NENA
THE 9-1-1 ASSOCIATION

Validation Policy Overview

FEBRUARY 9, 2022

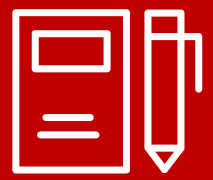
Describing the Certificate Validation Policy

We will provide an overview of

- What the Validation Policy (VP) is
- What roles participate in validation
- How information is validated prior to certificate issuance
- …with examples along the way

What is the Certificate Validation Policy?

- **Describes validation**
  - The guidelines for making sure that entities are who they say they are – sort of like a background check



- **Lists stakeholder roles and responsibilities**
  - From agencies, to users, to the CA and ICAs, and other entities in between

- **Details the process of verifying information**
  - Different data requires different processes

Why do we need a Validation Policy?

So that we can issue trustworthy certificates to prevent bad actors from disrupting emergency services and safely engage with other entities and networks we interact with

What is validation?

- Validation is the process of verifying the identity of entities requesting NG9-1-1 certificates, as outlined in the Certificate Policy
- Validation allows a CA to establish Certificate Warranties indicating that the CA followed the guidelines in the CP, VP, and CPS (if applicable) to verify the accuracy of information in the certificates they issue

NG9-1-1 Certificate Warranties

- **Legal Existence**
  - The Subject in the certificate exists and is legally valid in the Jurisdiction of Incorporation.
- **Identity**
  - The Identifier, Role(s), Agency affiliation and Owner are correct and have been validated within the NG9-1-1 validation chain.
- **Accuracy of Information**
  - The CA has taken all steps reasonably necessary to verify accuracy.

The CA warrants these to Relying Parties, in accordance with the CP, VP, and CPS (if applicable)

NG9-1-1 Certificate Warranties

- Subscriber Agreement
  - The Subject in the certificate has entered into a Subscriber Agreement with the CA, RA, or LRA, or if affiliated, the Agency has acknowledged and accepted the Terms of Use
- Status
  - The CA will run an online repository with current status of the certificate (valid or revoked) consistent with CP and CPS (if applicable)
- Revocation
  - The CA, RA, or LRA will revoke the certificate for any reasons outlined in the CP, VP, and CPS (if applicable)

Roles and Responsibilities

- **CA** Certificate Authority
- **ICA** Intermediary Certificate Authority
- **RA** Registration Authority
- **LRA** Local Registration Authority
- **Entities** These, as well as Services, Elements, Agencies, and Users (Agents)

Entities

- **Services** — A NG9-1-1 service, such as an ECRF
- **Elements** — A specific element of a service, such as one ECRF server within a cluster that make up the entire ECRF service
- **Agencies** — A NG9-1-1 Agency, such as a PSAP
- **Users** — Agents (and future, Automaton)

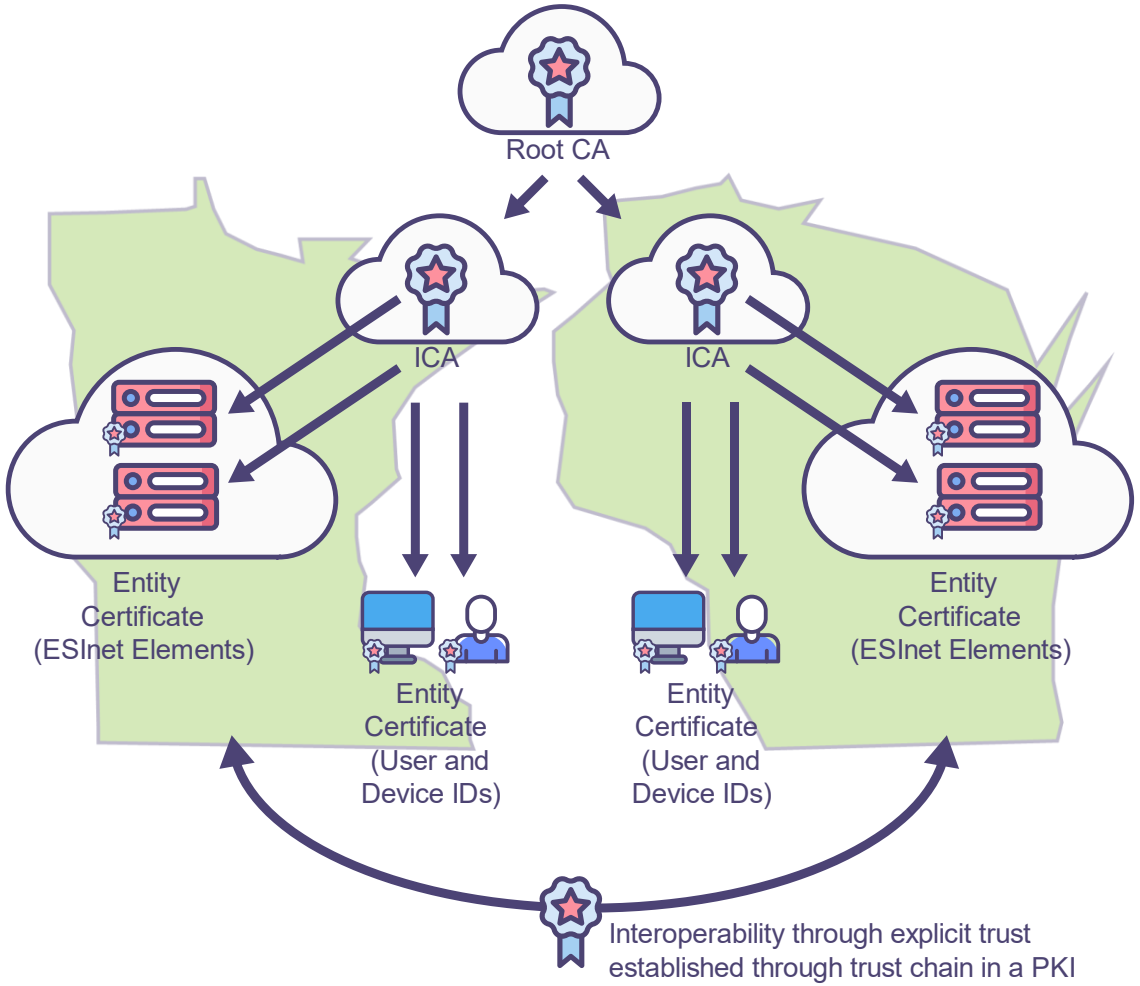
Each of these need NG9-1-1 certificates and must be validated by the VP.

NG9-1-1 Certificate Types and Who Validates Them

- **Root Certificate**
  - Validated by an auditable ceremony per the CP
- **ICA Certificate**
  - Validated by the RA for the CP, or the RA in the CPS governing the signing ICA
- **Agency Certificate**
  - The RA for the ICA
- **Service Certificate**
  - The RA or LRA for a CA with delegated authority to perform validation
- **Element Certificate**
  - The RA or LRA for a CA with delegated authority to perform validation
- **User Certificate**
  - The RA or LRA for a CA with delegated authority to perform validation

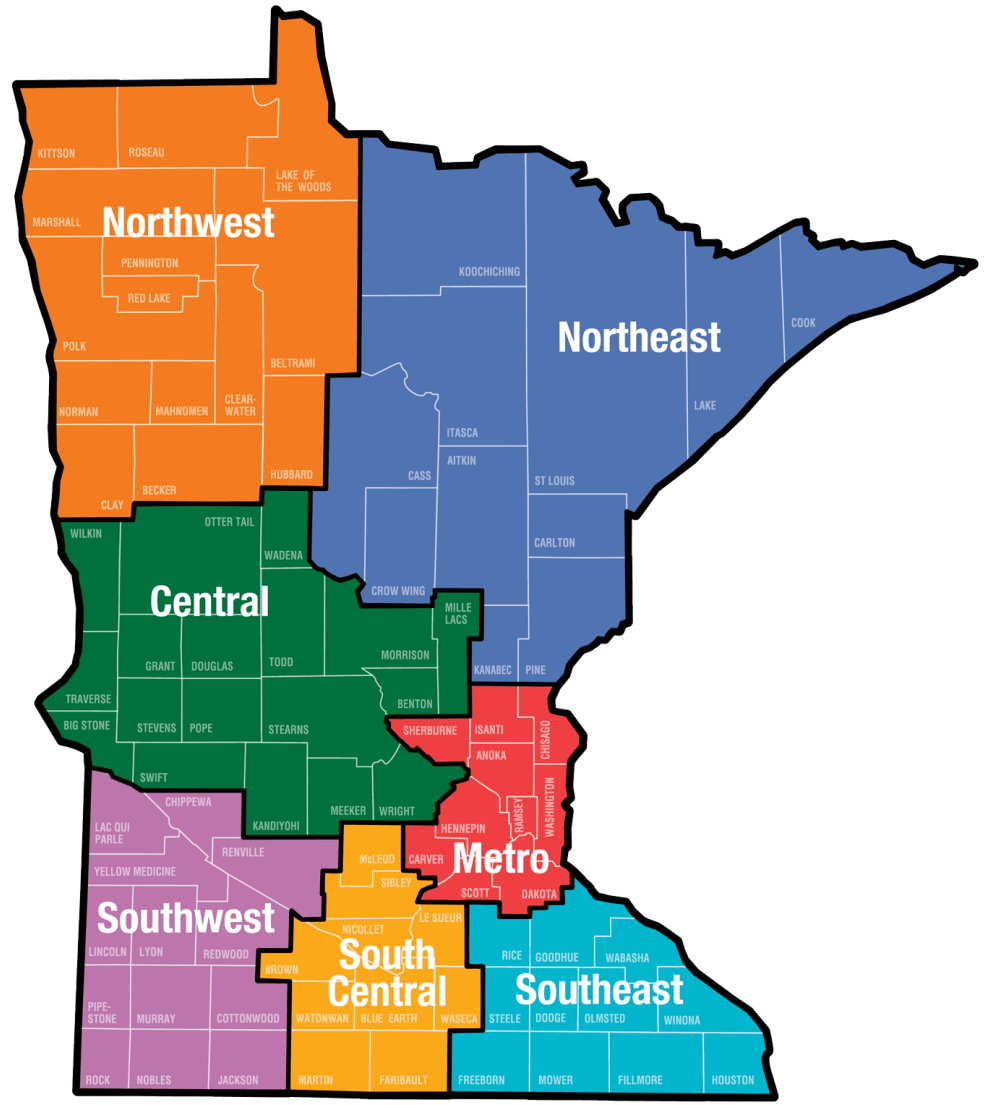
An Example – A PKI Spanning Multiple States

- Sharing a root of trust in a PKI allows one element to trust that another element is a 9-1-1 entity
- This eases things like transferring calls between ESInets or querying elements in a different ESInet
- Also, since there is no trust, you need it within your own ESInet too
- It also enhances security by establishing a trust chain unique to NG9-1-1
- Establishing that NG9-1-1 has its own trust chain has significant impact to standards development
- Every system needs certificates anyway; i3 just standardizes them to enhance interoperability in NG9-1-1



Example Case: Minnesota

- Minnesota has a statewide emergency communications board, which could serve as the Governing Authority/Policy Authority for a statewide Issuing Certificate Authority (ICA) under the Root CA (the PCA) – which would have its own Certificate Practice Statement (CPS)
- The state agency for Emergency Communication Networks could manage the day-to-day technical operations of ICA (or its vendor could) serving as the Managing Authority for the overall ESInet
- The same state agency could designate employee(s) as the Registration Authority (with proper separation of Roles!)
- The 7 communications regions could provide Local Registration Authority (LRA) functions, validating each county/municipal Agency and PSAP with more local knowledge than the state
- This is just an example; jurisdictions have a lot of flexibility in how to deploy a leg of the PKI



What Does a NG9-1-1 Certificate Contain?

```
OBJECT IDENTIFIER 1.3.6.1.4.1.55670.1.1
[0] (1 elem)
UTF8String agencyId/
foo.allegheny.pa.us/
urn:emergency:service:responder.psap,
urn:emergency:service:responder.police.local,
urn:emergency:service:responder.fire.local,
urn:emergency:service:responder.ems.local/
```

Each CP release has a unique OID.

"ID Type" field here is "agencyID" because the certificate is for an agency.

Agency IDs have a globally unique FQDN.

These Roles convey that the Certificate holder is an Agency that answers 9-1-1 calls, and is also a police, fire, and EMS agency

Specific Verification Occurs Prior to Issuing a NG9-1-1 Certificate

- Role
- Agency Identity
- Owner
- Applicant's Legal Existence and Identity
- Applicant's Physical Existence – Place of Operations
- Method of Communication
- Applicant's Operational Existence
- Name, Title, and Authority of Contract Signer and Certificate Approver
- Signature on Subscriber Agreement and NG9-1-1 Certificate Requests
- Approval of NG9-1-1 Certificate Request
- Applicant on Denied Lists or Other Legal Unapproved Lists
- Parent/Subsidiary/Affiliate Relationship

Verification of Role

- The RA or LRA validates that the requested Roles for the Subject conform to Roles in the appropriate registery(ies)
- For example, Agency certificates must have one or more Roles from the Agency Roles registry (STA-010.3 Section 10.27) and one or more Roles from the urn:emergency:service:responder namespace (or its sub-registries) as defined in STA-010.3 Section 10.5
  - Roles for a PSAP that dispatches Fire, Law, and EMS would include “PSAP”, “Dispatch”, and “urn:emergency:service:responder.psap”

Verification of Agency Identity

- The RA or LRA must confirm that the Agency ID (in the form of a Fully-Qualified Domain Name or FQDN) is under the Agency's control
- Four, and only four, methods can be used to prove this:
  - Agreed-upon DNS record change (random value or request token)
  - Agreed-upon IP address change in DNS
  - Agreed-upon Change to Website (v2)
  - Agreed-upon Change to Website (ACME)
- It's all about an Agency proving they own a web presence.

Verification of Owner

- Owners are verified in a few different ways, depending on the type of certificate.
- If the Owner is an Agency, an electronic signature is required from the Agency whose FQDN matches the Owner field
- When the Owner is a CA, the fact that the CA issued the certificate is sufficient to validate the Owner as being the CA.
- Private Entities need a sponsor Public Safety Entity to be the Owner for its Agency, Agent, Element, and Service certificates. If there is no sponsor, the Private Entity needs an Agency certificate approved by the Managing Authority for the CA or CPS.

Verification of Applicant's Legal Existence and Identity

- The RA or LRA must:
  - Verify the certificate applicant is a legally-recognized Public Safety Entity or a Private Entity with a valid public safety purpose
  - Ensure the Applicant's name in the certificate request is its legal name
  - For private entities, obtain the Applicant's Registration Number or the date of their incorporation or registration. Also ensure the request did not come from a Registered Agent.
  - Verify that the Applicant or the element which they control is performs a legitimate public safety function required for NG9-1-1
  - Verify the identify of the entity's Principal Individual in a face-to-face meeting
  - Verify the Agency ID
- Depending on the type of entity, information obtained from a Qualifying Government Information Source (QGIS), or Qualified Independent Information Source (QIIS) may be used for verification

Verification of Applicant's Physical Existence – Place of Operations

- The CA, RA, or LRA must verify that the applicant's physical address is where they conduct operations
- A QGIS, QIIS, or Qualified Government Tax Information Source (QTIS) may be used; if not available, a site visit must be conducted to verify the applicant's address

Verification of Method of Communication

- The RA or LRA must verify the applicant's communication method – either telephone number, fax number, email address, or postal address
- The information must match that found within a QGIS, QIIS, or QTIS
- The information must also be used to contact the entity or its parent, subsidiary, or affiliate to verify the contact information can truly be used to reach the applicant

Verification of Applicant's Operational Existence

- The CA, RA, or LRA must verify that the applicant engages in its stated roles.
- This can follow the method established for verifying a Public Safety Entity's legal existence (described previously), with a few additional stipulations, such as for Private Entities, verification must only rely upon information in a QGIS or QIIS, and allowances, such as allowing verification of Public Safety Entities via confirmation with a superior governing Public Safety Entity or a judge active in the Entity's political subdivison.

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

- The RA or LRA must verify
  - The Name, Title, and Agency of the Contract Signer and the Certificate Approver, and that they are legal agents representing the applicant
  - The signing authority of the Contract Signer
  - The authority of the Certificate Approver to submit the NG9-1-1 Certificate Request for the applicant, to provide the applicant's information to the issuing CA, and approve certificate requests submitted by a Certificate Requester
- The VP specifies the means by which this information can be verified, such as through Independent Confirmation from Applicant
- Contract Signers and Certificate Approvers can be "trusted" based on prior contracts they have signed or approved, reducing the need for revalidation each time a certificate is requested

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

- The CA, RA, or LRA must verify the Contract Signer's signature on Subscriber Agreements, and the Certificate Requester's signature on Certificate Requests
- This can be done by
  - Contacting the applicant using the Verified Method of Communication or via mailed letter, to the attention of the Certificate Requester or Contract signer, and obtaining a response from someone who identifies themselves as the person that provided the signature
  - Use of a secure signature process with appropriate logins that identify the signers or digital signatures that use verified certificates

Verification of Approval of NG9-1-1 Certificate Request

- If a Certificate Request was submitted by a Certificate Requestor, before the CA issues the certificate, the CA, RA, or LRA needs to verify that the request was reviewed and approved by a Certificate Approver.
- This can be done by
  - Contacting the Certificate Approver using a Verified Method of Communication and obtaining oral or written confirmation
  - Notifying the Certificate Approver that one or more requests are available for approval, and having them log into a secure website to do so; the login action and approval within the system serves as verification
  - Verifying the Certificate Approver's signature on the certificate request

Verification of Applicant on Denied Lists or Other Legal Unapproved Lists

- The RA or LRA must verify that the Applicant, Contract Signer, Certificate Approver, and the Applicant's Jurisdiction of Incorporation, Registration, or Place of Operations
  - are not any government deny lists, or other such lists (i.e. prohibited persons
  - Are not in countries that are prohibited from doing business with the CA's jurisdiction
- This can be verified by examining
  - US Bureau of Industry and Security (BIS) Denied Persons List
  - BIS Denied Entities List
  - US Treasury Department List of Specially Designated Nationals and Blocked Persons
  - US Government export regulations
- If the CA has operations in other countries, the CA needs to verify the lists and regulations of those other countries as well

Verification of Parent/Subsidiary/Affiliate Relationship

- If the RA or LRA, when verifying an Applicant, has used information from the Applicant's parent, subsidiary, or affiliate, the relationship between the Applicant and the other entity must be verified.
- Verification can be performed by
  - Examining information about the relationship in a QIIS or QGIS
  - Obtaining Independent Verification from the related entity
  - Using an existing, verified contract between the CA or RA and the related entity
  - Obtaining a Verified Professional Letter
  - An authenticated resolution that approves the creation of the Subsidiary or Applicant

Other Notable Guidelines

- The RA or LRA must identify and resolve discrepancies in Certificate Applications before issuance, by having a person that was not responsible for the initial collection of information conduct a thorough review and follow the VP's guidelines for discrepancy resolution
- The VP details the "expiration dates" of validated information. For example, the Address of Place of Operations is good for three years; after such time it must be verified again when issuing new certificates
- Identity and Background Verification of employees of the CA, RA, or LRA that will engage in the processes outlined in the VP, prior to hire
- VP allows for delegation of CA functions to other entities (like RAs) and subcontractors and contains guidelines on what a RA, ICA, and LRA must follow; the CA is ultimately responsible
- Other guidelines such as Data Records, Data Security, and Audits are simply per the CP and are not expanded upon in the VP.

Questions?

Contact admin@ng911ioc.org with any questions.