Smartcard interoperability testing in a technology confused Market.

Alan Berg*, Jaap van Ginkel[†]
Universiteit van Amsterdam, Informatiseringscentrum, Amsterdam

*a.m.berg@ uva.nl
[†]j.v.ginkel@uva.nl

Abstract

This paper describes the outcome of a smartcard project that was funded by the Gigaport initiative [1] and occurred over an extended period of time at the Information centre (Informatersingscentruim) of the University of Amsterdam. The technologies involved have the potential to secure communication and authorization for web based applications and therefore can be considered a major component in a telecommuting or distant learning infrastructure.

The emphasis of this paper is knowledge sharing of potential pitfalls of applying these types of technology and is designed for providing interested innovators and potential decision makers with communication over baseline terminology/technology.

The project plan was to examine the feasibility of building authorization for an electronic shop for the whole student population of Holland and in specific Amsterdam University via standard Microsoft ^{tm} technologies [2,10] placed under the conventional PKI infrastructure of SURFNET. This project thus reflected our perception of how the commercial market place could potentially evolve within a discrete and relatively short time frame.

The project was split into a number of sections:

(1) Technology Feasibility testing, named trial one.
(2) Communication of limitation via the documentation of limitations.
(3) Reorientation of the project focus to achieve a realistic and more limited system specification, named trial two.

The project can be considered a success as number important conclusions were made. Chief among these conclusions being that administration issues and complex details in the certificate structure makes the use of this particular instance of PKI not immediately relevant for us for large scale deployment outside the campus boundaries e.g. the Internet.

Keywords: PKI, Smartcard, Interoperability.

Overview of trail one and two.

The commercial market place has impact on the market place for Educational IT infrastructure. There is a tension between building systems via open standards and using commercial products that sometimes use and sometimes do not use open standards. Commercial products can sometimes, by ignoring or warping open standards build more personalized or feature rich infrastructure. For the system integrator the drag from user demand is towards the commercial, but from the long-term maintainability for the open standard and open source solutions. Within this framework, from a practical point of view it is important to be able to differentiate the capability of products.

The emphasis of the Informatersingscentruim smartcard project was to test how a Microsoft/ Active Directory Public Key Infrastructure (PKI) [7] could sit under the national PKI infrastructure of SURFNET [2..4]. The tension between open standards and possibly open standard system soon becomes apparent. To achieve a realistic project target it was decided to build shopping services for software downloads for students. The authentication of students would be via smartcards. The smartcards would contain certificates that were unique to the student and would be generated by a Microsoft ^{tm} oriented PKI software. In detail the Subordinate Certificate Authority using Windows2000 was to sit under the production Root Certificate Authority of Surfnet. The system failed due to very strong incapability in the details of the X509 certificate for the subordinate Authority. The incapability had strong implications for how SURFNET could proceed with working with Microsoft related PKI infrastructures.

The failure to build the infrastructure was not considered a failure of project extent as these where exactly the results that were being tested for. To fine-tune the knowledge over functionality boundaries two sub tests were performed:

(1) The creation of a Microsoft only solution, which included Smartcard logon to a Windows 2000 forest. As expected the Microsoft only approach worked. However, surprisingly you had to treat the system in exactly the right and tender way as the system has a number of unwanted[8] and poorly documented limitations.

(2) The creation of non-homogenous web services where students may use the smartcard to store their client certificate and authenticate against a website via their web browser. This situation was helped somewhat by the use of a middleware solution to allow standard certificates on the smartcards and

not just ones generated for the express purpose of workstation logon.

An infrastructure of the two market leader web servers; Internet Information Server (5 and Beta 6) and Apache (versions 1.3 and 2) was used and were made to work Microsoft PKI web server certificates and also to work in collaboration to build one virtual service. The underlying operating systems were; Linux, Windows200 server, Windows 2000 professional and Windows XP.

Trial One took place within a laboratory situation. Creation of a single sign on Solution via smart cards in a Microsoft only environment was shown to be realistic. However, the obvious implication that you then become dependent on one manufacture for your infrastructure was a big enough minus to make this and unrealistic in a non-homogenous campus wide system. Other problems were also found that should also be considered a major minus. Microsoft is transitioning their product range from Windows 2000 server technology to an upgraded Windows .Net environment. Compatibility problems emerged and security-patching problems aggravated this easily ruffled platform.

Trial two took place with the help of a small group of around thirty end users. Trial two highlighted logistic problems: How does one place logos on smartcards? How does one transport certificate revocation lists (to be explained later) and how does one maintain a safe and coherent set of services? The positive outcome of the trial was that the technology as implemented is secure, cheap (and cheaper by the moment) and relatively easy to use for the end user. Trail two therefore highlights that the real cost of a smartcard project, with reference to placing in a highly mixed campus wide system, is the maintenance and administration of the secure PKI infrastructure. Please note that this cost is not loaded towards cost of adequately equipping or training the end user, but rather one of continued administration.

A more detailed view of trail one.

The original plan for trial one was create a PKI allowing certificates to be generated within a laboratory situation with the, express, delegated authority of the production authority for Surfnet. This is shown figuratively in figure one.

As can be seen in table one there is a break in the chain of authority. This point was caused by the way the logon station requires certain attributes in certificates to point to Certificate Revocation Lists (CRL). The simplest form of CRL is a list of certificates that have been invalidated. The list contains the name of the certificate and a checksum. Each CA and subordinate CA needs to maintain its own list and the logon server needs to be able to find and download the most current lists otherwise no logon would be allowed. In the situation examined we found that two attributes are a minimum requirement for the logon server to do its work. The CDP and the AIA attributes. The CDP attribute explains where to find a certificate revocation list. The AIA attribute explains where it finds the certificate of the parent authority. Suffice to say the certificate published to the Windows PKI from the Surfnet PKI failed to fulfill these criteria at that moment in time.

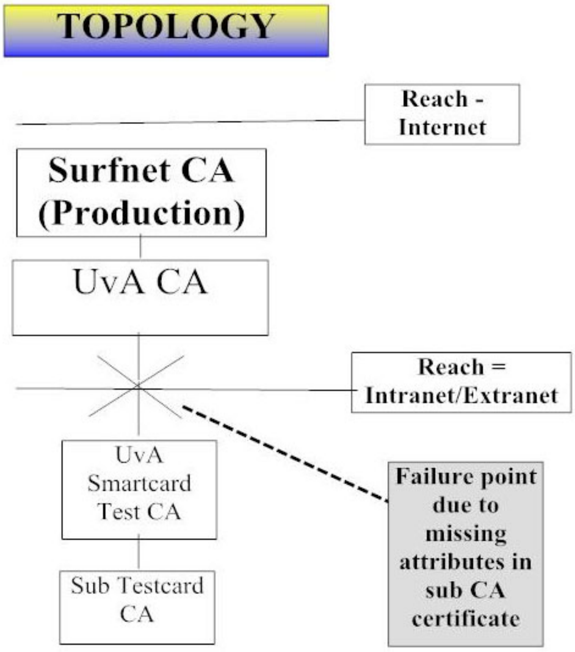

Figure 1. Topological diagram of planned Infrastructure and the final outcome due to certificate revocation issues.

After accepting this diminished structure we tested functionality under Windows 2000 forest. The forest contained 35,000 fake users and four mail servers. The fake records were synchronized with an LDAP server via a Metadirectory product. The author had in mind that perhaps later it would be possible to export details of the certificates from Active Directory to LDAP to allow advertisement of certificates to the outside world. However time constraints stopped the project members from exploring this issue further.

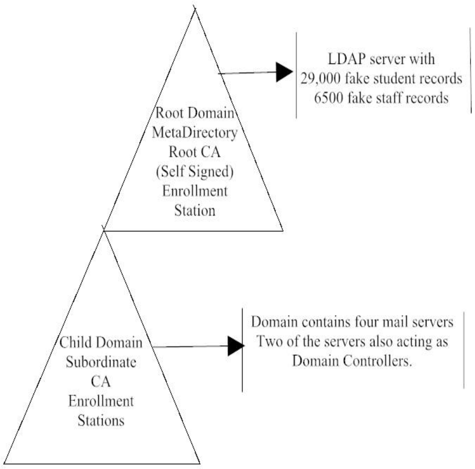

Figure two. A topological diagram of trial one as seen from a Windows forest perspective.

Middleware (by the company Safesign [6]) was also tested that allowed any standard X509 certificate to be registered within a Microsoft or Netscape browser. Further we tested the compatibility of use of certificates with an Apache/Linux combination IIS/Windows series.

The middleware fulfilled expectations allowing the users certificate to be registered in the web browser. The users were able to login via SSL to both Apache and IIS web servers, the web servers certificates were generated from the self signed authority, the logins worked. For the Apache web server (version 1.39/2.ox) the Certification Revocation lists needed to be downloaded and installed by hand for the server after the expiration of the previous list. The automation of this is a scripting chore

Main conclusions of trail one.

The main conclusion from trial ONE was the one mentioned over Certificate Revocation Lists. Without the correct CDP and AIA attributes in the subordinate certificate authorities certificate smartcard logon within a windows forest was impossible. A second conclusion of importance was that the middleware software for allowing the registration of the certificate in the Internet Explorer browser worked efficiently in every windows environment except Windows XP.

Overview of trail two.

Trial two was user orientated. How would users interact with smartcards. What would they find useful and not? What were the main costs and pressures bubbling up from a user study. To limit the extent of the trial and allow for good contact between the technical group and the poor humans that may need to use this technology the user set was made as minimal as could be considered realistic a group of around thirty users were chosen. It is no coincidence that this number is comparable to the user set of a middle size LAN.

The main conclusion from this experiment was that the end user could see the point in the technology and is in general looking forward to an extension of services at the appropriate time. This is very encouraging, suggesting that the technology is ripe for implementation. It would only take a small push to take this tool further and into a LAN environment.

User feedback from trail two.

The following lists intention is to give you an idea of the type of issues that a users within the trial considered relevant. The list is not too long as the trials ran smoothly and in this case no news is good news.

Issue: *Maximum transfer rate from the shop is limited*
This was to do with sitting behind a packet filtering router.

Issue:*After a certain period the connection would break.*
We believe this was to do with the download time for large files.

Issue: *Too many pop up warnings.*
This was to do with the lack of the self-signed root certificate existing in the root store of the users computer. It is also sometimes the result of extra security options being set in Internet Explorer.

Issue: *The Apache server failed once*.
This was an issue where the administrator of the server (the main author in this case) failed to copy the current certificate revocation list to the Apache server machine.

Issue: *Why do I get a blue screen of death?*
The middleware drivers do not behave stably on some laptops that run windows XP. Older versions of the drivers had no issues.

Issue: *The plastic card was damaged in my wallet.*
The quality of smartcard printing was good, but not at the same quality level as bank machine cards.

Issue: *It takes longer to log in than normal.*
The initial handshaking of an SSL session takes a little bit more time (around 20 seconds) than basic authentication. This factor needs to balance against the value of increased security.

Discussion

The authors feel that the pilot has been very productive. It is sometimes hard to put into words the emotion of knowing how a complex system behaves, not just theoretically but in practice. The Windows2000 PKI has a definite personality that has to be treated in exactly the right way. It does not like patching and has to sit correctly in a hierarchy and behave best with systems with a like mind or in this case a like OS and then it performs well. Therefore the overall conclusion from the author is this technology is still best tasked for intranet/extranet environments with a homogenous software background.

The logon to IIS 5, IIS 6, and Apache 2 and Apache 1.3 servers had no real technical issues and worked smoothly. It is of course a little problematic to maintain an Apache machine in this scenario than an IIS server due to the need to physically copy certification revocation lists and generate hashes every other week, but this can easily be automated.

The end user trial showed a positive response from the users point of view the installation of the middleware was not difficult and the use of the smartcard reader was intuitive. This fact came as a positive surprise as one would expect a certain degree of fouling with device driver installation. The main issue encountered was that of an extra delay in logon time compared with basic authentication, but this was not considered more than a minor annoyance.

From the administrator's perspective, the sensitivity of the Windows environment to patching and compatibility to versions of itself and open standard software has been seen throughout the trials. The infrastructure worked well when tasked with the well-known responsibility of generating client certificates. Printing smartcards was a chore and the administration associated with printing letters and restoring pin numbers is quite high. The administrative burden of distributing and maintain smart cards and their associated certificates are the stumbling block to wide scale deployment.

Conclusion

In conclusion the project highlighted a number of technical barriers, which were overcome or diverted around. The project has been useful for knowledge building and dissemination and we have gained a real insight into the properties and the habits of an advanced Windows 2000 PKI.

Smartcard technology is ripe for use if implemented with realistic expectations and methodology.

Acknowledgements.

I would like to acknowledge the user group of trial two who suffered a series of fulfilling and satisfying technological glitches.

References

[1] Technologieverkenning PKI-chipkaarten
http://www.gigaport.nl/netwerk/access/ta/ne_pki-kaart.html

[2] Projectvoorstel toegang SURFdiensten
http://www.gigaport.nl/netwerk/access/ta/pki/uva/

[3] A certificate compatibility test between Apache + mod_ssl and Windows2000 certificate infrastructure.
http://www.gigaport.nl/netwerk/access/ta/pki/uva/uva-apache-w2k.pdf

[4] Provisional Report Smartcard PKI experiment UvA http://www.gigaport.nl/netwerk/access/ta/pki/uva/uva-pki-tussenrapport.pdf

[6] Safesign homepage
http://www.aeteurope.nl/html/safesign.html

[7] Windows 2000 PKI introduction
http://www.microsoft.com/technet/treeview/default.asp?url=/technet/prodtechnol/windows2000serv/evaluate/featfunc/pkiintro.asp

[8] Problems Installing Certificate Services After You Apply the Q323172 Patch
http://support.microsoft.com/default.aspx?scid=kb%3Ben-us%3B328595

[9] Apache homepage
http://httpd.apache.org/

[10] Microsoft Windows homepage
http://www.microsoft.com