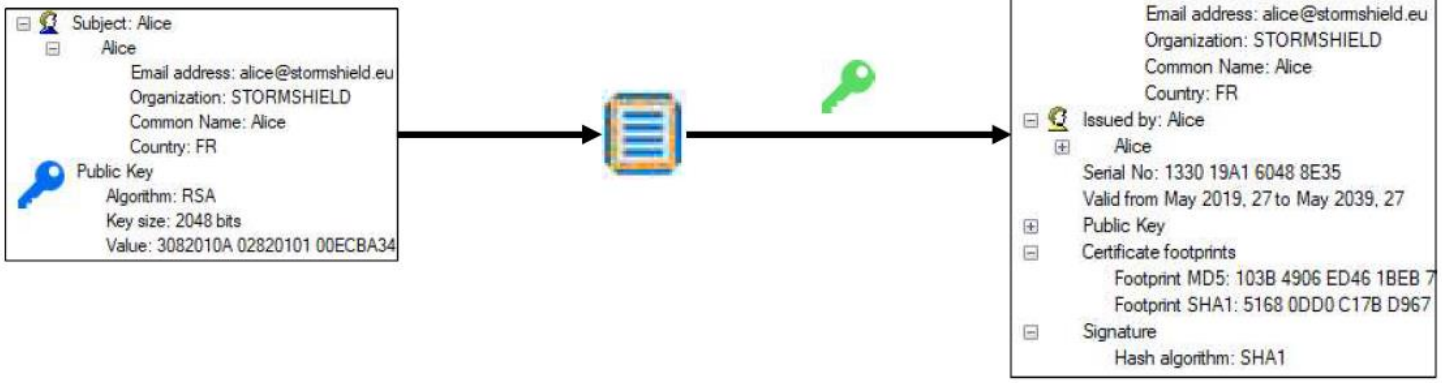
Bloc 3
Infrastructure à clé publique

- Certificat autosigné

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



Bloc 3
Infrastructure à clé publique

- Chiffrement du haché avec la clé privée
  - > Signature numérique
- > certificat auto-signé
  - Champ **Subject** et **Issued by** identiques
- Avoir une relation de confiance
- Clé privée + certificat
  - > identité numérique d'une personne
- Perte d'ordinateur -> perte de la clé privée

Bloc 3
Infrastructure à clé publique

- PKI (Public Key Infrastructure)

Bloc 3
Infrastructure à clé publique

- Autorité de certification
  - Tiers de confiance :
    - signature du certificat
  - Gère les certificats :
    - CSR Certificate Signing Request
  - Peut gérer les identités numériques (PKCS#12)
    - Clé privée + certificat utilisateur + certificat CA
  - Publie
    - les certificats
    - la CRL (Certificate Revocation List)

Bloc 3
Infrastructure à clé publique

- Format des certificats

  Défini par la norme X509, un certificat contient :

  - Version et numéro de série du certificat
  - Algorithme et valeur de la signature du certificat
  - Issuer : DN (Distinguished Name) de la CA
  - Période de validité (date de début et date de fin)
  - DN du détenteur du certificat
  - Informations sur la clé publique (clé publique et algorithme)
  - Possibles extensions qui conditionnent l'usage du certificat, par exemple liste des points de distribution de la CRL (CRLDP)