1 Généralité

- Qu'elle est l'architecture générale d'une application eID en ligne ?

  Client / PC-SC / Reverse Proxy / Serveur applicatif

  TODO figure architecture JPG
- A quel niveau se fait/font la/les vérification(s) de certificats ?
  TODO discussion sur la sécurité au niveau général

2 Reverse-Proxy

- Pourquoi ai-je besoin de recompiler apache ?

  Parce que apache va mettre des en-têtes en plus et vérifier la validité OCSP

- Comment recompiler apache ?

  TODO CFR RAPPORT
- Comment configurer apache en HTTPS ? Doit-on passer par la configuration d'un virtualHost ?

  FICHIER CONFIG - discussion UVCW
- Qu'est ce que OCSP ? Comment l'activer et l'utiliser ?

  OCSP signifie "Online Certificate Status Protocol". Ce protocole va vérifier la validité des certificats. Pour l'activer, il faut ajouter la ligne "SSLUseOCSP on" dans le fichier de configuration (httpd.conf) de Apache.

  TODO ligne en cas de refus
- Comment creer un certificat pour le site ? Pourquoi tant d'étapes lors de la création de certificats ? Que fait chacune ?

  CFR RAPPORT

3 Applicatif serveur

- Comment récupérer les entêtes eID en PHP ?

  ```
  $entetes = getallheaders();
  $entete1 = $entetes["SSL_CLIENT_S_DN"];
  $entete2 = $entetes["SSL_CLIENT_M_SERIAL"];
  $entete3 = $entetes["SSL_CLIENT_CERT"];
  $entete4 = $entetes["SSL_CLIENT_VERIFY"];
  ```

Il ne reste ensuite qu'à les traiter correctement en php.
Note : l'en-tête « SSL_CLIENT_CERT » indique le résultat de l'authentification du client sur le serveur apache. Elle peut donc être utilisée comme un premier moyen de sécurité pour tester si le client passe bien par le reverse-proxy et vérifier que le statut de son authentification est bien « SUCCESS ».

– Comment résoudre les problèmes d'accent ?

pending, UTF8
Exemple de problème : la chaîne «
`J\xC3\xA9r\xC3\xB4me`
» devrait s'afficher « Jérôme », elle reste pourtant elle-même, malgré un décodage utf8.

Possibilité de résolution :
Voici une fonction en php, qui convertit les représentations des caractères spéciaux posant problème en leur représentation utf8, pour un affichage correct :

```
/*Cette fonction prend une chaine "en-tête" envoyée par le reverse proxy,
et la retourne, convertie pour un affichage correct en php.
Argument : la chaîne "en-tête"
Retourne : la chaîne convertie
*/
function adapt_utf8($chaine){
$ascii = array(
"\\xC3\\x80","\\xC3\\x81","\\xC3\\x82","\\xC3\\x83","\\xC3\\x84","\\xC3\\x85",
"\\xC3\\x86","\\xC3\\x87","\\xC3\\x88","\\xC3\\x89","\\xC3\\x8A","\\xC3\\x8B",
"\\xC3\\x8C","\\xC3\\x8D","\\xC3\\x8E","\\xC3\\x8F","\\xC3\\x90","\\xC3\\x91",
"\\xC3\\x92","\\xC3\\x93","\\xC3\\x94","\\xC3\\x95","\\xC3\\x96","\\xC3\\x97",
"\\xC3\\x98","\\xC3\\x99","\\xC3\\x9A","\\xC3\\x9B","\\xC3\\x9C","\\xC3\\x9D",
"\\xC3\\x9E","\\xC3\\x9F","\\xC3\\xA0","\\xC3\\xA1","\\xC3\\xA2","\\xC3\\xA3",
"\\xC3\\xA4","\\xC3\\xA5","\\xC3\\xA6","\\xC3\\xA7","\\xC3\\xA8","\\xC3\\xA9",
"\\xC3\\xAA","\\xC3\\xAB","\\xC3\\xAC","\\xC3\\xAD","\\xC3\\xAE","\\xC3\\xAF",
"\\xC3\\xB0","\\xC3\\xB1","\\xC3\\xB2","\\xC3\\xB3","\\xC3\\xB4","\\xC3\\xB5",
"\\xC3\\xB6","\\xC3\\xB7","\\xC3\\xB8","\\xC3\\xB9","\\xC3\\xBA","\\xC3\\xBB",
"\\xC3\\xBC","\\xC3\\xBD","\\xC3\\xBE","\\xC3\\xBF");

$trad_ascii = array(
"\xC3\x80","\xC3\x81","\xC3\x82","\xC3\x83","\xC3\x84","\xC3\x85","\xC3\x86",
"\xC3\x87","\xC3\x88","\xC3\x89","\xC3\x8A","\xC3\x8B","\xC3\x8C","\xC3\x8D",
"\xC3\x8E","\xC3\x8F","\xC3\x90","\xC3\x91","\xC3\x92","\xC3\x93","\xC3\x94",
"\xC3\x95","\xC3\x96","\xC3\x97","\xC3\x98","\xC3\x99","\xC3\x9A","\xC3\x9B",
"\xC3\x9C","\xC3\x9D","\xC3\x9E","\xC3\x9F","\xC3\xA0","\xC3\xA1","\xC3\xA2",
```

```
"\xC3\xA3","\xC3\xA4","\xC3\xA5","\xC3\xA6","\xC3\xA7","\xC3\xA8","\xC3\xA9",
"\xC3\xAA","\xC3\xAB","\xC3\xAC","\xC3\xAD","\xC3\xAE","\xC3\xAF","\xC3\xB0",
"\xC3\xB1","\xC3\xB2","\xC3\xB3","\xC3\xB4","\xC3\xB5","\xC3\xB6","\xC3\xB7",
"\xC3\xB8","\xC3\xB9","\xC3\xBA","\xC3\xBB","\xC3\xBC","\xC3\xBD","\xC3\xBE",
"\xC3\xBF");

$chaine_retour = utf8_decode(str_replace($ascii,$trad_ascii,$chaine));
return $chaine_retour;
}
```

4 Applicatif client

– Comment lire les données sur la carte via une applet ?

L'applet doit, avant de commencer toute opération avec la carte, charger la librairie eidlib. Il faut ensuite initialiser la liaison avec le lecteur de cartes. Les données peuvent ensuite être récupérées dans 2 objets :

- le premier pour les données d'identité (objet de type BEID_ID_data)
- le second pour les données d'adresse (objet de type BEID_Address)

Les données se récupèrent ensuite via les méthodes définies pour ces objets (voir documents eID Belgium).

Exemple avec code :

1. Phase d'initialisation de l'applet :

```
idData = null;
addrData = null;

//chargement de la librairie eidlib
java.lang.System.loadLibrary("eidlibj");

//initialisation avec le lecteur de cartes
BEID_Long CardHandle = new BEID_Long();
BEID_Status oStatus = eidlib.BEID_Init("", 0, 0, CardHandle);
```

2. Démarrage de l'applet

```
//l'objet idData contiendra les données d'identité
idData = new BEID_ID_Data();
BEID_Certif_Check CertCheck = new BEID_Certif_Check();

//Obtention des données d'identité sur la carte
BEID_Status oStatus = eidlib.BEID_GetID(idData, CertCheck);

//l'objet addrData contiendra les données de l'adresse
```

```
addrData = new BEID_Address();
BEID_Certif_Check CertCheck = new BEID_Certif_Check();

//Obtention des données de l'adresse sur la carte
BEID_Status oStatus = eidlib.BEID_GetAddress(addrData, CertCheck);
```

3. Récupération de données d'identité ou d'adresse

Il suffit maintenant de récupérer les données souhaitées via les méthodes prévues (voir API) à ces objets, exemples :

```
//Récupération du nom de famille dans l'objet idData via la méthode getName()
String nom = idData.getName() ;

//Récupération de la rue dans l'objet addrData via la méthode getStreet()
String rue = addrData.getStreet() ;
```

– Puis-je récupérer la photo ? Comment ?

Oui, le principe est identique à la récupération des données d'identité ou d'adresse, mais on passe ici via un objet BEID_Bytes pour récupérer la photo et pouvoir la traiter ensuite comme un fichier ou dans un objet Image.
Exemple avec code :

```
//objet de type BEID_Bytes qui contiendra la photo
BEID_Bytes Picture = new BEID_Bytes();
BEID_Certif_Check CertCheck = new BEID_Certif_Check();
BEID_Status oStatus = new BEID_Status();

//Obtention des données de la photo sur la carte
oStatus = eidlib.BEID_GetPicture(Picture,CertCheck);

//création d'un fichier « photo.jpg » à partir des données de la photo récupérée.
FileOutputStream oFile = new FileOutputStream("photo.jpg");
oFile.write(Picture.getData());
oFile.close();
```

– Pourquoi dois-je signer mon applet ?

Accès à une ressource en dehors de la VM

– Comment lire sur la carte en javascript ?

Il faut tout d'abord charger une applet possédant les méthodes nécessaires à la lecture sur la carte eID (l'archive eidlib.jar du middelware possède déjà un applet de ce type : be.belgium.eid.BEID_Applet.class).
Une fois un nom attribué à l'applet (paramètre name dans la balise ap-

plet), les récupérations des données s'effectuent comme dans un applet Java, mais dans des balises Javascript.
Note : les méthodes définies pour l'applet du middleware sont disponibles dans le document eID Belgium.
Exemple avec code :

```
//balise applet à appeler dans votre page web
<applet
    codebase = "emplacement_de_votre_archive_eidlig.jar"
    archive  = "eidlib.jar"
    code     = "be.belgium.eid.BEID_Applet.class"
    name     = "BEIDtest"
    width   = "0"
    height   = "0"
    hspace   = "0"
    vspace   = "0"
    align   = "middle">
    <param name="Reader" value="">
    <param name="OCSP" value="0">
    <param name="CRL" value="0">
</applet>
```

Il ne reste ensuite qu'à utiliser les méthodes adéquates (voir API) dans des balises Javascript.
Exemple avec code :

```
<script language="javascript">
    function GetData()
    {
        /*récupération du nom sur la carte grâce à la méthode
        getName() et copie du résultat dans un champ
        de formulaire de la page appelé « name »*/

        document.getElementById('name').value = document.BEIDcetic.getName();

        /*récupération du premier prénom sur la carte grâce
        à la méthode getFirstName1() et     copie du résultat
        dans un champ de formulaire de la page appelé « firstName »*/
        document.getElementById('firstName').value = document.BEIDcetic.getFirstName1
    }
</script>
```

– Comment traiter les erreurs liées à la carte ? Existe-t-il une documentation des codes d'erreurs et leur signification ?

PAS trouvé ex. "-12227" si carte pas dans le lecteur

– J'ai le problème « cannot initialise, library already loaded »

Il faut malheureusement redémarrer le navigateur.

Pas d'autre solution connue pour le moment.

- Où dois-je héberger mon applet ?

  question de la sécurité
- Comment gérer une connexion d'une applet vers un serveur d'application ?

  Une solution est de gérer cela via des sockets et l'envoi de messages entre l'applet et un serveur.
  Le serveur principal crée une instance d'un serveur particulier pour chaque client connecté. L'applet chargée sur le poste de l'utilisateur est l'applet Client.

- Lorsque l'applet Java utilise un objet certcheck (vérification de certificat), comportement différent selon le browser :
  - Firefox : fenêtre vide de demande d'authentification supplémentaire - IE : fenêtre de demande d'authentification supplémentaire contenant les certificats présents dans le navigateur

5 Tests

- Où puis-je trouver un kit de test ?

  www.eid-shop.be

- Carte de test, comment se présente-t-elle ?

- Autre truc de test :

  Appletviewer local ne nécessite pas de signer l'applet pour le test

6 Divers

- Où puis-je trouver d'autres références ?

  TODO liste des références