



Sécurité des usages du WEB

Pierre DUSART

Damien SAUVERON

Résumé

- Contenu :

Nous nous intéresserons à expliquer les solutions pertinentes pour établir la confiance en un site WEB en termes de sécurité, notamment par l'usage de certificats numériques.

Par quelques exemples explicatifs, nous nous efforcerons de montrer qu'il est très facile de mettre en place ces solutions.

On s'intéressera aux futurs modèles WEB qui s'intégreront directement dans un environnement hardware sécurisé.



Problématique (context of problem)

- Pour le site : Accès protégé aux données d'un site
 - ⊙ Accès limité aux données sensibles après identification
 - ⊙ Propriété intellectuelle
 - ⊙ Intelligence économique
 - Pour l'utilisateur : Confiance de l'internaute sur le site
 - ⊙ Transfert de données sécurisée (entre sa machine de travail et celle de son domicile)
 - ⊙ Problème d'Usurpation identité (Actions faites sans son consentement : vente d'actions spéculatives par exemple)
 - ⊙ Site marchand : risque de piratage du moyen paiement ou non envoi marchandises
- 

Accès par mot de passe

● Exemple :

<http://www.commentcamarche.net/forum/affich-1790690-mot-de-passe-sur-une-page-web>

● Fichier html :

```
<form name="form1" method="POST"
action="verif.php">
<input type="password" name="mdp">
</form>
```

● Fichier verif.php :

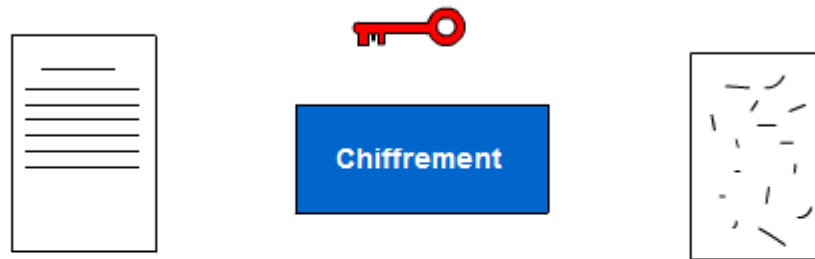
```
<?php if($_POST['mdp'] == "ton mot de passe")
{ include('ta page d'index de photo.htm ou
.html'); } ?>
```



Aller plus loin...

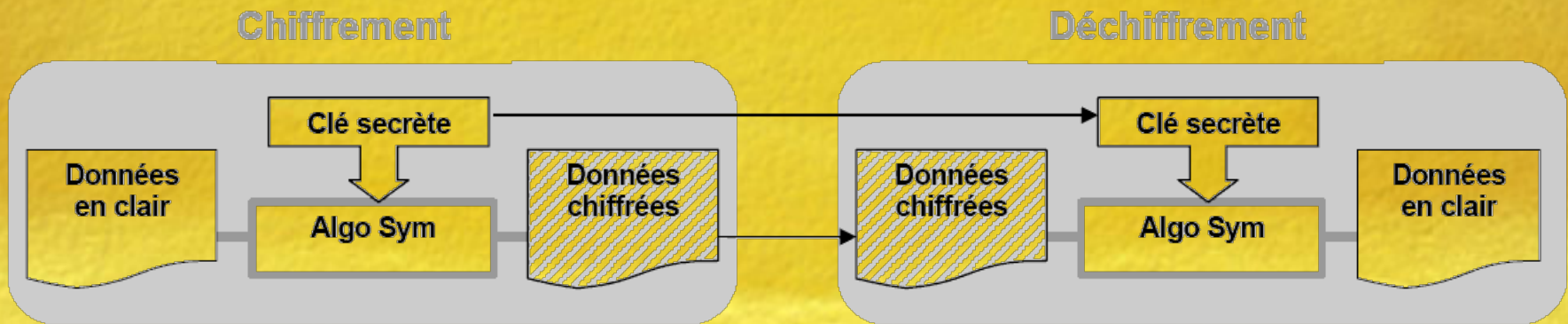
avec la Cryptographie (art des
messages secrets ou science de
la confiance)

Le chiffrement des données



Source : <http://www.formation.ssi.gouv.fr/autoformation/signature.html>

Cryptographie symétrique



Source : www.urec.cnrs.fr/IMG/pdf/GERET-060124-Les_algorithmes_cryptographiques.pdf

- Symétrique = **même clef secrète** de chaque côté
- C'est bien (rapide, sûr) mais il faut se rencontrer pour se donner la clef (ou échange sécurisé de la clef)

Une seule clef



Source : <http://www.formation.ssi.gouv.fr/autoformation/signature.html>

Déchiffrement par clef

```
<!-- DEBUT DU SCRIPT MAILTO ANTI SPAM-->
<!-- Script provenant de http://www.toulouse-rennaissance.net/c_outils/
-->
<script type="text/javascript">
<!--
    var a, s, n;
    function Crypt(s) {
        r='';for(i=0;i<s.length;i++)
            {n=s.charCodeAt(i);
             if (n>=8364) {n = 128;}
              r += String.fromCharCode( n - 3 ); }
    return r;}
    a ="pdlowr=";
    m='&#64;';d=unescape(m);
    var nom = "protection";
    var domaine = "votre_site.com";
    var aro = nom + d + domaine;
    document.write('<a href='+Crypt(a) + aro + '>');
    document.write(arro + '</a>');
    // -->
</script>
<!-- FIN DU SCRIPT MAILTO ANTI SPAM-->
```

Explication : chiffrement de César

- Pour chiffrer, chaque lettre est remplacée par celle trois rangs plus loin dans l'alphabet :

A devient D, B devient E, ...

- Pour déchiffrer, le décalage est effectué dans l'ordre inverse :

"**pdlowr**="

devient

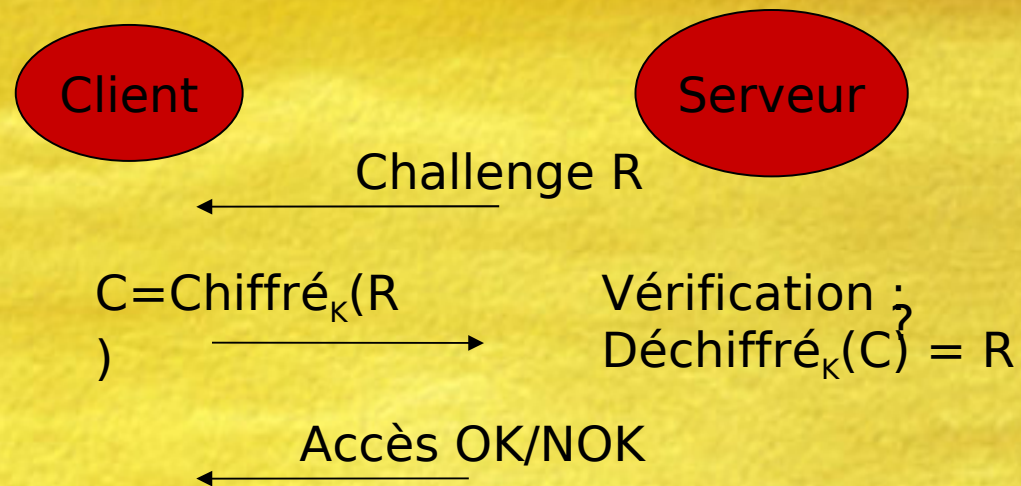
"**mailto:**"

- On se protège ainsi des robots de spam

Montrer que l'on connaît la clef ou dérivation d'une clef maître

- Pour vérifier qu'une personne appartient bien à un groupe (une clef secrète en commun)

- Envoi Nombre aléatoire (Challenge)
- Renvoi d'une réponse = Challenge Chiffré
- Test si Challenge envoyé = Déchiffrement(réponse)



Attaque : Phishing

From: PayPal Security Department [service@paypal.com]
Subject: [SPAM:99%] Your PayPal Account

PayPal *The way to send and receive money online*

Security Center Advisory!

We recently noticed one or more attempts to log in to your PayPal account from a foreign IP address and we have reasons to believe that your account was hijacked by a third party without your authorization. If you recently accessed your account while traveling, the unusual log in attempts may have been initiated by you.

If you are the rightful holder of the account you must **click the link below** and then complete all steps from the following page as we try to verify your identity.

[Click here to verify your account](#)

http://211.248.156.177/.PayPal/cgi-bin/websecrmd_login.php

If you choose to ignore our request, you leave us no choice but to temporarily suspend your account.

Thank you for using PayPal!

Please do not reply to this e-mail. Mail sent to this address cannot be answered. For assistance, [log in](#) to your PayPal account and choose the "Help" link in the footer of any page.

To receive email notifications in plain text instead of HTML, update your preferences [here](#).

PayPal Email ID PP697

Protect Your Account Info

Make sure you never provide your password to fraudulent persons.

PayPal automatically encrypts your confidential information using the Secure Sockets Layer protocol (SSL) with an encryption key length of 128-bits (the highest level commercially available).

PayPal will never ask you to enter your password in an email.

For more information on protecting yourself from fraud, please review our Security Tips at <http://www.paypal.com/securitytips>

Protect Your Password

You should never give your PayPal password to anyone, including PayPal employees.

- L'attaquant crée un site qui est identique au vrai site.
- Il vous invite à rentrer identité (login)/mot de passe en invoquant différents subterfuges (compte désactivé, vérification de paramètres,...)
- Le faux site recueille ainsi tous les renseignements personnels ou secrets.



Comment contrer cette attaque?

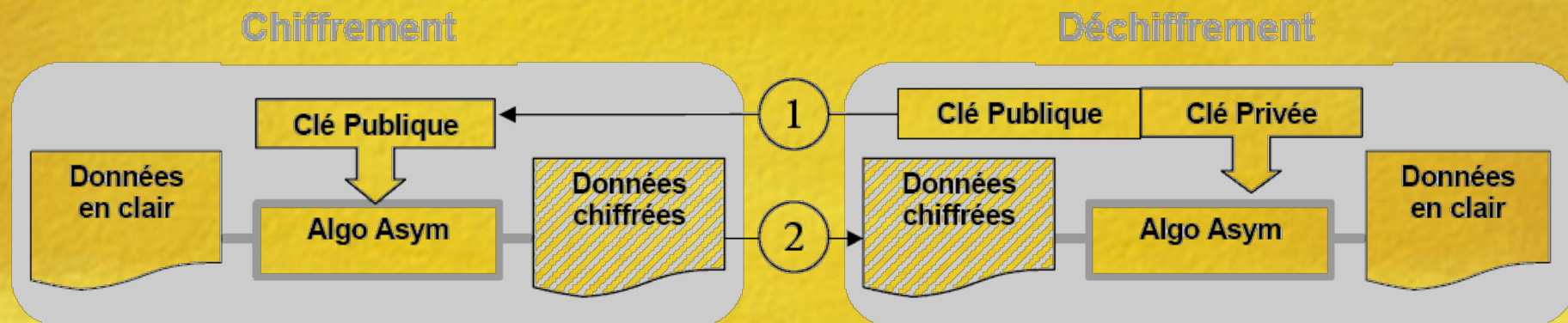
- Le site n'est pas en fait pas le bon:
 - ⊙ L'internaute identifie le site à son aspect et non à son adresse réelle. Les pirates utilisent des adresses de sites contenant une faute de frappe, ou bien des sous-domaines.
 - ⊙ Dans la panique, les réflexes de contrôles de l'internaute sont altérés (par exemple si on lui annonce que son compte bancaire a été vidé...)
 - ⊙ Dans certains cas, l'adresse du site est piratée (Pharming)
 - Il « suffit » d'un moyen pour pouvoir identifier le site rapidement.
 - Si l'on a été piraté, le seul moyen est de changer très rapidement sa clef.
- 



Problème Crypto symétrique

- Le problème de la cryptographie à clef secrète est la gestion des clefs :
 - ⊙ Comment changer sa clef (pas facile lorsque c'est la clef d'un groupe)
 - ⊙ Comment s'échanger la clef sans se rencontrer?
 - ⊙ Comment écarter une personne du groupe?
 - ⊙ Lui enlever la clef? Impossible
 - ⊙ Changer la clef de tous les autres? Contraignant.
 - Résolu avec la cryptographie à clef publique
- 

Cryptographie à clef publique



Source : www.urec.cnrs.fr/IMG/pdf/GERET-060124-Les_algorithmes_cryptographiques.pdf

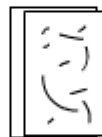
- Il y a une clé publique qui sert à chiffrer et une clé privée (secrète) qui sert à déchiffrer.
- Chaque personne dispose d'une paire de clefs (publique/privée)
- Les clefs publiques sont diffusées (page WEB, annuaires, ...)

Deux clefs : une pour chiffrer, l'autre pour déchiffrer

La **clé jaune** sera diffusée



Chiffrement



Déchiffrement

La **clé rouge** restera secrète!

Source : <http://www.formation.ssi.gouv.fr/autoformation/signature.html>



Création de clefs

- Chaque personne peut créer son propre couple de clefs (publique/privée)
 - Chaque clé a une unique clé inverse correspondante.
 - Une des deux clefs est choisie comme étant publique : elle est peut être diffusée partout, mis dans un annuaire, une page WEB, ...
- 



Deux usages de la cryptographie à clef publique

- L'ordre de présentation des clefs a une grande importance!
 - Chiffrement : même usage que la cryptographie à clef secrète
 - ⊙ On chiffre avec la clef publique de la personne.
 - ⊙ Elle pourra déchiffrer avec sa clef privée.
 - Signature : la personne montre qu'elle dispose de la clef privée sans la dévoiler :
 - ⊙ Elle chiffre le message ou une partie du message avec sa clé privée (on dit qu'elle signe le message)
 - ⊙ Tout le monde peut déchiffrer le message en utilisant la clé publique (tout le monde peut vérifier la signature)
- 



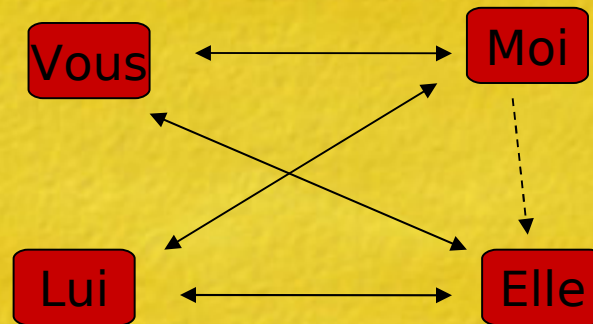
Signature

- On prouve que l'on connaît sa propre clé privée en chiffrant un message avec cette clef.
- Seul problème : pas de relation directe avec l'identité de la personne!

**Cette clé publique est-elle
authentique?**



Modèle « Toile de Confiance »



- Transmission de la confiance : je certifie que c'est bien « Untel » qui dispose de cette clef privée.
- Il existe une chaîne de confiance : « Elle » est identifiée par « Moi » grâce à « Vous »
- Modèle gratuit mais limité à un groupe réduit de personnes et dont la fiabilité est réduite si une personne (nœud) est malveillant.

Modèle « Infrastructure »



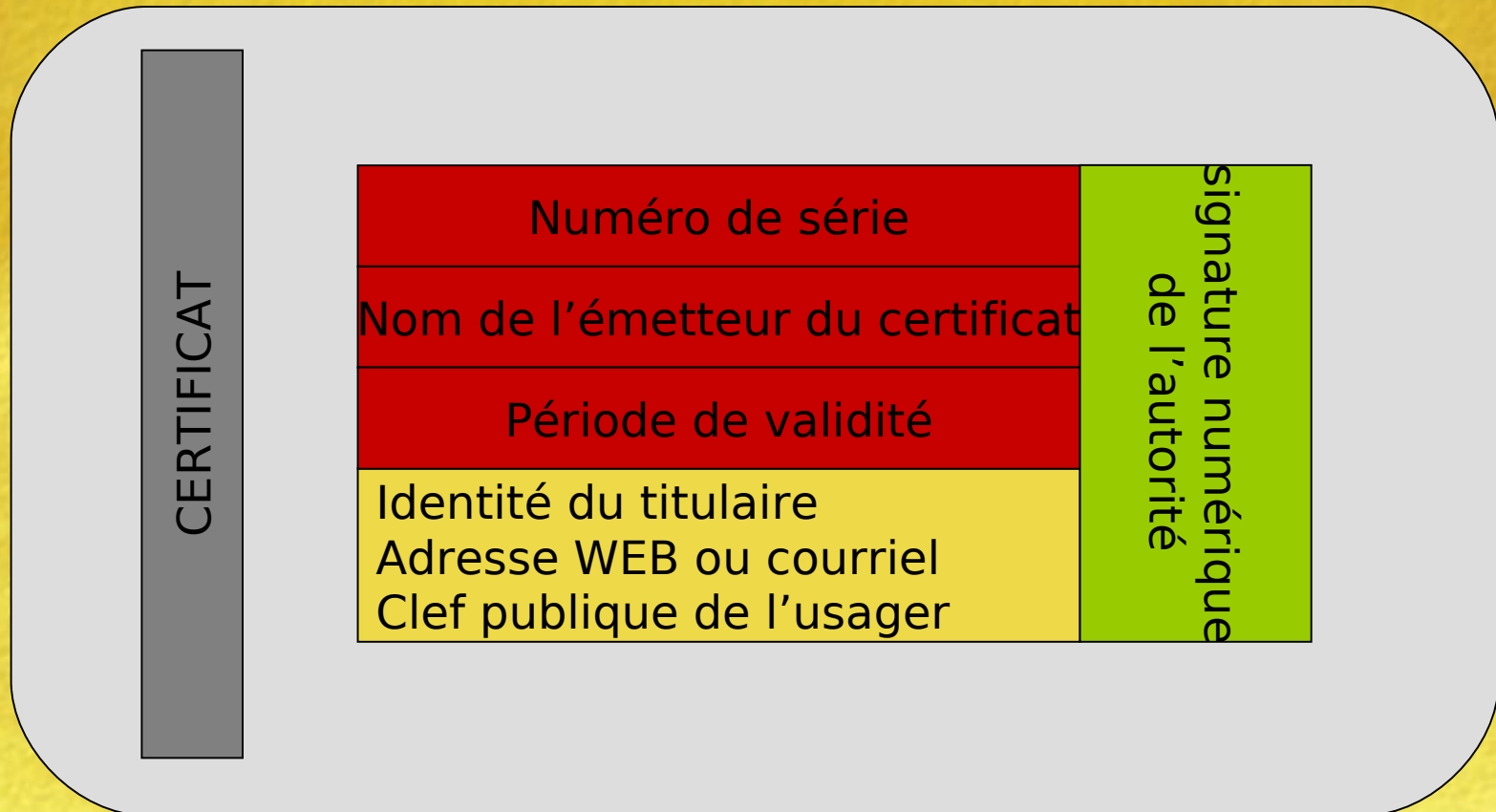
- Modèle du Tiers de confiance : La relation clef-identité est validée par une autorité.
- Chaîne de confiance : « Elle » est identifiée par AC et peut être vérifiée par « Moi ».
- Modèle payant à base de petits éléments de confiance (certificats)



Certificat

- Un **certificat électronique** est une carte d'identité numérique dont l'objet est d'identifier une entité (physique ou non-physique).
 - Le certificat numérique ou électronique est un lien entre l'entité physique et l'entité numérique (virtuelle). L'autorité de certification sert de personne (tiers) de confiance et atteste du lien entre l'identité physique et l'entité numérique.
 - Les standards le plus utilisés pour la création des certificats numériques sont X.509 ou OpenPGP.
- 

Contenu d'un certificat



Authentification par Certificat

- **HTTPS avec SSL sont souvent utilisés en mode « dissymétrique », où uniquement le serveur possède un certificat**, le client n'en possédant pas. Ce certificat du serveur permet de chiffrer (avec une clé de session) toutes les données transmises dans les deux sens et d'authentifier le serveur.
- Pour authentifier le client, le serveur demandera classiquement un mot de passe ou un numéro de carte bancaire ou ... au client.
- **L'avantage est que ces données d'authentification ne circuleront pas en clair sur le réseau**, tous les échanges étant chiffrés. C'est ainsi que fonctionne un **serveur Web sécurisé**, celui de votre banque peut-être.
- Généralement, lorsqu'un client avec son navigateur se connecte sur un serveur Web sécurisé, ce dernier lui envoie son certificat (pour fournir sa clé publique ...). Si ce certificat a été délivré par une autorité de certification reconnue par le navigateur du client, il est accepté de manière transparente pour l'utilisateur; sinon le navigateur demande à l'utilisateur s'il accepte ce type de certificat.

Authentification par certificat

The screenshot shows the eBay login page in Internet Explorer. The address bar displays a URL with a certificate icon and the text "eBay Inc. [US]". The page title is "eBay (https) : Protocole sécurisé par certificat". The main content area is divided into two sections: "Vous n'êtes pas encore membre ? Inscrivez-vous ici" and "Accéder à Mon eBay". The first section includes a "Je suis un visiteur" button and a list of benefits for members. The second section includes login fields for "Pseudo" and "Mot de passe", a checkbox for "Maintenir ma session ouverte", and an "Ouvrir une session" button. Annotations with arrows point to the certificate icon, the page title, the "Je suis un visiteur" button, and the "Site reconnu" text.

Ouvrir une session - Windows Internet Explorer

https://signin.ebay.fr/ws/eBayISAPI.dll?SignIn&UsingSSL=1&pUserId=&co_partnerId=2&siteid=71&ru=http%3A%2F... eBay Inc. [US] ebay

Fichier Edition Affichage Favoris Outils ?

Comment expliquer le... Ouvrir une session x

eBay (https) : Protocole sécurisé par certificat

Bienvenue sur eBay

Vous n'êtes pas encore membre ? Inscrivez-vous ici

Surveillez l'évolution de vos Affaires à suivre et de vos enchères en tant que visiteur.

Je suis un visiteur

Inscrivez-vous sur eBay pour pouvoir bénéficier des différents avantages réservés aux membres :

- **Surveillez** l'évolution de vos Affaires à suivre ou des objets sur lesquels vous enchérissez
- **Achetez** en toute sérénité grâce au programme de Protection des Achats PayPal
- **Rejoignez** la Communauté eBay et bien plus encore !

S'inscrire

Accéder à Mon eBay

Bienvenue. Ouvrez une session maintenant pour acheter, enchérir et vendre ou pour gérer votre compte.

Pseudo

[J'ai oublié mon pseudo](#)

Mot de passe

[J'ai oublié mon mot de passe](#)

☐ **Maintenir ma session ouverte pour toute la journée.** Ne cochez pas cette case si vous utilisez un ordinateur public ou partagé.

Ouvrir une session

Cadenas

Site reconnu

Vous avez des difficultés à ouvrir une session ? [Demandez de l'aide.](#)

Terminé

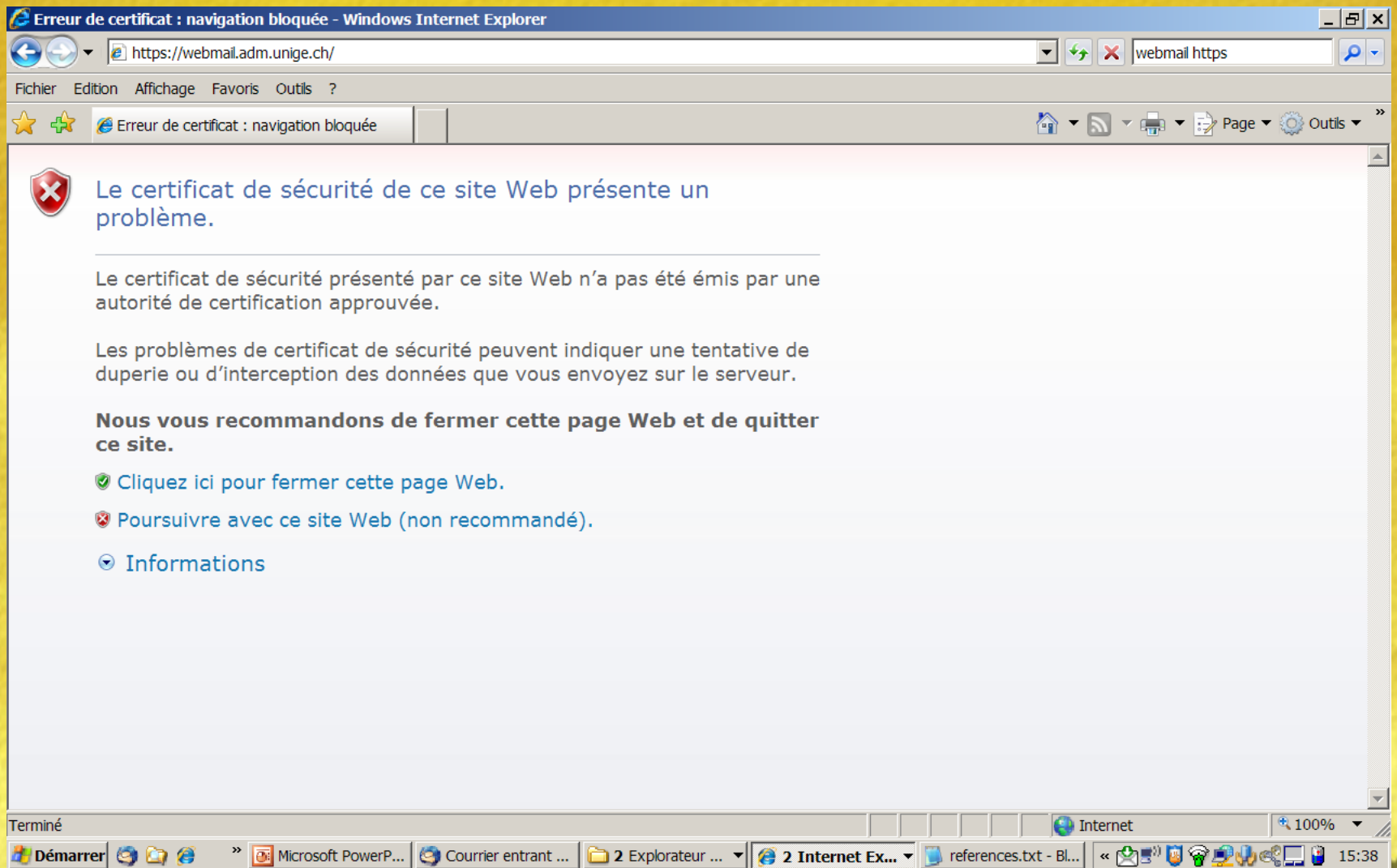
Démarrer Envoyés pour pier... signature Microsoft PowerPo... Ouvrir une sessi... ebay.JPG - Paint 10:37

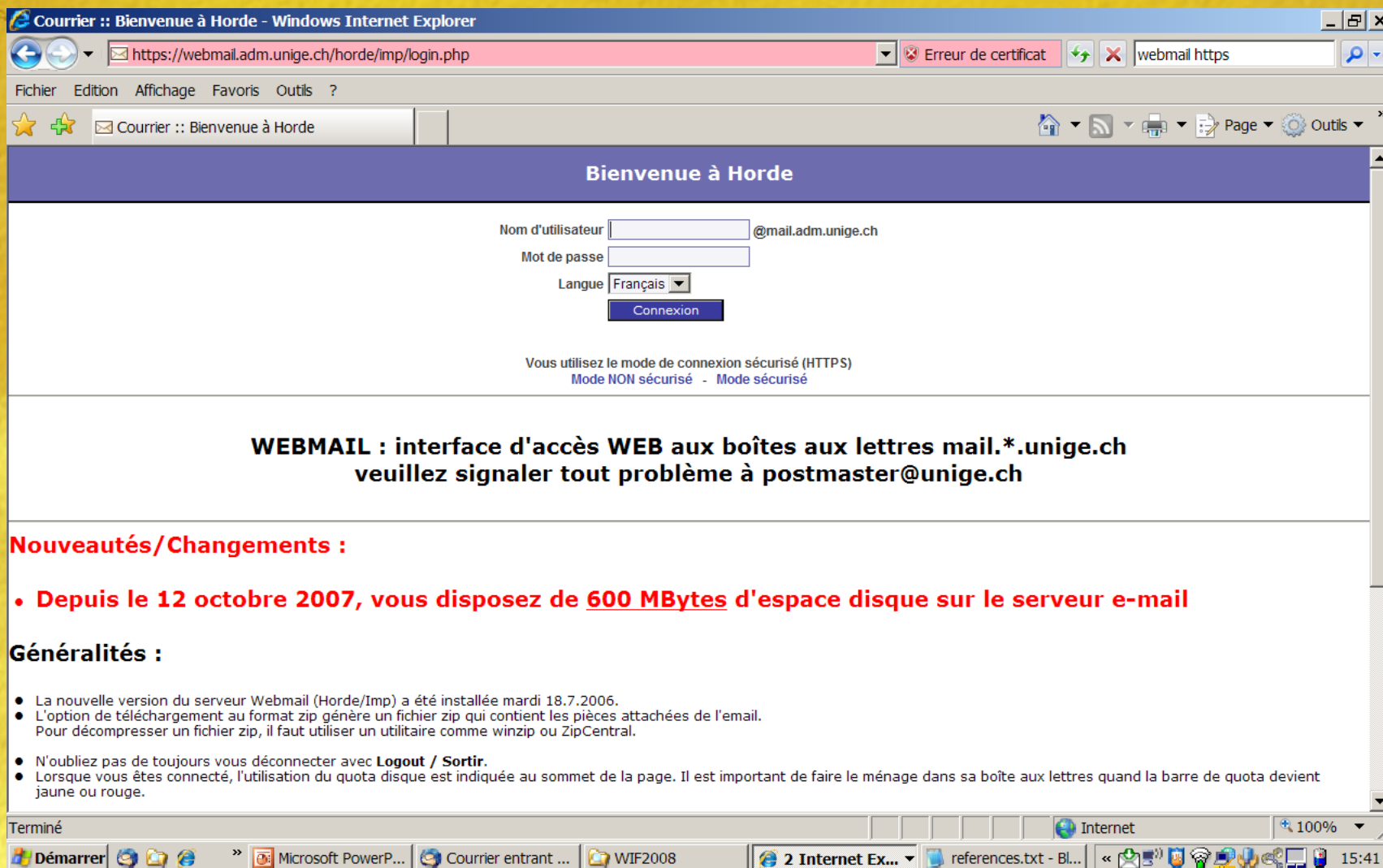


Indicateur visuel sur les navigateurs

- Un indicateur visuel "est **vert** quand vous êtes sur un site certifié : vous pouvez alors saisir vos informations personnelles en toute tranquillité.
 - Si cet indicateur est au **rouge**, alors cela signifie que vous êtes sur un **site potentiellement frauduleux**, c'est-à-dire se faisant passer pour un site : ne donnez alors aucune information sans avoir bien tout vérifié.
- 

Exemple

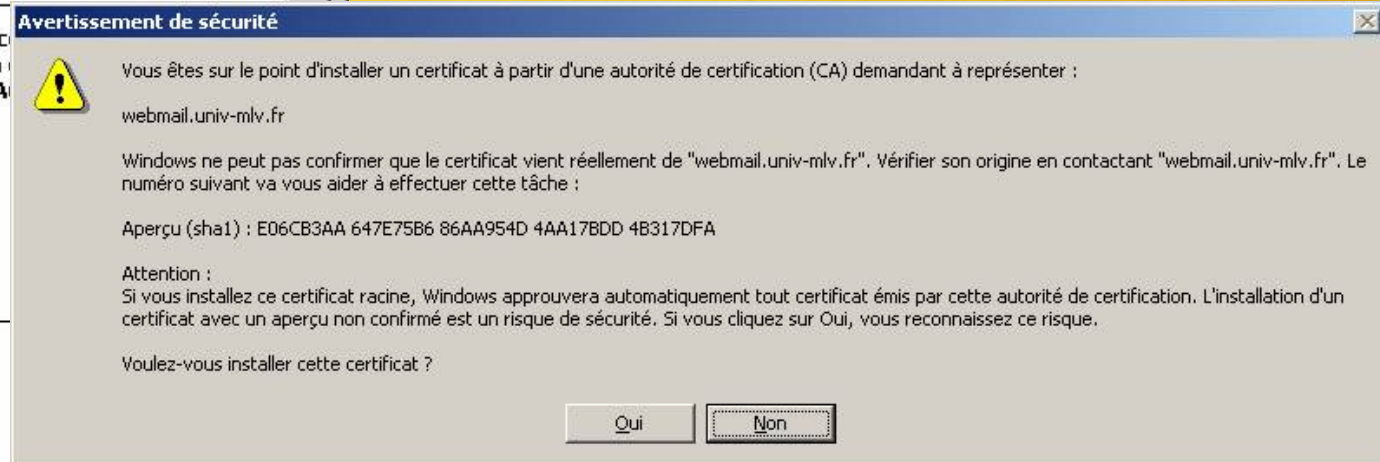
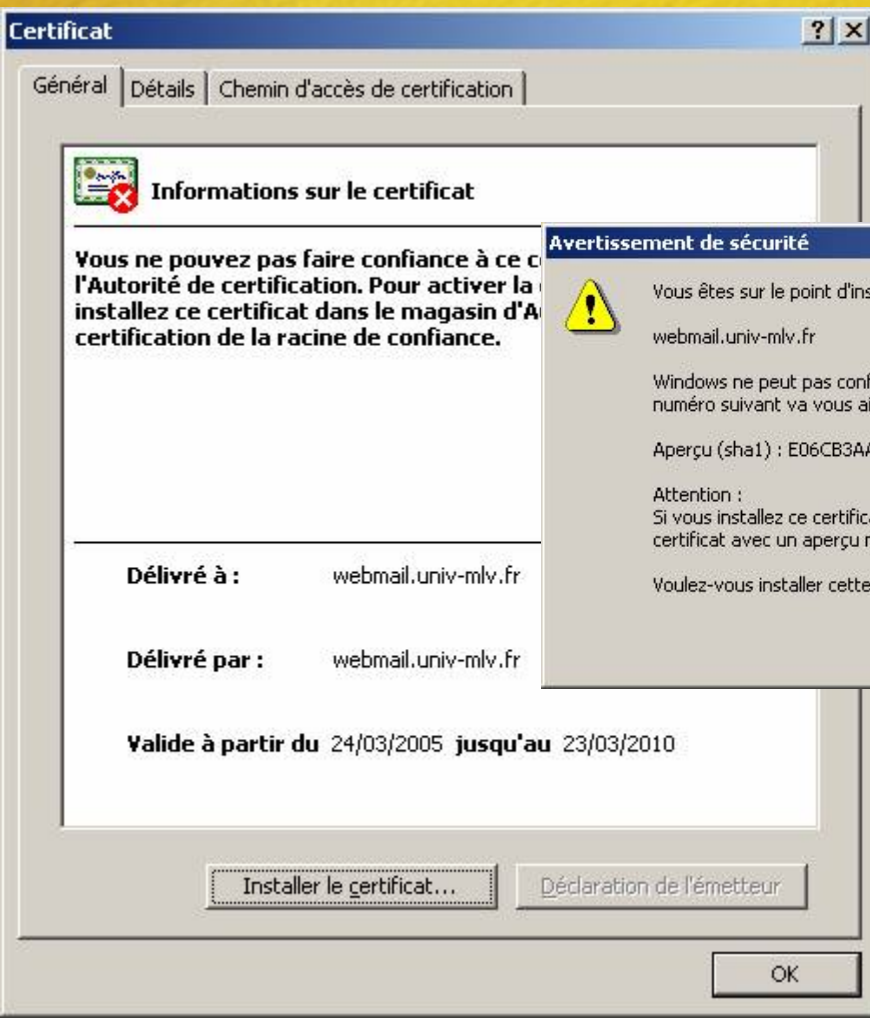




Certificats reconnus

- Le problème précédent ne vient pas du fait que le site est frauduleux mais que le certificat n'est pas reconnu.
- Navigateur « Internet Explorer »
 - ⦿ Menu Outils/Options Internet
 - ⦿ Onglet Contenu/Bouton Certificats

Import de certificat





Création de certificat

● Etapes

- ⊙ Génération d'un couple de clef
- ⊙ Ajout des données d'identification
- ⊙ Ajout d'une durée de validité
- ⊙ Signature par une autorité ou auto-signature

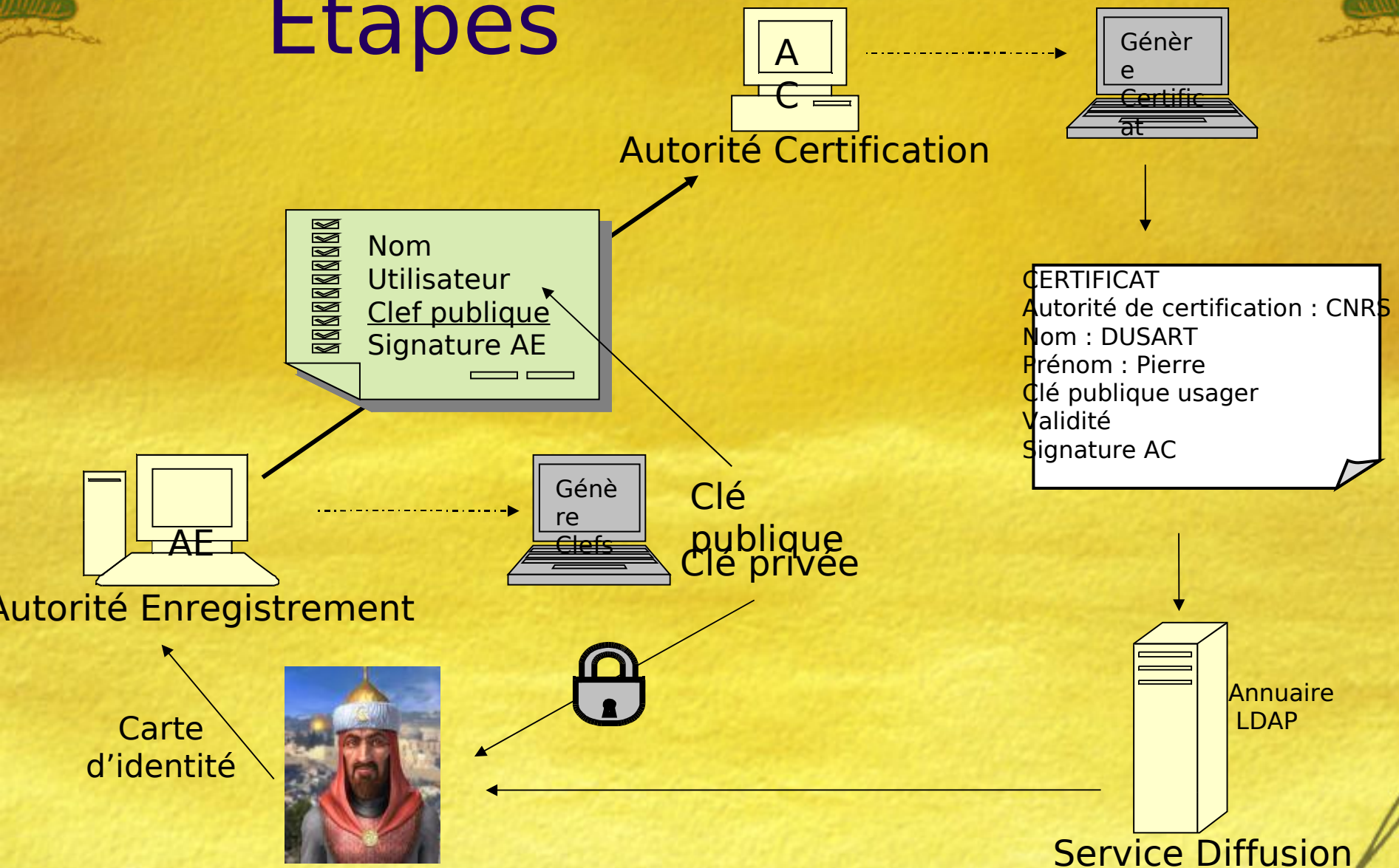
● Exemple d'installation avec OpenSSL

<http://www.linux-france.org/prj/edu/archinet/systeme/ch24s03.html>

● Normalement deux entités :

- ⊙ Une entité d'enregistrement
 - ⊙ Une entité de certification
 - ⊙ Système IGC (Infrastructure de Gestion de Clefs) ou PKI (Public Key Infrastructure) : règles d'enregistrement mises en œuvre
- 

Etapes





Apport des Certificats

- Authentification du site : l'identité du site est vérifiée et approuvée.
 - Chiffrement possible : la clé publique incluse dans le certificat est utilisée pour chiffrer les premiers messages (puis clé symétrique par session)
 - Délégation : on peut installer des certificats qui signeront de nouveaux certificats.
 - Révocation : on peut invalider un certificat (pour retirer une personne du groupe)
- 



Quelques limites des certificats

● Organisationnelles :

- ⊙ Mises à jour régulières non faites
- ⊙ S'il y a un trou dans les procédures, tout peut tomber (faux certificats)

● Techniques :

- ⊙ Divulcation par l'utilisateur de la clef privée
 - ⊙ Récupération des clefs par intrusion
 - ⊙ Délicat transfert du certificat par l'utilisateur sur un nouvel ordinateur
- 



L'authentification du client

- Dans ce que l'on a vu jusqu'ici, elle était faite avec un password
 - Problèmes :
 - ◎ Attaques actives :
 - Attaques par force brute
 - Attaques par dictionnaire
 - Ingénierie sociale
 - Attaque de l'homme du milieu (Man in the middle)
 - ◎ Attaques passives :
 - Keylogger
 - Sniffer ? : non le problème a été résolu par le canal sécurisé
- 



L'authentification du client

- Comment se protéger de ces attaques ?
 - ⊙ avec un certificat ! On a vu tous les avantages et pourtant, il y a des inconvénients ...
 - Lesquels ?
 - ⊙ C'est lourd à mettre en place, à gérer et non transparent pour un usager néophyte
 - ⊙ Ne protège pas contre toutes les attaques
 - ⊙ Trojan, keylogger
 - Vers d'autres solutions pour renforcer l'authentification
- 



Les facteurs d'authentification

● Ce que l'entité connaît

⊙ un mot de passe, un code PIN, une phrase secrète, etc.

● Ce que l'entité détient

⊙ une carte magnétique, RFID, une clé USB, un PDA, une carte à puce, etc.

● Ce que l'entité est ou sait faire

U ⊙ empreinte digitale, empreinte rétinienne, structure de la
N main, structure osseuse du visage ou tout autre élément
I biométrique
Q ⊙ biométrie comportementale tel que signature
U manuscrite, reconnaissance de la voix, un type de calcul
E connu de lui seul, etc.





L'authentification forte

- C'est une procédure d'identification qui requiert la **combinaison d'au moins deux « facteurs » de types différents.**
 - Pourquoi est-ce plus sécurisé qu'une authentification classique (faible) ?
 - ⦿ Il faut voler les différents facteurs à la fois
 - ⦿ Cela complique la tâche de l'attaquant (le pirate)
- 

Exemples de combinaisons

- Une carte à puce et une empreinte digitale



+



- Une carte à puce et un PIN

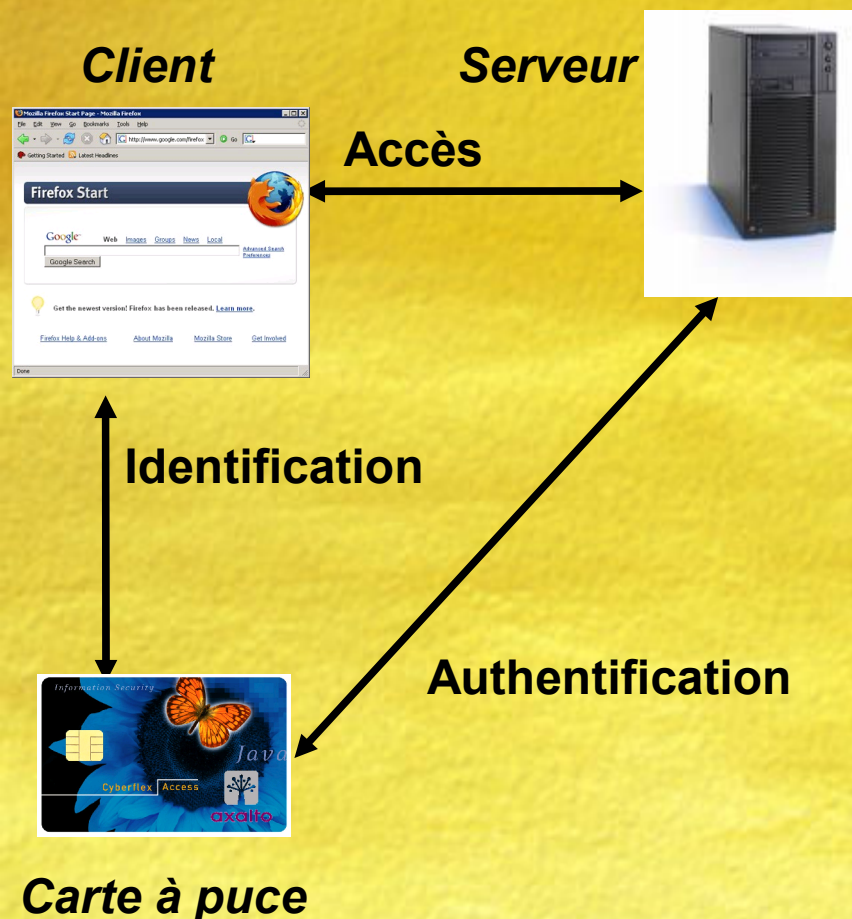


+

1234

Attention, la **puce** de la carte **est réellement utilisée** au contraire des authentifications classiques en ligne

Scénario d'authentification forte



● Ce qui existait :

○ Application cliente

- ⊙ Demande l'authentification à la carte
- ⊙ Gère la « demande de PIN »
- ⊙ Relais les communications carte/serveur
- ⊙ Récupération du contenu

● Aujourd'hui :

○ Application cliente

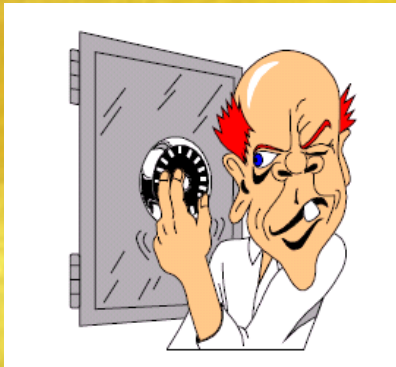
- ⊙ Demande l'authentification à la carte
- ⊙ Gère la « demande de PIN »
- ⊙ Récupération du contenu sur le serveur

○ Carte à puce

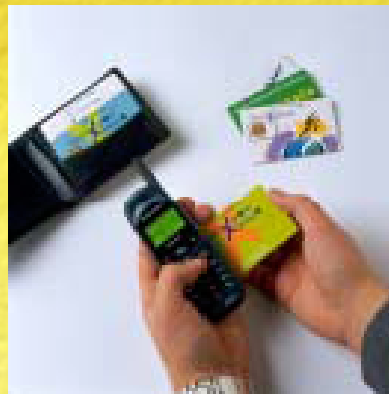
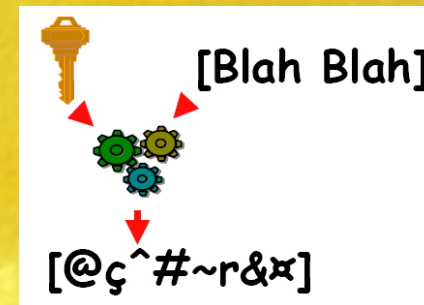
- ⊙ Communique avec le serveur

Avantages de la carte à puce

La sécurité du stockage



Calcul cryptographique



La portabilité

La facilité d'utilisation

Le coût



La technologie Java Card

- Technologie permettant de faire fonctionner des applications écrites en langage Java pour carte à puce
 - Elle définit une plate-forme sécurisée, portable, multi-applicative et dynamique
 - Plus de 2 Milliards de Java Card déployées
 - Elle vient de connaître une évolution majeure le **31 mars 2008** en se tournant vers le web
- 

Comparatif Web et Java Card

● Le Web

◎ Avant 2000

- ◎ Les années 90: déploiement rapide
- ◎ 1995: Applet Java pour le Web
 - Code mobile sécurisé
- ◎ 2000: Bulle Internet (Web 1.0)

◎ Depuis 2000

- ◎ Le Web est partout pour tout : DSL, WiFi, 3G, VPNs, VoIP, ...
- ◎ Pléthore de technologies intelligentes : CSS, DOM, JavaScript (AJAX), RSS, XML, SOAP (Web Service)
- ◎ Web 2.0 : Applications plus riche, WebMail, Blog, Calendrier, sites de réseaux sociaux, Mashups

● Java Card

◎ Avant 2000

- ◎ Les années 90: déploiement mondial
- ◎ 1997: Applet Java Card pour les cartes
 - Code sécurisé pour cartes
- ◎ 2000: Wap pour téléphones mobiles

◎ Depuis 2000

- ◎ Déploiement massif de SIM Java Card 2.x
- ◎ Nombreuses applications : Cartes SIM de grande capacité, Migration EV, marché de l'identification et de la sécurité émergente
- ◎ Nouveautés : mémoires de grande taille, TCP/IP, Java Card 3.0 supportant les servlets

Le “Web World” JC 3.0

■ Protocole de communication

- ◆ HTTP ☒ C'est le protocole pour communiquer en JC 3.0
- ◆ HTTPS, SSL/TLS ☒ La sécurité est le coeur de JC 3.0 !

■ Contenu statique

- ◆ Pages HTML/XML
- ◆ Images, sons... ☒ JC 3.0 embarque un serveur web classique pour fournir les ressources statiques.
- ◆ Flash

■ Langages “Java” pour générer du contenu dynamique

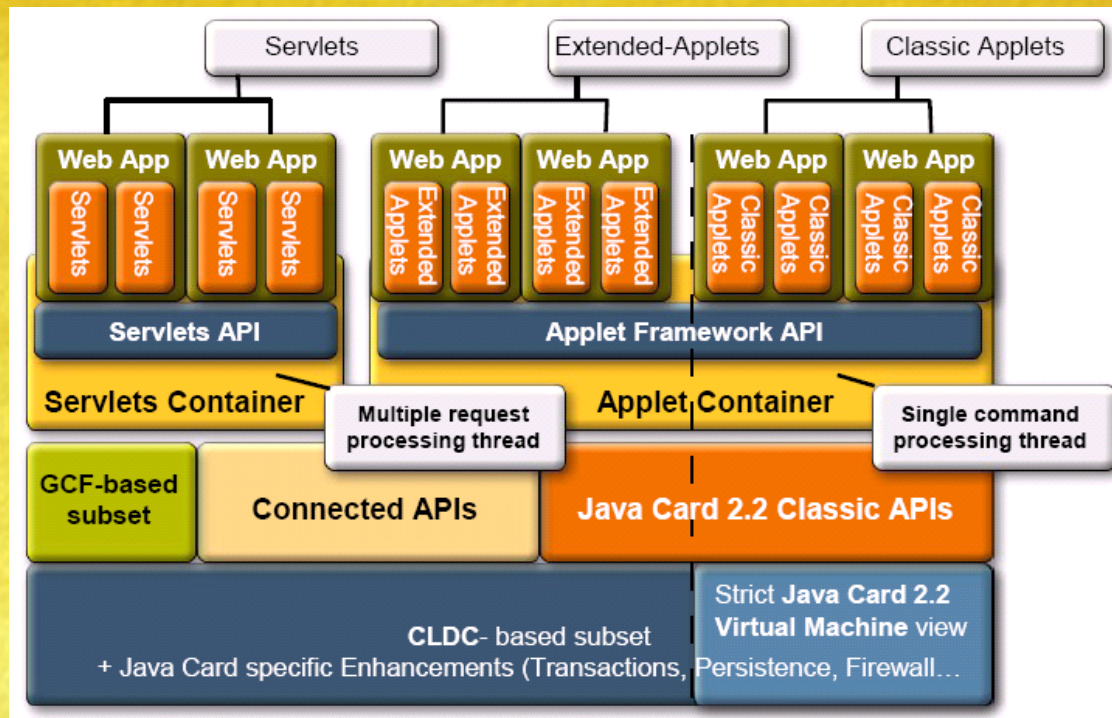
- ◆ Applet ☒ Pas de surcout !
- ◆ Servlet ☒ Modèle d'application dédié pour JC 3.0
- ◆ JSP (Java Server Page) ☒ Nécessite un compilateur Java embarqué
MAIS Les recherches sont en cours pour trouver un compromis basé sur un convertisseur/compilateur hors carte

■ Les autres langages

- ◆ PHP ☒ Un interprète PHP embarqué n'est pas une préoccupation
- ◆ JavaScript / Jscript / ECMAScript ☒ Pas de surcout !

JC 3.0 embarque un serveur Web

- ◎ JC 3.0 se veut être tout d'abord une **plate-forme d'exécution sécurisée**
- ◎ JC 3.0 veut rendre la carte comme **un élément du réseau**
- ◎ Cela a alors conduit à **intégrer un serveur Web** (pour les ressources statiques) afin de compléter l'ensemble des services



Web 2.0 et JC 3.0

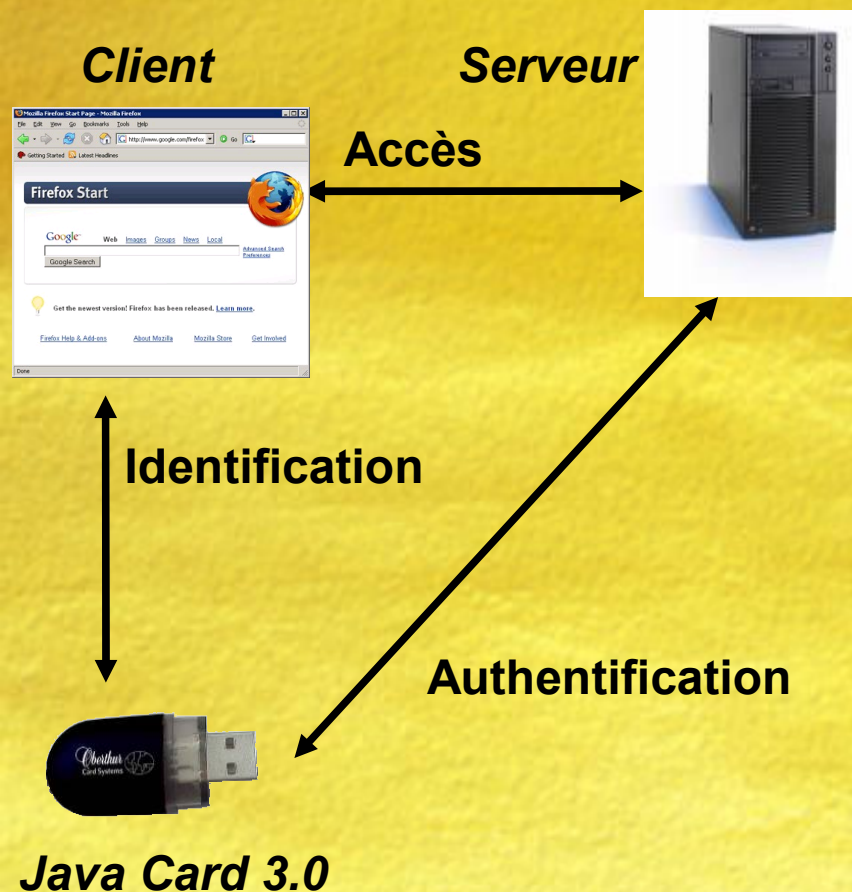
● Web 2.0

- ⊙ Les applications Desktop migrent de plus en plus sur le web
- ⊙ Applications Web plus riches et dynamiques (AJAX)
- ⊙ Applications Web sur téléphones

● JC 3.0 : applications web embarquées

- ⊙ TCP/IP + HTTP(S) sur des protocoles rapides (USB)
- ⊙ Un moteur de Servlet embarqué peut fournir le contenu statique (fichiers) et dynamique (Servlet)
- ⊙ Permet la sécurité des applications Web
- ⊙ Opportunités pour un serveur web Personnel

Authentification avec JC 3.0



● Aujourd'hui :

○ Application cliente

- Demande l'authentification à la carte
- Gère la « demande de PIN »
- Récupération du contenu sur le serveur

○ Carte à puce

- Communique avec le serveur

● Demain :

○ Application cliente

- Demande l'authentification à la carte
- Récupération du contenu sur le serveur

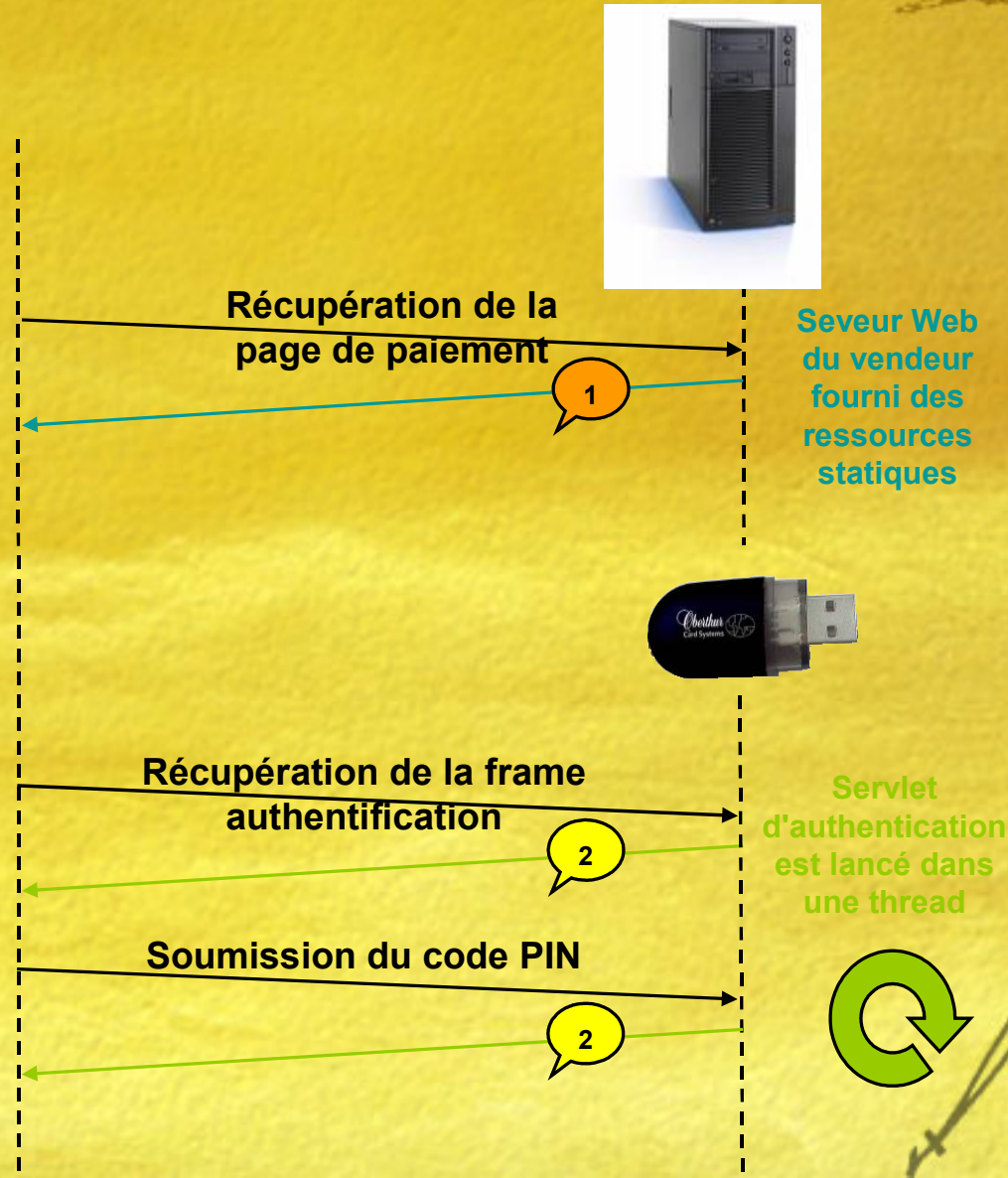
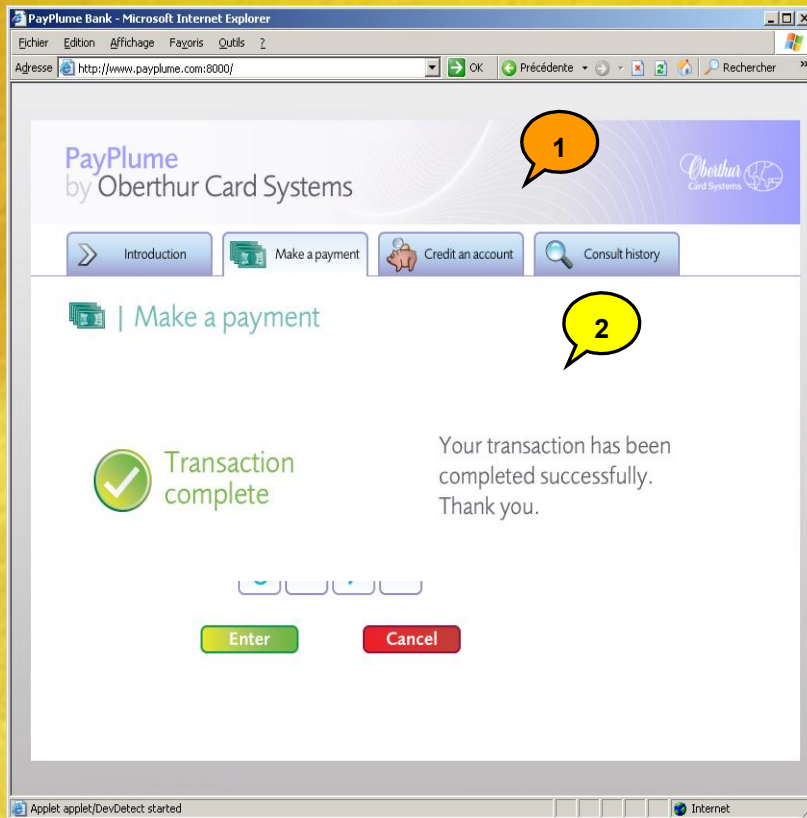
○ Java Card

- **Fournit une interface HTML pour traiter les demandes de PIN**

- Communique avec le serveur

Scenari : Sécurité de bout en bout

End-to-end security—Server-to-Card



1 Code HTML généré par le serveur du vendeur

2 Code HTML généré par token client

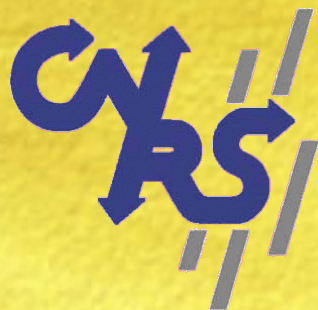


Conclusions

- Il y a différentes solutions de sécurité, ***adaptées à ce que l'on veut sécuriser et au niveau de sécurité que l'on veut atteindre***
 - De plus en plus les éléments de sécurité deviennent omniprésents et s'intègrent au Web (exemple : Java Card 3.0)
 - ***À vous de jouer ...***
- 

Les compétences de l'équipe SSD DMI/XLIM

- L'équipe « Smart Secure Devices »
 - ⊙ La carte à puce
 - ⊙ La cryptographie
 - ⊙ Les réseaux sécurisés
 - ⊙ En particulier les réseaux mobiles ad hoc



Université
de Limoges



Remerciements

● Crédits

- Gemalto
 - Oberthur Card Systems
 - Sun microsystems
- 