NIOC PSAP Credentialing Agency (PCA) Certificate Validation Guidelines

Abstract: This document provides the security requirements needed to support the secure validation for issuance of Certificates in NG9-1-1 by the PCA Certification Authorities (CAs) in the NG9-1-1 Public Key Infrastructure.

NG9-1-1 Interoperability Oversight Commission (NIOC) Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Validation Guidelines

V1.0.0
NIOC Approval: 2/9/2022

Prepared at the request of NIOC by:
National Emergency Number Association (NENA) 9-1-1 Core Services Committee, PCA Certificate Policy Working Group

Published by NIOC
Printed in USA

1 Background

This is a companion document to the NG9-1-1 Interoperability Oversight Commission (NIOC) Certificate Policy (CP). This CP is available at https://ng911ioc.org/library.[1] The CP states:

> *Certification Authorities (CAs), and the infrastructure they support, form the basis for one of the primary mechanisms for providing assurance of identity. The widely placed trust in CAs is at the heart of security mechanisms used to protect sessions and transactions for Next Generation 9-1-1 (NG9-1-1). National Emergency Number Association's (NENA's) i3 and associated standards require Transport Layer Security (TLS) throughout the ecosystem to allow for secure communications and a single shared root of trust to assist with interoperability. TLS relies on CAs to identify Servers and Clients. The root of trust in the NG9-1-1 Public Key Infrastructure (PKI) is the Public Safety Answering Point (PSAP) Credentialing Agency (PCA).*
>
> *The purpose of this document is to provide security requirements needed to support the secure issuance of Certificates in NG9-1-1 by the PCA CAs in the NG9-1-1 PKI. In particular, this document has been developed to provide an appropriate level of assurance to support government emergency services including public safety, and applications, i.e., a high level of assurance as defined in the Validation Policy (VP). The level of assurance refers to the strength of the Binding between the Public Key and the entity whose name is cited in the Certificate, the policies used to control the use of the corresponding Private Key, and the overall security provided by the PKI itself.*
>
> *The PCA is a functional element in the NENA i3 Standard for Next Generation 9-1-1 core services[2] which establishes a root of trust for the NG9-1-1 ecosystem to facilitate interoperable security between disparate NG9-1-1 environments. The i3 standard includes not only a shared root of trust to build a PKI, but it also standardizes how identities are conveyed across NG9-1-1, and what roles those identities have in the NG9-1-1 ecosystem. In addition to participating within a PKI in a trusted environment, the standardization of conveying identities and roles provides for powerful abilities to manage permissions and other security configurations in NG9-1-1 that work across different NG9-1-1 environments and disparate public safety systems. The PCA as set forth in this document supports all of the functionality as required by the i3 standard to provide a PCA.*[3]

While the CP provides for guidance on certificate issuance, management and how the PKI infrastructure is operated, the CP states throughout that validation procedures for Participants will be handled in a separate Validation Policy.[4] This document is that Validation Policy. It

---

[1] See NIOC Certificate Policy, available at https://ng911ioc.org/library/, last retrieved 5 May 2021 ("CP").

[2] See NENA STA-010.3-2021. Available at https://cdn.ymaws.com/www.nena.org/resource/resmgr/standards/nena-sta-010.3-2021_i3_stand.pdf. ("i3")

[3] See CP at "Foreword".

[4] See Id.

incorporates the whole of the CP by reference. As of this writing, that is version 1.01 of the CP dated 03/10/2021.

1.1 Governing Authority

The governance structure that represents the participants for a PKI is known as the Policy Authority (PA). The NG9-1-1 Interoperability Oversight Commission (NIOC) was convened by the NENA Executive Board to serve as the independent PA for the PCA. The PA is responsible for identifying the appropriate set of requirements for a given community and oversees the CAs that issue Certificates for that community.

1.2 Guidelines for the Issuance and Management of NG9-1-1 Certificates

NIOC utilized the CA/Browser Forum's Guidelines for the Issuance and Management of Extended Validation Certificates, also known as the Extended Validation Guidelines to create this document (the "Guidelines"). Version 1.7.2 of the Extended Validation Guidelines served as a baseline to establish the Guidelines for issuing NG9-1-1 certificates.[5]

These Guidelines describe an integrated set of technologies, protocols, identity proofing, lifecycle management, and auditing practices specifying the minimum requirements that must be met in order to issue and maintain NG9-1-1 Certificates. Subject information from valid NG9-1-1 Certificates can then be used in a special manner by certain relying-party software applications (e.g., Next Generation Core 9-1-1 Services [NGCS] applications) in order to provide users with a trustworthy confirmation of the identity and/or Role of an entity in NG9-1-1.

In NG9-1-1, every entity carries a certificate. Validation for NG9-1-1 is done in a manner largely in sync with prevailing guidelines for extended validation in operating commercial CA services, but with specific and substantial changes that reflect unique circumstances in NG9-1-1.

The trust chain that comprises the NG9-1-1 PKI sits at the heart of security and interoperability in NG9-1-1. Holding an NG9-1-1 Certificate affords an entity a substantial amount of privilege within the NG9-1-1 environment, as NENA's i3 and related standards describe hundreds of interactions that MUST be accepted so long as the interaction is initiated by an entity with an NG9-1-1 certificate. A malicious entity holding an NG9-1-1 Certificate presents substantial risk to the emergency calling infrastructure of the United States, Canada, Europe and beyond. Accordingly, issuance of an NG9-1-1 certificate requires a very high level of scrutiny and investigation prior to issuing a certificate.

As of this writing, these Guidelines assume a PKI that covers the NG9-1-1 systems of the United States. These Guidelines also assume an objective to establish interoperability with the emergency calling systems of Europe and Canada under the assumption that they will employ a

[5] Version 1.7.2 represented the Extended Validation Guidelines, as adopted by the CA/Browser Forum as of Ballot SC27, passed by the Forum on 19 February 2020 and effective as of 27 March 2020. Copyright © 2007-2020, members of the CA/Browser Forum. This work is licensed under a Creative Commons Attribution 4.0 International license.

substantially similar trust framework. These Guidelines assume an update to this document will be required in establishing such expansion or interoperability of the PKI beyond the United States.

1.3 Document History

Version	Description	Adopted	Effective
1.0.0	Initial NG9-1-1 Certificate Validation Guidelines development for NIOC	2/9/2022	2/9/2022

Table of Contents

2 Scope

These Guidelines for the issuance and management of NG9-1-1 Certificates describe certain of the minimum requirements that a CA must meet in order to issue Certificates for NG9-1-1 in accordance with NENA standards and in accordance with policies and procedures established by NIOC to establish a PKI for NG9-1-1. These Guidelines incorporate the requirements established by the NIOC CP by reference.

Entities can be CAs, Agencies, Users, Elements or Devices. Each of these entities is validated prior to issuance of a certificate in accordance with these Guidelines. The Root Certificate for the NG9-1-1 PKI is the PSAP Credentialing Agency (PCA), which is operated by NIOC.

3 Purpose

3.1 Purpose of NG9-1-1 Certificates

NG9-1-1 Certificates are intended to:

- sign certificates of subsidiary Intermediate Certification Authorities (ICAs)
- provide for interoperability in NG9-1-1 through explicit trust
- provide for security through establishing TLS within a PKI
- verify the authenticity of signed Records
- provide non-repudiation of signed Records
- express an entity identity and Role within the trust chain for NG9-1-1
- verify the authenticity of executable code in NG9-1-1.

NG9-1-1 Certificates MUST be used for some of these actions, and MAY be used for others as described in these Guidelines.

3.2 Types of NG9-1-1 Certificates

NG9-1-1 Certificates fall into multiple categories and are either CA Certificates credentialing a CA or an end-entity Certificate credentialing an Agency, Service, User, Element, or Role. Below is a summary of the types of NG9-1-1 Certificates allowable under these Guidelines.

Type of Cert	Description	Validation Done By
Root Certificate	The offline root certificate comprising the basis of the trust chain for the PKI.	Self-signed by the root CA in an auditable ceremony per the CP.
ICA Certificate	A certificate for an ICA.	The RA for the CP for a Tier-2 ICA, or the RA in the CPS governing the signing ICA.
Agency Certificate	A certificate issued to an agency. ID example: psap.fairfax.virginia.us	The RA for the ICA.

Type of Cert	Description	Validation Done By
Service Certificate	A certificate issued to a service instance in a particular NGCS or Agency	The RA or LRA for a CA with Delegated Authority to perform Validation
Element Certificate	A certificate issued to a physical or virtual entity that is addressable and has a unique identity (elementID)	The RA or LRA for a CA with Delegated Authority to perform Validation.
User Certificate (Agent)	A certificate issued to a person or automaton*. These are always issued by an ICA. ID example: dhandy@psap.fairfax.virginia.us	The RA or LRA for a CA with Delegated Authority to perform Validation.

*future work

3.3 Primary Purposes

The primary purposes of NG9-1-1 Certificates are described in the following subsections.

3.3.1 Explicit Assurances

NG9-1-1 Certificates focus on the identity of the Identifier[6] in the SubjectAltName in the Certificate as well as the behavior of the Identity within the NG9-1-1 PKI and chain of trust for NG9-1-1. As such, contrary to Certificates used for commercial purposes, an NG9-1-1 Certificate SHALL provide explicit assurances as to the following:

1. That the Identity named in the NG9-1-1 Certificate is a legitimate and trustworthy NG9-1-1 entity;
2. That the Identity named in the NG9-1-1 Certificate complies with applicable laws;
3. That it is "safe" to conduct NG9-1-1 operations with the Identity named in the NG9-1-1 Certificate.

The NG9-1-1 PKI policy requirements support the secure issuance of Certificates in NG9-1-1 by the PCA CAs. These policies reflect a High level of Assurance commensurate with NIST SP-800-63 series Identity Assurance Level 3.[7] A table outlining NIST Assurance levels is below:

[6] "Identifier" has the meaning as specified in i3 at Section 2.1.

[7] See NIST 800-63 at Section 6, Retrieved 2 November 2020 at: https://pages.nist.gov/800-63-3/sp800-63-3.html#sec6.

Impact Categories	Assurance Level		
	1	2	3
Inconvenience, distress or damage to standing or reputation	Low	Moderate	High
Financial loss or agency liability	Low	Moderate	High
Harm to agency programs or public interests	N/A	Low/Moderate	High
Unauthorized release of sensitive information	N/A	Low/Moderate	High
Personal Safety	N/A	Low	Moderate/High
Civil or criminal violations	N/A	Low/Moderate	High

3.3.2 Identify Certification Authorities in the NG9-1-1 PKI

The NG9-1-1 PKI includes two types of CAs: the Root Certification Authority, which is the PCA, and ICAs, which are either signed by the Root Certificate or are signed by an ICA in accordance with the CP.

3.3.3 Identify and Describe the Role(s) of Agents in the NG9-1-1 PKI

The NG9-1-1 PKI includes a population of Agents. Public safety personnel, the devices they use and/or devices that take actions throughout the PKI comprise this population of Agents. Agent Certificates include the identity of the Agent, their Agency affiliation and a list of their Roles in the NG9-1-1 PKI.

3.3.4 Identify and Describe the Role(s) of Elements in the NG9-1-1 PKI

The NG9-1-1 PKI includes a population of Elements and Services. Element or Service Certificates credential either Functional Elements or Services within the NG9-1-1 PKI as described in i3. An Element Certificate will include the identity of the Element, its Agency affiliation, and a list of its Role(s) in the NG9-1-1 PKI.

3.3.5 Identify and Describe Roles

Agents, Elements, Services and CAs hold one or more Roles in the NG9-1-1 PKI. These Roles are used to express what the Element or Agent is allowed to do within the PKI. When performing Validation, the Validator SHALL validate that the Applicant has a legitimate and valid purpose to act in one or more Roles within the NG9-1-1 PKI using the process as described below.

3.3.6 Secure Transactions Inside of NG9-1-1 Through Explicit Trust

Transactions in NG9-1-1 are allowed provided that the initiator presents credentials traceable to the PCA. By establishing a PKI with a shared root of trust, the NG9-1-1 community can safely and securely engage in transactions within and between different NG9-1-1 systems and can achieve interoperability by having a shared convention for establishing trustworthiness of entities between different systems as well as what Roles entities are allowed to perform between these systems.

3.3.7 Signing of Records

NG9-1-1 allows for the signing of Records, including records in a public safety communications logger or JSON payloads signed with JWS. When signing is required, records are signed with a Certificate traceable to the PCA.[8]

3.4 Secondary Purposes

Secondary purposes of NG9-1-1 are described in the following subsections.

3.4.1 Secure Transactions Into/Outside of the NG9-1-1 PKI Through Explicit Trust

It is a long-term objective to establish or investigate feasibility of establishing shared trust between the NG9-1-1 PKI and other PKIs for interoperability purposes, including the Federal Bridge Certification Authority, PKI(s) that may be established for any Public Safety Broadband Networks, the SHAKEN CA and/or PKIs established for next-generation emergency calling environments internationally that Relying Parties in the NG9-1-1 PKI have reason and need to interoperate with. Accordingly, it is a secondary purpose of NG9-1-1 Certificates to secure transactions and establish interoperability with other trust environments once trust is established between the PCA and any other Root CA.

3.5 Excluded Purposes

NG9-1-1 Certificates are not intended to be used outside of public safety for identity proofing for commercial or general identity proofing purposes, such as to secure access to a public website through TLS, electronically signing emails or documents unless as expressly required for interoperable NG9-1-1 communications or signing executable code for commercial applications unless used for NG9-1-1 or public safety operations.

3.6 Documents Incorporated by Reference and References

- NENA STA-010.2-2016, incorporated by reference
- NENA STA-010.3-2021, incorporated by reference
- NIOC CP v. 1.01 (Public Safety Answering Point (PSAP) Credentialing Agency (PCA) Certificate Policy), incorporated by reference
- CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates (v 1.6.4 and up) ("Baseline Requirements"), for reference only
- CA/Browser Forum Guidelines for the Issuance and Management of Extended Validation Certificates Guidelines v 1.7.2[9]

3.7 Definitions

Capitalized terms are defined in the Baseline Requirements and the CP except where provided below:

---

[8] See i3 at 5.10.

[9] Retrieved 22 June 2021 at https://cabforum.org/baseline-requirements-documents. \"Baseline Requirements"

Applicant: The entity or entities applying for a Certificate for a Subject.

Appropriate Authority: The governing body (whether governmental or otherwise) with legal or other official responsibility to certify the legitimacy of certain claims regarding a Subject or Applicant, such as the existence of a Public Safety Entity or Private Entity with a valid public safety purpose or specific information about a Subject or Applicant. An Appropriate Authority may maintain a Qualified Independent Information Source (QIIS) or Qualified Government Information Source (QGIS), in which case the QIIS or QGIS is sufficient to validate information and direct communication with the Appropriate Authority is not necessary.

Authority: A source other than the Certificate Approver, through which verification occurs that the Certificate Approver is expressly authorized by the Applicant, as of the date of the NG9-1-1 Certificate Request, to take the Request actions described in these Guidelines.

Authorization Domain Name: A domain name used for the purposes of Validation under these Guidelines.

Baseline Requirements: The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates as published by the CA/Browser Forum and any amendments to such document.

Business Entity: This entity has the same meaning as "Private Entity".

Certificate Approver: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve NG9-1-1 Certificate Requests submitted by other Certificate Requesters.

Certificate Requester: A natural person who is either the Applicant, employed by the Applicant, an authorized agent who has express authority to represent the Applicant, or a third party that completes and submits an NG9-1-1 Certificate Request on behalf of the Applicant.

Confirmation Request: An appropriate out-of-band communication requesting verification or confirmation of the particular fact at issue.

Confirming Person: A position within an Applicant's organization that confirms the particular fact at issue.

Contract Signer: A natural person who is either the Applicant, employed by the Applicant, or an authorized agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

Delegated Authority: The authorization to act on behalf of another entity for official purposes, such as to act under contract to a Public Safety Entity as a Certificate Requester for that Public Safety Entity, or to act as an RA or LRA.

Guidelines: This document.

NG9-1-1 Certificate: A certificate that contains subject information specified in these Guidelines and that has been validated in accordance with these Guidelines.

NG9-1-1 Certificate Renewal: The process whereby an Applicant who has a valid unexpired and non-Revoked NG9-1-1 Certificate makes an application, to the CA that issued the original certificate, for a newly issued NG9-1-1 Certificate for the same organizational name and Domain Name prior to the expiration of the Applicant's existing NG9-1-1 Certificate but with a new 'valid to' date beyond the expiry of the current NG9-1-1 Certificate and a new serial number.

NG9-1-1 Certificate Reissuance: The process whereby an Applicant who has a valid unexpired and non-revoked NG9-1-1 Certificate makes an application, to the CA that issued the original certificate, for a newly issued NG9-1-1 Certificate for the same organizational name and Domain Name prior to the expiration of the Applicant's existing NG9-1-1 Certificate but with a 'valid to' date that matches that of the current NG9-1-1 Certificate.

NG9-1-1 Certificate Request: A request from an Applicant to the CA requesting that the CA issue an NG9-1-1 Certificate to the Applicant, which request is validly authorized by the Applicant and signed by the Appropriate Authority.

NG9-1-1 Certificate Warranties: In conjunction with the CA issuing an NG9-1-1 Certificate, the CA and its Root CA, during the period when the NG9-1-1 Certificate is Valid, promise that the CA has followed the requirements of these Guidelines and the CA's NG9-1-1 Policies in issuing the NG9-1-1 Certificate and in verifying the accuracy of the information contained in the NG9-1-1 Certificate.

NG9-1-1 OID: An identifying number, in the form of an "object identifier," that is included in the *certificatePolicies* field of a certificate that: (i) indicates which CA policy statement relates to that certificate, and (ii) is either the PCA policy identifier or a policy identifier that, by pre-agreement, marks the certificate as being an NG9-1-1 Certificate. The OID for this document is maintained in a registry in accordance with the rules of the CP.

NG9-1-1 Policies: Auditable NG9-1-1 Certificate practices, policies and procedures, such as a certification practice statement and certificate policy, that are developed, implemented, and enforced by the Root CA and its subordinate CAs.

Incorporating Agency: In the context of a Private Entity, the government agency in the Jurisdiction of Incorporation under whose authority the legal existence of the entity is registered (e.g., the government agency that issues certificates of formation or incorporation). In the context of a Public Safety Entity, the entity that enacts law, regulations, or decrees establishing the legal existence of Public Safety Entities.

Independent Confirmation From Applicant: Confirmation of a particular fact received by the CA pursuant to the provisions of the Guidelines or binding upon the Applicant.

Individual: A natural person.

Jurisdiction of Incorporation: In the context of a Private Organization, the country and (where applicable) the state or province or locality where the organization's legal existence was

established by a filing with (or an act of) an appropriate government agency or entity (e.g., where it was incorporated). In the context of a Public Safety Entity, the country and (where applicable) the state or province where the Entity's legal existence was created by law.

Jurisdiction of Registration: In the case of a Business Entity, the state, province, or locality where the organization has registered its business presence by means of filings by a Principal Individual involved in the business.

Legal Agency: Where an agent acts on behalf of a principal within the scope of their authority which has been granted to them expressly or can be implied from the circumstances. Their acts bind the principal and the third party unless it follows from the circumstances of the case that the agent undertakes to bind themselves only.[10]

Legal Agent: An individual who has Legal Agency conferred upon them.

Legal Entity: A Private Entity, Public Safety Entity, or Non-Commercial Entity.

Legal Existence: A Private Entity, Public Safety Entity, or Business Entity has Legal Existence if it has been validly formed and not otherwise terminated, dissolved, or abandoned.

Local Registration Authority (LRA): A trusted party who may perform Validation and assert the accuracy of information presented by the Certificate Requester and/or to the Certificate Approver and/or on behalf of the RA. For example, supervisory personnel at a Public Safety Entity may be deemed a Local Registration Authority to validate employees at their organization to receive NG9-1-1 Certificates. See Section 11.2.2.

Place of Operation: The location of any entity (such as a PSAP, communications center or headquarters) where the Applicant's operations are conducted.

Principal Individual: An individual of a Private Entity or Public Safety Entity, that is either an owner, partner, managing member, director, or officer, as identified by their title of employment, or an employee, contractor or Legal Agent authorized by such entity or organization to conduct business related to the request, issuance, and use of NG9-1-1 Certificates.

Private Organization: A non-governmental legal entity (whether ownership interests are privately held or publicly traded) whose existence was created by a filing with (or an act of) the Incorporating Agency or equivalent in its Jurisdiction of Incorporation.

Public Safety Entity: An entity officially charged with the safety of life and property, usually a government organization, that may hold an NG9-1-1 Certificate in accordance with these Guidelines.

Private Entity: An entity that is not a government organization that may hold an NG9-1-1 Certificate in accordance with these Guidelines in support of one or more Public Safety Entities.

---

[10] Adapted from trans-lex.org legal dictionary. Retrieved 22 June 2021 from https://www.trans-lex.org/911000/_/prerequisites-and-effects-of-agency/. This document does not provide legal advice.

Qualified Government Information Source (QGIS): A database maintained by a government organization (e.g. SEC filings) that meets the requirements of these Guidelines.

Qualified Government Tax Information Source (QTIS): A Qualified Governmental Information Source that specifically contains tax information relating to Private Organizations, Business Entities, or Individuals.

Qualified Independent Information Source (QIIS): A regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information.

Registration Agency: A Governmental Agency that registers business information in connection with an entity's business formation or authorization to conduct business under a license, charter or other certification. A Registration Agency MAY include but is not limited to (i) a State Department of Corporations or a Secretary of State; (ii) a licensing agency, such as a State Department of Insurance; or (iii) a chartering agency, such as a state office or department of financial regulation, banking or finance, or a federal agency such as the Office of the Comptroller of the Currency or Office of Thrift Supervision.

Registered Agent: An individual or entity that is: (i) authorized by the Applicant to receive service of process and business communications on behalf of the Applicant; and (ii) listed in the official records of the Applicant's Jurisdiction of Incorporation as acting in the role specified in (i) above.

Registration Authority (RA): Per the CP.

Registration Number: The unique number assigned to a Private Organization by the Incorporating Agency in such entity's Jurisdiction of Incorporation.

Role: An enumerated role in the NG9-1-1 PKI maintained in a registry. One or more Roles may be assigned to any NG9-1-1 PKI member.

Signing Authority: One or more Certificate Approvers designated to act on behalf of the Applicant.

Sponsorship: The act of a Public Safety Entity taking responsibility for a Private Entity's possession of an NG9-1-1 Certificate.

Subject: Per the CP.

Validation: The act of validating an entity to be a part of the NG9-1-1 PKI in accordance with this policy, which includes verifying the identity of the entity requesting a Certificate, confirming their Agency affiliation, and validating that the requester has a legitimate and valid purpose to participate in the NG9-1-1 PKI.

3.8 Abbreviations and Acronyms

Term	Expansion
BIS	(US Government) Bureau of Industry and Security
CSO	Chief Security Officer
DNS	Domain Name System
FQDN	Fully Qualified Domain Name
NENA	NENA: The 9-1-1 Association (or National Emergency Number Association)
NG9-1-1	Next-Generation 9-1-1
NGCS	Next Generation Core Services
NIOC	NG9-1-1 Interoperability Oversight Commission
PCA	PSAP Credential Agency
PSAP	Public Safety Answering Point
IRS	Internal Revenue Service
ISP	Internet Service Provider
QGIS	Qualified Government Information Source
QTIS	Qualified Government Tax Information Source
QIIS	Qualified Independent Information Source
SEC	(US Government) Securities and Exchange Commission

3.9 Conventions

Terms not otherwise defined in these Guidelines shall be as defined in applicable agreements, user manuals, Certification Practice Statements (CPSes), and Certificate Policies (CP) of the CA issuing NG9-1-1 Certificates.

This section defines keywords, as they are be interpreted in NENA documents. The form of emphasis (UPPER CASE) shall be consistent and exclusive throughout the document. Any of these words used in lower case and not emphasized do not have special significance beyond normal usage.

1. MUST, SHALL, REQUIRED: These terms mean that the definition is a normative (absolute) requirement of the specification.
2. MUST NOT: This phrase, or the phrase "SHALL NOT", means that the definition is an absolute prohibition of the specification.

3. SHOULD: This word, or the adjective "RECOMMENDED", means that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. SHOULD NOT: This phrase, or the phrase "NOT RECOMMENDED" means that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behavior described with this label.
5. MAY: This word, or the adjective "OPTIONAL", means that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option "must" be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option "must" be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

These definitions are based on IETF RFC 2119.[11]

4 Certificate Warranties and Representations

4.1 NG9-1-1 Certificate Warranties

When the CA issues an NG9-1-1 Certificate, the CA represents and warrants to Relying Parties, during the period when the NG9-1-1 Certificate is Valid, that the CA, or the RA or LRA on the CA's behalf, has followed the requirements of these Guidelines and the Certificate Policy and applicable CPS in issuing and managing the NG9-1-1 Certificate and in verifying the accuracy of the information contained in the NG9-1-1 Certificate. The NG9-1-1 Certificate Warranties specifically include, but are not limited to, the following:

1. **Legal Existence:** The CA or RA or LRA has confirmed with the Appropriate Authority in the Subject's Jurisdiction of Incorporation that, as of the date the NG9-1-1 Certificate was issued, the Subject named in the NG9-1-1 Certificate legally exists as a valid organization or entity in the Jurisdiction of Incorporation;
2. **Identity:** The CA or RA or LRA has confirmed that, as of the date the NG9-1-1 Certificate was issued, that the Identifier, Role(s), Agency affiliation, and Owner are correct and have been validated by an RA or LRA in the NG9-1-1 validation chain.
3. **Accuracy of Information:** The CA has taken all steps reasonably necessary to verify that all of the other information in the NG9-1-1 Certificate is accurate, as of the date the NG9-1-1 Certificate was issued;

[11] https://datatracker.ietf.org/doc/html/rfc2119

4. **Subscriber Agreement:** The Subject named in the NG9-1-1 Certificate has entered into a legally valid and enforceable Subscriber Agreement with the CA or RA or LRA that satisfies the requirements of these Guidelines or, if they are affiliated, the Agency has acknowledged and accepted the Terms of Use;
5. **Status:** The CA will follow the requirements of these Guidelines and maintain a 24 x 7 online-accessible Repository with current information regarding the status of the NG9-1-1 Certificate as Valid or Revoked, and consistent with the CP and the applicable CPS; and
6. **Revocation:** The CA or RA or LRA will follow the requirements of these Guidelines and revoke the NG9-1-1 Certificate for any of the revocation reasons specified in these Guidelines, and consistent with the CP and the applicable CPS.

4.2 By the Applicant

NG9-1-1 Certificate Applicants make the commitments and warranties set forth in the NG9-1-1 CP and the applicable CPS.

5 Community and Applicability

5.1 Issuance of NG9-1-1 Certificates

The CA MAY issue NG9-1-1 Certificates, provided that the Root CA and its subordinate CAs satisfy the requirements in these Guidelines and the applicable CP and CPS.

If a court or government body with jurisdiction over the activities covered by these Guidelines determines that the performance of any mandatory requirement is illegal, then such requirement is considered reformed to the minimum extent necessary to make the requirement valid and legal. This applies only to operations or certificate issuances that are subject to the laws of that jurisdiction. The parties involved SHALL notify NIOC of the facts, circumstances, and law(s) involved, so that NIOC may revise these Guidelines accordingly.

5.2 NG9-1-1 Policies

5.2.1 Implementation

Each CA and Relying Party SHALL conform with all requirements in NENA i3 Standard and the NIOC CP and the applicable CPS.

5.2.2 Disclosure

Per the CP.

5.3 Commitment to Comply with Recommendations

Each CA SHALL publicly give effect to these Guidelines and represent that they will adhere to the latest published version by incorporating them into their respective CPSes, using a clause such as the following (which must include a link to the official version of these Guidelines):

[Name of CA] conforms to the current version of the NG9-1-1 Interoperability Oversight Commission Certificate Policy and Validation Policy published at ng911ioc.org. In the event of any inconsistency between this document and those policies, those policies take precedence over this document.

A valid link SHALL always be maintained by NIOC, subject to best-effort availability, at: https://ng911ioc.org/library

In addition, the CA MUST include (directly or by reference) the applicable requirements of these Guidelines in all contracts with Subordinate CAs, RAs, LRAs, and subcontractors that involve or relate to the issuance or maintenance of NG9-1-1 Certificates. The CA MUST enforce compliance with such terms.

5.4 Insurance

No stipulation.

5.5 Obtaining NG9-1-1 Certificates

5.5.1 General

The CA MAY only issue NG9-1-1 Certificates to Applicants that meet the Private Entity, Public Safety Entity and Non-Commercial Entity requirements specified below.

5.5.2 Private Entity Subjects

Private Entities are eligible to be issued NG9-1-1 Certificates in the capacity that they can demonstrate a valid public safety purpose in an enumerated Role. Where a Private Entity operates NG9-1-1 services for a Public Safety Entity, the NG9-1-1 Certificate will normally be issued to that Public Safety Entity, even when a Private Organization operates as a Legal Agent of a Public Safety Entity (for example, contractors). An Applicant qualifies as a Private Organization if:

1. The Private Entity serves a public safety purpose in an enumerated Role; and
2. The Private Entity can prove Sponsorship; and
3. The entity's Jurisdiction of Incorporation, Registration, Charter, License, and/or its Place of Business is not in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
4. The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

Items 1-4 above MAY be waived if the issuance of such certificates is expressly approved by the applicable MA or its Legal Agent.

5.5.3 Public Safety Entity Subjects

Most NG9-1-1 Certificates will be issued to Public Safety Entities, unless special circumstances are approved by NIOC or the appropriate MA. An Applicant qualifies as a Public Safety Entity if:

1. The entity's legal existence was established by the political subdivision in which the entity operates;
2. The entity is directly involved in public safety operations, such as operating an NG9-1-1 PSAP or NG9-1-1 Core Services network, directly responding to incidents and/or providing material support for such activities;
3. The entity can demonstrate that it serves in a Role enumerated in i3 or the applicable registry(ies);
4. The entity is not in any country where the CA is prohibited from doing business or issuing a certificate by the laws of the CA's jurisdiction; and
5. The entity is not listed on any government denial list or prohibited list (e.g., trade embargo) under the laws of the CA's jurisdiction.

5.5.4 Business Entity Subjects

Business Entities are subject to the same requirements as Private Organizations.

5.5.5 Non-Commercial Entity Subjects

Non-Commercial Entities are subject to the same requirements as Private Organizations.

6 NG9-1-1 Certificate Content and Profile

Per the CP, except as elaborated below.

6.1 Issuer Information

Per the CP; otherwise, no stipulation.

6.2 Subject Distinguished Name Fields

Per the CP; otherwise, no stipulation.

6.3 Subject Common Name Field

Per the CP; otherwise, no stipulation.

6.4 Subject Jurisdiction of Incorporation or Registration Field

Per the CP; otherwise, no stipulation.

6.4.1 Subject Registration Number Field

Per the CP; otherwise, no stipulation.

6.4.2 Subject Organizational Unit Name Field

Per the CP; otherwise, no stipulation.

6.5 Subject Organization Identifier Field

Per the CP; otherwise, no stipulation.

6.6 Other Subject Attributes

Per the CP; otherwise, no stipulation.

6.7 Certificate Policy Identification

Per the CP.

6.8 Certificate Policy Identification Requirements

Per the CP; otherwise, no stipulation.

6.9 Subscriber Certificates

Per the CP; otherwise, no stipulation.

6.10 Root CA Certificates

Per the CP.[12]

[12] The Root CA is the PCA.

6.11 Subordinate ICA Certificates

Per the CP; otherwise, no stipulation.

6.12 Subscriber Certificates

Per the CP; otherwise, no stipulation.

6.13 Maximum Validity Period For Certificates

Per the CP; otherwise, no stipulation.

6.14 Subscriber Public Key

Per the CP; otherwise, no stipulation.

6.15 Certificate Serial Number

Per the CP; otherwise, no stipulation.

6.16 Additional Technical Requirements for Validating Certificates

Per the CP; otherwise, no stipulation.

6.17 Certificate Extensions

6.17.1 Subject Alternative Name Extension

Certificate field: subjectAltName:OtherName

Required/Optional: **Required**

Contents: This extension MUST conform to the requirements of the NIOC CP.

The CA SHALL validate that the information in the Subject Alternative Name Extension is correct according to procedures allowed under this Validation Policy.

6.17.2 Organization Identifier Field

The NENA Registry System maintains sub-OIDs for the CP (as requested in the CP)[13] under an Internet Assigned Numbers Authority (IANA)-registered Private Enterprise Number for NIOC.[14]

7 NG9-1-1 Certificate Request Requirements

7.1 General Requirements

7.2 Documentation Requirements

No stipulation.

---

[13] See the CP.

[14] 55670, see https://www.iana.org/assignments/enterprise-numbers/enterprise-numbers.

7.3 Role Requirements

The following Applicant roles, as assigned by the Principal Individual, are required for the issuance of an NG9-1-1 Certificate.

1. **Certificate Requester:** The NG9-1-1 Certificate Request MUST be submitted by an authorized Certificate Requester. A Certificate Requester is a natural person who is either the Applicant, employed by the Applicant, an authorized Legal Agent who has express authority to represent the Applicant, or a third party that completes and submits an NG9-1-1 Certificate Request on behalf of the Applicant. If the Subscriber and the CA are affiliated, then the Certificate Requester Terms of Use applicable to the requested NG9-1-1 Certificate MUST be acknowledged and agreed to by the Applicant or their authorized representative.
2. **Certificate Approver:** The NG9-1-1 Certificate Request MUST be approved by an authorized Certificate Approver. A Certificate Approver is a natural person who is either the Applicant, employed by the Applicant, or an authorized Legal Agent who has express authority to represent the Applicant to (i) act as a Certificate Requester and to authorize other employees or third parties to act as a Certificate Requester, and (ii) to approve NG9-1-1 Certificate Requests submitted by other Certificate Requesters.
3. **Contract Signer:** A Subscriber Agreement applicable to the requested NG9-1-1 Certificate MUST be signed by an authorized Contract Signer. A Contract Signer is a natural person who is either the Applicant, employed by the Applicant, or an authorized Legal Agent who has express authority to represent the Applicant, and who has authority on behalf of the Applicant to sign Subscriber Agreements.

   The Applicant MAY authorize one individual to occupy two or more of these roles. The Applicant MAY authorize more than one individual to occupy any one of these roles.

7.4 Requirements for Subscriber Agreement and Terms of Use

Section 9.6.3 of the NG9-1-1 CP applies equally to NG9-1-1 Certificates. In cases where the Certificate Request does not contain all necessary information about the Applicant, the CA MUST additionally confirm the data with the Certificate Approver or Contract Signer rather than the Certificate Requester.

7.5 NG9-1-1 Certificate Request Requirements

The Certificate Request requirements in Sections 3 and Section 4 of the NG9-1-1 CP[15] apply equally to NG9-1-1 Certificates subject to the requirements of these Guidelines.

[15] See the CP as of 12 May 2021.

8 Verification Requirements

8.1 General Overview

This part of the Guidelines sets forth Verification Requirements and Acceptable Methods of Verification for each such Requirement**.**

8.2 Verification Requirements for NG9-1-1 Certificate Types

Before issuing an NG9-1-1 Certificate, the CA, RA or LRA MUST ensure that all Subject organization information to be included in the NG9-1-1 Certificate Subject Alternative Name extension conforms to the requirements of, and is verified in accordance with, these Guidelines and matches the information confirmed and documented by the CA.

8.2.1 Verification of the Root Certificate

Per the CP.

8.2.2 Verification of ICA Certificates

Per the CP.

8.2.3 Verification of Agency Certificates

All Verification Requirements in 8, except for 8.6 when it does not apply in accordance with the CP.

8.2.4 Verification of all Other Certificates

Verification requirements under 8.4, 8.6, 8.12 and 8.15.

8.3 Verification Methods

8.3.1 Acceptable Methods of Verification – Overview

The CA is responsible for ensuring the completion of all verification steps reasonably necessary to satisfy each of the requirements set forth in the subsections below. In most cases, the RA or LRA will perform the actual Validation. The CA is ultimately responsible for taking any additional verification steps that may be reasonably necessary under the circumstances to satisfy the applicable Verification Requirement.

8.4 Verification of Role

To verify a Subject's Role, the RA or LRA MUST do the following:

1. Validate that the requested Roles attested for the Subject conforms to Roles enumerated in the appropriate registry(ies).[16] [17]

8.5 Verification of Agency Identity

For Agency Certificates, a Subject's Agency will be in the format of a Fully-Qualified Domain Name (FQDN). To verify a Subject's Agency for an Agency Certificate, the RA or LRA MUST confirm control of the FQDN using one of the following methods:

8.5.1 DNS Change

The RA or LRA may confirming the Applicant's control over the FQDN by confirming the presence of a Random Value or Request Token for either in a DNS CNAME, TXT or CAA record for either:

1. An Authorization Domain Name; or
2. an Authorization Domain Name that is prefixed with a label that begins with an underscore character.

If a Random Value is used, the CA SHALL provide a Random Value unique to the Certificate request and SHALL not use the Random Value after

1. 30 days of the Applicant's Attestation; or
2. if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate as specified in the applicable CPS.

Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the labels of the validated FQDN.

8.5.2 IP Address

Confirming the Applicant's control over the FQDN by confirming that the Applicant controls an IP address returned from a DNS lookup for A or AAAA records for the FQDN. This may confirm the Applicant's control of the IP Address by:

1. Observing an agreed-upon change in the IP address associated with an A or AAAA record attested by the Applicant within:
    a. 30 days of the Applicant's attestation; or
    b. if the Applicant submitted the Certificate request, the timeframe permitted for reuse of validated information relevant to the Certificate.

---

[16] For Agency Certificates, the Agency must have one more or Roles from the Agency Roles registry; and must also have one or more Roles from the urn:emergency:service:responder registry or the appropriate subregistry(ies). See i3 at Section 10.

[17] For Agent Certificates, the Agent must have one or more Roles from the Agent Roles registry or the appropriate subregistry(ies). See Id.

Once the FQDN has been validated using this method, the CA MAY NOT also issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method.

8.5.3 Agreed-Upon Change to Website v2

Confirming the Applicant's control over the FQDN by verifying that the Request Token or Random Value is contained in the contents of a file or website at the FQDN in a manner specified by the RA or LRA.

1. The entire Request Token or Random Value MUST NOT appear in the request used to retrieve the file or access the website, and
2. the CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received).

The file or website containing the Request Token or Random Number:

1. MUST be located on the Authorization Domain Name, and
2. SHOULD be located under the "/.well-known/pki-validation" directory, and
3. MUST be retrieved via either the "http" or "https" scheme, and
4. MUST be accessed over an Authorized Port.

If the CA follows redirects, the following apply:

1. Reedirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231,[18] Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538,[19] Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.
3. Redirects MUST be to resource URLs accessed via Authorized Ports.

If a Random Value is used, then:

1. The CA MUST provide a Random Value unique to the certificate request.
2. The Random Value MUST remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

Note: CAs MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

---

[18] https://datatracker.ietf.org/doc/html/rfc7231

[19] https://datatracker.ietf.org/doc/html/rfc7538

8.5.4 Agreed-Upon Change to Website - ACME

Confirming the Applicant's control over a FQDN by validating domain control of the FQDN using the ACME HTTP Challenge method defined in Section 8.3 of RFC 8555.[20] The following are additive requirements to RFC 8555.

The CA MUST receive a successful HTTP response from the request (meaning a 2xx HTTP status code must be received). The token (as defined in RFC 8555, Section 8.3) MUST NOT be used for more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values, in which case the CA MUST follow its CPS.

If the CA follows redirects, the following apply:

1. Redirects MUST be the result of a 301, 302, or 307 HTTP status code response, as defined in RFC 7231, Section 6.4, or a 308 HTTP status code response, as defined in RFC 7538, Section 3. Redirects MUST be to the final value of the Location HTTP response header, as defined in RFC 7231, Section 7.1.2.
2. Redirects MUST be to resource URLs with either the "http" or "https" scheme.
3. Redirects MUST be to resource URLs accessed via Authorized Ports.

Note: CAs MUST NOT issue Certificates for other FQDNs that end with all the labels of the validated FQDN unless the CA performs a separate validation for that FQDN using an authorized method. This method is NOT suitable for validating Wildcard Domain Names.

8.5.5 Any Other Method

Any other method not included in this section SHALL NOT be used.

[20] https://datatracker.ietf.org/doc/html/rfc8555

8.6 Verification of Owner

The RA or LRA MUST confirm the identity of the Owner[21] by an electronic signature provided by an Agency Certificate whose FQDN matches the "Owner" field. The signing of the Certificate Signing Request by the Owner is sufficient to validate the Agent.

When the Owner is a CA, the fact that the Certificate is issued by the CA is sufficient to validate the Owner as being the CA.

Private Entities SHOULD have a sponsor that is a Public Safety Entity that is the Owner for its Agency, Agent, Element and Service Certificates. If a Private Entity does not have a sponsor, it MUST have an Agency Certificate approved by the appropriate MA for that CPS.

8.6.1 Verification of Owner for Agency Certificates

Per the CP.

8.7 Verification of Applicant's Legal Existence and Identity

8.7.1 Verification Requirements

To verify the Applicant's legal existence and identity, the RA or LRA MUST do the following:

1. **Legal Existence:** Verify that the Applicant is a legally recognized Public Safety Entity or a Private Entity with a valid public safety purpose, in existence and validly formed (e.g., enabling statute, ordinance, municipal incorporation, joint powers agreement or similar; or articles of incorporation, business registration or similar) in the Applicant's Jurisdiction of Incorporation.
2. **Organization Name:** Verify that the Applicant's formal legal name in the Applicant's jurisdiction matches the Applicant's name in the NG9-1-1 Certificate Request.
3. **Registration Number:** For Private Entities, obtain the specific Registration Number assigned to the Applicant in the Applicant's Jurisdiction of Incorporation or Registration. Where the Applicant does not have a Registration Number, the CA SHALL obtain the Applicant's date of Incorporation or Registration.
4. **Registered Agent:** Private Entities that obtain a Certificate SHALL NOT do so through a legal Registered Agent.
5. **Public Safety Function:** Verify that the Applicant or the element which they control is performs a legitimate public safety function required for NG9-1-1, such as by validating an enumerated Role, or for Private Entities, reviewing available information about the company's mission statement and business purposes.
6. **Principal Individual:** Verify the identity of the identified Principal Individual per section 8.7.2.
7. **Agency Identity**: Verify the agency identity per section 8.5.

[21] Per the CP at 7.1.2.11; an Agency Certificate may not have an Owner.

8.7.2 Acceptable Method of Verification

1. **Private Entity Subjects:** Unless verified under subsection (4), all items listed in Section 8.2 MUST be verified directly with the Appropriate Authority. Such verification MAY be through direct contact with the Appropriate Authority in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained directly from a QGIS, Incorporating or Registration Agency, or from a QIIS.
2. **Public Safety Entity Subjects:** Unless verified under subsection (4), all items listed in Section 8.7.1 MUST either be verified directly with, or obtained directly from, one of the following:
    a. a QGIS in the political subdivision in which such Public Safety Entity operates;
    b. a superior governing Public Safety Entity in the same political subdivision as the Applicant (e.g., an elected sheriff may verify the legal existence of functions within their own sheriff's office), or
    c. from a judge that is an active member of the federal, state, or local judiciary within that political subdivision.

Any communication from a judge SHALL be verified in the same manner as is used for verifying factual assertions that are asserted by an attorney.

Such verification MAY be by direct contact with the appropriate Public Safety Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a QIIS.

1. **Principal Individual:** A Principal Individual MUST be validated in a face-to-face setting. The CA MAY rely upon a face-to-face validation of the Principal Individual performed by the RA or LRA, provided that the CA has evaluated the validation procedure and concluded that it satisfies the requirements of the Guidelines for face-to-face validation procedures. Where no face-to-face validation was conducted by the RA, or the RA's face-to-face validation procedure does not satisfy the requirements of the Guidelines, the CA SHALL perform face-to-face validation.

    a. **Face-To-Face Validation:** The face-to-face validation MUST be conducted before either an employee or Legal Agent of the CA, an RA or an LRA. The face-to-face validation MAY be performed virtually (e.g., via video conference). The Principal Individual(s) MUST present the following documentation directly to the RA or LRA:

        i. A Personal Statement that includes the following information:

            1. Full name or names by which the person is, or has been, known (including all other names used)
            2. Official Title, including Agency affiliation;
            3. Address at which the person can be located, and

4. An affirmation that all of the information contained in the Certificate Request is true and correct.

ii. The RA or LRA MUST:

1. Verify the Principal Individual's full name, official title and Agency affiliation through a QGIS, QIIS, government-issued identification or equivalent.

2. Attest to the signing of the Personal Statement and the identity of the signer; and

b. **Verification of Validator:** The CA MUST verify that the RA or LRA actually did perform the services and did attest to the identity of the Individual.

8.8 Verification of Applicant's Physical Existence – Place of Operations

8.8.1 Verification Requirements

To verify the Applicant's physical existence and business presence, the CA, the RA or LRA MUST verify that the physical address provided by the Applicant is an address where the Applicant conducts operations (not, for example, a mail drop or P.O. box, or 'care of' (C/O) address, such as an address for a Legal Agent of the organization) and is the address of the Applicant's Place of Operations.

8.8.2 Acceptable Methods of Verification

Applicants SHALL provide a Place of Operations and this SHALL be validated by one of the following:

a. For Applicants listed at the same Place of Operations address in the current version of either at least one QGIS (other than that used to verify legal existence), QIIS or QTIS, the CA, RA or LRA MUST confirm that the Applicant's address, as listed in the NG9-1-1 Certificate Request, is a valid address for the Applicant by reference to such QGIS, QIIS, or QTIS, and MAY rely on the Applicant's representation that such address is its Place of Operations;

b. For Applicants who are not listed at the same Place of Operations address in the current version of either at least one QIIS or QTIS, the CA, the RA or LRA MUST confirm that the address provided by the Applicant in the NG9-1-1 Certificate Request is the Applicant's address, by obtaining documentation of a site visit to the address, which MUST be performed by a reliable individual or firm. The documentation of the site visit MUST:

i. Verify that the Applicant's Place of Operations is located at the exact address stated in the NG9-1-1 Certificate Request (e.g., via permanent signage, employee confirmation, etc.),

ii. Identify the type of facility (e.g., official government building, office in a commercial building, etc.) and whether it appears to be a permanent operations location,

iii. Indicate whether there is a permanent sign (that cannot be moved) that identifies the Applicant, and

iv. Indicate whether there is evidence that the Applicant is conducting ongoing activities at the site (not that it is just, for example, a mail drop, P.O. box, etc.).

8.9 Verified Method of Communication

8.9.1 Verification Requirements

To assist in communicating with the Applicant and confirming that the Applicant is aware of and approves issuance, the RA or LRA MUST verify a telephone number, fax number, email address, or postal delivery address as a Verified Method of Communication with the Applicant.

8.9.2 Acceptable Methods of Verification

To verify a Verified Method of Communication with the Applicant, the RA or LRA MUST:

1. Verify that the Verified Method of Communication belongs to the Applicant, or a Parent/Subsidiary or Affiliate of the Applicant, by matching it with: a QGIS, QTIS, or QIIS; and
2. Confirm the Verified Method of Communication by using it to obtain an affirmative response sufficient to enable a reasonable person to conclude that the Applicant, or a Parent/Subsidiary or Affiliate of Applicant, can be contacted reliably by using the Verified Method of Communication.

8.9.3 Verification of Applicant's Operational Existence

8.9.4 Verification Requirements

The CA, RA or LRA MUST verify that the Applicant does engage in its stated Role by verifying the Applicant's, or Affiliate/Parent/Subsidiary's, operational existence. The CA, RA or LRA MAY rely on its verification of a Public Safety Entity's legal existence under Section 8.2 as verification of its operational existence.

1. Acceptable Methods of Verification
    a. Private Entity Subjects: Verification MUST be through a QGIS or QIIS.
    b. Public Safety Entity Subjects: The Applicant's legal existence MUST either be verified directly with, or obtained directly from, one of the following:
        i. a QGIS in the political subdivision in which such Public Safety Entity operates;

ii. a superior governing Public Safety Entity in the same political subdivision as the Applicant (e.g., an elected sheriff may verify the legal existence of functions within their own sheriff's office), or

iii. from a judge that is an active member of the federal, state, or local judiciary within that political subdivision.

Any communication from a judge SHALL be verified in the same manner as is used for verifying factual assertions that are asserted by an attorney.

Such verification MAY be by direct contact with the appropriate Public Safety Entity in person or via mail, e-mail, Web address, or telephone, using an address or phone number obtained from a QIIS or QGIS.

8.10 Verification of Name, Title, and Authority of Contract Signer and Certificate Approver

8.10.1 Verification Requirements

For both the Contract Signer and the Certificate Approver, the RA or LRA MUST verify the following.

1. **Name, Title and Agency:** The name and title of the Contract Signer and the Certificate Approver, as applicable. The RA MUST also verify that the Contract Signer and the Certificate Approver are Legal Agents representing the Applicant.
2. **Signing Authority of Contract Signer:** That the Contract Signer is authorized by the Applicant to enter into the Subscriber Agreement (and any other relevant contractual obligations) on behalf of the Applicant, including a contract that designates one or more Certificate Approvers on behalf of the Applicant.
3. **Authority of Certificate Approver:** Through a source other than the Certificate Approver their self, that the Certificate Approver is expressly authorized by the Applicant to do the following, as of the date of the NG9-1-1 Certificate Request, to:
    a. Submit, and, if applicable, authorize a Certificate Requester to submit, the NG9-1-1 Certificate Request on behalf of the Applicant; and
    b. Provide, and, if applicable, authorize a Certificate Requester to provide, the information requested from the Applicant by the CA for issuance of the NG9-1-1 Certificate; and
    c. Approve NG9-1-1 Certificate Requests submitted by a Certificate Requester.

8.10.2 Acceptable Methods of Verification – Name, Title and Legal Agency

Acceptable methods of verification of the name, title, and Legal Agency status of the Contract Signer and the Certificate Approver include the following:

1. **Name and Title:** The RA or LRA MAY verify the name and title of the Contract Signer and the Certificate Approver by any appropriate method designed to provide reasonable

assurance that a person claiming to act in such a role is in fact the named person designated to act in such role**.**

2. **Legal Agency:** The RA or LRA MAY verify the Legal Agency of the Contract Signer and the Certificate Approver using one of the following methods:
    a. Contacting the Applicant using a Verified Method of Communication for the Applicant, and obtaining confirmation, either by:
        i. Obtaining an Independent Confirmation from the Applicant (as described in Section 8.12.3), or a verified professional letter verifying that the Contract Signer and/or the Certificate Approver, as applicable, has been authorized to act on behalf of the Applicant as its Legal Agent; or
        ii. By obtaining confirmation from a QIIS or QGIS that the Contract Signer and/or Certificate Approver is an employee of the Applicant.
    b. Via a certification from the Contract Signer (including in a contract between the CA or RA and the Applicant signed by the Contract Signer), provided that the employment or Legal Agent status and Signing Authority of the Contract Signer has been verified.

8.10.3 Acceptable Methods of Verification – Signing Authority

Acceptable methods of verification of the Signing Authority of the Contract Signer, and the Authority of the Certificate Approver, as applicable, include:

1. **Resolution:** The Signing Authority of the Contract Signer, and/or the Authority of the Certificate Approver, MAY be verified by reliance on a properly authenticated resolution that confirms that the person has been granted such Signing Authority, provided that such resolution (i) is certified by an appropriate officer of the organization (e.g., secretary), and (ii) the can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification;
2. **Independent Confirmation from Applicant:** The Signing Authority of the Contract Signer, and/or the Authority of the Certificate Approver, MAY be verified by obtaining an Independent Confirmation from the Applicant (as described in Section 8.12.3);
3. **Contract between CA and Applicant:** The Authority of the Certificate Approver MAY be verified by reliance on a contract between the CA, RA or LRA and the Applicant that designates the Certificate Approver with such Authority, provided that the contract is signed by the Contract Signer and provided that the agency and Signing Authority of the Contract Signer have been verified;
4. **Prior Equivalent Authority:** The Signing authority of the Contract Signer, and/or the Authority of the Certificate Approver, MAY be verified by relying on a demonstration of Prior Equivalent Authority.

a. Prior Equivalent Authority of a Contract Signer MAY be relied upon for confirmation or verification of the signing authority of the Contract Signer when the Contract Signer has executed a binding contract between the CA, RA or LRA and the Applicant with a legally valid and enforceable seal or handwritten signature. The CA MUST record sufficient details of the previous agreement to correctly identify it and associate it with the NG9-1-1 application. Such details MAY include any of the following:
    i. Agreement title,
    ii. Date of Contract Signer's signature,
    iii. Contract reference number, and
    iv. Filing location.
b. Prior Equivalent Authority of a Certificate Approver MAY be relied upon for confirmation or verification of the Authority of the Certificate Approver when the Certificate Approver has performed one or more of the following:
    i. Under contract to the CA, has served (or is serving) as an LRA for the Applicant, or
    ii. Has participated in the approval of one or more certificate requests, for certificates issued by the CA and which are currently and verifiably in use by the Applicant. In this case the CA MUST have contacted the Certificate Approver by Verified Method of Communication or have accepted a signed and notarized letter approving the certificate request.

5. **QIIS or QGIS**: The Signing Authority of the Contract Signer, and/or the Authority of the Certificate Approver, MAY be verified by a QIIS or QGIS that identifies the Contract Signer and/or the Certificate Approver as an officer, director or other senior official of the Applicant.
6. **Contract Signer's Representation/Warranty:** Provided that the RA or LRA verifies that the Contract Signer is an employee or Legal Agent of the Applicant, the CA MAY rely on the signing authority of the Contract Signer by obtaining a duly executed representation or warranty from the Contract Signer that includes the following acknowledgments:
    a. That the Applicant authorizes the Contract Signer to sign the Subscriber Agreement on the Applicant's behalf,
    b. That the Subscriber Agreement is a legally valid and enforceable agreement,
    c. That, upon execution of the Subscriber Agreement, the Applicant will be bound by all of its terms and conditions, and
    d. That serious consequences attach to the misuse of an NG9-1-1 certificate.

8.10.4 Pre-Authorized Certificate Approver

Where the CA and Applicant contemplate the submission of multiple future NG9-1-1 Certificate Requests, then, after the RA or LRA:

1. Has verified the name and title of the Contract Signer and that he/she is an employee or Legal Agent of the Applicant; and
2. Has verified the Signing Authority of such Contract Signer in accordance with one of the procedures in Section 8.10; then

   The CA, RA or LRA and the Applicant MAY enter into a written agreement, signed by the Contract Signer on behalf of the Applicant, whereby, for a specified term, the Applicant expressly authorizes one or more Certificate Approver(s) designated in such agreement to exercise Authority with respect to each future NG9-1-1 Certificate Request submitted on behalf of the Applicant and properly authenticated as originating with, or otherwise being approved by, such Certificate Approver(s).

   Such an agreement MUST provide that the Applicant shall be obligated under the Subscriber Agreement for all NG9-1-1 Certificates issued at the request of, or approved by, such Certificate Approver(s) until NG9-1-1 Certificate Request Authority is Revoked, and MUST include mutually agreed-upon provisions for:

   a. authenticating the Certificate Approver when NG9-1-1 Certificate Requests are approved,
   b. periodic re-confirmation of the NG9-1-1 Authority of the Certificate Approver,
   c. secure procedures by which the Applicant can notify the CA that the NG9-1-1 Certificate Request Authority of any such Certificate Approver is Revoked, and
   d. such other appropriate precautions as are reasonably necessary.

8.11 Verification of Signature on Subscriber Agreement and NG9-1-1 Certificate Requests

Both the Subscriber Agreement and each non-pre-authorized NG9-1-1 Certificate Request MUST be signed. The Subscriber Agreement MUST be signed by an authorized Contract Signer. The NG9-1-1 Certificate Request MUST be signed by the Certificate Requester submitting the document, unless the Certificate Request has been pre-authorized in line with Section 8.10.4 of these Guidelines. If the Certificate Requester is not also an authorized Certificate Approver, then an authorized Certificate Approver MUST independently approve the NG9-1-1 Certificate Request. In all cases, applicable signatures MUST be legally valid and contain an enforceable seal or handwritten signature (for a paper Subscriber Agreement and/or NG9-1-1 Certificate Request), or a legally valid and enforceable electronic signature (for an electronic Subscriber Agreement and/or NG9-1-1 Certificate Request), that binds the Applicant to the terms of each respective document.

8.11.1 Verification Requirements

1. **Signature:** The CA, RA or LRA MUST authenticate the signature of the Contract Signer on the Subscriber Agreement and the signature of the Certificate Requester on each NG9-1-1 Certificate Request in a manner that makes it reasonably certain that the person named as the Contract Signer in the applicable document is, in fact, the person who signed the document on behalf of the Applicant.
2. **Approval Alternative:** In cases where an NG9-1-1 Certificate Request is signed and submitted by a Certificate Requester who does not also function as a Certificate Approver, approval and adoption of the NG9-1-1 Certificate Request by a Certificate Approver in accordance with the requirements of Section 8.12 can substitute for authentication of the signature of the Certificate Requester on such NG9-1-1 Certificate Request.

8.11.2 Acceptable Methods of Signature Verification

Acceptable methods of authenticating the signature of the Certificate Requester or Contract Signer include the following:

1. Contacting the Applicant using a Verified Method of Communication for the Applicant, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response from someone who identifies themselves as such person confirming that they did sign the applicable document on behalf of the Applicant;
2. A letter mailed to the Applicant's or Agent's address, as verified through independent means in accordance with these Guidelines, for the attention of the Certificate Requester or Contract Signer, as applicable, followed by a response through a Verified Method of Communication from someone who identifies themselves as such person confirming that they did sign the applicable document on behalf of the Applicant; or
3. Use of a signature process that establishes the name and title of the signer in a secure manner, such as through use of an appropriately secure login process that identifies the signer before signing, or through use of a digital signature made with reference to an appropriately verified certificate.

8.12 Verification of Approval of NG9-1-1 Certificate Request

8.12.1 Verification Requirements

In cases where an NG9-1-1 Certificate Request is submitted by a Certificate Requester, before the CA issues the requested NG9-1-1 Certificate, the CA, RA or LRA MUST verify that an authorized Certificate Approver reviewed and approved the NG9-1-1 Certificate Request.

8.12.2 Acceptable Methods of Verification

Acceptable methods of verifying the Certificate Approver's approval of an NG9-1-1 Certificate Request include:

1. Contacting the Certificate Approver using a Verified Method of Communication for the Applicant and obtaining oral or written confirmation that the Certificate Approver has reviewed and approved the NG9-1-1 Certificate Request;
2. Notifying the Certificate Approver that one or more new NG9-1-1 Certificate Requests are available for review and approval at a designated access-controlled and secure website, followed by a login by, and an indication of approval from, the Certificate Approver in the manner required by the Web site which shall be at least two-factor authentication; or
3. Verifying the signature of the Certificate Approver on the NG9-1-1 Certificate Request in accordance with Section 8.11.2 of these Guidelines.

8.12.3 Independent Confirmation from Applicant

An Independent Confirmation from the Applicant is a confirmation of a particular fact (e.g., confirmation of the employee or agency status of a Contract Signer or Certificate Approver, confirmation of the NG9-1-1 Authority of a Certificate Approver, etc.) that is:

1. Received by the RA or LRA from a Confirming Person (someone other than the person who is the subject of the inquiry) that has the Appropriate Authority to confirm such a fact, and who represents that he/she has confirmed such fact;
2. Received by the RA or LRA in a manner that authenticates and verifies the source of the confirmation; and
3. Binding on the Applicant.

An Independent Confirmation from the Applicant MAY be obtained via the following procedure:

1. **Confirmation Request:** The RA or LRA MUST initiate a Confirmation Request via an appropriate out-of-band communication, requesting verification or confirmation of the particular fact at issue as follows:
    a. **Addressee:** The Confirmation Request MUST be directed to:
        i. A position within the Applicant's organization that qualifies as a Confirming Person (e.g., an elected official, an individual serving in an official role in a Public Safety Entity, an Individual appointed by an elected official, CSO, Director, etc.) and is identified by name and title in a current QGIS, QIIS, QTIS, or by contacting the Applicant using a Verified Method of Communication; or
        ii. A named individual verified to be in the direct line of management above the Contract Signer or Certificate Approver by contacting the Applicant's human resources department by phone or mail (at the phone number or address for the Applicant's Place of Business, verified in accordance with these Guidelines, or through publicly-available records).

b. **Means of Communication:** The Confirmation Request MUST be directed to the Confirming Person in a manner reasonably likely to reach such person. The following options are acceptable:

i. By paper mail addressed to the Confirming Person at:

1. The address of the Applicant's Place of Operations as verified by the CA in accordance with these Guidelines, or

2. The address for such Confirming Person specified in a current QGIS, QTIS, QIIS, or

ii. Via a method of communication as listed in 8.11 to the Confirming Person for such person listed in a current QGIS, QTIS, QIIS.

2. **Confirmation Response:** The RA or LRA MUST receive a response to the Confirmation Request from a Confirming Person that confirms the particular fact at issue. Such response MAY be provided to the RA or LRA by any method of communication as listed in 8.11 so long as the Confirming Person can reliably verify that it was provided by a Confirming Person in response to the Confirmation Request.

3. The RA or LRA MAY rely on a verified Confirming Person to confirm their own contact information. The RA or LRA MAY rely on this verified contact information for future correspondence.

8.12.4 Qualified Independent Information Source (QIIS)

A Qualified Independent Information Source (QIIS) is a regularly-updated and publicly available database that is generally recognized as a dependable source for certain information. A database qualifies as a QIIS if it is determined that:

1. Industries other than the certificate industry rely on the database for accurate location, contact, or other information; and

2. The database provider updates its data on at least an annual basis.

The RA or LRA SHALL document which QIIS it uses to verify any fact at issue. The LA or LRA SHALL use a documented process to check the accuracy of the database and ensure its data is acceptable, including reviewing the database provider's terms of use.

8.12.5 Qualified Government Information Source (QGIS)

A Qualified Government Information Source (QGIS) is a regularly-updated and current, publicly available, database designed for the purpose of accurately providing the information for which it is consulted, and which is generally recognized as a dependable source of such information provided that it is maintained by a Public Safety Entity or a unit of government. The RA or LRA SHALL document which QGIS it uses to verify any fact at issue. Nothing in these Guidelines shall prohibit the use of third-party vendors to obtain the information from the Public Safety Entity or a unit of government provided that the third party obtains the information directly from the Public Safety Entity or a unit of government.

8.12.6 Qualified Government Tax Information Source (QTIS)

A Qualified Government Tax Information Source is a QGIS that specifically contains tax information relating to Private Organizations, Business Entities or Individuals (e.g., the IRS in the United States).

8.13 Other Verification Requirements

8.13.1 High Risk Status

No stipulation.

8.13.2 Denied Lists and Other Legal Unapproved Lists

1. **Verification Requirements:** The RA or LRA MUST verify whether the Applicant, the Contract Signer, the Certificate Approver, the Applicant's Jurisdiction of Incorporation, Registration, or Place of Operations:
    a. Is identified on any government denied list, list of prohibited persons, or other reputable list that prohibits engaging in business or other specified activities with such organization or person under the laws, regulations, technical standard or best practice, of CA's jurisdiction(s) of operation; or
    b. Has its Jurisdiction of Incorporation, Registration, or Place of Operations in any country with which the laws of the CA's jurisdiction prohibit doing business or other specified activities.

The CA MUST NOT issue any NG9-1-1 Certificate to the Applicant if the Applicant, the Contract Signer, or Certificate Approver or if the Applicant's Jurisdiction or Registration or Place of Operations is on any such list.

2. **Acceptable Methods of Verification:** The RA or LRA MUST take reasonable steps to verify with the following lists and regulations:
    a. If the CA has operations in the U.S., the CA MUST take reasonable steps to verify with the following US Government denied lists and regulations:
        i. United States Bureau of Industry and Security (BIS) Denied Persons List - http://www.bis.doc.gov/dpl/thedeniallist.asp

ii. BIS Denied Entities List - https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list
iii. US Treasury Department List of Specially Designated Nationals and Blocked Persons - http://www.treas.gov/ofac/t11sdn.pdf
iv. US Government export regulations

b. If the CA has operations in any other country, the CA MUST take reasonable steps to verify with all equivalent denied lists and export regulations (if any) in such other country.

8.13.3 Parent/Subsidiary/Affiliate Relationship

An RA or LRA verifying an Applicant using information of the Applicant's Parent, Subsidiary, or Affiliate, when allowed under these Guidelines, MUST verify the Applicant's relationship to the Parent, Subsidiary, or Affiliate. Acceptable methods of verifying the Applicant's relationship to the Parent, Subsidiary, or Affiliate include the following:

1. QIIS or QGIS: The relationship between the Applicant and the Parent, Subsidiary, or Affiliate is identified in a QIIS or QGIS;
2. Independent Confirmation from the Parent, Subsidiary, or Affiliate: An RA or LRA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by obtaining an Independent Confirmation from the appropriate Parent, Subsidiary, or Affiliate (as described in Section 8.12.3);
3. Contract between CA or RA and Parent, Subsidiary, or Affiliate: An RA or LRA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a contract between the CA, or the RA and the Parent, subsidiary, or Affiliate that designates the Certificate Approver with such NG9-1-1 Authority, provided that the contract is signed by the Contract Signer and provided that the Legal Agency and Signing Authority of the Contract Signer have been verified;
4. Verified Professional Letter: An RA or LRA MAY verify the relationship between an Applicant and a Parent, Subsidiary, or Affiliate by relying on a Verified Professional Letter; or
5. Resolution: An RA or LRA MAY verify the relationship between an Applicant and a Subsidiary by relying on a properly authenticated resolution that approves creation of the Subsidiary or the Applicant, provided that such resolution is (i) certified by the appropriate officer (e.g., secretary), and (ii) the CA can reliably verify that the certification was validly signed by such person, and that such person does have the requisite authority to provide such certification.

8.14 Final Cross-Correlation and Due Diligence

For NG9-1-1 Certificates:

1. The results of the verification processes and procedures outlined in these Guidelines are intended to be viewed both individually and as a group. Thus, after all of the verification processes and procedures are completed, the RA or LRA MUST have a person who is not responsible for the collection of information review collection of all of the information and

documentation assembled in support of the NG9-1-1 Certificate Application and look for discrepancies or other details requiring further explanation.

2. The RA or LRA MUST obtain and document further explanation or clarification from the Applicant, Certificate Approver, Certificate Requester, QIISes, and/or other sources of information, as necessary, to resolve discrepancies or details that require further explanation.
3. The CA MUST refrain from issuing an NG9-1-1 Certificate until the entire corpus of information and documentation assembled in support of the NG9-1-1 Certificate Request is such that issuance of the NG9-1-1 Certificate will not communicate factual information that the CA knows, or the exercise of due diligence should discover from the assembled information and documentation, to be inaccurate. If satisfactory explanation and/or additional documentation are not received within a reasonable time, the CA MUST decline the NG9-1-1 Certificate Request and SHOULD notify the Applicant accordingly.
4. The normal operating language of the CA SHALL be American English. When the Applicant does not possess the language skills necessary to operate in the normal operating language of the CA, a CA MAY:
    a. Rely on language translations of the relevant portions of the documentation, provided that the translations are received from a Translator; or
    b. When the CA has utilized the services of an RA or LRA, the CA MAY rely on the language skills of the RA or LRA to perform the Final Cross-Correlation and Due Diligence. Notwithstanding the foregoing, prior to issuing the NG9-1-1 Certificate, the CA MUST review the work completed by the RA or LRA and determine that all requirements have been met.

8.15 Requirements for Re-use of Existing Documentation

For each NG9-1-1 Certificate Request, including requests to renew existing NG9-1-1 Certificates, the CA MUST perform all authentication and verification tasks required by these Guidelines to ensure that the request is properly authorized by the Applicant and that the information in the NG9-1-1 Certificate is still accurate and valid. This section sets forth the age limitations on the use of documentation collected by the CA.

8.15.1 Validation For Existing Subscribers

If an Applicant has a currently valid NG9-1-1 Certificate issued by the CA, a CA MAY rely on its prior authentication and verification of information that has been verified before issuing the NG9-1-1 Certificate in accordance with the stipulations in the CPS for the CA.

8.15.2 Re-issuance Requests

Per the CP.

8.15.3 Age of Validated Data

1. Except when permitted otherwise in Section 8.15.1, the age of all data used to support issuance of an NG9-1-1 Certificate (before revalidation is required) SHALL NOT exceed the following limits:
    a. Legal existence and identity – three years;
    b. Assumed name – three years;
    c. Address of Place of Operations – three years;
    d. Verified Method of Communication – thirteen months;
    e. Operational existence – three years;
    f. Agency Identity – three years;
    g. Name, Title, Agency, and Authority – three years, unless a contract with the CA specifies a different term, in which case, the term specified in such contract controls. For example, the contract MAY include the perpetual assignment of roles until Revoked by the Applicant or CA, or until the contract expires or is terminated.
2. The periods set forth above SHALL begin to run on the date the information was collected by the CA.
3. The CA MAY reuse a previously submitted NG9-1-1 Certificate Request, Subscriber Agreement, or Terms of Use, including use of a single NG9-1-1 Certificate Request in support of multiple NG9-1-1 Certificates containing the same Subject to the extent permitted under Sections 8.9 and 8.10.
4. The CA MUST repeat the verification process required in these Guidelines for any information obtained outside the time limits specified above except when permitted otherwise under section 8.15.1.

9 Certificate Issuance by a Root CA

Per the CP.

9.1.1 Identity and Background Verification

Prior to the commencement of employment of any person by the CA, RA or LRA for engagement in the processes under these Guidelines, whether as an employee, Legal Agent, or an independent contractor of the CA, RA or LRA, the CA, RA or LRA MUST:

1. Verify the Identity of such Person: Verification of identity MUST be performed through:
    a. The personal (physical or virtual) presence of such person before trusted persons who perform human resource or security functions, and
    b. The verification of well-recognized forms of government-issued photo identification (e.g., passports and/or drivers licenses); and
2. Verify the Trustworthiness of such person: Verification of trustworthiness SHALL include background checks, which address at least the following, or their equivalent:
    a. Confirmation of previous employment,
    b. Check of professional references;

c. Search of criminal records (local, state or provincial, and national) where allowed by the jurisdiction in which the person will be employed; and
d. For Public Safety Entities, that existing background check procedures for identifying the trustworthiness of employees is sufficient to meet the requirements of these Guidelines.

3. In the case of employees already in the employ of the CA, RA or LRA at the time of adoption of these Guidelines whose identity and background has not previously been verified as set forth above, the CA, RA or LRA SHALL conduct such verification within three months of the date of adoption of these Guidelines under the applicable CPS.

10 Certificate Revocation and Status Checking

Per the requirements in the PCA CP, the Certificate Revocation and Status Checking Requirements apply equally to all NG9-1-1 Certificates.

11 Employee and third party issues

11.1 Trustworthiness and Competence

11.1.1 Training and Skills Level

No Stipulation.

11.1.2 Separation of Duties

Per the CP.

11.2 Delegation of Functions to Registration Authorities and Subcontractors

11.2.1 General

The CA MAY delegate the performance of all or any part of a requirement of these Guidelines to an Affiliate, RA or LRA, or subcontractor, provided that the process employed by the CA fulfills all of the requirements of these Guidelines.

The party that so delegates any such performance remains wholly responsible for ensuring that all requirements of this document and the CP are met.

11.2.2 Local Registration Authority (LRA)

The RA for a CA MAY authorize the Subject of a valid NG9-1-1 Certificate to perform the RA function and authorize the CA to issue NG9-1-1 Certificates at the Tier controlled by the Subject's issuing CA. In such case, the Subject SHALL be considered an LRA, and the following Requirements SHALL apply:

1. The LRA SHALL NOT authorize the CA to issue Certificates at a Tier other than for the Tier that the CA directly issues Certificates.
2. In all cases, the LRA MUST be an organization verified by the RA in accordance with these Guidelines.

3. The RA MUST monitor compliance with these Guidelines by the LRA.
4. The Final Cross-Correlation and Due Diligence requirements of these Guidelines equally apply to the LRA; and
5. The audit requirements of these Guidelines SHALL apply to the LRA, except in the case where the CA maintains control over the Private Key used to issue the Certificates authorized by the LRA, in which case, the LRA MAY be exempted from the audit requirements.

11.2.3 Guidelines Compliance Obligation

In all cases, any delegate having delegated Authority must be contractually obligated to the delegator to comply with all applicable requirements in these Guidelines and to perform them as required of the delegator itself. The delegator SHALL enforce these obligations and internally audit each of their delegate's compliance with these Requirements on an annual basis.

11.2.4 Allocation of Liability

Per the CP.

12 Data Records

Per the CP.

13 Data Security

Per the CP.

14 Audit

Per the CP.

14.1 Eligible Audit Schemes

Per the CP.

14.2 Per the CP Audit Period

Per the CP.

14.3 Audit Record

Per the CP.

14.4 Pre-Issuance Readiness Audit

No stipulation.

14.5 Per the CP Regular Self Audits

Per the CP.

14.6 Per the CP Auditor Qualification

Per the CP.

14.7 Per the CP Root CA Key Pair Generation

Per the CP.

15 Liability and Indemnification

Per the CP.

16 Acknowledgements

The National Emergency Number Association (NENA) 9-1-1 Core Services Committee, PCA Certificate Policy Working Group developed this document at the request of the Next Generation 9-1-1 Interoperability Oversight Commission.

Members	Employer
Steve O'Conor, ENP, 9-1-1 Core Services Committee Co-Chair, WG Co-Chair	NG9-1-1 Consulting Services, LLC
Theresa Reese, 9-1-1 Core Services Committee Co-Chair, WG Co-Chair	Ericsson Inc.
Brandon Abley, ENP	NENA
Tom Breen, ENP	SecuLore Solutions, LLC
Guy Caron, ENP	Bell Canada
Mark Fletcher, ENP	911inform, LLC
Suresh Gursahaney	MicroAutomation Inc
Diane Harris, ENP	Zetron Inc
Rob Howard	NYC3 Cyber Command
Chris Kellett	CRTC Emergency Services (9-1-1)
Erik Loberg	GeoComm Inc.
Oscar Marcia	Eonti
Roger Marshall	Comtech Telecommunications Corp.
Steve McMurrer, ENP	Fairfax County VA
William Mertka	Synergem Technologies Inc.
Roman Mezhericher	City of New York
Jackie Mines	Mission Critical Partners, LLC

Members	Employer
Dan Mongrain	Motorola Solutions, Inc.
Michael Newburn	AT&T
Brian Rosen	Consultant
Matthew Schreiner	Mission Critical Partners, LLC
Michael Smith	Equature/DSS Corp.
Tom Soulos	MicroAutomation Inc.
Jamie Taylor	City of Lee's, Summit MO
Fabricio Velez	Nokia
C. A. Patrick Voigt-ENP	Synergem Technologies Inc.
Curtis Wolfenberger Sr	INdigital