KEY-MANAGEMENT

PHILOSOPHY

Philips Crypto B.V.

PHILIPS

KEY-MANAGEMENT

PHILOSOPHY

Document No. 9922 154 13304

Subject to modification without prior notice.

Printed in The Netherlands

KEY-MANAGEMENT PHILOSOPHY for the NEW GENERATION CRYPTO EQUIPMENT

1 INTRODUCTION

1.1 General

Cryptography is a means of protecting information against unauthorised inspection and manipulation. Protection is obtained by transforming the original information or **plain text** into a **cryptogram** which makes no sense to anyone for whom it is not intended. The transformation operation is called **encryption** and the process of retrieving the plain text from the cryptogram is called **decryption**.

Encryption and decryption are usually carried out by means of a **cryptographic algorithm** which is able to perform a large number of transformations, depending on some additional information known as the **key**.

Many cryptographic algorithms have been published in the literature, and their relative strengths (i.e. the degree of difficulty involved in recovering the plain text – or even the key – from the cryptogram) have been widely discussed. This paper proceeds from the assumption that, with the exception of the key, everything about an algorithm itself is public knowledge, and that therefore the protection afforded by cryptography depends entirely on the secrecy of the specific key that is in use at any given time.

It will be apparent that certain problems are inherent in the handling of keys within a secure communication system. On the one hand the need to preserve the secrecy of keys is essential; on the other hand keys must be generated, distributed, copied, transported, stored, transformed, published, authenticated and, finally, destroyed. These problems, of course, play an important role during the installation of a crypto system; in addition – because of the limited period of validity of each key, the dynamics of the system and the constant possibility of compromise, they are also continuously present throughout the system's operational lifetime.

In designing a key-management system capable of providing secure and efficient solutions to these problems, many factors must be taken into account. The following paragraphs contain a more detailed survey of the most important of these factors – namely the type of network concerned, the security services to be provided, and the type of crypto systems to be used.

1.2 Types of network

There are many ways of characterising communications networks, e.g. data rate, reliability, signalling methods, switching (circuit, message or packet), etc. For the purpose of designing key-management systems, the following classification seems appropriate:

(a) Random networks with end-to-end security

Usually the network has many subscribers, each of which is able to communicate with any of the others. The actual physical route of information flow is not known beforehand and is transparent to the subscribers. End-to-end security must be provided between each pair of subscribers.
The public telephone service is an example of this type of network.

(b) Point-to-point networks

These networks can be regarded as simplified versions of the random networks. Usually a special leased or dedicated connection is set up between two parties who wish to have secure communications with each other.

(c) Broadcast networks

In this type of network, one party transmits a message to one or more receiving parties, without immediate (on-line) reply (confirmation).

Radio networks and telex with store-and-forward switches are examples of broadcast networks.

(d) Conference networks

This type of network is similar to the broadcast network but occurs only rarely as a separate network on its own; it is usually established within either a random network or a broadcast network and is therefore considered separately.

1.3 Security services

The combination of a cryptographic system and a key-management system offers security services to the subscribers of a network. These services include:

(a) Authenticity

- Peer entity: are you sure that you are communicating with the right party?
- Data origin: what is the source of the incoming information?
- Equipment: is the cryptographic equipment original? (i.e. not fake, not bugged, not tampered with)
- Access control: are you allowed access to the communication system from a specific terminal?

(b) Confidentiality

- Data confidentiality: protection against unauthorised interpretation of the data.
- Traffic confidentiality: protection against revealing when communication is actually taking place.
- Identity concealment: protection against revealing who is communicating with whom.

(c) Integrity

- Protection against manipulation of the transmitted data, i.e. has the transmitted information been intentionally or unintentionally changed (deletions, repetitions, insertions, etc.)?

(d) Non-repudiation

- Protection against the denial of transmission or reception of information.

Not **all** these security services have to be available in **every** secure communications system; the provision of specific services depends largely on what the user requires and on what major threats are perceived to be applicable.

1.4 Cryptographic systems

Present-day cryptographic algorithms can be divided into two groups, namely classical (symmetric, secret-key) algorithms and public key (asymmetric) algorithms.

The encryption and decryption keys for a classical cryptographic algorithm are essentially the same and have to be kept secret. In a public-key cryptographic system both keys are different and it is practically impossible to determine the decryption key given the encryption key; it is therefore only necessary to keep one of the two keys secret.

The opinion is widely held that a public-key crypto system really has no key-management problem. The major problem here, however, is the authenticity of the public key.

2. GENERAL PHILOSOPHY

In a well-designed secure communications system, the users will hardly be aware of the security measures; i.e. the operation of the security system will mostly be transparent to the users.

The design philosophy for Philips Usfa's New Generation Crypto Equipment therefore features the following aspects:

- the use of high-grade cryptographic algorithms derived from Usfa's long experience in the theory, design and production of cryptographic equipment;

- the provision of full protection with a minimum of operator actions;

- the provision of highly reliable equipment which meets or exceed the requirements of international organisations such as TNO or PTT;

- the provision of a tailor-made secure communications system for each customer (which implies a separate, non-obligatory, consultancy phase);

Above all, the equipment must be highly cost-effective.

Experience has demonstrated that, too often, the key-management system represents a heavy financial or procedural burden for the owners or operators of a secure communication system. Philips Usfa's New Generation Crypto Equipment therefore is prepared for key-management systems that have the following features:

- infrequent exertion by operators or organisation - most of the effort is expended during system installation;

- extreme flexibility - virtually no restrictions on future expansion;

- minimal requirement for supporting equipment;

- state-of-the-art hardware for the intelligent user-token, namely the Smart Card (chip card).

2.1. Cryptographic algorithms

Each customer is able to have his own cryptographic algorithm. To the best of our knowledge, each algorithm will be practically unbreakable in that the investment in time, money and resources needed to break a system will be extremely high. Algorithms may be tested and approved by organisations such as TNO, and details of algorithms can be placed at the disposal of the customer concerned.

2.2 Consultancy

A customer can be best served only by a secure communications system that is tailor-made for his organisation and its security requirements. An efficient system can be designed only if the specific problems, and the feasible alternative solutions, are thoroughly understood – both by Usfa and by the customer.

Usfa will therefore offer a consultancy service to potential buyers, with the aim of providing each customer with a detailed proposal for a tailor-made security system capable of being implemented (possibly step-by-step) with Usfa's new product range.

3. PROPOSED KEY-MANAGEMENT SYSTEMS

3.1 Random networks with end-to-end security

Assuming that a symmetric cryptographic algorithm will be used in this type of network, the main problem here is to provide each pair of subscribers with a unique key which is not available to any other pair.

In its simpler form (i.e. for small systems), an on-line Key Distribution Centre or a Key Cube (off-line KDC) might be considered. An on-line KDC, however, is expensive; it is also impractical in operation because, prior to each secure session, the user has to contact the KDC to obtain a new session key.

In a Key Cube system for a network with a total of N subscribers, each subscriber terminal stores 2 x (N – 1) keys. This number grows linearly with the number of subscribers and therefore has a practical limit of a few thousand subscribers.

For its New Generation Crypto range, Philips Usfa has designed a new key-management system based on an intelligent user-token such as the Smart Card. This system employs the off-line KDC (Key Cube) principle with an additional key-storage-reduction scheme newly developed by Philips Usfa.

The system, which is known as PHILKEY 2000, has the following features:

- Each subscriber has his own personal keycard which is used with the security equipment to establish secure and private communication with any of the other subscribers;

- a PIN number can be supplied together with the keycard, thereby ensuring that the card can be used only by the authorised card-holder;

- each subscriber can use his keycard with any terminal; specific 'limited-access' configurations can also be defined and cryptographically secured;

- a subscriber can verify the identity of the called party by means of an identity message displayed on the crypto equipment;

- the system is secure against the introduction of fake terminals and interrogation by unauthorised parties;

- with existing Smart Card technology the system capacity is in excess of 1.5 million subscribers. Due to a logarithmic relationship between the number of subscribers and the amount of key information stored, however, the size of the system is virtually unlimited;

- the keycards can be replaced at suitable intervals (say every one or two years); replacements can be carried out in random subscriber order and may take as long as the period of use;

- the keycards can carry additional key material, e.g. for special nets (VIP nets) or for conferencing - see also 3.4;

- collusion by means of genuine cards and equipment is unprofitable in practice;

- keycards can be manufactured in strict secrecy by Philips Usfa: PC-based equipment for filling the cards and printing names on them will be available to customers.

3.2. Point-to-point networks

Two situations can be identified in this context:

- point-to-point connection within one organisation;

- point-to-point connection between two (possibly mutually distrusting) organisations.

Although in the latter situation there may well be an authority which is trusted by both organisations, we will assume that there is not.

(a) Point-to-point connection within one organisation

Here again the proposed cryptographic system is symmetric and therefore all that is necessary is to generate a secret key and load it into the device at each end. This can be done in many ways. Philips Usfa offers the following alternatives:

- crypto devices (equipped with a keyboard and display) capable of generating keys themselves without the aid of supporting equipment; plus a key-transfer device which can store a few keys and is used for transport purposes;

- a special key-generation device which generates one or more keys when connected to a crypto device, and which can also be used for transport purposes;

- PC-based equipment which can be purchased from Philips Usfa to load key material into the crypto devices; in this case the crypto devices are equipped with card-readers. Remote key-transformation and replacement are possible with this type of equipment.

(b) Point-to-point connection between two organisations

In this case the proposed cryptographic system (in particular the RSA public key system) is asymmetric. Each organisation generates its public and secret keys, using one of the last two alternatives in 3.2(a). They then exchange their public keys, using a courier service (DHL) to ensure authenticity. These keys can then be used to exchange a secret key for use in the actual symmetric cryptographic system used for the encryption and decryption of information.

3.3 Broadcast networks

Crypto modules for use with radio equipment are able to store several (30) net keys and device-unique keys, the latter being used for key transfer by the network controller(s). The controller functionality may be built into the radio or may optionally be obtained by using a special key-generation device in conjunction with a radio.

In small radio nets, each radio in the network can be given a controller functionality by fitting a Key Cube.

Crypto equipment for telex networks with store-and-forward switches largely fall under the category described in 3.2(a), but may additionally have the automatic key-selection feature, which enables a receiving telex equipment to determine which key was used for message encryption at the transmitting station.

3.4. Conference networks

A conference within a random network with end-to-end security can be established in two ways: pre-programmed or automatically.

For pre-programmed conferences, special keys present in the keycards can be selected manually for use by the participating subscribers. It is also possible for an organisation to use special conference cards (Red, Green or Gold cards) for selected members.

Automatic conferencing is set up as follows: after a conference bridge has been established by the telephone switch, the initiating subscriber's device addresses each participating subscriber's device with the unique key information shared by each pair, and sends a randomly generated or stored conference key to those devices. Automatic conference setup will be available in future and will depend on the specific switches used in the network.

4. CONCLUDING REMARKS

Many technical and theoretical details, which were felt to be inappropriate in a commercial presentation, have been omitted from this report.

The classification of networks adopted herein was based purely on the different key-management problems; there are of course many other classifications, such as circuit-, message- or packet-switch networks, ISDN, IBCN, etc.

Usually the key-management system forms a separate overlay on the network, but existing signalling procedures in the network may impose some restrictions on the key-management system.

The actual cryptographic algorithms used in the equipment depend heavily on who the customer is. It is appropriate here to stress the importance of having various algorithms for the various customer groups. The implementation should be such that these algorithms can be interchanged – i.e. there should be a common functional interface.

ATTENTION
Our new name and address are as follows:
Philips Crypto B.V.
P.O. Box 218, 5600 MD EINDHOVEN, Netherlands
Tel: 40 722600 Fax: 40 723658 Telex: 35000 phtc nl

Philips Crypto B.V.

Hurksestraat 9
Postbus 218
5600 MD EINDHOVEN
Netherlands

Telephone: +31 40 722600
Telex: 35000 phtc nl
Fax: +31 40 723658