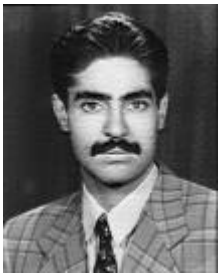
"Authentification dynamique par carte à puce internet, une possible alternative à l'usage polémique des *cookies* et des *WebBugs*"

Bibliographie.

Pascal Urien

Pascal Urien est ingénieur de l'école Centrale de Lyon et Docteur en Informatiques. Il a déposé une dizaine de brevets dans des domaines relatifs aux réseaux et cartes à puces, et rédigé une dizaine de publications . Il est responsable d'un programme de recherches au sein de la société Bull CP8 relatif à l'intégration des puces électroniques dans les réseaux et architectures distribuées sécurisées, ainsi que l'application de ces techniques au commerce électronique. La technologie carte à puce internet («iSimplify!»), issue de ce programme de recherches, a reçu le sésame de la *Meilleure Innovation Technologique* lors du salon cartes'2000 (Paris octobre 2000) et le *Advanced Card Award 2001* (Londres Février 2001), dans la catégorie *Most innovative Product of Year*. Pascal enseigne également les technologies IP dans différentes universités.

Hayder Saleh



Hayder Saleh est titulaire d'un DEA MISI et réalise une thèse cifre sur la définition d'architecture de communication sécurisé.

Adel Tizraoui

Adel Tizaoui est ingénieur INI.et titulaire d'un DEA MISI Il poursuit une thèse cifre relative à la sécurité du commerce des objets virtuel dans l'internet.

Résumé

Ce papier présente une méthode d'authentification dynamique, mettant à profit une interaction entre un document XML et une carte à puce internet. Notre objectif principal est de proposer une alternative à l'emploi des *cookies*, parfois utilisés pour constituer et consulter le profil d'un internaute à son insu. La technologie carte à puce internet transforme une carte à puce en un nœud du réseau internet, qui embarque des applications client et (web) serveur; et supporte en particulier le protocole HTTP. Ce concept innovant a reçu le sésame de la Meilleure Innovation Technologique lors du salon cartes'2000, et un Advanced Card Award 2001 (*Most InnovativeProduct of the Year*).

Summary

This paper describes an original authentication procedure, which works with an interaction between an XML document and an Internet smartcard. Our objective is to propose an alternative to cookies, sometimes used to constitute and consult a net surfer profile, without its agreement. Our internet smart card technology, transforms a smart card into an internet node, running client and (web) server applications; and supporting in particular the HTTP protocol. This innovating concept received a Sesame as the *Best Technological Innovation* at cartes' 2000, and an Advanced Card Award 2001 (*Most Innovative Product of the Year*).

"Authentification dynamique par carte à puce internet, une possible alternative à l'usage polémique des *cookies* et des *WebBugs*"

Pascal Urien
Bull CP8 R&D
68 route de Versailles BP 45, 78431 Louveciennes Cedex
eMail: Pascal.Urien@Bull.net
Tel: 01 39 66 42 30
Fax: 01 39 66 44 61

Hayder Saleh
Phd Student
Hayder.saleh@bull.net

Adel Tizraoui
Phd Student
Adel.Tizraoui@bull.net

1. Introduction.

Dans le contexte d'une croissance exponentielle de la *net économie*, de plus en plus d'entreprises offrent des services marchands sur le web. Ainsi des sites d'un type nouveau, *les portails*, présentent aux consommateurs des liens sur des services ou des produits de consommation courante. D'une manière explicite (par des mécanismes classiques de *login* et mot de passe) ou implicite (au moyen de *cookies* par exemple) il est nécessaire d'identifier l'internaute afin de lui associer un profil utilisateur et lui fournir un environnement personnalisé sur le site web visité.
Parce que le protocole HTTP ne comportait pas de mécanismes d'identification réellement efficaces, la société Netscape Corporation a rédigé dans les années 95, une spécification intitulée "Persistent Client State HTTP Cookie" [7,8], qui permet d'une part d'enregistrer une information persistante côté client, et d'autre part de communiquer ces données au serveur à chaque nouvelle session.
Un cookie se présente sous forme d'un fichier stocké dans un répertoire particulier, par exemple /windows/cookies pour le navigateur IE5. Un cookie est analogue à une clé primaire (*primary key*) d'une base donnée, gérée par un site web. Cette base permet d'établir les goûts et les préoccupations d'un internaute. A partir d'un identifiant (le cookie) le portail gère le profil de son client et en conséquence lui délivre une information personnalisée.
Ce mécanisme pose des problèmes évidents de confidentialité, en effet un site web collecte de l'information sans aucun engagement vis à vis de son visiteur. Aujourd'hui ces données sont échangées ou communiquées sans contraintes particulières. Cependant de nombreux serveurs renseignent (de manière informelle) leurs hôtes sur l'exploitation des informations produites lors des visites du site (c'est la notion de *Privacy Policy*).
De manière plus formelle, le projet P3P [9], "Platform for Privacy Preferences", en cours de développement au W3C consortium, propose de définir un contrat entre un internaute et un site WEB. Le site se conforme à un protocole de confidentialité définit par un *Policy Reference File;* ses différents sous ensembles respectent des règles de gestion de l'information (les *P3P policy*) qui sont communiquées au navigateur, lequel accepte ou refuse en fonction des préférences de l'internaute.
La confidentialité des informations personnelles et le respect de l'anonymat de l'internaute sont des points clés, nécessaires au développement de la net économie. Au début des années 2000, des particuliers et des associations d'utilisateurs ont poursuivi en justice la société *DoubleClick* [11,12] pour l'usage d'une nouvelle technique à base de cookies, les *WebBugs* [10]. Un WebBug est un lien sur une image, dont la dimension est typiquement 1 pixel. L'internaute est identifié sur un site B par un cookie (C_B) stocké sur son disque dur. Lorsqu'il se connecte à un site A, ou il désire rester anonyme, la page d'accueil comporte un WebBug qui pointe sur le site B (DoubleClick par exemple). Lors du chargement de cette image le cookie C_B est émis vers le site B, qui gère par ailleurs un profil de ses visiteurs (par exemple DoubleClick a racheté une compagnie de marketing *AbacusDirectCorp*, qui maintient une base de données ou sont répertoriées 90% des ménagères Américaines). Grâce à un accord commercial entre B et A, le site B délivre au site A un profil de son visiteur, le cookie permet donc la concaténation de plusieurs sources d'informations (une jointure de relations en quelques sortes…).

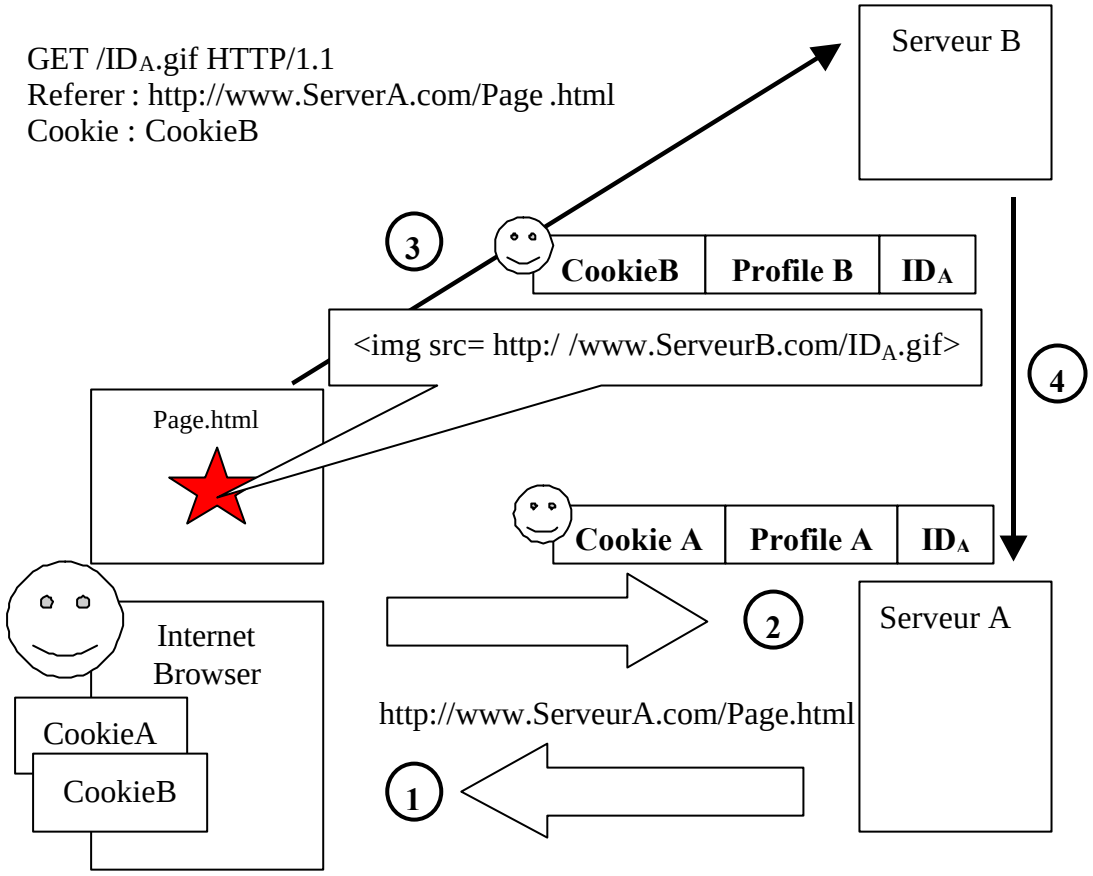


Figure 1: La technique du *WebBug*.

2. Une nouvelle technique d'identification d'un internaute.

Classiquement un internaute remplit un formulaire qui contient un login et un mot de passe, et obtient en retour un cookie qui sera utilisé comme un identifiant temporaire ou permanent. Les navigateurs actuels ne permettent pas une réelle gestion de ces objets, en particulier il n'est pas possible d'interdire les cookies de sites suspects, ou de définir une politique de durée de validité. Compte tenu de ces éléments nous proposons de mettre en place une technique d'identification (éventuellement forte) approuvée par l'utilisateur, mais qui n'implique pas la mémorisation de nombreux mots de passe ou l'usage fréquent de formulaires. Cette technique originale utilise une nouvelle génération de cartes à puce internet (iSimplify!) associée aux technologies XML. Une carte internet comporte un serveur web embarqué, les entités XML étant identifiées par des URLs et transportées par le protocole HTTP, il devient donc possible d'utiliser des interactions entre cartes à puce et documents XML.

3. Les cartes à puces internet.

Les cartes à puces internet (figure 1) ont fait l'objet de plusieurs publications [1,2,3,4], notamment lors du dernier salon infosec'2000 [2]. Une carte à puce peut embarquer plusieurs applications identifiées par un nombre de 16 octets au plus, dénommé Application Identifier (AID).

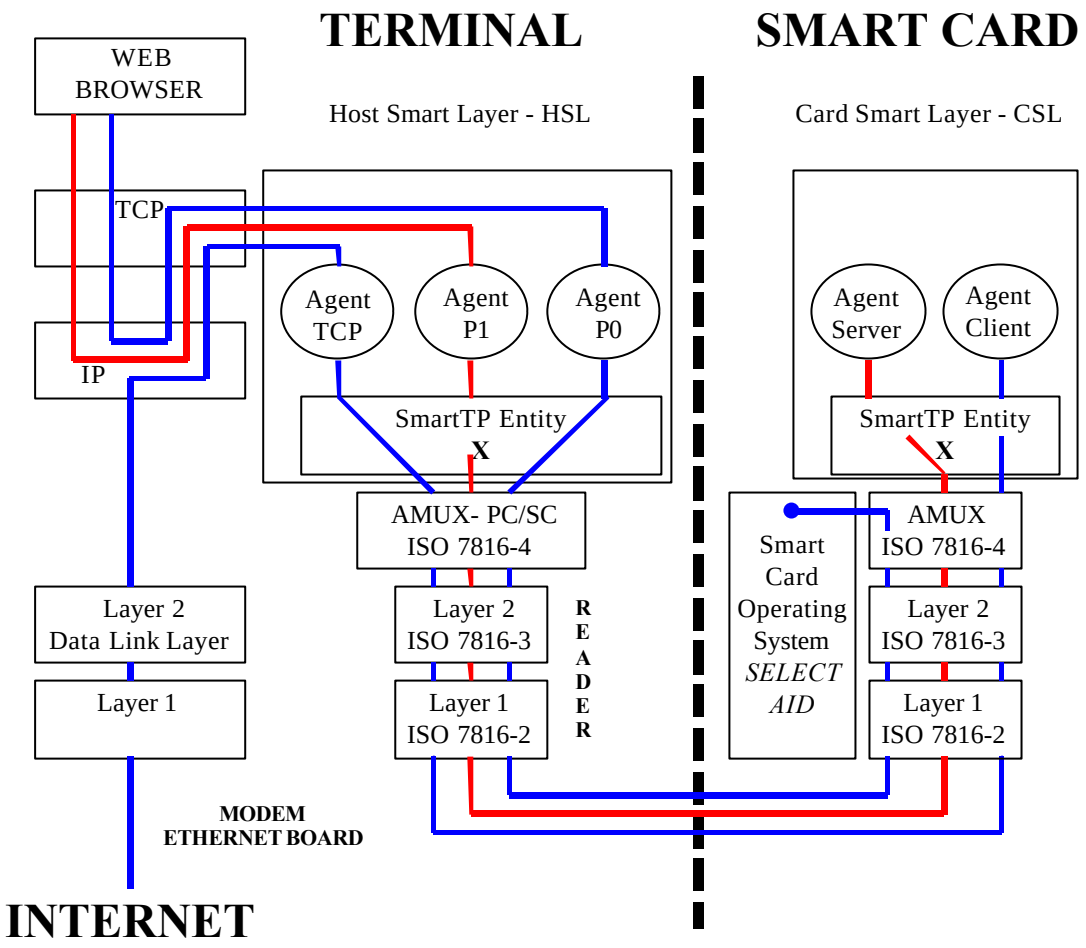


Figure 2 - Carte à puce internet

Nous avons défini deux types d'URLs associées aux cartes internet:

- Des URLs permettant la détection et la sélection d'une application carte particulière, par exemple l'URL http://127.0.0.1:8082/?write=00A40400054A54455354 sélectionne l'application JTEST (AID = 5A 54 45 53 54), en cas de succès on obtient un fichier image de 1 pixel, dans le cas contraire un statut d'erreur HTTP est délivré (c'est une technique que nous nommons ***CardBug***).
- Des URLs permettant d'accéder à des ressources gérées par une application carte particulière.

Le tableau 1 illustre le contenu d'une carte internet qui comporte un applet nommé JTEST

Nom de la ressource	Sémantique	Format
http://127.0.0.1:8080/	Page d'accueil de la carte	Page HTML
http://127.0.0.1:8080/name.txt	Nom du porteur - *Pascal.Urien*	Entité XML
http://127.0.0.1:8080/key1.gif	*card bug* – présence d'une clé DES key1	Fichier GIF
http://127.0.0.1:8080/Key1=69DA379EF99580A8	DES chiffrement d'un bloc de 8 octets	Entité XML
http://127.0.0.1:8080/Key1=+69DA379EF99580A8	DES^{-1} chiffrement d'un bloc de 8 octets	Entité XML

Tableau 1, Carte internet d'identification.

La carte comporte le nom de son porteur (name.txt), un petit fichier image (key1.gif) indiquant la disponibilité d'une clé DES nommée key1, enfin deux procédures invoquées par des URLs de chiffrement (DES_{key1} et sa fonction inverse DES_{key1}^{-1}).

4. Détection d'une carte internet

D'un point de vue du serveur il est nécessaire de détecter la présence d'une carte internet, afin de conduire une identification de l'internaute. Nous utilisons une technique originale que nous nommons *CardBug* (figure 3). Un lien sur une image, incrusté dans une page HTML, permet de détecter et d'activer une application carte à puce. Un javascript déclenche, en cas de succès, le chargement d'un nouveau document XML.

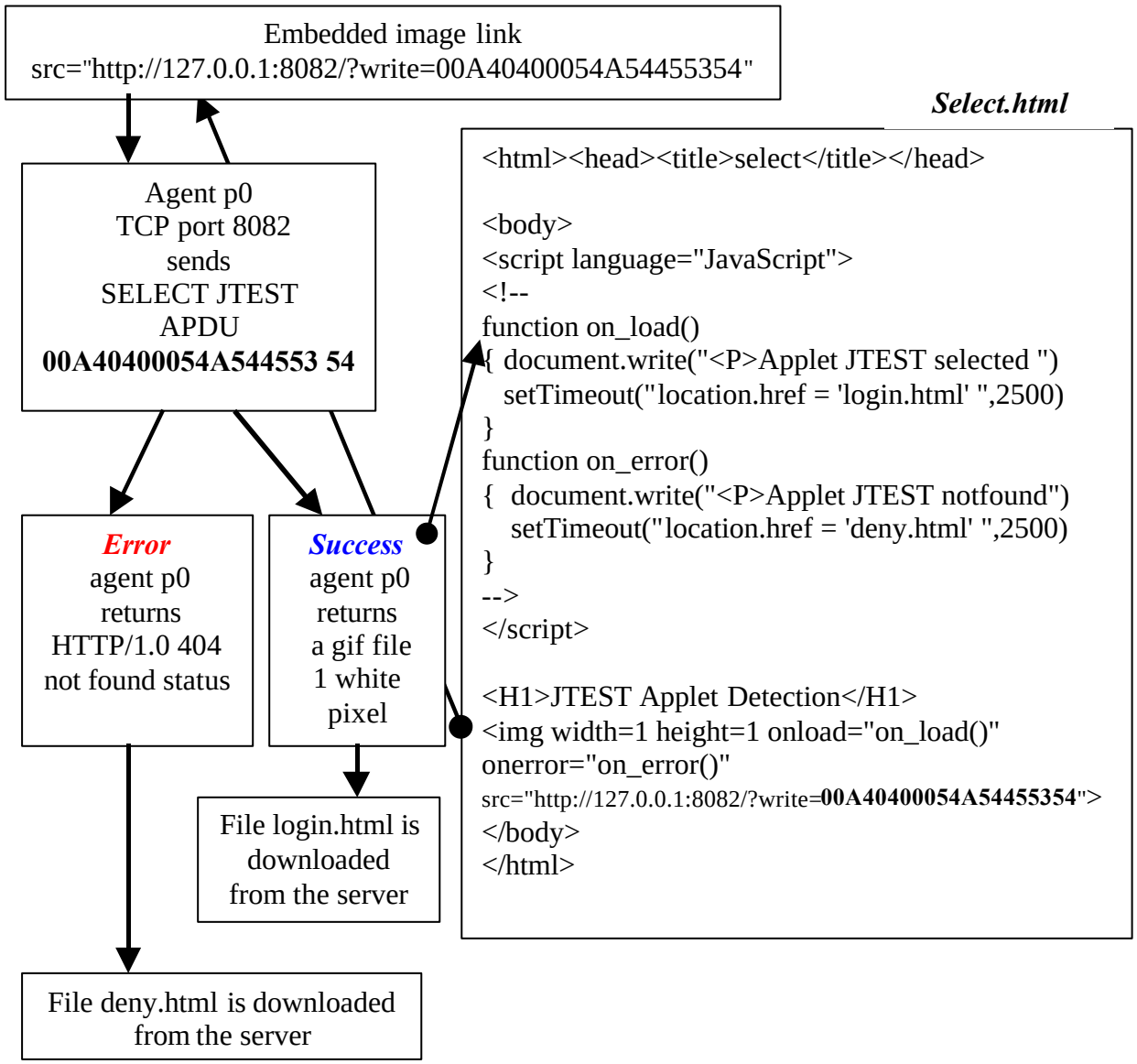


Figure 3 - Mécanisme du Card Bug.

5. Interaction avec XML

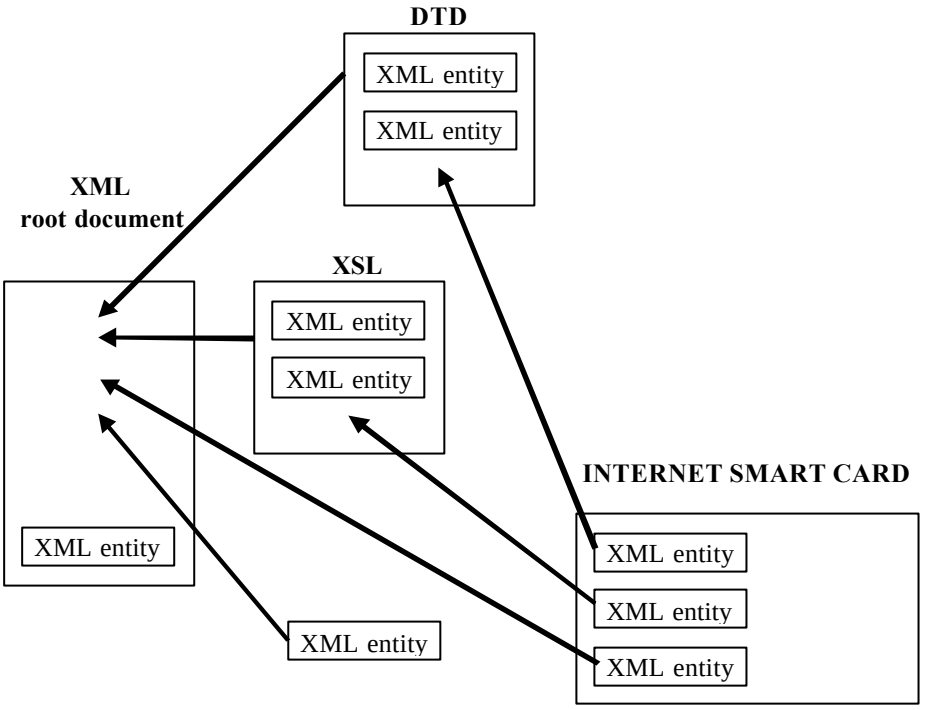


Figure 4 - Interaction entre un document XML et une carte internet.

Les documents ***XML*** [5] sont constitués d'unités de données, dénommées *entités,* qui sont si nécessaire transportées par le protocole HTTP. Une carte internet supportant nativement ce protocole, il devient donc possible d'importer des entités XML stockées dans des cartes. D'un point de vue logique un document XML se présente sous forme d'un arbre d'éléments, délimités par des balises (les *tags*). Chaque élément possède un contenu, qui peut être un autre élément ou divers objets XML tels que entités ou chaînes de caractères. Un fichier ***DTD*** (*Data Type Declaration*), contient une description (et éventuellement des pointeurs vers d'autres fragments de description) de la grammaire associée à un document XML. Il décrit en fait les structures autorisées d'un document XML. Tout ou partie d'un fichier DTD peut être logé dans une carte à puce.

Un arbre XML est généralement associé à un fichier de processeur de feuille de style ***XSL*** [6] (eXtensible Style sheet Language) permettant de construire une page HTML, qui est une représentation des données associées aux éléments XML. Cette page peut comporter des composants logiciels, tels que javascript ou applet, qui seront exécutés par le navigateur. Schématiquement l'interaction entre une carte internet et un document XML se déroule en trois étapes (figure 4) :

1. Un navigateur télécharge la "racine" d'un document XML, cette dernière contient des pointeurs sur des objets XML tels que entités, DTD et XSL. Le document complet est assemblé par le navigateur, et inclut en particulier des entités importées d'une ou plusieurs cartes à puce.

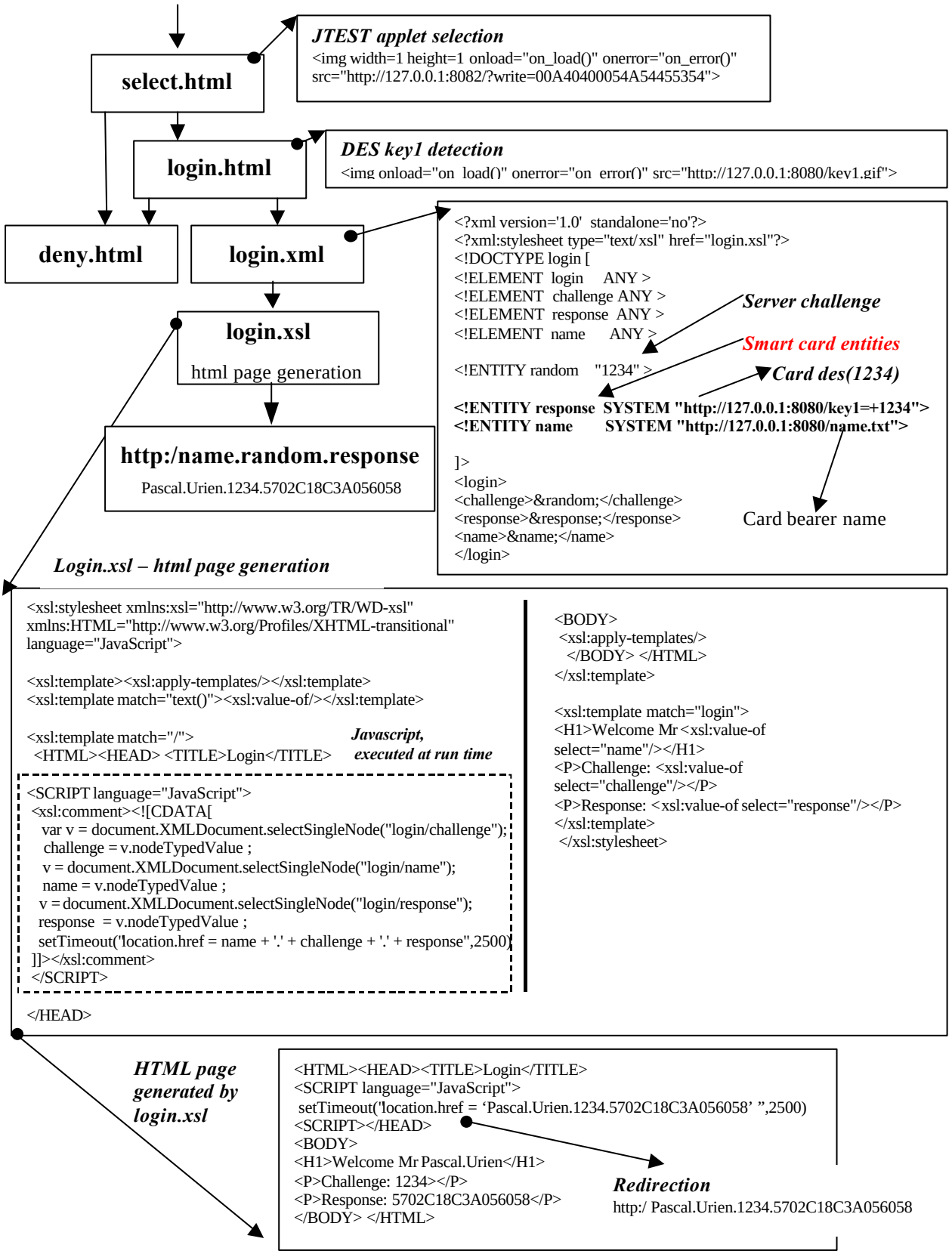


Figure 5 – Mécanisme d'authentification d'un internaute.

2. Une page HTML est construite par le processeur XSL. Cette dernière comporte des composants logiciels (java script, applet) qui seront exécutés avec des paramètres d'appels déduits des contenus d'éléments importés de carte internet.

3. La page produite est chargée par le navigateur, les composants logiciels associés sont exécutés.

6. Un scénario d'identification d'un internaute.

Une internaute accède (figure 5) à un lien sur un fichier (*select.html*) qui nécessite une authentification. Cette page contient un *CardBug* destiné à activer une application JTEST embarquée dans une carte internet.

En cas de succès la page login.html est chargée, et un deuxième *CardBug* teste la disponibilité d'une clé DES *key1* dans la carte à puce.

Après avoir détecté la présence de la clé d'authentification key1, le navigateur charge la page login.xml qui contient un nombre aléatoire (l'entité &*random = 1234*) généré par le serveur.

Une première entité carte (&*response*= 5702C18C3A056058) pointe vers le chiffrement DES de cet aléa (DES(random)), une deuxième entité *(&name* = Pascal.Urien) pointe vers le nom du porteur de la carte.

Le document XML final comporte trois éléments (challenge, response, name) dont les contenus sont respectivement un aléa produit par le serveur, la réponse de la carte à puce à ce dernier, et le nom de l'internaute.

A partir de cet arbre XML et d'un fichier XSL (login.xsl) une page HTML est construite, elle intègre un java script qui force le chargement d'une nouvelle page déduite de name.challenge.response, et identifiée par l'URL,

http:/Pascal.Urien.1234.5702C18C3A056058,

De manière générique ce mécanisme peut être utilisé pour obtenir une ressource (Object) qui requiert des droits d'accès, l'URL http:/name.challenge.response/Object (ou *challenge* est un nombre aléatoire délivré par le serveur, *response* une fonction secrète de ce nombre $F_{(challenge)}$ et *name* le nom de l'internaute) est un pointeur authentifié par une carte internet de cet objet.

7. Conclusion.

Nous avons montré qu'il est possible d'identifier de manière automatique et fiable un internaute, sans avoir recours aux cookies. Nous pensons que ce mécanisme peut renforcer la confiance des internautes et donc favoriser le développement de services marchands sur internet

8. Références

[1] Pascal Urien, Hayder Saleh - "Une nouvelle approche de la carte à puce réseau" - 3° journées réseaux, Ministère de l'Education Nationale de la Recherche et de la Technologie – Montpellier décembre 1999.

[2] Pascal Urien, Hayder Saleh, Adel Tizraoui "La carte à puce internet, une architecture ouverte et adaptée aux applications distribuées multimédia sécurisées", infosec'2000 CNIT Paris la Défense – juin 2000

[3] Pascal Urien " Internet Card, a smart card as a true Internet node", Computer Communications, volume 23, issue 17 pp 1655-1666- October 2000.

[4] Pascal Urien, Hayder Saleh, Adel Tizraoui "Internet Card, a smart card for internet", Protocols for Multimedia Systems (PROMS) Cracow Poland, October 22-25 2000.

[5] Extensible Markup Language (XML) 1.0 (Second Edition), W3C Recommendation 6 October 2000.

[6] Extensible Stylesheet Language (XSL) Version 1.0, W3C Candidate Recommendation 21 November 2000.

[7] Netscape Corporation – "Persistent Client State HTTP cookies" - http://www.netscape.com/newsref/std/cookie_spec.html

[8] D.Kristol –"HTTP State management Mechanism" RFC 2109 February 1997

[9] W3C - "Platform for Privacy Preferences (P3P) Project" - http://www.w3.org/P3P/

[10] Web bugs faq, http://www.privacyfoundation.org/education/webbug.html

[11] DoubleClick accused of unlawful consumer data use" – January 28, 2000 – http://news.cnet.com/news/0-1005-200-1534533.html

[12] USA Today - "Activists charge DoubleClick double cross" – 06/07/00 – http://www.usatoday.com/life/cyber/tech/cth211.htm