3. Practices and procedures

cyber_Folks S.A.
ul. Franklina Roosevelta 22, 60-829 Poznan
tel.: (+48) 12 296 36 63, fax: (+48) 12 395 33 65
hotline / infolinia: (+48) 501 DOMENY (366 369)
support@certyfikatyssl.pl , www.certyfikatyssl.pl , www.domeny.pl

1. PRACTICES AND PROCEDURES

This section describes the certificate application process, including the information required to make and support a successful application.

1.1. CERTIFICATE APPLICATION REQUIREMENTS

All Certificate applicants must complete the enrolment process, which may include:
- Generate a RSA key pair and demonstrate to CYBER_FOLKS S.A. ownership of the private key half of the key pair through the submission of a valid PKCS#10 Certificate Signing Request (CSR)
- Make all reasonable efforts to protect the integrity the private key half of the key pair
- Submit to CYBER_FOLKS S.A. a certificate application, including application information as detailed in this CPS, a public key half of a key pair, and agree to the terms of the relevant subscriber agreement
- Provide proof of identity through the submission of official documentation as requested by CYBER_FOLKS S.A. during the enrolment process Certificate applications are submitted to CYBER_FOLKS S.A.

1.1.1. RESELLER

Resellers operate in conformity with this CPS following the procedures specified in Reseller agreement.

1.1.2. METHODS OF APPLICATION

Generally, applicants will complete the online forms made available by CYBER_FOLKS S.A. or by approved RAs at the respective official websites. Under special circumstances, the applicant may submit an application via email; however, this process is available at the discretion of CYBER_FOLKS S.A.

1.2. APPLICATION VALIDATION

Prior to issuing a Certificate or issuing a Site Seal, CYBER_FOLKS S.A. employs controls to validate the identity of the subscriber information featured in the certificate application. Such controls are indicative of the product type:

1.2.1. SECURE SERVER CERTIFICATES

CYBER_FOLKS S.A. utilizes a two-step validation process prior to the issuance of a secure server certificate. This process involves CYBER_FOLKS S.A., automatically or manually, reviewing the application information provided by the applicant (as per section 1.3 of this CPS) in order to check that:

1. The applicant has the right to use the domain name used in the application.
- Validated by reviewing domain name ownership records available publicly through Internet or approved global domain name registrars.

• Validation may be supplemented through the use of the administrator contact associated with the domain name register record for communication with CYBER_FOLKS S.A. validation staff or for automated email challenges.
• Validation may be supplemented through the use of generic emails which ordinarily are only available to the person(s) controlling the domain name administration, for example webmaster@.., postmaster@.., admin@..
2. The applicant is an accountable legal entity, whether an organization or an individual.
• Validated by requesting official company documentation, such as Business License, Articles of Incorporation, Sales License or other relevant documents.
• For non-corporate applications, documentation such as bank statement, copy of passport, copy of driving license or other relevant documents.
The above assertions are reviewed through an automated process, manual review of supporting documentation and reference to third party official databases.

1.2.2. Domeny.pl SuperFAST SSL/ Domeny.pl SuperFAST Wildcard SSL

To validate these secure server certificates, CYBER_FOLKS S.A. checks that the Subscriber has control over the Domain name at the time the Subscriber submitted its enrolment certificates by reviewing the application information provided by the applicant (as per Section 1.3 of this CPS); and

a) Reviewing domain name ownership records publicly available through Internet approved global domain registrars and using generic e-mails which ordinarily are only available to person(s) controlling the domain name administration, for example, webmaster@ . . ., postmaster@ . . ., admin@; or
b) Requesting documentation that verifies control of the domain.

1.2.3. Domeny.pl Secure IT OV Free / Domeny.pl Smart SSL

CYBER_FOLKS S.A. operates a website identity assurance database referred to as IdAuthority. The database contains pre-validated identification records for known domain names and uses automated algorithms to marry domain name ownership records (from global domain name registrars) with company ownership identification records (from official government and third party company information sources).
If IdAuthority contains sufficient pre-validated records for the domain name used in an application, CYBER_FOLKS S.A. may employ the data held by IdAuthority to expedite the validation process. If application data matches the records held by IdAuthority, manual validation intervention is not required. In the event that the application data does not match the prevalidated records, the application is processed manually by a CYBER_FOLKS S.A. validation officer in accordance with the two-step process outlined in section 1.2.1 of this CPS.

1.2.4. Domeny.pl Smart Plus SSL/ Domeny.pl Professional SSL/ Domeny.pl Professional Wildcard SSL/ Domeny.pl

Safe SSL/ Domeny.pl Safe Plus SSL/ Domeny.pl SuperSafe Wildcard SSL
These certificates are processed by a CYBER_FOLKS S.A. validation officer in accordance with the process outlined in section 1.2.1
of this CPS. CYBER_FOLKS S.A. may employ the data held by IdAuthority to expedite the validation process. If application data matches the records held by IdAuthority, manual validation intervention is not required. In the event that the application data does not match the pre-validated records, the application is processed manually by a CYBER_FOLKS S.A. validation officer in accordance with the process outlined in section 1.2.1 of this CPS.

1.2.5. Domeny.pl Intranet SSL

Intranet certificate applications are only accepted for servers on internal networks, which are defined as non-Fully Qualified Domain Names and non-public IP addresses. During the application process CYBER_FOLKS S.A. verifies in real time that the common name (server name) submitted in the application is neither a Domain Name nor a publicly available IP address. Upon successful verification that the Intranet certificate cannot be used publicly on the Internet, the certificate will be issued.
CYBER_FOLKS S.A. validates that an Intranet certificate cannot be used as a public certificate. As the Intranet certificate is restricted for use only within a closed network, the company identity associated with the certificate need not, nor is, validated.

1.2.6. PERSONAL SECURE EMAIL CERTIFICATE

The Personal Secure Email Certificate is persona non-validated. CYBER_FOLKS S.A. only validates the right for the applicant to use the submitted email address. This is achieved through the delivery via email of unique login details to online certificate collection facilities hosted by CYBER_FOLKS S.A. The login details are sent via email to the address submitted during the certificate application.
Once logged into the online certificate collection facilities and prior to the installation of the Personal Secure Email Certificate, CYBER_FOLKS S.A. validates using an automated cryptographic challenge that the applicant holds the private key associated with the public key submitted during the application process. If the automated challenge is successful, CYBER_FOLKS S.A. will release the digital certificate to the subscriber.

1.2.7. CODE SIGNING CERTIFICATE

Code Signing Certificates and Time Stamping Certificates are processed by a CYBER_FOLKS S.A. validation officer in accordance with the process outlined in section 1.2.1 of this CPS. CYBER_FOLKS S.A. may employ the data held by IdAuthority to expedite the validation process. If application data matches the records held by IdAuthority, manual validation intervention is not required. In the event that the application data does not match the pre-validated records, the application is processed manually by a CYBER_FOLKS S.A. validation officer in accordance with the process outlined in section 1.2.1 of this CPS.

1.3. VALIDATION INFORMATION FOR CERTIFICATE APPLICATION

Applications for CYBER_FOLKS S.A. certificates are supported by appropriate documentation to establish the identity of an applicant.
From time to time, CYBER_FOLKS S.A. may modify the requirements related to application information for individuals, to respond to CYBER_FOLKS S.A.'s requirements, the business context of the usage of a digital certificate, or as prescribed by law.

1.3.1. APPLICATION INFORMATION FOR ORGANIZATIONAL APPLICANTS

The following elements are critical information elements for a CYBER_FOLKS S.A. certificate issued to an Organization. Those elements marked with PUBLIC are present within an issued certi_cate and are therefore within the public domain.
Those elements not marked with PUBLIC remain confidential in line with the privacy and protection of data provisions outlined in this CPS.

- Legal Name of the Organization (PUBLIC)
- Organizational unit (PUBLIC)
- Street, city, postal code, country (PUBLIC)
- National Court Registry Number, TIN, Statistical Number (PUBLIC)
- VAT-number (if applicable)
- Server Software Identification
- Payment Information

- Administrator contact full name, email address and telephone
- Billing contact persons and organizational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber agreement, signed (if applying out of bands)

1.3.2. SUPPORTING DOCUMENTATION FOR ORGANIZATIONAL APPLICANTS

Documentation requirements for Organizational applicants include any / all of the following:

- Articles of Association
- Business License
- Certificate of Compliance
- Certificate of Incorporation
- Certificate of Authority to Transact Business
- Tax Certification
- Corporate Charter
- Official letter from an authorized representative of a government organization
- Official letter from office of Dean or Principal (for Educational Institutions)
- Domeny.pl may accept at its discretion other official organizational documentation supporting an application.

1.3.3. APPLICATION INFORMATION FOR INDIVIDUAL APPLICANTS

The following elements are critical information elements for a CYBER_FOLKS S.A. certificate issued to an individual:

- Legal Name of the Individual (PUBLIC)
- Organizational unit (PUBLIC)
- Street, city, postal code, country (PUBLIC)
- VAT-number (if applicable)
- Server Software Identification
- Payment Information
- Administrator contact full name, email address and telephone
- Billing contact persons and organizational representative
- Fully Qualified Domain Name / Network Server Name / Public or Private IP (PUBLIC)
- Public Key (PUBLIC)
- Proof of right to use name
- Proof of existence and organizational status of the Organization
- Subscriber agreement, signed (if applying out of bands)

1.3.4. SUPPORTING DOCUMENTATION FOR INDIVIDUAL APPLICANTS

Documentation requirements for Individual applicants shall include identification elements such as:

- Passport
- Driving License
- Bank statement

CYBER_FOLKS S.A. may accept at its discretion other official documentation supporting an application.

1.4. VALIDATION REQUIREMENTS FOR CERTIFICATE APPLICATIONS

Upon receipt of an application for a digital certificate and based on the submitted information, CYBER_FOLKS S.A. confirms the following information:

- The certificate applicant is the same person as the person identified in the certificate request.
- The certificate applicant holds the private key corresponding to the public key to be included in the certificate.
- The information to be published in the certificate is accurate, except for non-verified subscriber information.
- Any agents who apply for a certificate listing the certificate applicant's public key are duly authorized to do so.

In all types of CYBER_FOLKS S.A. certificates, the subscriber has a continuous obligation to monitor the accuracy of the submitted information and notify CYBER_FOLKS S.A. of any changes that would affect the validity of the certificate. Failure to comply with the obligations as set out in the subscriber agreement will result in the revocation of the Subscriber's Digital Certificate without further notice to the Subscriber and the Subscriber shall pay any Charges payable but that have not yet been paid under the Agreement.

1.4.1. THIRD PARTY CONFIRMATION OF BUSINESS ENTITY INFORMATION

CYBER_FOLKS S.A. may use the services of a third party to confirm information on a business entity that applies for a digital certificate. CYBER_FOLKS S.A. accepts confirmation from third party organizations, other third party databases and government entities.

CYBER_FOLKS S.A.'s controls may also include National Court Registry transcripts that confirm the registration of the applicant company and state the members of the board, the management and Directors representing the company.

CYBER_FOLKS S.A. may use any means of communication at its disposal to ascertain the identity of an organizational or individual applicant. CYBER_FOLKS S.A. reserves right of refusal in its absolute discretion.

1.4.2. SERIAL NUMBER ASSIGNMENT

CYBER_FOLKS S.A. assigns certificate serial numbers that appear in CYBER_FOLKS S.A. certificates. Assigned serial numbers are unique.

1.5. TIME TO CONFIRM SUBMITTED DATA

CYBER_FOLKS S.A. makes reasonable efforts to confirm certificate application information and issue a digital certificate within reasonable time frames.

CYBER_FOLKS S.A. assures that all certificates will be issued within 2 working days after the receipt of all required validation information as per this CPS.

1.6. APPROVAL AND REJECTION OF CERTIFICATE APPLICATIONS

Following successful completion of all required validations of a certificate application CYBER_FOLKS S.A. approves an application for a digital certificate.

If the validation of a certificate application fails, CYBER_FOLKS S.A. rejects the certificate application.

CYBER_FOLKS S.A. reserves its right to reject applications to issue a certificate to applicants if, on its own assessment, by issuing a certificate to such parties the good and trusted name of CYBER_FOLKS S.A. might get tarnished, diminished or have its value reduced and under such circumstances may do so without incurring any liability or responsibility for any loss or expenses arising as a result of such refusal.

Applicants whose applications have been rejected may subsequently re-apply.

1.7. CERTIFICATE ISSUANCE AND SUBSRIBER CONSENT

CYBER_FOLKS S.A. issues a certificate upon approval of a certificate application. A digital certificate is deemed to be valid at the moment a subscriber accepts it (refer to section 1.9 of this CPS). Issuing a digital certificate means that CYBER_FOLKS S.A. accepts a certificate application.

1.8. CERTIFICATE VALIDITY

Certificates are valid upon issuance by CYBER_FOLKS S.A. and acceptance by the subscriber. Generally, the certificate validity period will be as specified in the standard Subscriber Agreement, however CYBER_FOLKS S.A. reserves the right to offer validity periods outside of this standard validity period.

1.9. CERTIFICATE ACCEPTANCE BY SUBSCRIBERS

An issued certificate is either delivered via email or installed on a subscriber's computer / hardware security module through an online collection method. A subscriber is deemed to have accepted a certificate when:

- the subscriber uses the certificate, or
- 30 days pass from the date of the issuance of a certificate

1.10. VERIFICATION OF DIGITAL SIGNATURES

Verification of a digital signature is used to determine that:

- the private key corresponding to the public key listed in the signer's certificate created the digital signature, and
- the signed data associated with this digital signature has not been altered since the digital signature was created.

1.11. RELIANCE ON DIGITAL SIGNATURES

The final decision concerning whether or not to rely on a verified digital signature is exclusively that of the relying party. Reliance on a digital signature should only occur if:

- the digital signature was created during the operational period of a valid certificate and it can be verified by referencing a validated certificate;
- the relying party has checked the revocation status of the certificate by referring to the relevant Certificate Revocation Lists and the certificate has not been revoked;
- the relying party understands that a digital certificate is issued to a subscriber for a specific purpose and that the private key associated with the digital certificate may only be used in accordance with the usages suggested in the CPS and named as Object Identifiers in the certificate profile; and
- the digital certificate applied for is appropriate for the application it is used in.

Reliance is accepted as reasonable under the provisions made for the relying party under this CPS and within the relying party agreement. If the circumstances of reliance exceed the assurances delivered by Domeny.pl under the provisions made in this CPS, the relying party must obtain additional assurances. Warranties are only valid if the steps detailed above have been carried out.

1.12. CERTIFICATE SUSPENSION

CYBER_FOLKS S.A. does not utilize certificate suspension.

1.13. CERTIFICATE REVOCATION

Revocation of a certificate is to permanently end the operational period of the certificate prior to reaching the end of its stated validity period. CYBER_FOLKS S.A. may revoke a digital certificate if any of the following occur:

- There has been loss, theft, modification, unauthorized disclosure, or other compromise of the private key associated with the certificate;
- The Subscriber or CYBER_FOLKS S.A. has breached a material obligation under this CPS or the relevant Subscriber Agreement;

- Either the Subscriber’s or CYBER_FOLKS S.A.’s obligations under this CPS or the relevant Subscriber Agreement are delayed or prevented by a natural disaster, computer or communications failure, or other cause beyond the person's reasonable control, and as a result another person’s information is materially threatened or compromised;
- There has been a modification of the information pertaining to the Subscriber that is contained within the certificate;
- A personal identification number, Private Key or password has, or is likely to become known to someone not authorized to use it, or is being or is likely to be used in an unauthorized way;
- A Subscriber's Digital Certificate has not been issued in accordance with the policies set out in this CPS;
- The subscriber has used the Subscription Service contrary to law, rule or regulation, or CYBER_FOLKS S.A. reasonably believes that the Subscriber is using the certificate, directly or indirectly, to engage in illegal or fraudulent activity;
- The certificate was issued to persons or entities identified as publishers of malicious software or that impersonated other persons or entities;
- The certificate was issued as a result of fraud or negligence;

The certificate, if not revoked, will compromise the trust status of CYBER_FOLKS S.A.;

1.13.1. REQUEST FOR REVOCATION

The Subscriber can request revocation of a certificate. Prior to the revocation of a certificate CYBER_FOLKS S.A. will verify that the revocation request has been:

- Made by the organization or individual entity that has made the certificate application.
- CYBER_FOLKS S.A. employs the following procedure for authenticating a revocation request:
- The revocation request must be sent by the Administrator contact associated with the certificate application.
- CYBER_FOLKS S.A. may if necessary also request that the revocation request be made by either / or the organizational contact and billing contact.
- Upon receipt of the revocation request CYBER_FOLKS S.A. will request confirmation from the known administrator out of bands contact details, either by telephone or by fax.
- CYBER_FOLKS S.A. validation personnel will then command the revocation of the certificate and logging of the identity of validation personnel and reason for revocation will be maintained in accordance with the logging procedures covered in this CPS.

1.13.2. EFFECT OF REVOCATION

Upon revocation of a certificate, the operational period of that certificate is immediately considered terminated.

The serial number of the revoked certificate will be placed within the Certificate Revocation List (CRL) and remains on the CRL until some time after the end of the certificate’s validity period.

An updated CRL is published every 24 hours; however, under special circumstances the CRL may be published more frequently.

1.14. RENEWAL

Depending on the option selected during application, the validity period of CYBER_FOLKS S.A. certificates is detailed in the relevant field within the certificate.

Renewal fees are detailed on the official CYBER_FOLKS S.A. websites and within communications sent to subscribers approaching the certificate expiration date.

Renewal application requirements and procedures are the same as those employed for the application validation and issuance requirements detailed for new customers.

1.15. NOTICE PRIOR TO EXPIRATION

CYBER_FOLKS S.A. shall make reasonable efforts to notify subscribers via e-mail of the imminent expiration of a digital certificate.

Notice shall ordinarily be provided within a 60-day period prior to the expiry of the certificate.