An International Model for Next-Generation 9-1-1 and Emergency Calling Systems in the United States, Canada and Beyond

Brandon Abley
Director of Technology
NENA: The 9-1-1 Association

Agenda

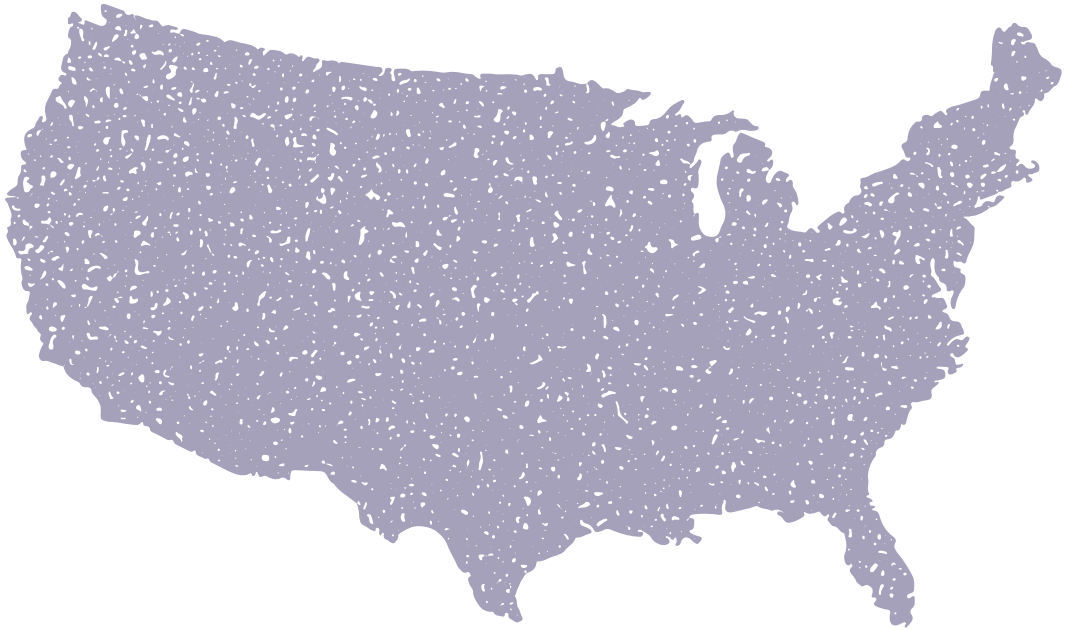
- Context in North America
- Public Key Infrastructure and Managing Trust
- Location-Based Routing Interoperability and the Forest Guide
- Trans-Continental Plugtests

About NENA

- NENA: the 9-1-1 Association is THE standards, policy, advocacy and education organization for 9-1-1 in North America and beyond
- NENA has over 15,000 members and growing
- NENA technical and operational standards govern how 9-1-1 and NG9-1-1 systems work across the United States and the world
- NENA is the only open-standards organization dedicated to 9-1-1 issues

9-1-1 in the United States

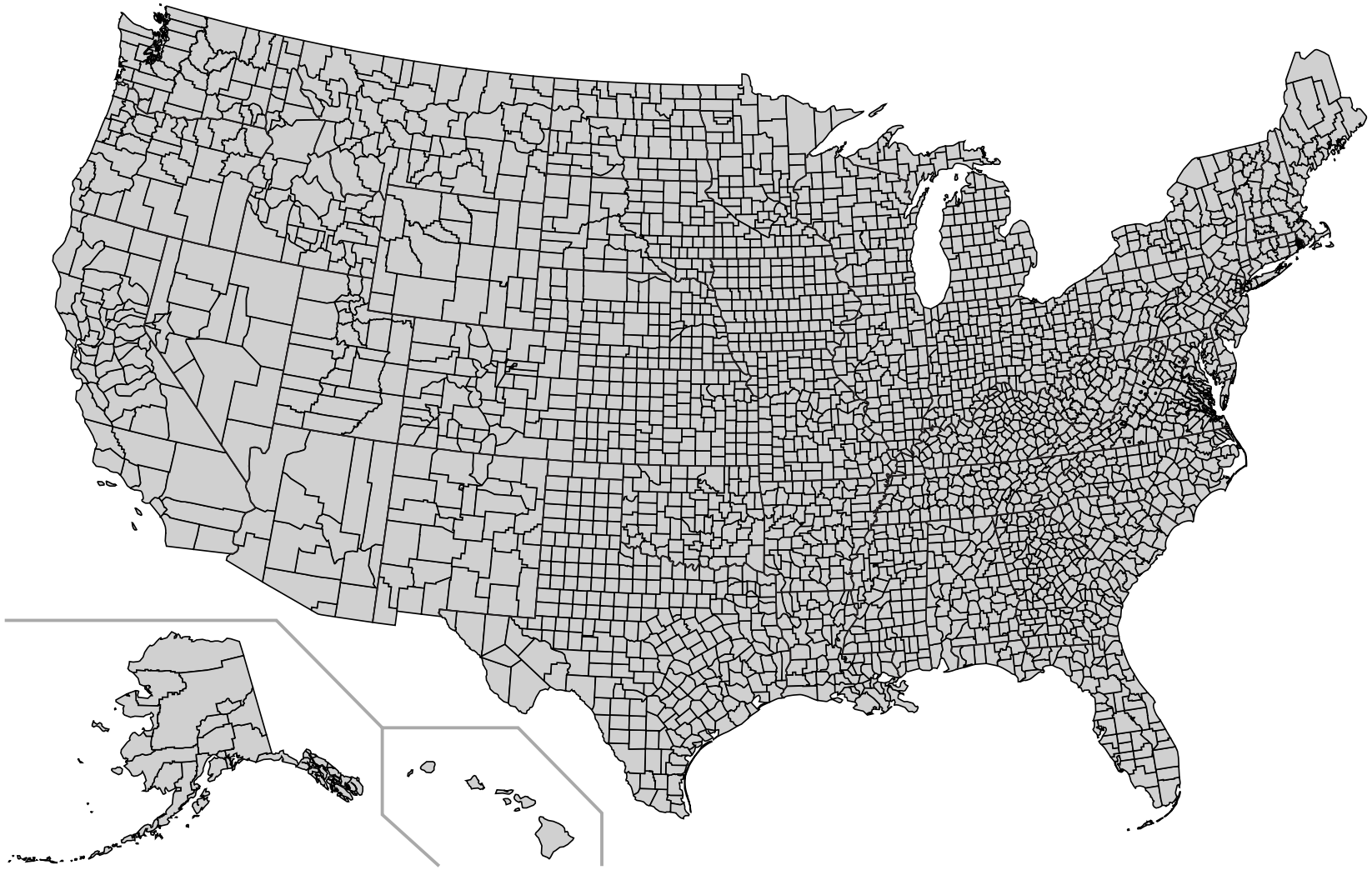
- 9-1-1 is the universal number to reach emergency services in the United States, Canada and Mexico
- In USA, enforced both by statute (state and national law) as well as regulatory (Federal Communications Commission)
- International equivalents: 1-1-2, 9-9-9, 1-1-9
- In many cases, dialing the emergency number for another region will transfer the caller to the correct service (e.g., 1-1-2 in USA often reaches 9-1-1)



Key Challenges in USA

- Number of PSAPs: over 6000 PSAPs
- Number of jurisdictions: thousands of jurisdictions for 9-1-1 purposes
- Lack of interoperability: 9-1-1 service is the responsibility of competitive private industry and state and local government, so there are many different systems in the country; for 9-1-1, USA is like 56+ countries, not one
- Uneven funding: every locality has a different funding levels, not always fair
- Legacy Networks: by deploying a single emergency number service early (1960s!), USA has to support very old technologies in addition to modern ones

Over 3000 jurisdictions for 9-1-1 in USA



. . . and more in North America

. . . and more and more

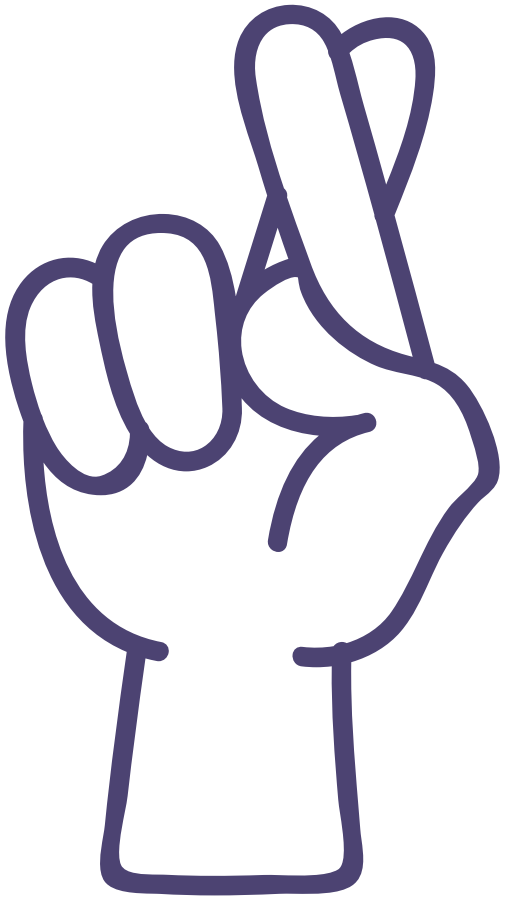
. . . and more and more and more

9-1-1 Issues are Complicated in USA

- USA has had 9-1-1 as a universal telephone number for over 50 years
- 9-1-1 is considered an essential service in the US; any failure of 9-1-1 is highly publicized and the public considers the service as **always on**
- Due to its long service life, USA 9-1-1 has many legacy technologies to support
- With over 3000 counties that each have some individual control over how 9-1-1 is handled in each jurisdiction, political and funding issues are diverse
- For 9-1-1 purposes, USA is analogous to 56 or more countries, not one
- This makes the North American model analogous to the international model

NG9-1-1 has Trust Issues

- Generally, even mundane transactions via IP require a secure connection (TLS)
- Modern security convention utilizes zero-trust framework: Trust nobody
- . . . **especially** when someone says you can trust them
- Public Key Infrastructure (PKI) establishes a chain of trust
- NG9-1-1 standards (i3) require that the PCA be created for the NG9-1-1 PKI
- The PCA is a Certificate Authority (CA) for NG9-1-1
- NENA is establishing the PCA to fulfill needs that arose from the standards development community



Statement of Problem

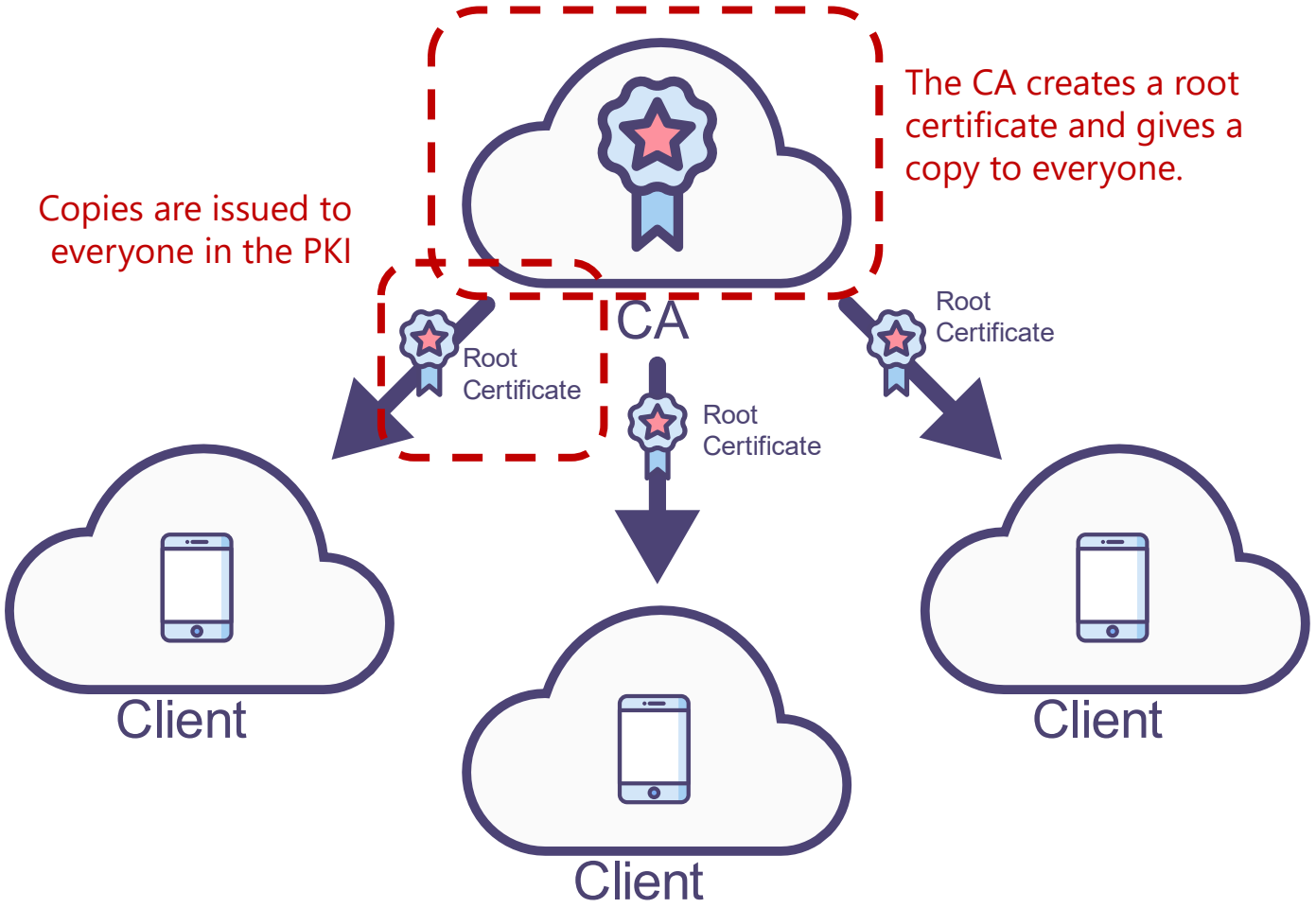
If you remember one thing about PKI:

- Trust nobody
- Especially if someone claims trustworthiness
- Always check with a third party to establish trust

Key Terms

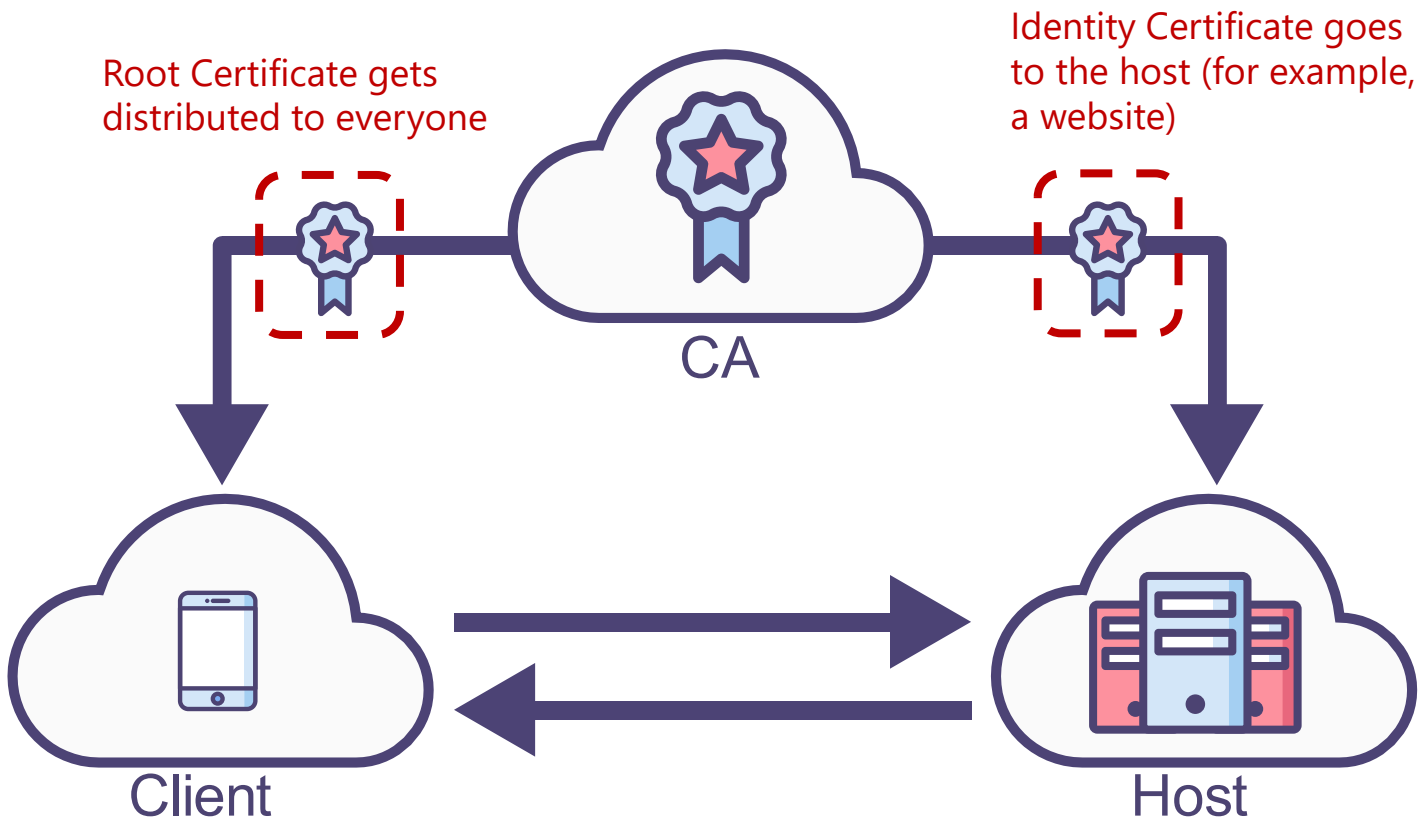
- TLS: Transport Layer Security
- PKI: Public Key Infrastructure
- CA: Certificate Authority
- ICA: Issuing Certificate Authority
- PCA: PSAP Credentialing Agency
- Root Certificate
- Identity Certificate (or just “certificate”)

Root + Identity Certificate



- To establish PKI, the first step is to create and sign a root certificate
- Everyone in the PKI must get a copy
- The easiest way to distribute the root certificate is to just pre-install it.
- For example, about 400 root certificates are pre-installed in Google Chrome; this is how the public internet negotiates trust
- Certificates can be installed manually, but this introduces management overhead to the PKI

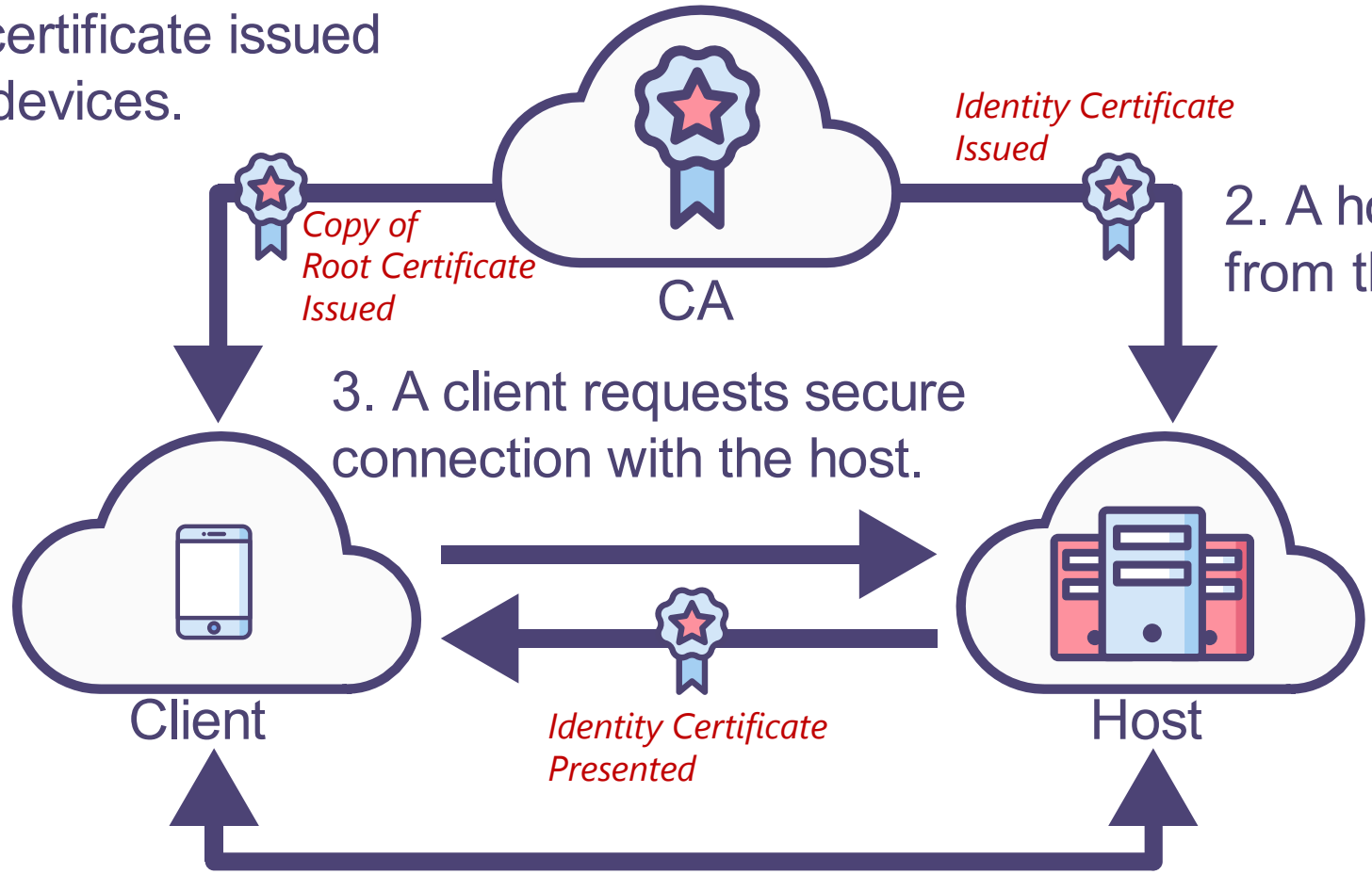
Root + Identity Certificate



- PKI has root certificates and identity certificates
- Both are used by the client to establish trust
- The root certificate is the basis of the trust chain. The root certificate is created by the CA and issued to everyone.
- Individual entities then each get their own unique identity certificate.
- Whenever a secure session is set up between a client and a host, the host presents its identity certificate. The client checks to make sure the host's identity certificate shares the same root certificate that it has a copy of.

Certificate Exchange

1. Root certificate issued to client devices.



2. A host gets their identity certificate from the CA to prove their identity.

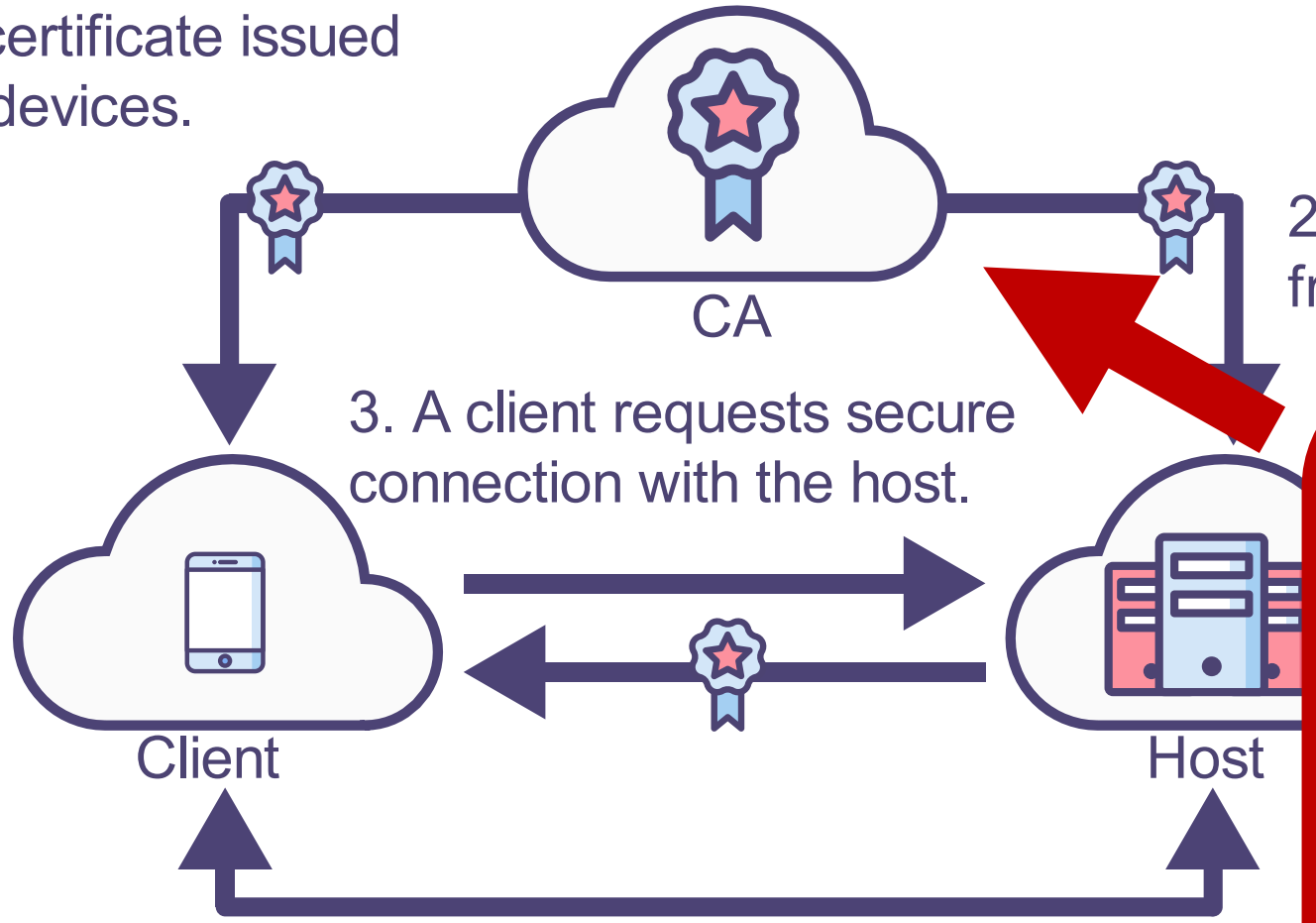
3. A client requests secure connection with the host.

4. Host responds with its signed certificate.

5. Client can confirm that the host certificate is valid because it can trace trust back to the CA.

Certificate Exchange

1. Root certificate issued to client devices.



2. A host gets their identity certificate from the CA to prove their identity.

3. A client requests secure connection with the host.

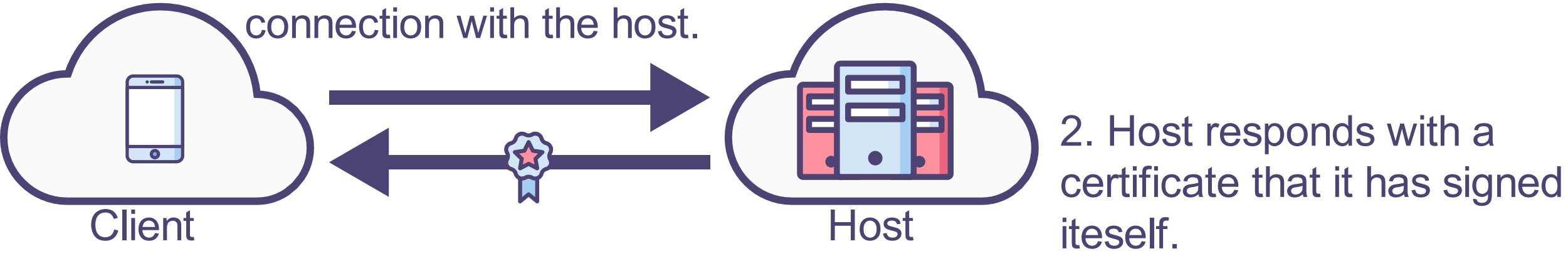
5. Client can confirm that the host certifica
is valid because it can trace trust back to th

Trust comes from the Certificate Authority (CA) and its root certificate

The client does not trust the host until it can determine through the CA's chain of trust that it is a trusted entity. This is analogous to a background check

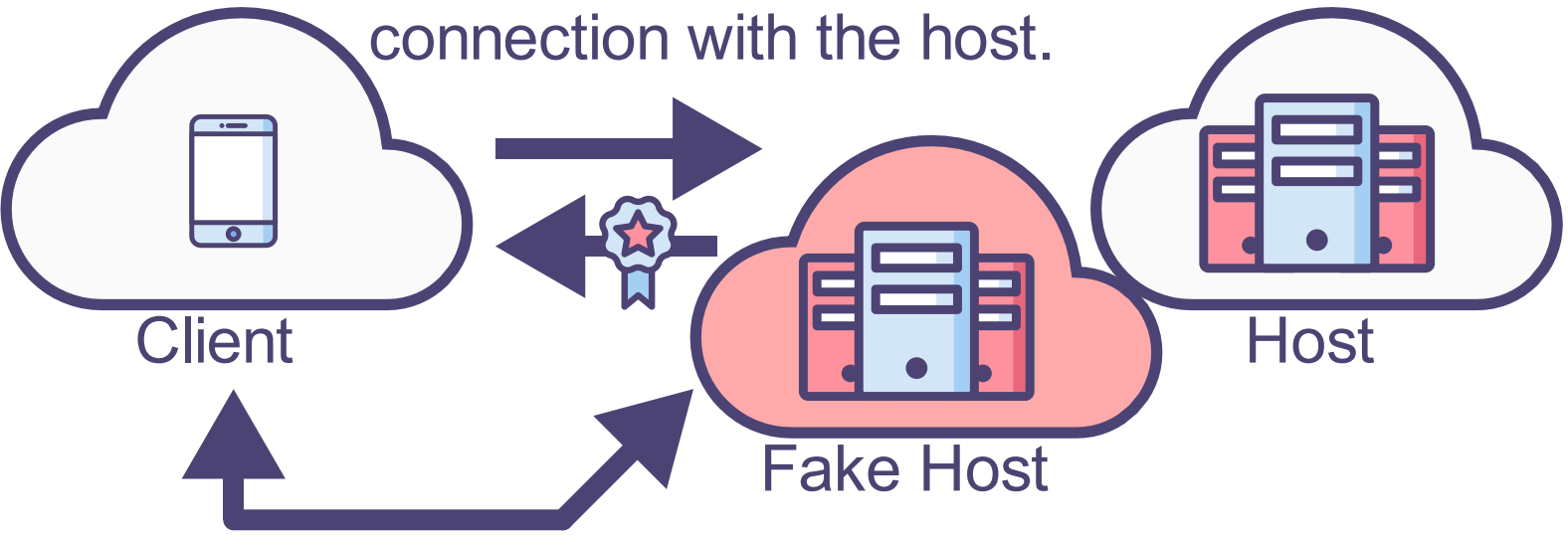
In PKI there is NO trust until trust is proven by tracing back to the CA

Self-Signed Certificate (NOT ALLOWED)



- It’s very easy to generate a certificate
- Why not just generate your own without dealing with a third party CA and save time and money?
- What could possibly go wrong . . . ?

Self-Signed Certificate (NOT ALLOWED)



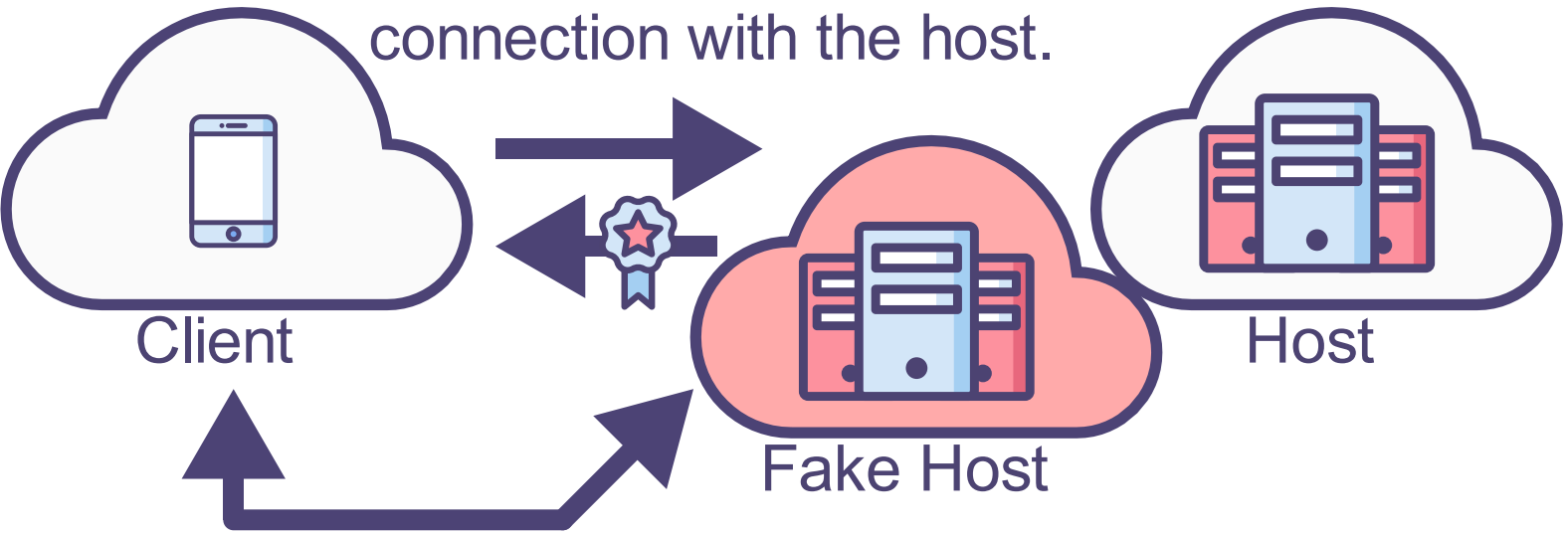
2. Fake host intercepts, claiming to be the host, with a certificate it signed itself.

3. The client can't tell the difference between the real host or the fake host because it does not verify their identity with a third party.

. . . turns out if I trust self-signed certificates, I am easily fooled

That's what you get for trusting people

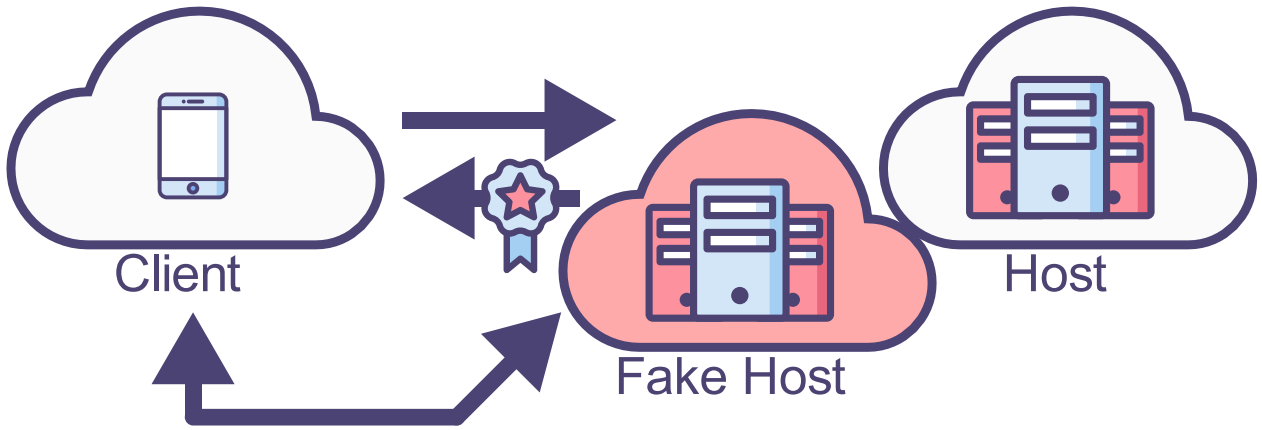
Self-Signed Certificate (NOT ALLOWED)

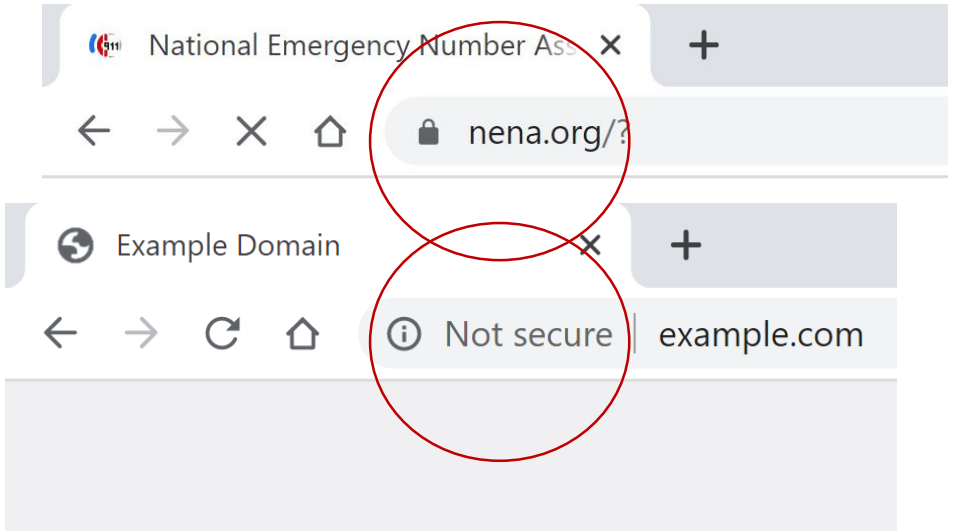


2. Fake host intercepts, claiming to be the host, with a certificate it signed itself.

3. The client can't tell the difference between the real host or the fake host because it does not verify their identity with a third party.

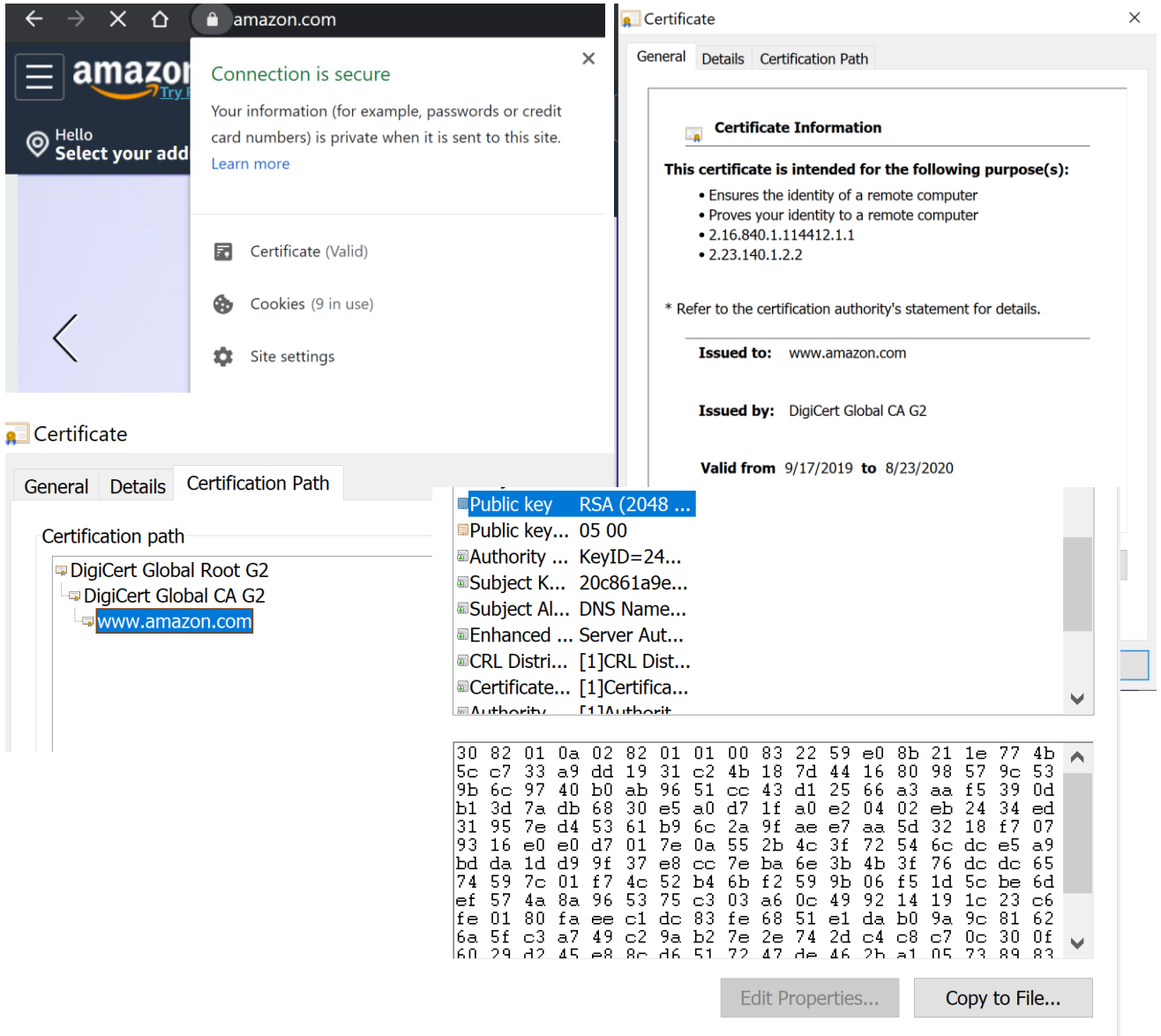
Inconvenient, but Necessary





- Managing certificates from a CA is inconvenient
  - It costs money
  - They need to be renewed
  - You feel foolish if you let them expire
- However, it is necessary; both as a best practice, and it is required under standards (i3)
- Web browsers will warn you if you even try to access to public website and TLS fails
- . . . so it is a very modest requirement for 9-1-1
- However, NG9-1-1 has special needs for how it handles trust

Example: amazon.com



- It is easy in most web browsers to look at the certificate and see an example of a PKI
- The public internet has many CA providers are all mutually agreed-upon to be trustworthy, and you can get a certificate from any one of them
- All of their root certificates (400+) are included in major web browsers. This is the foundation of trust over the public internet
- For example, you can see amazon.com's certificate issued by DigiCert. My web browser has their root certificate already installed, so it can confirm amazon.com is safe and that I am at the real amazon.com

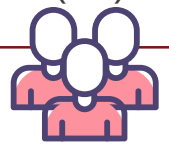
What is PKI?

- PKI (Public Key Infrastructure) is a set of:
  - Roles
  - Policies
  - Hardware
  - Software
  - Procedures
- . . . needed to create and manage a chain of trust through creation and management of certificates
- It is similar to the chain of trust for the public internet, but limited to an industry with a special need for managing identity
- In NG9-1-1, inter-jurisdiction interoperability is one such special need
- PKI involves a lot of technology
- However, PKI is much more than technology
- “Soft” side—governance, policies—are more important and complicated than the technology

Chain of Trust

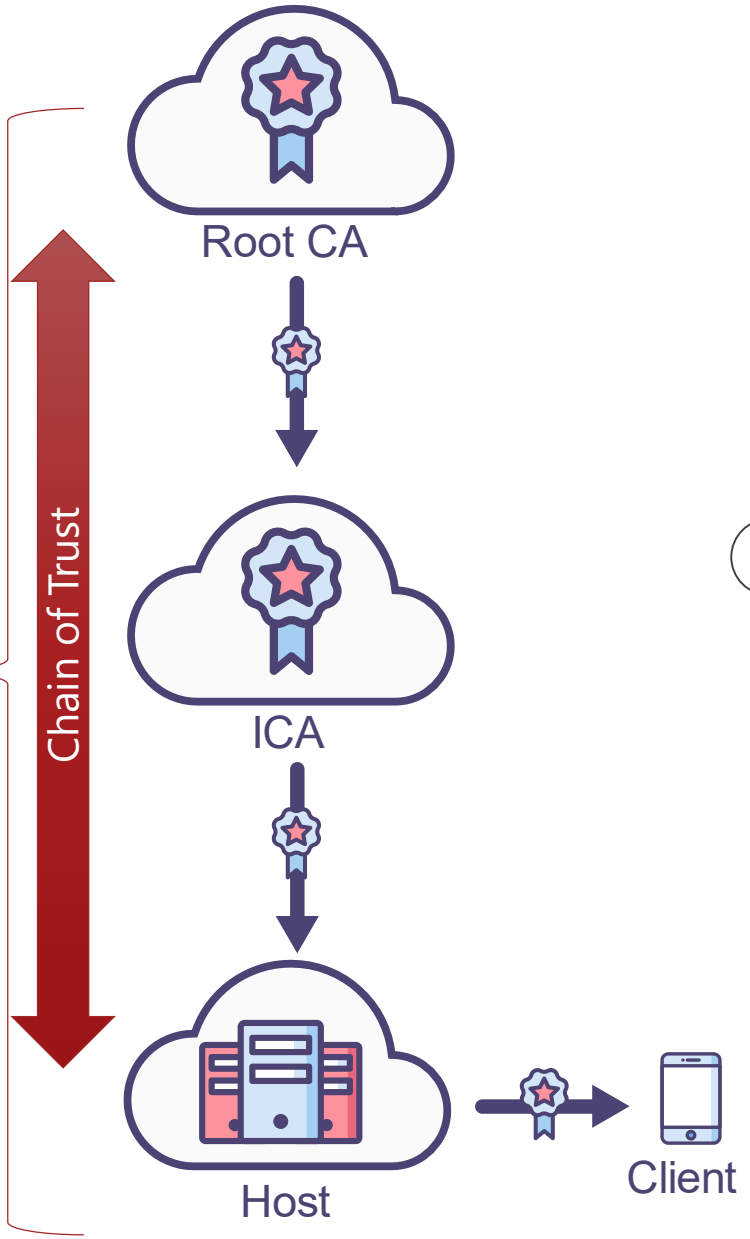
① **Governance**:
- Specifications / Standards
- Certificate Policy (CP)

Policy Authority (PA)



Management Authority (MA)

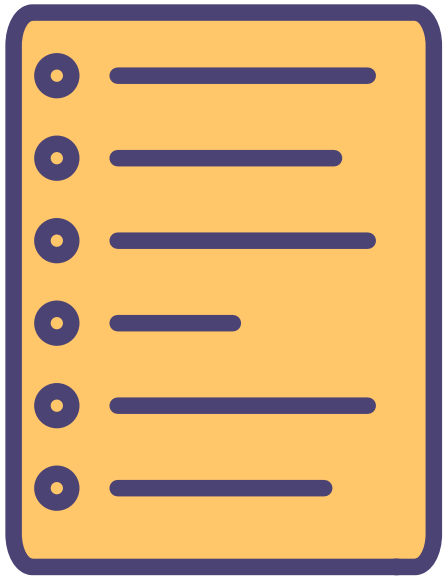
③ **Operations**:
- Subscriber Identification
- Certificate Lifecycle Management
- Compliant Device Management



Certification Authority (CA)

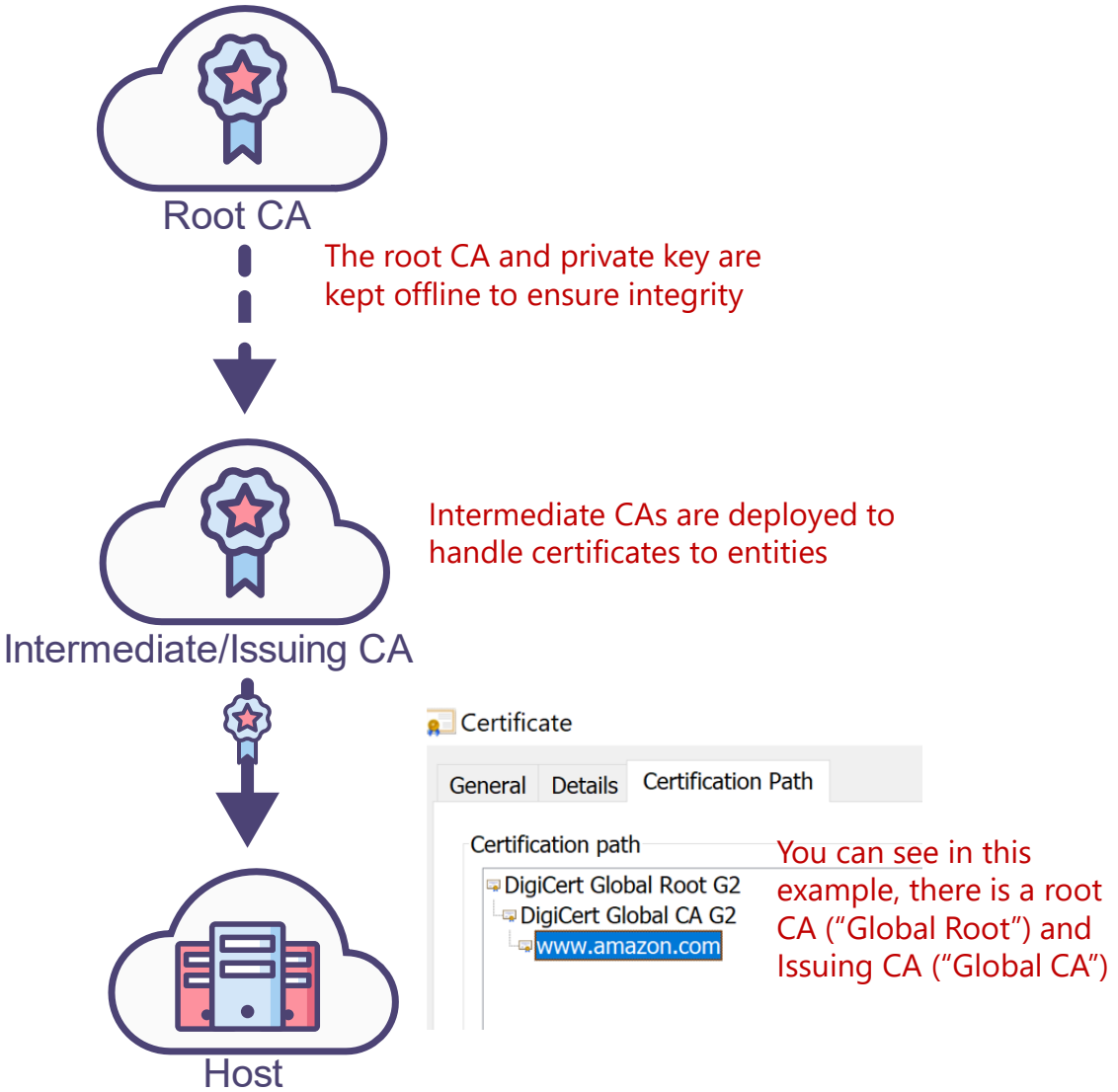
② **Technology**:
- Public Key Infrastructure (PKI)
- Certificate Practice Statement (CPS)
- Repositories
- CRL / OCSP infrastructure

The CP



- The Certificate Policy CP is the most important part of a PKI
- The CP describes how certificates are issued, who can get one, how certificates are revoked and suspended, how long a certificate is valid, what the trust chain looks like, and more
- In a PKI, it is a founding document analogous to a constitution or set of bylaws
- Before you have a PKI, you must have a CP
- All parties must agree to the CP

Securing the Root

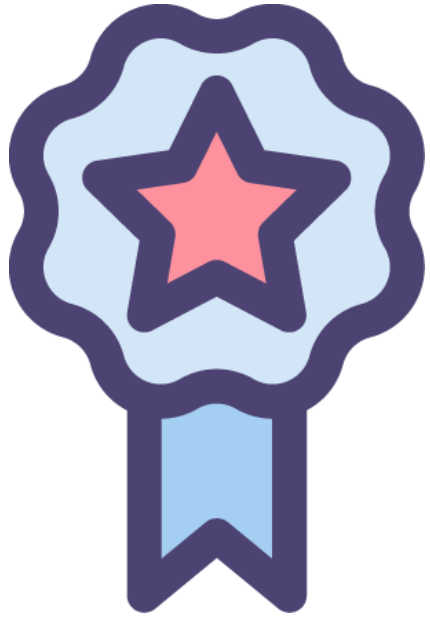


You can see in this example, there is a root CA ("Global Root") and Issuing CA ("Global CA")

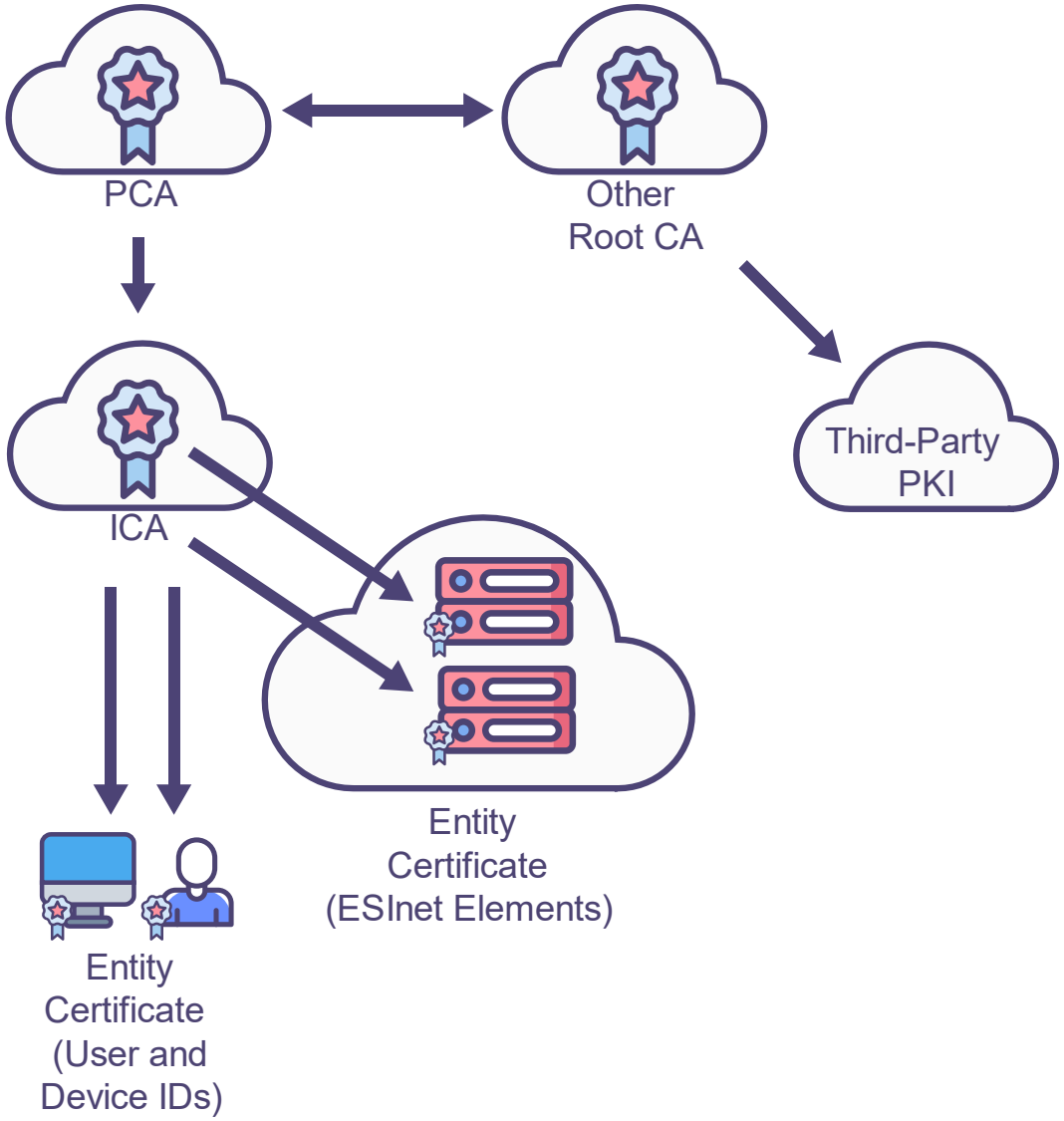
- Every certificate is signed (created) with a set of random numbers called a private key
- This must be kept secret. Anyone that steals your private key can pretend to be you.
- If the private key is compromised, the certificate MUST be revoked
- If the root certificate's private key is compromised, the entire PKI is compromised
- For this reason, the CA private key is typically stored offline, in a physical vault, on special secured hardware
- The Root CA itself is also offline, so that it can never be attacked. There is always an intermediate CA that interacts with other agents, never directly the root.

The PCA

- PSAP Credentialing Agency
- The PCA is a CA, but for 9-1-1
- Root of trust for NG9-1-1 and emergency calling
- NG9-1-1 PKI and PCA are not special technically
- However, PCA is the root CA in the NG9-1-1 PKI
- It is a required functional element in i3
- PCA may not necessarily be limited to NG9-1-1
- NENA plans to issue stand up and operate PCA for USA in 2020

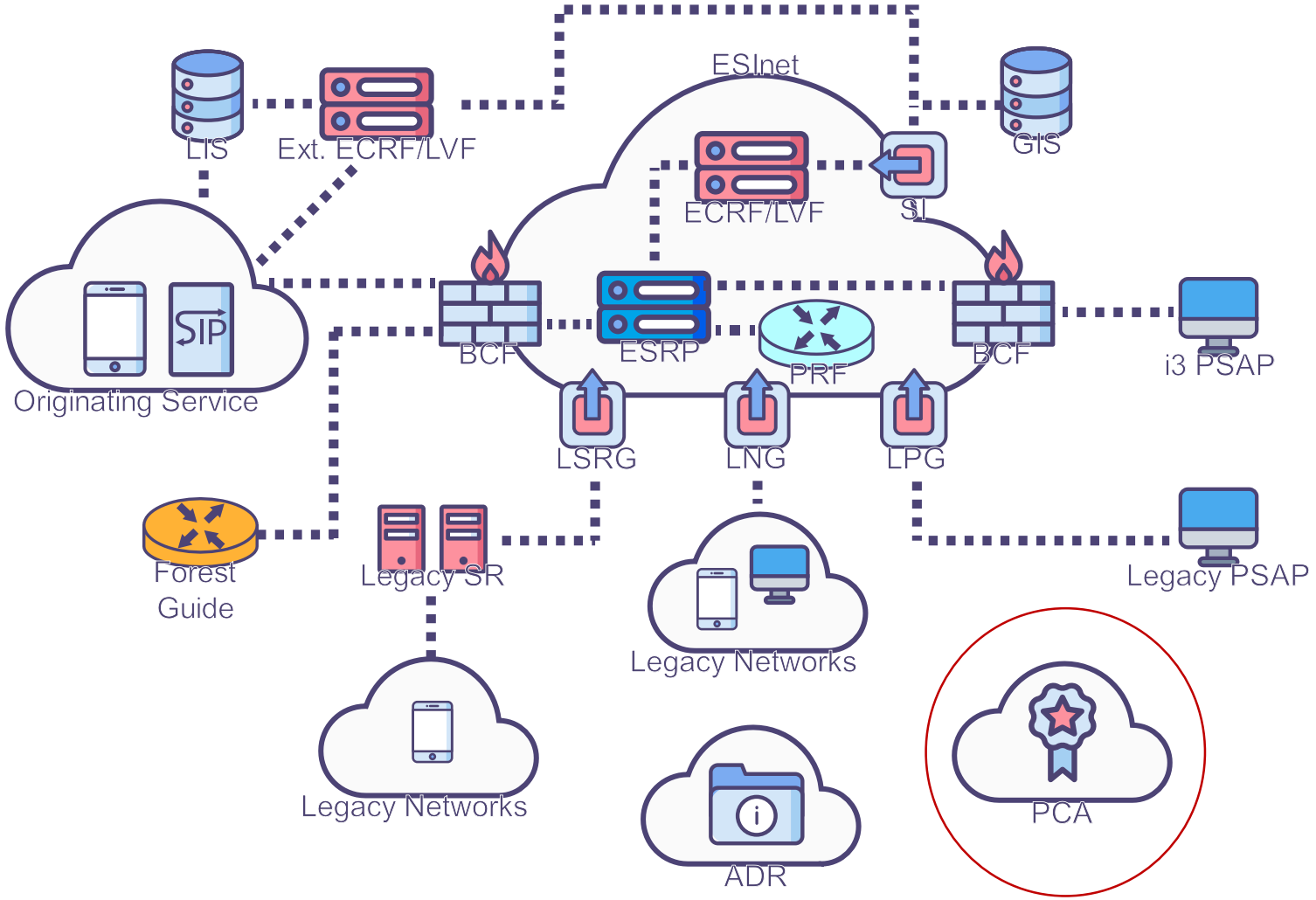


The PCA



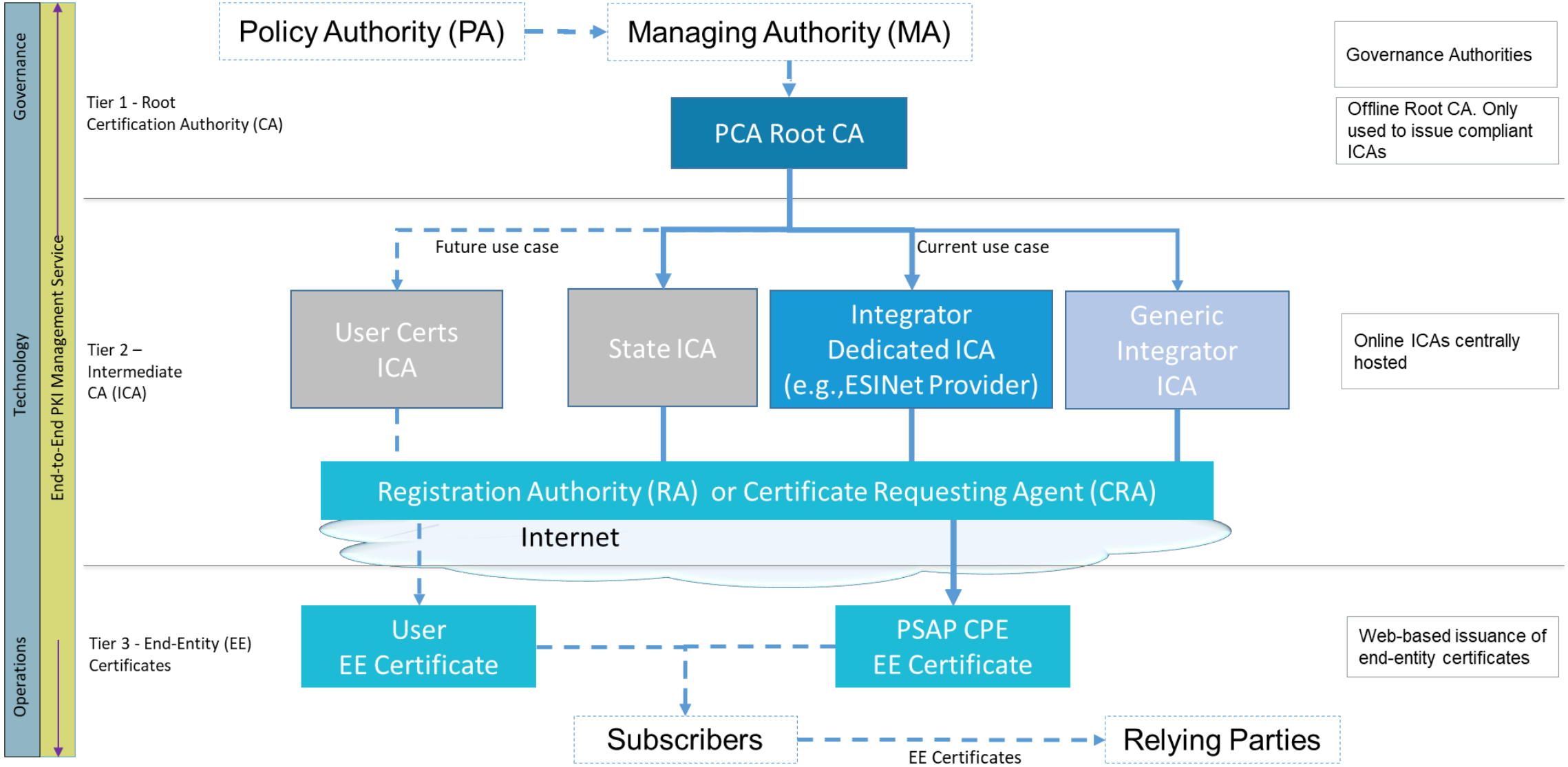
- Many interactions between elements in NG9-1-1 require TLS, and transactions MUST be accepted from sources with credentials traceable to PCA
- Credentials must carry a certificate in the PCA trust chain
- It is expected 9-1-1 authorities/ states/ regions would operate Intermediate Certificate Authorities (ICAs) that issue end-entity certificates within the trust chain
- 9-1-1 service providers could also operate an ICA as part of their service offering and manage credentials on your behalf
- PCA or ICA may be cross-signed with other CAs, depending on policies (some specific cross-signings are recommended in i3)

In NG9-1-1, There is no Trust



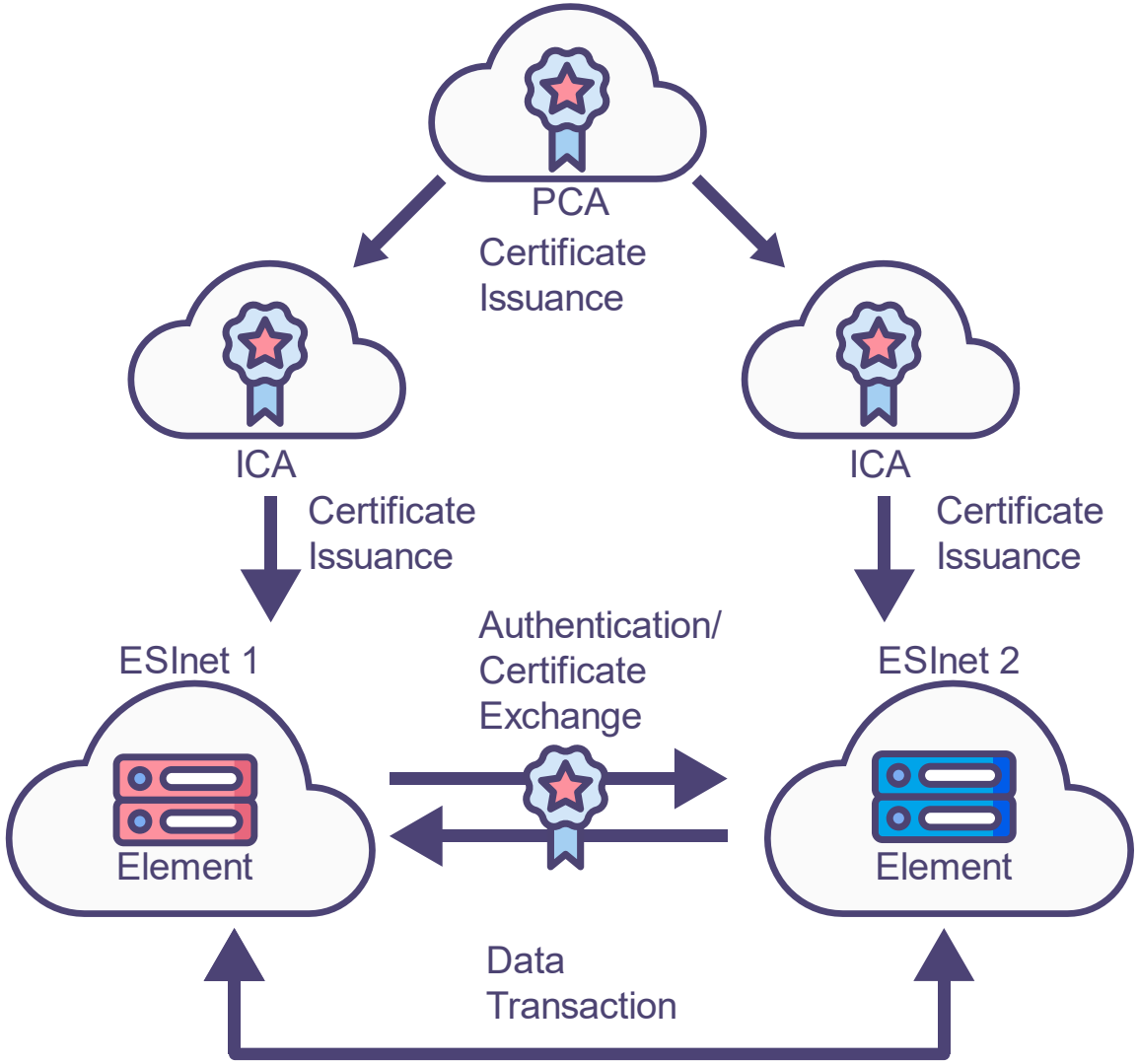
- Many elements in NG9-1-1 talk to each other to do various things
- Generally these transactions require TLS where applicable
- Even within the same ESInet, functions will check credentials
  - They are not trusted just because they are in the same ESInet
- In NG9-1-1, there is a special CA for this: the PCA

Certificate Distribution



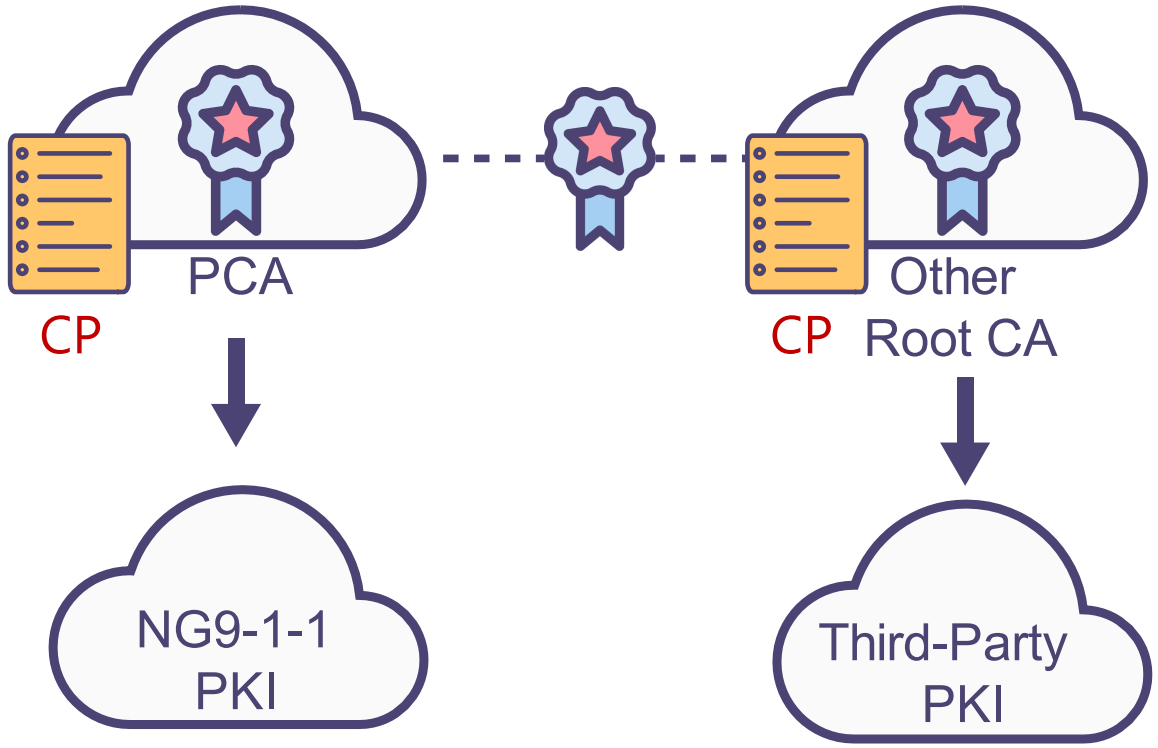
What Does it Mean for You?

- 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



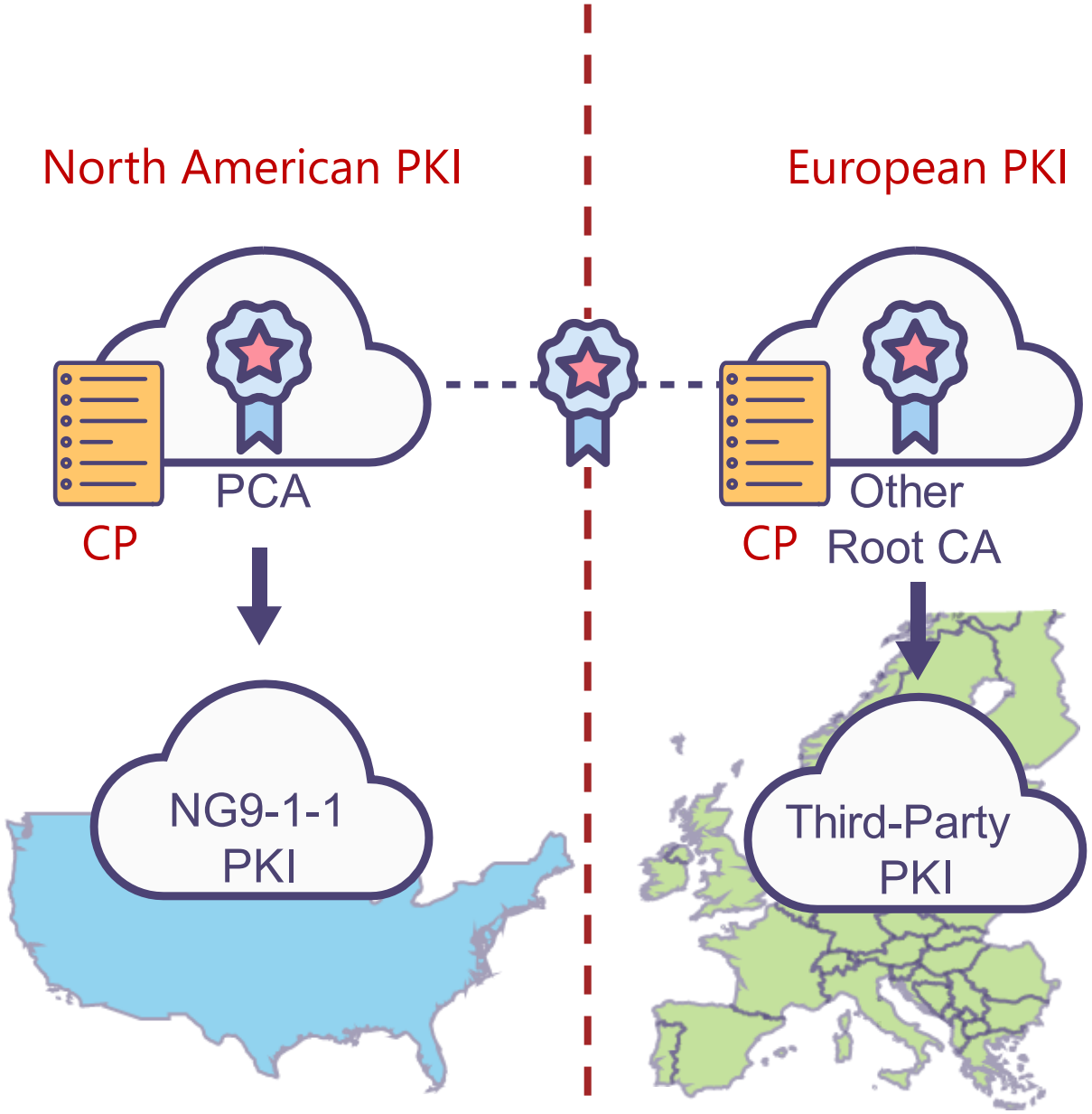
Extending Trust

- Technically, it is very easy to extend trust from one PKI and into another
- You need only sign each others' root keys—that's it
- This extends the privilege from PKI into another PKI
- Simple in concept



Extending Trust

- Technically, it is very easy to extend trust from one PKI and into another
- You need only sign each others' root keys—that's it
- This extends the privilege from PKI into another PKI
- Simple in concept
- By cross-signing another root CA, you accept ALL members of the second PKI into your PKI
- Also, you are responsible for your users doing no harm to the second PKI
- You must honor certificate issuance, revocation, expiration, renewal, etc. across both domains
- Technically, easy—logistically, difficult!

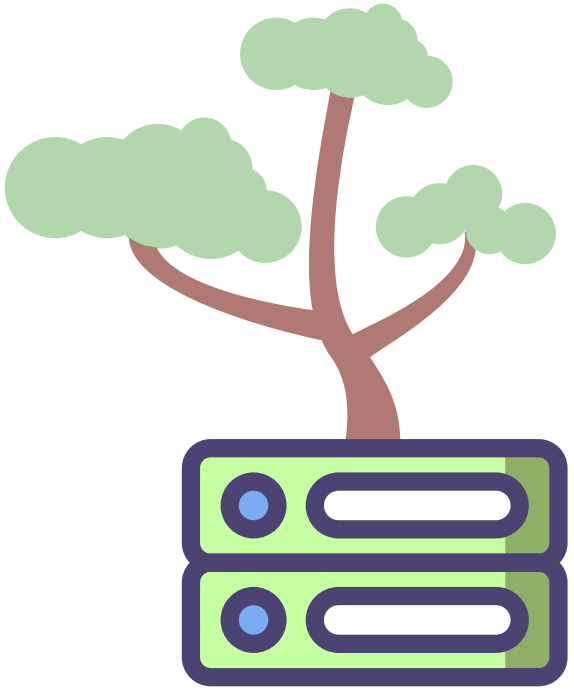


Remaining Challenges

- Establishing a PKI for an entire industry is an enormous task
- PCA will require support from the entire community (service providers, 9-1-1 authorities, PSAPs and vendors)
- Though PCA is not a new cost (purchase of certificates is always required), it is still a cost
- Existing deployments and business relationships at state/local level (such as government-run PKI) may complicate PCA integration for some stakeholders
- PKI is unfamiliar territory for the 9-1-1 industry
- Risks are mitigated through independent oversight and transparency
- Deployment of PCA root certificate is a logistical challenge; getting vendor support to bake it in will be ideal, but we need their support

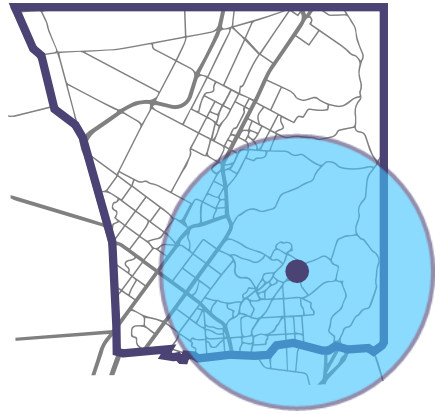
NG9-1-1 gets LoST in the Forest without a Forest Guide

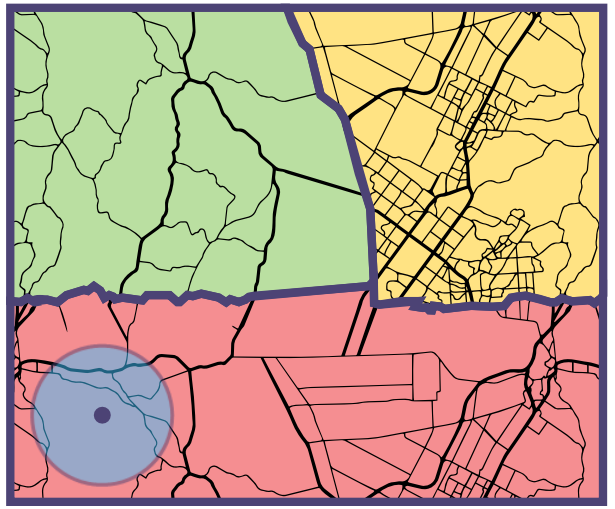
- The Forest Guide is an enhancement to location-based routing in IETF internet standards for emergency calling
- It is designed to resolve queries when there is no destination for a location
- Its main use case is to aid in interoperability
- IETF envisions emergency services with a network of forest guides to provide for global interoperability



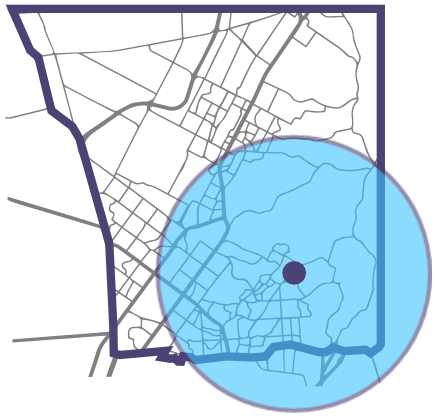
LoST and PIDF-LO

- LoST and PIDF are essential concepts to understanding the Forest Guide
- Created by IETF as internet standards
- i3 incorporates them
- LoST is Location-to-Service Translation
- PIDF is Presence Information Data Format
- (In most NG9-1-1 literature you see “PIDF-LO”, or PIDF Location Object)





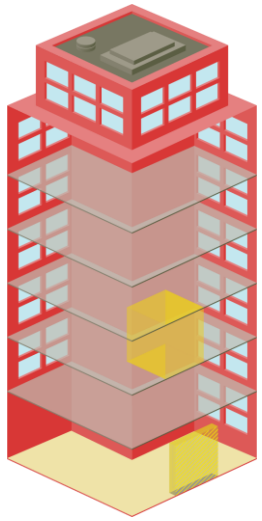
LoST and PIDF-LO



Geometry

X=38.80587
Y=-77.059400
Z= 20m

CNF=90%
UNC=20m
Z-UNC= 2.4m`

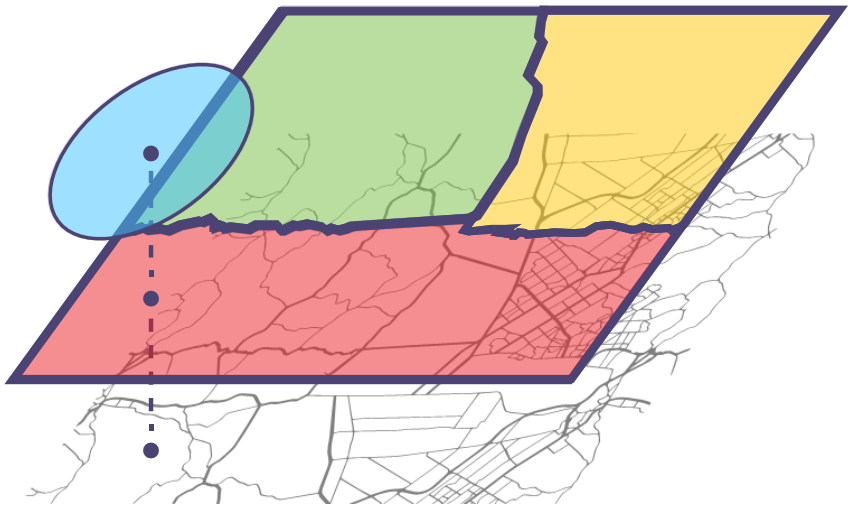


Civic Address

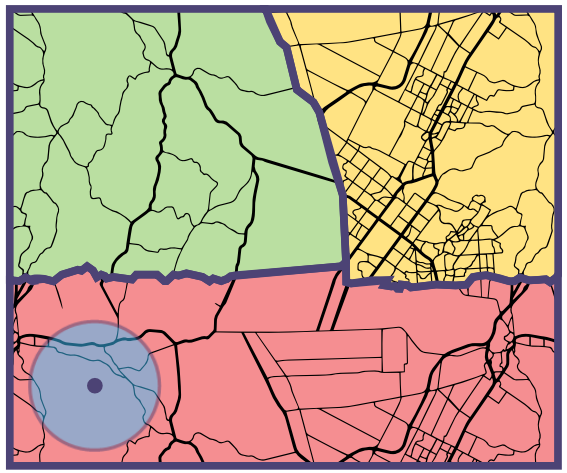
1700 Diagonal Rd
Alexandria, VA 22314

- Internet Standard, IETF 6848
- Location in NG9-1-1 is expressed in this format
- Can be expressed with geometry (a point)
- Uses WGS-84 reference ellipsoid (standard coordinate system)
- Though PIDF-LO supports many shapes, with caller location, we generally expect a point, circle or ellipsoid
- Shapes convey location +uncertainty
- Can be expressed as a civic address (dispatchable location)
- Included in signaling information in the SIP header

LoST

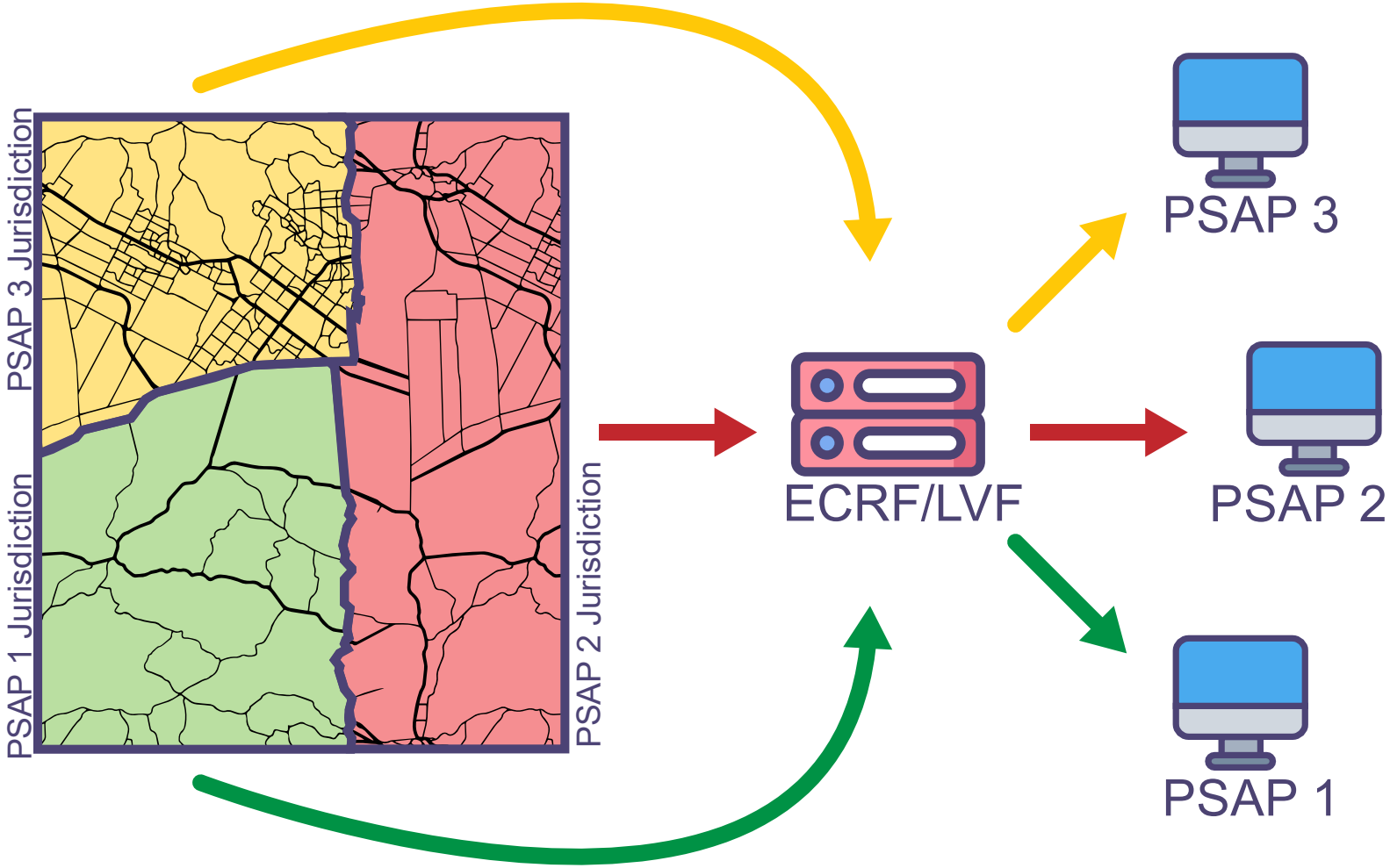


Location
(PIDF-LO)
+
Service area
Polygons
(GIS Layer)
+
Civic address
information



- Internet Standard, IETF 5222
- LoST servers are used in NG9-1-1 including (ECRF/LVF and Forest Guide)
- Ingests location (PIDF-LO) in a query, and finds the service at that location (Location-to-Service Translation)
- Created many years ago assuming services would need a standards-based way to find a service at a location (e.g., food delivery, rideshare services)
- However, outside of NG9-1-1, most services use a proprietary method
- However, LoST is a good solution for NG9-1-1, because NG9-1-1 needs interoperability
- In NG9-1-1, LoST is used by the ECRF to find the correct PSAP at a location or LVF to validate a location

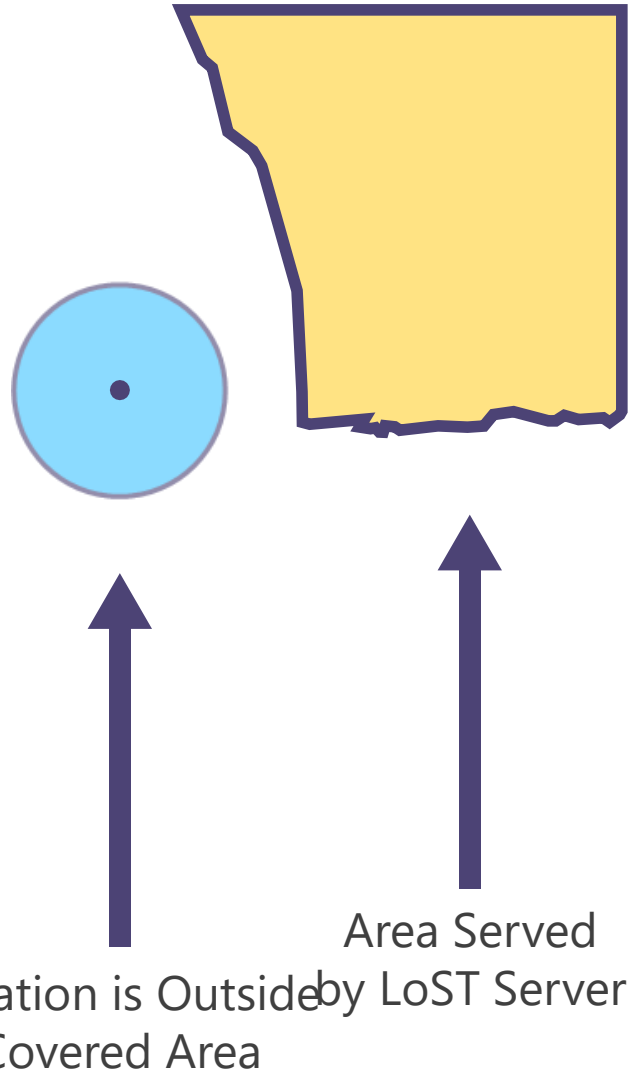
Location-Based Routing



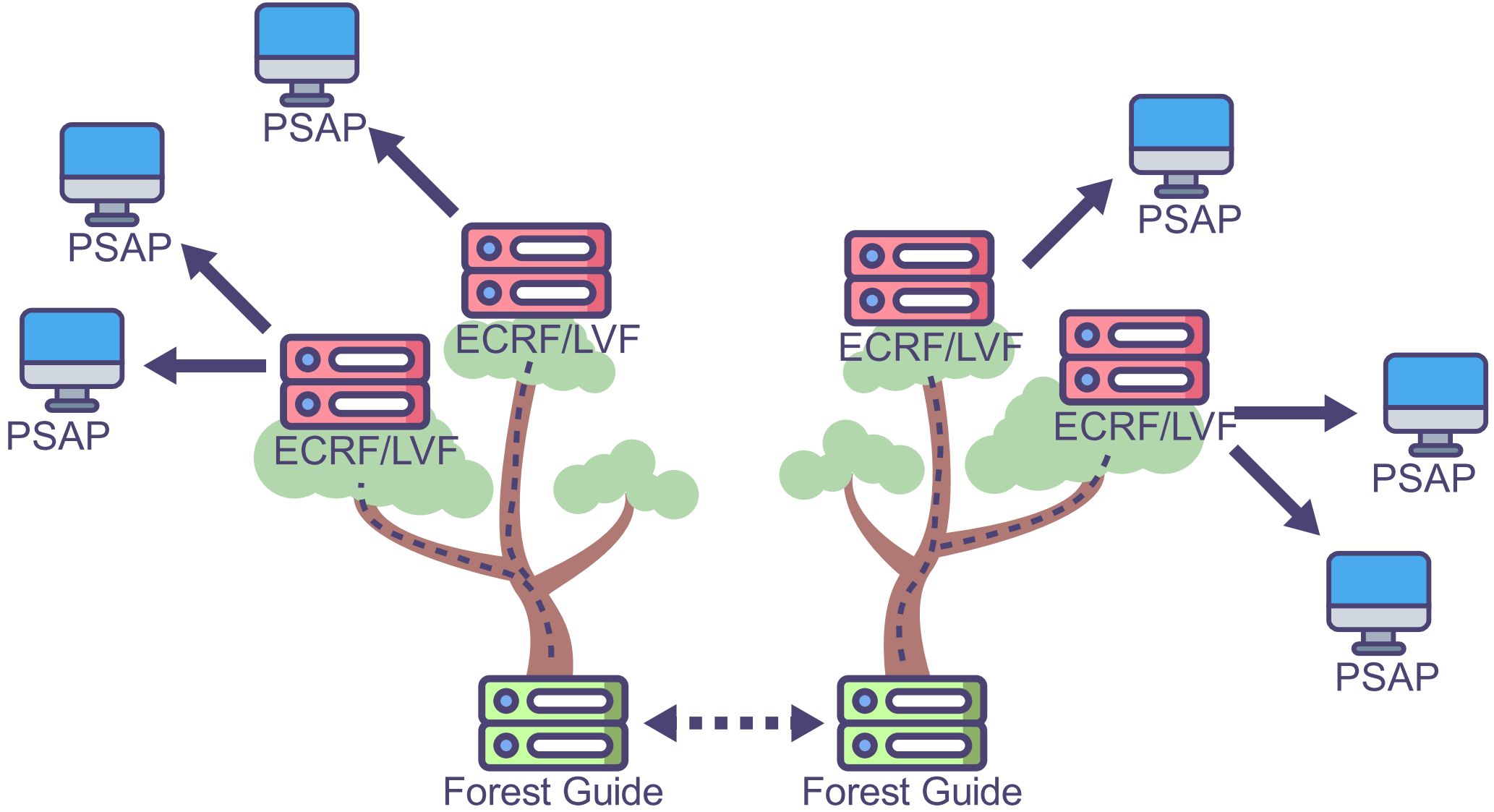
- An individual's location is expressed in PIDF-LO
- The LoST server ingests the location, and compares it to service area boundaries for each service (in NG9-1-1, PSAPs)
- The correct PSAP receives the call

What does a Forest Guide do?

- LoST servers in NG9-1-1 (ECRF) map caller location to the appropriate service (PSAP)
- Sometimes, an ECRF has a location that it cannot resolve, and it needs help
- The common case for this is during call transfer to a distant PSAP
- The purpose of the Forest Guide is to help find the ECRF that serves a location (ESInet) when a query cannot resolve
- Forest Guide is an IETF standard; NENA i3 requires that we use one
- This session assumes geodetic location, but the Forest Guide is a LoST server, so it can also handle a civic address

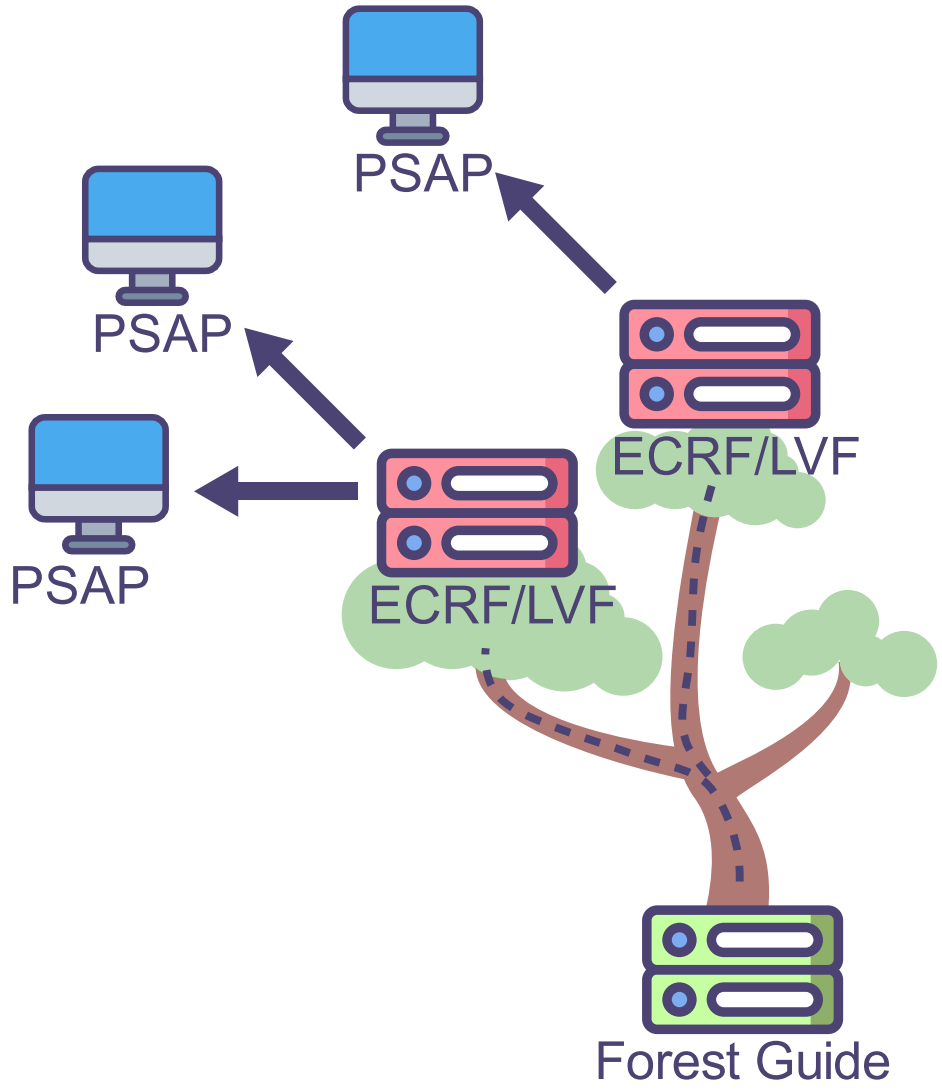


Lost in the Forest? Get a Forest Guide!

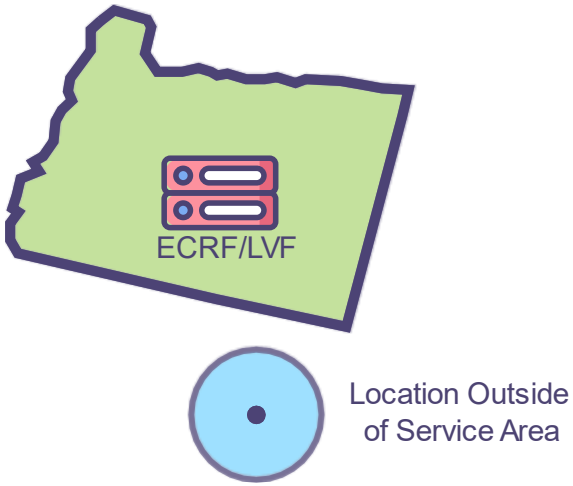


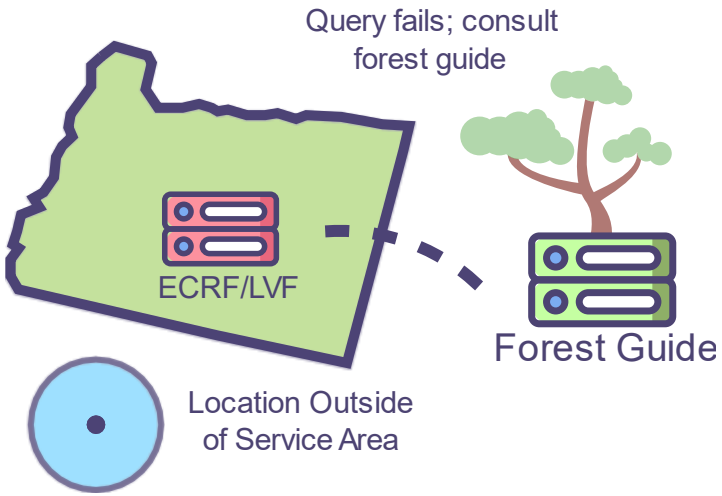
Forest Guide Fundamentals

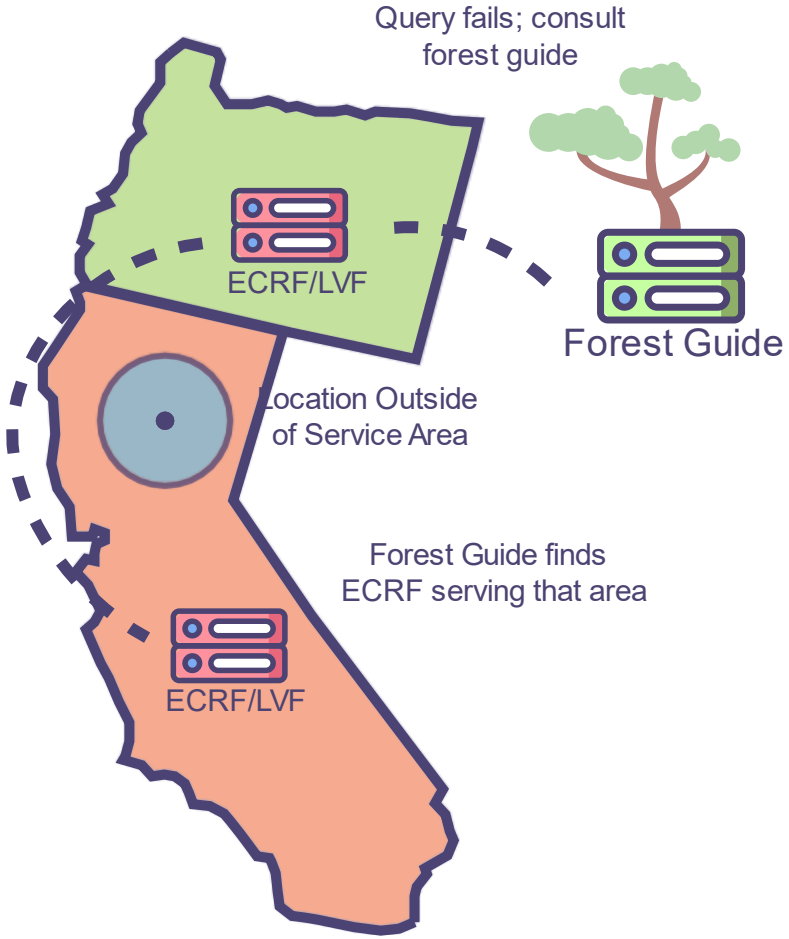
- IETF 5582 organizes the global LoST routing infrastructure into trees
- NENA i3 adopts this convention; organizing ECRFs/LVFs as trees
- 5582 does not dictate the scope of each tree, but i3 assumes nominally that each “tree” is a state-level or equivalent ECRF
- The tree extends into branches and leaves (subordinate ECRFs/PSAPs)
- Each node represents a LoST server (ECRF)
- Each node knows about itself, its children and its parent
- Each tree references a Forest Guide to help its children find other trees
- Additionally, each Forest Guide helps other Forest Guides find its children



Forest Guide Fundamentals





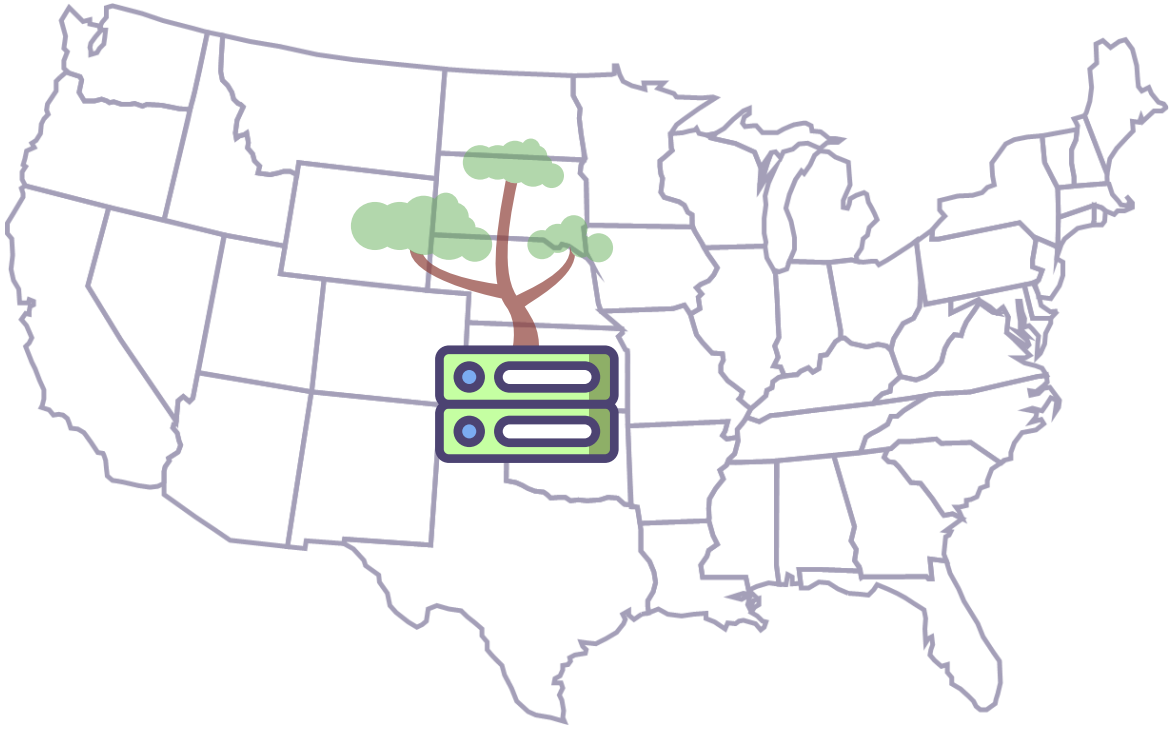


- The primary purpose for a Forest Guide is to find the correct ECRF when a LoST query does not resolve (cannot find the right destination for a location)
- The Forest Guide finds the right ECRF for that location

Forest Guide Fundamentals

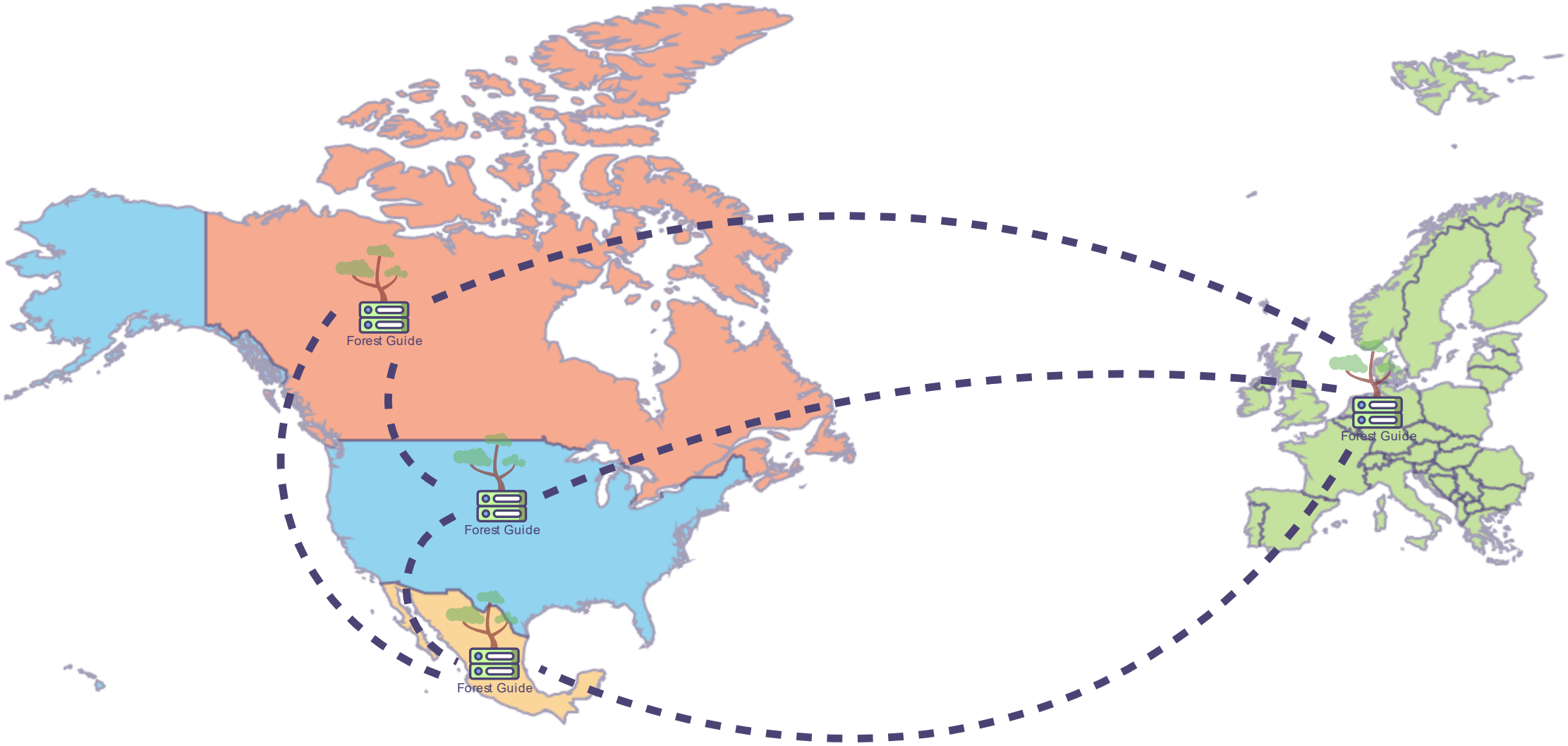
A very typical use case for the Forest Guide is transfer to a distant PSAP, where routing information is not shared between jurisdictions

North American Forest Guide

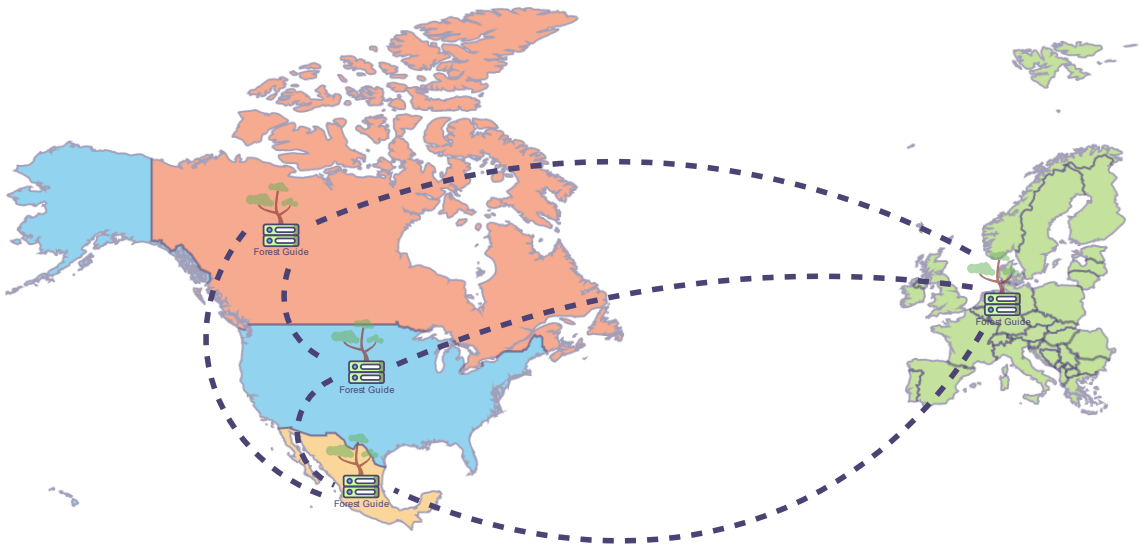


- i3 assumes a Forest Guide is (initially) operated for the United States
- NENA will deploy a USA Forest Guide for USA in 2020
- Project is approved and funded through NENA's board
- Sustainability model assumes modest fees for interconnection with the USA Forest Guide
- RFP publication/vendor selection ~Spring 2020
- Service availability ~end of 2020
- This project assumes at least the USA; there are no technical barriers to incorporating other regions
- USA? Forest Guide will map to other Forest Guides as other regions (Europe) deploy Forest Guides

International Context



International Context



- Ideal design assumptions are that each country ot region establishes a Forest Guide
- The worldwide NG9-1-1 ecosystem includes Forest Guides to find each tree in each forest
- In NG9-1-1, this means that any query to any LoST server (like the ECRF) should resolve somewhere if there is some place it cannot resolve
- This means that every NG9-1-1 call originated and handled properly will find an ESInet if one exists for that location
- If the ECRF does not have an answer for a location, the Forest Guide will
- If the Forest Guide doesn’t have an answer, then it will ask other Forest Guides
- If the networks are all properly configured, if there is no answer, it means there is no ESInet discoverable at that location

Remaining Challenges

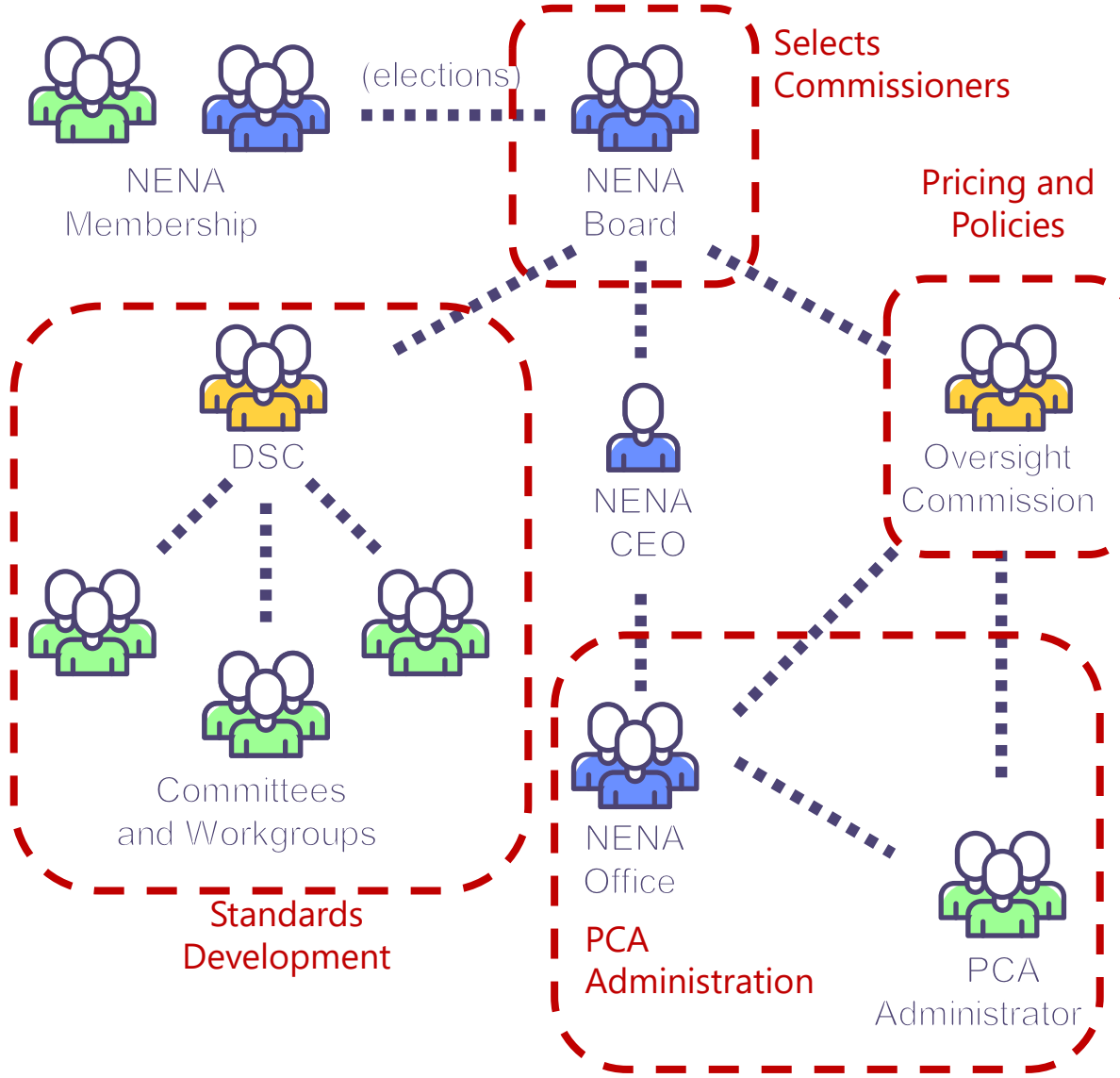
- Technically, developing the USA Forest Guide is relatively simple, however, management challenges are substantial
- Every market in USA has a different management model (state/regional/local ESInet)
- Deploying the USA Forest Guide will require buy-in and participation from all stakeholders
- The Forest Guide will require a sustainable funding model; building it is straightforward, managing to scale is more complicated
- Managing GIS for a state ESInet is difficult enough; Forest Guide will minimally need information about every state
- Though the promises of international interoperability for NG services are ideal, practical issues of international coordination are very difficult
- However, as a non-profit with an international footprint, NENA is in an ideal position to manage these technicalities
- There is no (technical) limit to expanding coverage of the USA Forest Guide; that is subject to national law/regulation/treaties and governance

Conclusion

- The Forest Guide is fairly simple, but extremely important
- It is an Internet Standard (like PIDF and LoST), however, NENA standards adopt and extend that standard
- The Forest Guide is for interoperability and for discovery of an ESInet when location queries fail to resolve
- NENA plans to deploy the USA Forest Guide in 2020
- The North American Forest Guide will be overseen by an independent oversight body representative of emergency services and industry partners

Governance

- The Oversight Commission will consist of members nominated from a variety of representative stakeholder groups affected by PCA
- NENA Board will review and approve nominations to PCA, which will operate under established bylaws
- NENA Office will provide executive function for the Commission, including administration of the contract with the PCA Administrator and handling finances
- The PCA Administrator will be required to follow the standards developed by NENA as an SDO
- The Commission will develop policies for the PCA with input by the Administrator and NENA Office, including pricing, certificate policy development and enforcement



Trans-Continental Plugtest

- NENA ICE9 and EENA PlugTest 4 are planned to be a joint interoperability test
- Focus on end-to-end call flows that span international boundaries
- Use case: routing errors, nomadic callers

Will test:

- ESInet / NGCS interoperability between US and European environments, with lab-to-lab testing taking place between the NENA ICE lab location and the ETSI lab supporting EENA PlugTests
- Multimedia communications interoperability over this same infrastructure
- International peering scenarios
- *Time permitting*—IoT/non-interactive calls

Questions?

Brandon Abley
Director of Technology

@911NENA911
/911NENA911

NENA
THE 9-1-1 ASSOCIATION