Metadata Signing and Update

SWITCH

Serving Swiss Universities

Patrik Schnellmann
patrik.schnellmann@switch.ch

What is in the SWITCHaai Metadata?

- List of federation entities (IdP and SP)
- Configuration relevant for communication between entities
  - IdP SSO and AA endpoints
  - IdP's certificate KeyNames used to sign assertions
  - SP's endpoint(s)
  - ...
- Trust anchors for credentials used by entities
  - Root CA and intermediate certificates

How the IdP loads the Metadata

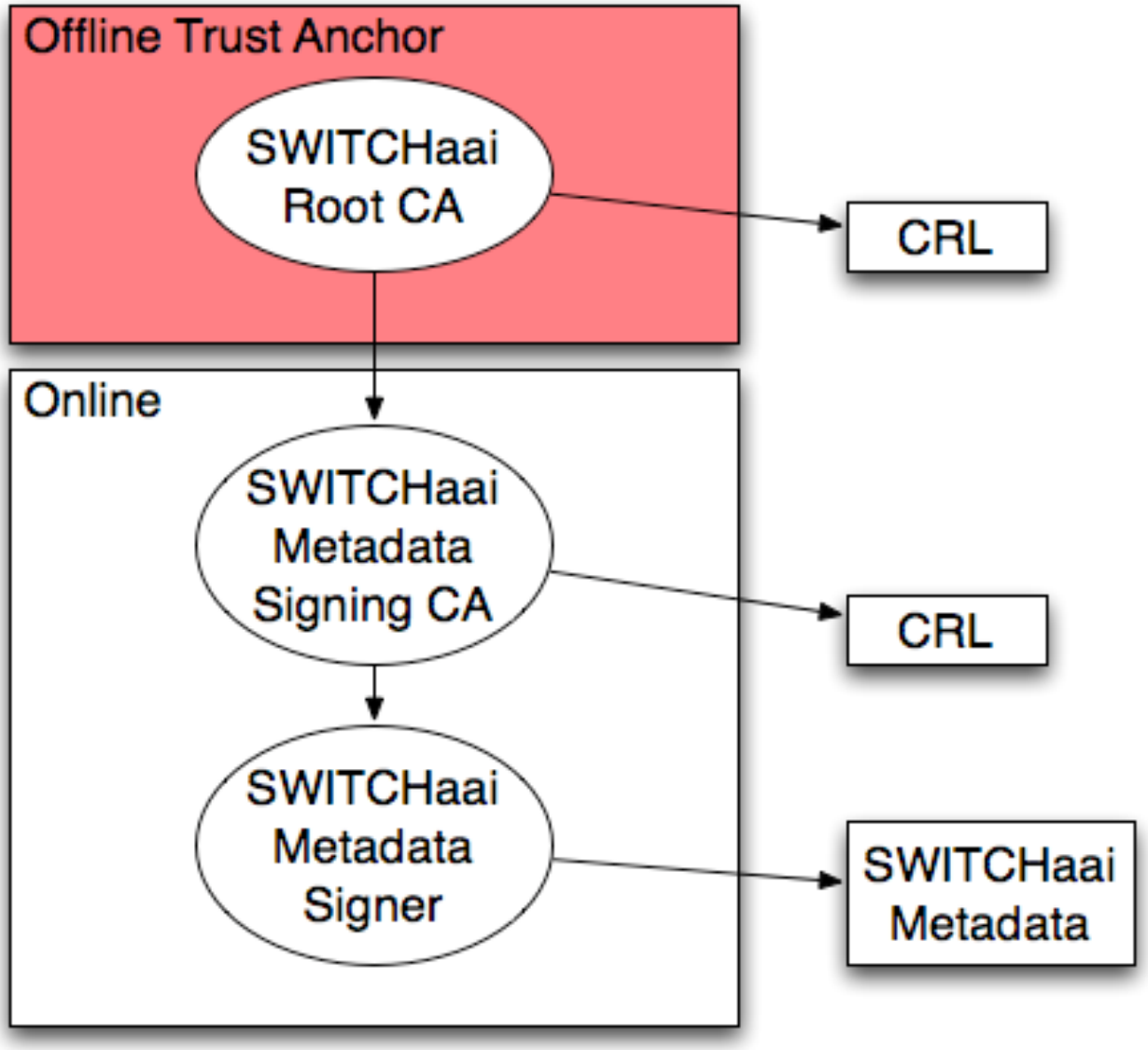
- Download from a URL
  - http://www.switch.ch/aai/federation/SWITCHaai/metadata.switchaai_signed.xml
- The metadata is signed by a certificate.
- This certificate has been installed on your IdP (metadata.crt).
- The IdP verifies the signature on the metadata by using the Metadata Signer Certificate.

Why trust the Metadata?

- Because it is from SWITCH?
- Because it is signed?
- ... Yes, but ...
- How do you know it is from SWITCH - who signed it?
- Make sure the IdP uses the trust anchor from SWITCH.
- Make sure the signature has been made by a certificate signed by this trust anchor.
- SWITCH needs to make sure the signing certificate's key does not get compromised.

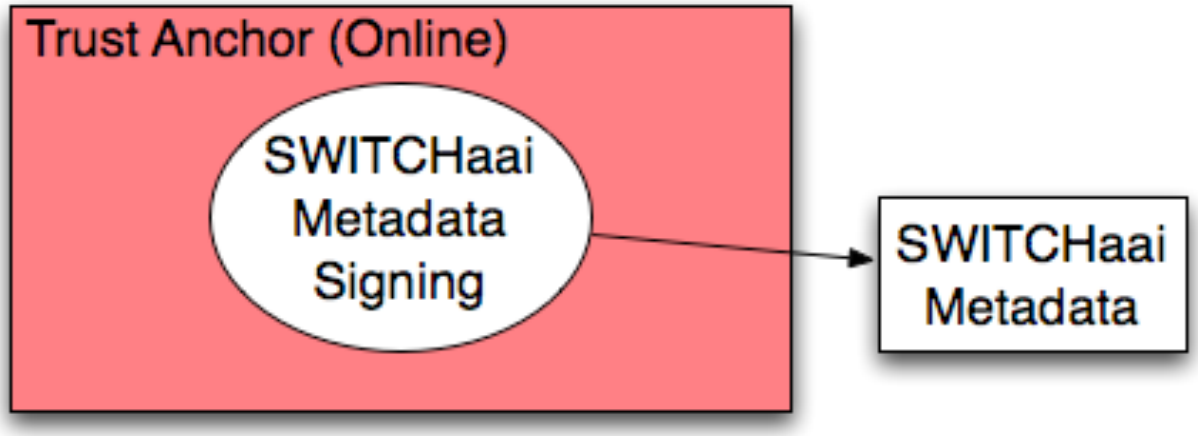
Metadata Signing - New infrastructure

- 2048 bit key
  on Hardware token
  (poor man's HSM)
- Trust anchor different
  from Signer certificate
- Revocation in case
  of key compromise



Metadata Signing up to now

- Self-signed Metadata Signer Certificate
- 1024 bit key on Metadata Signing Server



Metadata Signing - comparison

MD Signing up to now

- 1024 bit key on Metadata Signing Server
- Self-signed Metadata Signer Certificate

New infrastructure

- 2048 bit key on Hardware token (poor man's HSM)
- Trust anchor different from Signer certificate
- Revocation in case of key compromise
- Limited validity of metadata (5 d)

⇨ With the new solution, SWITCH sets the level for state-of-the-art metadata signing.

Distribution points for CA, CRL, Metadata

- CA
  http://ca.aai.switch.ch/SWITCHaaiRootCA.crt.pem
  http://ca.aai.switch.ch/SWITCHaaiMetadataSigningCA2008.crt.pem

- CRLs
  http://crl.aai.switch.ch/SWITCHaaiRootCA.crl
  http://crl.aai.switch.ch/SWITCHaaiMetadataSigningCA2008.crl

- Metadata
  http://metadata.aai.switch.ch/metadata.switchaai.xml
  http://metadata.aai.switch.ch/metadata.aaitest.xml
  (SWITCH will only publish signed metadata.)

⇨ See: https://www.switch.ch/aai/metadata/

Improved Signing - Improved Security?

- Measures taken:
  - Offline trust anchor
  - Revocation list for signing certificate
  - Limited life-time of federation metadata
  - Use only signed metadata on IdP

- Signature can ensure integrity of metadata, but:
  - Administrators are still responsible for its content