Échanges sécurisés de données

Utilisation d'OpenSSL pour PHP

Sujet : développer en PHP, une Infrastructure à Clés Publiques (ICP) en utilisant OpenSSL

Aide : http://www.manuelphp.com/php/ref.openssl.php

En utilisant les fonctions PHP d'OpenSSL, il vous est demandé de développer un site Internet avec une interface suivant le cahier des charges défini dans les parties A, B, C, D, E.
L'ensemble de votre code doit être transmis sous forme d'un fichier .ZIP à lionel.clot@cstb.fr

Une attention particulière sera portée sur l'interface et sur la qualité du code : commentaires, nommage des variables, des fonctions, etc…

Pour réaliser ce TP, vous devrez utiliser un serveur Apache local tel que xampp, EasyPHP ou wamp
Attention, lors des appels aux fonctions d'openssl, il est très souvent nécessaire de passer un talbeau de paramètres nommé (configargs dans la doc). Ce tabeau doit au moins contenir le chemin vers le fichier openssl.cnf. Par exemple :

```
$config = array(
        "config" => "C:\\xampp\\php\\extras\\openssl\\openssl.cnf"
);
```

A. Générer un certificat racine d'une autorité de certification

- Générer une clé privée
- Générer une requête à partir de la clé privée et en utilisant les données suivantes :

```
$dn = array(
   "countryName" => "FR",
   "stateOrProvinceName" => "Sophia",
   "localityName" => "Valbonne",
   "organizationName" => "iut",
   "organizationalUnitName" => "iut_iotia",
   "commonName" => "b",
   "emailAddress" => "iut@univ.fr"
);
```

- A partir de la clé privée et de la requête, générer certificat racine autosigné valide pour une durée de 3 ans.
- Exporter de la clé privée dans un fichier téléchargeable.
- Exporter de la requête dans un fichier téléchargeable.
- Exporter du certificat racine dans un fichier téléchargeable.

B. Générer un certificat personnel à partir du certificat racine

Complétez le code précédent en ajoutant la génération d'un certificat

- Génération d'une clé privée
- Génération d'une requête à partir de la clé privée en saisissant au travers d'un formulaire les informations suivantes :
    - Nom et Prénom (commonName)
    - E-mail (emailAddress)
    - Ville (localityName)
    - Département (stateOrProvinceName)
    - Pays (countryName)
    - Organisation (organizationName), par exemple : IUT
    - Nom de l'unité (organizationalUnitName), par exemple : IOTIA
- A partir de cette requête, du certificat racine et de la clé privée racine, générer le certificat personnel valide pour une durée de 1 an.
- Exporter la clé privée dans un fichier téléchargeable.
- Exporter la requête dans un fichier téléchargeable.
- Exporter le certificat dans un fichier téléchargeable.

C. Chiffrement/déchiffrement d'un texte :

- Récupération de la clé publique à partir du certificat généré dans la partie B.
- Chiffrer un texte (saisi dans un formulaire) en utilisant cette clé publique.
- Déchiffrer le texte chiffré en utilisant votre clé privée (afficher à l'écran le texte déchiffré).

D. Signature d'un document

- Téléchargement (*upload*) d'un document.
- Signature de ce document.
- Exportation de la signature dans un document téléchargeable (*download*).

E. Vérification de la signature d'un document

- Téléchargement (*upload*) de la signature et du document correspondant.
- Vérification de la signature. Affichage du résultat à l'écran.