GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials: Network, Endpoint, and Cloud (Security 401)"
at http://www.giac.org/registration/gsec

Meeting the Challenges of PKI Implementation

GSEC: Assignment Version 1.4b (July 2003)
Option 1

James P. McNellie

December, 2003

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

ABSTRACT

This paper will explore Public Key Infrastructure (PKI) initiatives as they pertain to the US Government, and corporate entities. The goal of the paper is to examine the challenges of the US Government PKI smart card rollout, and several e-commerce PKI rollouts. Included in the research is an examination of interoperability, risks undertaken, costs, and successes and shortfalls of the implementations.

PKI Background

In its most simplified form, Public Key Infrastructure (PKI) represents a delegated identification management system that uses public and private cryptographic key-pairs for its security foundation. Historically, before 1976 and the discovery of the Diffie-Hellman algorithm, a shared, secret (symmetric) key was used for cryptosystems. The major problem with this system was the management of the one key used, and in particular, the delivery issue, so the recipient of the one secret key could share the key with the sender. The same key was then used for both encryption and decryption, so the key had to be in the possession of both sender and recipient. A major shortfall was that the key had to be distributed privately, therefore protected from compromise.

The basic principle of a PKI is that it is a security system that encrypts and decrypts using openly accessed Public Keys with secret Private Keys. A Public Key is “public” in the sense that it can be displayed on a public-server using a directory such as the Lightweight Directory Access Protocol (LDAP) or sent to a recipient by email or delivered otherwise. A Private key is the “critical” secret key, used for decryption, and to sign a message using, for example, a digital signature such as the SHA1 or MD5 algorithms. This Private Key is never revealed to anyone.

A Public Key system or PKI uses asymmetric algorithms so that the key used for encryption is different from the key used for decryption. The algorithms are called “public-key” because the *encryption* key can be made public, whereas the *decryption* key must be kept secret. (Schneier, p. 4) The PK Infrastructure is a collection of databases, services, applications, protocols and standards that surround the use of digital certificates for secure communications and data storage. Defined as an infrastructure, a PKI can be used for a variety of purposes. It is standardized, relatively easy to use (a large benefit is its transparency to the end-user) and it should be cost-effective (Fossen, P.16). [1]

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

Critical to the PK infrastructure is the Root Certificate Authority (Root CA). For example, the DOD system, under the sponsorship of the NSA, is responsible for delivering the mathematically related key-pairs to end-users through subordinate Certificate Authorities (CA)—worldwide DoD bases. A Local Registration Authority (LRA) can assist in administrating the Certificates; these LRAs also fall under the system hierarchy.

The certificate, an X.509 v.3 standard, is then delivered to the end-user as the digital equivalent of a paper certificate (e.g., a passport or a driving license). The CA, forms the basis of a hierarchical designed "trust model" or a chain of CAs that lead back to the Root CA. The Certificate Authority is based on a "contractual" trust model that can identify the end-users with certainty, and issues these keys for the principle of secure information exchange. The CA issues Public Key (PK) certificates that contain a host of digital security information and the keys are based on complex mathematical algorithms. These algorithms, as one example, use a series of instructions designed by manipulating factorization of very long prime integers, which equate to the long rows of digits or "keys" in the end certificate product.

The issued Certificate stores the public-private key pairs; however, the keys or encrypted integer files are kept in separate files. The public key is actually the certificate referred to as a "digital certificate", and it "binds" the identity of the end-user to the certificate. The separately filed Private Key is used primarily for decryption and digital signatures.

Some of the information contained within the public certificate contain the CA that issued the certificate, the identity of the owner, the algorithm used, the hashing algorithm used for digital signing in secure emails (S/MIME v.3) and the dates of the certificate validity. The certificate is then signed by the CA to prevent fraudulent usage. The private key is included but is not an integral part of the public certificate. [2]

PKI is composed of many functions. This multi-factor relationship adds to its technical architecture. The pertinent elements that PKI provides through its certificate scheme are: Confidentiality, Integrity, Authentication and Non-Repudiation. Besides the CAs and the digital certificates mentioned above, key management principles, session keys and hybrid encryption methods are important components that enable the entwined technologies to communicate and interoperate for the purposes of crypto-system security. [3]

Additionally, PKI is a consistently evolving security process in government and e-commerce. It has greatly reduced the problems of key management that plagued the cryptography community for decades. PKI integrates digital identities and signatures, presents an end-to-end trust model, and shapes a complicated architecture. The

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

main disadvantage of Public Key technology is its slow speed, so it is used for its effectiveness in “encryption” rather than “decryption”. PK systems will speed up as computer processors speed up and will possibly reach symmetric cryptography speeds—eventually; however, as bandwidth increases, the need to encrypt data faster than public-key crypto systems will always be there.

As the multi-factor e-commerce sign-on market continues to turn more and more towards PKI technology, the crucial pre-stages of planning, user training and e-business interaction will bring interesting challenges to global governments and e-Commerce alike.

U.S. Department of Defense (DoD) Implementation

A PKI e-security system can be a large-scale design. The U.S. government’s DoD is progressively facing malicious attacks from various sources worldwide. The leading challenge of a large-scale implementation of an e-security rollout in this malicious culture is to protect data communication as it crosses widely dispersed and insecure networks that have been plagued with an increased volume of “malware”. (Skoudis, 2004) While DoD strengthen up their network defenses, Internet attacks on Business-to-Business (B2B) networks are causing escalating costs attempting to realize their return-on-investment (ROI). While B2B ventures suffer, The U.S. Government, and DoD in particular, have been spending millions of dollars to seek secure advantages on a much larger scale of operations.

PKI seems to be moving forward in the last few years compared to the near stagnation and the considerable commercial criticism of the 90s.
The single-factor, User ID/password sign-on, continues to wane in popularity since it has been noted as a weak, ill managed, overdue and ready to-be-replaced security method. PKI is an important part of a multiple-factor sign-on method and had been more or less “heard but not seen” before the 9-11-2001 U.S. terrorism disasters. Now it is an e-security design that is once again being favorably planned and implemented in many large-scale enterprises, such as within the U.S. government.

Most end-users desire non-technical, with as little change as possible, and applications as non-complex as possible to complete their work. The implementers of PKI are attempting to make their initiatives as a more robust security system that has these end user features. [4]

With advances being made in e-business open standards and interoperability, DoD has been more frequently utilizing commercial-off-the-shelf or COTS technology, thereby forming much needed alliances with commercial public-key corporations and vendors. Companies like RSA, VeriSign, and Sun Microsystems are bidding for DoD contracts on cooperative projects that look for solutions to communicate safely over emergent, insecure networks.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

While the discussions for the issue of a PKI standard are ongoing, aside from RSA's Public Key Cryptography Standards (PKCS), a global standard has not yet appeared on the horizon. However, the DoD is actually leading the way, partnered with the National Institute of Standards and Technology (NIST) and the NSA. Through its well-known "closed-system" with large segments classified or behind military (.mil) firewalls, for national security reasons (e.g., personnel troop strengths, deployment data, and sensitive planning data)--the DoD continues to push forward its mandates for PKI implementation.

DoD CAC Initiative

Furthermore, the DoD as the largest investor in PKI technology, with the number of personnel stationed worldwide comprising nearly 4 million active duty USA, USAF, USN service members, family members and government contractors, has tested forms of PKI since the early 90s. Specifically, a DoD mandated priority project started in 1993 that has focused on smart card technology. DoD's Common Access Card or CAC has followed US corporations such as finance, healthcare and insurance industries into smart card utilization [5].

So what is this Smart Card or Common Access Card?

The CAC is an updateable, individually carried data storage device, credit-card size with 32-64kb of memory that runs at near 1–Mhz processor clock speed. With Java Card Runtime Environment, it is interoperable, backward compatible used for secure communications online through a card reader; and shares a barcode, a magnetic stripe and it's the Defense Department's "new age' or "new century" Standard ID card that will have embedded in it health data, biometric identifiers and much more. These devices have been used in many institutions including: Global systems for Mobile Communications cell phones and financial services, and have been in use in Europe for many years. Eventually, over 4 million DoD personnel will receive the smart cards. The CAC "token" hardware, as it is referred to, will form part of the overall strategy adopted by the DOD community--one of "Defense in Depth" in which PKI is one of the important supporting infrastructures involved. [6] Once totally implemented, all unclassified e-mail transmissions through DOD channels will require encryption and a digital signature through a '2-factor' authentication online.

Digital signing and local sign-on will be provided by the CAC. It can be standardized to contain the certificates (e.g., three: one each for identity, e-mail signature, and e-mail encryption) and the critical private key for secure authentication within the PKI. In addition, e-commerce compatibility using LDAP and X.500 Directory Service standards are being used throughout the PKI.

Government Pilot Programs

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The first PKI CAC Pilot, was distributed to Defense and Accounting Service (DFAS) for secure Web access at selected sites in Hawaii. PK certificates were downloaded and the pilot was expanded to integrate, and store PK certificates and encryption keys in a prototype of the new DOD CAC format. The benefit was the feasibility of integrating both electronic facility access control and computer system authentication, and encryption functions to a smart card token. This was first accomplished on a small-scale only with Pilot programs.

The large-scale DoD CAC-PKI rollout had not been without challenges—in particular numerous delays. A major implementation challenge soon occurred when the ID/CAC project was expanded, with a "no later than" deadline set to Oct 2003—this occurred after a previous 2002 delay. However, as recently as the summer of 2003, a senior DOD official again recommended that DOD extend the deadline date to spring of 2004. It seemed that when all the conditions of site administration were taken into account, the sheer volumes of personnel in Europe, Asia and other remote sites, either without local RAs to service their accounts, or due to the sheer numbers to schedule. These multiple factors drew the large project to a slow-down.

Still, the government program managers continued to signal avid interest in looking toward the next stages of PKI technology. In *Government Computer News*, Dawn Onley remarks that mobility in the field is a major issue with how troops are mobilized using PKI technologies. Other comments settled upon issues containing the smart-readers and middleware—which have now been settled. "*You still have to think about other security measures, you still have to lock down your operating systems and have personal firewalls; we need overlapping layers of protection,"* remarked Jim Degenford, PKI Program management office advocate. In the same article, he commented that the next version of PKI would be "more hardened" with biometrics soon to be added [7].

To date, a few of the successful smaller scale PKI Pilot programs have been:

- The Defense Travel Service (DTS): using PKI certificates to authenticate users, control system access and identify travelers. Digital signatures are used for approval of travel orders; expenses vouchers and protect the integrity of all financial transactions.

- The military Absentee Voting over the Internet: This program was a shared federal, state, and local initiative that involved the states of South Carolina, Florida, Texas, and Utah. The PK certificates provide a trusted model for identification and authentication of voters; and integrity and confidentiality of all systems transactions, used in the 2000 General Election. Though the

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

results were small scale the tests were contributed to larger voting systems and Internet-based registration.

- The Defense Message System-Medium Grade services (MGS): Part of the larger DoD mandate to upgrade service and security for all electronic mail sent within the Department. MGS integrates COTS e-mail products that meet Government security standards for information security. The aim is to benefit large groups of users in specific geographic locations to register and begin using PK certificates in their daily business. High–grade services, for example are a higher class of PKI certification (Class 4) and use stricter requirements in their key usage and protection.

Pilot programs continue to be a focus in the government, as the Defense Department announced in June 2003 that it would begin accepting proposals to test methods to streamline information technology. The funding of the acquisitions is through a central pool of money and the program will support development of commercial products to shorten the deployment time to field the systems.

Some other Pilot program examples are: the US Navy's e-business pilot project program funding and the Service Deputy Surgeons General for Medical Appointments on the Web program at a cost of $2million. [6] One of the primary challenges of these programs will be the interchange of information between them. That is, the interoperability hurdle that the independent pilots were able to overcome. Also, will the PKI deployments use the same standards? And will systems have similar vendor equipment? Another issue will be the certificates accepted since the Pilots may be using a different "chain of CAs" in their structure? As the PKI technology continues to improve and evolve, these and other dilemmas should be simplified.

The largest DoD CAC project (i.e., the ID Management system) is now due to be completed in the second quarter of 2004. Interoperability was the big winner in the Pilot successes as challenges were met, and commercial technology was integrated with government requirements, thus enabling military and DoD custom applications. However, the major task of the immense and global PKI/CAC rollout with worldwide DoD responsibilities will be to meet the longer-term cost-to-benefit challenge, the geographic-logistic mission coverage issues and the essential progress to stay ahead of hi-tech evolution in today's accelerated Public Key market.

If eventually successful, an outcome could easily be envisioned with the DoD program and its smart card implementation using two or more authentication factors (Biometrics?) in a future scenario expanding into new fronts. Veterans,

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

dependents, and millions of federal, and state workers could be issued the “smart cards” or identity cards. The technology may be put first into driver’s licenses, and union cards. On the other hand, a major challenge to the personal identity smart cards could arise with the civil liberties issue as ID management advocates foster their agenda wherever it may take them and us. That is *only* in the US, European sensitivities may arise in various European Union countries and further delay ID rollouts. Political issues could always cloud any global-based PKI standard. For example, in future conflicts using communication with allies or coalitions, will all be using the same type of authentication? One can only hope the United Nations has this for action somewhere on their “to do” list. Much work and agreement on this front will remain to be seen.

.

Other Government Initiatives

Aside from the huge DoD CAC rollout of the last few years, the US government has many other initiatives that have their goal as PKI defense. Even with the DoD forging ahead of PKI technology for their troops and dependents stationed worldwide, smaller agencies with lower outlays of funds have attempted within much tighter budgets to plan, implement and train their personnel in PKI fundamentals.

In one deployment, in October 2003, the Defense Information Systems Agency (DISA) began deploying a commercial application of its Global Combat Support System. It will provide single sign-on that authenticates identity and account management. Using Public Key technology, the system will give combat support personnel logistics data, audit, and reporting capabilities. Northrop Grumman Corporation and DISA will jointly develop the venture—providing the crucial interoperability. [8] Thus, another partnership was formed of government and e-commerce in the PK Defense arena.

Furthermore, the government has set into motion a Gateway—the *e-authentication Gateway*--that has been initiated so any type of sensitive or personal data can be securely supported. Users of all types of e-business with the government can then use the Gateway to validate end-users identities and credentials. Finance, Healthcare (the HIPAA initiative), the IRS tax office, and the FBI, to name but a few are included within the E-Authentication Gateway. However, similar to the DoD’s large CAC initiate, the e-Authentication has also met delays. The rollout deadline has now passed and the administrators are looking toward a March 2004 deadline at this time. [9]

Other government agencies such as the FBI have formed a contract with Northrop Grumman and Entrust Inc., this year to provide Public-key infrastructure

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

for authenticating FBI personnel for access to electronic systems and secure information exchange among intelligence agencies. Subcontractor, Schlumberger ltd., a contractor that has worked with RSA on the DoD CAC rollout, will also work with Northrop on this $4 million program. The President and chief executive officer of Entrust, in a statement, remarked," *They have set an aggressive timetable to develop and deploy a secure PKI architecture that meets the IT security needs of their dedicated staff while also aiding to combat the growing threats against our citizens."* [10]

On a personal note I think this statement sounds very similar to the post-mandated statements made by officials after the DoDs large-scale implementation; however, their much smaller size is an advantage. In the near term, we should see if PKI is the InfoSec system that will grow in demand in *sma*ll as well as *large* government agencies.

E-Commerce or Business-to-Business (B2B) PKI Implementations

The US Government has a major advantage of size when it comes to any type of comparison with today's daily e-business or e-commerce markets. It also has large budget outlays that most companies could scarcely afford, or discuss, let alone to consider any portion to spend on PKI security systems--except possibly one of the top 10 on the "Fortune 500" list. Another advantage of a DoD type large-scale initiative is in using a "closed" Chain of Certificate custody where the Root Certificate (DoD) or "Trust" model is known to all end-users-by design, and where all users usually know who they are dealing with.
Outlined below are a few DoD and B2B similarities and differences.

B2B is contrasted by primarily using an "open system" such as the e-commerce transactions online where business clients may be unknown to the corporate entity selling their products. Likewise, in a B2B transaction, a client would be charged a fee to acquire a Certificate from a CA to do business—unlike the members of a closed DoD network. This is in the form of a digital certificate cost from a "*reputable"* Certification Authority. With this transaction, a liability cover is incurred that has been called a 'relying party agreement' and sets out what standards of care the CA has used, what liability cover they are providing and where they really are if you want to visit them or sue them. [11]

A question then arises: can a reputable CA be counted upon to pay liability costs? Or is legal counsel a good idea in this situation? No standards seem to be in place at the time of this writing, so CA liability remains a "sticky" point that will take some time before it is resolved. So, as in other markets--let the "buyer beware." DoD, with their 'closed' architecture, has no comparable liability to note since their CA "Trust Chain" is a permanent, government, and mostly restricted system with end users (within the system) paying no fee.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

So, even with major differences such as size, costs, and considerable differences in CA chains, there remains one primary factor—that of secure communications on 'untamed' and potentially malicious networks that *do* put DoD and B2B on an equal footing. Defense in Depth" is an equalizer that drives both B2B and governments everywhere to seek out a secure PKI. Government and e-business are looking toward continuing evolving standards to use for dependable Internet security, and both are currently fostering closer partnerships in the war of information warfare.

Since B2B evolves increasingly around purchases online with credit card transactions, then it's always a good idea to know whom you are dealing with in any website purchase--just as you would know your financial institution when you use a Pin number and bankcard at an ATM. One secure method used online is through Secure Sockets Layer (SSL) encryption that has been around since the first days of the Internet and has been used by almost all successful e-commerce enterprises to keep data private and out of malicious attacker's reach.

Authorization in B2B is similar to the government's method since Access Control Lists (ACL) are used in both to authorize certain users to use only certain accounts, and only with definitive user-rights to specific files and folders. In B2B, financial accounts wouldn't be viewed or modified by, for example, Human Resource personnel, so "access" is important in both government and B2B. In addition, confidentiality, integrity and non-repudiation are equally pertinent to all forms of PK systems used in e-commerce.

The benefit of a strong *authentication* factor is paramount to e-security. RSA Security, Inc. remarks that the real key to e-business security is *authentication* that positively identifies and proves the authenticity of those with whom you're doing business. Without authentication, other authentication measures that are implemented can be ineffective. Allowing for the increased costs, a B2B PKI can provide end-to-end authentication in comparison to the single-factor password and its difficult management that have become ineffective.
Why? Humans tend to "weaken" passwords thus making them relatively easy to guess, steal or crack. RSA adds that the more authentication factors you use, the more certain you'll be that users are who they say they are, and with a token or smart card combined with PIN protection, (2-factor) much like an ATM transaction, then the more secure the online transaction world will be. [12]

Both DoD and e-business smart cards protect their private keys by never letting them leave the token cards. In like fashion, the smart cards combined with digital certificates (the Public Keys) produce an even stronger level of authentication. Smart cards in the B2B sector have been used for decades, and the usage is increasing in other, new sectors. Europe and Asia are the leaders in this area as end-users have used smart cards for banking, mass transportation, patient requirement cards, terminal usage in mass retailer stores [13], and employee

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

access control, amongst other methods. The U.S. usage is growing as witnessed by the widespread DoD PKI CAC project and emerging government pilots.

In the e-commerce world, PKI doesn't seem to be for everyone. DoD can spend large amounts of funds for a national defense posture, unlike medium to smaller B2B ventures. In contrast, web commerce is driven by costs and the bottom-line of Return on Investment (ROI) that is critical to keep a company lucrative. A PKI investment for medium to smaller companies can be typically restrictive, yet expensive all important e-security defense costs must rise in the present abusive Internet environment. Further funds will need to be spent amongst vendors to cope with PKI's basic constraints of ensuring validity periods and Certificate Revocation Lists (CRL) are correct.

As PKI technology takes off further, U.S. companies are taking examples from their European and Asian partners. A few examples follow: Cylink Corporation deployed its NetAuthority PKI to act as the certificate authority for the U.S. Postal Service's NetPost. Certified in 2001, the Internet-based service protects and authenticates digital exchanges among government agencies. Entrust Technologies, Inc. was involved in an arrangement back in 1998 with the Government of Canada and the Republic of Singapore that coordinated e-commerce policies bases on Public Key systems. Interoperability was a prime focus as the two countries agreed to work to enable secure, authenticated transactions for businesses, governments and individuals. Entrust's initiatives are being used by the United States Patent and Trademark Office. [14]

Summary

PKI implementations in government and in e-business are growing, and rightfully so with the Internet attacks prevalent today. Privacy legislation and the issue of identity cards worldwide seem to be permanent issues in the media. From asylum seekers to increased vigilance due to terrorism, strong security is being aggressively sought throughout society, government and Business. E-security in the strongest form of Public Key Infrastructure continues to evolve through lower costs, decreased complexity, end user transparency, and PKI-ready applications that are appearing in IT sales. A weaker form of e-security, user identity and passwords, provides authentication—in a much less secure form and can't evolve. [15]

To date, PKI has *not* been without its delays, criticism and human errors. It will most likely continue in the future. As Information Assurance Managers seek lower costs and better standards, civil rights, privacy disputes and e-security choices will be subjects of contention and compromise. Change will be necessary as the leading PKI market vendors ensure that their products interoperate, and that greed and propriety don't dominate the much-needed e-security.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

The PKI arena will have to move to medium or smaller projects in both government and civilian business ventures. Hopefully, research and development, and a good marketing program will continue to assist progress in this area.

Moreover, PKI progression should be helped by the health care industry and its compulsory HIPAA compliance for data privacy.
At the same time, company and government investment in smart card technology is helping to make token usage a more permanent fixture in modern society. This should substantially improve e-security and the future case for PKI. B2B companies can then ask themselves if the cost of a strong PKI is long-term beneficial versus a lesser cost and ineffective security.

The objective of e-security is the continuous search for a total “Defense in Depth” policy. The PKI “Trust” model will succeed only when interoperability amongst government and commercial vendors seek out common standards, and a policy to cooperate toward community benefit.

© SANS Institute 2004, Author retains full rights.

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

General References:

1. Schneier, Bruce. Applied Cryptography. New York: John. Wiley & Sons, Inc., 1996.

2. Skoudis, Ed. Malware. Fighting Malicious Code. New Jersey: Prentice-Hall. 2004

3. RSA Security, Inc. Info@rsacsecurity.com. URL:http://www.rsasecurity.com

List of References

1. Fossen, Jason. Windows 2000 PKI, Smart Cards, and The Encrypting File System, Vol. 5.3. SANS Institute, 2003.

2. An Introduction to PKI, ArticSoft, 9 September 2003 URL: http://www.articsoft.com/wp_pki_intro.htm

3. Harris, Shon. CISSP All-in-One Certification Exam Guide. Berkeley: McGraw-Hill/Osbourne, 2002.

4. PKI Deployment—Business Issues, OASIS PKI Member Section, 2002. P.12.

5. Emigh, Jacqueline. Who do you trust? IT Service Management Forum. June 7, 2002. URL: http://www.networking.earthweb.com/netsecur/print.php/1355271

6. Department of Defense. PKI: Unlocking the Door to eBusiness. 2001. Pps. 2, 12-13. URL: http://www.iatf.com

7. Onley, Dawn. "Smart-card rollout might need more time", Government Computer News. July 21, 2003. http://www.gcn.com/22_19/dodcomputing/22782-1.html

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.

8. French, Matthew. DOD solicits rapid IT acquisition projects. June 16, 2003. URL:http://www.fcw.com/print.asp

9. Frank, Diane. Davis eyes E-Authentication delays", Federal Computer Week. October 16, 2003. URL: http://www.fcw.com/print.asp

10. Michael, Sara. Entrust to provide PKI for FBI. Federal Computer Week. October 21, 2003. URL: http://www.fcw.com/fcw/articles/2003/1020/web-pki-10-2103.asp

11. PKI-managing liability. ArticSoft. 2003. P.1 URL: http://www.articsoft.com

12. RSA Security, Inc. e-Security: Do you Know Who You're Doing e-business with? 2001. P.1-2

13. Smart Cards and Retail Payments Infrastructure: Status, Drivers, and Directions", Smart Card Alliance, October 2002, p.4. URL: http://www.smartcardalliance.org/

14. Armstrong, Ilena. Public Key Infrastructure from Pilot to Production. SC Magazine. July 2001. URL:http://www.scmagazine.com/scmagazine/2001_07/cover/cover.html

15. Villacres, Caline. Smartcard vs. password. June, 2003. URL:http://www.scmagazine.com/scmagazine/2003_09/feature_1/

© SANS Institute 2004, As part of GIAC practical repository. Author retains full rights.