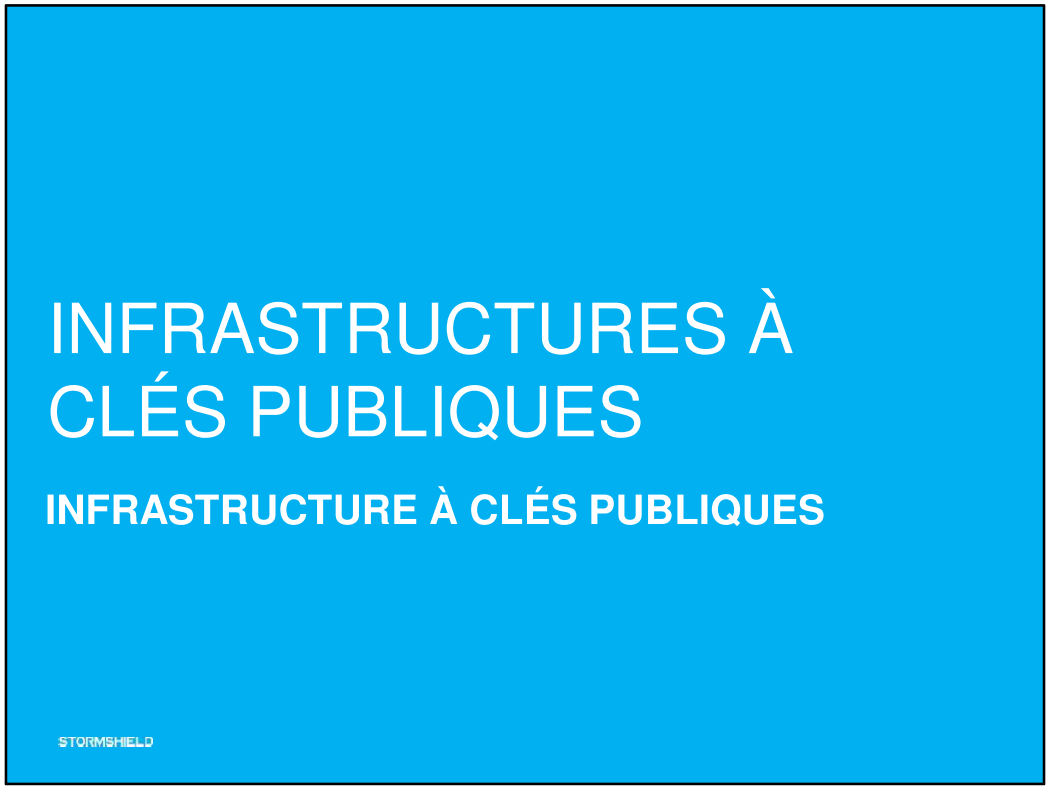
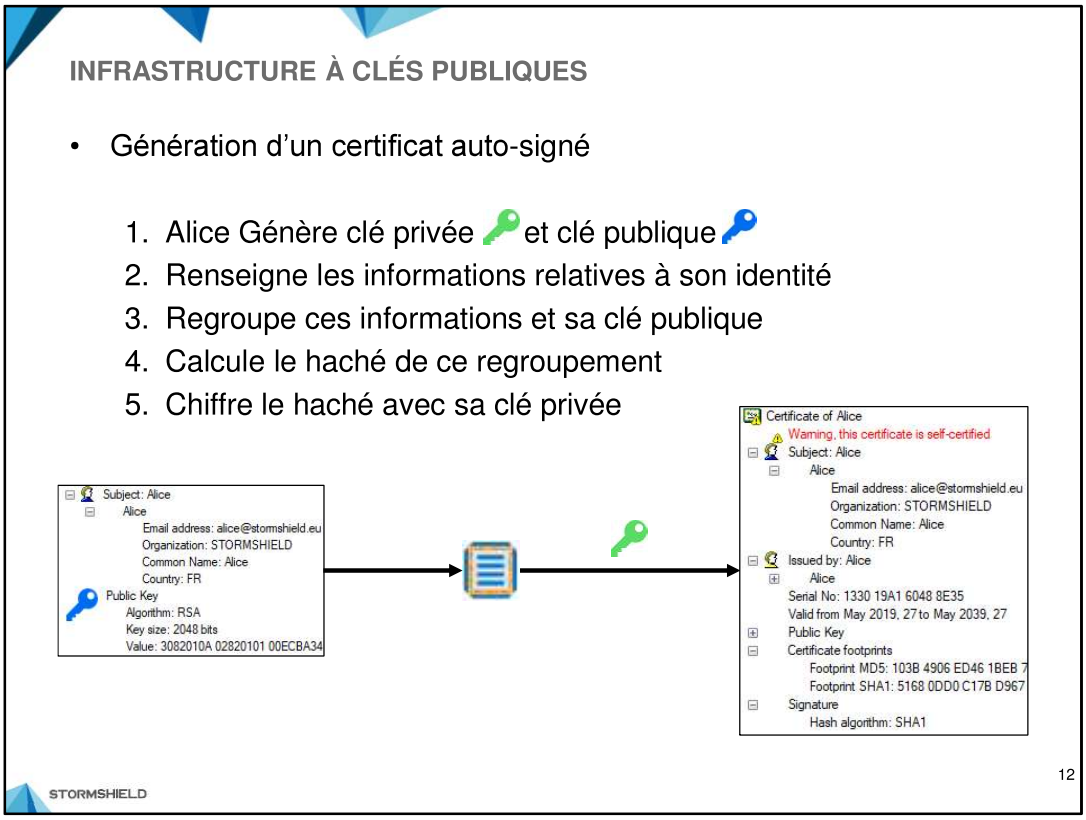



## Programme du module

- ✔ Qu'est-ce que la cryptographie ?
- ✔ Eléments de cryptographie
- ➔ Infrastructures à clés publiques
  - PKI Stormshield Network
  - Création d'une autorité de certification
  - Création d'une identité serveur
  - Création d'une identité utilisateur
  - Gestion des identités et certificats
  - Révocation de certificats et CRL
  - Lab – PKI




## Certificat auto-signé

1. Alice crée une bi-clé asymétrique, composée d'une partie publique (clé publique) et d'une partie privée (clé privée),
2. Alice renseigne l'ensemble des informations permettant de l'identifier,
3. Alice regroupe ces informations et sa clé publique dans un fichier structuré,
4. Alice calcule le haché de l'ensemble de ces données,
5. Alice chiffre le haché avec sa clé privée (signature numérique).
6. Le fichier obtenu est un certificat auto-signé, et contient entre autres l'algorithme de signature utilisé et les hachés résultants (selon les différents algorithmes choisis lors de l'opération).

Le certificat auto-signé identifie une personne dans l'exemple ci-dessus, un système ou un équipement.

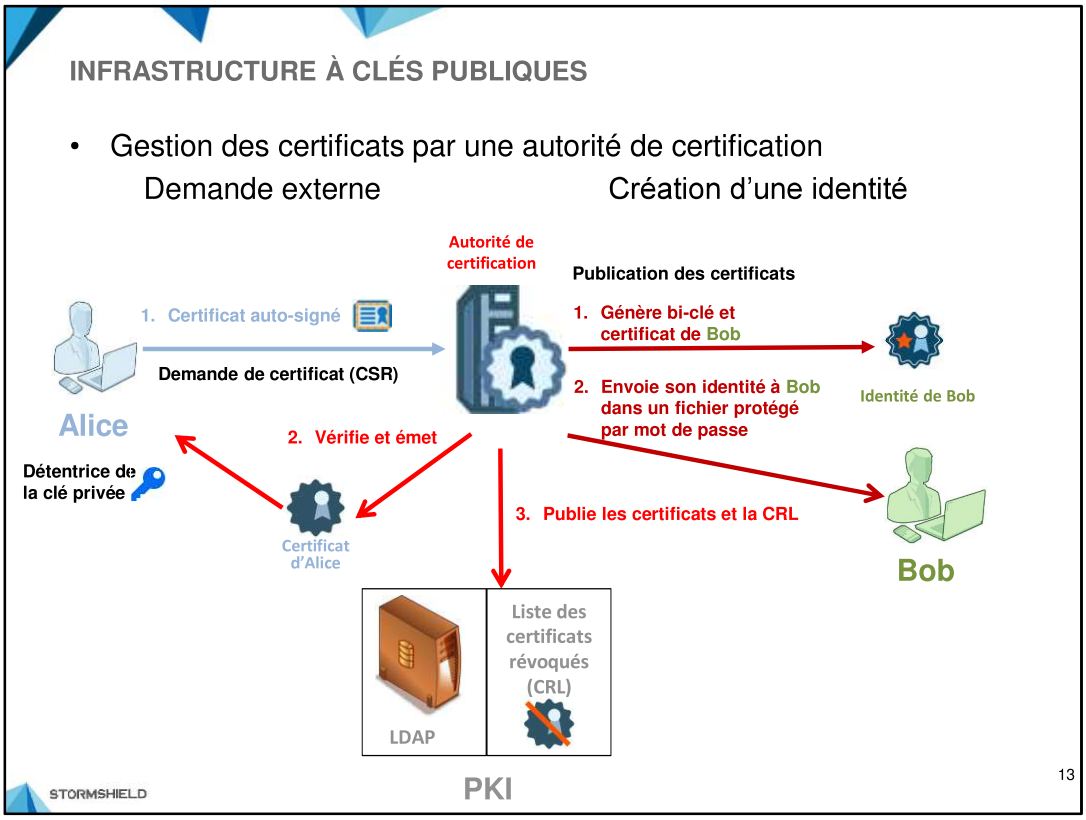
Remarquez que le champ « Subject » et le champ « Issued by » sont identiques, ce qui est toujours le cas pour un certificat auto-signé.

Alice peut transmettre son certificat à ses correspondants, afin que ces derniers puissent l'authentifier, en revanche, elle ne doit jamais transmettre sa clé privée à quiconque.

L'ensemble [clé privée + certificat] représente l'identité numérique d'une personne.

## Inconvénients

- En cas de perte ou de vol de son ordinateur, Alice n'a plus accès à sa clé privée,
- La gestion d'un grand nombre d'utilisateurs en entreprise ne peut pas s'appuyer sur des certificats auto-signés,
- Les personnes d'une organisation doivent avoir une relation de confiance avec Alice pour utiliser son certificat.




## Autorité de certification (Certification Authority)

Une autorité de certification est un tiers de confiance permettant dans un périmètre défini (Entreprise, Agence, Continent,…) de gérer les certificats, voire les identités numériques de toutes les entités (personnes, systèmes, équipements) amenées à échanger entre elles de manière sécurisée.

Elle est garante de l'authenticité des certificats et de leur contenu, justifiant ainsi la relation de confiance envers cette CA et les différents utilisateurs. En effet, sur présentation d'un certificat, il est vérifié qu'il est acceptable en s'appuyant sur la validité de la signature de ce certificat par la CA.

L'autorité de certification signe (atteste de la validité de) les certificats ainsi que la liste des certificats révoqués (CRL : Certificate Revocation List).

Certaines architectures peuvent inclure des sous autorités qui sont sous la responsabilité d'une autorité racine (CA root).

## Demande externe

**1 –** Alice envoie une demande de certificat (CSR = Certificate Signing Request) à la CA,

**2 –** La CA vérifie l'authenticité de l'identité du demandeur, et émet un certificat signé pour Alice,

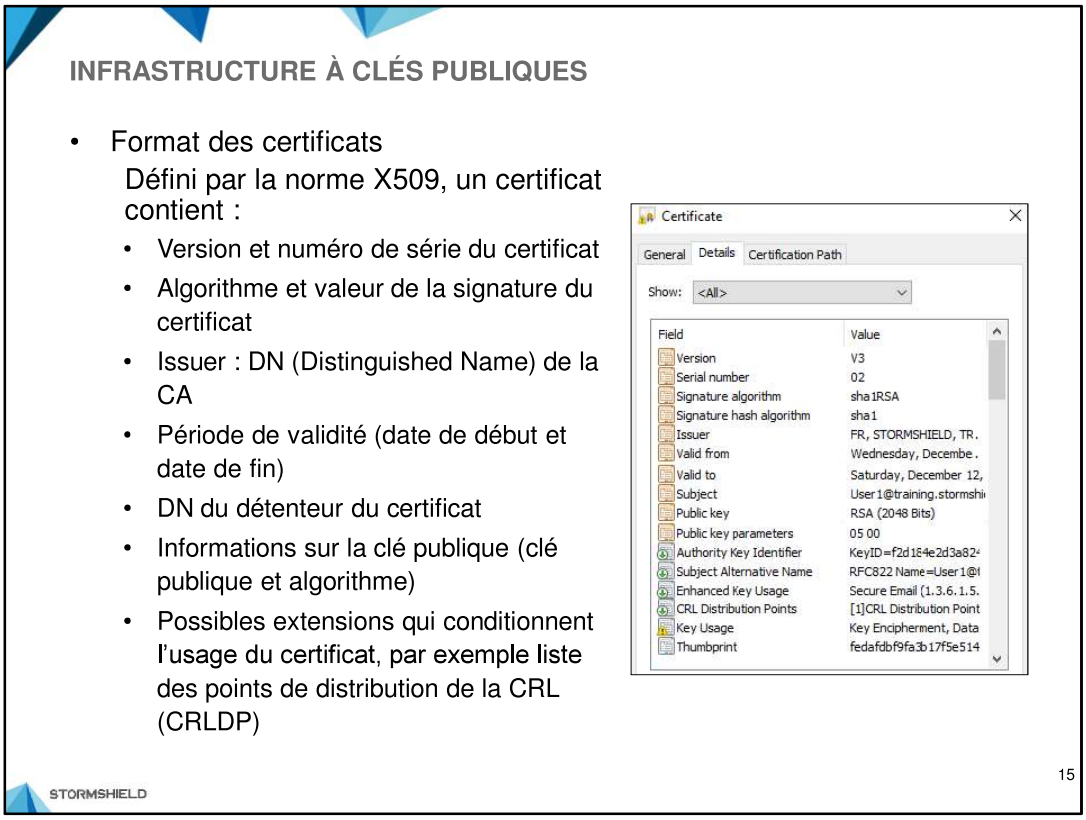
**3 –** La CA publie le certificat sur un annuaire, pour le rendre visible à tous..

## Création d'une identité numérique

**1 –** La **CA** crée pour l'utilisateur **Bob** une bi-clé asymétrique, composée d'une partie publique (clé publique) et d'une partie privée (clé privée), renseigne les informations relatives à **Bob**, puis génère et signe un certificat pour **Bob**,
**2 –** La **CA** génère un fichier contenant l'identité numérique de **Bob**, protège ce fichier par mot de passe puisqu'il contient la clé privée de **Bob**, et lui envoie (exemple de fichier .p12) ,
**3 –** La **CA** publie le certificat sur un annuaire, pour le rendre visible à tous.

La **CA** est également responsable de relayer, après vérification, les demandes de révocation.

**NOTE**
Une CSR contient un certificat auto-signé pour faciliter le travail de l'administrateur de la CA : vérification de l'intégrité de la demande, par conséquent vérification de la validité de la bi-clé du demandeur (clé publique + clé privée), la clé publique proposée dans la CSR permettant de vérifier que la signature numérique du demandeur (décrit sur la page précédente) est correcte




## Infrastructure à clés publiques

L'infrastructure qui héberge les informations publiques (annuaire, CRL) et qui permet d'accéder aux certificats de l'organisation, d'effectuer un renouvellement de certificat, ou de le révoquer est nommée PKI (Public Key Infrastructure).
Un certificat peut contenir du texte (extensions .pem, .crt) ou des données binaires directement (extensions .cer, .der).

La validité du certificat est remise en cause à l'expiration de ce dernier (limitation dans le temps), ou de l'expiration de la CA ; en cas de perte ou de vol de la clé privée du propriétaire, en cas de départ du propriétaire de la société.

## Liste des certificats révoqués

La CRL est un fichier signé par la CA, qui liste les numéros de série des certificats révoqués avant leur expiration. Cette liste doit être accessible publiquement pour permettre aux utilisateurs de s'assurer que les identités qui leur sont présentées sont encore valides.

## Stockage des identités numériques par la CA

Lorsque la CA génère les bi-clés, il est simple de contrôler la robustesse des clés et de les sauvegarder, mais cela nécessite la mise en place d'une procédure sécurisée pour délivrer son identité à un utilisateur final. Il existe pour cela un container protégé standardisé nommé PKCS#12 qui contient traditionnellement :
[clé privée du porteur + certificat du porteur (contenant sa clé publique) + certificat de la CA signataire].