



Testimony of Neville Pattinson
Director of Business Development, Technology and Government Affairs
Axalto, Inc.

Before the
Subcommittee on Oversight & Investigations
House Committee on Veterans' Affairs

October 6, 2004

Good morning, Mr. Chairman, Congresswoman Hooley and members of the subcommittee. Thank you for the opportunity and privilege to testify today at this hearing on Smart Card initiatives at the Department of Veterans' Affairs.

My name is Neville Pattinson and I am Director of Business Development, Technology and Government Affairs at Axalto (formally Schlumberger Smart Cards and Terminals prior to our IPO in May 2004). Axalto, which is based in Austin, Texas, is the largest supplier of Microprocessor Smart Cards. I have been directly involved with identity systems utilizing Smart Cards for over seven (7) years. In 2001, I was appointed as the Common Access Card Program Manager for Axalto and tasked to deliver the Department of Defense with their Java based Smart Cards (CAC). I led the effort that achieved the first ever FIPS 140-1 Level 2 certified Java Card along with achieving the demanding card body security and durability specification required by the Department of Defense. Axalto has now supplied over 5.5 million cards to the Department of Defense and several other government agencies via the GSA Smart Card prime contractors.

In addition to my position at Axalto, I am a Certified Information Systems Security Professional (CISSP); Chairman of the OpenCard Consortium; Board member of the International Biometric Industry Association (IBIA); an active member of the Smart Card Alliance and am an active member of the International Association of Privacy Professionals (IAPP). I am also honored to be representing a loose coalition of the three leading Smart Card manufacturers called the American Smart ID Card Alliance, which is a strong voice for security, privacy and efficiency of this technology in ID management.

Identity Management System Experience

Both Schlumberger and Axalto deployed identity systems throughout the company utilizing Smart ID Cards in order to secure our information, networks and facilities. We learned that implementing a corporate-wide identity system had several benefits. Our company realized that the information we managed – both ours and our customers' – was a valuable asset that required tight security and access control. Historically, our employees were required to maintain several username and passwords to access the many systems and facilities. Each independent system was enrolled separately and had its own administrator and community of users. Our employees ended up having to

maintain multiple “identities” – which was not only cumbersome, but totally inefficient and ultimately not secure. By implementing an enterprise-wide Identity Management System, all employees’ identities were managed centrally. Each of the legacy independent systems was then converted to use the Identity Management System as the only user authentication mechanism. By specifying standards across the enterprise – from physical access systems to desktop computing standards – we were able to migrate the company to an unprecedented level of global interoperability in less than two years. This allowed us to use the same corporate Smart ID Card badge for every level of employee. This system was based on similar technology to that deployed by the Department of Defense for authentication and access to any computer or facility in our multiple locations worldwide.

We have also seen a much higher degree of accountability as we use digital signatures on our e-mail to verify our content and maintain accuracy of the information. Secure communications are also possible when we use the encryption capabilities on top of digital signatures.

For example, when an employee terminates, the quick revocation of their credential becomes possible by informing the Identity Management System, which in turn disables access by that individual to all company resources – including building access control or logical access to computing or network services.

Identity Management Systems

Identity Management Systems are very beneficial when a centralized directory is maintained. An Identity Management System includes the:

- application to join the system by a user;
- enrollment of the individual;
- issuance of the credential and Smart ID Card; and
- management of the credential.

Without such a System in place, the security and interoperability of an enterprise is likely to suffer and add complexities and difficulty in securing all the issuance stations.

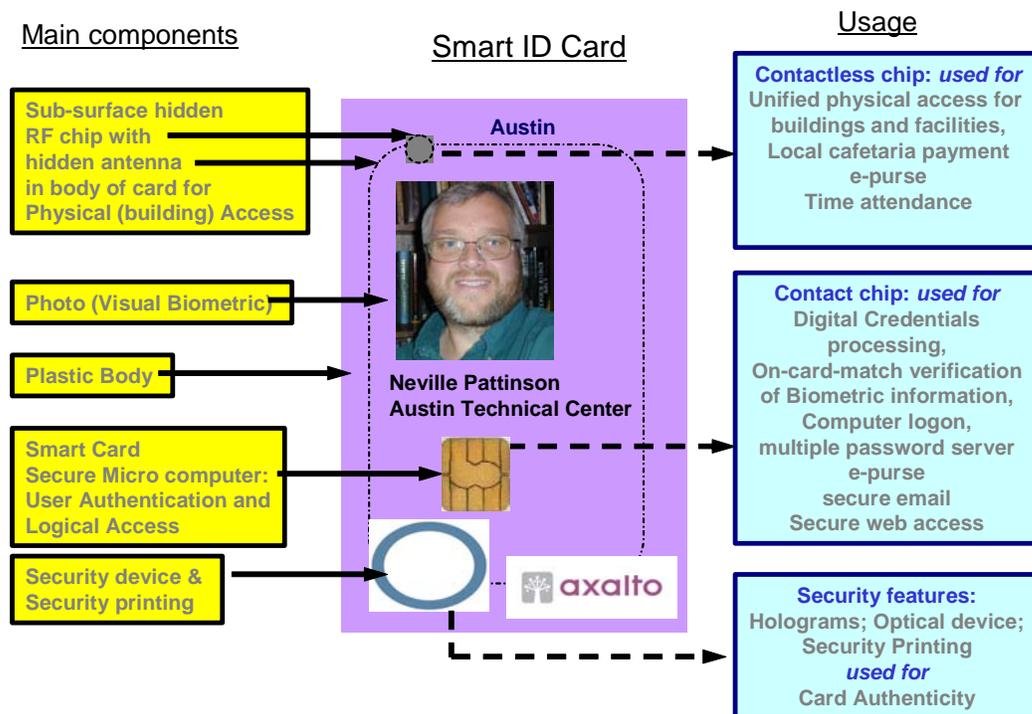
Physical access systems have traditionally been standalone implementations that cover a building, or a collection of buildings on a site. There is little connectivity of these systems over geographical distance or within corporations. It is also necessary to view physical access control as the responsibility of the local security officer, granting access rights to visitors from other locations by using their corporate identity and their Smart ID Card. However, the access rights to logical computing and network services should be done on an enterprise-wide scope ensuring a consistent and secure approach.

Smart ID Cards are a vital link in the chain of trust of an Identity Management System. They combine several security technologies into one convenient form factor. They are the local security agent of the issuer in the hands of the card-holder. Smart ID Cards consist of a physical badge in the shaped of a plastic card that incorporates several features such as visual security devices or printing, a tamper resistant Smart Card chip for logical access plus credential storage and optionally a second or possibly a third device for contactless RF physical access systems. Typically a photograph of the card-

holder is printed onto the card along with other identifying information such as affiliation, expiry date, name, etc.

Figure 1 shows a typical Smart ID Card for visual, logical and Physical Access authentication & usage.

Figure 1. Smart ID Card Overview



Benefits

Some additional benefits that have been seen after deploying Identity Management Systems are:

- Support desk cost reduction for resetting forgotten passwords;
- Increased physical access security and access control of employees;
- Decreased costs in operating multiple different physical access systems
- Highly secure access to IT infrastructure both locally and remotely via Smart ID Card enabled VPN connection; and
- High accountability, data integrity and confidentiality of users in system – for example, users can be certain of who sent an e-mail and also determine only specific users who are able to read the e-mail on arrival.

Other Benefits

- Smart ID Cards are privacy enhancing. The technology, when used in conjunction with defined best practices, will significantly augment an Identity Management System and protect the privacy of the users.
- An Identity Management System can assist organizations with HIPAA compliance, for example. Accountability of users, along with maintaining privacy of patient information, can be achieved with a comprehensive Identity Management System.
- Biometrics offer a strong mechanism for initially identifying a user (one-to-many matching) and subsequently verifying the user (one-to-one matching). When biometrics are combined with Smart ID cards they can support both types of verification. In Texas, to reduce fraud, a Medicaid pilot is using match-on-card fingerprint technology to authenticate the identity of individual as the receiver of the benefits.

Veterans' Affairs Identity Management System Implementation

We commend the Department of Veterans' Affairs for embarking on its own Identity Management System using Smart ID Cards for its employees. As there are already legacy physical access systems in place in several VA facilities, the project has embraced both a two and a three chip Smart ID Card. Both Smart ID Card variants are to contain a contact smart card chip for logical access and credential storage along with a second chip for new physical access systems as recommended by the IAB. One of the card variants will also contain a third chip for supporting the installed base of existing physical access systems based on RFID technology.

The Smart card project team within Veterans Affairs has spent considerable time performing feasibility studies and prototype evaluations in many areas to ensure the correct application of the technology to their systems and processes. This planning effort will lead to a better implementation as the project begins its rollout to the intended VA staff and contractor population. What they have learned will also benefit other agencies in their programs as all Federal agencies embrace the new HSPD-12 credentialing initiative.

Recommendations

It is important to define the scope of the Identity Management System along with specifying system-wide standards, specifications, privacy and security policies to ensure interoperability, consistency and proper usage. One should use standards and open specifications avoiding blind alleys or non-interoperability. It is important to define the criteria for enrollment, and the user authentication mechanisms once enrolled. A common data model is also important to ensure interoperability. Any project should first conduct a pilot, then revisit prior to commencing the enterprise-wide deployment. Once established, the Identity Management System will require maintenance and enhancements over time. I would recommend any program follow the well-proven: *“Plan, Do, Check and Act”* approach to implementation.

The usage of PINs along with Smart ID Cards is a good user authentication mechanism to determine user presence with the card. However, as biometrics become more established and the application determines the need to increase the authentication of the user, biometric authentication should be introduced where appropriate and cost effective as either a replacement or addition to the user’s PIN.

Summary

Smart ID cards are a vital link in the chain of trust of any Identity Management System. The ability to master identity management within an enterprise or government agency brings tremendous savings, electronic communications security, user accountability, increased privacy and consolidated access control. Smart ID Cards are a convenient, proven, portable, cost-effective highly-secure technology for assisting with the management of identity. When combined with biometrics, the Smart ID Card offers a strong three-factor authentication of the card holder with: (1) Something they have (card); (2) Something they know (PIN); and (3) Something they are (biometric).

There is a wealth of experience within US Government agencies in deploying Smart ID Card-based Identity Management Systems. The Inter- Agency Board (IAB) and the Federal Identity Credentialing Committee (FICC) have also endorsed Smart ID Cards. The efforts to create the Government Smart Card – Interoperability Specification V2.1 by the National Institute of Standards and Technology (NIST) and the recent Homeland Security President Directive (HSPD-12) declaring an aggressive timeline for all federal agencies to implement a “Common Identification Standard” – makes it clear that interoperability is paramount for any government agency Identity System.

Thank you for the opportunity to testify before this distinguished subcommittee. I look forward to working with the members of the subcommittee in providing any help and guidance on this issue.