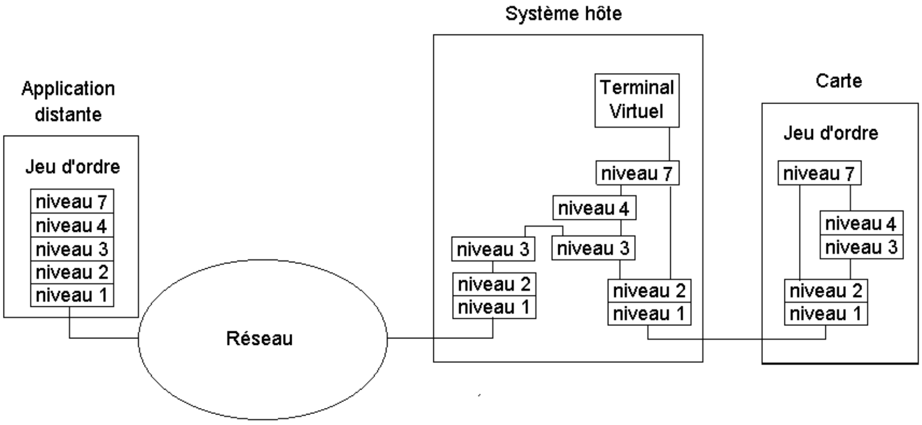
Happy Birthday, Smart Card WEB server !

Pascal Urien, January 2009

The first smart card WEB server was born on January 12th 1999, a memorable Tuesday, due to snow falls that created heavy traffic jams around Paris. At the afternoon end, highways were closed and even some drivers spent the night in their cars. So I had to wait for the end of these traffic jams in my office, in Bull Louveciennes until 10 pm. During these hours, I wrote the last code lines, of the first Java card WEB server. I was in a hurry to see it at work. I drove back to home, had a quick dinner, and then push HTML pages in my smart card, while eating my dessert. Finally at midnight I started my browser with the URL http://127.0.0.1, it was working!. I said to my wife "great new, the first smart card web server is running" and I drunk a victorious glass of red Bordeaux. She was not really convinced, and could not believe that such event was occurring on her dining room table. But it was the truth…

The story began in November 1997, the day I was engaged by the CP8 Company. At that time I was a research engineer specialized in networking and embedded computing. I designed communication boards and operating systems for the Bull Company. I was also a lecturer in several French universities and I was teaching computer designs, operating systems, networking, WEB technologies and Windows programming. Since 1995 I was writing the WSPLUG shareware, a WEB server dedicated to Windows 3.1 and Windows 95 environments. It was my first experiments with eCommerce, and thanks to Compuserve facilities, I earned about 100$, which were spent in fine restaurants.

In February 1998, I was in the office of Michel Ugon, the inventor of the SPOM, i.e. a smart card equipped with microprocessor and internal memories. I asked me to think about new applications for smart cards. A few weeks later, I came back with two proposals, peer to peer networks, based on contactless smart cards and smart cards as IP nodes. The second idea won unanimous support, the *SmartNet* project was born.



The *Sm@rNet* Project Architecture, February 1998

During the summer 1997, I read while windsurfing in south of France, a heavy book from Guy Pujolle, a famous professor teaching networking at the University of Versailles. I was looking for a partnership student, so in March 1998, I sent a first email to Guy Pujolle, in which I described the project by a few words, "smart card is a network computer". The answer was "OK, let's do it". But in 1998, in the dot-com bubble context, it was very difficult to find students for research projects. Hayder Saleh volunteered for this job; it was a skilled student from Bagdad, who got a grant for studying in France. After a short training he was speaking and writing French in a very phonetically way, but he was a cleaver guy opened to new technologies.

During the spring 1998, I designed the SmartTP (*Smart Transfer Protocol*) protocol making a logical bridge between TCP and the ISO 7816 transport. I built an experimental platform emulating smart cards and terminals, and equipped with two serial ports. Two separate applications simulated dialogs between browser and smart card; they were linked via a null modem cable. Hayder was in charge to implement a meticulous emulation of the T=1 protocol.

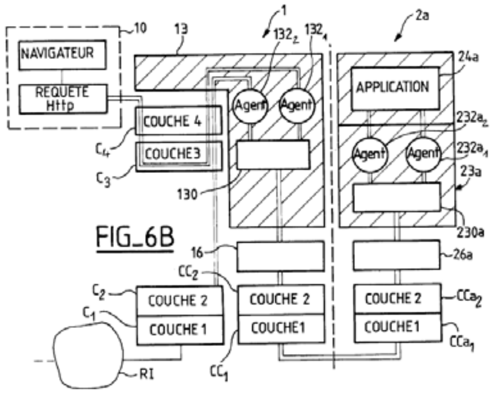
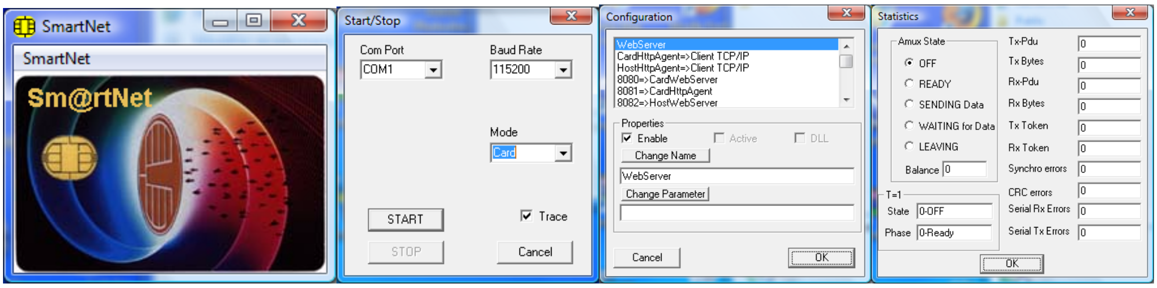


FIG_6B

The first patent, August 13th, 1998.

In July, the first SmartTP specification was released and validated with the Windows platform. I wrote a patent proposal and forwarded it to our intellectual property department. Several rough debates were needed for convicting them that my idea made sense. I renumber a heated discussion with a patent consultant explaining me that “smart cards are not and will never be WEB servers”. Finally I won on points, and the patent was issued on August 13th 1998. In October we presented a live demonstration of our PC platform to marketing attendees. It showed a browser downloading HTML page from a smart card emulated WEB server. Yes it should be possible to do that!



Com Port: COM1
Baud Rate: 115200
Mode: Card
☑ Trace

WebServer
CardHttpAgent=>Client TCP/IP
HostHttpAgent=>Client TCP/IP
8080=>CardWebServer
8081=>CardHttpAgent
8082=>HostWebServer

Properties
☑ Enable ☐ Active ☐ DLL
WebServer

Amux State
● OFF
○ READY
○ SENDING Data
○ WAITING for Data
○ LEAVING
Balance: 0

T=1
State: 0-OFF
Phase: 0-Ready

Tx-Pdu	0
Tx Bytes	0
Rx-Pdu	0
Rx Bytes	0
Tx Token	0
Rx Token	0
Synchro errors	0
CRC errors	0
Serial Rx Errors	0
Serial Tx Errors	0

The Sm@rNet Simulation platform, in September 1998

At the end of his internship, Hayder took some vacations in Bagdad. I redacted a PHD proposal and began the fight for its funding. In 1998 it was not easy to deploy smart card readers because no standards were clearly defined. CP8 was using serial devices called *TLP 224*, working with proprietary APIs, the “CP8 AKL”. During the autumn, I intensively practiced ISO 7816 dialogs, and I successfully integrated the TLP 224 reader to the software platform.

When Hayder come back from Iraq in November, I got a temporary funding; we started a PHD work with Guy Pujolle and continued the job. The next big step was to physically design a smart card WEB server. Hopefully a revolution had occurred within the smart cards landscape. CP8 released its first Java card, “Odyssey” offering 7 Kilo Bytes of memory for data and code. We bought *Java for dummies*, and learned java cards programming in CP8 corridors and at the coffee machine. Furthermore our office neighbors were a group of friendly Indian engineers, designing the programming kit for Odyssey products.

As I mentioned before, I was a teaching expert of embedded systems, programming and WEB technologies. It didn’t take me a long time for coding a WEB server for java cards. The critical issue was mainly the protocol (SmartTP) transporting HTTP packets between smart card and browser, which had been previously validated. Mid-January 1999, the first smart card WEB server was running: 3,5 KB were consumed by the java program and 3,5 KB were available for its content.

January 1999, the first smart card WEB server, designed with an Odyssey Java card and a TLP 224 reader.

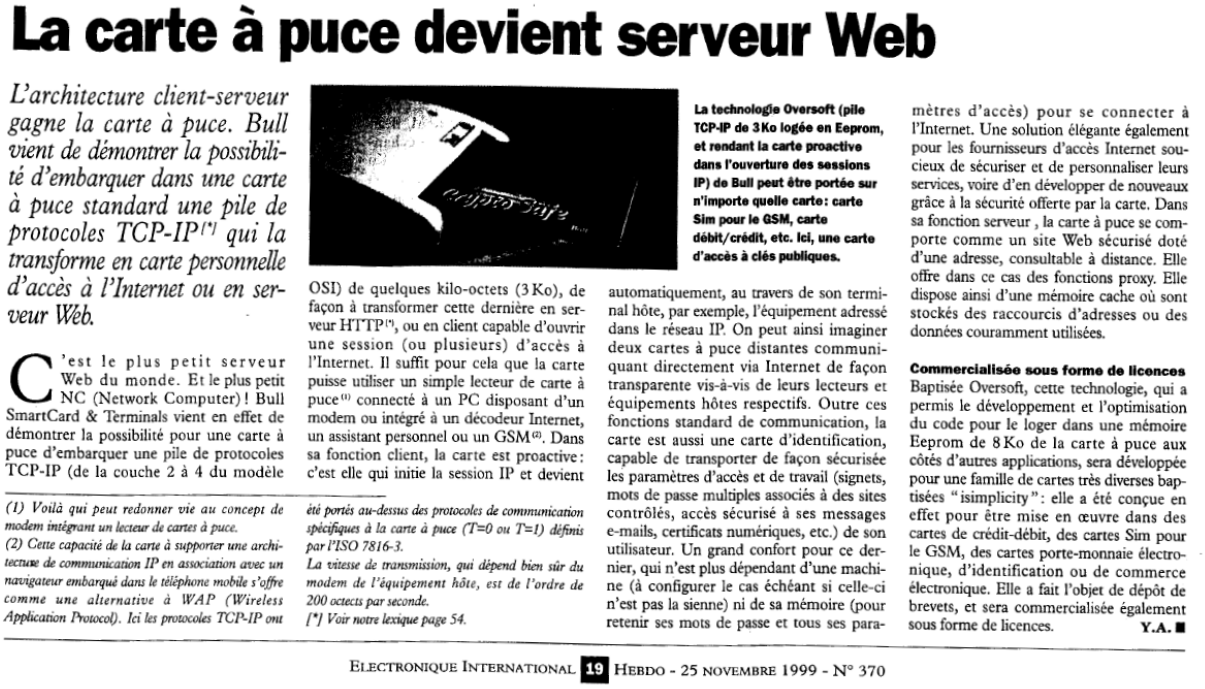
After some additional tests and improvements I sent a victorious email to the BULL staff, “the first world smart card WEB server is running, you can use at my IP address”. Gerard Roucairol, who was heading BULL researches, made an enthusiastic response, in French “*J’en reste sur le cul*”. But nothing else occurs during a few weeks, the company managers were using a proxy for their internet surf, and weren’t able to configure it. So they could reach my smart card WEB server…

I was a little depicted, but I submitted a first paper proposal to a French conference, JRES99, organized by the CNRS research agency. I took a risk, because I could be fired for that, but my pioneer spirit was stronger.

In March 99, I was invited to the traditional lunch offered by CP8 to its inventors of the year. David Levy, the company CEO chaired this event, it was my table neighbor. We had a long talk about the smart card WEB server. My students were prepared to a possible delay for my afternoon talk, at the university of Paris Dauphine. I was one hour late, and I said them “the story is beginning”, there were “hurrah!” in the room.

During the spring 1999, I made a 48 hours trip with my CEO to the SUN headquarters in the San Francisco area, where I demonstrated the smart card WEB server. SUN suggested to freely distribute this technology and to make money with services. David Levy replied that “he didn’t suppose that Americans were communists”. I also suggested an open approach, i.e. code source publication, but the answer was “if you do that, you are fired”.

The technology got a new name *OverSoft*, because “Over” is smarter than “Micro”. It was officially announced at the Cartes’99 fair. The first French paper was published in December 99 at JRES99, the first revue paper appears in Computers Communications in 2000, and I was not fired…



crypto Safe

La carte à puce devient serveur Web

L'architecture client-serveur gagne la carte à puce. Bull vient de démontrer la possibilité d'embarquer dans une carte à puce standard une pile de protocoles TCP-IP[*] qui la transforme en carte personnelle d'accès à l'Internet ou en serveur Web.

La technologie Oversoft (pile TCP-IP de 3 Ko logée en Eeprom, et rendant la carte proactive dans l'ouverture des sessions IP) de Bull peut être portée sur n'importe quelle carte: carte Sim pour le GSM, carte débit/crédit, etc. Ici, une carte d'accès à clés publiques.

C'est le plus petit serveur Web du monde. Et le plus petit NC (Network Computer) ! Bull SmartCard & Terminals vient en effet de démontrer la possibilité pour une carte à puce d'embarquer une pile de protocoles TCP-IP (de la couche 2 à 4 du modèle OSI) de quelques kilo-octets (3 Ko), de façon à transformer cette dernière en serveur HTTP[*], ou en client capable d'ouvrir une session (ou plusieurs) d'accès à l'Internet. Il suffit pour cela que la carte puisse utiliser un simple lecteur de carte à puce[1] connecté à un PC disposant d'un modem ou intégré à un décodeur Internet, un assistant personnel ou un GSM[2]. Dans sa fonction client, la carte est proactive : c'est elle qui initie la session IP et devient automatiquement, au travers de son terminal hôte, par exemple, l'équipement adressé dans le réseau IP. On peut ainsi imaginer deux cartes à puce distantes communiquant directement via Internet de façon transparente vis-à-vis de leurs lecteurs et équipements hôtes respectifs. Outre ces fonctions standard de communication, la carte est aussi une carte d'identification, capable de transporter de façon sécurisée les paramètres d'accès et de travail (signets, mots de passe multiples associés à des sites contrôlés, accès sécurisé à ses messages e-mails, certificats numériques, etc.) de son utilisateur. Un grand confort pour ce dernier, qui n'est plus dépendant d'une machine (à configurer le cas échéant si celle-ci n'est pas la sienne) ni de sa mémoire (pour retenir ses mots de passe et tous ses paramètres d'accès) pour se connecter à l'Internet. Une solution élégante également pour les fournisseurs d'accès Internet soucieux de sécuriser et de personnaliser leurs services, voire d'en développer de nouveaux grâce à la sécurité offerte par la carte. Dans sa fonction serveur , la carte à puce se comporte comme un site Web sécurisé doté d'une adresse, consultable à distance. Elle offre dans ce cas des fonctions proxy. Elle dispose ainsi d'une mémoire cache où sont stockés des raccourcis d'adresses ou des données couramment utilisées.

Commercialisée sous forme de licences

Baptisée Oversoft, cette technologie, qui a permis le développement et l'optimisation du code pour le loger dans une mémoire Eeprom de 8 Ko de la carte à puce aux côtés d'autres applications, sera développée pour une famille de cartes très diverses baptisées "isimplicity" : elle a été conçue en effet pour être mise en œuvre dans des cartes de crédit-débit, des cartes Sim pour le GSM, des cartes porte-monnaie électronique, d'identification ou de commerce électronique. Elle a fait l'objet de dépôt de brevets, et sera commercialisée également sous forme de licences. **Y.A.** ■

[1] Voilà qui peut redonner vie au concept de modem intégrant un lecteur de cartes à puce.

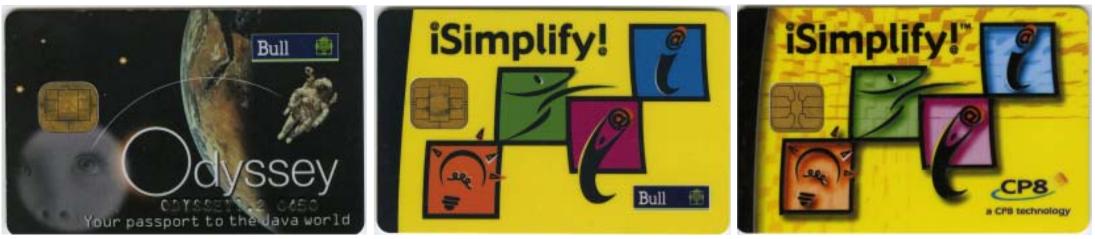
[2] Cette capacité de la carte à supporter une architecture de communication IP en association avec un navigateur embarqué dans le téléphone mobile s'offre comme une alternative à WAP (Wireless Application Protocol). Ici les protocoles TCP-IP ont été portés au-dessus des protocoles de communication spécifiques à la carte à puce (T=0 ou T=1) définis par l'ISO 7816-3.

La vitesse de transmission, qui dépend bien sûr du modem de l'équipement hôte, est de l'ordre de 200 octects par seconde.

[*] Voir notre lexique page 54.

ELECTRONIQUE INTERNATIONAL 19 HEBDO - 25 NOVEMBRE 1999 - N° 370

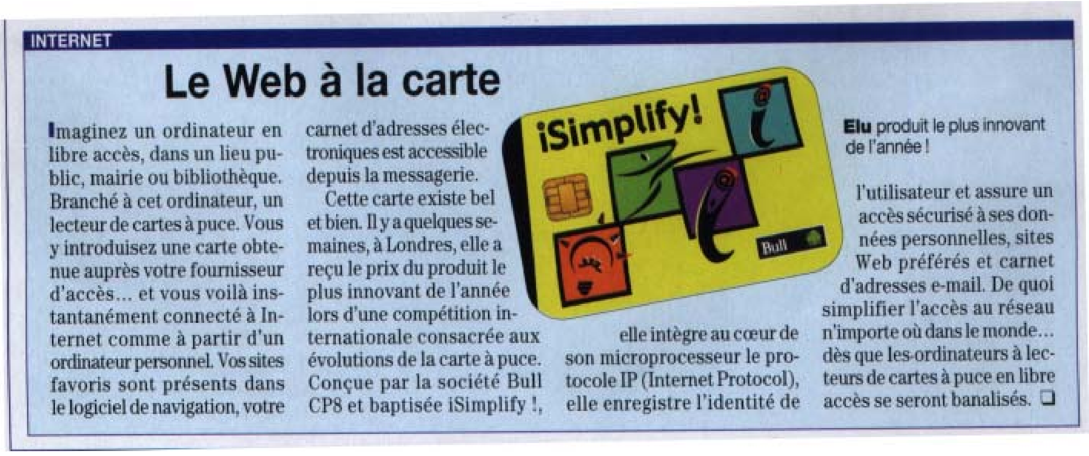
November 1999, the first press release



Three designs of the smart card WEB server

Sesames Award, Paris 2000 (left part) and Advanced Card Award, London 2001 (right part)

A new PHD student, Adel Tizraoui completed the research team in 2000. One fine morning of May 2000, Hayder read in the subway an advertisement for the innovation competition, “Les Sésames” organized during the cartes’2000 event. It took a couple of days to convict our staff that we should participate to this competition. Finally I was authorized to do it, I wrote and submit our entry; we got the Sesame of the Best Technological Innovation. During the autumn 2000, a new name was given to the smart card WEB server, the iSimplify! card. A few hundred cards were produced and printed for the cartes’2000 fair. We (the research team) designed a football quiz (the “Zizou applet”), driven by an HTTP interface; every lucky winner was gratified with a true soccer.


iSimplify!
Bull

INTERNET

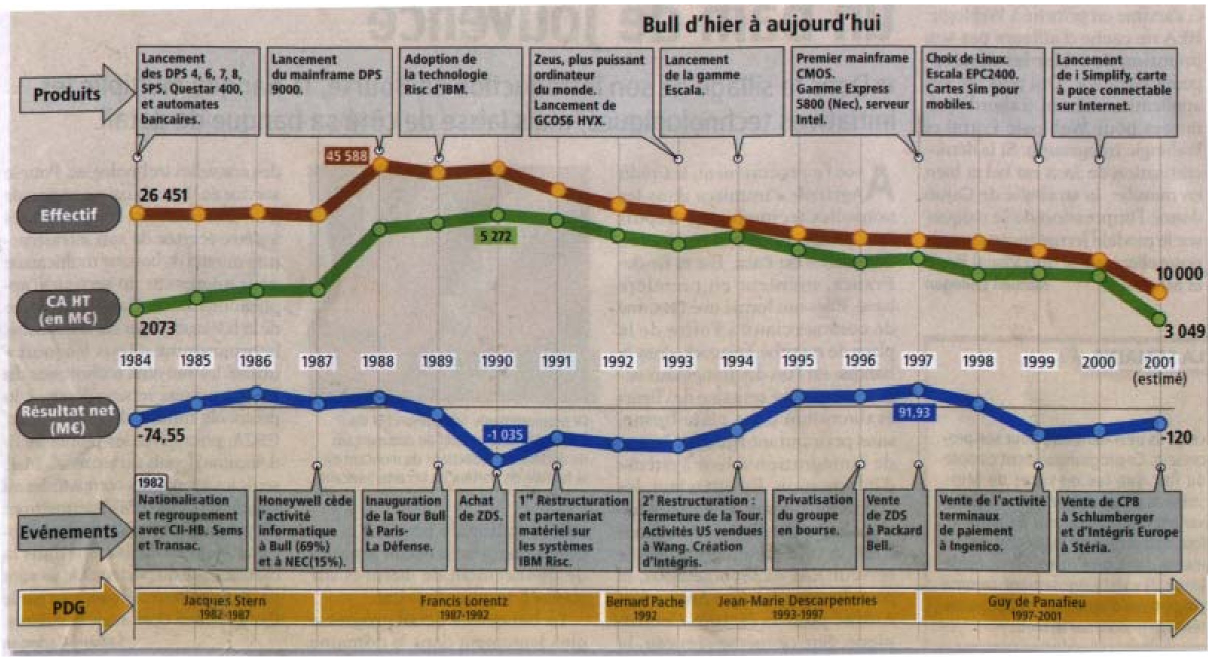
Le Web à la carte

Imaginez un ordinateur en libre accès, dans un lieu public, mairie ou bibliothèque. Branché à cet ordinateur, un lecteur de cartes à puce. Vous y introduisez une carte obtenue auprès votre fournisseur d'accès... et vous voilà instantanément connecté à Internet comme à partir d'un ordinateur personnel. Vos sites favoris sont présents dans le logiciel de navigation, votre carnet d'adresses électroniques est accessible depuis la messagerie.

Cette carte existe bel et bien. Il y a quelques semaines, à Londres, elle a reçu le prix du produit le plus innovant de l'année lors d'une compétition internationale consacrée aux évolutions de la carte à puce. Conçue par la société Bull CP8 et baptisée iSimplify !, elle intègre au cœur de son microprocesseur le protocole IP (Internet Protocol), elle enregistre l'identité de l'utilisateur et assure un accès sécurisé à ses données personnelles, sites Web préférés et carnet d'adresses e-mail. De quoi simplifier l'accès au réseau n'importe où dans le monde... dès que les ordinateurs à lecteurs de cartes à puce en libre accès se seront banalisés. ❑

Elu produit le plus innovant de l'année !

April 2001, an insert in the French magazine Sciences & Avenir.



2002, an insert in the French magazine “01 informatique” illustrates the launching of the first iSimplify! product, based on a smart card WEB server

CP8 was bought in 2001 by Schumberger. The iSimplify! product disappeared. The research team released 9 patents and dozens of publications; it integrated OSI concepts, server and client paradigms and XML technologies in the smart card ecosystem. After a strong internal lobbying, I published the IETF draft entitled “Smart Transfer Protocol” in June 2001.

A Short Bibliography

Pascal Urien, Hayder Saleh. "Une nouvelle approche de la carte a puce reseau", December 1999, JRES 99 Montpellier.

Pascal Urien "Internet Card, a smart card as a true Internet node", Computer Communication, volume 23, issue 17, October 2000.

Internet Draft, “SmartTP, Smart Transfer Protocol”, June 2001,
http://bgp.potaroo.net/ietf/all-ids/draft-urien-smarttp-00.txt

Pascal Urien, Hayder Saleh, Adel Tizraoui , "XML Smartcards", Springer Verlag, LNCS 2093 IEEE International Conference on Networking, ICN'01, July 11-13, 2001, Colmar, France.

Pascal Urien, "Programming internet smartcards with XML scripts", Springer Verlag, LNCS 2140, e-Smart 2001, September 2001.

Pascal Urien, "Internet smartcard benefits for Internet security issues", Campus-Wide Information Systems, Volume 20, Number 3, 2003, pp. 105-114.