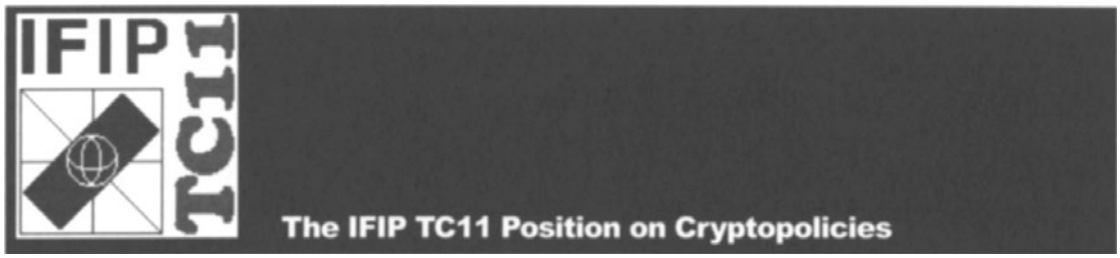
26



(This proposal has been prepared by the special task force for voting on the TC11 meeting 1997)

a)IFIP TC11 recognizes the highly important role of cryptographic mechanisms. In the Global Information Infrastructure GII and in Electronic Commerce these mechanisms will influence acceptability, usage, and competitiveness.

b)IFIP TC11 takes notice that for the convenience of discussion it is helpful to distinguish between the differing objectives for the use of cryptographic mechanisms - presevation of confidentiality, provision of the ability to authenticate people/organisations, provision of the ability to prove the integrity/completeness of data, etc.

c)IFIP TC11 is fully convinced that a range of cryptographic mechanisms are required to meet the security needs of the GII. Users may select the most effective for their specific purposes.

d)IFIP TC11 recognizes that cryptography at the same time is prone to potential abuse by criminals. In this context law enforcement plays also an important role and we face the situation that different countries exhibit different attitudes.

e)Being aware that responsibilities for crime prevention and detection lies at national governments and that business is less and less related to national boarders IFIP TC11 recognizes that cryptographic services and cryptographic applications cannot be bound to a nation's territory.

f)IFIP TC11 recognizes the technical consensus that forbidding or restricting the use of strong cryptography is from a technical standpoint ultimately unfeasible.

Taking the above said into account IFIP TC11 takes the following position on the use and regulation of cryptography:

(I) Cryptography has equal impact and importance when data are stored or transmitted. A distinction is unrealistic in a world of networked computers.

(II) It is the prime goal that, whoever is involved in the process, cryptographic procedures and keys are handled in a way that full confidence of all partners, including the public at large, is assured.

(III) It is desirable that voluntary and free use be in place for all types of cryptography.

(IV) While a business will generally take precautions to protect itself against lost/forgotten/stolen keys, such considerations should be carefully separated from the law enforcement considerations, even though the mechanisms for each may be the same or overlap.

(V) When establishing key management and cryptography infrastructures this should be primarily driven by the users needs and not by regulatory requirements.

(VI) Law enforcement shall not establish methods in the cryptograhy context that infringe on a citizen's expectations of personal privacy and integrity within a country.

(VII) IFIP TC11 assumes that organised and major crime will successfully avoid or evade any requirement to comply with a key deposit scheme. Law enforcers must therefore not rely primarily on key deposit schemes when addressing the issue of criminal intelligence gathering. Research should be conducted, which results in a set of appropriate, acceptable, and well focused alternative methods.

(VIII) In cases where keys are deposited at third parties it is necessary that commercial and privacy interest as well as commercial liabilities must be guaranteed in all phases. This is particularly necessary if such systems allow law enforcement to access data in clear or keys, under proper legal constraint.

(IX) There is a great need that cryptographic methods and especially digital signatures be recognized by national and international law. Such recognition carries with it responsibilities for assuring availability of relevant keys throughout any legally specified retention period and liabilities for improper disclosure of or change to keys whilst they are being kept.

(X) Any legal or regulatory arrangement between two nations, in respect to cryptography and access to relevant materials, must be symmetric.