Singaporean Journal Scientific Research (SJSR)
ISSN: 2231 - 0061Vol.3, No.1pp.141 - 145

available at: : http://www.iaaet.org/sjsr

Key Management Techniques for Controlling the Distribution and Update of Cryptographic keys.

[1]T.Lalitha, [2]R.Umarani and [3]G.M.Kadharnawaz
[1]Senior Lecturer, Department of MCA, Sona College of Technology, Salem, Tamilnadu., India. lalithasrilekha@rediffmail.com
[2]Assoc.Prof., Department of Comp. Science, Sri Saradha College for Women, Salem, Tamilnadu, India. umainweb@gmail.com
[3]Director,Department of MCA, Sona College of Technology, Salem, Tamilnadu., India nawazse@yahoo.co.in

***Abstract*-Key management plays a fundamental role in cryptography as the basis for securing cryptographictechniques providing confidentiality, entity authentication, data origin authentication,data integrity, and digital signatures. The goal of a good cryptographic design isto reduce more complex problems to the proper management and safe-keeping of a smallnumber of cryptographic keys, ultimately secured through trust in hardware or softwareby physical isolation or procedural controls. Reliance on physical and procedural security(e.g., secured rooms with isolated equipment), tamper-resistant hardware, and trust in alarge number of individuals is minimized by concentrating trust in a small number of easilymonitored, controlled, and trustworthy elements.**

***Keyword*-**Key Management, Cryptography, Algorithm, Secret Key.

1. INTRODUCTION

Systems providing cryptographic services require techniques for initialization and key distributionas well as protocols to support on-line update of keying material, key backup/recovery, revocation, and for managing certificates in certificate-based systems.

Key management [1]is the set of techniques and procedures supporting the establishmentand maintenance of keying relationships between authorized parties.

Key management encompasses techniques and procedures supporting:

- Initializationof system users within a domain
- Generation, distribution, and installation of keying material
- Controlling the use of keying material.
- Update, revocation, and destruction of keying material and
- Storage, backup/recovery, and archival of keying material.

2. CLASSIFYING KEYS BY ALGORITHM TYPE AND INTENDED USE

The terminology of TableI is used in reference to keying material. A symmetric cryptographicsystem is a system involving two transformations – one for the originator andone for the recipient – both of which make use of either the same secret key (symmetrickey) or two keys easily computed from each other. An asymmetric cryptographic systemis a system involving two related transformations – one defined by a public key (the publictransformation), and another defined by a private key (the private transformation) with theproperty that it is computationally infeasible to determinethe private transformation fromthe public transformation.

TABLE 1 PRIVATE, PUBLIC, SYMMETRIC AND SECRET KEYS

Term	**Meaning**
private key, public key	paired keys in an asymmetric cryptographic system
symmetric key	key in a symmetric (single-key) cryptographic system
secret	adjective used to describe private or symmetric key

Table II indicates various types of algorithms commonly used to achieve the specifiedcryptographic objectives. Keys associated with these algorithms may be correspondinglyclassified, for the purpose of controlling key usage .The classification givenrequires specification of both the type of algorithm (e.g., encryption vs. signature) and theintended use (e.g., confidentiality vs. entity authentication).

TABLE 1I TYPES OF ALGORITHMS COMMONLY USED TO MEET SPECIFIED OBJECTIVES

Cryptographic objective	**Algorithm type**	
	public-key	***symmetric-key***
confidentiality	encryption	encryption
data origin authentication	signature	MAC
key agreement	Diffie-Hellman	various methods
entity authentication	1.signature 2.decryption 3.Customized	1.MAC 2.encryption

3. KEY MANAGEMENT OBJECTIVES, THREATS AND POLICY

Keying relationships in a communications environment involve at least two parties (asender and a receiver) in real-time. In a storage environment, there may be only a singleparty, which stores and retrieves data at distinct points in time.

The objective of key management is to maintain keying relationships and keying materialin a manner which counters relevant threats, such as:

- Compromise of confidentiality of secret keys.
- Compromise of authenticity of secret or public keys. Authenticity requirements includeknowledge or verifiability of the true identity of the party a key is shared orassociated with.
- Unauthorized use of secret or public keys.

A. Security policy and key management

Key management is usually provided within the context of a specific security policy. A securitypolicy explicitly or implicitly defines the threats a system is intended to address. Thepolicy may affect the stringency of cryptographic requirements, depending on the susceptibilityof the environment in question to various types of attack. Security policies typicallyalso specify:

- Practices and procedures to be followed in carrying out technical and administrativeaspects of key management, both automated and manualresponsibilities and accountability of each party involved andthe types of records (audit trail information) to be kept, to support subsequent reportsor reviews of security-related events.

4. TRADE OFFS AMONG KEY ESTABLISHMENT PROTOCOLS

In selected key management applications, hybrid protocols involving both symmetricand asymmetric techniques offer the best alternative. More generally, the optimal use of available techniques generally involvescombining symmetric techniques for bulk encryption and data integrity with public-keytechniques for signatures and key management.

A. Public-key vs. symmetric-key techniques (in key Management)

Primary advantages offered by public-key (vs. symmetric-key) techniques for applicationsrelated to key management include:

- Simplified key management. To encrypt data for another party, only the encryptionpublic key of that party need be obtained. This simplifies key management as onlyauthenticity of public keys is required, not their secrecy.
- On-line trusted server not required. Public-key techniques allow a trusted on-lineserver to be replaced by a trusted off-line server plus any means for delivering authenticpublic keys (e.g., public-key certificates and a public database provided byan entrusted on-line server). For applications where an on-line trusted server is notmandatory, thismay make the systemmore amenable to scaling, to support very largenumbers of users.
- Enhanced functionality. Public-key cryptography[2] offers functionalitywhich typicallycannot be provided cost-effectively by symmetric techniques (without additional onlinetrusted third parties or customized secure hardware). The most notable such featuresare non-repudiation of digital signatures, and true (single-source) data originauthentication.

5. PUBLIC KEY CERTIFICATES

Public-key certificates are a vehicle by which public keys may be stored, distributed or forwardedover unsecured media without danger of undetectable manipulation. The objectiveis to make one entity's public key available to others such that its authenticity (i.e., its statusas the true public key of that entity) and validity are verifiable. In practice, X.509 certificatesare commonly used.

A. Definition

A public-key certificate [4]is a data structure consisting of a data part and a signaturepart. The data part contains cleartext data including, as a minimum, a public keyand a string identifying the party (subject entity) to be associated there with. The signaturepart consists of the digital signature of a certification authority over the data part, therebybinding the subject entity's identity to the specified public key.

The Certification Authority (CA) is a trusted third party whose signature on the certificatevouches for the authenticity of the public key bound to the subject entity. The significanceof this binding (e.g., what the key may be used for) must be provided by additionalmeans, such as an attribute certificate or policy statement. Within the certificate, thestring which identifies the subject entity must be a unique name within the system (distinguishedname), which the CA typically associates with a real-world entity. TheCA requiresits own signature key pair, the authentic public key of which is made available to each partyupon registering as an authorized system user. This CA public key allows any system user,through certificate acquisition and verification, to transitively acquire trust in the authenticityof the public key in any certificate signed by that CA.Certificates are a means for transferring trust, as opposed to establishing trust originally.The authenticity of the CA's public keymay be originally provided by non-cryptographicmeans including personal acquisition, or through trusted couriers; authenticity is required, but not secrecy.

Examples of additional information which the certificate data part might contain include:

- A validity period of the public key.
- A serial number or key identifier identifying the certificate or key.
- Additional information about the subject entity (e.g., street or network address).
- Additional information about the key (e.g.,algorithm and intended use).
- Quality measures related to the identification of the subject entity, the generation of the key pair, or other policy issues.

- Information facilitating verification of the signature (e.g., a signature algorithmidentifier, and issuing CA's name).
- The status of the public key.

B. Creation of public-key certificates

Before creating a public-key certificate for a subject entity A, the certification authorityshould take appropriate measures (relative to the security level required, and customarybusiness practices), typically non-cryptographic in nature, to verify the claimed identity ofA and the fact that the public key to be certified is actually that of A. Two cases may bedistinguished.

- Trusted party creates key pair. The trusted party creates a public-key pair, assignsit to a specific entity, and includes the public key and the identity of that entity in the Certificate. The entity obtains a copy of the corresponding private key over a secure (authenticand private) channel after proving its identity (e.g., by showing a passport or trustedphoto-id, in person). All parties subsequently using this certificate essentially delegate trustto this prior verification of identity by the trusted party.
- Entity creates own key pair. The entity creates its own public-key pair, and securelytransfers the public key to the trusted party in a manner which preserves authenticity.(e.g., over a trusted channel, or in person). Upon verification of the authenticity (source) ofthe public key, the trusted party creates the public-key certificatethe signer.

C. Use and verification of public-key certificates

The overall process whereby a party B uses a public-key certificate to obtain the authenticpublic key of a party A may be summarized as follows:

- (One-time) acquire the authentic public key of the certification authority.
- Obtain an identifying string which uniquely identifies the intended party A.
- Acquire over some unsecured channel (e.g. from a central public database of certificates, a public-key certificate corresponding to subject entity Aand agreeing with the previous identifying string.

1) (a) Verify the current date and time against the validity period (if any) in the certificate, relying on a local trusted time/day-clock.
   (b) Verify the current validity of the CA's public key itself.
   (c) Verify the signature on A's certificate, using the CA's public key.
   (d) Verify that the certificate has not been revoked .

If all checks succeed, accept the public key in the certificate as A's authentic key.

D. Attribute certificates

Public-key certificates bind a public key and an identity, and include additional data fieldsnecessary to clarify this binding, but are not intended for certifying additional information.Attribute certificates are similar to public-key certificates, but specifically intended to allowspecification of information (attributes) other than public keys (but related to a CA, entity,or public key), such that it may also be conveyed in a trusted (verifiable) manner. Attributecertificates may be associated with a specific public key by binding the attribute informationto the key by the method by which the key is identified, e.g., by the serial number of a

Corresponding public-key certificate, or to a hash-value of the public key or certificate. Attribute certificates may be signed by an attribute certification authority, created inconjunction with an attribute registration authority, and distributed in conjunction with anattribute directory service More generally, any party with a signature keyand appropriate recognizable authority may create an attribute certificate. One applicationis to certify authorization information related to a public key. More specifically, this maybe used, for example, to limit liability resulting from a digital signature, or to constrain theuse of a public key (e.g., to transactions of limited values, certain types, or during certainhours).consulted.

6. KEY LIFE CYCLE ISSUES

Key management is simplest when all cryptographic keys are fixed for all time. Cryptoperiods[3] necessitate the update of keys. This imposes additional requirements, e.g., on certificationauthorities which maintain and update user keys. The set of stages through which akey progresses during its existence, referred to as the life cycle of keys, is discussed in thissection.

A. Lifetime protection requirements

Controls are necessary to protect keys both during usage and storage. Regardinglong-term storage of keys, the duration of protection required depends on the cryptographicfunction (e.g., encryption, signature, data origin authentication/integrity) and thetime-sensitivity of the data in question.

Security impact of dependencies in key updates:Keying material should be updated prior to crypto period expiry. Updateinvolves use of existing keying material to establish new keying material, through appropriatekey establishment protocols and key layering .To limit exposure in case of compromise of either long term secret keys or past sessionkeys, dependencies among keying material should be avoided. For example, securinga new session key by encrypting it under the old session key is not recommended (sincecompromise of the old key compromises the new).

Lifetime storage requirements for various types of keys:Stored secret keys must be secured so as to provide both confidentiality and authenticity.Stored public keys must be secured such that their authenticity is verifiable. Confidentialityand authenticity guarantees, respectively countering the threats of disclosure and modification,may be provided by cryptographic techniques, procedural (trust-based) techniques, orphysical protection (tamper-resistant hardware).Signature verification public keys may require archival to allow signature verificationat future points in time, including possibly after the private key ceases to be used. Someapplications may require that signature private keys neither be backed up nor archived: suchkeys revealed to any party other than the owner potentially invalidates the property of nonrepudiation.Note here that loss (without compromise) of a signature private key may beaddressed by creation of a new key, and is non-critical as such a private key is not needed foraccess to past transactions; similarly, public encryption keys need not be archived. On theother hand, decryption private keys may require archival, since past information encryptedthereunder might otherwise be lost.Keys used for entity authentication need not be backed up or archived. All secret keysused for encryption or data origin authentication should remain secret for as long as thedata secured thereunder requires continued protection (the *protection lifetime*), and backupor archival is required to prevent loss of this data or verifiability should the key be lost.

B. Key management life cycle

Except in simple systems where secret keys remain fixed for all time, cryptoperiods associatedwith keys require that keys be updated periodically. Key update necessitates additionalprocedures and protocols, often including communications with third parties in public-keysystems. The sequence of states which keying material progresses through over its lifetimeis called the key management life cycle.

Life cycle stages may include:

- User registration – an entity becomes an authorized member of a security domain.This involves acquisition, or creation and exchange, of initial keyingmaterial such asshared passwords or PINs by a secure, one-time technique (e.g., personal exchange,registered mail, trusted courier).
- User initialization – an entity initializes its cryptographic application (e.g., installsand initializes software or hardware), involving use or installation (see below) of initialkeying material obtained during user registration.
- Key generation – generation of cryptographic keys should include measures to ensureappropriate properties for the intended application or algorithm and randomness inthe sense of being predictable (to adversaries) with negligible probability . An entity may generate its own keys, or acquire keys from a trusted systemcomponent.
- Key installation – keying material is installed for operational use within an entity'ssoftware or hardware, by a variety of techniques including one or more of the following: manual entry of a password or PIN, transfer of a disk, read-only-memorydevice, chipcard or other hardware token or device (e.g., key-loader). The initial keying materialmay serve to establish a secure on-line session throughwhich working keys areestablished. During subsequent updates, new keying material is installed to replacethat in use, ideally through a secure on-line update technique.
- Key registration – in association with key installation, keying material may be officiallyrecorded (by a registration authority) as associated with a unique name whichdistinguishes an entity. For public keys, public-key certificates may be created by acertification authority (which serves as guarantor of this association), and made availableto others through a public directory or other means
- Normal use – the objective of the life cycle is to facilitate operational availability ofkeying material for standard cryptographic purposes. Under normal circumstances, this state continues until cryptoperiodexpiry; it may also be subdivided – e.g., for encryption public-key pairs, a pointmay exist at which the public key is no longer deemed valid for encryption, but theprivate key remains in (normal) use for decryption.
- Key backup – backup of keying material in independent, secure storage media providesa data source for key recovery (point 11 below). Backup refers to short-termstorage during operational use.
- Key update – prior to crypto period expiry, operational keying material is replaced bynew material. This may involve some combination of key generation, key derivationexecution of two-party key establishment protocols, orcommunications with a trusted third party. For public keys, update and registrationof new keys typically involves secure communications protocols with certificationauthorities.
- Archival– keying material no longer in normal use may be archived to provide asource for key retrieval under special circumstances (e.g., settling disputes involvingrepudiation). Archival [5] refers to off-line long-term storage of post-operational keys.
- key de-registration and destruction – once there are no further requirements for thevalue of a key or maintaining its association with an entity, the key is de-registered(removed from all official records of existing keys), and all copies of the key are destroyed. In the case of secret keys, all traces are securely erased.
- Key recovery – if keying material is lost in a manner free of compromise (e.g., due toequipment failure or forgotten passwords), it may be possible to restore the materialfrom a secure backup copy.
- Key revocation – it may be necessary to remove keys from operational use prior totheir originally scheduled expiry, for reasons including key compromise. For publickeys distributed by certificates, this involves revoking certificates.

7. CONCLUSION

Key management plays a fundamental role in cryptography as the basis for securing cryptographictechniques providing confidentiality, entity authentication, data origin authentication, data integrity, and digital signatures. The goal of a good cryptographic design isto reduce more complex problems to the proper management and safe-keeping of a smallnumber of cryptographic keys, ultimately secured through trust in hardware or softwareby physical isolation or procedural controls. Reliance on physical and procedural security(e.g., secured rooms with isolated equipment), tamper-resistant hardware, and trust in alarge number of individuals is minimized by concentrating trust in a small number of easilymonitored, controlled, and trustworthy elements.

REFERENCES

1. National Institute of Standards and Technology.
2. R. Rivest, A. Shamir, L. Adleman. A Method for Obtaining Digital Signatures and Public-Key Cryptosystems. Communications of the ACM, Vol. 21 (2), pp.120–126. 1978. Previously released as an MIT "Technical Memo" in April 1977, and published in Martin Gardner's Scientific American.
3. http://www.discretix.com/PDF/Using%20Public%20Key%20Cryptography%20in%20Mobile%20Phones.pdf
4. http://dlc.sun.com/pdf/316194901A/316194901A.pdf
5. http://www.safecomprogram.gov/NR/rdonlyres/7C31664D-5B0B-4128-A85B-