Enabling The Standard for Automated Demand Response

OpenADR 2.0 – Security

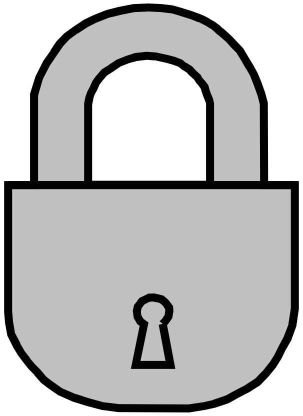
Rolf Bienert
Technical Director

Content

1. A little history
2. NIST and SGIP reviews
3. Security Options
4. OpenADR - NetworkFX model
5. Certificate types
6. Jim Zuber – Technical Implementation

History

- Initially username/password authentication in OpenADR 1.0
- Lots of discussions in the Profile and Security working groups to determine what is needed
- Cyber Security became increasingly important
- Created Security Use Case document
- Eventually decided on current setup



NIST & SGIP reviews

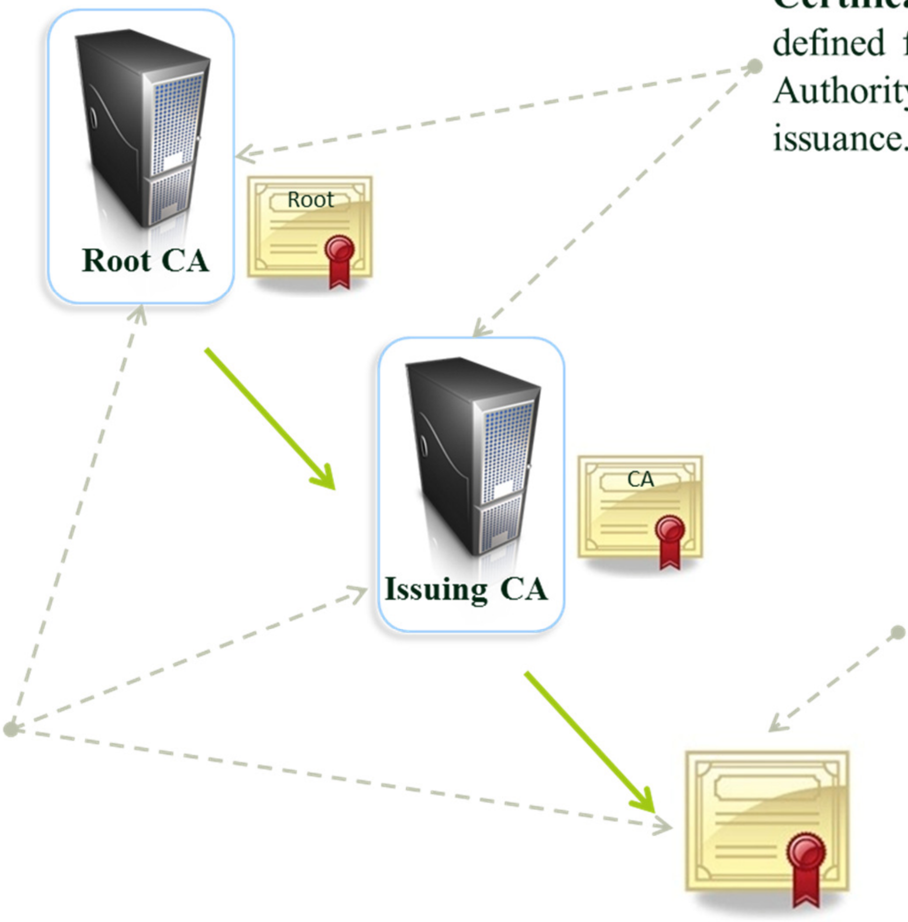
- OpenADR 2.0 in SGIP Catalog of Standards
- SGIP follows NIST guidelines for security and performed reviews
- Guidelines from NIST SPs and NISTIR
  - http://csrc.nist.gov/publications/PubsSPs.html
  - http://csrc.nist.gov/publications/PubsNISTIRs.html
- OpenADR 2.0 went through several review cycles with NIST experts

NIST – National Institute of Standards and Technology
SGIP – Smart Grid Interoperability Panel

Security Options

- Requirements:
  - Server and Client certificates
  - Non-deprecated cyphers
  - Non-depreciated TLS versions
  - **Trusted Root**
- Standard Security: TLS1.2 with server and client certificate
- High Security Option: Add XML wrapper for increased non-repudiation requirements

Security Options – Trusted Root



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

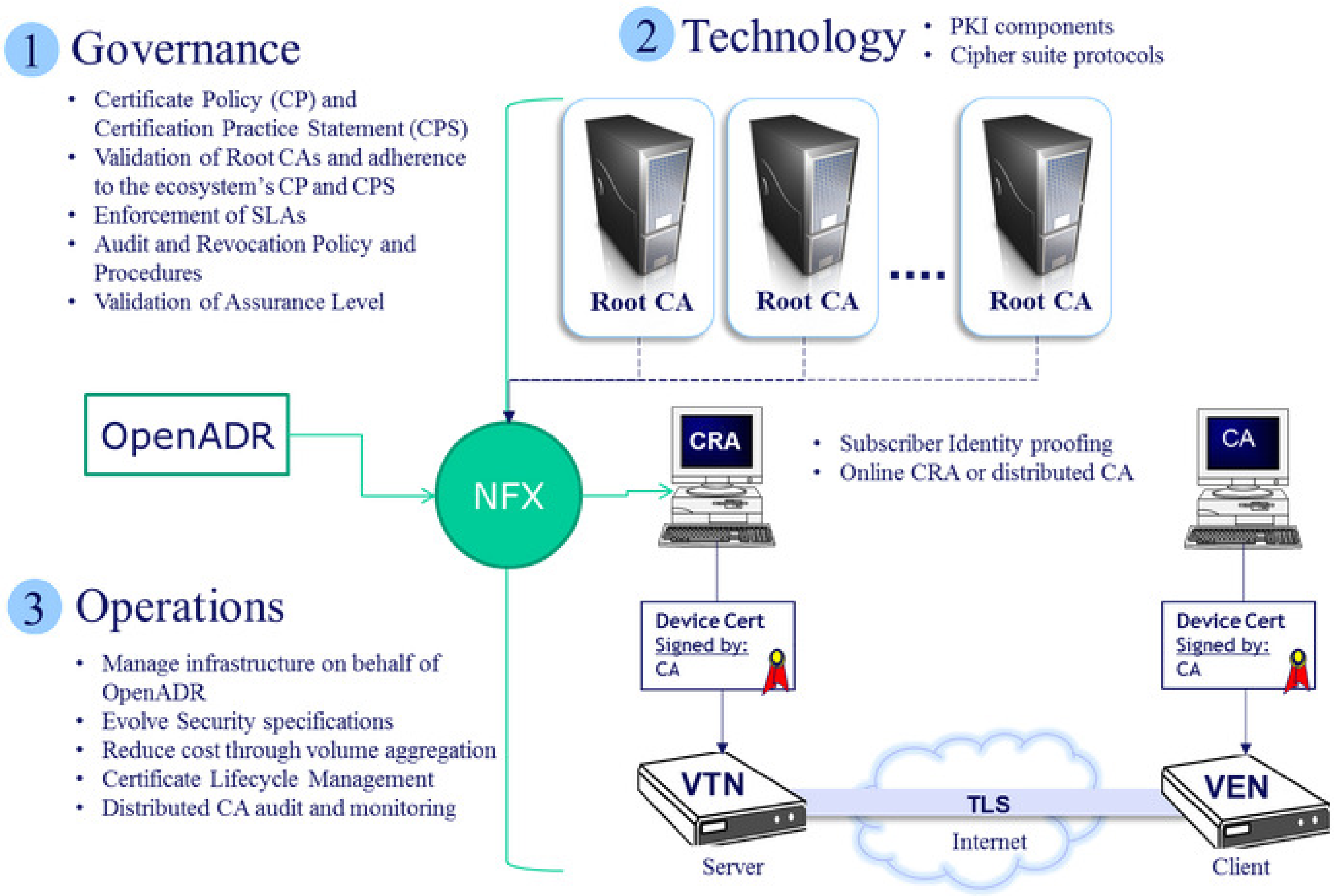
Certificate Policy defined to govern the public key infrastructure. Allows relying parties to access the assurance level (trust) of the certificate.

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

OpenADR – NetworkFX model

- Alliance started discussions with certificate providers
- Due to the initially low volume, little interest to create specific OpenADR setup
- Eventually engaged with NetworkFX, a spin off from the cable industry to manage the program
- NFX is the program administrator; currently Symantec is the Certificate Authority
- Note: Once certified, OpenADR can only recommend to use our process.

OpenADR – NetworkFX model



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

- Subscriber Identity proofing
- Online CRA or distributed CA

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 Types

- Test Certificates – testing with test harness, some test servers in the field
  - Will not work with production certificates
- Production Certificates – 20 year validity, traceable
  - Low quantity programs
  - High quality programs
- Trial Certificates – Purchased through Alliance account, 5-year validity, easier entry into small scale deployments
- Visit http://www.openadr.org/cyber-security

openADR ALLIANCE