Recommendation T/SF 56 (Copenhagen 1987)

SERVICES AND FACILITIES FOR INFORMATION SECURITY IN VISUAL TELEMATIC SERVICES

Recommendation proposed by Working Group T/WG 7 "Services and facilities" (SF)

Text of the Recommendation adopted by "Telecommunications" Commission:

"The European Conference of Posts and Telecommunications Administrations,

considering

1. several teleconferencing services are being harmonised by CEPT, in which real-time, or quasi-real-time visual telematic services are provided between two or more terminals,
2. visual telematic services are a useful alternative to face-to-face meetings, but that business customers will be reluctant to use the service unless confidentiality can be assured,
3. revenue potential will be maximised if the level of security of visual telematic services is perceived to be acceptable to customers of the Administrations,
4. services and facilities for information security in visual telematic services may be provided in several different ways, according both to local circumstance, and to the organisation of the networks that support the service,
5. visual telematic services conforming to the CEPT Recommendation for security may have an operational requirement to interwork with non-conforming terminals, or with terminals operated by Administrations outside CEPT,
6. information confidentiality and key-management comprise the set of security supplementary services that have the greatest economic justification in visual telematic services,
7. the options for information confidentiality currently being considered by CEPT Administrations, and available to CEPT technical groups (as notified on 1987-05-06) are: The American Data Encryption Standard; The GRETAG privacy system and the B-CRYPT system,
8. the options for key-management available to CEPT technical groups are: Manual exchange of secret key; Bilateral master key protocols; Stand-alone number-theoretic systems; and a visual services derivative of CCITT X.ds7 Public directory number-theoretic key-management system,

recommends that

1. the following guide is adopted for the further detailed study of the optional information security supplementary services for visual telematic services,
2. three network service security options have currently been identified, which can be used by Administrations at their discretion, in which:
   - 2.1. for a minimum cost solution, the security supplementary services may be implemented between the network nodes supporting the visual telematic services so as to provide protection to those parts of the route of the bearer network that are most exposed to monitoring or attack,
   - 2.2. at a higher cost than 2.1., the security supplementary services may be provided on an end-to-end basis, thus protecting the local network part of the visual telematic service route, as well as the inter-nodal network,
   - 2.3. in order to provide a harmonised procedure for dealing with non-conforming terminals, an interworking capability may provide facilities for secure visual telematic services by means of a relay node or gateway, offering conversion facilities for visual telematic services deploying differing security parameters,

3. there should be compatibility between terminals of the visual telematic services that have invoked the same set of security supplementary services,
4. direct inter-communication should be possible between terminals arranged in different network security topologies of clause 2. of this Recommendation,
5. the method/system of information confidentiality should ensure that for visual telematic services:
   5.1. the method/system is available to customers of all CEPT Administrations without restriction, and should be multi-sourced,
   5.2. the cost is reasonable compared to the functionality offered,
6. subject to bilateral agreement between the Administrations participating in the visual telematic service, any other arrangement may be used for confidentiality and interworking with terminals conforming to the CEPT Recommendations for confidentiality effected by means of the conversion facility described in clause 2.3. of this Recommendation,
7. manual exchange of secret keys is adopted, pending Recommendations from CCITT on systems that can be used for key-management."

Annex

1. THE VISUAL TELEMATIC SERVICES MARKET

Several teleconferencing services are being harmonised by CEPT in which real-time, or quasi-real-time visual services, sometimes accompanied by speech, text or graphic services, are provided between two or more terminals by means of high-speed bearer services.

Market surveys in several countries indicate that these visual telematic services are a useful alternative to face-to-face meetings, but that business customers are reluctant to use the service unless confidentiality can be assured to a level commensurate with commercial practice.

Therefore CEPT is recommending a repertoire of supplementary services for information security in visual telematic services that are appropriate and acceptable to its Administrations for protecting inter-European visual telematic services.

The Security of other telematic services that may be used in conjunction with visual services, for example, speech (if not part of the implementation of the visual telematic service), Teletex and graphic services, facsimile and telewriting, are addressed in separate CEPT-SF Recommendations for the security of each individual telematic service.

2. NETWORK SECURE SERVICE OPTIONS

The services and facilities for information security in visual telematic services may be provided in several different ways according to the organisation of the networks that support the service.

The choice of security options, as represented by the network secure service options described in 2.1. to 2.3., will be determined by each Administration taking cognisance of local circumstance, the compromise between the requirements of the customer, the threats to the network and the cost of the various options. However, regardless of which network security topology is chosen, the security framework for international visual telematic services should enable:

(a) complete compatibility between terminals of the visual telematic services terminals that have invoked the same set of security supplementary services,
(b) the ability to intercommunicate directly between terminals arranged in different network security topologies.

2.1. Inter-nodal protection

For a minimum cost solution, the security supplementary services may be implemented between the network nodes supporting the visual telematic services so as to provide protection only on those parts of the route of the bearer network that are most exposed to monitoring or attack, e.g.: satellite and terrestrial radio links (see Figure 1 (T/SF 56)).

The location of the security supplementary services at a network node enables the Administration to dimension the security functionality on a shared basis at strategic network switching centres, thus reducing considerably the cost of security. However, the option requires that the Administration deals with key-management and control because the information security equipment is located in the premises of the Administration.

2.2. End-to-end protection

In this option, every terminal for visual telematic services that requires security supplementary services will need the additional functionality included within the terminal. Therefore the total volume of security equipment, and its reflection in the tariff or the purchase price of the terminal, would be greater than that of 2.1. However, the local network part of the Videoconferencing link would also be protected as well as the links between network nodes (see Figure 2 (T/SF 56)).

2.3. Interworking of non-compatible terminals

Assuming that Administrations comply with the CEPT Recommendation on confidentiality for visual telematic services, then international interworking will consist of direct interconnection between compatible terminals that are structured in a security topology of either 2.1. or 2.2.

However, this Recommendation also acknowledges that, subject to bilateral agreement, other means of confidentiality may also be used. Indeed visual telematic services conforming to the CEPT Recommendation for security may have an operational requirement to interwork with non-conforming terminals, or with terminals operated by Administrations outside CEPT.

In order to provide a harmonised procedure for dealing with non-conforming terminals, a third network security option is defined in this Recommendation in which secure interworking is still possible by deploying a secure relay node or gateway offering a value-added conversion facility for visual telematic services having differing information protection parameters (see Figure 3 (T/SF 56)).

In this option the secure functionality is stripped off the visual telematic services information at a secure gateway, and new secure functionality asserted for the completion of the information flow to its destination. As the sensitive information is processed without protection within the gateway, its standards of physical security should be sufficiently high to maintain overall security, and the operating standards at the gateway must be trusted by all users.

All three options (2.1. to 2.3.) should be available for Administrations to use, as appropriate to local circumstances. Therefore implementation should allow the interworking of terminals when they have invoked the supplementary information security services, regardless of which the three network secure service options for visual telematic services have been adopted by any Administration.

3. SECURITY SUPPLEMENTARY SERVICE REQUIREMENTS

An analysis of the economic justification of supplementary information security services for visual telematic services follows. Definition of terms is consistent with the vocabulary of ISO/TC97/SC21 in regard to security architecture:

3.1. Access control

In visual telematic services that do not use permanently dedicated arrangements of networks, some mechanism for access control to visual conferences may be needed. However, it is unclear that this will be implemented as part of the supplementary services for information security.

3.2. Information confidentiality

Information Confidentiality is required to ensure the privacy of communication, which may be exposed to open bearer services involving satellite and terrestrial radio routes. It is unlikely that the full commercial potential of visual telematic services will be achieved in the business sector unless customers can be assured that confidentiality is maintained to at least commercial standards.

3.3. Information integrity

It may be technically feasible for an attacker to insert, remove or alter information flowing between visual services terminals in a way that deceives the users. But because of the interactive nature of the service, and the continuous flow of information, disruptions and replay attacks will be perceived quickly by the users. Therefore Integrity is allocated a relatively low commercial priority.

3.4. Authentication

Most visual telematic conferences are expected to take place between participants who would recognise any attempt to impersonate others involved in the conference or communication. However, in conferences between participants who, for instance, are meeting for the first time, some method of authentication may be necessary.

3.5. **Non-repudiation**

There are only very few occasions in which participants of visual telematic services would be able to benefit by claiming not to have been involved in a conference. Therefore non-repudiation is allocated a low commercial priority.

This does not necessarily apply to other telematic services such as Teletex, telewriting and facsimile, which may be used in conjunction with visual telematic services, but are outside the scope of this Recommendation.

4. INFORMATION CONFIDENTIALITY OPTIONS

The following privacy service options are known to CEPT technical groups, and are characterized in Table 1 (T/SF 56):

4.1. The American Data Encryption Standard.

4.2. The Swiss GRETAG privacy system.

4.3. The British Telecom B-CRYPT system.

Noting the factors described in Table 1 (T/SF 56), it is recommended that the method/system of information confidentiality should ensure that, for visual telematic services:

— it is available to the customers of all CEPT Administrations without restriction,

— it is multi-sourced,

the cost is reasonable compared to the functionality offered.

5. KEY-MANAGEMENT

Key-management facilities are described in the context of the visual telematic services security framework to ensure compatibility of overall security for intercommunication.

The following key-management options are known to CEPT technical groups, and are characterized in Table 2 (T/SF 56):

5.1. Manual exchange of secret key.

5.2. Bilateral master key protocol.

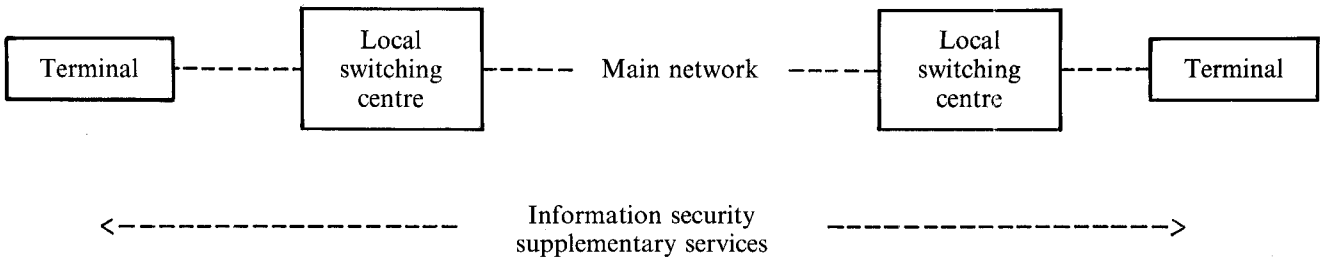
5.3. Stand-alone number-theoretic systems.

5.4. A visual services derivative of CCITT X.ds7 Public directory number-theoretic key-management system.

Noting the factors described in Table 2 (T/SF 56), it is recommended that, because of the complexity of agreeing and adopting a key-management scheme, key-management should be the subject of a separate SF Recommendation. In the meantime, it is recommended that:

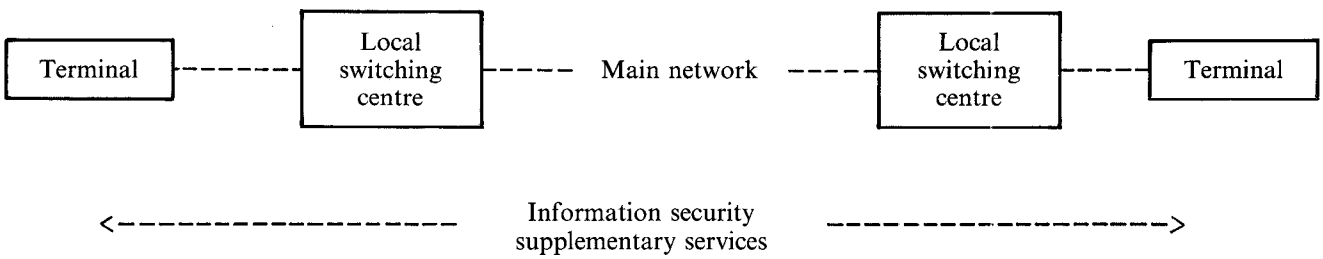
— a manual method of exchange of secret key visual telematic services is adopted,

— a review of the method of key-management for visual telematic service is carried out when the CCITT X.ds7 draft Recommendation has been adopted.



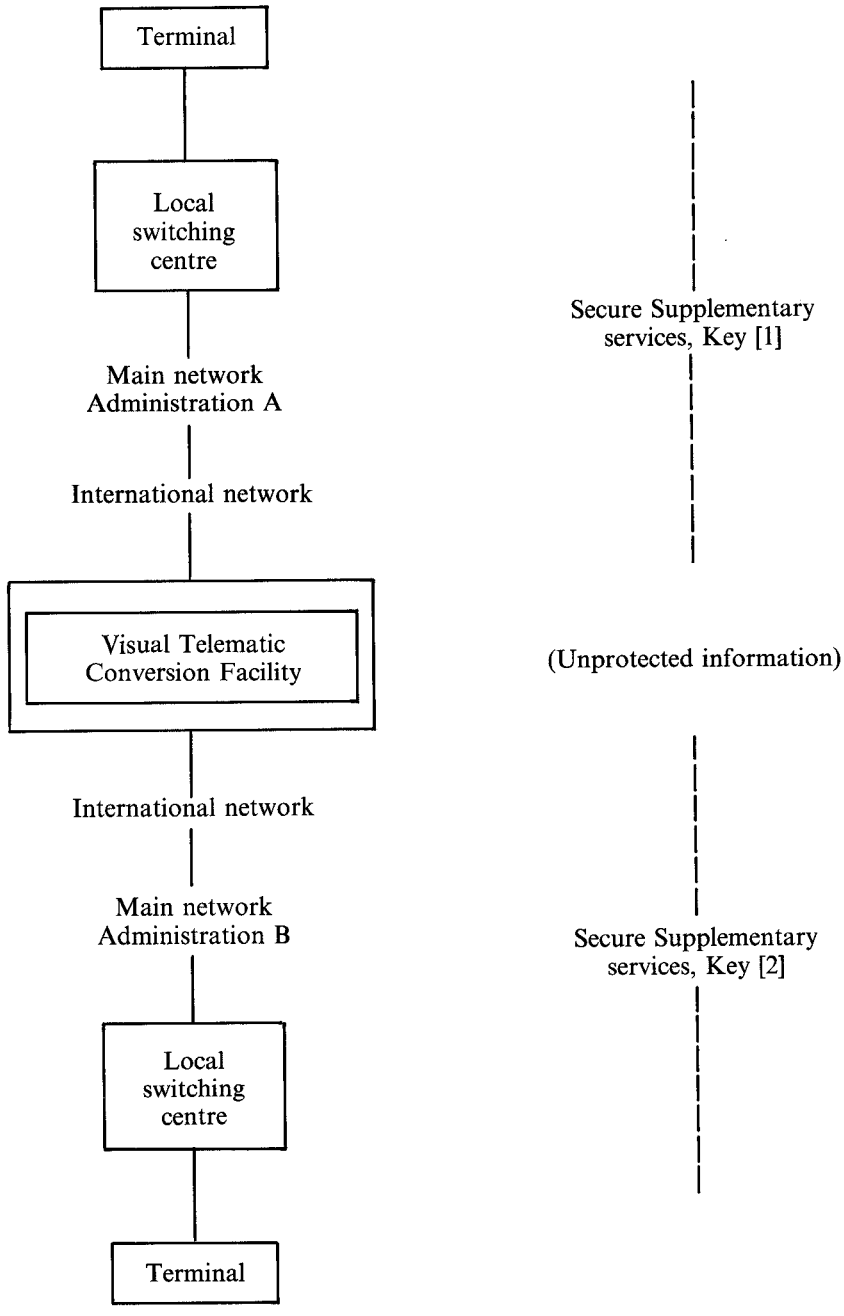
(Dimensioned according to traffic)

Figure 1 (T/SF 56). Inter-nodal network protection.



(One per terminal invoking security supplementary services)

Figure 2 (T/SF 56). End-to-end protection.



Note. For clarity the Conversion Facility is shown in the international network. In practice it would be associated with the network of one of the Administrations.

Figure 3 (T/SF 56). Conversion facility for the interworking of non-compatible terminals.

CHARACTERISTICS	DES	GRETAG	B-CRYPT
Published algorithm	Yes	No	No
Details available to PTTs	Yes	??	For manufacture
Sourced within the CEPT	No	Yes	Yes
Export within CEPT (1)	Doubtful	Yes	Yes
Export to USA/Japan (1)	Yes	Yes	Yes
Export World (1)	No	Yes	No
Level of privacy	Commercial	??	Commercial
Key size	56 bits	??	64 bits
Price	$100	$20,000	$100

Notes.

(1) Restrictions may differ according to the manufacturing source.

(2) Whereas DES and B-CRYPT are integrated circuits, GRETAG is a stand-alone encryption unit containing additional functionality.

Table 1 (T/SF 56). Information confidentiality analysis.

CHARACTERISTICS	Manual	Master-key	Num-theoret	CCITT
Type of process	Manual	Automatic	Automatic	Automatic
Unprotected secret information to be sent	Yes	When new master-key	No	No
Originator identifiable	No	Yes	??	Protocol extension
Destination identifiable	No	Yes	??	Protocol extension
Peer entity authentication	Yes	Yes	??	Yes
Public directory	No	No	Yes	Yes
Certified directory	No	No	No	Yes
Complexity	Low	Low	Medium	High
Operating cost	High	Medium	Low	Low

Table 2 (T/SF 56). Key-management.