# Chapter - 3

# STANDARDISATION AND SECURITY

## 3.1 Introduction :

3.1.1 For efficient and effective communication over any network, standards play a crucial role. It is more so when the network is electronic-based. Along with the various standards for message, operating system and system software, to name a few, a very high level of security at various levels has to be secured while designing and developing of any networking application. The Committee discussed this issue with emphasis on the financial transactions that would be transmitted through the network.

3.1.2 The INFINET is essentially an Internet Protocol (IP) network and hence all the applications should be built around TCP/IP. In order to make optimum use of the communication resources and to facilitate smooth implementation of the applications on the network, the RBI had constituted a few sub-groups for standardisation of different information technology components like networking products, system software, and messaging standard.

3.1.3 Standards will have to be adhered to while dealing with

- Intranet standards that need to be adhered to by the banks.
- Design issues for a Global Web Server for the bank.
- Networking Equipments
- Security and Key management related issues.
- DNS and IP Addressing.
- WAN internetworking options

The details relating to Intranet Standards, Global Web Server for bank and networking equipment are given in **Annexure 8.**

## 3.2 Security Standards

3.2.1 It would be advisable to build security features at the application level, because of the critical nature of financial data transfer. The financial messages should have the under noted features :

- The receipt of the message at the intended destination
- The content of the message should be the same as the transmitted one
- Sender of information should be able to verify its receipt by the recipient
- Recipient of the message could verify that the sender is indeed the person
- Information in transit should not be observed, altered or extracted
- Any attempt to tamper with the data in transit will need to be revealed
- Non-repudiation

These features boil down essentially to **authentication** (to verify the identity of the sender of the message to the intended recipient to prevent spoofing or impersonation),

**authorisation** (to control the access to specific resources for unauthorised persons), **confidentiality** (to maintain the secrecy of the content of transmission between the authorised parties), **integrity** (to ensure that no changes/errors are introduced in the messages during transmission) and **non-repudiation** (to ensure that an entity cannot later deny the origin and receipt and contents of the communication).

3.2.2 At present, there are a number of security standards available for different financial applications. Details of these standards are given in **Annexure 9**. These international standards should be examined and adopted keeping in view the requirements of the Indian banking industry. For this purpose, concerted efforts and co-ordination among the Reserve Bank of India, Indian Banks Association and Bureau of Indian Standards would require to be set in place.

3.2.3 There should be an appropriate institutional arrangement for key management and authentication. This is normally done through Certification Agencies. For the banking and financial sector, the RBI may consider appointing IDRBT as the Certification Agency. There should also be an institutional arrangement for appropriate assessment of participants of the financial network in terms of their credit-worthiness, financial soundness, etc. These assessments will provide valuable input to the banking and financial sector.

3.2.4 The INFINET is a CUG network for the exclusive use of the Banking and Financial Sector. The VSAT network is a TCP/IP network. The applications that are currently built and the ones being planned will assume that they have a secure and robust TCP/IP backbone network. There are several limitations in the TCP/IP networks and the banks need to have a suitable strategy to ensure their corporate network is reliable, secure, robust and fault tolerant.

3.2.5 The TCP/IP protocol has been built in the Unix environment initially for connectivity of multi-vendor, distributed and heterogeneous systems. This protocol is a common framework for communication. The need to secure this environment is realised subsequently and today the limitations are identified and plugged by appropriate solutions. Some of the limitations in the TCP/IP environment are sequence number attacks, spoofing, ICMP redirects, bogus RIP routes, inverse DNS lookup etc.

3.2.6 Many of the users will use the Telnet and FTP. In native TCP/IP, passwords and session are sent in the clear. TFTP configuration files often contain passwords. It is absolutely essential to protect the bank's corporate network by designing and implementing access control security.

3.2.7 Initially the INFINET will be a CUG network, but in due course this network will have to be connected to public networks, SWIFT etc. It is essential to look at the possibility of having firewall implementations and they need to meet the following criteria:

- All in and out traffic must pass through the firewall. The firewall should check and authorise the traffic. The firewall in itself should be immune to penetration.
- Implementation of firewalls can be done using packet filtering routers, application and circuit level gateways and also network translation devices.
- Statefull multilayer inspection gateways combine the advantages of the above and also gives a better performance, flexibility and security. This environment can handle all kinds of applications, namely, Transmission Control Protocol (TCP), User Datagram Protocol (UDP), Remote Procedure Call (RPC), Internet Control Message Protocol (ICMP) etc. New applications can be added easily and this environment is totally transparent to end-users.
- Firewalls are used to implement access control security as well as to provide for user authentication and to ensure data integrity by using encryption. It is important that the banks have their own security policy and then design security solutions accordingly. Regular reviews of Security Policies and their implementation are also important. Highly secured (e.g., funds related), secured, non-secured messages should be clearly demarcated in the security policy. Banks are, therefore, advised to have dedicated groups with enough competence and capability.

3.2.8 Since security is the prime concern for the banking and financial sector, continuous research should be carried out as is done in the Internet community. Institutions like IDRBT should have collaborative arrangements with national and international agencies for carrying out research in this field. Such Institutions could develop Tiger teams (hackers) and the banks can engage the team to test and determine the strength of the firewall implementation.

**Annexures 10 and 11** depict locating firewalls and a typical configuration of a firewall implementation respectively.

### 3.3 Message Standards

3.3.1 The robust communication network would provide the channel for instant / intact transmission of the message. The message transmitted over the network should make sense to the receiver of the message and this is possible only if the transmitter as well as the receiver is adopting the same message formats. For achieving / ensuring this standardisation of message formats is required. With this in view, the INFINET User Group constituted a Sub-Group on standardisation of Message Formats for the banking sector. The Sub-Group had studied the message formats available in SWIFT, UN/EDIFACT and COMET and observed that most of the banking industry message requirements are included in the SWIFT message standards. Detailed analysis on the methodology for adoption of SWIFT format as given by the Sub-Group is given in **Annexure 12**. This Committee recommends the adoption of the recommendations of the Sub-Group.

### 3.4 Standards for System Software

3.4.1 The Reserve Bank of India constituted a Sub-Group under the Chairmanship of Prof.N.L.Sarda of the Indian Institute of Technology, Powai, Mumbai to study and recommend standards for System Software keeping in view the proposed RTGS for large value funds transfer which will have integration with the securities settlement system for DvP transactions as also with the existing Deposit Accounts Departments (DADs) of the Reserve Bank of India for remittance of funds across the country for Banks' local requirements. The system could have a link with other netting systems like Clearing, Electronic Clearing Services (ECS), Electronic Funds Transfer (EFT), EFTPOS (EFT at Point of Sale) etc. These systems will have links with the banks through the 'gateways' of INFINET through the software for sending and receiving messages regarding funds transfer. Other banks' internal systems will not have direct linkages with the systems running at the RBI.

3.4.2 The securities settlement system is required to be directly linked to the RTGS system for settlement of transactions on a DvP basis. The transfer of funds between the various accounts of a bank maintained at DADs or between a DAD and the RTGS system, requires linkages between the DADs and the RTGS system. Thus, it is appropriate to have a synchronous relationship between these systems. The communication between the gateways and the servers at the RBI (RTGS or Securities Services), could as well be message based to obviate the need for synchronisation. In such an event, it is important to ensure that there is a guaranteed and in-order delivery and there is no duplication of messages.

3.4.3 A transaction messaging approach will suffice for any distributed application whose requirements are characterised by one or more of the following :

- the need to have various applications or application components communicate with each other
- the communications need for assured delivery - but not real time or instantaneous delivery; if one component is not available, it is acceptable for a message to be delivered once the component becomes available at a later stage
- the interoperation need to encompass diverse operating systems and hardware platforms

3.4.4 On the other hand, if an application needs one of the following :

- access to multiple resource types
- recovery coordinated across different resources
- an environment where application security, scheduling, load balancing and general resource optimisation are available
- real-time, or interactive, on-line communications
- a common application development and / or execution environment

then an On-line Transaction Processing (OLTP) approach is probably required. In effect, the OLTP approach offers more - and demands more - of its adherents.

3.4.5 The Sub-Group on Systems Software recommended that a common TP Monitor may be used for all application systems running at the RBI which require direct interfaces. Thus, in particular, the RTGS system, the accounting systems at all DADs and the securities settlement system, should use a common TP Monitor. This will help in maintaining a synchronous relationship between the systems. The communication requirements between the banks' gateways and the RBI should be managed by the use of a standard Messaging and Queuing middleware. However, if a bank desires to use a TP Monitor instead of the Messaging system, the same should be compatible with the one being used by the RBI.

3.4.6 The requirements as recommended by the Sub-Group on Systems Software on the essential and desired functionalities for the TP Monitor and Messaging products are given in **Annexure 13**. The choice of product would depend on the support for these functions as well as the price / performance ratio of the product with respect to the existing / proposed infrastructure.

### 3.5 Recommendations

3.5.1 The participating banks will set up their corporate network with INFINET as the backbone. While doing so, they may ensure that their corporate network is a TCP/IP network. In view of this, some suggestions and recommendations are given for appropriately configuring Wide Area Network (WAN) inter- networking devices.

3.5.2 One of the important aspects of this exercise is to look at security management. It would be appropriate to have a single agency, say, IDRBT as the certification agency entrusted with the task of ESCROW services for software and for key certification.

3.5.3 Banks should adopt a widely used standard of cryptography procedures to prevent data tamper during transmission. This should be implemented at the application level supplementing the security already provided at the network level. A combination of DES and RSA cryptographic algorithm may be used for the purpose.

3.5.4 As regards EFTPOS,, the technology should be allowed to evolve into standard - based solutions for multi-vendor heterogeneous environment working cooperatively and collectively. Card layout with Europay, Master card VISA (EMV) specifications appears most suitable.

3.5.5 The INFINET will be operational by the end of June 1999 and the user community should think in terms of quickly having mechanisms to utilise the same for end to end data transfer. This will require robust, secure and standards compliant messaging infrastructure to provide corporate e-mail solution with value added services as needed. The Committee recommends that banks may initiate the process of identifying a suitable e-mail / groupware solution, which can run on the INFINET.

3.5.6 The Committee recommends that for both inter-bank and intra-bank applications, it is necessary to have an application architecture keeping in mind the INFINET as the backbone. The requirements document and the specifications for each of the applications will have to be prepared considering the VSAT backbone and its characteristics and limitations while casting the applications.

3.5.7 The Committee recommends that the RBI and banks should have a Standing Committee with members having enough competence and capability to attend to regular reviews of security policies / message formats / system software and their implementations. In addition, this Standing Committee may study security issues in the banking and financial sector world wide and bring out research reports for the benefit of the INFINET user group members. The IDRBT may provide secretariat and logistics support for the proposed Standing Committee.