

Security Characteristics of Cryptographic Mobility Solutions

Sarbari Gupta

Electrosoft Services, Inc.

sarbari@electrosoft-inc.com

Abstract

This paper focuses upon the security characteristics of cryptographic mobility (CM) solutions. CM solutions allow the roaming user to make use of their cryptographic credentials from any workstation or system that has network connectivity to the appropriate credential server(s), without the need to carry portable software or hardware tokens. While CM implementations have a greater potential for security vulnerabilities than traditional (non-mobile) cryptographic implementations, it is anticipated that the demand for products in this technology category will continue to grow in the future.

1 OVERVIEW

Traditionally, systems that use public-private key pairs for user authentication, digital signature or message confidentiality protection store the user's private keys and private user data in encrypted form on the client system's hard drive. However, this mechanism does not allow the user to *roam*, that is, to access the private key information from any generic client terminal, in order to digitally sign or encrypt material from that terminal.

Within a public key infrastructure (PKI), a user *credential* is a cryptographically protected object, that may contain the owner's private key(s), public key certificate(s), certificates for CAs within the owner's PKI hierarchy, trust roots relevant to the user, and other domain-specific parameters such as user IDs, cryptographic algorithm names, salt values, etc. PKI credentials may reside in hardware or software tokens.

Cryptographic roaming is highly advantageous for many business and consumer applications. Such solutions make cryptography accessible from a wide variety of client systems, including public kiosks and terminals. Currently, there are two fundamental mechanisms for providing roaming access to public key credentials – these are described below.

- Portable credentials – the user carries their cryptographic credentials in a portable format

(which may be hardware or software). Smart cards and other types of hardware tokens, and software credentials stored on portable media such as floppies are examples of portable credentials. While the portable hardware token approach is sound from the security perspective, it often requires special hardware at the client workstation, and is often cumbersome, impractical or cost-prohibitive for most roaming scenarios. Conversely, software portable tokens are cheap and easy to deploy. However, very often, software portable tokens are protected using password-based encryption techniques (such as PKCS#5 [P1]). Within a roaming environment, where public terminals and kiosks may be used for secure transactions, such a software portable token may easily be subjected to offline brute-force password guessing attacks, against a reasonably small password space.

- Credential Servers – this approach makes use of online Credentials Server(s), which allows the credential owner to make use of their private key material after they have successfully authenticated themselves to one or more online Authentication Servers. In this approach, all or portions of the user's private key material and private data are stored, in a protected form, on a system that is accessible to the online authentication and credential servers.

In this paper, we will focus on the latter approach for mobility, and analyze the generic security characteristics. We will refer to such solutions as **Cryptographic Mobility (CM)** solutions. There are several CM products and techniques that are currently available. References to some of the major schemes are listed at the end of this paper. This paper is organized as follows. Section 2 defines a generic architecture for CM systems, while Section 3 describes the generic operational phases. Section 4 discusses some of the attributes that characterize a CM solution, while Section 5 describes the security issues that are more likely to arise in CM implementations. Section 6 analyzes the applicability of a CM solution, Section 7 provides brief,

high-level descriptions of some of the currently available CM products, and Section 8 presents some conclusions.

2 ARCHITECTURE OF A CRYPTOGRAPHIC MOBILITY SOLUTION

A generic CM system comprises several functional components as illustrated in Figure 1. Each of the components is further described below. It may be noted that although the functional components are shown as distinct boxes the figure, two or more of the components may be instantiated on the same physical system for a given CM implementation.

Client Station: This component represents various shared workstations and/or public kiosks that may be utilized by a CM user to interact with the CM system. The Client Station can be used to initialize a roaming credential through interactions with the Initialization Server. The Client Station can also be used to activate and use the roaming credential for secure data exchange. The CM user is required to authenticate to one or more Authentication Servers, following which, the user's credentials are made available with the cooperation of the Credential Server(s). The Client

Station may run some kind of GUI-based client software that is provided as a part of the specific mobility solution.

Initialization Server: The Initialization Server is responsible for the creation of roaming credentials, and the establishment of the authentication information for the roaming user. If new certificates need to be issued to the user during the creation of the roaming credentials, this component may interact with a Certification Authority. The Initialization Server will also typically interact with the Authentication and Credential Servers to populate their databases with the appropriate data for the user.

Authentication Server(s): This is the component that is responsible for authenticating the roaming user before they are allowed access to their credentials. The Authentication Server may need to maintain an authentication database that allows it to determine whether a given user's authentication attempt was successful.

Credential Server(s): This component may hold all or portions of the user's cryptographic credentials. The held credentials may be stored in a backend data store.

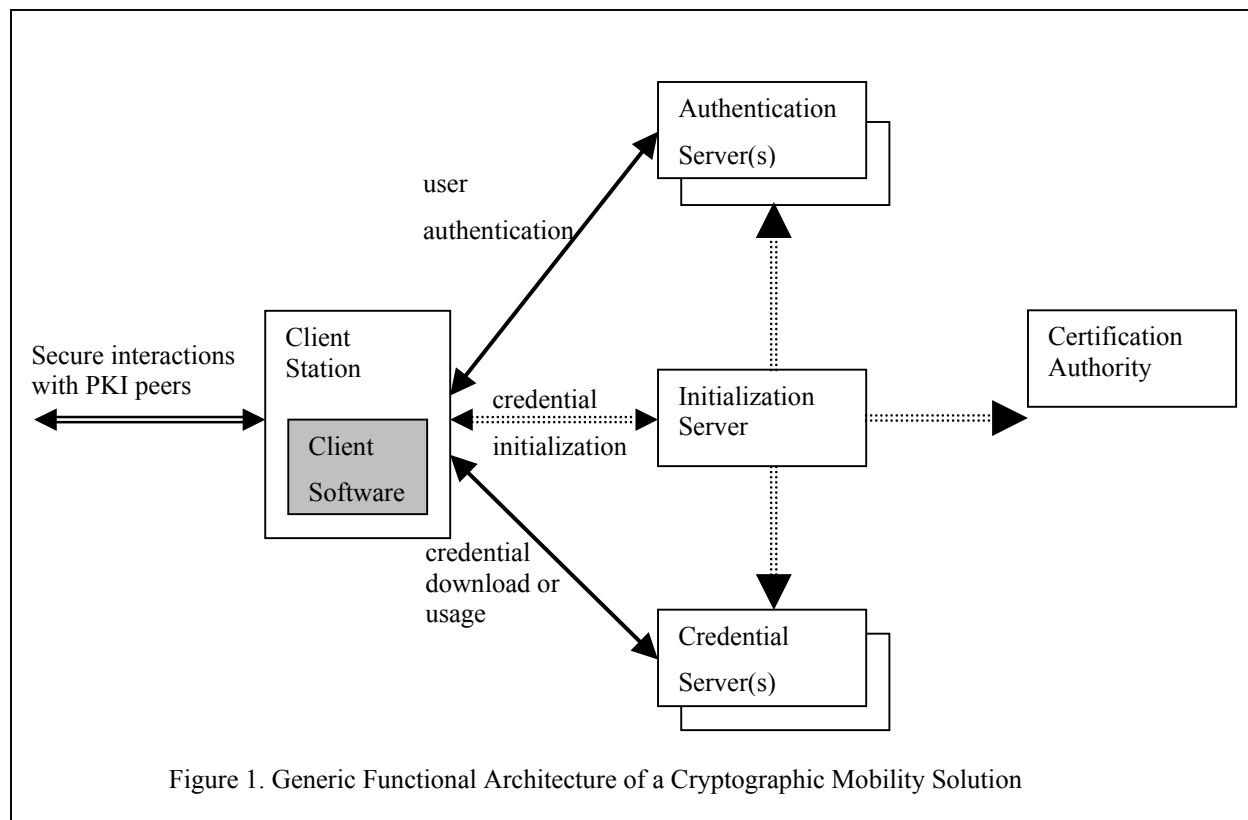


Figure 1. Generic Functional Architecture of a Cryptographic Mobility Solution

Certification Authority (CA): The CA component is responsible for the generation of signed certificates for roaming credential use, if that is necessary to the CM solution. The Initialization Server interacts with the CA component to create and initialize special roaming credentials.

3 OPERATIONAL PHASES OF A CRYPTOGRAPHIC MOBILITY SOLUTION

Although there are varied schemes for implementing a CM solution, the majority of the schemes can be broken down into some generic operational phases. These are described below.

Credential Initialization Phase - During this phase, the user's PKI credentials may be created and/or packaged to accommodate roaming usage. The Client Station component interacts with the CM Initialization Server to perform the steps needed to establish a set of roaming-capable credentials, and make them accessible to the user. Some CM solutions can package existing user credentials into a roaming accessible form, while others require the generation of specially-crafted credentials to support roaming usage. In the latter type, the CM solution will typically require generation of new key pairs, and the issuance of new certificates. In some cases, the CM solution may provide its own Certification Authority or certificate generation function. In other cases, the CM solution can pass the certificate signing request to an external Certification Authority.

During the Initialization Phase, information is collected for the authentication of the roaming user. This information is used to populate the Authentication Server database. Additionally, the roaming credential package is handed to the Credential Server for access over the Internet.

Authentication Phase - This phase of the roaming protocol occurs each time the user wishes to establish their connection to their online credential server to download or make use of their roaming credentials. During this phase, the online user operating from a generic workstation or terminal authenticates to the Authentication Server to assert and establish their identity. Although there are wide variations in the technologies and protocols used between the Client Station and the Authentication Server, the human user at the Client session almost uniformly is required to provide an account identity and a password. The user may also be required to provide answers to one or more questions to provide restricted, personal, information.

The user provided account name, password, and perhaps other user secrets that are required, may be used in a variety of ways to authenticate to the remote Authentication Server(s). Some schemes use a challenge-response protocol using the user-provided password, others use the password for a local operation (at the Client Station) to unlock private key functions to authenticate to the Authentication Server(s). Yet other schemes use some form of strong password schemes using strong secrets that are provided by remote, online server(s).

The frequency of the authentication phase during a user session, and the ability to invoke multiple uses of the user's private roaming credentials, varies considerably with the particular scheme under consideration. For ease of use, some schemes allow caching of the user provided authentication information so that the user is only required to provide this information once during the course of a session regardless of the number of times the roaming credential is used and the variety of applications that invoke the user private key. While very convenient for the user, this approach of single sign-on is fraught with risk in terms of credential hijack by subsequent users of the Client Station. Other CM schemes take the conservative approach of necessitating a user authentication to the Authentication Server(s) each time the user private key is used. This approach provides much greater security for the roaming credential and supports other associated security functions, such as auditing the use of the private keys for purposes of fraud detection and non-repudiation; however, the user's convenience factor is greatly reduced.

Credential Download Phase - Many of the CM technologies involve an intermediate phase of credential download to the Client Station. The credential download follows the authentication phase and precedes the credential usage phase. The downloaded material may be part or all of the user's credentials and other private user data, and is always protected with additional layer(s) of cryptography to prevent credential misuse at or to the Client Station. The additional layer(s) of cryptographic protection may be unlocked using a session authentication key or through user provided secrets.

Credential Usage Phase - The most significant operational phase of a CM solution is the actual use of the user's private key for authentication, digital signature, or message decryption functions. During this phase, the user has the ability to make use of their credentials, either by unlocking a local copy of their

credentials, or by availing of online services that assist in completing the usage of the credentials.

Some CM schemes allow the download of a copy of the user's credentials to the local client station. This copy is cryptographically protected and may be unlocked for use after the user provides a PIN or passphrase. The user is able to make repeated use of the local copy of the credential without involving the remote Authentication or Credential Servers. This type of scheme is typically faster and easier to use. However, the local copy of the user's credentials on the Client Station may be subjected to offline attacks and unauthorized reuse.

In certain CM schemes, the user's credentials or key material is never actually downloaded to the local Client Station. Each use of the roaming credential requires the involvement of one or both of the Authentication and Credential Servers. This type of scheme, though possibly slower and more tedious to use, has the benefit that it never exposes the user's credentials at the Client Station or allows its copy or reuse by an attacker.

Credential Release Phase - The final phase of a CM scheme is the Credential Release Phase, during which the Client Station scrubs any downloaded key material and authentication information from memory and magnetic storage, and formally ends the current user session. This phase may be implemented unilaterally within the Client Station, or it may require the Client Station to interact with the Credential and/or Authentication Servers to inform them about the termination of the roaming user session.

4 CHARACTERISTICS OF CM SOLUTIONS

There are some common characteristics in nearly all of the cryptographic mobility solutions that are available. These are enumerated below.

- Client Station does not need special hardware such as token readers – The fundamental reason to seek out a CM solution is to avoid the use of special hardware tokens and token readers. Thus all CM implementations share this common attribute.
- Client Station needs vendor-specific CM client software that has to be either downloaded or installed in a trusted manner – In all of the CM products studied, there is a need for a vendor-specific client software module that performs the needed operations (such as authenticating the user, downloading and storing a local copy of the credentials or key materials, and enabling the use of the user's PKI credentials for private key operations. Since this piece of software collects the user's authentication information as well as handles the user's private key usage, the assurance level for the software has to be fairly high.
- User needs to remember authentication information, whether it is a password, or answers to a series of personal questions – The roaming user has to authenticate to an online server to acquire the ability to use public key credentials for subsequent authentication operations. However, the user cannot use public key operations during the initial authentication phase for obvious reasons. The user also cannot typically use other strong mechanisms such as hardware One-Time-Password generators (e.g. SecurID cards) since that would involve the usage of hardware tokens. Thus, most CM implementations make use of secret sharing schemes, such as passwords or answers to personal questions for the initial authentication phase.
- Users interact with remote Authentication Servers to authenticate themselves to the system – Since the user is assumed to be working from a Client Stations that does not have a local copy of their credentials, all roaming solutions necessarily involve a remote authentication function where the authentication information supplied by the human user is transported through some means to a remote server which verifies them to identify and authenticate the user.
- An authenticated user is able to perform cryptographic operations using their private key – The fundamental goal of a roaming PKI user is to ultimately use their private key for digital signature or data decryption operations. All CM implementations provide this facility through different mechanisms.
- Credential is unusable after the end of the user's session – The premise of a roaming user is that they avail of a shared Client Station when attempting to use their PKI credentials. Thus, it is very important that upon the last user leaving the Client Station, there be no residual ability to make use of the last user's credentials by the subsequent user. All CM implementations use this as a common functional goal.
- Part or all of a user's PKI credentials are stored on an online remote credential server -The user's

authentication information is stored on a database accessible to an online authentication server.

5 SECURITY ISSUES WITH CM SOLUTIONS

CHARACTERISTICS THAT ADD SECURITY VULNERABILITIES

Due to the fundamental nature of a cryptographic mobility solution, in that it makes use of remote authentication and credential servers, there are a number of additional security issues that may arise. Depending upon the particular implementation of CM, some or many of these issues may be sidestepped through the use of novel schemes. This section will describe some of the security issues that are particularly relevant when assessing a CM implementation. The various architectural components of a CM system have their own characteristics that may introduce additional security vulnerabilities. Some of these characteristics are described below.

- The Client Station is assumed to be a shared access workstation or kiosk that has network connectivity to the CM Server entities, possible over the Internet. The Client Station is also assumed to use some form of CM client software that has to be installed.
- The Authentication Server(s) are assumed to be available online, possibly over the Internet, for access by Client Stations. The Authentication Server is also expected to have some form of database (possibly on a backend system,) that holds user data that can be used to complete the authentication step.
- The Credential Server(s) are also assumed to be online and available for network-based attacks. The Credential Server has to ascertain that the user has been properly authenticated before allowing the download or use of their private keys. The private key material for CM users is typically held in some kind of database at the backend of the Credential Server.
- The three primary architectural components of a CM system interact with each other using online protocols over shared and (often) untrusted networks. Thus, these protocols may be attacked by network intruders.

POTENTIAL SECURITY VULNERABILITIES

When evaluating the security of a CM solution, a number of questions should be asked. The answers must then be taken collectively to determine the specific security vulnerabilities that exist for a given system. The security relevant questions to be asked include:

- How and where are client key pairs generated? Depending upon whether the user's key pair is generated at the Client Station or on a server, the non-repudiation claims of a private key may be stronger or weaker. To support a strong case for non-repudiation, the server system must never handle the unencrypted private keys or private key material for a user.
- Where is the user's private key actually used – at the Client Station or on a remote server component? The location of “usage” of the private key has an impact on the non-repudiation properties of the CM implementation.
- How is the client private key deposited at the Credential Server? The Credential Server must hold all or part of the user's private key in order to allow the user to have roaming access to the private key. However, the mechanism for protecting the private key while the credential server holds it is very significant in determining whether a capture of the protected private key container, leads to the ability to use that private key.
- How is the client private key protected at the Credential Server?
- What are the security characteristics of the authentication protocol between the Client Station and the Authentication Server(s)? Are the protocols susceptible to man-in-the-middle and eavesdropping attacks? Does the scheme reveal the CM user's authentication information to the Authentication Server?
- How is the client private key made available for use at the Client Station?
- Can the user's private key be compromised at the Client Station?
- How is the client private key disabled at the end of the user's session?
- How does the user establish trust in the Client Software? How does the user know the source of the Client Software and establish trust in its integrity?
- How does the Client Module handle the sensitive authentication information that is collected from the user – is it held in memory or is it cleared after each use?

- How does the Client Module handle the local copy of the user's credentials that is obtained from the Credential Server – is it held in memory for ease of use or is it cleared after each use?
- How does the Client Module establish trust in the Authentication and Credential Servers? If SSL is used, how are the PKI trust roots established in the Client Station?
- Can the Authentication Server(s) be compromised such that the authentication database becomes available to the attacker? If so, what can the attacker do with the captured information?
- Can the Credential Server be compromised such that the Credential Database becomes accessible to the attacker? If so, what can the attacker achieve with the captured information?
- Can the CM user be subjected to Denial-of-Service attacks through the compromise or disablement of the Authentication and Credential Servers?

6 APPLICABILITY OF CM SOLUTIONS

In this section, the major issues that affect the decision to deploy a CM solution are briefly explored. While CM solutions may be recommended in certain usage scenarios, they are definitely not advisable in others. This section attempts to clarify some of the issues that should be considered before adopting a CM product.

REQUIREMENTS THAT DRIVE THE SELECTION OF A CM SOLUTION

The decision to deploy a cryptographic mobility solution is usually made because of some requirements that are levied due to the characteristics of the user, the user's IT environment, or the secure application. Some of the typical requirements that drive an organization to consider a CM implementation are:

- Users are highly mobile, and need to use variety of systems/workstations, operated and controlled (possibly) by various organizations
- Hardware cryptographic tokens too expensive or cumbersome or infeasible due to requirement to have compatible readers
- Users are in an IT environment where dedicated workstations are infeasible or prohibitively expensive
- Software cryptographic tokens not practical or secure enough

- Simple user interface is required – user only needs to provide user ID and password, and answer simple personal questions
- User or application requires strong authentication, and/or message encryption

CONTRAINDICATIONS FOR SELECTION OF CM SOLUTIONS

Some environments and user populations exhibit requirements that are contraindications for certain types of CM products. When these requirements exist within an environment, extra caution must be exercised in selecting a CM product that meets these requirements. These include:

- Strong, legally binding non-repudiation of electronic transactions is an absolute must
- Recovery of encryption keys is essential
- Long term archival and possible usage of the protected data
- Guaranteed access to credentials for decryption and signatures – zero tolerance for denial-of-service situations

7 A SAMPLING OF CM TECHNOLOGIES AND PRODUCTS

In this section, several of the leading products and technologies that provide CM solutions are identified and described very briefly. It should be mentioned that the information contained in this section is based upon data collected from the vendor websites and dialogue with vendor personnel. The goal was to develop a brief, high-level description of each product, rather than to provide detailed technical coverage of each product. These descriptions should not be used to evaluate the products – the interested reader is directed to contact the vendor directly to obtain more technically accurate and up to date information on each product.

ENTRUST ROAMING PKI

Entrust has been providing a PKI mobility solution within Entrust/Roaming™, a complementary product to Entrust/PKI® 5.0 [E1]. Entrust/Roaming™ makes use of a public Directory Server to store the cryptographic profiles for users, encrypted with a strong symmetric key. A strong password authentication mechanism named SPEKE is used to securely download the strong keys that can decrypt the user's protected cryptographic

profiles, and hence make use of the private key material held inside.

SPEKE stands for Simple Password-authenticated Exponential Key Exchange [E2]. It provides *strong password authentication* to prove knowledge of a small secret (namely, a password) without revealing it to anyone.

An Entrust profile contains the PKI credentials for a given user. Typically, the profile is stored locally on the hard drive in a form that is protected with a user-chosen password. This protection format provides very little resistance against a concerted offline dictionary-based attack. Hence, in the Entrust Roaming solution, the standard user profile is further encrypted with a strong symmetric key K ($K \geq 128$ bits) and stored on a Directory Server. The Entrust solution also makes use of an online Roaming Server that authenticates the user using the SPEKE protocol, establishes a shared strong key S based upon the authentication, and provides the user with $E_S(K)$ such that the user is then able to retrieve K and hence unlock and use their cryptographic profile. The downloaded roaming profile can then be used similar to a local Entrust profile stored on the local hard drive.

VERISIGN ROAMING

The VeriSign PKI roaming solution is a part of the VeriSign OnSite PKI offering [V1, V2, V3, V4]. It uses multiple, independent Roaming servers, each of which provides a component of the key that the user employs to retrieve and decrypt his or her *roaming credentials* from the Storage Server. The technique for utilizing multiple Roaming Servers, to recreate the strong key that can be used to decrypt the protected roaming credentials, is based upon the password-hardening protocol published by Warwick Ford and Burt Kaliski. In the Ford-Kaliski scheme, a user interacts with two or more Roaming Servers to harden the user's password into a strong secret, without revealing the user's password or the derived strong secret to any of the Roaming Servers. The user's roaming credentials are held on an online Storage Server in a strongly encrypted form. The user may download the protected credentials from the Storage Server, and unlock them using the strong secret that is derived with the assistance of the Roaming Servers.

ARCOT ID MOBILITY

Arcot has a patented cryptographic camouflaging scheme that it uses as the cornerstone of its ArcotID mobility solution [A1, A2, A3, A4]. In this solution,

multiple PKI credentials for a user may be bundled into a protective package called a "key bag", encrypted with a strong symmetric key. Each user also possesses an ArcotID, which comprises the Arcot certificate, and the camouflaged Arcot private key. The user may download his or her "key bag" and ArcotID from an online Card Server, after authenticating to it using shared secrets. The user then supplies a PIN to the ArcotID allowing the de-camouflaging and use of the Arcot private key for authenticating to an Arcot Authentication Server (AS). [It may be noted that the unique feature of the cryptographically camouflaged Arcot private key is that it can only be unlocked with the correct PIN – however, many incorrect PINs will also yield a plausible private key to attackers, who now have to use the candidate key to authenticate to the AS. The AS is configured to lock out a user after a certain number of failed attempts.] Upon successful authentication to the Authentication Server, the user is able to retrieve a portion of the symmetric key that protects the user's "key bag". The user's supplied PIN is used to generate the other portion to recreate the key that may be used to decrypt the "key bag" to allow access to the contained credentials for normal PKI based operations.

SINGLESIGNON.NET APPLIANCE

SingleSignon.Net's *Secure Identity Appliance*TM is at the heart of its Practical PKI offering [S1, S2, S3]. The Secure Identity Appliance is a hardened "black box" that can be connected to a corporate network, and store sensitive information for users. In this scheme, each user's private key is split into two components, one of which is held by the appliance, and the other is derived from the user's password. When a roaming user needs to make use of their PKI credentials for secure transactions, they authenticate to the appliance using a password-based strong mechanism to establish a secure channel. A digest of the data to be signed is then transported to the appliance over the secure, authenticated channel, and the appliance generates a partial signature using the component of the user's private key that is held by the appliance. The user then performs another partial signature operation on the returned data using the other component of the private key (that is derived from the user's password) to complete the signature on the target data. The final signature may be validated using the user's public key using the normal mechanisms. Since the appliance has to participate in every invocation of the user's private key, it can perform other operations as well, such as revocation checking, usage analysis, auditing, etc.

MICROSOFT PROFILES

In recent versions of its operating systems, Microsoft provides a roaming profile scheme that allows the profile to be a container of PKI credentials for a user [M1, M2]. A properly authenticated domain user is able to download their profile from a central server to the local workstation. The user profile is protected using the MS Data Protection API (DPAPI). Under the MS DPAPI scheme, a master key is created for each user at first logon. Two copies of the master key are stored in the user's profile. The first is copy is protected using a 160-bit RC4 key that is derived from the user's logon password. The second copy is protected using a derivative of the Domain Controller's master key. In order to use the encrypted profile that is downloaded to the local workstation, the user's password is used to unlock the user's master key. The master key is used to retrieve the key that protects the private keys in the user's key store.

RSA SECURITY KEON WEBPASSORT

RSA Security's Web Passport offering is primarily for organizations that require the use of PKI credentials with Web Applications that provide security services such as digital signatures, VPN access or secure email [R1, R2, R3]. The product has two main components, the Web Passport Server and the Web Passport Plug-in. The former resides on a web server and is used to enforce authentication and authorization policies that determine the authorizations that users have to web resources.

Users can authenticate to the Web Passport Server using a variety of mechanisms, including passwords and SecurID authenticators. Once authenticated, the user's virtual (smart) card is downloaded from a LDAP directory to the Web Passport Plug-in on the Client Station. The virtual card is a protected container for the user's PKI certificates and private keys. Once downloaded, the virtual card can be accessed through the Microsoft Cryptographic API or the PKCS#11 interface from any application that has the capability to invoke these APIs.

The Web Passport Client Plug-in may be installed on the Client Station manually. If it is not present when the user tries to access a Web Passport protected resource, the plug-in is automatically downloaded from the web. The Web Passport virtual card contains up to two user certificates as well as the corresponding private key(s). The private key(s) are encrypted with 112-bit

ROAMING

3DES2EDE-CBC secret key, while the secret key is protected using a PIN Unlock Key (PUK). The PUK is a random 128-bit RC4 key. Web Passport uses cookies to keep track of authentication state, PKI credential state, key contained names, etc.

The Web Passport product supports PKI credentials from any of the industry leading CAs. It allows users to have multiple virtual cards (possibly issued by different CAs and different organizations) and allows the user to have simultaneous access to multiple sets of virtual cards.

BALTIMORE UNICERT OPTION FOR ROAMING

The UniCERT PKI product offers an optional component for roaming credential usage [B1, B2, B3]. It allows subscribers to digitally sign transactions and participate in secure online applications from a web browser without requiring the use of hardware tokens. The Baltimore CM product comprises a number of components. The Roaming Server coordinates the operation of the UNICERT roaming facility. The Roaming Administrator component allows system administrators to initialize and manage the UniCERT Roaming system by creating and updating roaming users. The Protected Encryption Key (PEK) Server deals with roaming user authentication before allowing them access to their signing key, and comprises hardware cryptographic modules. In order to insulate the Roaming and PEK Servers from direct network-based attacks from the Internet, a Proxy Server is used. There are two kinds of applets that are used within the UniCERT roaming system: a Signing Applet that can download and make use of roaming credentials to sign web data, and a Change Passphrase Applet which allows the passphrase protecting the user's signing key to be changed.

The use of two dedicated servers (Roaming and PEK) implies that both servers need to be successfully attacked in order to compromise the system. The PEK Server stores double encrypted end-user keys, while internal sequence numbers protect against brute force attacks. If fault-tolerance and high availability is required, or high volume is anticipated, multiple PEK and Roaming Servers may be deployed. The Baltimore roaming solution will work with certificates issued by any standards-compliant CA including Baltimore's UniCERT.

HUSH COMMUNICATIONS ROAMING SOLUTION

The Hush Key Server Network provides outsourced management and hosting of PKI credentials [H1, H2]. The Hush Key Server stores and manages the subscriber public and private keys through the use of a Private Key Database and a Public Key Database. The former holds the user private keys, protecting them with a “private alias” derived from a user-generated passphrase that the user never shares with any other entity. The User ID and passphrase are passed through a message digest repeatedly to generate over 1 million characters that comprise the “private alias” for the user. The “private alias” is used as a means of anonymizing and strengthening the storage of user private keys on remote servers. The private alias is used as an index into the Hush Key Private Key Database such that the private keys are nearly anonymous. The private alias is also used to authenticate the user within the Hush system.

The Public Key Database stores the corresponding user public keys. It is indexed by the user’s email address and contains the user’s public key certificate and revocation status. The Hush Encryption Engine facilitates public key exchange between two parties in a transparent fashion – when needed, a connection is automatically made between the first party and the Hush Key Server to retrieve the public key of the second party. The Hush Key Server also supports user key pair generation and registration with a CA. Hush offers a secure email solution using this roaming PKI scheme.

8 CONCLUSIONS

In studying various technologies and products that are currently available to support cryptographic mobility, it is clear that some areas of vulnerability remain as common elements to most available solutions. It is interesting to note that all of the systems referenced in this paper, offer strong mechanisms for user authentication, and use strong protocols for authentication and credential download that are not susceptible to active or passive man-in-the-middle attacks. All of the systems use Client Station modules that store password and key information in volatile memory only, depending upon operating system facilities to keep the information from being copied to disk. However, some of the common vulnerabilities are discussed below.

Most of the techniques described above, rely upon the use of downloaded software that comprise the Client

Station Module. The downloaded module is a signed component, in most cases. However, when used from a shared workstation or public kiosk, it is difficult to have assurance regarding the trust roots that are configured into the web browsers and other PKI applications. It is also possible that rogue software implanted on these workstations captures the users keystrokes, (and hence their passwords and other authentication information,) and transfers them to some configured location. The rogue software may also affect the entropy of the random numbers generated on the workstation and hence adversely influence key pair generation, symmetric session key generation, etc.

Another area of vulnerability of roaming solutions is the susceptibility to denial-of-service attacks. A roaming solution implicitly requires the availability of one or more online servers. If any of these servers are made unavailable, the user will not have access to their cryptographic credentials, and may have to settle for unsecured interactions to meet their functional objectives. All roaming solutions should therefore address this problem by providing a high degree of redundancy to ensure that the roaming user is able to access their credentials.

Many of the solutions described above, store the user credentials on a single online server, in such a way, that the password-protected version of the credentials are available to an attacker that compromises that online server. It is well known that credentials protected by PKCS#5 type password-based cryptography are susceptible to offline password cracking attacks. Thus, the solutions that employ two or more servers in a way that the compromise of one server does not allow password-protected credentials to fall into the hands of an attacker are inherently more secure than solutions that employ a single server.

Additionally, online servers that hold credential or authentication information are high value targets for attackers. Hence, these systems must be implemented to use various types of available protections to lessen their vulnerability to such attacks. The use of proxy servers, firewalls, FIPS 140-1 approved hardware cryptographic devices, hardened operating systems, physical, personnel and operational security measures, should be employed to strengthen the security of these systems.

Some of the solutions studied cause the user’s private keys, and/or the passwords that provide access to private keys, to be available to a roaming server system at some point during the initialization process. If these private keys are used for authentication or digital signature operations, the non-repudiation claims of the system are intrinsically weakened in such situations.

Despite these common weaknesses and potential vulnerabilities, it is our belief that cryptographic mobility solutions will continue to see greater adoption in the future. Due to the intrinsic nature of our current lifestyle, the user will necessarily be away from their home/office/workstation, but will continue to require access to high-grade cryptography as they pursue their personal and work-related goals. Thus, it is anticipated that the security issues with mobility solutions will be resolved with the help of innovative engineering skills, and CM implementations of PKI will gain rapid acceptance.

9 FURTHER INFORMATION

Further information about the analysis of cryptographic mobility solutions may be obtained by contacting the author, Sarbari Gupta at sarbari@electrosoft-inc.com.

10 REFERENCES

[A1] "Securing Digital Identities," Presentation to the Federal PKI TWG, September 2000.

[A2] "Arcot Key Authority: Solution for controlled access to Conventional Private Keys," Arcot Systems White Paper.

[A3] D. Hoover, B. Kausik, "Software smart cards via cryptographic camouflage," IEEE Symposium on Security and Privacy, 1999.

[A4] "Arcot WebFort™ Overview: Strong Authentication and Secure Signing Using Software," Arcot System White Paper.

[B1] "Roaming: Secure Electronic Transactions Without Boundaries", <http://www.baltimore.com/unicert/unicert/roaming.html>

[B2] UniCERT Roaming UniCERT Extended Technology" Baltimore White Paper.

[B3] "UniCERT Extended Technology – Roaming Version 1.0 Administrator's Guide," Baltimore UniCERT documentation.

[E1] "Secure Roaming with Software Tokens," Presentation to the Federal PKI TWG, September 2000.

[E2] Jablon, David, "Strong Password-Only Authenticated Key Exchange," ACM Computer Communication Review, vol. 26, no. 5, Oct. 1996.

[H1] "Hush Encryption Engine™ White Paper Version 2.0," Hush White Paper, July 2001.

[H2] "Services: Hush Key Server Network" http://www.hush.com/services/key_server_network/.

[M1] Finnegan, Sean, "Crypto, Key Protection, and Crypto, Key Protection, and Mobility in Windows Mobility in Windows," Microsoft Presentation.

[M2] Guttman, Peter, "How to recover private keys for Microsoft Internet Explorer, Internet Information Server, Outlook Express, and many others," White paper available at <http://www.cs.auckland.ac.nz/~pgut001/pubs/breakms.txt>.

[P1] "PKCS#5 v2.0 - Password-Based Cryptography Standard," RSA Laboratories, March 1999.

[R1] Carboni, E., "RSA Keon Mobile Credentials," Presentation to the Federal PKI TWG.

[R2] "RSA Keon Web PassPort: Technical Overview," A white paper from RSA Security.

[R3] Mark Diodati, "Frequently Asked Questions, RSA Keon Web PassPort, RSA Security Paper, May 2001.

[S1] "The SingleSignOn.Net Difference," SingleSignOn.Net White Paper.

[S2] Bhatt, Harish, "Towards Practical PKI," SingleSignOn.Net White Paper.

[S3] Boyd, Colin, "Digital Multisignatures," *Cryptography and Coding*, Oxford University Press, 1989, pp 241-246.

[V1] Ford, Warwick, "Server- Assisted Generation of a Strong Secret from a Password," Presentation to the Federal PKI TWG.

[V2] Ford, W. and Kaliski, B., "Server-Assisted Generation of a Strong Secret from a Password," Proceedings of the IEEE Fifth International Workshop on Enterprise Security, 2000.

[V3] "VeriSign Personal Trust Service," VeriSign Product Literature.

[V4] "Administrator's Guide: ROAMING SERVICE," VeriSign Product documentation.