OpenADR Alliance Overview

6/18/14

Oscar Marcia
President
NetworkFX, Inc.

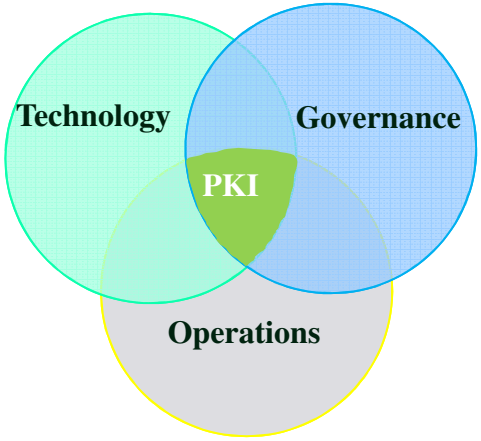
…Building Communities of Trust

Content

1. NetworkFX Approach
2. OpenADR Architecture
3. Public Key Infrastructure
4. The Role of Governance and Operation in a Successful PKI
5. OpenADR PKI
6. Certificate Issuance Process
7. New Types of certificate requests

Our Approach

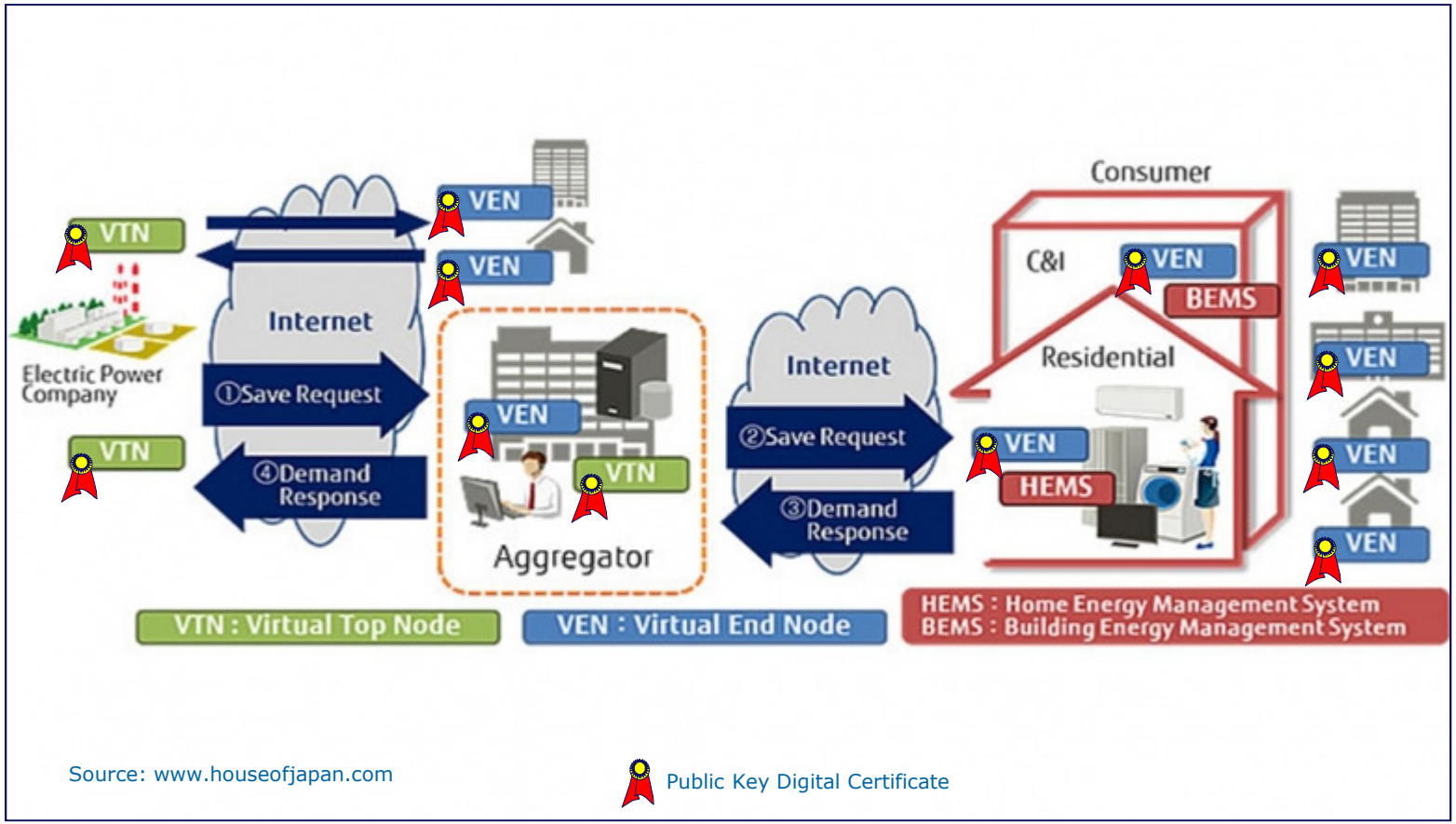
- **Technology:** Design, Architecture, and Hosting of Public Key Infrastructures
- **Governance:** Policy Development for Managing Certificates
- **Operations:** Digital Certificate & Key Lifecycle Issuance and Management



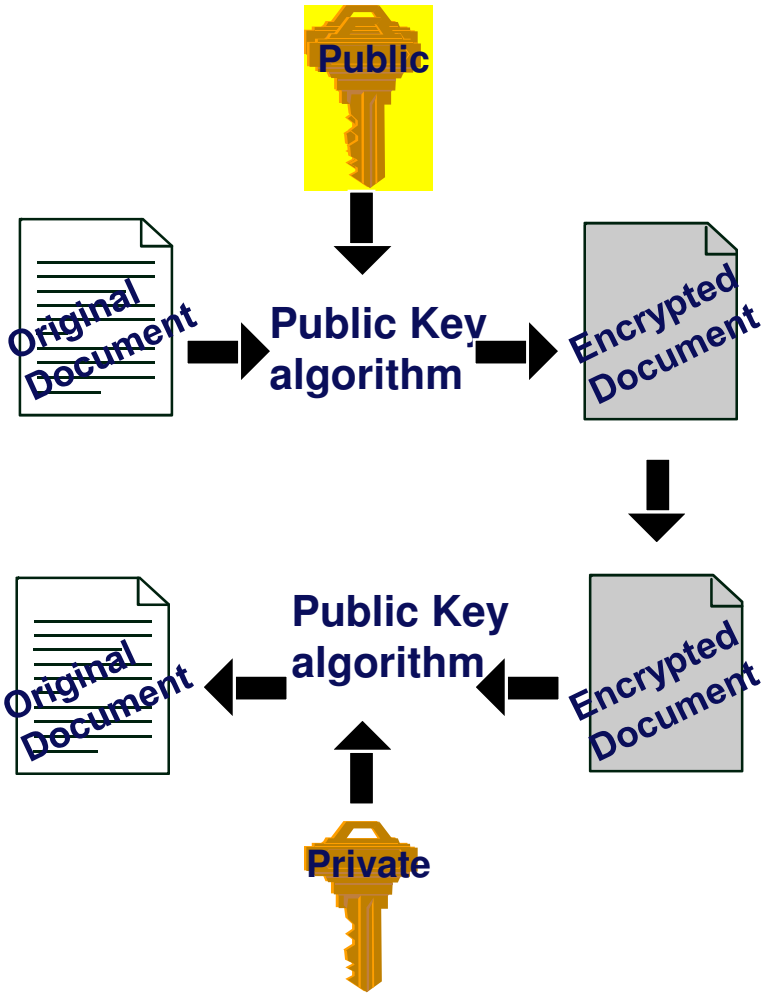
Governance and Active Operations Management makes PKI Effective

OpenADR Architecture

VEN/VTN Authentication based on digital certificates

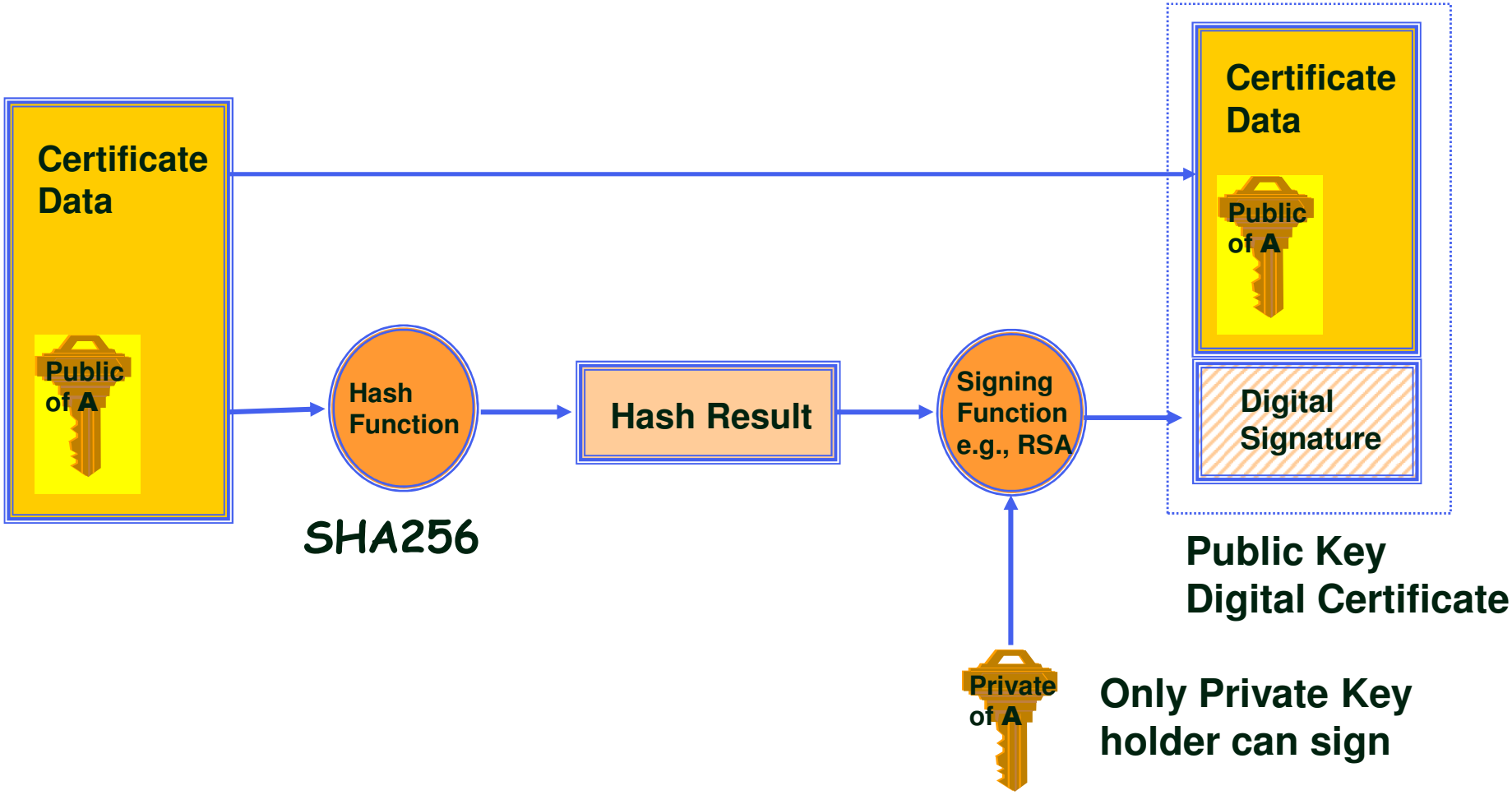


Public Key Cryptography

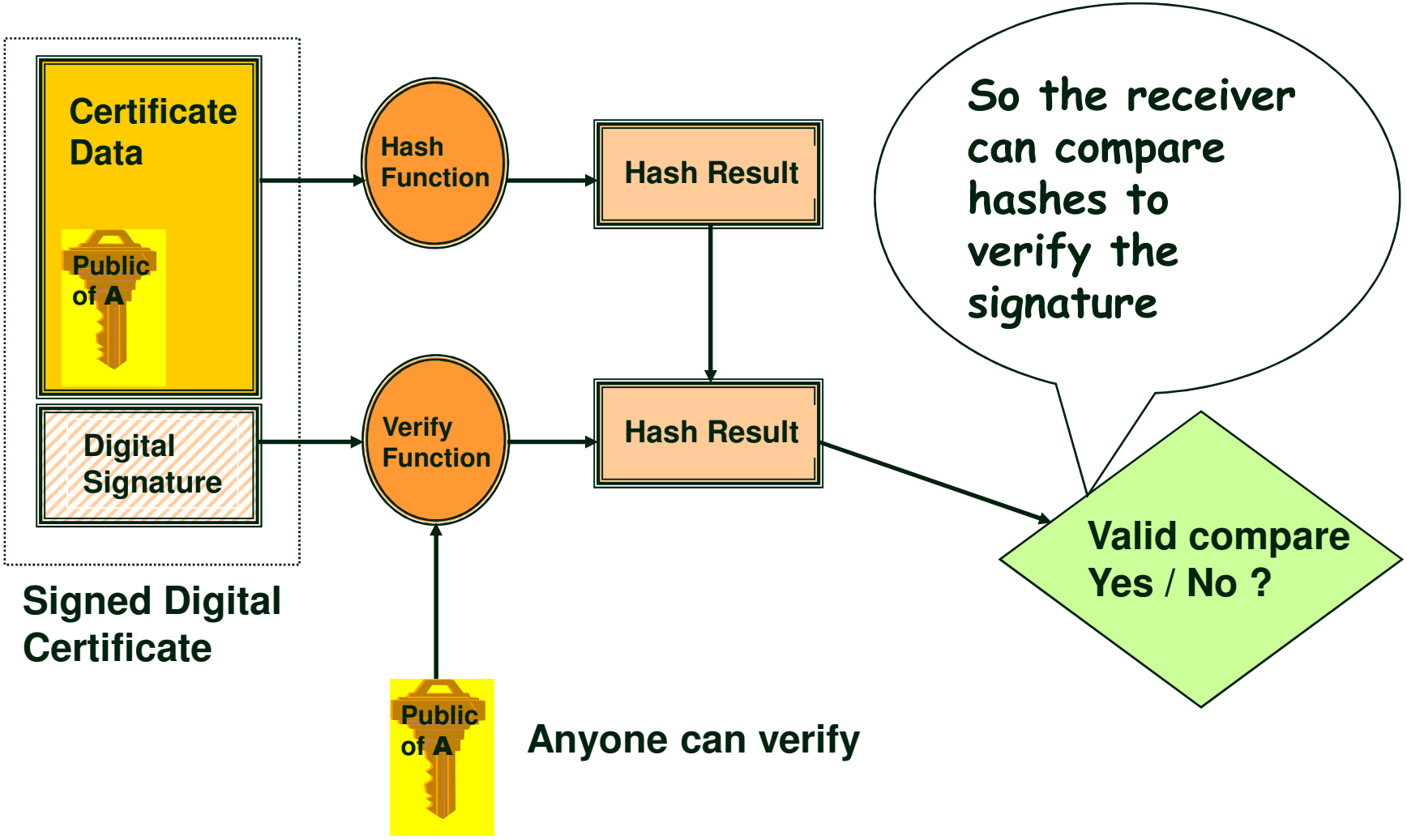


- Two keys = Public/Private key pair
- Mathematically related, but not identical, *public* & *private key pairs*
  - ***Public Keys*** are widely distributed
  - ***Private Keys*** are held securely by owners
- Data encrypted with one key can be decrypted only with the other key of the pair (a.k.a. *"Asymmetric Key"*)
- **RSA** and **ECC** are examples of public key algorithms

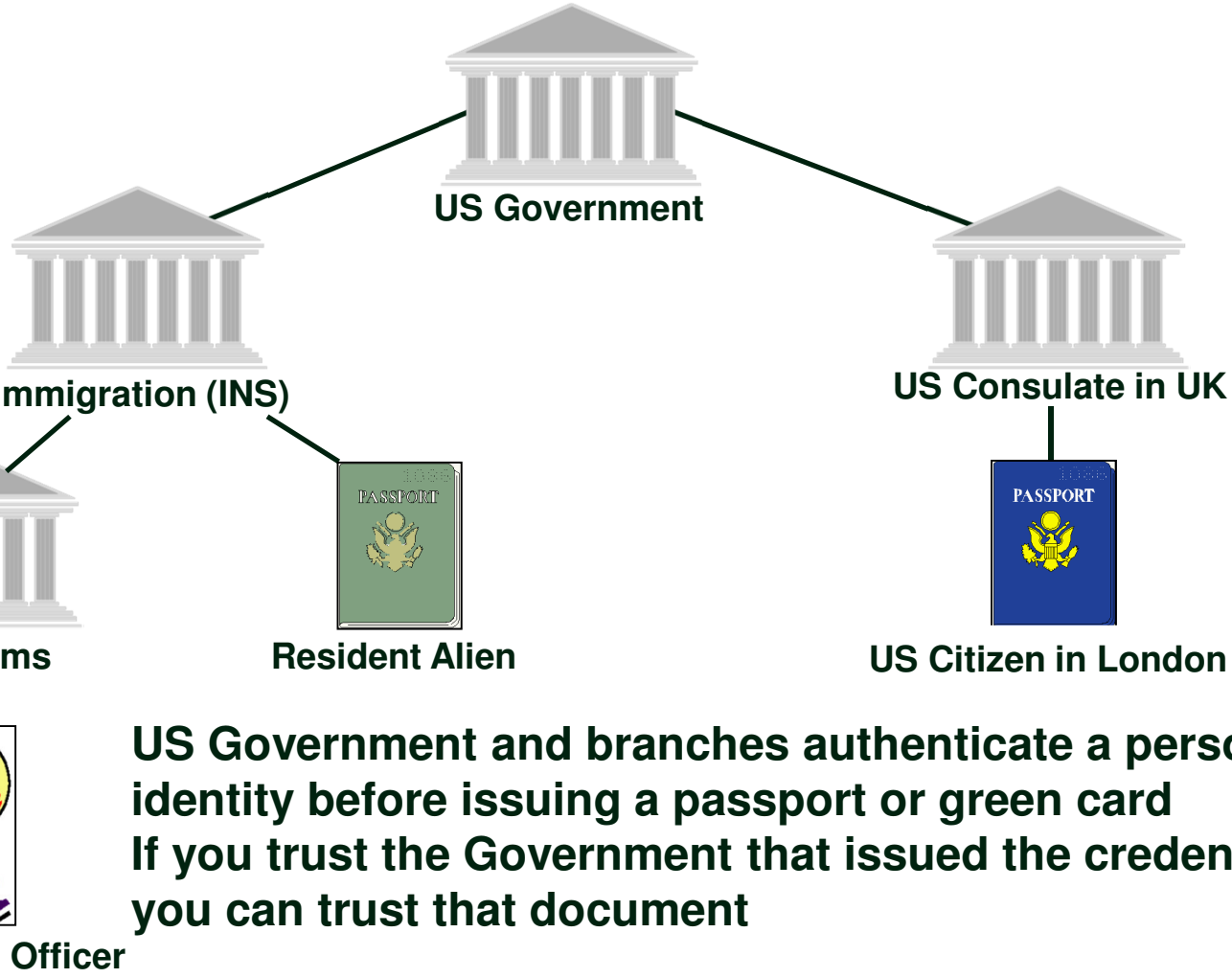
Digital Certificate *Signing*



Digital Signature *Verification*

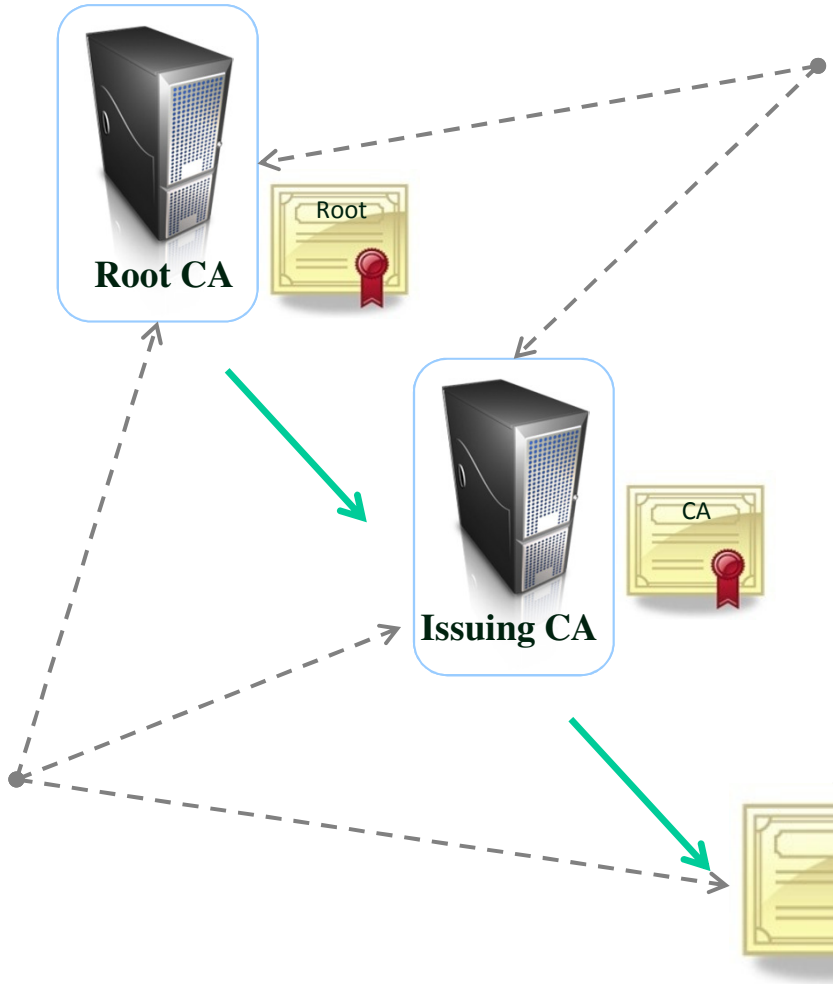


A Trust Hierarchy is needed



US Government and branches authenticate a person's identity before issuing a passport or green card
If you trust the Government that issued the credentials, you can trust that document

How we Govern Trust

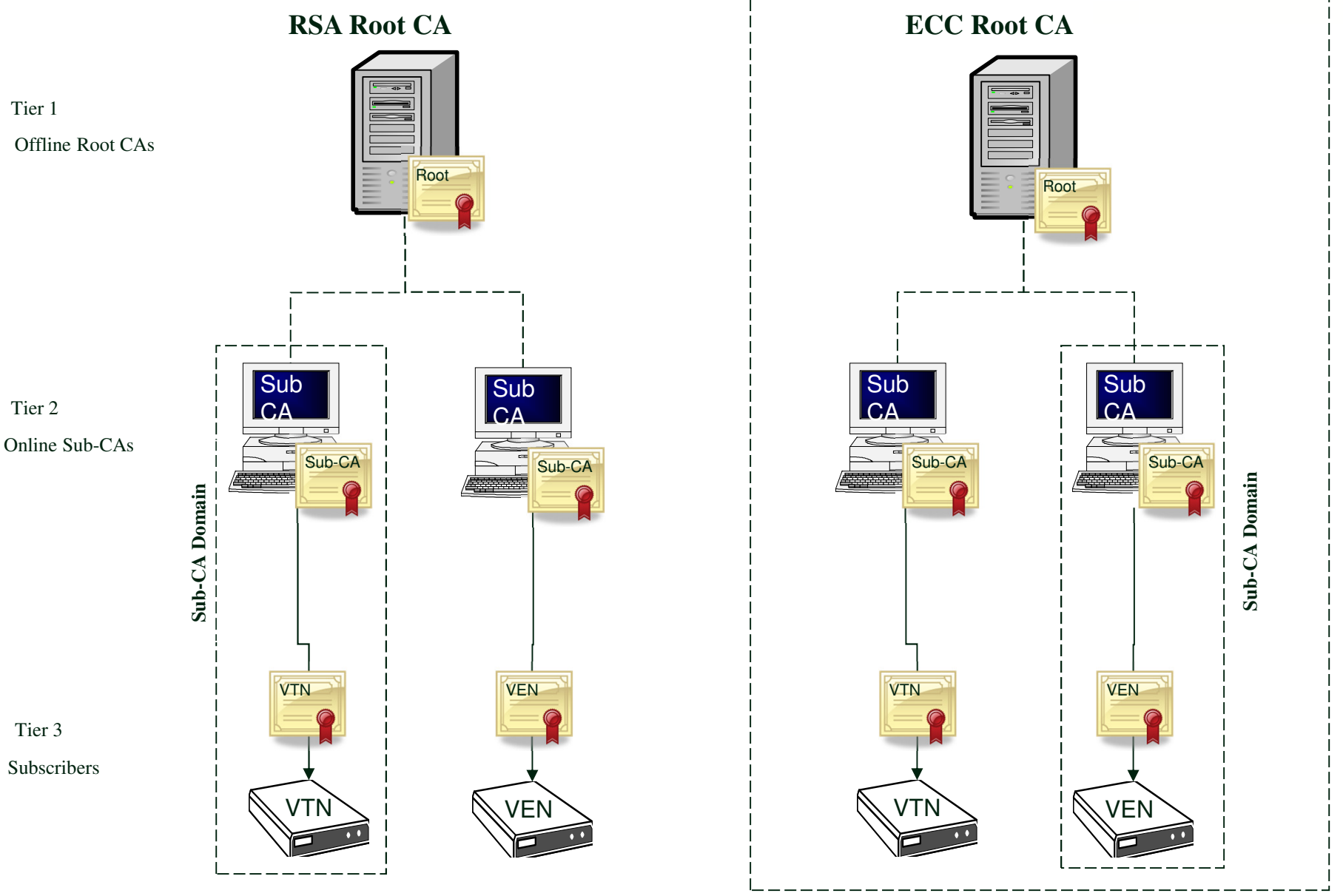


Certificate Practice Statement defined for each Certification Authority (CA) to govern certificate issuance.

Certificate Policy defined to govern the public key infrastructure. Allows relying parties to access the assurance level (trust) of the certificate.

Certificate Lifecycle Management tracks issuance, expiration and revocation of certificates to preserve the chain of trust.

OpenADR Alliance PKI Architecture

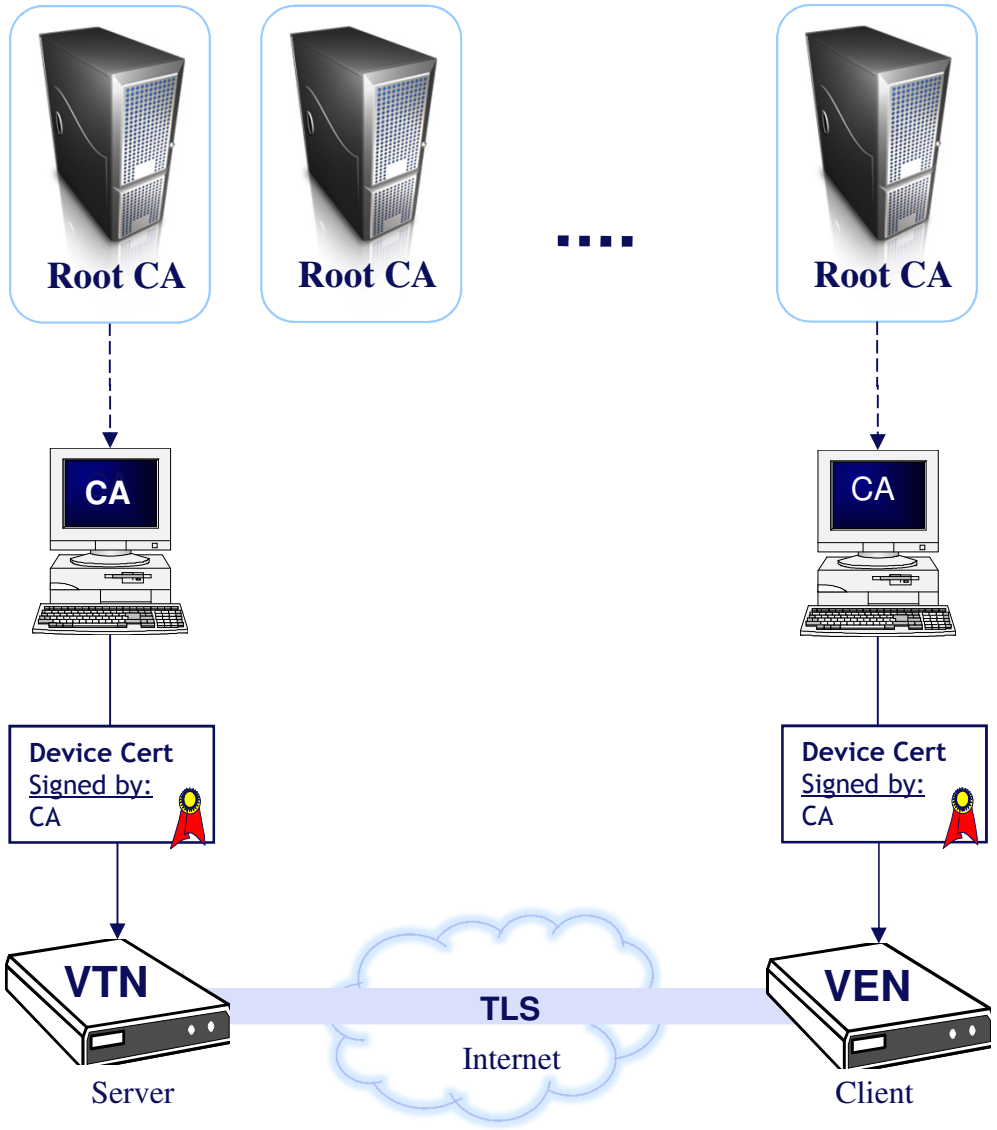


OpenADR 3-Tier PKI Technology

1
- Multiple Offline Root CAs (RSA, ECC)
- Issues Sub CAs
- Governed by OpenADR Security requirements

2
- Manufacturer CAs (RSA, ECC)
- Issues device certificates
- Governed by OpenADR Security requirements

3
- (RSA or ECC) Device certificates embedded in manufacturer's device
- Governed by OpenADR Security requirements



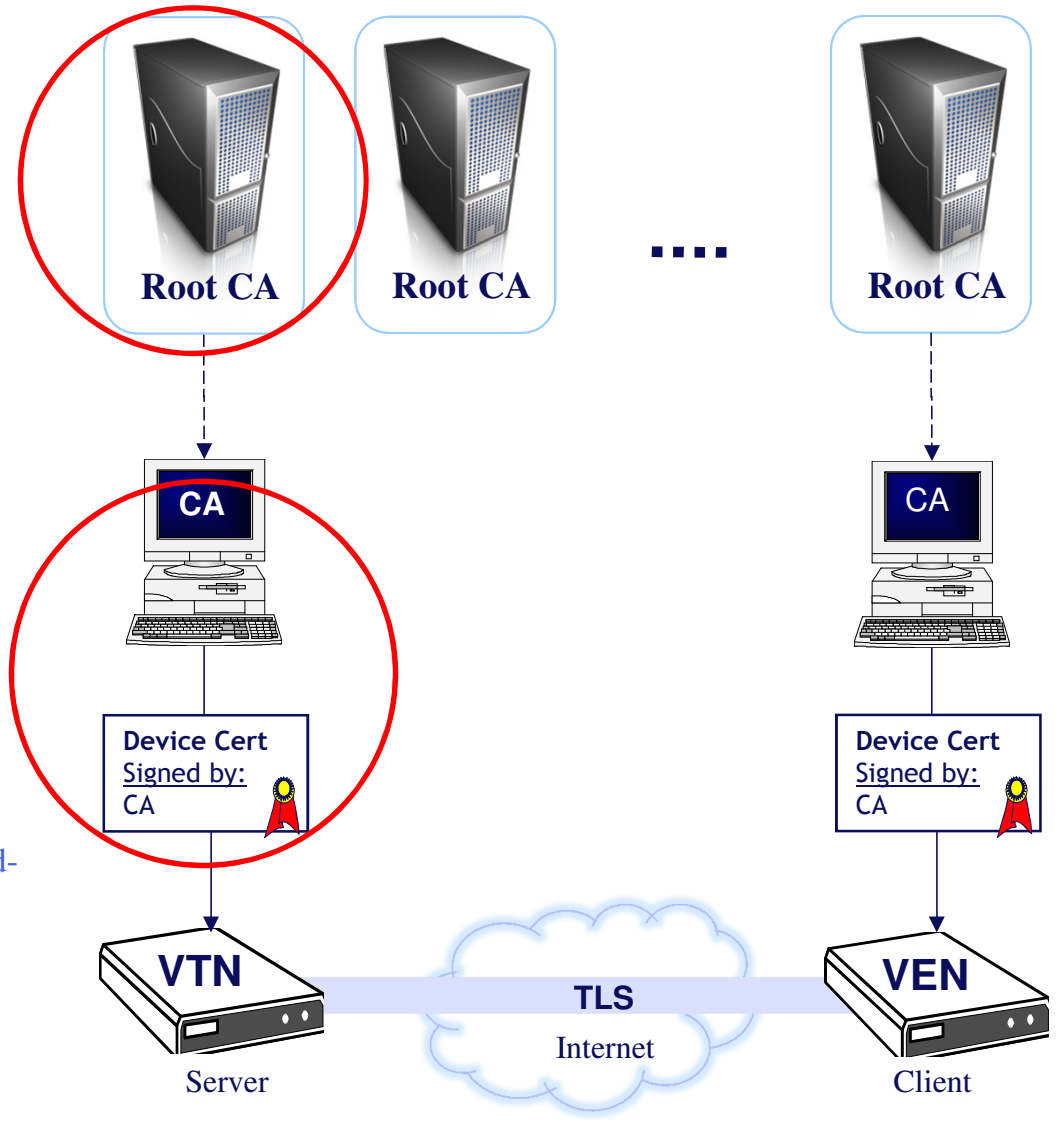
The Role of Governance and Operation in a Successful PKI

1. Multiple service providers (SP) and a complex RSA/ECC infrastructure requires:
   - •Root CA monitoring
   - •Certificate Policy
   - •Certification Practice Statement

2. PKIs with distinct groups working independently require:
   - •A central end-to-end authority
   - •Control of desired assurance level

OpenADR Specifications

3. Certification Authorities (CA) and end-entity certificates require:
   - •Certificate management process
   - •Appropriate revocation policy
   - •CA monitoring



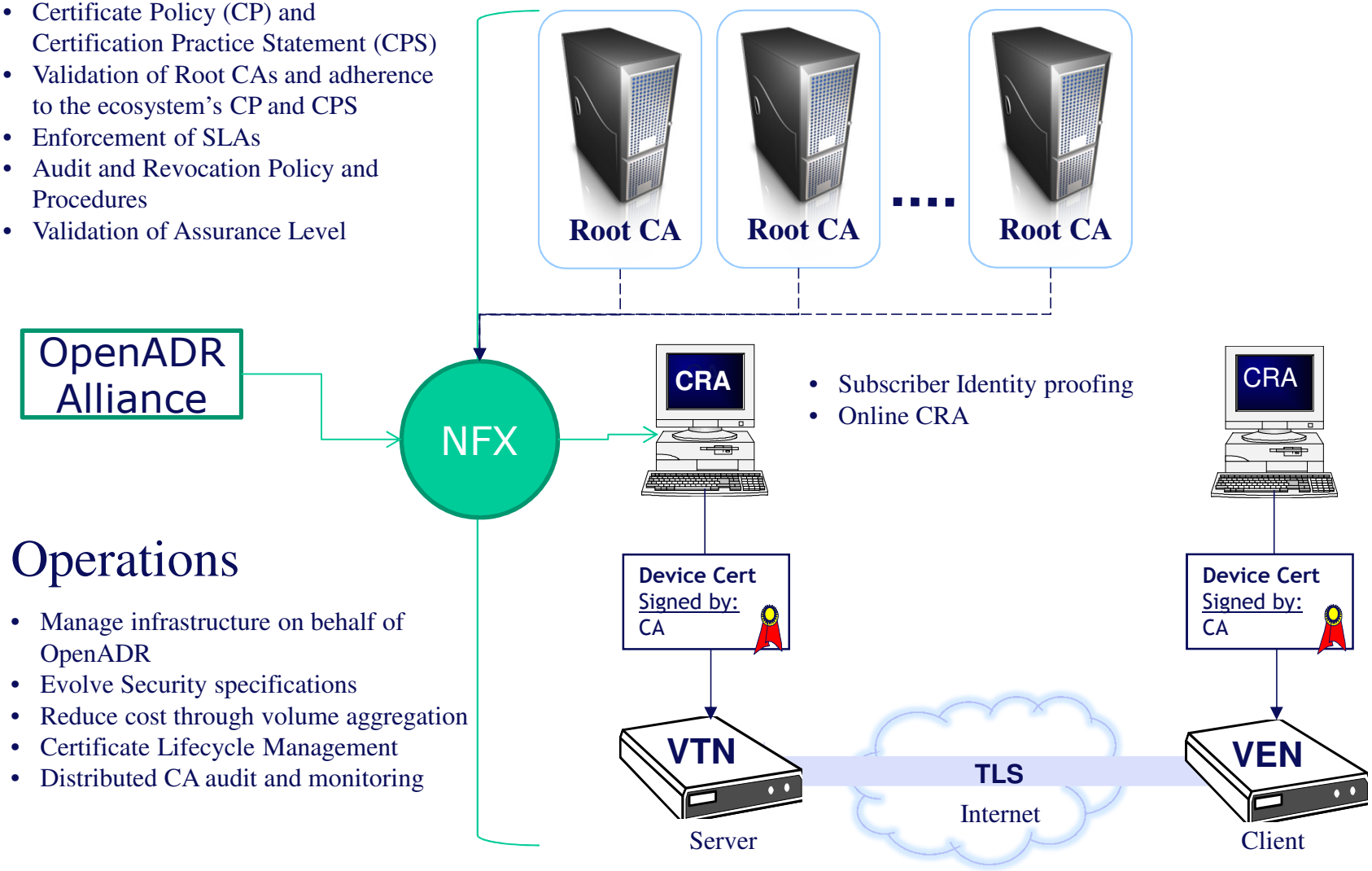
NetworkFX End-To-End Solution

1 Governance

- Certificate Policy (CP) and Certification Practice Statement (CPS)
- Validation of Root CAs and adherence to the ecosystem's CP and CPS
- Enforcement of SLAs
- Audit and Revocation Policy and Procedures
- Validation of Assurance Level

2 Technology

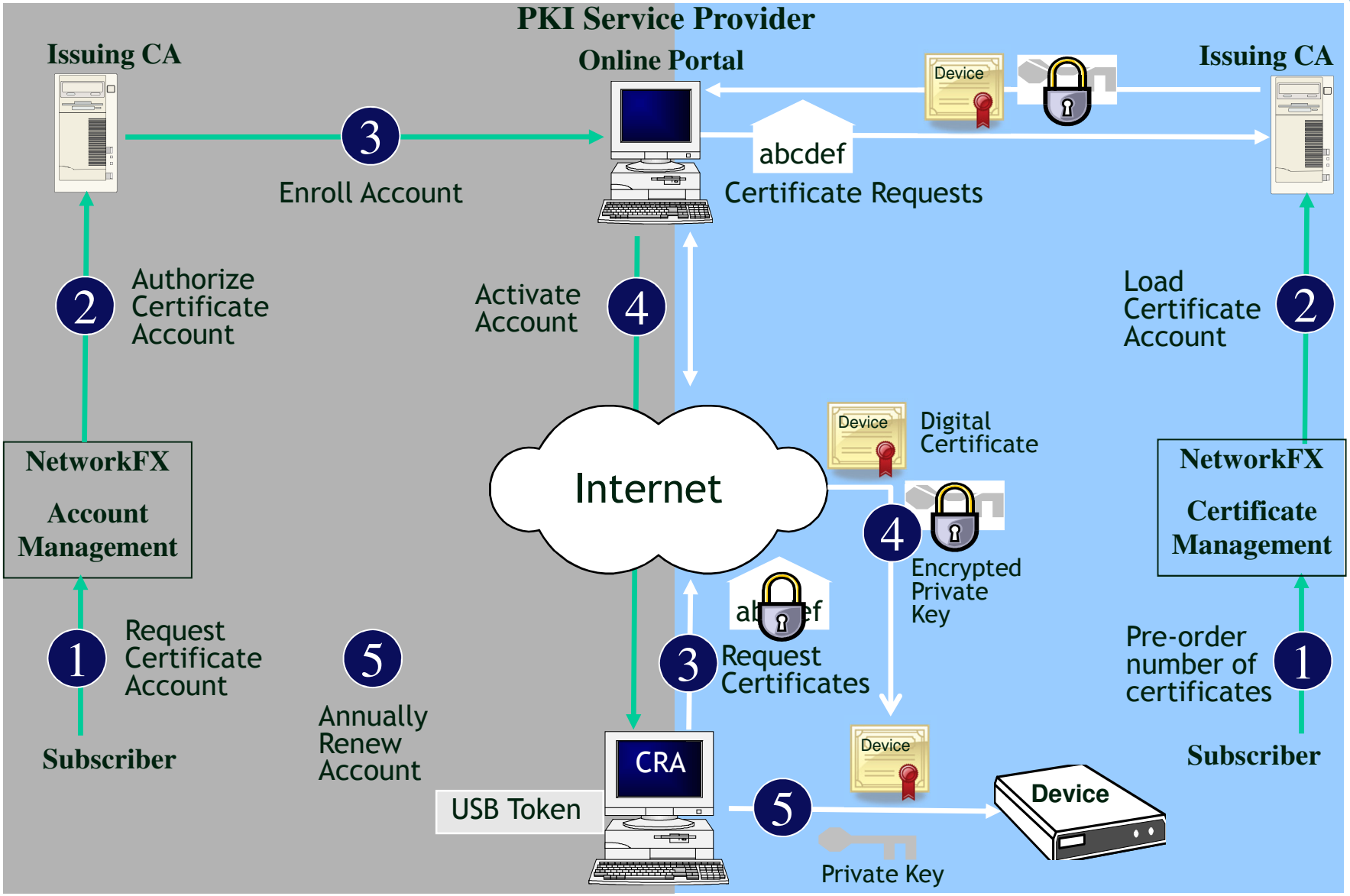
- PKI components
- Cipher suite protocols



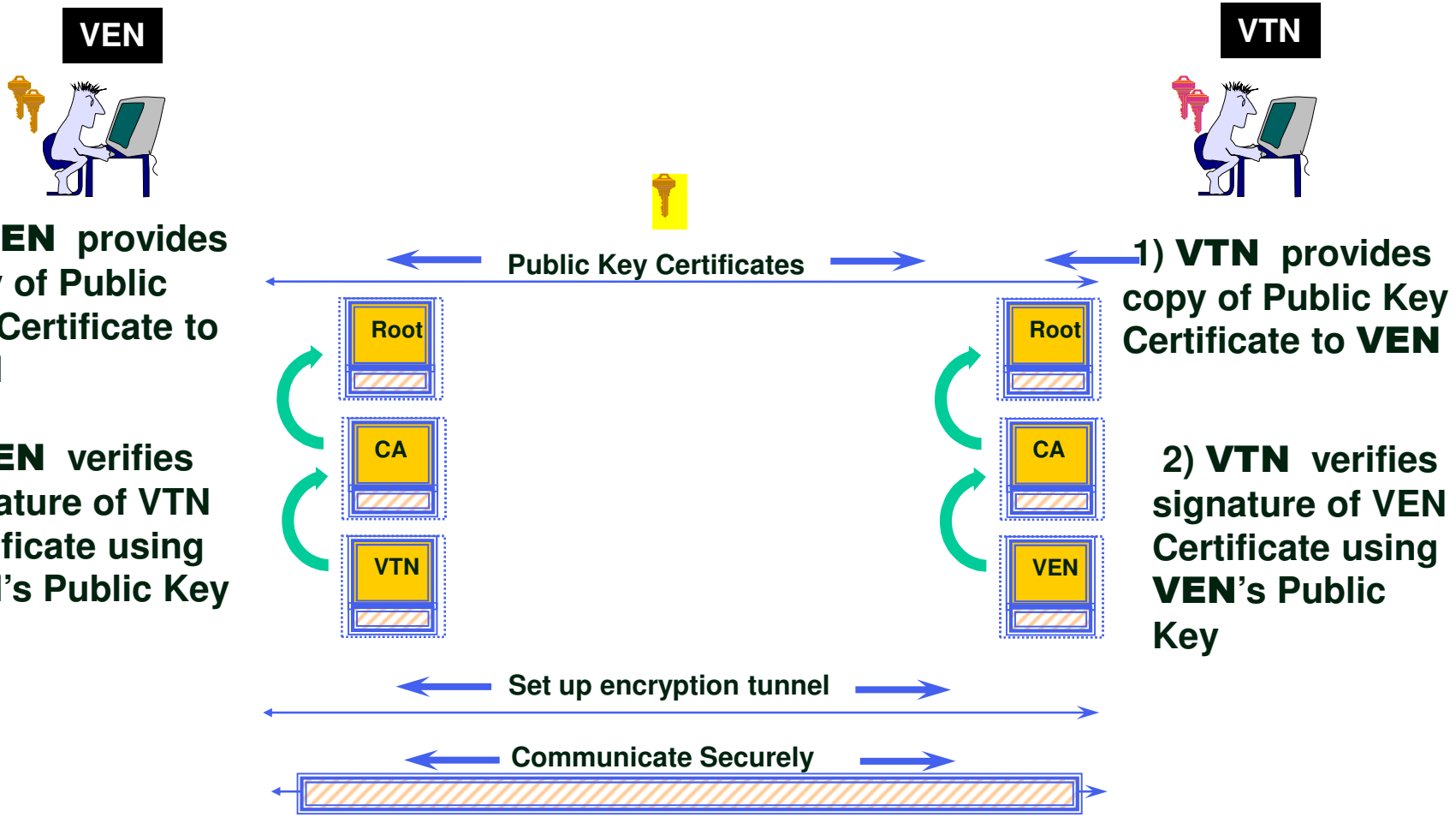
3 Operations

- Manage infrastructure on behalf of OpenADR
- Evolve Security specifications
- Reduce cost through volume aggregation
- Certificate Lifecycle Management
- Distributed CA audit and monitoring

Certificate Lifecycle Management

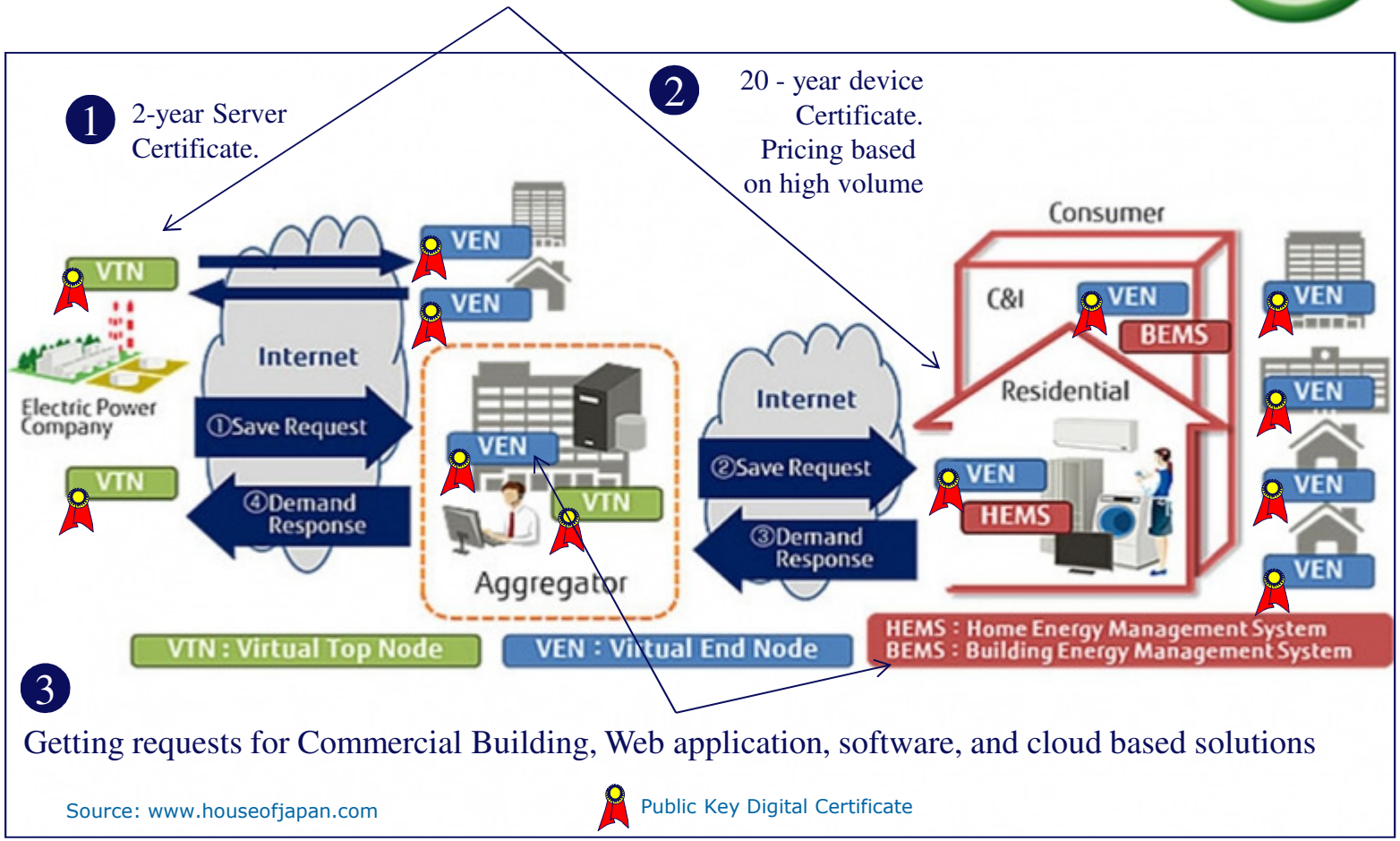


VEN / VTN Authentication



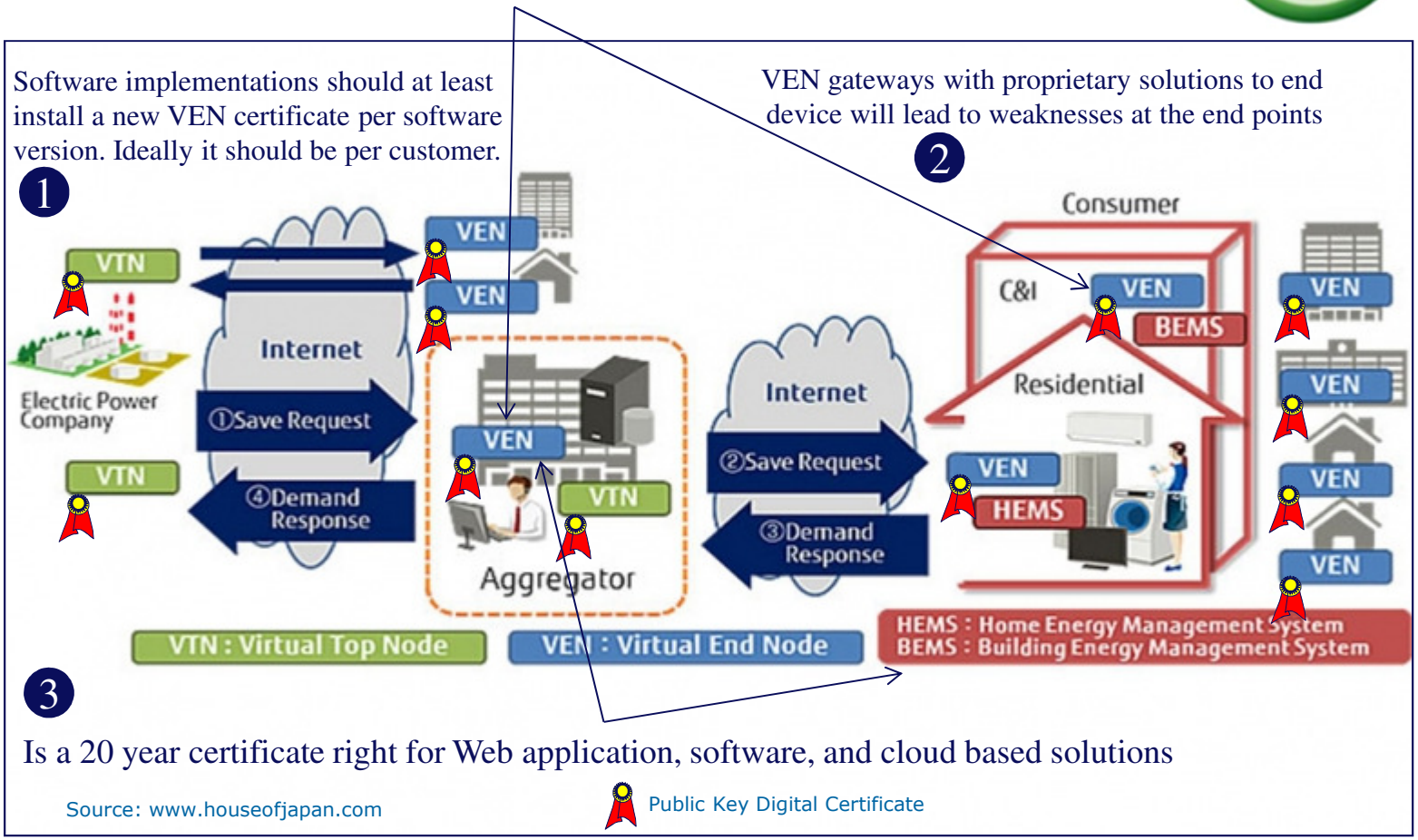
OpenADR PKI

Initial design based on Residential VEN devices and VTN servers



OpenADR PKI

Security concerns with new requests



NETWORKFX™

Oscar Marcia
President

NetworkFX, Inc.
858 Coal Creek Circle
Louisville, Co. 80027

Tel 303 661 3462
Fax 303 661 9199
Cell 720 470 9294

o.marcia@networkfx.net

www.networkfx.net