreement (see the "staff member form" in [Böt]) binding them to certain guidelines. In particular, a U-RA should comply with the security requirements according to section 4.2. The U-CA will publish these guidelines together with a list of all U-RAs it has nominated. Moreover, the identity of a U-RA will be personally checked by a staff member of the U-CA with the aid of an official identity card with photograph.

4. Security of the U-CA equipment

Due to the participation in a PKI, 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 subscribers. The requirements for the U-CA are naturally higher since the misuse of a U-CA key would withdraw trustworthiness from all subordinate certificates.

4.1. Security requirements for the U-CA

The following demands are made on the U-CA:

- Two computers are used for the services of the U-CA:
 - All certificates are *exclusively* generated *off line* on a dedicated certification computer which at no time has a network connection. Moreover, this computer is physically especially protected.

Any data exchange with networked computers will be performed by U-CA staff using external data carriers (e.g. floppy disk or magnetic tape).

- Information (e.g. the certificates generated) is made available and organizational tasks handled via a second dedicated database

computer.

For technical reasons, this computer must have a network connection; special care must therefore be taken to protect it from misuse.

Unauthorized access to this computer is prevented by using suitable hard- and software. For example, access to the WWW server is only possible via HTTPS.

- *No automated* data processing takes place. All media containing keys are stored in a safe location if they are not in use.
- Secret keys of the U-CA for the generation of digital signatures are exclusively generated and used by the U-CA staff on the dedicated certification 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 U-CA staff and must never be stored as plain text or sent through unprotected network connections. The peripherals are not used on other computers. The secret key to the *U-CA root certificate* may only be accessed in the presence of at least two U-CA staff members (double-check principle).
- The secret signature key to the U-CA root certificate is exclusively used to sign the individual certifier certificates of the U-CA staff. The secret signature keys of the certifier certificates are exclusively used to sign end entity keys and certificate revocation lists (CRLs). *Under no circumstances* may these secret signature keys be used for confidential and/or authentic communication with the U-CA; for these purposes, therefore, *different* key pairs are used which are, of course, certified by the U-CA.
- Asymmetric key pairs of the U-CA for the generation of signatures have a minimum length of 2048 bits RSA (or a comparable level). All signature keys are exclusively generated by the U-CA itself.
- The integrity of all relevant data and programs on the computers of the U-CA is regularly verified with the aid of cryptographic applications. All data are treated confidentially by the U-CA staff; all legal data protection regulations in force are complied with.
- A data backup is performed for all relevant (electronic) U-CA 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 which, in particular, is intended to permit long storage times for certificates and CRLs.

4.2. Security requirements for U-RAs

The following demands are made on the U-RAs appointed by the UNICORE project:

- If a representative of the U-RA is to be provided at a site, this person must be registered as fully qualified U-RA.
- Access to the administration interface (a WWW interface) must be protected by nontrivial passwords (minimum length: 8 characters).

In particular, the passwords must not be disclosed to other persons, filed as plain text or sent through unprotected network connections.

- All data must be treated confidentially by the U-RAs; all legal data protection regulations in force must be complied with.

4.3. Security requirements for end entities

The end entity's secret key (see 3.2) 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 entity'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 the PIN may be disclosed to other persons.

Password or PIN must never be filed as plain text (i.e. stored on the disk) or sent through unprotected network connections.

Security requirements for users (SSL, code signing)

Users in terms of this policy are individual persons forming a subset of the end entities.

- 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. A minimum length of 1024 bits is recommended e.g. for code signing.
- 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 the gateways and NJSs of the UNICORE sites

- The asymmetric key pair for gateways and NJSs must have a minimum length of 1024 bits RSA (or a comparable level).
- Since the secret key is normally unlocked once the gateways and NJSs are started (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.

It is *urgently* recommended not to start gateways or NJSs *automatically* since the secret key must then be available as plain text or in an equivalent form in a file. Should it be impossible for technical or organizational reasons to operate gateways or NJSs in such a mode, particular importance must be attached to the system security of the server computers.

5. Certification rules

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

End entities 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 U-CA will convince itself of the identity of the key holder requesting certification in a suitable manner by technical and organizational measures prior to certification. In this connection, the U-CA can also demand 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* with one of the U-RAs prior to certification. Responsibility lies with that U-RA. U-CA staff members may also simultaneously exercise the function of a U-RA, but must then abide by the rules for U-RAs.

Under no circumstances will certificates be processed *automatically*, and they are exclusively granted under the following conditions:

- The public key to be certified has the minimum length defined in section 4.3.
- The registering authority (i.e. the U-CA or a U-RA) has duly convinced itself of the key holder's identity.
- The U-CA has duly convinced itself that the key holder is in possession of the correct asymmetric key pair.

The newly issued certificate is transmitted to the certificate holder immediately after certification (e.g. 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 U-CA certificates.

Each certificate contains a serial number assigned by the U-CA, and the U-CA ensures in the certification process that no serial number has been assigned more than once.

For the time being, certificates are not automatically extended by the U-CA; applications for re-certification must be filed, where 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 U-CA during certification; however, extensions can also be proposed in the CSR.

The U-CA makes known all extensions it has supported. In particular, the U-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. The U-CA will only generate certificates according to X.509v3, if possible, and will only support widely used standard extensions (cf. X.509v3, PKIX, Netscape).

If the U-CA receives a CSR with unknown certificate extensions, it will not issue a certificate.

The LRZ has been assigned a private enterprise number ("1.3.6.1.4.1.7650") by the Internet Assigned Numbers Authority (IANA; see [IANA]). The LRZ assigns the object identifier (OID) "1.3.6.1.4.1.7650.1" to the U-CA. The U-CA thus introduces a certificate extension in conformity with X.509v3.

The certificate extension is called "unicoreKeyUsage" and corresponds to OID "1.3.6.1.4.1.7650.1". The certificate extension can assume the values "unicoreClient", "unicoreGateway", "unicoreNJS" and "unicoreApplet".

5.1. Rules for the certification of end entities

End entities wishing to be certified first generate a personal asymmetric key pair and subsequently transmit the CSR to the responsible U-RA. This is done for the time being via a suitable WWW interface of the U-CA.

The end entities must *personally* introduce themselves to one of the U-RAs. Only in this way will it be possible to verify the end entities' identity and correctly allocate the information contained in the certificate to the end entities.

For the process of verification it is necessary to present an identity card/passport or a comparable document. The U-RA confirms the verification by countersigning the user form and passes this original user form on to the U-CA (see 3.3).

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

Additional rules for the certification of the gateways and NJSs of the UNICORE sites

In addition to the above-described certification rules for end entities, specific guidelines are valid for the certification of the gateways and NJSs of the UNICORE sites which are not allocated to an individual but to a computer (name).

An administrator of the UNICORE site whose gateways and NJSs are to be certified transmits the CRS to the responsible U-RA. 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

The CSR is transmitted for the time being via a suitable WWW interface of the U-CA.

6. Management of certificates

All subscribers to the UNICORE-PKI basically agree to the publication of their certificate. It is possible, however, to individually object to publication in applying for a certificate. However, this objection does not prevent a possibly necessary publication of the certificate as an integral part of a CRL (see section 7.).

The U-CA is responsible for making publicly available all certificates it has issued including both its own and the higher-level CA certificates. New certificates and CLRs issued by the U-CA (see section 7) will be published within a reasonable period of time (normally within one week).

For making certificates publicly available the U-CA establishes 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 U-CA's partner institutions.

7. Revocation of certificates

The U-CA can revoke certificates issued by it at any time prior to the expiry of the period of validity without explicitly specifying any reasons. Causes for the revocation of a certificate may be, for example, the discovery of improper actions by a U-CA staff member or failure to comply with individual guidelines of this policy. Other reasons may be a U-CA staff member leaving an institution or a change of name.

Each certificate holder can request the U-CA or that U-RA which has certified him to revoke or initiate the revocation of a certificate issued for him without giving reasons. The U-CA will 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 subscriber's own secret key is known to have been misused or compromised, each such subscriber should immediately notify the U-CA or the relevant U-RA and initiate the revocation of his own certificate.

Certificates can only be revoked by the U-CA. Moreover, that U-RA which has registered the certificate holder can initiate a revocation without giving reasons.

All revoked certificates are published by the U-CA in a CRL made available to all subscribers. This CRL contains the date of CRL issuance (e.g. in the form of a time stamp) and is digitally signed by the U-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 subscriber basically has the possibility of applying for a new certificate.

Immediately after starting its own operation, the U-CA will issue a new (empty) CRL. Subsequently, new CRLs will be issued at regular intervals (e.g. monthly), even if no further certificates have been revoked by the U-CA in the meantime. Old CRLs will be archived to enable verification of the validity of certificates even at a later date.

For making CRLs publicly available the U-CA establishes information services (directories) whose task is to distribute certificates and CRLs (see section 6). Since

many software products at present only insufficiently support the processing of CRLs, the U-CA will inform its certificate holders accordingly and, if possible, 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 subscriber as his subject name. A DN contains a sequence of uniquely identifying name attributes by which all the subscribers in a hierarchy can be referenced; no umlauts, unusual special characters etc. will be used within this DN for reasons of interoperability.

Prior to certification, the correctness and uniqueness of the specified DN is verified by the U-CA; no name is assigned more than once.

The DN of each user follows the scheme below:

```
CN    =    "<complete name>",
EMAIL=    "<e-mail address>",
O      =    "<organization>",
[OU    =    "<organizational unit>",]
[L     =    "<city/locality>",]
[ST    =    "<state/province>",]
C      =    "DE"
```

Deviations from this scheme are only possible after prior agreement with the U-CA.

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

8.1. Choice of a name for U-CAs and end entities

The choice of unique end entity DNs is primarily governed by the U-CA guidelines. U-RAs are subject to the same rules for naming as users.

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

A valid e-mail address is adopted in the DN via the attribute "EMAIL=". Optionally, further attributes such as "OU=" ("organizational unit"), "L=" ("city/locality") and "ST" ("state/province") can be included in the DN.

If a name occurs several times within one organization, the U-CA will choose unique DNs by suitable name additions. The U-CA is furthermore responsible for checking the affiliation of the user to the institution concerned and for ensuring that all certified users have different DNs. This is done with the aid of a U-RA.

Additional rules for the gateways and NJSs of the UNICORE sites

Certificates for the gateways and NJSs must contain a distinguished name in the "CN=" attribute. This attribute must not contain wildcards nor any numerical IP addresses.

The optional attribute "EMAIL=" must contain a valid e-mail address (e.g. the address of the server administrator).

9. Miscellaneous

This document was drawn up under the UNICORE project at the Leibniz Computer Centre of the Bavarian Academy of Sciences (LRZ) in Munich and was approved by the U-CA Board.

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 U-CA services.

The U-CA reserves the right not to fulfil certificate signing requests. Furthermore, no guarantee can be assumed for the availability of the U-CA services. On account of the status as a research project, there is at present no possibility of offering the U-CA services on a 7-day/24-hour basis.

Documentation and data protection

All activities within the framework of this policy will be documented as far as technically feasible. The U-CA, all U-RAs and all UNICORE staff members having access to data must treat the data arising in certification as confidential and comply with the respective data protection guidelines.

All subscribers to UNICORE-PKI (i.e. end entities, U-CA staff and U-RAs) agree to the storage and processing of their data by the U-CA.

Declaration by the U-CA staff

All U-CA staff members must sign a declaration by hand prior to their appointment (see the "staff member form" in [Böt]) in which they are informed about their duties.

Agreements between U-CA and U-RA

The U-CA requires the signing of an agreement (see the "staff member form" in [Böt]) binding the U-RA to certain guidelines. This agreement is to be signed by hand by the person acting as U-RA; it can be obtained from the U-CA.

Declaration by the end entities

All end entities of the UNICORE-PKI must sign a declaration by hand prior to their certification (see the "user form", the "UNICORE site form" and the applet signer form" in [Böt]) informing them about their rights and duties and about the risks and dangers in the employment of public key systems.

This declaration is kept by the U-CA and primarily contains the agreement to the guidelines of this policy.

Fees

The U-CA reserves the right to impose fees for certain services. However, this will not be done for the time being.

10. References

[Böt]

Ernst Boetsch:
UNICORE Certification Authority (U-CA).
Version 1.3 (2000-06-28);
<https://unicore-ca.lrz-muenchen.de/doc/u-ca.ps>

[KeLie]

Stefan Kelm, Britta Liedke:
DFN-PCA -- The World Wide Web Policy.
Certification Guidelines for the PCA Project.
As of 1 April 1999. Version: 1.0 (FINAL VERSION).
<http://www.pca.dfn.de/dfnpca/policy/wwwpolicy.html>

[DFN-PCA]

<http://www.pca.dfn.de/>

[IANA]

Internet Assigned Numbers Authority:
<http://www.iana.org/>

[PCA/Low]

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

[PKIX]

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

11. Abbreviations

CA:	<u>C</u> ertification <u>A</u> uthority
CPS:	<u>C</u> ertification <u>P</u> ractice <u>S</u> tatement
CRL:	<u>C</u> ertificate <u>R</u> evocation <u>L</u> ist
CSR:	<u>C</u> ertificate <u>S</u> igning <u>R</u> equest
DFN:	Verein zur Förderung eines <u>D</u> eutschen <u>F</u> orschungs <u>n</u> etzes e.V
DN:	<u>D</u> istinguished <u>N</u> ame (X.500 name)
FTP:	<u>F</u> ile <u>T</u> ransfer <u>P</u> rotocol
IANA:	<u>I</u> nternet <u>A</u> ssigned <u>N</u> umbers <u>A</u> uthority
ITU:	<u>I</u> nternational <u>T</u> elecommunication <u>U</u> nion
LDAP:	<u>L</u> ightweight <u>D</u> irectory <u>A</u> ccess <u>P</u> rotocol
NJS:	<u>N</u> etwork <u>J</u> ob <u>S</u> upervisor
OID:	<u>O</u> bject <u>I</u> dentifier
PCA:	<u>P</u> olicy <u>C</u> ertification <u>A</u> uthority
PKI:	<u>P</u> ublic- <u>K</u> ey <u>I</u> nfrastructure
PIN:	<u>P</u> ersonal <u>I</u> dentification <u>N</u> umber
RFC:	<u>R</u> equest for <u>C</u> omment
RSA:	<u>R</u> ivest, <u>S</u> hamir, <u>A</u> dleman (developers of the RSA algorithm)
SSL:	<u>S</u> ecure <u>S</u> ockets <u>L</u> ayer
U-CA:	<u>U</u> NICORE <u>C</u> ertification <u>A</u> uthority
U-RA:	<u>U</u> NICORE <u>R</u> egistration <u>A</u> uthority
WWW:	<u>W</u> orld <u>W</u> ide <u>W</u> eb

12. Change History

This section briefly¹ documents the modifications of this policy in the transition to the respective next version and is not an integral part of the policy:

- 0.9 (2000-11-27): This version will be presented to the U-CA Board for approval. Modifications to the previous version:
- 3. (Preliminary remarks) + 3.2. + 4.3. + 5.1. + 8.:
WWW servers no longer receive certificates, but certificates are issued to the gateways and NJSs of the UNICORE sites
 - 3.1.:
No liability and warranty under the Digital Signature Act
 - 3.2.:
Incorporation of the U-CA into the DFN certification hierarchy
 - 3.3.:
Indication of what the U-RA must verify and that the U-RA countersigns the user form. The U-RA is recommended to keep a second original safe on site.
Updating of the rule on how to transmit registered data to the U-CA.
 - 4.3.:
In the "Security requirements for the gateways and NJSs of the UNICORE sites" reference to an automated start of the systems
 - 5.:
Only U-RAs are allowed to check users.
 - 5.1.:
Only U-RAs are allowed to check users. Besides an identity card or passport, other comparable documents are also allowed (adaptation to [KeLie])
Indication that the U-CA countersigns the user form and adaptation to the changes in section 3.3..
Updating of the "Additional rules for the certification of the gateways and NJSs of the UNICORE sites"
 - 8.:
The attribute "OU=" becomes optional. The rules for the "U-login" are deleted without replacement.
In the section on "Certificate extensions" reference to the UNICORE-specific extensions
 - 9.:
Reference to the U-CA Board.
 - References:
URL of IANA
 - Abbreviations:
New acronyms "IANA", "NJS" and "OID"
 - Change history:
Footnote illustrating what is not documented in the history.

¹ For example, the correction of mistakes and the slight alteration of formulations for improved comprehension or adaptation to modifications in preceding and succeeding paragraphs are *not* documented here.

0.8 (2000-06-28): New: Verification of a U-RA's identity in section 3.3.

0.7 (1999-12-17): First publication on the discussion within the UNICORE project

1. Paper forms

1.1. User form

SUBSCRIBER DECLARATION IN CONNECTION WITH A CERTIFICATION BY THE UNICORE-CA

The certificate holder (i.e. the undersigned user) declares that the applicable version of the certification guidelines (policy) of the UNICORE-CA (certifier) was known to him/her at the time of undersigning and that he/she agrees to this policy.

The certificate holder furthermore declares that he/she is aware of the risks of careless handling of his/her secret key. He/she confirms that he/she is aware that UNICORE-CA certificates should only be used for tasks within UNICORE and that they are not related to the Digital Signature Act. Moreover, the UNICORE-CA does not assume any liability for the certificates issued.

The certificate holder is conscious of the fact that a desired publication of the certificate (e.g. via WWW, X.500, anonymous FTP etc.) also makes the certificate holder's full name and e-mail address publicly known since this information is an integral part of the certificate.

The certificate holder has *personally* and truthfully transmitted the data below, which are required pursuant to the policy, to the UNICORE-CA via a WWW interface.

In connection with the completion of the corresponding WWW forms, moreover, an asymmetric key pair was generated by the certificate holder's WWW browser and the public key was automatically transmitted together with the other data.

Data of the certificate holder:

family name:	...
first name(s):
title:	... (opt)
sex:	male/female
valid e-mail address
telephone	... (opt)

Data of the institution/organization:

name:	...
street, house number:	...

postcode, place:
country: ...
fax: ... (opt)

Document for verifying identity:

type: identity card/passport
number: ...
issuing country: ...

Data of the client key:

type: client
X.509-DN: ...
length: ...
fingerprint: ...

Publication of the certificate: yes/no

Processing registration authority: ...

date

signature of the certificate holder

All data produced during certification will be treated confidentially by the UNICORE staff and only used for UNICORE purposes. The certificate holder agrees to the storage and processing of these data within UNICORE.

signature of the certificate holder

The undersigned registration authority confirms that it has verified the certificate holder's identity and relevant data with the aid of an (identity card/passport) and that the certificate holder has personally signed the subscriber declaration.

signature of the registration authority

The undersigned certification authority confirms that it has convinced itself of the authenticity of this form.

date

signature of the certification authority

"UNICORE user 1.0" form

1.2. U-RA form

DECLARATION BY THE REGISTRATION AUTHORITY IN CONNECTION WITH A CERTIFICATION BY THE UNICORE-CA

The undersigned (i.e. the registration authority) declares that the applicable version of the certification guidelines (policy) of the UNICORE-CA was known to him/her at the time of undersigning and that he/she agrees to this policy.

The undersigned moreover declares that he/she is entitled to assume the function of a UNICORE-CA registration authority for the organization specified below. Within the framework of this activity, the undersigned will comply with the guidelines for the registration of users laid down in the UNICORE-CA policy. All data produced during certification will be treated confidentially by the undersigned and only used for UNICORE purposes.

The undersigned furthermore declares that he/she is aware of the risks of a negligent verification of a user's identity.

The undersigned has truthfully transmitted the following data required pursuant to the policy to the UNICORE-CA.

Data of the undersigned:

family name: ...
first name(s): ...
title: (opt)
sex: male/female
valid e-mail address ...
telephone: ...

Data of the institution/organization:

name: ...
street, house number: ...
postcode, place: ...
country: ...
fax: (opt)

date signature

The undersigned agrees to the storage and processing of his/her own data within UNICORE.

signature

The undersigned certification authority confirms that it has convinced itself of the authenticity of this form.

date signature of the certification authority

"U-RA 1.0" form

1.3. Site form

DECLARATION BY A UNICORE SITE IN CONNECTION WITH A CERTIFICATION BY THE UNICORE-CA

The undersigned (certificate holder, i.e. the administrator of the UNICORE site) declares that he/she is entitled to operate the gateway and network job supervisor (NJS) of the UNICORE site specified below and that the applicable version of the certification guidelines (policy) of the UNICORE-CA (certifier) was known to him/her at the time of undersigning and that consent is given to this policy.

The undersigned furthermore declares that he/she is aware of the risks of a careless handling of the secret key of the gateway and NJS. He/she confirms that he/she is aware that UNICORE-CA certificates should only be used for tasks within UNICORE and are not related to the Digital Signature Act. Moreover, the UNICORE-CA does not assume any liability for the certificates issued.

The undersigned has transmitted the public key of the gateway and NJS to the UNICORE-CA together with the data necessary according to the policy and requests a certification of this key.

The asymmetric key pair was personally generated by the undersigned.

Data of the certificate holder:

family name:	...
first name(s):	...
title:	(opt)
sex:	male/female
valid e-mail address:	...
telephone:	...

Data of the institution/organization (UNICORE site):

name:	...
-------	-----

street, house number: ...
postcode, place: ...
country: ...
fax: (opt)

Data of the server key:

type: gateway/NJS
X.509-DN: ...
length: ...
fingerprint: ...

Publication of the certificate: yes/no

date

signature of the certificate holder

All data produced during certification will be treated confidentially by the UNICORE staff and only used for UNICORE purposes. The certificate holder agrees to the storage and processing of these data within UNICORE.

signature of the certificate holder

The undersigned certification authority confirms that it has convinced itself of the authenticity of this form.

date

signature of the certification authority

"UNICORE site 1.0" form

1.4. Applet signer form

DECLARATION BY A UNICORE DEVELOPER IN CONNECTION WITH A CERTIFICATION BY THE UNICORE-CA

The undersigned (certificate holder) declares that he/she is entitled to develop UNICORE applets and that the applicable version of the certification guidelines (policy) of the UNICORE-CA (certifier) was known to him/her at the time of undersigning and that consent is given to this policy.

The undersigned furthermore declares that he/she is aware of the risks of a careless handling of the secret key for signing UNICORE applets. He/she confirms that he/she is aware that UNICORE-CA certificates should only be used for tasks within UNICORE and are not related to the Digital Signature Act. Moreover, the UNICORE-CA does not assume any liability for the certificates issued.

The undersigned has transmitted the public key for signing UNICORE applets to the UNICORE-CA together with the data necessary pursuant to the policy and requests a certification of this key.

The asymmetric key pair was personally generated by the undersigned.

Data of the certificate holder:

family name:	...
first name(s):	...
title:	(opt)
sex:	male/female
valid e-mail address:	...
telephone:	...

Data of the institution/organization:

name:	...
street, house number:	...
postcode, place:	...
country:	...
fax:	(opt)

Data of the key for signing applets

type:	applet
X.509-DN:	...
length:	...
fingerprint:	...
Publication of the certificate:	yes/no

date

signature of the certificate holder

All data produced during certification will be treated confidentially by the UNICORE staff and only used for UNICORE purposes. The certificate holder agrees to the storage and processing of these data within UNICORE.

signature of the certificate holder

The undersigned certification authority confirms that it has convinced itself of the authenticity of this form.

date

signature of the certification authority

"UNICORE applet signer 1.0" form

1.5. Staff member form

DECLARATION BY A UNICORE STAFF MEMBER IN CONNECTION WITH A CERTIFICATION BY THE UNICORE-CA

The undersigned (i.e. UNICORE staff member) declares that the applicable version of the certification guidelines (policy) was known to him/her at the time of undersigning and that he/she agrees to this policy.

All data produced during certification will be treated confidentially by the undersigned and only used for UNICORE purposes.

Data of the undersigned

family name:	...
first name(s):	...
title:	(opt)
sex:	male/female
valid e-mail address:	...
telephone:	...

Data of the institution/organization:

name:	...
street, house number:	...
postcode, place:	...
country:	...
fax:	(opt)

date

signature

The undersigned agrees to the storage and processing of his/her own data within UNICORE.

signature

The undersigned certification authority confirms that it has convinced itself of the authenticity of this form.

date

signature of the certification authority

"UNICORE staff 1.0" form