Infrastructure à clés publiques

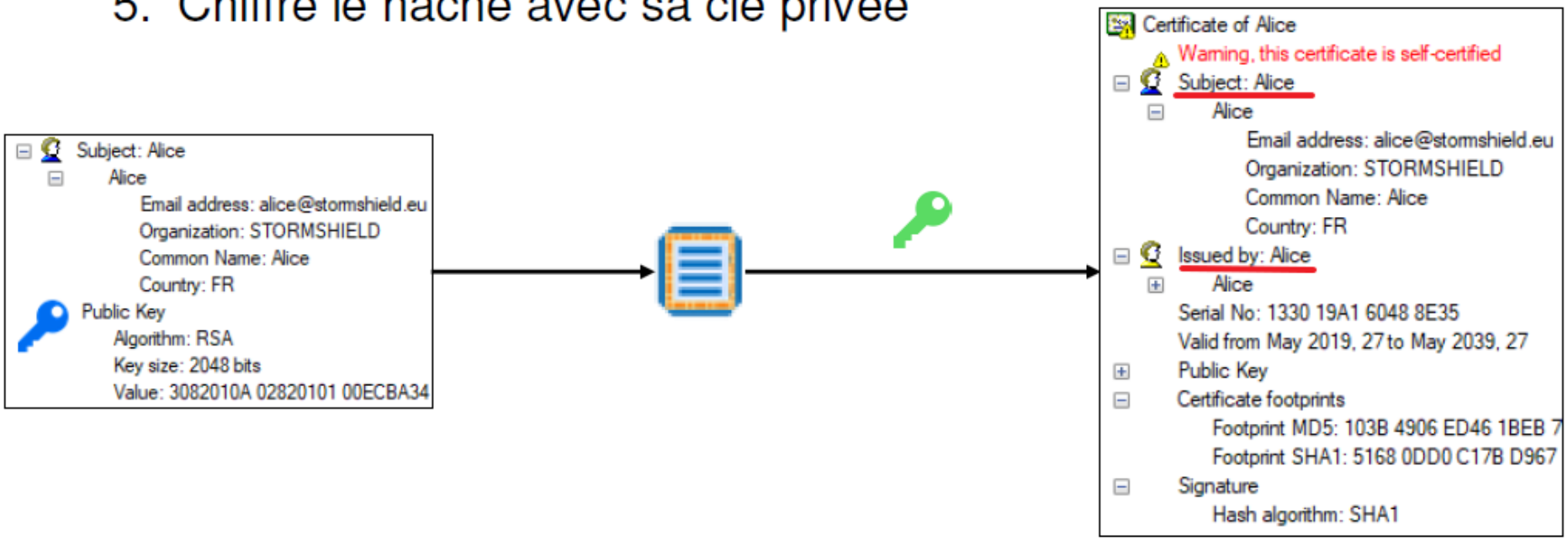
PKI

Infrastructure à clés publiques

- Certificat autosigné :
  - Créer la bi-clé asymétrique
  - Fournir ses informations d'identité
  - Regrouper clé publique et ses informations
  - Calculer le haché de l'ensemble
  - Signer le haché avec sa clé privée (signature numérique)
  - > certificat autosigné (+ algo)
  - > champ Subject et Issued by identique

- Génération d'un certificat auto-signé

1. Alice Génère clé privée et clé publique
2. Renseigne les informations relatives à son identité
3. Regroupe ces informations et sa clé publique
4. Calcule le haché de ce regroupement
5. Chiffre le haché avec sa clé privée



Infrastructure à clés publiques

- Certificat autosigné :
  - Transmettre son certificat pour être identifiée
  - « Confiance » dans ce certificat
  - Clé privée + certificat = identité numérique
  - Si perte de l'ordinateur -> perte de la clé privée

Infrastructure à clés publiques

- Autorité de certification :
  - Tiers de confiance
  - Périmètre défini
  - Gère les certificats et les identités numériques
  - Garante de l'authenticité des certificats
  - Signe (atteste) les certificats et la liste des certificats révoqués (CRL)

- Gestion des certificats par une autorité de certification