

CorporateID Accreditation specifications

Document Reference: CorporateID Accreditation Specifications



January 2006

Appendix 1: Certification and Registration Procedures

I. Introduction: Digital Certificates

Digital certificates

A digital certificate allows each participant of an electronic transaction to prove his identity towards the other participants. They are used as the digital equivalent of an ID card.

Digital certificates find their applications in 'secure' electronic mail (S/MIME) by guaranteeing the confidentiality of the message and by guaranteeing the authenticity of the message's author and content through digital signatures.

Digital certificates are also applied in electronic commerce (SSL), so the Merchant (server) can prove his identity to his Customers (clients) and vice versa.

Digital certificates are used to establish:

- authentication (certainty of the other party's identity)
- confidentiality (secrecy of exchanged content)
- integrity (inability to change content afterwards)
- non-repudiation (proof of the transaction validity afterwards)

Cybertrust offers digital certificates for individuals (also called PersonalSign certificates) and digital certificates for organisations (SureServer certificates and SureCodeSign certificates).

The level of assurance they provide regarding a person's identity differentiates certificates for individuals. The assurance level depends on how a person's identity is verified during the certification request process. Cybertrust offers 3 classes of assurance (Class 1- 3 Digital certificates).

Each category of certificate will be developed in the following paragraphs.

II. Digital Certificates for Individuals

A. Types of Certificates: Generality and Procedures

1. PersonalSign 2

General

Cybertrust PersonalSign 2 certificates are intended for certain communications and transactions that require a minimum verification of the identity.

PersonalSign 2 certificates can be distributed for communications and transactions with a low value and little risk.

The verification of the applicant's identity is done by a Registration Authority using a copy of an identity proof.

Assurance level

PersonalSign 2 certificates may provide reasonable , but not certain assurance of a subscriber's identity , based on an automated on-line process that compares the applicant's name, address, and other personal information on the certificate application against a signed identity proof .

Although PersonalSign 2 online identification process is a high level method of authenticating a certificate applicant's identity , it does not require the applicant's personal appearance before a Registration Authority .

Cybertrust accepts liability up to 2480 euro per damage caused by a false identity in the certificate used according to the CPS.

Content

Typical content of information published on a PersonalSign 2 certificate includes the following elements:

- Applicant's e-mail address
- Applicant's name
- Applicant's public key
- Code of the applicant's country
- Issuing Certification Authority
- CA's digital signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

Submitted documents to identify the applicant and issuing procedure

The applicant must submit to the Registration Authority the printed subscriber agreement and the registration form correctly signed together with a signed copy of an identity proof such as an identity card, driver's license or passport.

The following steps describe the milestones to issue a PersonalSign 2 certificate:

- The applicant fills out the request online on the web site and submits the required information.
- The CA verifies automatically the applicant's e-mail address by sending an e-mail with a URL where the applicant can start the registration procedure.
- The applicant fills out the registration form : e-mail address, common name, country code, verification method billing information as part of the online request . The applicant accepts the online subscriber agreement and a key pair is generated on an applicant's device (computer, smart card or token ...)
The public key and the online request are sent to CA GlobalSign . The applicant sends to the Registration Authority for verification the printed certificate request correctly signed together with the method of verification he has chosen
- The Registration Authority crosschecks the printed certificate request and the request online, compares its data and signature with the ones appearing on the identity proof.
- After positive verification and acceptance by the RA, the Certification Authority issues the certificate to the applicant. The CA publishes the issued certificate in an online database.

2. PersonalSign 2PRO

General

Cybertrust PersonalSign 2PRO certificates are intended for certain communications and transactions that require a minimum verification of the identity.

PersonalSign 2PRO certificates can be distributed for communications and transactions with a low value and little risk.

The verification of the applicant's identity is done by a Registration Authority using a copy of an identity proof within the professional context.

Assurance level

PersonalSign 2PRO certificates may provide reasonable, but not certain assurance of a subscriber's identity, based on an automated on-line process that compares the applicant's name, address, and other personal information on the certificate application against a signed identity proof.

Although PersonalSign 2 online identification process is a high level method of authenticating a certificate applicant's identity, it does not require the applicant's personal appearance before a Registration Authority.

Cybertrust accepts liability up to 2480 euro per damage caused by a false identity in the certificate used according to the CPS.

Content

Typical content of information published on a PersonalSign 2PRO certificate includes the following elements:

- Applicant's e-mail address
- Applicant's name
- Name of the Organisation
- Applicant's public key
- Code of the applicant's country
- Issuing Certification Authority
- CA's digital signature
- Type of algorithm
- Validity period of the digital
- Serial number of the digital certificate

Submitted documents to identify the applicant and issuing procedure

The applicant must submit to the Local Registration Authority the printed subscriber agreement and the registration form correctly signed together with a signed copy of an identity proof such as an identity card, driver's license or passport and the Articles of Association/Incorporation or any official document proving the professional context.

The following steps describe the milestones to issue a PersonalSign 2PRO certificate:

- The applicant fills out the request online on the web site and submits the required information.
- The CA verifies automatically the applicant's e-mail address by sending e-mail with a URL where the applicant can start the registration procedure.
- The applicant fills out the registration form: e-mail address, common name, organisational information, country code, and verification method, billing information as part of the online request.
The applicant accepts the online subscriber agreement and a key pair is generated on an applicant's device (computer, smart card or token ...)

The public key and the online request are sent to CA GlobalSign . The applicant sends to the Local Registration Authority for verification the printed certificate request correctly signed by the applicant and the legal representative of the company together with the method of verification he has chosen, and the Articles of Association of the organisation.

- The Local Registration Authority crosschecks the printed certificate request, compares the personal data and signature with the ones appearing on the identity proof .The professional context is verified by checking the signature of the legal representative with the mentioning of the name in the Articles of Association. The LRA sends the all documents to the RA.
- After positive verification and acceptance by the RA, the Certification Authority issues the certificate to the applicant. The CA publishes the issued certificate in an online database.

B. Renewal and Revocation of PersonalSign Certificates

Renewal and revocation are allowed for all types of PersonalSign certificates.

1. Renewal of PersonalSign Certificates

The renewal of a PersonalSign certificate is based on the same key pair and unchanged data.

The user authenticates him using his certificate and password and confirms the renewal of this certificate.

No documents have to be sent for the renewal, and after processing the payment, the RA accepts the new certificate.

The Certification Authority issues the renewed certificate to the applicant. The CA publishes the issued certificate in an online database.

2. Revocation of PersonalSign Certificates

A PersonalSign Certificate has to be revoked when the private key of the certificate is compromised or when the data in the certificate are no longer correct.

The user can revoke the certificate based on a password (online) or based on a signed request for revocation if the password cannot be recovered.

If the certificate revocation is based on a password, the CA automatically revokes the certificate.

If the certificate revocation is based on a signed request, the RA compares the signature and the serial number on the signed request for revocation and the one mentioned on the certificate that has to be revoked.

The Certification Authority revokes the certificate to the applicant. The CA publishes the issued certificate in an online database (CRL).

C. Archiving of PersonalSign Certificates

The LRA/RA has the obligation to archive each successful/ unsuccessful, renewed and revoked request in a reliable manner (the printed subscriber agreement, registration form and identity proof and status for PersonalSign 2PRO and 3PRO).

III. Digital Certificates for Organizations

A.Types of Certificates : Generality and Procedures

1. SureServer

General

Cybertrust SureServer certificates are used for proving the identity and the ownership of a domain name and for enabling confidential communication between a web server and the connected customers.

The verification of the applicant's identity is done by the RA on the basis of the Articles of Association of the organization, company database, domain name services and on a phone call to the organisation.

Assurance level

SureServer certificates provide a high level of identity assurance by requiring the Articles of Association of the organisation.
Cybertrust accepts liability up to 80.000 euro per damage caused by a false identity in the certificate used according to the CPS.

Content

Typical content of information published on a SureServer certificate includes the following elements:

- Applicant's domain name
- Name of the Organisation
- Applicant's public key
- Code of the applicant's country
- Issuing Certification Authority
- CA's digital signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

Submitted documents to identify the applicant and issuing procedure

The applicant must submit to the Registration Authority the online agreed subscriber agreement and the registration form correctly signed by the legal representative of the organization together with the Articles of Association/Incorporation or any official document proving the legal existence of the company and the authority of the applicant to act on behalf of this organisation.

The following steps describe the milestones to issue a SureServer certificate:

- The applicant creates his Certificate Signing Request (CSR) and generates his key pair.
- The applicant goes on the CA website and follows the online procedure
- The applicant can start the registration online by submitting his CSR.
- The applicant fills out the registration form: data about the organisation, billing information as part of the online request.

- The applicant confirms this data and accepts the online subscriber agreement.
- He prints out the registration form (1 document)
The public key and the online request are sent to the CA. The applicant sends the printed registration form of the certificate request correctly signed and dated by the legal representative of the company together with the Articles of Association of the organization.
- The Registration Authority verifies the ownership of the domain name, the official existence of the applicant as an organisation in a public database ,cross-checks the printed certificate request and the request online , compares the signature of the legal representative with the mentioning of the name in the Articles of Association . The Registration Authority ends up his verification by a phone call to the organisation to have confirmation of the legal representative's identity.
- After positive verification and acceptance by the RA, the Certification Authority issues the certificate to the applicant. The CA publishes the issued certificate in an online database.

2. SureCodeSign

General

Cybertrust SureCodeSign certificates are used for signing software that Software vendors or individual developers distribute over the Internet.

The verification of the applicant's identity is done by the RA on the basis of the Articles of Association of the organisation, company database, and on a phone call to the organisation if the applicant is an organisation

Assurance level

SureCodeSign certificates provide a high level of identity assurance by requiring the status of the organisation.

Cybertrust accepts liability up to 80.000 euro per damage caused by a false identity in the certificate used according to the CPS.

Content

Typical content of information published on a SureCodeSign certificate includes the following elements:

- Applicant's email address
- Name of the Organisation
- Applicant's public key
- Code of the applicant's country
- Issuing Certification Authority
- CA's digital signature
- Type of algorithm
- Validity period of the digital certificate
- Serial number of the digital certificate

Submitted documents to identify the applicant and issuing procedure

The applicant must submit to the Registration Authority the printed subscriber agreement and the registration form correctly signed by the legal representative of the organisation together with the Articles of Association/Incorporation or any official document proving the legal existence of the company and the authority of the applicant to act on behalf of this organisation

The following steps describe the milestones to issue a SureCodeSign certificate:

- The applicant fills out the request online on the web site and submits the required information.
- The CA verifies automatically the applicant's e-mail address by sending an e-mail with a URL where the applicant can start the registration procedure.
- The applicant fills out the registration form: e-mail address, common name, country code, organisational information, billing information as part of the online request. The applicant accepts the online subscriber agreement and a key pair is generated on an applicant's device (computer, smart card or token,...)
The public key and the online request are sent to CA GlobalSign . The applicant sends to the Registration Authority for verification the printed certificate request correctly signed together with the status of the organization or the method of verification he has chosen
- The Registration Authority cross-checks the printed certificate request and the request online verifies the official existence of the applicant as an organisation in a public database , compares the signature of the legal representative with the mentioning of the name in the Articles of Association . The Registration Authority ends up his verification by a phone call to the organisation to have confirmation of the legal representative's identity.
- After positive verification and acceptance by the RA, the Certification Authority issues the certificate to the applicant. The CA publishes the issued certificate in an online database.

B. Renewal and Revocation of SureServer and SureCodeSign Certificates

Renewal and revocation are allowed for SureServer and SureCodeSign certificates .

1. Renewal of SureServer and SureCodeSign Certificates

The renewal of SureServer and SureCodeSign certificates is based on the same key pair and unchanged data.

The user can renew the certificate based on a password (online) or based on a signed request for renewal if the password cannot be recovered.

If the certificate renewal is based on a password, the user authenticates himself using his certificate and password and confirms the renewal of this certificate .The printed request has to be sent to the RA for verification (signature).

If the certificate renewal is based on a signed request, the RA compares the signature and the serial number on the signed request for renewal and the one mentioned on the certificate that has to be renewed.

After processing the payment, the RA accepts the new certificate.

The Certification Authority issues the renewed certificate to the applicant. The CA publishes the issued certificate in an online database.

2. Revocation of SureServer and SureCodeSign Certificates

A SureServer or an SureCodeSign Certificate has to be revoked when the private key of the certificate is compromised or when the data in the certificate are no longer correct .

The user can revoke the certificate based on a password (online) or based on a signed request for revocation if the password cannot be recovered.

If the certificate revocation is based on a password, the certificate is automatically revoked by the CA.

If the certificate revocation is based on a signed request, the RA compares the signature and the serial number on the signed request for revocation and the one mentioned on the certificate that has to be revoked.

The Certification Authority revokes the certificate to the applicant. The CA publishes the issued certificate in an online database (CRL).

C. Archiving of SureServer and SureCodeSign Certificates

The RA has the obligation to archive each successful/ unsuccessful, renewed and revoked requests in a reliable manner (the printed subscriber agreement, the registration form and the supporting documentation).

IV. Conclusion: Training and Accreditation – Audit – Relevant Legal Documents

Training and Accreditation

Only accredited persons may hold the position of an RA. Minimum 2 persons have to be accredited.

For accreditation the persons who shall fulfil the RA function shall read the training material provided by Cybertrust and confirm receipt and understanding of the documents. The training consists of a general presentation on PKI, digital certificates and Public Key Cryptography and explains the procedures to be followed by the accredited persons to perform the RA or LRA functions.

To access the secured registration authority application (WebConnect Tool), the accredited persons receive a special administration certificate. This administration certificate is strictly personal and will be immediately revoked if the person leaves or is no longer accredited. As part of the training material, the RA will also receive the WebConnect User manual.

Audit

CA GlobalSign has the right to organise an audit yearly, to verify if the procedures have been followed. The aim of the audit is to investigate whether the minimum conditions that an RA has to meet are being fulfilled and whether or not the procedures described here are being observed. An extensive report of the audit will be made.

If in the annual audit, a person turns out not to comply with or, more specifically, is not following the procedures according to this document, Cybertrust shall remove him/her from his/her registration function.

Relevant Legal Documents

The applicant must take notice of and is bound by the following documents:

- The Certificate Practice Statement (CPS)
- The Subscriber Agreement
- The Data Protection Policy (if applicable)
- The Consumer Policy
- The Limited Warranty Policy

These documents are available on the CA GlobalSign web site (see www.globalsign.net/repository)

Appendix 2: RA Technical Specifications and Requirements

General Requirements

Cybertrust developed a fully specialised web-based Registration Authority application, named "WebConnect", for the administration of a Registration Authority. This RA application is protected with special Cybertrust issued administration certificates for each accredited person of the Registration Authority. The application is accessible via a standard Internet connection with a desktop computer, and optionally a smart card & reader.

WebConnect at this time requires at least one Windows 95/98/ME or NT4 or 2000 or XP system, with a Microsoft Internet Explorer 5+ or Netscape Communicator 4+ browser installed. Cybertrust advises systems based on at least an Intel Pentium II processor with 128 MB of RAM installed. The CorporateID Customer shall itself provide all systems used by the accredited persons.

Optionally, the systems used by the accredited persons can be further protected with a security device for storing the administration certificate. This however is an unsupported option.

Security Precautions

The Registration Authority agrees to ensure that all used systems and archives are under constant supervision by accredited persons, or are locked in a room of which the keys are only available to these accredited persons. The room or office, where these systems and archives are installed, should be equipped with an alarm system.

All passwords will be chosen based on a random combination of letters and numbers. The passwords should be changed at least every month and in no way these passwords should be written down on paper. In case of a possible infringement on the safety of the secrecy of a password, Cybertrust should be warned within 24 hours of the first indications. The administration certificate will be revoked immediately and replaced by a new one.

The CorporateID Customer agrees to follow all security guidelines that will be sent regularly by Cybertrust.

Every two years this appendix will be updated to ensure full compliance with possible changes to Cybertrust security policies. The CorporateID Customer agrees to comply with this new version within one month from receipt.

Technical Specifications

The RA can distribute certificates from Cybertrust 's technical back-end. The RA function includes the use of an administration certificate (optionally on a smart card) and a web-based Registration Authority Application named "WebConnect".

A typical Certification Authority architecture exists of two parts: the Certification Authority kernel and several Registration Authority front-end applications.

The Certification Authority kernel is the technical infrastructure for issuing, distributing and revoking certificates. It consists of a Hardware Signing Unit, a LDAP accessible Database Backend and a Certificate Management System. Cybertrust manages this secure infrastructure with specialised IT personnel. The Registration Authority application is the web-based application used by the Registration Authority in order to interact with Cybertrust's kernel. It is the Registration Authority who approves the certificate request (based on the verification procedures) and initiates the issuance of the certificate by Cybertrust.

Through an encrypted channel that is part of the Registration Authority application, the accredited person can access the certificate requests and can initiate a.o. the issuance, revocation or renewal of certificates.

