User Authentication Through the Use of Public Key Infrastructure (PKI)

Robert T Meacham

East Carolina University

Summer 2013 ICTN 6823

Abstract

The information I would like to cover in this paper will be in the use of the Public Key Infrastructure (PKI). The key area of focus will be on its use in the authentication of users in relation to network access for segments of the Department of Defense (DoD) Global Information Grid (GIG) infrastructure. I will discuss views from its implementation, expansion, benefits, issues and management perspective briefly in order to provide a better understanding of the impact this change has had on security and the management of such an undertaking. Details pertaining to the infrastructure, methods of implementation and usage will be discussed. Then a look into the effects of policies and the importance of documenting the methods used to implement user authentication through the Public Key Infrastructure within the organization. Without good management and the implementation of policies and procedures in place, the likelihood of misinterpretation and security flaws can occur that will directly affect the confidentiality, integrity and availability of an organization infrastructure.

Introduction

Let's first start off by defining what the Public Key Infrastructure is. Of the plethora of definitions I encountered when trying to sum this up I choose the following excerpt that I believe best encompasses what Public Key Infrastructure is; "A public-key infrastructure (PKI) consists of protocols, services, and standards supporting applications of public-key cryptography. The term PKI, which is relatively recent, is defined variously in current literature. PKI sometimes refers simply to a trust hierarchy based on public-key certificates, and in other contexts embraces encryption and digital signature services provided to end-user applications as well. A middle view is that a PKI includes services and protocols for managing public keys, often through the use of Certification Authority (CA) and Registration Authority (RA) components, but not necessarily for performing cryptographic operations with the keys" (*4.1.3.1 What is a PKI?* (2012).

In short it's a method that uses encryption to provide user authentication digitally through the use of a trusted third party, the Certification Authority, to verify the user and create the certificates. This has become extremely important and useful in this age of ecommerce and global networking.

The following table helps depict the basic components of PKI. (Al-Khouri, 2011)

Component	**Description**
Digital Certificates	Electronic credentials, consisting of public keys, which are used to sign and encrypt data. Digital certificates provide the foundation of a PKI.
Certification Authoritie(S) – CAs	Trusted entities or services that issue digital certificates. When multiple CAs are used, they are typically arranged in a carefully prescribed order and perform specialized tasks, such as issuing certificates to subordinate CAs or issuing certificates to users
Certificate Policy and Practice Statements	Documents that outline how the CA and its certificates are to be used, the degree of trust that can be placed in there certificates, legal liabilities if the trust is broken, and so on.
Certificate Repositories	A directory of services or other location where certificates are stored and published.
Certificate Revocation Lists (CRL)	List of certificates that have been revoked before reaching the scheduled expiration date.

What is authentication; authentication as it will be referenced to in this paper, can be defined as a process or protocol that allows one to authenticate their credentials or identity in order to gain access to information systems or facilities in which services can be given to users in order to perform specific functions (Mallow). Once a user has been successfully authenticated, access to resources such as buildings, share drives, Intranet and other shared resources can be granted. Great concern should be considered when choosing a method of authentication and its implementation in order to help alleviate potential flaws based on the human factors ability to circumvent the designed security structure (Braz, Jean-Marc).

In respects to the Public Key Infrastructure usage in the Department of Defense, it began to appear in greater usage at the turn of the century with a mandatory implementation soon to follow for all unclassified networks. The unclassified network is better known as the Non-secure Internet Protocol Routed Network (NIPRNet) and will be referred as this throughout the paper. This implementation entailed the establishment of a supporting infrastructure to include new hardware, software, training and policies. This implementation needed to be as seamless as possible and able to integrate with current and future systems with as little disruption in the daily operations as possible.

The medium used to hold the certificates need for the Public Key Infrastructure would be the currently utilized smart card. Its current usage was primarily used as an Identification Card and other applications such as access to buildings and cafeteria food payment. This implementation occurred due to the need for a more secure method of authentication, streamlining of automated process requiring signatures and greater security in communications.

A few methods of tokens are used currently throughout the DoD. The use of soft and hard certificates are used based off the need of implementation. Soft certificates were primarily

used in the beginning while the finalization of what type of hardware, software and smartcard where going to be utilized. They are still utilized in some applications where using a physical certificate methods is not feasible or practical. The primary use is through a physical smartcard similar to a credit card. This method is used on both unclassified and classified systems. The need for separate tokens is required due to the sensitivity of material that can be accessed with each token and the technology used.

Expansion

After the initial setup and trial phases occurred throughout the globe, implementation became mandatory for users to long onto computer assets, accessing certain web sites and shared network resources, particular documents, and access to certain facilities where all done through the use of a single Smart Card that contained a user's certificates.

The potential vulnerability released by National Institute of Standards and Technology (NIST) in June of 2010 for the recommendation for transitioning of cryptographic algorithms and key size,(PKI and Public Key Enabling. 2013) lead to the mandate of a review for the implementation of a stronger hash algorithm. The current use of Secure Hash Algorithm (SHA) -1 is suggesting to be converted to SHA-256. A full conversion to SHA-256 has not occurred at the time of this writing.

Another more recent event, after several years of this technology's usage on the unclassified network, it became mandatory for the implementation of the Public Key Infrastructure be placed on the classified secret network, an already perceived secure network. This network is better known as the Secure Internet Protocol Routed Network (SIPRNet). This entailed a completely separate mirrored Public Key Infrastructure of the unclassified network or NIPRNet. New hardware and software had to be purchased and disseminated across the globe.

Policy modifications to the NIPRNet were used with stricter rule sets due to the nature of the material handled on the SIPRNet. ("Department of Defense", 2011) Continued expansion persists with integration into more applications and systems as technologies, reliability and demand become more prominent.

Benefits

With any form of user authentication, there will be advantages and disadvantages. The key differences in them are generally related to their robustness, reliability and ease of use. The use of just a user name and password may be the simplest and most common form but also can provide the weakest form of security. Passwords can be relatively easy to crack or forget. If they are easy to recall they are usually weak, if they are strong they can be hard to recall.

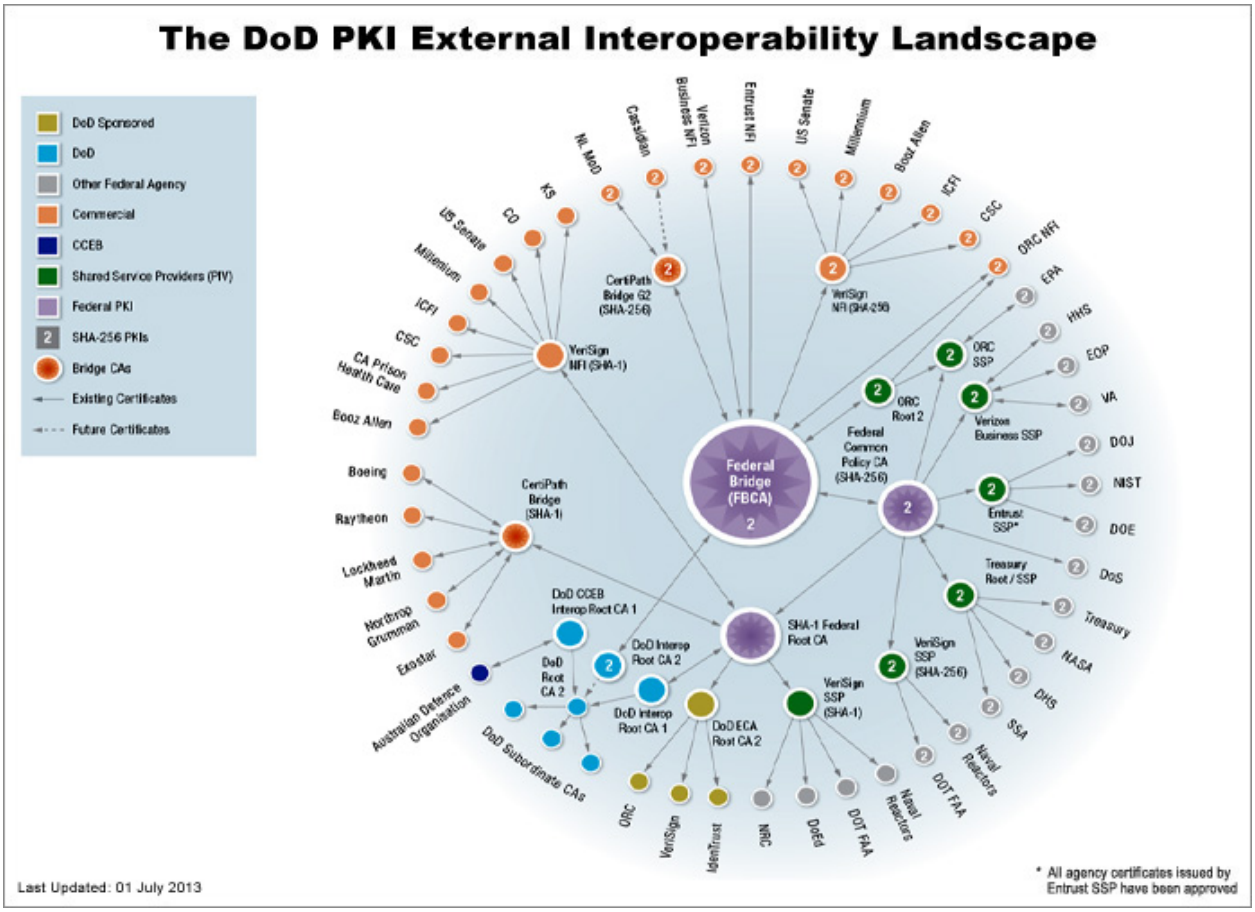
Many benefits have been gained through the use of Public Key Infrastructure throughout the DoD. From the users perspective the ease of using the same access code and smart card for several years vice using a username and password that had to be changed on a frequent basis. They also gained the ability to digitally sign documents and access multiple restricted websites from different Domains all with the same credentials. This also aided administrators in managing a single account that might have previously required multiple user logon accounts.

The use of two factor authentication aided in increasing security of user authentication in that it required the use of something known, personal identification number (PIN), and something owned, soft or hard certificate, to gain access to resources that previously only requiring a username and password. The ability to digitally provide signatures on electronic documents also aides in becoming compliant with the Government Paperwork Elimination Act (GPEA) (Rhodes, K. 2004)

PKI uses asymmetric encryption and digital signatures techniques (Varvitsiotis A. 2000). This method allows sender A to send signed and or encrypted message to recipient(s) B and others. User B and others can verify and or decrypt the message using one of the two keys referenced to the user, the public key, created for user A.

This is done with confidence through the use of certificate creation handled by a Certificate Authority (CA), a trusted third party. This trusted third party is the key to PKI in that they are the entity verifying that everyone is who they say they are. Without this fundamental, trust, the system as a whole is unreliable and provides no additional security measure. In fact compromise of this third party could be detrimental to an organization.

The current DoD PKI external interoperability architecture is depicted in the following diagram. It was extracted in its native form for ease of readability. ("The DoD PKI" 2013)



Issues

As with anything in life there will always be some disadvantage or issues. Issues with PKI can stem from several areas as noted by Correll (2000). Primary areas of concern are in with the Certification Authorities. That is who is approved and by what means to become a CA. Are they part of your organizations security design? How secure are their practices? What methods were used to identify a user? Is the private key really secured? This refers to the accountability of the smart card. Is it in your possession or stored in a secure manner when not in use? These are all concerns needing to be considered with the implementation and management of PKI.

For the Public Key Infrastructure, in respects to the user interaction, the ability to use a smart card for multiple means of access is an advantage until it becomes compromised, inoperable or misplaced. The reissuing of a new one can be tedious and time consuming due to the security measures involved in the creation and issuing process.

Another potential vulnerability that circumvents the intent is when a user can logon with someone else's token or password if not maintained properly because the PIN was written down and token left unattended or even worse given to you.

Some disadvantages associated with PKI are related to the initial and maintenance cost, potential invasiveness of data collected, reestablishment of credentials, scalability and reliability. The cost associated with PKI or biometric systems is typically more expensive than that of non PKI or biometric authentications systems.

Digital signatures are a form of authentication in that they provide reliability and legitimacy of data. A digital signature is typically based on a one-way hash function that is encrypted with a private key. It can then be verified by using the public key thus enabling the

verification and legitimacy of the file. If this is compromised it again negates the validity of the signature.

The storing of this data is also another primary concern. If not properly protected, one's information could be compromised. It is also more tedious to establish someone's access with a smart card holding a user's certificates than a password. The resetting of someone's password is much less daunting than having to reset someone's digital certificates, perhaps due loss, malfunction of the smart card or the user forgetting the PIN.

Malfunctions in the system can cause undue denials or even worse gain unauthorized access. Accuracy and reliability are also a concern. Systems have improved over the years and become much more accurate and reliable.

Certification Authorities are a critical component of a PKI because of their connection of organizations, employees, and others components. This is because of the importance that the certification authority has in the PKI trust model. The Certification Authority is the entity that the other users of the PKI trust to guarantee the association between a public key and a specific user or entity. If the certification authority is compromised the impacts can be catastrophic to an organizations operation.

This is especially true if the compromise is not detected for some period of time and now erroneous certificates could be issued to individuals or organizations that could be used to gain access or forged digital signatures. Since all parties trust the certificates issued by the certification authority, an undetected compromise could result in the systems that rely on those certificates to allow otherwise unauthorized access.

Simply stated, due to the trust the system places in the certificates issued by the certification authority, the system may securely allow otherwise unauthorized access based on

the compromise. Even if the compromise is detected in a timely manner, the impacts can be catastrophic to an agency's operations regardless of whether a loss of data occurs from the compromise. Should a Certification Authority be compromised, the agency would have to go through the time consuming and costly process of reissuing digital certificates in accordance with the organizations policies and procedures. This could mean thousands of certificates for some organizations and possible shut down of systems (Rhodes, Keith A).

Management

Management from the initial implementation to the continued maintenance of the Public Key Infrastructure for the DoD seems to be a daunting task to undertake. Issues from methods of deployment, policy, reporting and maintenance have all required the need for skilled managers in order to successfully achieve the current status of the Public Key Infrastructure throughout the DoD.

As mentioned previously, the key component of the PKI lies with the CA. Some of their duties are to guarantee the key uniqueness for users, maintain a database of certificates, revoke certificates, maintain a list of revoked certificates, and arrange for the availability and distribution of certificates.

Key roles have been implemented to aid in the total management of the PKI. Some of these roles are listed as follows (PKI and Public Key Enabling, 2013)

End user: End users are individuals, or organizational components represented by an individual, that accesses the PKI system to acquire public/private keys and certificates. These keys are used to encrypt date and other messages transmitted between computer systems.

Local Registration Authority (LRA): A LRA is an individual assigned the responsibility of managing end user access to the PKI system. LRAs register users in the PKI system and provide assistance and information on PKI-related topics to users.

Trusted Agent (TA): A TA is an individual who supports an LRA by performing the face-to-face user authentication and distribution of the Certificate Registration Instruction forms for the LRA. The TA role is optional, and can be used where needed to reduce the demands on an LRA.

Registration Authority (RA): A RA is an individual assigned the responsibility of authorizing and managing the LRAs access to the PKI system. RAs are also responsible for revoking certificates when required. Through the use of these elements, management of the PKI can be maintained in a more secure and reliable manner.

Policies and Documentation

With everything mentioned thus far, little or none of this can have any real value if it is not documented and implement in accordance with a local or higher policy. Guidelines must be established for implementation, usage, legality and continuity. Without such guidance and boundaries, one will quickly find the security measures that they thought they were implementing have either been adverted or simply not updated and configured properly thusly negating the time and money spent on the original implementation plan.

Users should sign a legal and binding agreement that informs them of their rights and responsibilities. It should advise them of the consequences for sharing or giving unauthorized individuals access to material and locations or circumventing security measurement's that are in place. Defining what is acceptable and unacceptable when accessing information systems and the consequences of violating these policies needs to be clear and concise. This is of even greater importance when dealing in the area of finances, health and government due to the

important nature of the material they work with. These aspects of policy and documentation are a key issue in dealing with user authentication as they aid in mitigating potential issues outside of the technical means in place.

Conclusion

In this paper I have covered a few aspects in reference to user authentication methods and the concerns in relationship to the security, implementation, management and policies in respects to the Public Key Infrastructure and its use throughout the Department of Defense.

Overall the implementation of PKI into the DoD has provided the perception of a more enhanced and secure enclave along with providing some added convenience to the user. This was accomplished through key management aspects with the use of CAs, LRA's, RA's and TA's as being the primary controlling entities. These entities are the key to maintaining the reliability of the infrastructure in relation to providing integrity of the certificates issued to users.

In nearly a decade the DoD has implemented a robust Public Key Infrastructure that encompasses a global network across multiple classification systems. With continuing expansion and maintenance, PKI will aid in providing the DoD a more robust and secure method of user authentication for years to come.

References

4.1.3.1 What is a PKI? (2012). RSA Laboratories. Retrieved from http://www.rsa.com/rsalabs/node.asp?id=2268

*Al-Khouri, A. M. (2011-05-30). PKI in Government Identity Management Systems. International journal of network security & its applications, 3(3), 69-96.

Braz. C, Jean-Marc, R. *Security and Usability: the case of the User Authentication* methods. Retrieved from http://brazc.uqam.ca/paperIHM06.pdf

Cowley, J. (2013-01-01). Communications and Networking: An Introduction. Springer London. Retrieved from http://link.springer.com.jproxy.lib.ecu.edu/chapter/10.1007/978-1-4471-4357-4_8/fulltext.html

Committee on Government Reform Serial No. 108-133. (Sep. 9, 2003). Advancements in Smart Card and Biometric Technology. Retrieved from HTTP://congressional.proquest.com.jproxy.lib.ecu.edu/congressional/docview/t29.d30.hrg-2003-hgr-0074?accountid=10639

*Corell,S. Ten Risks of PKI: In Favour of Smart Card-Based PKI, Network Security, Volume 2000, Issue 5, 1 May 2000, Pages 12-14, ISSN 1353-4858, http://dx.doi.org/10.1016/S1353-4858(00)05023-6. Retrieved from (http://www.sciencedirect.com/science/article/pii/S1353485800050236)

Cowley, J. (2013-01-01). Communications and Networking: An Introduction. Springer London. Retrieved from http://link.springer.com.jproxy.lib.ecu.edu/chapter/10.1007/978-1-4471-4357-4_8/fulltext.html

Department of Defense INSTRUCTION NUMBER 8520.03. (13 May, 2011). Identity

Authentication for Information Systems. Retrieved from http://www.dtic.mil/whs/directives/corres/pdf/852003p.pdf

*Hunt, R. Technological infrastructure for PKI and digital certification, Computer Communications, Volume 24, Issue 14, 15 September 2001, Pages 1460-1471, ISSN 0140-3664, http://dx.doi.org/10.1016/S0140-3664(01)00293-6. Retrieved from (http://www.sciencedirect.com/science/article/pii/S0140366401002936)

Mallow, C. *Authentication methods and techniques.* Retrieved from http://www.giac.org/cissp-papers/2.pdf

Public Key Infrastructure (PKI) Overview (2013). SSL Shopper. Retrieved from http://www.sslshopper.com/public-key-infrastructure-pki-overview.html

Public Key Infrastructure (PKI) and Public Key Enabling (PKE). (6 July, 2013). Information Assurance Support Environment. Retrieved from http://iase.disa.mil/pki-pke/

Raina, K. (2003-05-01). PKI Security Solutions for the Enterprise: Solving HIPAA, E-Paper Act, and Other Compliance Issues. Wiley. Retrieved from http://web.ebscohost.com.jproxy.lib.ecu.edu/ehost/detail?sid=942144ab-972a-4c1c-aac3-c95aff180c68%40sessionmgr112&vid=1&hid=103&bdata=JnNpdGU9ZWhvc3QtbGl2ZQ%3d%3d#db=nlebk&AN=85522

Rhodes, K. A. (2004) Public Key Infrastructure: Examples of Risk and Internal Control Objectives Associated with Certificate Authorities. Retrieved from http://www.gpo.gov/fdsys/pkg/GAOREPORTS-GAO-04-1023R/pdf/GAOREPORTS-GAO-04-1023R.pdf

Stapko, T. (2007, August) Practical Embedded Security: Building Secure Resource-Constrained

Systems. Newnes, Burlington, MA. Retrieved from http://site.ebrary.com.jproxy.lib.ecu.edu/lib/eastcarolina/docDetail.action?docID=10190330

The DoD PKI External Interoperability Landscape. (1 July, 2013) [Diagram illustration of DoD PKI Interoperabilty]Retrieved from http://iase.disa.mil/pki-pke/interoperability/index.html

*Thompson, M. R., Essiari, A., Mudumbai, S. Certificate-based authorization policy in a PKI environment, ACM Transactions on Information and System Security (TISSEC). Volume 6 Issue 4, November 2003Pages 566-588 ACM New York, NY, USA doi>10.1145/950191.950196 Retrieved from http://dl.acm.org.jproxy.lib.ecu.edu/citation.cfm?id=950196

*Varvitsiotis, A.P., Scaling issues in large PKI communities, Future Generation Computer Systems, Volume 16, Issue 4, February 2000, Pages 361-372, ISSN 0167-739X, http://dx.doi.org/10.1016/S0167-739X(99)00060-6. Retrieved from (http://www.sciencedirect.com/science/article/pii/S0167739X99000606)