OpenADR Alliance Overview

6/18/14

Oscar Marcia
President
NetworkFX, Inc.
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

Source: www.houseofjapan.com
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

1. Certificate Data
2. Hash Function (SHA256)
3. Hash Result
4. Signing Function (e.g., RSA)
5. Digital Signature
6. Only Private Key holder can sign
Anyone can verify Certificate Data Hash Function Hash Result Valid compare Yes / No ?

Signed Digital Certificate

Hash Result

Public of A

Verify Function

Digital Signature

So the receiver can compare hashes to verify the signature

Valid compare Yes / No ?

Anyone can verify
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

Tier 1
Offline Root CAs

Tier 2
Online Sub-CAs

Tier 3
Subscribers

6/23/2014 © NetworkFX, Inc. 2014. All Rights Reserved. Proprietary/Confidential
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

- Server
- Client
- Internet
- TLS

Root CA

CA

Device Cert
Signed by: CA

VTN

VEN

© NetworkFX, Inc. 2014. All Rights Reserved.
Proprietary/Confidential
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

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
VEN / VTN Authentication

1) **VEN** provides copy of Public Key Certificate to **VTN**

2) **VEN** verifies signature of **VTN** Certificate using **VTN**’s Public Key

---

1) **VTN** provides copy of Public Key Certificate to **VEN**

2) **VTN** verifies signature of **VEN** Certificate using **VEN**’s Public Key

---

Set up encryption tunnel

Communicate Securely
OpenADR PKI
Initial design based on Residential VEN devices and VTN servers

1. 2-year Server Certificate.
2. 20-year device Certificate. Pricing based on high volume.
3. Getting requests for Commercial Building, Web application, software, and cloud based solutions.

Source: www.houseofjapan.com

Public Key Digital Certificate
OpenADR PKI
Security concerns with new requests

Software implementations should at least install a new VEN certificate per software version. Ideally it should be per customer.

VEN gateways with proprietary solutions to end device will lead to weaknesses at the end points.

Is a 20 year certificate right for Web application, software, and cloud based solutions?

Source: www.houseofjapan.com
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