Key rollover

Different KeyDescriptors

The KeyDescriptor stores a certificate, BUT the only interesting part are the public-key stored inside the certificate! The private part of the key is stored on the machine responsible for the Entity,

Some SAML implementations also looks at the notValidAfter value and refuses to use old certificates/keys

There are two types of keys/certificates used in the Metadata for an entity.

KeyDescriptor use="encryption"

Stores the public encryption key. Data sent TO the Entity could be encrypted with this key and then only decrypted by the Entity is self.

When changing this Key you first have to add the new key and active in the software BEFORE publishing it. If not the software might not be able to decrypt if the other end start using the new encryptionkey

KeyDescriptor use="signing"

Stores the public signing key. Data sent FROM the Entity could be signed with their private key and then verified with this key.

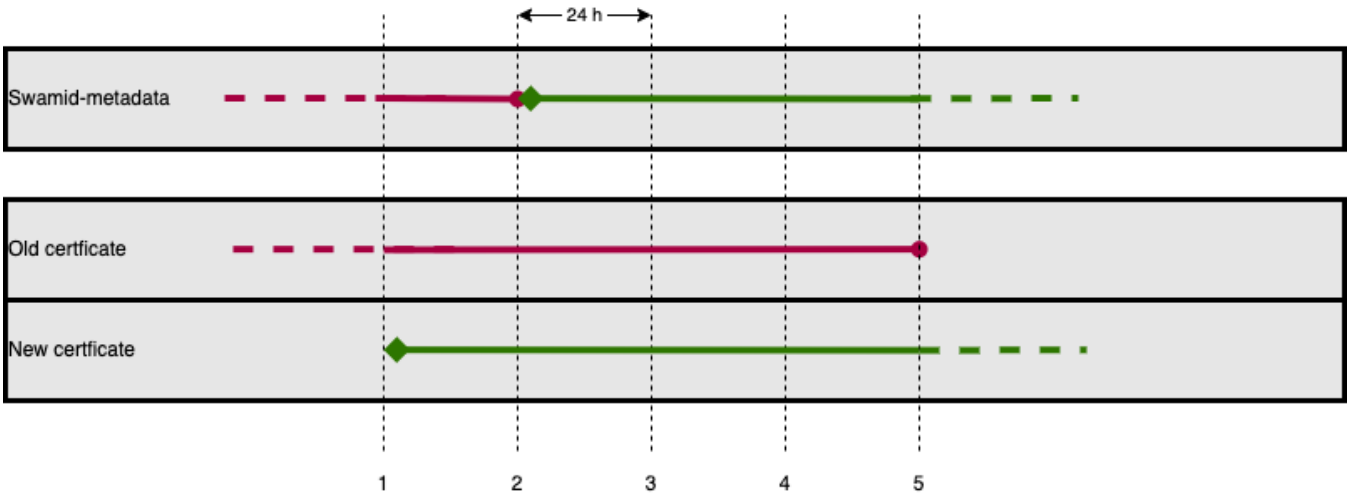
When changing this Key you first have to publish it BEFORE activating in the software. If not the receiver might not be able to verify the signature.

KeyDescriptor without any use

If attribut use is not present this key could be used both for signing and encryption.

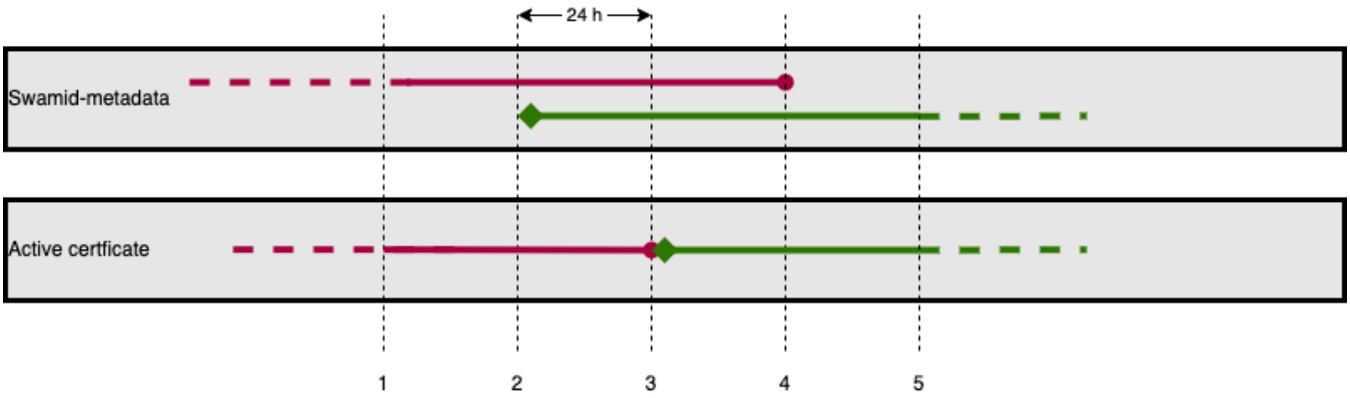
Doing Key rollover

Rolling encryption key



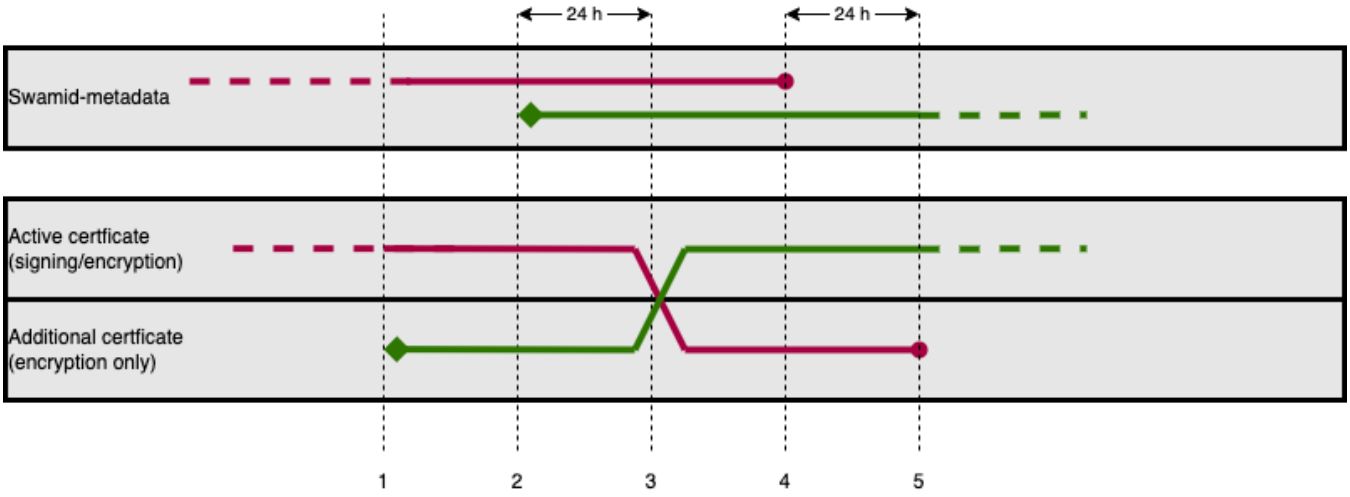
1. Create the key and add it to the software to be able to decrypt incoming messages.
2. Upload the new XML with the new cert to metadata.swamid.se/admin and request publication. Wait until you get confirmation of publication and then for at least 8 h more (recommended 24 h if in SWAMID and 48 h in eduGAIN) for all entities to pick up the new cert/key.
3. All encrypted messages should now come with the new key. Skip to 5
4. Skip to 5
5. Disable / remove key from software.

Rolling signing key



1. Create the key.
2. Upload the new XML with both new and old cert to metadata.swamid.se/admin and request publication. Wait until you get confirmation of publication and then for at least 8 h more (recommended 24 h if in SWAMID and 48 h in eduGAIN) for all entities to pick up the new cert/key.
3. All Entites should now have our new Signing-key/cert. Switch in software to start signing with new key. Disable / remove old key from software.
4. Request removal of old cert via metadata.swamid.se/admin .
5. We are done

Rolling combined encryption/signing key



1. Create the key and add it to the software to be able to decrypt incoming messages.
2. Upload the new XML with the old cert (marked use=signing) and new cert without any use attribute to metadata.swamid.se/admin and request publication. Wait until you get confirmation of publication and then for at least 8 h more (recommended 24 h if in SWAMID and 48 h in eduGAIN) for all entities to pick up the new cert/key.
3. All encrypted messages should now come with the new key and all Entites should now have our new Signing-key/cert. Switch in software to start signing with new key.
4. Request removal of old cert via metadata.swamid.se/admin and request publication. Wait until you get confirmation of publication and then for at least 8 h more (recommended 24 h if in SWAMID and 48 h in eduGAIN) for all entities to stop using the old encryption cert/key.
5. Disable / remove key from software.

Metadata during Key rollover

For information how the Metadata will look during each phase please look at Metadata during Key rollover

Steps in different software

- Shibboleth IdP
- Shibboleth SP
- ADFS
- SimpleSAMLphp