Exercice 1 – Certificats et annuaires électroniques.

1) Quel est le problème principal résolu par une infrastructure à clé publique ?

   Solution : clé publique pour le chiffrement et clé privé (à ne pas diffuser) qui permet de déchiffrer. Plusieurs entités. …

2) Pourquoi les certificats numériques sont-ils publiés dans un annuaire ?

   Solution : Le propre d'un certificat est d'être une donnée publique accessible à des entités qui ne se connaissent pas. L'utilisation de l'annuaire permet donc cette diffusion.

3) Pourquoi les listes de révocations sont-elles publiées dans un annuaire ?

   Solution : Si le certificat est révoqué par une AC (quelqu'en soit la raison : perte ou vol de la clé privée, etc…), cette info doit être diffusée le plus largement possible pour que plus personne n'utilise la clé publique. C'est ce que permet la diffusion de la CRL.

Exercice 2 – Certificats X.509

1) Qu'est-ce qu'un certificat X.509 et quelles informations principales contient-il ?

   Solution : le certificat X.509 contient la clé publique, le nom et la date, le tout signé par une AC.

2) Discuter les scénarios suivants en termes de sécurité :
   a. Deux certificats différents sont signés par la même clé privée

      Solution : aucun problème, un AC signe de nombreux certificats.

   b. Deux certificats différents contiennent la même clé publique

      Solution : Bizarre, deux personnes ont la même clé, et peuvent donc lire les messages destinés à l'autre. Problème de sécurité.

   c. Deux certificats différents ont le même sujet

      Solution : une personne peut avoir des certificats différents pour des clefs publiques différentes d'usages différents.

   d. Deux certificats différents ont le même numéro de série

Solution : Problème de sécurité, un certificat pourrait être utilisé à la place d'un autre si l'émetteur est le même. Aucun problème s'il provient de deux émetteurs différents.

e. Deux certificats différents ont le même émetteur

Solution : Aucun problème, un AC signe de nombreux certificats.

f. Deux certificats différents ont la même signature

Solution : Collision de la fonction de hachage. Une des signatures a été faite par un pirate qui a trouvé une collision ? Il faut alors révoquer TOUS les certificats émis avec cette fonction de hachage.

Exercice 3 – Validation X.509

1) Un dépôt de certificats est accessible via LDAP pour obtenir des certificats X.509. Supposons qu'une entité Alice veuille contrôler la validité de la signature d'un document signé par une entité Bob. Alice dispose au départ de l'identifiant de Bob et de l'adresse du dépôt de certificats. Lister la suite des six opérations qu'Alice doit réaliser pour contrôler la signature de Bob.

Solution :
a) Récupérer le certificat de Bob par une requête LDAP au dépôt.
*b) Identifier l'AC signataire du certificat de Bob grâce au champ **IssuerName.***
c) Vérifier que le certificat de l'AC correspondante (ici une profondeur de 1 dans la chaîne de certification est supposées, il s'agit d'AC racine) est possédé et qu'il a été vérifié préalablement, ou alors récupéré par une requête LDAP au dépôt.
d) Extraire la clé publique contenue dans le certificat de l'AC racine et vérifier la signature du certificat de l'AC racine en la vérifiant avec la clé publique extraire et en hachant les données en clair contenues dans le certificat de l'AC racine.
e) Vérifier la signature du certificat de Bob à l'aide de la clé publique de l'AC racine et en hachant les données en clair contenues dans le certificat de Bob.
f) Vérifier la signature du document signé par Bob à l'aide de la clé publique de Bob et en hachant le contenu du document.

Exercice 4 – Le porte-clés d'un certificat PGP

Un certificat (ou clé) PGP comporte plusieurs clés. Cet ensemble de clés est donc parfois appelé porte-clés du certificat. De plus, comme toujours en cryptographie à clé publique, chaque clé est formée de deux parties : une publique et une privée. Le porte-clés comporte toujours au moins une clé maîtresse (ou clé primaire), les autres clés sont appelées sous-clés. De plus, toutes les clés sont classées en clés de signature et clés de chiffrement.

1) La clé maîtresse est-elle une clé de signature ou de chiffrement ?

Solution : La clé maîtresse est une clé de signature.

2) La validité d'un certificat PGP repose sur des signatures : lesquelles ?

Solution : La certification repose sur les clés de signature. D'une part, le certificat est toujours auto-signé par sa clé maîtresse. D'autre part, il peut être signé par toute autre entité possédant une clé PGP, et par n'importe quelle clé de signature de cette entité.

3) Que penser de la durée de vie de la clé maîtresse ?

Solution : Typiquement, une signature électronique a une durée de vie importante. Plus une clé durera longtemps, plus elle récoltera de signatures et plus elle aura un niveau de confiance élevé. Ces signatures seront perdues lors d'un éventuel renouvellement. Il est donc en général probable que la durée de vie de la clé maîtresse soit extrêmement longue. Il est tout de même important d'avoir une date de péremption juste si la clé est compromise ou si son usage n'est plus d'actualité, ou si le certificat de révocation est perdu, etc…

4) Il est toujours possible d'ajouter à un certificat PGP des sous-clés de chiffrement. Y a-t-il un intérêt à posséder plusieurs sous-clés de chiffrement ?

Solution : Il est nécessaire de ne pas utiliser la clé maîtresse pour autre chose que la signature des sous-clés, afin de limiter son exposition. Cependant, il est parfois intéressant d'avoir plusieurs sous-clés de chiffrement, bien que cela n'apporte aucun avantage du point de vue de la sécurité : par exemple, avoir une sous-clé pour chiffrer ses mails personnels et une sous-clé pour chiffrer ses mails professionnels. De même, d'ailleurs, pour les sous-clés de signature.

5) Que penser de la durée de vie d'une clé de chiffrement ?

Solution : Une sous-clé doit être renouvelée périodiquement puisque lorsqu'une clé de chiffrement est compromise, un attaquant peut et pourra toujours lire tous les messages ayant été chiffrés avec cette clé. La durée de renouvellement peut ici être relativement courte puisque pour s'assurer de sa validité, les destinataires pourront vérifier la signature de toute sous-clé de chiffrement par la clé maîtresse, plus pérenne.

6) Il est toujours possible d'ajouter à un certificat PGP des sous-clés de signature. Y a-t-il un intérêt à posséder une sous-clé signature ? Expliquer pourquoi ?

Solution : Il est possible de séparer les utilisations : la clé maîtresse uniquement pour gérer les sous-clés et pour amasser les signatures récoltées, et les sous-clés pour

chiffrer ou signer des messages. Il est ainsi possible de révoquer ou changer facilement les seules sous-clés exposées.

7) Toute sous-clé d'un certificat OpenPGP doit être certifiée par la clé maîtresse. Pourquoi ?

Pour prouver que les sous-clés appartiennent à la clé maîtresse et n'ont pas été insérées par un attaquant, elles sont signées par la clé maîtresse.

Exercice 5 – Révocation PGP

1. Comment retirer une clé des serveurs de clés ?

   Solution : quasiment impossible. L'ensemble des serveurs se synchronisant, il faudrait avoir une fonction atomique permettant de supprimer en une fois l'ensemble des copies de la clé concernée sur l'ensemble des serveurs avant qu'ils ne se synchronisent entre eux.

2. Pourquoi faut-il créer un certificat de révocation dès la création d'une clé ?

   Solution : Pour pouvoir l'utiliser lorsque l'on en aura besoin, sans pour autant devoir retrouver le mot de passe de la clé privée (voir si jamais celle-ci a été détruite, impossibilité de générer le certificat de révocation).

3. A qui faut-il transmettre un certificat de révocation si une clé est compromise ?

   Solution : La plupart des serveurs de clé n'acceptent pas directement les certificats de révocation. Il faut d'abord importer le certificat dans son porte-clés (pour ajouter la révocation à la clé à révoquer), puis ensuite envoyer la clé révoquée aux serveurs.

4. Une clé a été compromise le 1er avril 2015. « *Il n'est pas utile de publier un certificat de révocation puisqu'elle va expirer le 10 mai 2015* ». Que pensez de ce raisonnement ?

   Solution : il faut absolument publier ce certificat de révocation pour éviter l'utilisation abusive de la clé.

5. Une sous-clé de chiffrement expire plus tôt que n'expire une clé OpenPGP. Y a-t-il un intérêt à cela ?

   Solution : Oui, cela permet de la changer en cas de compromission sur les chiffrements.

6. Une sous-clé de chiffrement expire plus tard que n'expire une clé principale ? Y a-t-il un intérêt à cela ?

   Solution : Aucun intérêt, la sous-clé de chiffrement est signée numériquement par la clé principale : la sous-clé devient inutilisable si la clé principale a expiré.