

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

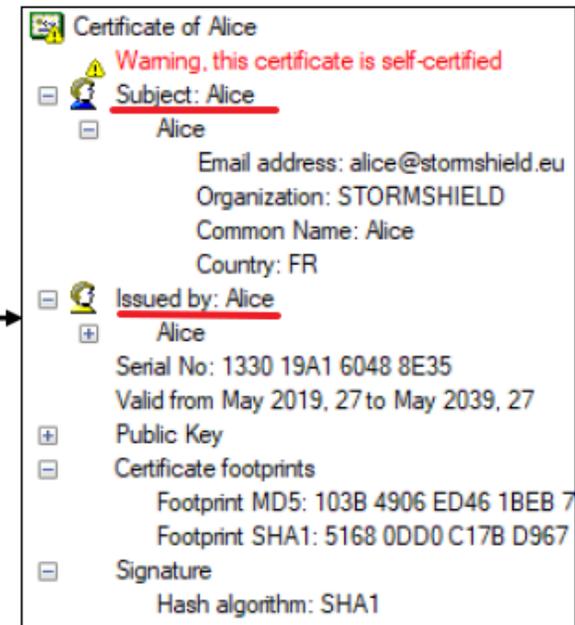
- Génération d'un certificat auto-signé

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



Subject: Alice
Alice
Email address: alice@stormshield.eu
Organization: STORMSHIELD
Common Name: Alice
Country: FR

Public Key
Algorithm: RSA
Key size: 2048 bits
Value: 3082010A 02820101 00ECBA34



Certificate of Alice
Warning, this certificate is self-certified

Subject: Alice
Alice
Email address: alice@stormshield.eu
Organization: STORMSHIELD
Common Name: Alice
Country: FR

Issued by: Alice
Alice
Serial No: 1330 19A1 6048 8E35
Valid from May 2019, 27 to May 2039, 27

Public Key

Certificate footprints
Footprint MD5: 103B 4906 ED46 1BEB 7
Footprint SHA1: 5168 0DD0 C17B D967

Signature
Hash algorithm: SHA1

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

Demande externe

Création d'une identité

