1. Introduction

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. INTRODUCTION

cyber_Folks S.A. ("cyber_Folks S.A., "CA") is a company that issues digital certificates to various subscribing entities, including private and public companies and individuals. Domeny.pl performs functions associated with public key operations which include receiving application requests for, issuing, revoking and renewing digital certificates and publication of Certificate Revocation Lists (CRL) and an Online Certificate Status Protocol (OCSP).

1.1. GENERAL

This document is the cyber_Folks S.A. Certification Practice Statement (CPS). The cyber_Folks S.A. CPS outlines the legal, commercial and technical principles and practices that cyber_Folks S.A. employs in approving, issuing, using, and managing certification services. This includes approving, issuing, using and managing Digital Certificates and maintaining a X.509 Certificate based public key infrastructure (PKIX). cyber_Folks S.A. may update and supplement this CPS with amendments in order to provide for additional product offerings and to comply with certain regulatory or industry standards and requirements.
The CPS is only one of many documents that are relevant to cyber_Folks S.A.'s certificate issuance practices. Other important documents include the cyber_Folks S.A. subscriber agreement, the relying party agreement, and other ancillary agreements that are posted on the cyber_Folks S.A. repository. These documents obligate parties using or relying on a cyber_Folks S.A. digital Certificate to meet a certain minimum criteria prior to their use or reliance on a cyber_Folks S.A. Certificate.

1.2. DOCUMENT NAME AN IDENTIFICATION

This document is the cyber_Folks S.A. CPS version 1.0, which was approved for publication on https://www.certy_katyssl.pl/repository by cyber_Folks S.A. Policy Authority. The CPS is a public statement of the practices of cyber_Folks S.A. and the conditions of issuance, revocation and renewal of a Certificate issued under cyber_Folks S.A.'s PKI hierarchy.
The cyber_Folks S.A. Policy Authority is responsible for determining the suitability of Certificate policies illustrated within the CPS. The Authority is also responsible for determining the suitability of proposed changes to the CPS prior to the publication of an amended edition.
Upon the Policy Authority accepting such changes deemed by the CA's Policy Authority to have significant impact on the users of this CPS an updated edition of the CPS will be published at the cyber_Folks S.A. repository (available at https://www.certy_katyssl.pl/repository), with seven (7) days notice given of upcoming changes and suitable
incremental version numbering used to identify new editions.
Revisions not denoted "significant" are those deemed by the CA's Policy Authority to have minimal or no impact on subscribers and relying parties using Certificates and CRLs issued by CA. Such revisions may be made without notice to users of the CPS and without changing the version number of this CPS.

1.3. CONFORMITY WITH APPLICABLE STANDARDS

The practices specified in this CPS have been designed to meet or exceed the requirements of generally accepted and developing industry standards related to the operation of CAs.

1.4. DIGITAL CERTIFICATE POLICY OVERVIEW

A digital Certificate is formatted data that cryptographically binds an identified subscriber with a public key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital Certificates are used in commercial environments as a digital equivalent of an identification card.

1.5. cyber_Folks S.A. CERTIFICATION AUTHORITY

In its role as a Certification Authority (CA) cyber_Folks S.A. provides Certificate services within the cyber_Folks S.A. PKI. The cyber_Folks S.A. CA will:

- Conform its operations to the CPS (or other CA business practices disclosure), as the same may from time to time be modified by amendments published in the Domeny.pl repository (https://www.certy_katyssl.pl/repository).
- Issue and publish certificates in a timely manner in accordance with the issuance times set out in this CPS.
- Distribute issued certificates in accordance with the methods detailed in this CPS.
- Notify subscribers via email of the imminent expiry of their Domeny.pl issued certificate (for a period disclosed in this CPS).

1.6. REGISTRATION AUTHORITIES

cyber_Folks S.A. does not employ any Registration Authorities.

1.7. SUBSCRIBERS

Subscribers are individuals, companies, or other entities that use cyber_Folks S.A.'s PKI services to provide supported transactions and communications. Subscribers are identified in and have the private key corresponding to the public key listed in an issued Certificate. Prior to being issued a Certificate, an applicant (a potential subscriber) must submit an application accompanied by certain verification information. cyber_Folks S.A. will only issue a Certificate to an applicant after the applicant has been approved and verified by cyber_Folks S.A.

In certain circumstances, cyber_Folks S.A. may issue a Certificate to an individual or entity that is different from the entity which actually applied for the Certificate. In such circumstances, the Subject of the Certificate will be the entity whose credentials have been submitted, and the term Subscriber shall apply to the entity which contracted with cyber_Folks S.A. for the issuance of the Certificate. Regardless of the Subject listed in the Certificate, the Subscriber always has the responsibility of ensuring that the Certificate is only used appropriately.

1.8. RELYING PARTIES

Relying parties use cyber_Folks S.A.'s PKI services to perform certain transactions, communications, or functions and may reasonably rely on issued Certificates and/or digital signatures that contain a verifiable reference to a public key that is listed in the subscriber Certificate. Not all of cyber_Folks S.A.'s Certificate products are intended to be used in e-commerce transactions or environments, and parties who rely on such Certificates do not qualify as a relying party.

Digital Certificates do not guarantee that a Certificate holder has good intentions or that the Certificate holder will be an ethical business operation. Relying Parties should always independently examine each Certificate holder to determine whether the Certificate owner is ethical and trustworthy.

1.9. OTHER PARTICIPANTS (RESELLERS)

cyber_Folks S.A. operates a network of resellers that allows authorized agents of cyber_Folks S.A. to integrate cyber_Folks S.A. digital Certificates into their own product portfolios. Resellers are

responsible for referring digital Certificate customers cyber_Folks S.A. cyber_Folks S.A. not the Reseller, maintains full control over the Certificate lifecycle process, including application, issuance, renewal and revocation. All Resellers are required to provide proof of organizational status and must enter into a Reseller agreement with cyber_Folks S.A. that requires them to comply with this CPS prior to being provided with Reseller status and facilities. Unless otherwise noted, all Certificates provided by Domeny.pl are also available through its Reseller program.

1.10. CERTIFICATE USAGE (GENERAL)

A digital Certificate is formatted data that cryptographically binds an identified subscriber to a public key. A digital Certificate allows an entity taking part in an electronic transaction to prove its identity to the other participants in such transaction. Certificates may be issued for individuals, organizations, government entities, educational institutions, or infrastructure components such as firewalls, routers, or other security devices.

1.11. PROHIBITED CERTIFICATE USE

Certificates may only be used in accordance with their intended purpose and in compliance with all applicable laws and regulations. Certificates may not be used to complete or assist in performing any transaction that is prohibited by law.
Each party using or relying on a Certificate shall be bound by and comply with the terms and conditions set forth in the applicable agreement between the party and cyber_Folks S.A. Low assurance Certificates may not be used as proof of identity and may not be held forth as establishing the legitimacy of the Certificate holder's business operations.
Digital Certificates do not guarantee that a Certificate holder has good intentions or that the Certificate holder will be an ethical business operation.
Certificates may not be used for any application requiring fail-safe performance systems such as the operation of nuclear power facilities, air traffic control systems, weapon control systems, or any other system where a failure of the system could cause any form of damage.

1.12. DEFINITIONS AND ACRONYMS

Acronyms:
CA Certificate Authority
CPS Certification Practice Statement
CRL Certificate Revocation List
PKI Public Key Infrastructure
PKIX Public Key Infrastructure (based on X.509 Digital Certificates)
SGC Server Gated Cryptography
SSL Secure Sockets Layer
URL Uniform Resource Locator
X.509 The ITU-T standard for Certificates and their corresponding authentication framework

Definitions:
Applicant: The Applicant is an entity applying for a Certificate.
Certificate: A message that, at least, states a name or identifies the CA, identifies the Subscriber, contains the Subscriber's public key, and contains a serial number.
Subscriber: The Subscriber is an entity that has been issued a Certificate.
Subscriber Agreement: The Subscriber Agreement is an agreement that must be read and accepted by an Applicant before applying for a Certificate. The Subscriber Agreement is specific to the Digital Certificate product type as presented during the product online order process.
Relying Party: The Relying Party is an entity that relies upon the information contained within the Certificate.

Relying Party Agreement: The Relying Party Agreement is an agreement that must be read and accepted by a Relying Party prior to validating, relying on or using a Certificate and is available for reference at https://www.certy_katyssl.pl/repository.