ARIN's RPKI Trust Anchor Demystified

Mark Kosters

ARIN Chief Technology Officer

The RPKI Ecosystem and Trust Anchors

The Resource Public Key Infrastructure (RPKI) ecosystem is comprised of

Repositories that contain Route Origin Authorizations (and soon Autonomous System Provider Authentication [ASPA] objects), certification revocation lists, and manifests

Validators that validate ROAs and ASPA objects feeding results to the ISP border routers

To validate the objects, the validators need to have a "bootstrap" to find out the root of the certificate tree and cryptically validate the secured objects (more RPKI hierarchy later).

The bootstrap information is called a Trust Anchor (TA).

Configured on each validator

The RPKI Ecosystem and Trust Anchors

Agenda

Brief tutorial on RPKI Certificates

ARIN's structure for ARIN-issued resources

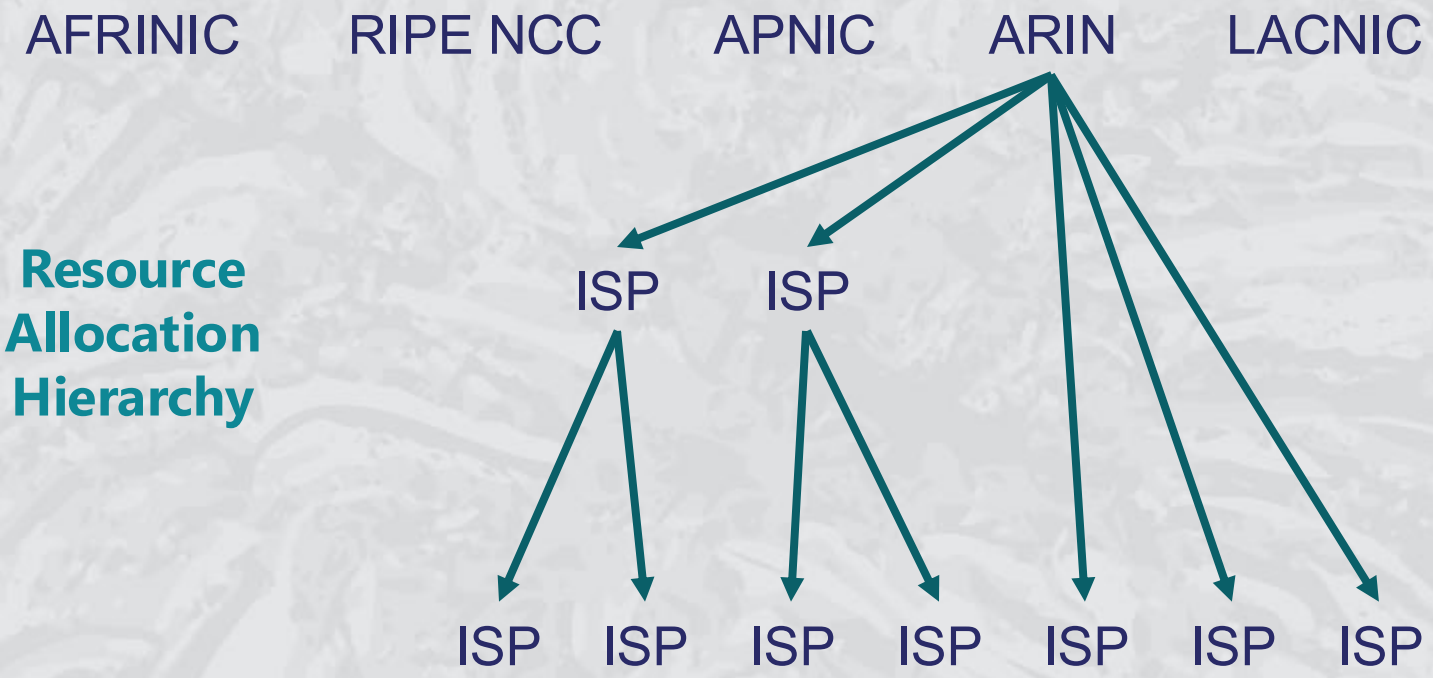
Why the Trust Anchor is important

Designing and exercising the signing process

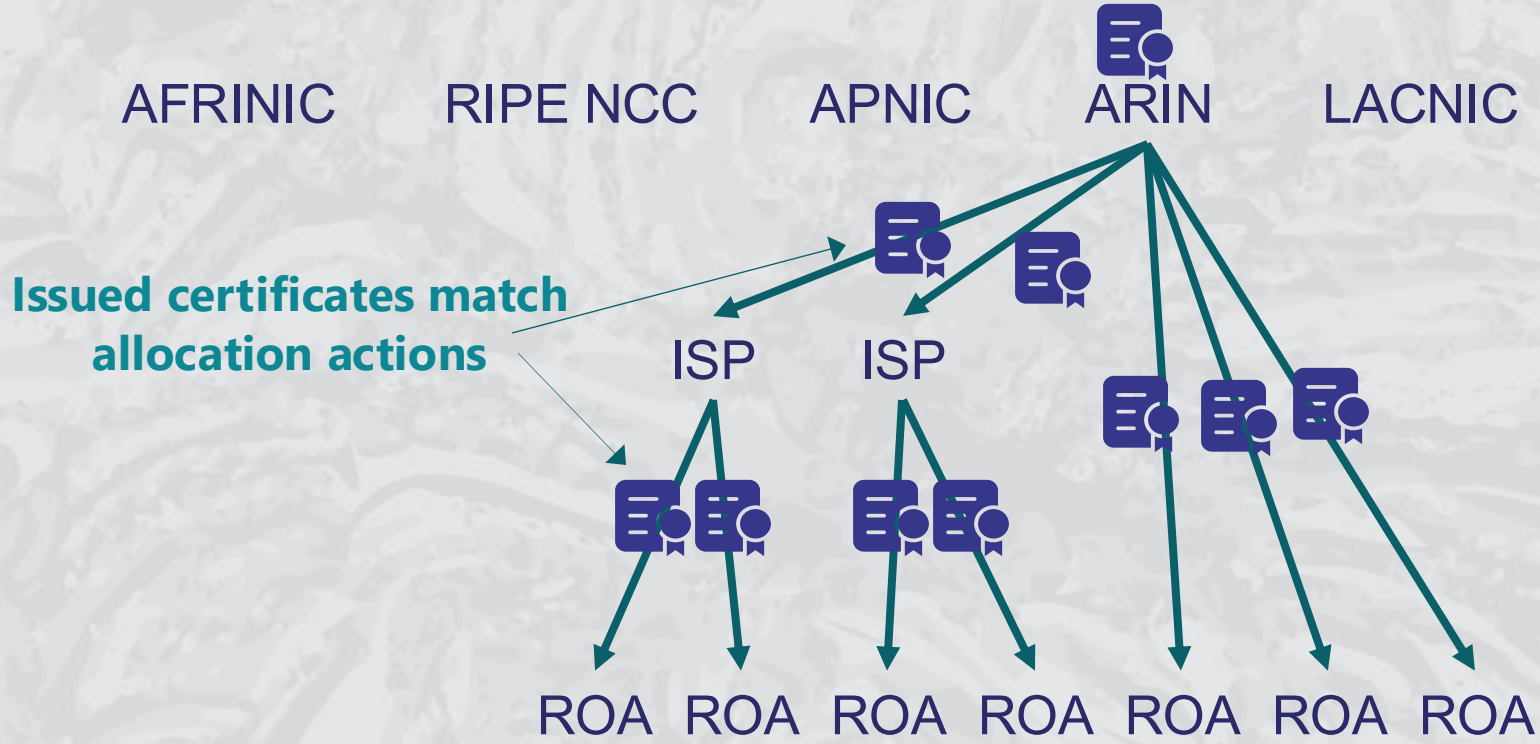
Brief Tutorial on RPKI Certificates

Resource Certificates

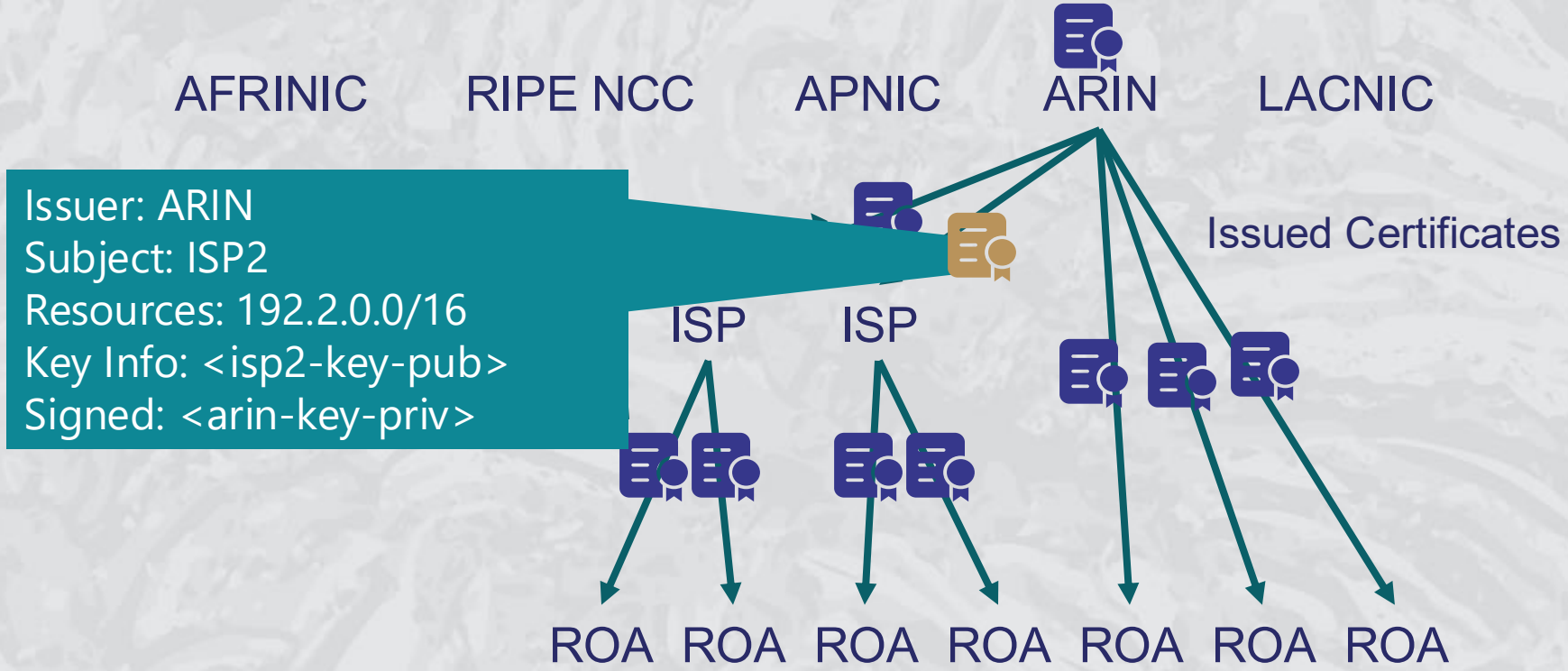
Resource Allocation Hierarchy



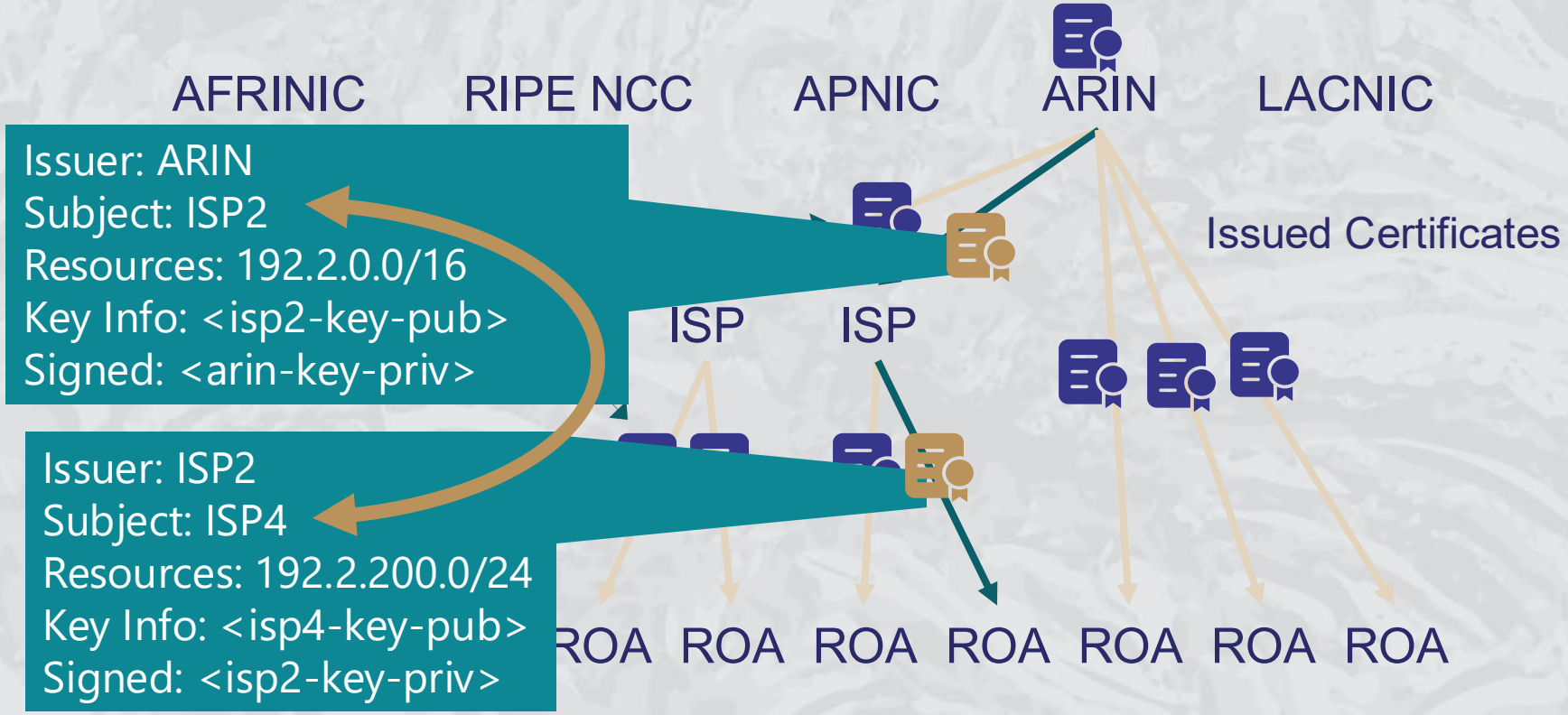
Resource Certificates



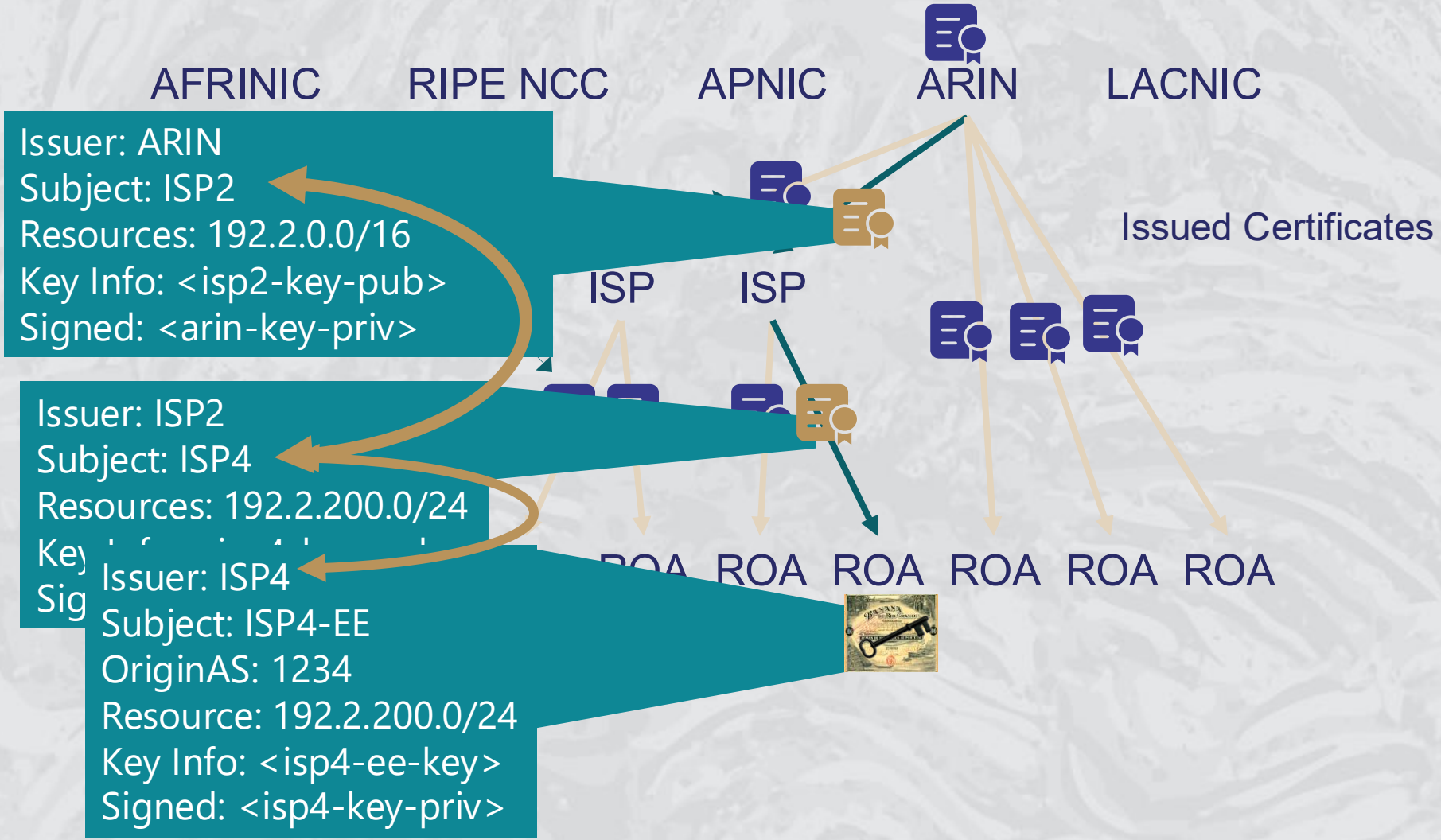
Resource Certificates



Resource Certificates



Resource Certificates



ARIN's Structure for RPKI Resources

ARIN's Trust Anchor Configuration

ARIN's Trust Anchor Configuration

- Offline Trust Anchor
  - Solely responsible for signing the online operational certificate
    - The servers are NOT on the network
    - The key is protected by offline hardware security modules (HSMs)
- Online Operational Certificate
  - Responsible for signing Organizational Certificates
    - The servers are on the network
    - The keys are protected by online HSMs
- Organization Certificate
  - Responsible for signing ROAs and ASPAs or Delegated Certificates
    - The servers are on the network
    - The keys are protected by online HSMs

Offline Trust Anchor Details

Solely responsible for signing the online operational certificate

- The servers are NOT on the network
- The keys are protected by offline hardware security modules

Online Operational Certificate signing request transferred by hand to/from the Offline Operational Certificate servers

Keys stored on the hardware security module

Offline Trust Anchor

The Offline Operational Certificate servers and their keys are protected by:

- Not being connected to the network
- Requiring physical access by a third person (operations person) with multi-factor entry to safe
- Monitoring safe with cameras
- Logging access entry
- Storing keys at two sites with dual-custody safes:
  - Can only be opened by two separate people (aka keyholders) with two separate combinations

Operational Online Certificate

- Responsible for signing Organization Certificates
  - The servers are on the network
  - The keys are protected by online HSMs
- Online operational certificate servers at two sites

Organization Certificate

Also called a **Resource Certificate**

- Signs ROAs
- Signs ASPAs
- Signs manifests
- Signs certificate revocation lists (CRLs)
- Signs over delegated certificates

Hosted Mode

ARIN is responsible for signing all ROAs, ASPAs, manifests, and CRLs on behalf of the customer

Delegated Mode

The customer is responsible for signing ROAs, ASPAs, manifests, and CRLs

Why the Trust Anchor is Important

Why the Trust Anchor is Important

- RPKI is a system based on trust
- Trust in a hierarchal system starts at the top of the tree
- ARIN is at the top of the tree

If there is compromise

- Hijacks of existing space can be created without knowledge of the resource holder
- Hijacks of space outside of ARIN's region can be placed into ARIN's RPKI system
- Compromise will lead to manual configuration settings on validators

As a result, we are very careful about ensuring strong security

Designing and Exercising the Process

Building this System and Inserting Trust

- Did not want to reinvent the wheel
- The DNS root is very similar to the RPKI trust anchor
- ICANN has a very well documented process for root DNS key signing
- ARIN staff witnessed the DNS root key signing process, and implemented methods to our own signing ceremony
- ARIN uses HSMs for secure storing of material

Signing Ceremony Overview

- The **offline operational certificate** has a six-month lifespan and need to be renewed within that period
- The **online operational certificate** also has a six-month lifespan and needs to be renewed within that period
- **Both certificates** are signed by the offline operational key
- Online operational certificate signing request **transferred by hand** to/from the offline operational certificate servers

Accessing the Keying Material

Requires

- Two keyholders
- An operations person
- A witness/master of ceremony (MC)

Follows a script that is very detailed

- Every step explicitly called out
- Every step initialed by the witness/MC
- Any deviation requires documentation
- Documentation stored in a safe at ARIN HQ by the witness/MC

Accessing the safe

- Operations person has access/control to the physical site
- Keyholders unlock the safe and hold the keying material
- Witness/MC ensures that the keyholders are the only ones who physically hold the keying material


ARIN 55
POWERED BY PARTICIPATION
Questions and Comments?
Thank you