T/3521TL/2778/9

4 February 1997

CESG INFOSEC MEMORANDUM NO. 15

AN HMG PUBLIC KEY INFRASTRUCTURE TO SUPPORT AUTHENTICATION

Issue 1.0

CESG ELECTRONIC INFORMATION SYSTEMS SECURITY MEMORANDUM NO. 15

AN HMG PUBLIC KEY INFRASTRUCTURE TO SUPPORT AUTHENTICATION

Issue 1.0

February 1997

Communications-Electronics Security Group

FOREWORD

This Memorandum is issued by the Communications-Electronics Security Group (CESG) of Government Communications Headquarters as part of its responsibility to advise HMG on Electronic Information Systems Security (Infosec).

It suggests an architecture for a public key infrastructure (PKI) to support authentication between communicating systems. The Memorandum will eventually form part of a suite of documents which collectively provide advice on the implementation of a PKI, and the use of the services enabled by such an infrastructure (e.g. electronic mail). The architecture as described in this document is an initial attempt at defining a PKI, and CESG will take into account any comments on its feasibility.

This Memorandum is intended for use by HMG, its contractors and suppliers.

General correspondence in connection with this document, including requests for additional copies, should be addressed to:

Communications-Electronics Security Group (X13)
Government Communications Headquarters
PO Box 144
Cheltenham GL52 5UE
United Kingdom

Technical correspondence in connection with this document should be sent to T27 at the above address.

CONTENTS

REFERENCES

a. ITU-T Recommendation X.500 (1993) | ISO/IEC 9594-1: 1993, Information Technology - Open Systems Interconnection - The Directory: Overview of Concepts, Models and Services.

b. ITU-T Recommendation X.501 (1993) | ISO/IEC 9594-2: 1993, Information Technology - Open Systems Interconnection - The Directory: Models.

c. Draft Amendment 1 to ITU Rec. X.501 (1993) | ISO/IEC 9594-2: 1993.

d. Draft Amendment 4 to ITU Rec. X.501 (1993) | ISO/IEC 9594-2: 1993.

e. Proposed Draft Amendment to ITU Rec. X.501 (1993) | ISO/IEC 9594-2: 1995.

f. ITU-T Recommendation X.509 (1993) | ISO/IEC 9594-8: 1993, Information Technology - Open Systems Interconnection - The Directory : Authentication Framework.

g. Technical Corrigendum 2 to X.509 (‘90 & ‘93) | ISO/IEC 9594-8 (‘90 & ‘93).

h. Draft Amendment 1 to ITU Rec. X.509 (1993) | ISO/IEC 9594-8 : 1993.

i. ITU-T Recommendation X.520 (1993) | ISO/IEC 9594-6: 1993, Information Technology - Open Systems Interconnection - The Directory: Selected Attribute Types.

j. Draft Amendment 2 to ITU Rec. X.520 (1993) | ISO/IEC 9594-6: 1995.

k. ITU-T Recommendation X.521 (1993) | ISO/IEC 9594-7: 1993, Information Technology - Open Systems Interconnection - Selected Object Classes.

l. Draft Amendment 1 to ITU Rec. X.521 (1993) | ISO/IEC 9594-7: 1995.

ABBREVIATIONS

ASCII	American Standard Code for Information Interchange
CA	Certification Authority
CESG	Communications-Electronics Security Group
CRL	Certificate Revocation List
EDI	Electronic Data Interchange
EDIFACT	EDI for Administration, Commerce and Transport
HMG	Her Majesty's Government
HTTP	Hypertext Transfer Protocol
ISDN	Integrated Services Digital Network
ITU	International Telecommunications Union
PCA	Policy Certification Authority
PKC	Public Key Cryptography
PKI	Public Key Infrastructure
RFC	Request for Comment
SMTP	Simple Mail Transfer Protocol
TLCA	Top Level Certification Authority

I. INTRODUCTION

A. Purpose and Scope

1. Interdepartmental discussions are currently in progress to determine the general requirement for a Public Key Infrastructure (PKI) within HMG, and the associated issues. In the expectation that these discussions will in due course endorse a need for some level of PKI service, CESG has been developing generic technical recommendations for supporting these services.

2. This document describes CESG's recommended architecture for an HMG public key infrastructure (PKI) to support authentication between communicating systems. The main objective of the recommendations is to facilitate pan-government secure communication services (e.g. electronic mail, file transfer, electronic trading and communication with the public). The framework is suitable for communications over both public bearers (e.g. X.400) and Internet technology (e.g. SMTP, HTTP). The objective is met by:

a. simplifying the implementation of such services within government,

b. ensuring secure communication between departments is possible,

c. facilitating future inter-operability with commercial users,

d. maximising the use of commercial technology in a controlled manner.

3. The HMG PKI should be capable of interoperating with other PKIs (e.g. those of other governments and commercial PKIs).

4. A companion publication to this document, CESG Infosec Memorandum No. 14, provides an architecture for a PKI to support the confidentiality of communications.

5. Although not a government standard as such, this document forms the current basis upon which government implementation trials in this area are moving forward. Depending upon the experience gained during these trials, it may well contribute to a future formal standard. Future CESG publications will define a data encapsulation protocol, protocols for key management within the PKI, and provide implementation guidance to product developers.

6. An architecture specifically for secure electronic mail is the subject of the CESG Architecture for Secure Messaging (CASM), which will be described in a separate series of publications. The PKI described in this Memorandum can be used to support CASM compliant mail systems.

7. Annex A of this document provides a tutorial on PKI and public key cryptography concepts.

B. Background

8. Over the past few years electronic mail has become the most popular medium for exchanging information within the IT industry. It is used by both people and computer processes to exchange a variety of 'message' formats, from simple ASCII to machine-readable business documents, eg. EDIFACT. Communication systems such as the Internet, which

support electronic mail, allow users to send mail over vast distances, and to many different countries.

9. There are currently two main ‘standards’ for electronic mail in widespread use. The first is based upon the work of the International Telecommunications Union (ITU) and is documented in the X.400 set of recommendations. The second is based upon work carried out by a number of organisations associated with the Internet and documented in a series of ‘Request For Comment’ papers (RFCs). The standards define the various protocols required to transfer mail from one user to another. For example, the protocol used to transfer mail between mail servers or switches is defined in X.400 as the P1 protocol, and for the Internet as the Simple Mail Transfer Protocol.

10. Security (be this for confidentiality, authentication or other aspects) is not a major feature within current implementations of these standards. The Internet does not provide its users with any confidentiality or integrity services. There are a number of ‘add-on’ products which provide these services, but none of them are approved for the protection of HMG protectively marked material. The X.400 recommendations do define a set of security services as part of the protocols, however these are specific to X.400 and few implementations are commercially available. The mail systems and the information they carry are therefore susceptible to component failure, user misuse, and malicious attack, which may result in:

a. the loss or disclosure of information,

b. the modification of information,

c. the impersonation of legitimate users,

d. the denial of message generation or receipt,

e. the denial of system services.

11. The popularity of electronic mail within government has meant that it has now been adopted for transferring official material within and between departments, and between government and commerce and other outside bodies. As much of this use became established before the new protective marking scheme was introduced in 1994, we have a de facto situation in which a significant proportion of this information now deserves a protective marking. Even where a protective marking is not formally warranted, users seek certain assurances from their electronic mail systems. These assurances can be provided to the user in the form of a number of user to user security services, such as:

a. data confidentiality,

b. data integrity,

c. proof of origin,

d. proof of delivery/receipt,

e. non-repudiation of origin,

f. non-repudiation of receipt

12. In addition to electronic mail, users will wish to make use of other communication services allowing them to download documents, engage in electronic trading, or access directories and databases for example. Authentication is important in these contexts as well, in order to assure the user that he is communicating with the correct remote entity, and to ensure that the origin of data can be established without doubt.

13. The security services are implemented in the form of an encapsulation protocol which conveys security information (eg. protective markings, digital signatures, user identities) between users. The services provided by the protocol are based upon public key cryptographic techniques. These techniques require the distribution of key material through trusted channels, and the ability to authenticate material distributed through untrusted channels. This document defines the authentication framework recommended to verify the authenticity of data objects within and communicated between computer systems.

14. CESG's policy for the development of products to provide these services is to encourage industry to incorporate CESG approved algorithms into their existing products. This has been done successfully in the past with CESG's RAMBUTAN chip. However it is now recognised that one of the major requirements for communications products is that they should interoperate with similar products developed by other manufacturers. In order to achieve this, it is no longer practical to provide only the algorithms to industry, and further guidance is now required. The objective of these recommendations is therefore to provide this guidance, and to encourage manufacturers to develop products which will be able to interoperate with similar products from other sources. This should enable a single architecture for secure communication to be implemented within HMG which maximises the use of commercial products, whilst minimising the infrastructure required to support them.

II. AUTHENTICATION FRAMEWORK

15. The authentication framework is based upon the ITU's directory authentication framework (Reference f). The framework employs digital signatures, generated using public key cryptographic techniques, to verify the authenticity of data objects within a mail system. It should be noted that the authentication framework described here is generic and may be used with other applications requiring strong authentication, eg directories. The following are examples of data objects which can be verified within this framework :

a. user data (eg. a file, message, or receipt);

b. system security data (eg. certificates or other security data such as a user's clearances);

16. At this time the framework is only intended to provide authentication for protectively marked material and data associated with the confidentiality service, the requirements for legal authentication will require further study. However the framework and security services should provide the necessary mechanisms to meet this requirement once the many issues have been resolved.

17. A digital signature allows an entity to 'sign' a data object in a way that cannot be easily forged. In this case a signature is generated by first computing a hash or digest of the data object, then enciphering the result using a secret authentication key that is only known to the entity carrying out the signing (Figure 1). Any entity can then verify the authenticity of the data object using the associated public authentication key and parameters. The entity generates a new digest from the data object and uses this, together with the public authentication key and parameters to verify the signature.

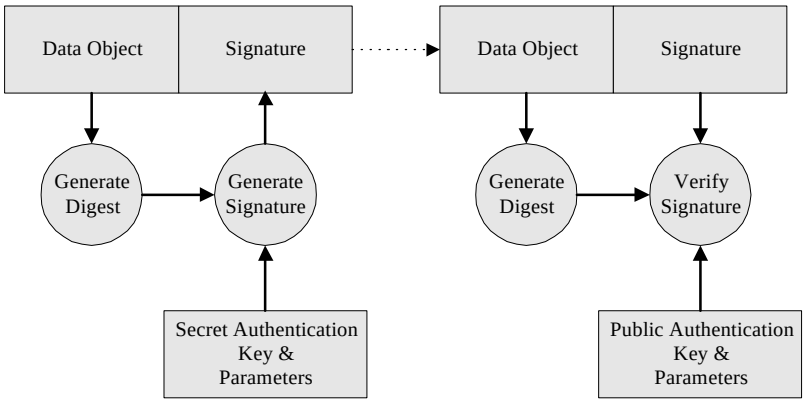

Figure 1 - Signature Generation and Verification

18. The public authentication keys are held within authentication certificates (Figure 2). The certificates are structures based upon version 3 of the X.509 certificate and selected extensions (See References f, g and h). The secret authentication keys are also held within structures, known as secret key tokens. The keys within the tokens may be enciphered with a user code which is distributed to the user via a different channel to the tokens themselves.

<table>
<tr><td colspan="10">Certificate Data</td><td colspan="2">Signature Structure</td></tr>
<tr><td rowspan="2">Version</td><td rowspan="2">Serial Number</td><td rowspan="2">Algorithm Identifier</td><td rowspan="2">Issuer</td><td colspan="2">Validity</td><td rowspan="2">Subject</td><td colspan="2">Subject Public Key Information</td><td rowspan="2">Authority Key Identifier (Extension)</td><td rowspan="2">Key Attributes (Extension)</td><td rowspan="2">Algorithm Identifier</td><td rowspan="2">Digital Signature</td></tr>
<tr><td>Valid From</td><td>Valid To</td><td>Public Authentication Key</td><td>Algorithm Identifier</td></tr>
</table>

Figure 2 - Authentication Certificate

A. Certification Authorities

19. A Certification Authority is responsible for generating and signing authentication certificates. The signatures appended to these certificates are generated from the authority's secret authentication key, and the parameters held within the authority's own authentication certificate. A Certification Authority may generate and sign its own authentication certificate, or the authority may be provided with its certificate by a higher level authority, so leading to the concept of a hierarchy of authorities. The Certification Authorities may or may not generate the keys themselves. For example, to provide a non-repudiation service users would generate their own secret and public authentication key pairs, then pass the public part to a Certification Authority. The Certification Authority would then satisfy itself that the user had the associated secret key before incorporating it into a certificate which the authority would then sign.

20. The certification hierarchy for HMG will consist of four types of certifying entity: Top Level Certification Authority, Policy Certification Authority, Certification Authority, and User (Figure 3).

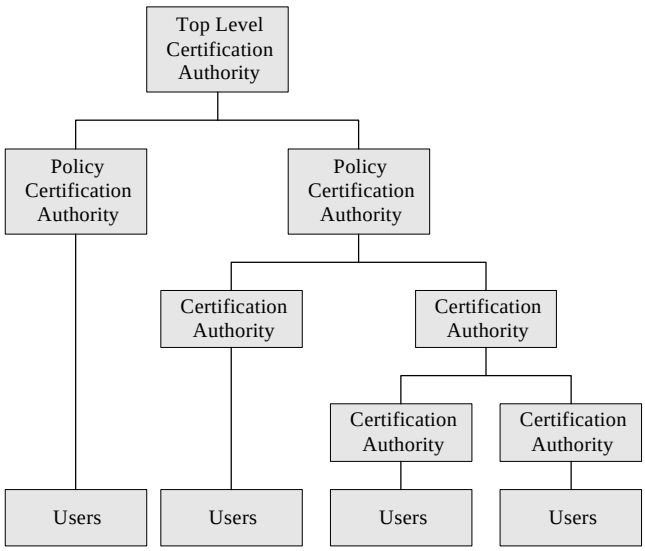

Figure 3 - Certification Hierarchy

a. The Top Level Certification Authority is deemed the 'root' of the hierarchy, and is responsible for signing the certificates used by the Policy Certification Authorities beneath it. The Top Level Certification Authority is also responsible for the management of cross certification, either between its subordinate Policy Certification Authorities, or between hierarchies.

b. A Policy Certification Authority is defined as the top of the certification path within a particular domain. It is responsible for allocating the secret authentication keys and certificates to Certification Authorities, and ensuring that all subordinate authorities conform to the defined security policy for certification, in addition to providing a point of reference for certification outside the domain (cross certification). In order to minimise the depth of the hierarchy a policy certification authority may also register users, and allocate their secret authentication keys and certificates.

c. A Certification Authority is responsible for registering users, allocating their secret authentication keys and associated certificates. In large organisations it may be necessary to add further layers to the hierarchy, in which case a hierarchy of Certification Authorities may be established. Therefore a Certification Authority may also allocate the secret authentication keys and certificates to authorities below it.

d. Users may only sign user data.

21. A certification path enables an entity to verify the authenticity of a certificate.A certification path is simply an ordered sequence of certificates between the certificate being verified and a point trusted by the verifier. Certification paths can become long and inefficient to process, therefore short paths are encouraged whenever possible.

22. A certificate must be associated with a uniquely identifiable entity, and the identity of that entity must be cryptographically bound to the key material within it. The method adopted for uniquely identifying entities within the system is based on the distinguished name convention defined in Reference a. It should be noted that an entity may be associated with more than one distinguished name. A naming authority is responsible for ensuring that each entity within its jurisdiction is provided with a unique distinguished name. This can only be ensured if the naming authority itself has a unique distinguished name, as all names assigned are subordinate to the authority. Therefore a naming authority must first register with a higher level authority. The highest level authority within the UK is the UK Name Registration Authority, which is part of the British Standards Institution. The certification authority and naming authority must work closely together, and may even be one and the same.

23. A distinguished name may be constructed from a number of attributes, such as telephone number, international ISDN number, role occupant, street address, house identifier, etc. However in order to simplify the processing of the certificates only a subset of the attributes defined in Reference i will be supported within the certificate. Therefore a combination of the following attributes may be used within a certificate to uniquely identify an entity: country name, organisation name, organisational unit name, locality name, surname, given name, initials, common name, and title. A naming authority may use other attributes to identify an entity, however only the above shall be used within certificates.

B. Certificate Revocation List

24. The ITU's directory authentication recommendations advocate that certificate revocation lists are used to indicate when a secret key is for some reason revoked. Furthermore they state that it is the issuing authority's responsibility to record this fact in a Certificate Revocation List (CRL). In the event of an authority's secret authentication key being revoked it will be necessary to re-issue the certificates of all the entities below it in the hierarchy. The

mechanisms for revoking these keys requires further study, and involves more than security issues. Such issues will be covered in future CESG Manuals.

C. Certificate Verification

25. All authentication certificates should be successfully verified before the data they hold is used. The process is carried out in three stages. The first stage checks any relevant data within the certificate being verified, such as its validity period. The second stage checks to ensure it has not been revoked, eg. if the associated secret key has been compromised, by checking the revocation list generated by the certificate's issuer. The final stage verifies that the signature is authentic, using information held within its issuer's certificate (Figure 4).

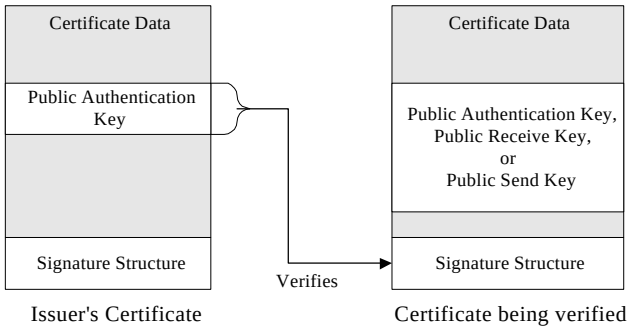

Figure 4 - Signature Verification

26. This process must now be carried out on the issuer's certificate, and all the certificates within the certification path until a trusted point is reached (Figure 5), e.g. the certificate of the Top Level Certification Authority (note, the TLCA public key is distributed out of band).

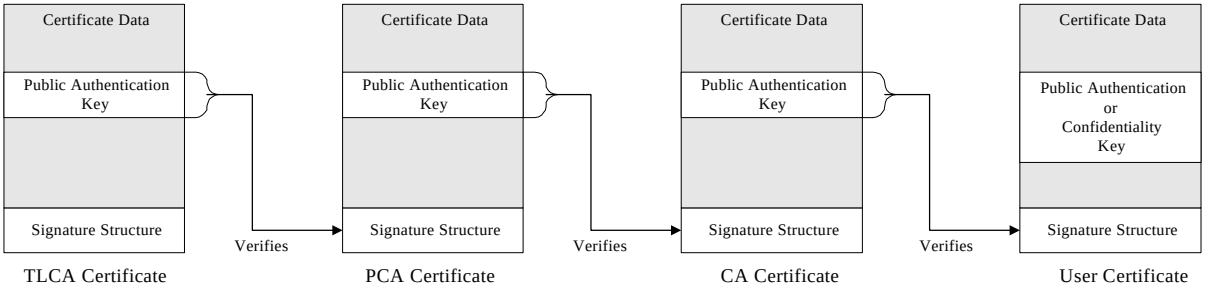

Figure 5 - Verification of Certification Path

D. User Data Verification

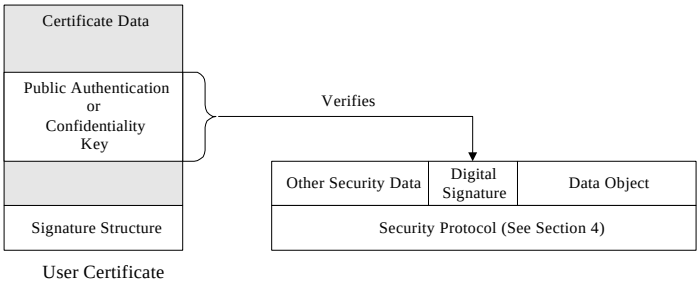

Figure 6 - User Data Verification

27. Signatures are also applied to user data inorder to verify its integrity and origin (Figure 6). The signatures generated are appended to the user data as part ofthe security protocol used to transfer data between two entities. A signature is verified using the public authentication key of the entity which signed the data object. Once the authenticity of the data object has been established, the certificate containing the public authenticationkey must itself be verified as described above.

Annex A A Guide to Public Key Infrastructures

Introduction

28. The following paragraphs provide a brief outline of the basic concepts of Public Key Cryptography and the rationale for a Public Key Infrastructure to support the maintenance and distribution of key material, certificates etc.

Background

29. Traditional cryptography is based upon the use of *symmetric* keys and is characterised by the fact that the same keys are used for both encryption and decryption. Essentially symmetric cryptography provides security services at the link level. Writer-to-reader security services such as authentication and non-repudiation require the use of additional off-line techniques.

30. However the proliferation of communications and networked information systems has resulted in an increasing demand for 'off-line' writer-to-reader services, in particular authentication and non-repudiation, to be provided 'on line'. In addition, there is a requirement for content integrity between originator and recipient. Furthermore, the provision of security services is no longer confined to the network domain and certain functionality is moving to the desktop in the user domain. The additional security functionality required by users can be achieved by the use of *asymmetric* or public key cryptography.

31. Public key cryptography (PKC) has been known as a concept for about twenty years. Stripped of the mathematics, which are complex, it is in essence a means for parties to communicate securely in electronic form *without prior exchange of dedicated secret key material*. This is the basic difference from traditional secret key cryptography. PKC takes a fair amount of computing power to run. This is why it is has only relatively recently started to become a practical proposition for non-specialists. PKC techniques lend themselves to not just the confidentiality aspects of information security, but to other services of increasing relevance to business, both HMG and outside. These services include integrity, authentication and non-repudiation.

32. PKC is characterized by the use of two different but mathematically related keys to perform the cryptographic functions. Each person/entity has a private and public key. The public key is available to the user community in general and is usually posted in an X.500 directory. The private key is known only to the person/entity to whom it is issued. Confidentiality, integrity and authentication (the latter two usually realized in the form of a digital signature) can be achieved by different manipulations of public/private key pairs. Other security functions are supported by additional cryptographic processes. It should be noted that the use of asymmetric cryptography does not exclude the use of symmetric cryptography to support certain functions within the overall scheme. Furthermore, it is normal practice to use one public/private key pair to perform the digital signature, and a different key pair (usually of longer key length) to provide confidentiality through the encryption of the one-time symmetric key. See below for a brief 'tour' of asymmetric cryptography and corresponding security services.

33. An essential feature of PKC is that it must be possible to prove the authenticity of a public key. To achieve this the public key element of those security services derived from the public/private key pair must be 'bound' to the identity of the user in a secure manner. This

binding is achieved by means of a public key certificate using the X.509 format. The management of the certificates, and the provision of user access to both the certificates and the public keys may be carried out using a *Public Key Infrastructure* (PKI). A PKI will enable end-users to obtain authentic key material for those individuals and system components with which they need to exchange data. A PKI will thus support confidentiality, authentication, integrity and non-repudiation services between end-users, between entities, or a combination of both. The PKI entities which allow for the provision of this material are referred to in CESG Infosec Memorandum No. 15 as *Certification Authorities* (CAs).

34. A PKI can also be used to support an extension to the confidentiality service by the creation and distribution of private keying material The PKI entities which provide this service are referred to by CESG Infosec Memorandum No. 14 as *Certificate Management Authorities* (CMAs), but are sometimes denoted in other publications as *Trusted Third Parties* (TTPs). A CMA can also provide an escrow service whereby private keys can be stored and subsequently released either to the registered owner to achieve data recovery should a key be lost, or to intelligence or law enforcement agencies under due process of law. It is certain that a large number of CMAs will exist in the Global Information Society representing various groupings of end users. Hence in order to facilitate the transaction processing across user groups it will necessary to harmonize the workings of CMAs.

35. PKC techniques appear certain to become an economical and favoured means of protecting HMG electronic data transactions, but their potential can only be fully realised as shown above by taking a pan-government approach which establishes a Public Key Infrastructure. This would have applications in e-mail, electronic data interchange (EDI) with business and finance, and formal messaging, all services which are being increasingly used by government departments. The existence of a PKI would also facilitate the interconnection of UK IT networks to other government and commercial networks both national and international.

36. The cost benefit associated with the use of e-mail and EDI for contracting is one factor forcing the pace as government departments strive to reduce their costs. In this electronic environment it is important to replicate the safeguards that have traditionally been applied to paper-based systems to provide adequate confidentiality, integrity and authentication services. Electronic systems will often use cryptographic techniques to provide equivalent services.

An overview of asymmetric cryptography

37. The following paragraphs define the major security services required for Asymmetric Cryptography.

Hashing

> The use of an algorithm to create a unique fingerprint for each document. A small change in the source document changes a large number of bits in hashing code (fingerprint).

Digital Signature

> This requires a public/private key pair. The signature is derived by the sender applying his private key to the data (or a hash of the data). This signature may then be verified by any recipient using sender's public key.

Encryption

This requires public/private key pair. Encryption of one-time symmetric confidentiality key is performed by sender using intended recipient's public key. Decryption of symmetric key performed by recipient using his private key.

38. The following paragraphs describe the stages involved in a secure messaging system using asymmetric public key cryptography.

Definition of Private/Public Key Pairs.

-Bob's key pair for digital signature - KEY SET ALPHA
-Bob's key pair for confidentiality - KEY SET BRAVO

-Alice's key pair for digital signature - KEY SET CHARLIE
-Alice's key pair for confidentiality - KEY SET DELTA

Scenario 1 - Bob Sends a Message to Alice

Bob

- Generates hashing code for document using hashing algorithm.
- Signs hashing code to provide digital signature using ALPHA private key.
- Appends hash code to document.
- Generates a one-time, symmetric key.
- Encrypts document using symmetric key.
- Encrypts the symmetric key using Alice's DELTA public key.
- Transmits message to Alice.

Alice

- Decrypts the one time symmetric key using DELTA private key.
- Decrypts document using one-time symmetric key.
- Strips off the signature from the hash code using Bob's ALPHA public key.
- Regenerates the document fingerprint using the hashing algorithm and compares with the received hash code.

-- If OK message is authentic and is the original.

Scenario 2 - Alice Sends a Message to Bob

Alice

- Generates hashing code for document using hashing algorithm.
- Signs hashing code to provide digital signature using CHARLIE private key.
- Appends hash code to document.
- Generates a one-time, symmetric key.
- Encrypts document using symmetric key.
- Encrypts the symmetric key using Bob's BRAVO public key.
- Transmits message to Bob.

Bob

- Decrypts the one time symmetric key using BRAVO private key.
- Decrypts document using one-time symmetric key.
- Strips off the signature from the hash code using Alice's CHARLIE public key.
- Regenerates the document fingerprint using the hashing algorithm and compares with the received hash code.

-- If OK message is authentic and is the original.