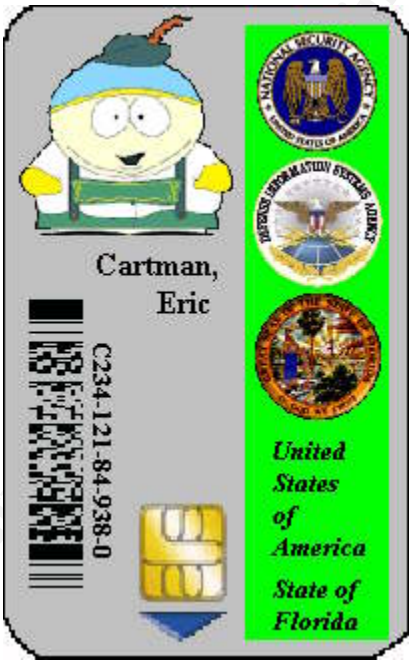
A Concept for Universal Identification

Daniel Williams

A Concept for Universal Identification



Daniel E Williams
December 13, 2001
SANS - Monday/Wednesday group
GSEC
Original Copy

Table of Contents

1.0 Introduction

The goal of this paper is to provide a detailed look at a new perspective for a unified, secure and consolidated form of personal identification. The advanced yet inexpensive technology exists today to step up modern identification to the next level. The combination of various forms of authentication with Public Key Infrastructure (PKI) can yield a versatile yet secure form of access to most anything requiring a key. Inexpensive smart cards with built in fingerprint readers are available, providing the secure storage of a smart card with a quite secure form of biometric authentication. Applications requiring increased security and authentication can use relatively inexpensive retina or iris scanners.

Recently has the government improved their identification to incorporate smart card technology. This form of identification can be used not just as a photo ID, but it can be used for secure messaging, secure web access, access to medical information and a host of other functions. The possibilities are virtually limitless.

Using the United States Postal Service (USPS) as a model, a very efficient, very distributed PKI can be designed and deployed [1]. The idea being the root CA would be controlled by the government, i.e. NSA (similarly, the DoD root CA is controlled by the NSA). Subordinate CA's (to issue certificates to the population) would be located at each state capital with local registration authorities / certificate issuance portals at every post office / zip code. Any person in America could get their certificates by going to a local post office. Consider combining the USPS with the Department of Motor Vehicles (DMV) in the same office, and you would get your drivers license complete with certificates in one shot.

This paper will describe the architecture and design for the concept of a universal identification. Privacy issues and the process towards a realistic deployment will be discussed.

[1] Tebbutt (Reference #1), Mayer (Reference #2), Alterman (Reference #4), McKenna (Reference #5)

2.0 Technology Overview

2.1 *Public Key Infrastructure*

A digital certificate is a cryptographic mechanism used to secure e-mail, secure online transactions, digitally sign executable code, and perform various other cryptographic functions. Public Key Infrastructure (PKI) is a technology mechanism, based on digital certificates, which is used to facilitate trusted data transactions. A PKI is comprised of a tree of hierarchically trusted certification authorities (CA), with the trust point for the entire system based on a single root CA. The root CA owns a self-signed digital certificate (the single point of absolute trust in the PKI) which digitally signs digital certificates for each of its subordinate CA's. The subordinate CA's then sign digital certificates for users, web servers, VPN gateways, etc. [2]

Public key cryptography is based on the idea of asymmetric cryptographic keys [3]. A key pair consists of a public and private key. The idea of asymmetric cryptography is that a private key is computed via some cryptographic algorithm, such as RSA, DSA, Blowfish, etc. The private key is then used to generate a public key. Thus, the two keys are mathematically related. The private key is kept only in the possession of the person who owns the key, while the public key is distributed to the masses. A public key can be used to encrypt an email for a user, and only the associated private key, held only by the recipient, can decrypt it. Likewise, a private key can be used to digitally sign a message, and only the associated public key can be used to verify the sender's digital signature. One would not encrypt a message using their private key, as everyone could decrypt it with the sender's public key. Likewise, one would not digitally sign a message with their public key because nobody has access to the associate private key to verify the digital signature.

2.2 *Biometrics*

Biometric technology consists of mechanisms that can read, decode and pattern a physical feature of a human being. Technology such as fingerprint scanners, retina scanners and bone structure scanners are some forms of biometric technology. Today, biometric technology is relatively cheap and is beginning to make its way into the commercial marketplace.

Biometric authentication can be extended to PKI to allow another factor of authentication, making a person's digital certificate even more secure. Typically, a user's certificate would be protected by a password or PIN number, but with biometric authentication a user can protect their digital certificate by using a thumbprint or retina scan.

[2] USPS, Section 1 (Reference #3)
[3] Curry (Reference #7), VeriSign (Reference #8), VeriSign (Reference #9)

2.3 *Smart Cards*

A smart card is a piece of cryptographic hardware used to securely store digital certificates. Most smart cards are shaped like a typical credit card or driver's license, and can easily fit into a wallet or act as a visual identification badge. Storing a digital certificate on a smart card is typically more secure than storing a digital certificate in a file on your computer because smart cards store the private key in a more secure manner. Most smart cards have a tamper-resistant rating from NIST (National Institute for Standards and Technologies), particularly the FIPS 140-1 or FIPS 140-2 certifications [4]. These two certifications have five levels of tamper-resistant ratings, from level 1 to level 5. Most software mechanisms for storing digital certificates are rated at FIPS 140-1 level 1 if at all, while most smart cards are rated at FIPS 140-1 level 1 or HIGHER (many are at level 2 and some are at level 3). The higher the level, the more tamper-resistant the smart card.

[4] NIST (Reference #13 and #14)

3.0 Public Key Infrastructure System Architecture

Public Key Infrastructure system architecture can be viewed from two angles - a physical system hierarchy and a certificate organizational structure.

3.1 *Physical PKI Hierarchy*

The physical PKI hierarchy would consist of a basic, three level hierarchy. The top level of the hierarchy would be only the root CA while the middle level of the hierarchy would be all the subordinate CA's. The bottom level of the hierarchy would be the end users, web servers, VPN gateways, etc. (end entities).

The following two figures depict physical PKI hierarchies. Figure 3.1.1 depicts the existing Department of Defense (DoD) PKI controlled by the Defense Information Systems Agency (DISA). Note, the root CA is controlled by the National Security Agency (NSA) and is housed in a very secure NSA building. Figure 3.1.2 depicts a proposed PKI architecture for civilian use.

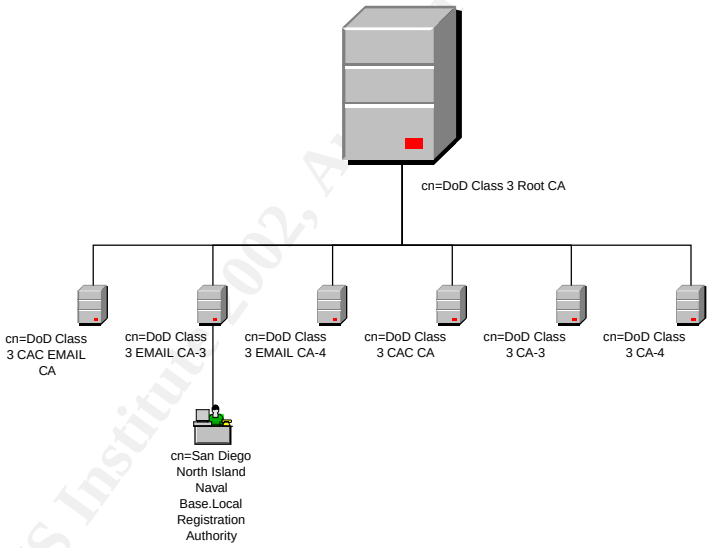


Figure 3.1**.1:** The existing physical PKI hierarchy for the Department of Defense

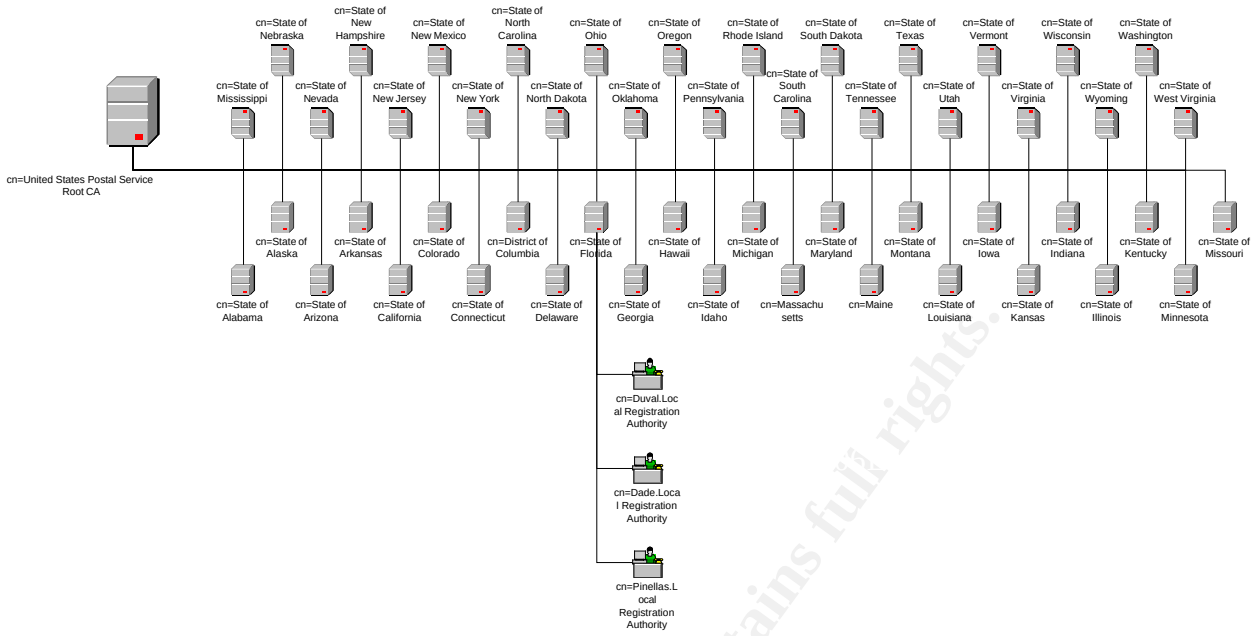


Figure 3.1.**2:** Example physical PKI hierarchy for the USPS

The example physical PKI hierarchy for the USPS depicts one root CA, possibly controlled by the NSA like the root for the DoD, and multiple subordinate CA's - one for each state and the District of Columbia. Each state has their own subordinate CA, possibly house at the state's capital, with local registration authorities (LRA) located in each county, possibly at every post office. The job of the LRA is to verify a person really is who they say they are much like when a person applies for a drivers license, they must submit a birth certificate, social security number and other forms of identification. Once a person's identity is verified, the LRA can issue a user their certificate(s).

In order to combine resources as well as an additional motivation for deploying so many LRA's, the department of motor vehicles could merge locations with the USPS so as to provide a smart card driver's license, issued with digital certificates, all in the same facility. Obviously, if the USPS controls the PKI, they must issue the certificates. However, the idea of this topic is to incorporate digital certificates and their uses with a standard form of identification such as the driver's license. Thus, the combination of these two government branches seems logical.

3.2 *Certificate Organizational Structure*

The certificate organizational structure would be a more detailed, complex hierarchy consisting of multiple levels of organization for classifying end-entity digital certificates. The levels of organizational units does not mirror the actual CA hierarchy. A CA can issue certificates with any organizational unit or distinguished name.

To convey the idea of a distributed PKI, hosted by the United States Postal Service for use among the general United States population, an example of the certificate organizational structure hierarchy is shown below in figure 3.2.1.

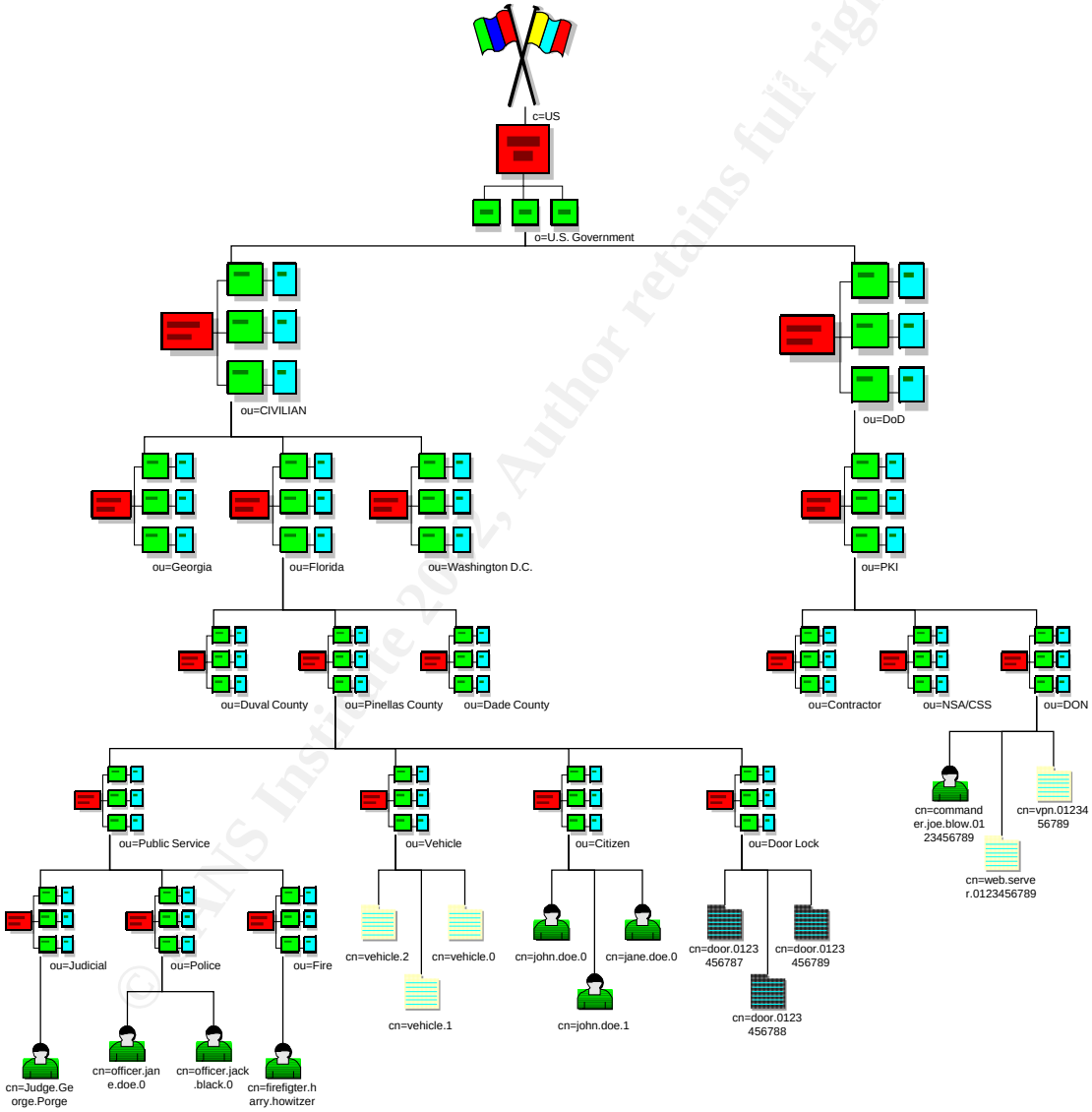


Figure 3.2.1: Example certificate organizational structure hierarchy for the U.S.P.S

The main right branch (just after O=U.S. Government) of this organizational tree is the existing DoD PKI organizational structure. The idea of a U.S.P.S controlled PKI for the general U.S. population is depicted in the main left branch (just after O=U.S. Government).

Notice the main organizational unit of the left branch is CIVILIAN, designating the general U.S. population. To further define and distribute organizational units, we can divide users into states, followed by county. Once at the county level, the tree can be branched off into several different organizational units (OU). An OU for normal residents (OU=Citizen), for vehicles (OU=Vehicle), for all locked doors in every home (OU=Door Lock) and a special OU for public servants such as police officers, fire fighters and judges (OU=Public Service → OU=Police, OU=Fire, OU=Judicial). All of these organizational units allow for very granular definition of roles in the community. For example, a police officer may be able to access a secure website because his or her certificate contains the OU=Police field.

The idea for having OU's for things such as vehicles and door locks is this - imagine if you didn't have to worry about having a key for your car? Imagine that when you first purchase your car, the combination of your certificate with the vehicle's certificate generates an encrypted key. Only your smart card can be used to decrypt this encrypted key, which is the code to start the ignition. Imagine that your vehicle could encrypt multiple codes, one for each driver in your house. Today, most car dealerships can make a new ignition key just by knowing the car's vehicle identification number (VIN) because the blueprints for each key are stored in their computer system. This capability can be updated for PKI by having the car dealership escrow the vehicles private key as it is generated as they roll the car off the assembly line, in case a person loses their smart card and needs a new key issued. The same idea is applied to door locks - use your smart card to unlock major doors in the house, such as your front and back doors.

3.3 *Biometrics Integration*

Biometrics promote a much more secure form of authentication. Biometric authentication can be extended to PKI to allow another factor of authentication, making a person's digital certificate even more secure. Typically, a user's certificate would be protected by a password or PIN number, but with biometric authentication a user can protect their digital certificate by using a thumbprint or retina scan. While retina and iris scans are currently the most accurate forms of biometric authentication, fingerprint readers are the cheapest and provide adequate security for certificate protection for civilians.

Today, the DoD uses a person's thumbprint when issuing one of their smart cards. The purpose of the thumbprint is not for authenticating a user to the smart card, but for unlocking the smart card in the case where the user cannot remember their PIN. Only the thumbprint of the card/certificate's owner can unlock the card. An encoded form of the thumbprint is stored on the surface of the card, and looks like a cryptic form of a bar code.

It is the proposal of this paper that biometrics should be used in conjunction with the proposed universal form of identification. Some smart card vendors actually make smart cards that have a biometric fingerprint reader built onto the smart card. Smart cards such as these provide greater security for protecting private keys.

4.0 Privacy Issues

Introducing security into any computer system inevitably introduces privacy issues [5]. How do we secure a system with information that should be private and confidential while still preserving that privacy and confidentiality? We can increase security by using biometrics, but where is that biometric information stored?

A fingerprint, unlike a PIN or password, cannot be randomly changed. We don't have unlimited choices for fingerprints as we do PINs or passwords. Compromising a fingerprint can be greatly avoided by using smart cards with integrated fingerprint readers because the fingerprint never leaves the card; it never travels over any open wires. Such security doesn't rely on a central database, but rather the security and tamper-resistance of the smart card itself.

Issuance of certificates is another issue. If we are to be held legally accountable for documents [6], emails and other transactions that we digitally sign, we must ensure the identity of a person when the digital certificate is issued. The current method for obtaining a driver's license is just to show some form of identification like your birth certificate, social security number card, etc. This method is probably still good enough for now, but as identity theft becomes more of a problem in the coming years, a more accurate method of identifying someone who doesn't already have this universal identification smart card will be necessary. Maybe we need to start taking more information about someone at their time of birth. Perhaps taking some kind of biometric or DNA reading when a person is born and giving that information to the parents, like an enhanced form of a birth certificate. Does the government keep a copy of this biometric or DNA information to authenticate the person when the first apply for their universal identification smart card? Where is this information stored?

Maybe, instead of taking and storing biometric or DNA readings, a person has a universal identification card issued when they are first born, and then the parents will lock it up in a safe place until their child is old enough to accept responsibility for carrying it. Perhaps instead of a social security card being issued when a child is born, a universal identification card is issued. There are many different possibilities for better identifying an individual without a universal identification card, starting with producing better documentation from birth (digitally signed by the delivering doctor and parents?).

[5] This entire section references the issues discussed in Connolly (Reference #10), Clarke (Reference #11) and Schwartz (Reference #12)
[6] Chen (Reference #6)

5.0 Conclusion

The always-on internet market is moving in such a way that most every home in America will have always-on internet access in the next few years (providers expanding, costs dropping - hopefully). Using smart cards and certificates for identification in addition to the visual photo ID is an undoubtedly more secure than just a visual photo ID, and can provide security to this growing market of fixed internet connections. But does combining all these features onto one form of ID decrease a person's overall security? Does the average person want to rely on ONE item to link everything together? What if the card is stolen? What if it is compromised? If someone loses a credit card, at least they might have another. If this ID is stolen, the thief could have access to much more than just your checking account. Where is your biometric information stored? On the smart card? In a central database? Who administrates the database? Who has access to the database? Does this ID promote increased government monitoring of computer activity? These are all questions which must be addressed in the near future if we are to bring true distributed and managed information security to the internet and into our homes.

6.0 Bibliography

1. Tebbutt, Dan of Network Magazine. "*Business Case: Going Postal In The Fight Against Government Paperwork*". 05 July 2001. URL: http://www.networkmagazine.com/article/NMG20010620S0010

2. Mayer, Merry of Government Computer News. "*USPS will use a PKI to manage electronic postage*". 07 Sep 1998. URL: http://www.gcn.com/archives/gcn/1998/september7/14.htm

3. United States Postal Service. "*Handbook AS-600, United States Postal Service Certification Practice Statement, Version 1*". 27 July 2001. URL: http://www.usps.com/cpim/ftp/hand/as600/

4. Alterman, Peter, Ph.D., Senior Advisor to the Chair, Federal PKI Steering Committee and Acting Director, Federal Bridge Certification Authority. "*The U.S. Federal PKI and the Federal Bridge Certification Authority*". 07 May 2001. URL: http://www.cio.gov/fpkisc/documents/alterman-terena.htm

5. McKenna, Ed of Washington Technology. *"Building Bridges of Security - Federal Group Fosters Agency PKI Cooperation*". 16 July 2001. URL: http://www.washingtontechnology.com/news/16_8/features/16847-1.html

6. Chen, Anne of eWEEK. "*PKI starts to deliver*". 02 Apr 2001. URL: http://techupdate.zdnet.com/techupdate/stories/main/0,14179,2701532,00.html

7. Curry, Ian. "An Introduction to Cryptography and Digital Signatures". Mar 2001 URL: http://www.entrust.com/resources/pdf/cryptointro.pdf

8. VeriSign, Inc. "*PKI - The VeriSign Difference*". © 1999. URL: http://www.verisign.com/whitepaper/enterprise/difference/index.html

9. VeriSign, Inc. "*Introduction to Public Key Cryptography*". © 1998. URL: http://www.verisign.com/repository/crptintr.html

10. Connolly, Chris of the Privacy Committee of New South Wales. "*Can Smart Card Technology Protect Privacy?*". August 1995. URL: http://www.austlii.edu.au/au/other/privacy/smart/311.html

11. Clarke, Roger. "*Smart Cards' Threats to Privacy*" PRIVACY ISSUES in SMART CARD APPLICATIONS in the RETAIL FINANCIAL SECTOR. 16 March 1996 URL: http://www.anu.edu.au/people/Roger.Clarke/DV/ACFF.html#Threats

12. Schwartz, Ari. "*Smart Cards at the Crossroads: Authenticator or Privacy Invader?*". December 1998. URL: http://www.cdt.org/digsig/idandsmartcards.shtml

13. National Institute of Standards and Technology (NIST). "FIPS PUB 140-1: Security Requirements for Cryptographic Modules". Last updated on December 04, 2001. URL: http://csrc.nist.gov/cryptval/140-1.htm

14. National Institute of Standards and Technology (NIST). "FIPS PUB 140-2: Security Requirements for Cryptographic Modules". Last updated on November 15, 2001. URL: http://csrc.nist.gov/cryptval/140-2.htm