SIMARGL LLC

Certificate Policy

SIMARGL llc
Version 1.0; April 5, 2021

5900 Balcones Drive, STE 100
Austin, TX 78731

fax: 512 696 1474
phone: 512 696 1559

hello@simargl.llc

INTRODUCTION

SIMARGL llc is an innovator in the field of Internet foundation services, providing advanced software and Internet solutions critical to the building of online presence and ecommerce. The SIMARGL Public Key Infrastructure ("SIMARGL PKI") has been established to provide a variety of digital certificate services.

PKI PARTICIPANTS

SIMARGL Policy Authority and Certification Authorities

The SIMARGL Policy manages SIMARGL Root Certificate Authorities and Intermediate CAs Authority. SIMARGL'spolicies are designed to ensure that the SIMARGL PKI complies, in all material respects, with U.S. and international standards and regulations, CA/Browser Forum Guidelines, and relevant law on electronic signatures.

Types of Certificates

All certificates issued under this policy MUST be X.509 v3 certificates.

Subscribers

A Subscriber, as used herein, refers to both the subject of the Certificate and the entity that contracted with the Issuer CA for the Certificate's issuance. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant.

CAs are technically also subscribers of certificates within the SIMARGL Public PKI, either as the primary Certificate Authority issuing a self- signed Certificate to itself, or as an Issuer CA issued a Certificate by a superior CA. References to "end entities" and "subscribers" in this CP, however, apply only to end- user Subscribers.

Certificate Usage

Certificates issued under this CP may be used for the purposes designated in the key usage and extended key usage fields found in the Certificate.

Prohibited Certificate Uses

Certificates do not guarantee that the subject is trustworthy, honest, reputable in its business dealings, safe to do business with, or compliant with any laws. A Certificate only establishes that the information in the Certificate was verified as reasonably correct when the Certificate issued. Code signing Certificates do not indicate that the signed code is safe to install or is free from malware, bugs, or vulnerabilities.

Certificates shall be used only to the extent the use is consistent with applicable law, and in particular shall be used only to the extent permitted by applicable export or import laws.

Policy administration

Organization Administering theDocument

This CP and the relevant documents referenced herein are maintained by the SIMARGL llc, which can be contacted at:

5900 Balcones Drive, STE 100
Austin, TX 78731

fax: 512 696 1474
phone: 512 696 1559

hello@simargl.llc

Contact Person
Attn: Legal Counsel
5900 Balcones Drive, STE 100
Austin, TX 78731

fax: 512 696 1474
phone: 512 696 1559

hello@simargl.llc

Revocation Reporting Contact Person
Attn: Support
5900 Balcones Drive, STE 100
Austin, TX 78731

fax: 512 696 1474
phone: 512 696 1559

hello@simargl.llc

Initial identity validation
An Issuer CA may use any legal means of communication or investigation to ascertain the identity of an organizational or individual Applicant. The Issuer CA may refuse to issue a Certificate in its sole discretion.

Definitions and Acronyms
Applicant: means a person, entity, or organization applying for a Certificate but which has not yet been issued a Certificate, or a person, entity, or organization that currently has a Certificate or Certificates and that is applying for renewal of such Certificate or Certificates or for an additional Certificate or Certificates.
Applicant Representative: as defined in the Baseline Requirements.
Application Software Vendor: means a developer of Internet browser software or other software that displays or uses Certificates.
Certificate: means an electronic document that uses a digital signature to bind a Public Key and an identity.
Key Pair: means a Private Key and its associated Public Key.
Private Key: means the Key of a Key Pair that is kept secret by the holder of the Key Pair and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.
Public Key: means the Key of a Key Pair that the holder of the may publicly disclose corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.
Subscriber: means either the entity identified as the subject in the Certificate.

CA Certification Authority
CP Certificate Policy
CRL Certificate Revocation List
PKI Public Key Infrastructure
X.509 The ITU-T standard for Certificates and their corresponding authentication framework.
ITU International Telecommunication Union

ITU-T ITU Telecommunication Standardization Sector

Repositories
The CAs maintain the Repositories to allow access to Certificate-related and Certificate revocation information. The information in the Repositories is accessible through a web interface, available on a 24x7 basis and is periodically updated as set forth in this CP. The Repositories are the only approved source for CRL and other information about Certificates.
The CA will adhere to the latest version of the CP published in the Repository.
The Repository can be accessed at https://simargl.llc/repository/
Web pages that can be used by ASVs to test their software with Certificates that chain up to each publicly trusted Root Certificate are hosted at https://simargl.llc/repository/
Publication of Certification Information
The CA publishes its CP, CA Certificates, Subscription Agreements, Relying Party Agreements, and CRLs in the Repositories.

Certificate application
Who Can Submit a Certificate Application
SIMARGL llc departments, locations, offices.

Key pair and certificate usage
Subscriber Private Key and CertificateUsage
The certificate shall be used lawfully in accordance with SIMARGL's Subscriber Agreement the terms of this CP. All Subscribers shall protect their Private Keys from unauthorized use or disclosure by third parties and shall use their Private Keys only for their intended purpose.

Relying Party Public Key and CertificateUsage
Relying Parties shall use software that is compliant with X.509 and applicable IETF PKIX standards. The Issuer CA shall specify restrictions on the use of a Certificate through certificate extensions and shall specify the mechanism(s) to determine certificate validity (CRLs and OCSP).
Relying Parties must process and comply with this information in accordance with their obligations as Relying Parties. A Relying Party should use discretion when relying on a Certificate and should consider the totality of the circumstances and risk of loss prior to relying on a Certificate. Relying on a digital signature or Certificate that has not been processed in accordance with applicable standards may result in risks to the Relying Party. The Relying Party is solely responsible for such risks. If the circumstances indicate that additional assurances are required, the Relying Party must obtain such assurances before using the Certificate.

Certificate revocation and suspension
Revocation of a Certificate permanently ends the operational period of the Certificate prior to the Certificate reaching the end of its stated validity period. Prior to revoking a Certificate, the Issuer CA shall verify that the revocation request was made by Subscribers. Other parties may submit Certificate Problem Reports to SIMARGL to report reasonable cause to revoke the Certificate. Issuer CAs must provide evidence of the revocation authorization to SIMARGL upon request.

Circumstances for Revocation
The Issuer CA shall revoke a Certificate within 24 hours after receipt and confirming one or more of the following occurred:
1. The Subscriber requests in writing that the Issuer CA revoke the Certificate;

2. The Subscriber notifies the Issuer CA that the original Certificate Request was not authorized and does not retroactively grant authorization;
3. The Issuer CA obtains evidence that the Subscriber's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise;

Revocation Checking Requirement for RelyingParties
Prior to relying on the information listed in a Certificate, a Relying Party shall confirm the validity of each Certificate in the certificate path in accordance with IETF PKIX standards, including checks for certificate validity, issuer-to-subject name chaining, policy and key use constraints, and revocation status through CRLs responders identified in each Certificate in the chain.

CRL Issuance Frequency
CRL issuance is comprised of CRL generation and publication. For Issuer CAs and online intermediate CAs, the interval between CRL issuance shall not exceed seven days and the value of the nextUpdate field is not be more than ten days beyond the value of the thisUpdate field. For Root CAs and Intermediate CAs that are operated in an off-line manner, routine CRLs may be issued less frequently than specified above, provided that the CA only issues CA Certificates, certificate-status-checking Certificates, and internal administrative Certificates. CRL issuance intervals for such offline CAs are no greater than 6 months and within 24 hours after revoking a Subordinate CA Certificate, and the value of the nextUpdate field is not more than twelve months beyond the value of the thisUpdate field.

On-line Revocation/Status Checking Availability
The Issuer CA shall ensure that the certificate status information distributed by it on-line meets or exceeds the requirements for CRL issuance.

End of subscription
The Issuer CA shall allow Subscribers to end their subscription to certificate services by having their Certificate revoked or by allowing the Certificate or applicable Subscriber Agreement to expire without renewal.

Physical controls
The CA maintains controls to provide reasonable assurance that CA facilities and equipment are protected from environmental hazards.

Site location and construction
No stipulation.

Physical access
No stipulation

Power and air conditioning
No stipulation

Water exposures
No stipulation.

Fire prevention and protection
No stipulation.

Media storage
No stipulation.

Waste disposal
No stipulation.

Off-site backup
No stipulation.

Number of Persons Required Per Task
The Issuing CA will utilize commercially reasonable practices to ensure that one person acting alone cannot circumvent safeguards.
The Issuing CA must ensure that no single Individual may gain access to End Entity Private Keys stored by the Issuing CA. At a minimum, procedural or operational mechanisms must be in place for Key recovery, such as a Split-Knowledge Technique, to prevent the disclosure of the Encryption Key to an unauthorized Individual.

Technical security controls
Key Pair Generation
Key Pairs for all PKI Service Providers and End Entities must be generated in such a way that the Private Key is not known by other than the Key holder.

Public Key Delivery to Certificate Issuer
Subscribers should deliver their Public Keys to the Issuer CA in a secure fashion and in a manner that binds the Subscriber's verified identity to the Public Key.

CA Public Key Delivery to Relying Parties
The Public Key corresponding to the Issuing CA's CA Private Signing Key may be delivered to Relying Parties in an online transaction in accordance with IETF PKIX Part 3, or other appropriate mechanism.

Key Sizes
Minimum Key length for other than elliptic curve base algorithm is 2048 bits and divisible by 8. Minimum Key length for elliptic curve group algorithm is 256 bits.

Key Usage Purposes (As per X.509 v3 Key Usage Field)
Keys may be used for authentication, non-repudiation, and data encryption. They may also be used for session Key establishment. CA Private Signing Keys are the only Keys permitted to be used for signing Certificates and CRLs. The Certificate Key Usage field must be used in accordance with PKIX-1 Certificate and CRL Profile. One of the following Key Usage values must be present in all Certificates: (i) Digital Signature; or (ii) Non-Repudiation. One of the following additional values must be present in CA Certificate-signing Certificates: (i) Key Cert Sign; or (ii) CRL Sign. The use of a specific Key is determined by the Key usage extension in the X.509 Certificate. This restriction is not intended to prohibit use of protocols (like the Secure Sockets Layer) that provide authenticated connections using Key management Certificates

Method of Destroying PrivateKey
The Issuer CA shall use individuals in trusted roles to destroy CA, RA, and status server Private Keys when they are no longer needed. Subscribers shall destroy their Private Keys when the corresponding Certificate is revoked or expired or if the Private Key is no longer needed. For

software cryptographic modules, the Issuer CA may destroy the Private Keys by overwriting the data. For hardware cryptographic modules, the Issuer CA may destroy the Private Keys by executing a “zeroize” command. Physical destruction of hardware is not required.

Certificate Operational Periods and Key Pair Usage Periods
Root CA Certificate 10 years.

Crl profile
If utilized, CRLs will be issued in the X.509. The CPS or other publicly available document will identify the CRL extensions supported and the level of support for these extensions.
Version Number(s)
The Issuing CA must issue X.509 CRLs in accordance with the PKIX Certificate and CRL Profile.
CRL and CRL Entry Extensions
All End Entity PKI software must correctly process all CRL extensions identified in the Certificate and CRL profile.

CA Information
All non-public information stored locally on Issuing CA equipment (not in the Repository) is considered confidential for purposes of this Policy. Access to this information will be restricted to those with an official need-to-know in order to perform their official duties. Any information pertaining to Issuing CA management of SIMARGL Certificates, such as compilations of Certificate information, shall be treated as confidential.

Self-audits
The Issuer CA shall perform regular internal audits of its operations, personnel, and compliance with this CP using a randomly selected sample of Certificates issued since the last internal audit. Audits of other certificate types will be at the discretion of the CA to gain reasonable assurance of compliance to applicable root program requirements.
Responsibility to Protect Private Information
Each PKI Participant is responsible for protecting the confidentiality of private information that is in its possession, custody or control with the same degree of care that it exercises with respect to its own information of like importance, but in no event less than reasonable care, and shall use appropriate safeguards and otherwise exercise reasonable precautions to prevent the unauthorized disclosure of private information

Limitations of liability
Issuer CAs may limit their liability to any extent not otherwise prohibited by this CP, provided that the Issuer CA remains responsible for complying with this CP.

Termination
This CP as amended from time to time, shall remain in effect until replaced by a newer version.

Governing law
For disputes involving Qualified Certificates, the laws of the state of Texas shall govern the interpretation, construction, and enforcement of this CP and all proceedings related hereunder, including tort claims, without regard to any conflicts of law principles, and Travis County, Texas shall be the non-exclusive venue and shall have jurisdiction over such proceedings.

Force Majeure
SIMARGL is not liable for a delay or failure to perform an obligation under this CP to the extent

that the delay or failure is caused by an occurrence beyond SIMARGL's reasonable control. The operation of the Internet is beyond SIMARGL's reasonable control.
To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting SIMARGL.