TxNotaryForm.com

Certificate Policy

TXNotaryForm.com
Version 1.0; April 5, 2021

SIMARGL LLC

5900 Balcones Drive, STE 100
Austin, TX 78731

phone: 512 696 1559

hello@simargl.llc

Introduction

TXNOTARYFORM.COM is a location of SIMARGL llc.
The TXNOTARYFORM.com Public Key Infrastructure (“TXNOTARYFORM PKI”) has been established to provide digital certificate services. This TXNOTARYFORM.com Certificate Policy, the policy under which TXNOTARYFORM.COM establishes and operates a Public Key Infrastructure (“PKI”) for issuing Certificates that can be used in an interoperable manner with other X.509 PKIs.

This policy describes the roles, responsibilities, and relationships of the PKI Service Providers and End Entities (collectively “Participants”), and the rules and requirements for the Issuance, acquisition, management, and use of TXNOTARYFORM.COM Certificates to verify Digital Signatures and to encrypt and authenticate electronic communications.

This document defines the creation and management of X.509 Version 3 Public Key Certificates for use in applications requiring authentication of an End Entity, digital signing of content by an End Entity, digital signing of content by a content signer, and data or message confidentiality between networked computer-based systems and/or Individuals. Such applications include, but are not limited to electronic mail, the transmission of confidential information, signature of electronic documents.

This document specifies the policies TXNOTARYFORM.COM adopts to meet the current versions of the following policies, guidelines, and requirements

Name of Policy/Guideline/ Requirement Standard	Location of Source Document/Language
the Online Notary Public Commissioning System Texas State	https://www.sos.texas.gov/statdoc/digital.shtml

Types of Certificates

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

Subscribers

The Issuing CA may issue TXNOTARYFORM.com Certificates to the following classes of Subscribers:
Notary Public Texas and Online Notary Public Texas.

Certificate Usage

A digital Certificate (or 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.
TXNOTARYFORM.com Certificates are intended to support verification of Digital Signatures in applications where: (i) the identity of communicating parties needs to be authenticated; (ii) a message or file needs to be bound to the identity of its originator by a signature; and/or (iii) the integrity of the file or message has to be assured.

Appropriate Certificate Uses

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. However, the sensitivity of the information processed or protected by a Certificate varies greatly, and each Relying Party must evaluate the application environment and associated risks before deciding on whether to use a Certificate issued under this CP.

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:

TXNotaryForm.com
5900 Balcones Drive, STE 100
Austin, TX 78731

fax: 512 696 1474
phone: 512 696 1559
info@txnotaryform.com

Contact Person

Attn: Legal Counsel
TXNotaryForm.com
5900 Balcones Drive, STE 100
Austin, TX 78731

fax: 512 696 1474
phone: 512 696 1559
info@txnotaryform.com

Revocation Reporting Contact Person

Attn: Support
TXNotaryForm.com
5900 Balcones Drive, STE 100
Austin, TX 78731

fax: 512 696 1474
phone: 512 696 1559
info@txnotaryform.com

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://txnotaryform.com/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://txnotaryform.com/repository/

Publication of Certification Information

The CA publishes its CP, CA Certificates, Subscription Agreements, Relying Party Agreements, and CRLs in the Repositories.

Uniqueness of Names

Document Signing Certificates Requiring A Notary Public Name and email.

Certificate application

Who Can Submit a CertificateApplication

- Notary Public Texas
- Online NotaryPublic Texas
- Insurance agents on behave of Notary Public Texas
- Insurance agents on behave of Online Notary Public Texas
- Bond company agent on behave of Notary Public Texas
- Bond company agent on behave of Online Notary Public Texas

Enrollment Process and Responsibilities

Applicants are responsible for submitting sufficient information and documentation for the Issuer CA to perform the required verification of identity prior to issuing a Certificate.

Certificate Update

Updating a TXNotaryForm.com Certificate means creating a new- TXNotaryForm.com Certificate that:

- Has the same or a different Public Key
- Has a different serial number and
- Differs in one or more other fields from the old Certificate.

For example, the Issuing CA may choose to update a TXNotaryForm.com Certificate of a Subscriber who gains an authorization. The old Certificate may or may not be revoked but must not be further re-keyed, renewed, or updated.

Identification and Authentication for Re-Key After Revocation

Revoked or expired TXNotaryForm.com Certificates may not be re-keyed, renewed, or updated. Applicants with revoked or expired TXNotaryForm.com Certificates will, upon reapplication, be subject to the same Identity Proofing procedures as first-time Applicants.

Identification and authentication for revocation requests

An End Entity may request Revocation or suspension of his, her, or its TXNotaryForm.com Certificate at any time for any reason. The Issuing CA, when faced with such a request, must adopt authentication mechanisms that balance the need to prevent unauthorized requests against the need to quickly revoke or suspend TXNotaryForm.com Certificates. Therefore, in the event the request is electronically submitted, the identity of the requestor may be authenticated on the basis of the Digital Signature used to submit the message.

Performing Identification and Authentication Functions

Applicants will complete a Certificate application and provide requested information in a form prescribed by the Issuing CA in accordance with this policy. An Applicant must also enter into a Certificate Agreement or Authorized Relying Party Agreement with the Issuing CA. All applications are subject to review, approval, and Acceptance by the Issuing CA. The Issuing CA may use the documents and data provided to verify Certificate information or reuse previous validations themselves. The data or document used in the prior validation is no more than end of commission prior to issuing the Certificate.

Certificate issuance

After all application and approval processes identified in this Policy are completed, the Issuing CA will:

- Issue the requested TXNotaryForm.com Certificate;
- Notify the Applicant of the TXNotaryForm.com Certificate's Issuance; and
- Make the TXNotaryForm.com Certificate available to the Applicant for Acceptance.

Notification to Subscriber by the CA of Issuance of Certificate

The procedures for notifying the Applicant of the TXNotaryForm.com Certificate's Issuance, and the procedure used to deliver or make the Certificate available to the Applicant must be secure and confidential.

Conduct Constituting Certificate Acceptance

Upon Issuance and installation of the Certificate, Subscribers are to be provided with the contents of the Certificate in a human-readable form for their review. The Issuing CA should require that the Subscriber review the Certificate and affirmatively communicate Acceptance of its content at the end of the retrieval process.

Key pair and certificate usage

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.

Certificate modification

The Issuing CA may allow for Certificate modification for any of the following changes during the Certificate's Operational Period:

- Legal name due to marriage, divorce or court petition
- Email address or
- Any attribute/extension of a Certificate.

Who May Request Certificate Modification

Subscribers with valid Certificates are entitled to request email modification and replacements.

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 TXNotaryForm.com to report reasonable cause to revoke the Certificate. Issuer CAs must provide evidence of the revocation authorization to TXNotaryForm.com 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;

The Issuing CA should revoke a Certificate within 24 hours and must revoke a Certificate within 5 days if one or more of the following events take place:

- The Certificate no longer complies with the requirements in the relevant section of the CA/B Forum Baseline Requirements.
- The Issuing CA obtains evidence that the Certificate was misused.
- The Subscriber or the cross-certified CA breached a material obligation under this CP, or the relevant agreement.
- The Issuing CA confirms a material change in the information contained in the Certificate.
- The Issuing CA confirms that the Certificate was not issued in accordance with the CA/B Forum Baseline Requirements, this CP.
- The Issuing CA determines or confirms that any of the information appearing in the Certificate is inaccurate.
- The Issuing CA’s right to issue Certificates under the CA/B Forum Baseline Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL Repository.
- The Issuing CA confirms a demonstrated or proven method that exposes the Subscriber’s Private Key to compromised methods or if there is clear evidence that the specific method used to generate the Private Key was flawed.

The Issuing CA may revoke any Certificate in its sole discretion, even if the Issuing CA believes that:

- Either the Subscriber's or the Issuing CA's obligations under this CP are delayed or prevented by circumstances beyond the party's reasonable control, including computer or communication failure, and, as a result, another entity's information is materially threatened or compromised.
- The Issuing CA received a lawful and binding order from a government or regulatory body to revoke the Certificate.
- The Issuing CA ceased operations and did not arrange for another Certificate authority to provide Revocation support for the Certificates.
- The technical content or format of the Certificate presents an unacceptable risk to Application Software Providers, Relying Parties, or others.
- The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States.

The Issuing CA shall revoke a Certificate if the binding between the Subject and the Subject's Public Key in the Certificate is no longer valid or if an associated Private Key is compromised.

The Issuing CA will revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs:

- The Subordinate CA requests Revocation in writing.
- The Subordinate CA notifies the Issuing CA that the original Certificate request was not authorized and does not retroactively grant authorization.
- The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key compromise or no longer complies with the requirements in the relevant sections of the CA/B Forum Baseline Requirements.
- The Issuing CA obtains evidence that the CA Certificate was misused.
- The Issuing CA confirms that the CA Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement.
- The Issuing CA determines that any of the information appearing in the CA Certificate is inaccurate or misleading.
- The Issuing CA or the Subordinate CA ceases operations for any reason and has not arranged for another CA to provide Revocation support for the CA Certificate.
- The Issuing CA or the Subordinate CA's right to issue Certificates under the CA/B Forum Baseline Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL Repository.
- The technical content or format of the CA Certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties.

Who Can Request Revocation

Different parties may request Certificate Revocation as follows:

- The Issuing CA may summarily revoke Certificates within its domain.
- An Insurance agent or Bond company agent can request the Revocation of an End Entity's TXNotaryForm.com Certificate on behalf of the End Entity.
- An End Entity is authorized to request the Revocation of his, her, or its own Certificate.
- Additionally, Subscribers, Authorized Relying Parties, Application Software Suppliers, and other third parties may submit Certificate Problem Reports informing the Issuing CA of reasonable cause to revoke the Certificate. Other third parties may submit Certificate Problem Reports informing the Issuing CA of reasonable cause to revoke the Certificate.

Procedure for Revocation Request

As described in this Policy, a Certificate Revocation request should be promptly communicated to the

Issuing CA, either directly or through the Agent authorized to Accept such notices on behalf of the Issuing CA. A Certificate Revocation request may be communicated electronically if it is Digitally Signed with the Private Key of the End. Alternatively, the End Entity may request Revocation by contacting the Issuing CA or its Agent in person and providing adequate proof of identification in accordance with this Policy or an equivalent method.

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 CertificateIssuer
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.

- Protects e-mail messages;
- Document signing;
- Allows data to be signed with the current time;

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
End Entity Certificates - Commissioned Notary Public no later Expire Date.

Certificate, crl, profiles
Certificate profile

TXNotaryForm.com Certificates will contain Public Keys used to authenticate the sender of an electronic messages and verify the integrity of such messages -- i.e., Public Keys used for Digital Signature verification. TXNotaryForm.com Certificates will be issued in the X.509 version 3. Nothing in this Policy would require an Authorized Relying Party to use or process non-standard Certificates.

Crl profile

If utilized, CRLs will be issued in the X.509. The CP 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.

Responsibility to Protect Confidential Information

Private Key Information

Private Keys are sensitive and confidential information and, therefore, Private Keys should be held in strictest confidence.

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 TXNotaryForm.com 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.

Notice and Consent to Use Private Information

PKI Service Providers will not disclose any information deemed confidential under this section, to any third party, except when: (i) authorized by this Policy; (ii) required to disclose by law, governmental rule or regulation, or court order; or (iii) when necessary to effect an appropriate use of a TXNotaryForm.com Certificate. All requests for disclosure of information considered confidential under this section must be made in writing.
The Issuing CA may choose to further define or restrict its disclosure of Certificate-related information. Unless prohibited by law, a PKI Service Provider will give all interested persons or parties reasonable prior written notice before disclosing any information considered confidential under this section.

Intellectual property rights

A Private Key will be treated as the sole property of the legitimate holder of the TXNOtaryForm.com Certificate containing the corresponding Public Key.

Representations and warranties

No joint venture, partnership, trust, agency, or fiduciary relationship is established or deemed to be established among any of the parties using this Policy or the PKI established pursuant hereto. Issuance of TXNotrayform.com Certificates in accordance with this Policy does not make the Issuing CA, an agent, fiduciary, trustee, or other representative of Subscribers or Authorized Relying Parties.

PKI Service Providers assume no liability whatsoever in relation to the use of TXNotrayform.com Certificates or associated Key Pairs for any use other than in accordance with this Policy or related agreements. Each End Entity will indemnify and hold the PKI Service Providers and their respective directors, officers, employees, agents and affiliates harmless from any and all liability arising out of the End Entity's use of a TXNotrayform.com Certificate for other than its intended use.

The PKI Service Providers, and their employees, servants or agents, make no representations or warranties, express or implied, other than as expressly stated in this Policy or in an agreement between the PKI Service Provider and an End Entity. Except as expressly prohibited in this Policy, PKI Service Providers may disclaim all warranties and obligations of any type, including without limitation: (i) any warranty of merchantability; (ii) any warranty of fitness for a particular purpose; (iii) any warranty of accuracy of information provided; and (iv)any warranty of non-infringement.

The PMA, Issuing CAs, are neither intermediaries nor guarantors of the underlying transactions between End Entities. Recourse, liability and dispute resolution for claims solely between End Entities (e.g., claims of non-performance not related to Subscriber identity) shall be under applicable law. Claims against PKI Service Providers are limited to showing that the PKI Service Providers operated in a manner inconsistent with this Policy, t or a related agreement or warranty. PKI Service Providers are responsible to an Authorized Relying Party only if the Authorized Relying Party has complied with all obligations, terms, and conditions of this Policy and of the applicable Authorized Relying Party Agreement, and only to the extent otherwise allowed by this Policy.

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

TXNotaryForm.com 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 TXNotaryForm.com reasonable control. The operation of the Internet is beyond TXNotaryForm.com reasonable control.

To the extent permitted by applicable law, Subscriber Agreements and Relying Party Agreements shall include a force majeure clause protecting SIMARGL.