ANNEXURES

Annexure

Annexure 1
(Para 2.1.2)

Architecture of the INFINET

In order to upgrade the country's payment and settlement systems, the Reserve Bank of India took the initiative of providing a communication backbone in the form of the satellite based INFINET using VSAT technology to the Banking and Financial Sector. The task of designing and developing the communication network (INFINET) was entrusted to the Institute for Development and Research in Banking Technology (IDRBT). The details of the INFINET are as follows:

2. The Closed User Group (CUG) Network for the banking and financial sector is called INFINET (Indian Financial Network). The INFINET using VSAT technology is a TDM/TDMA network with STAR topology for Data and with DAMA-SCPC overlay with mesh topology for voice and video traffic. This network will have about 500 VSATs to start with and will grow to support large number of VSATs in course of time. The Reserve Bank of India, commercial banks, cooperative banks and Financial Institutions will be the members of this CUG network. While IDRBT will be owning the HUB and the Network Management System (NMS) at Hyderabad, the VSATs will be owned by the user institutions of the network. The initial indent is for one half transponder with provision for one full transponder as the traffic and the number of users grow. The network will be operating in the Extended C-band frequency.

3. Protocols supported: ETHERNET, TCP/IP, X.25 SDLC, Token Ring, Sync bit transparent, Async byte transparent.

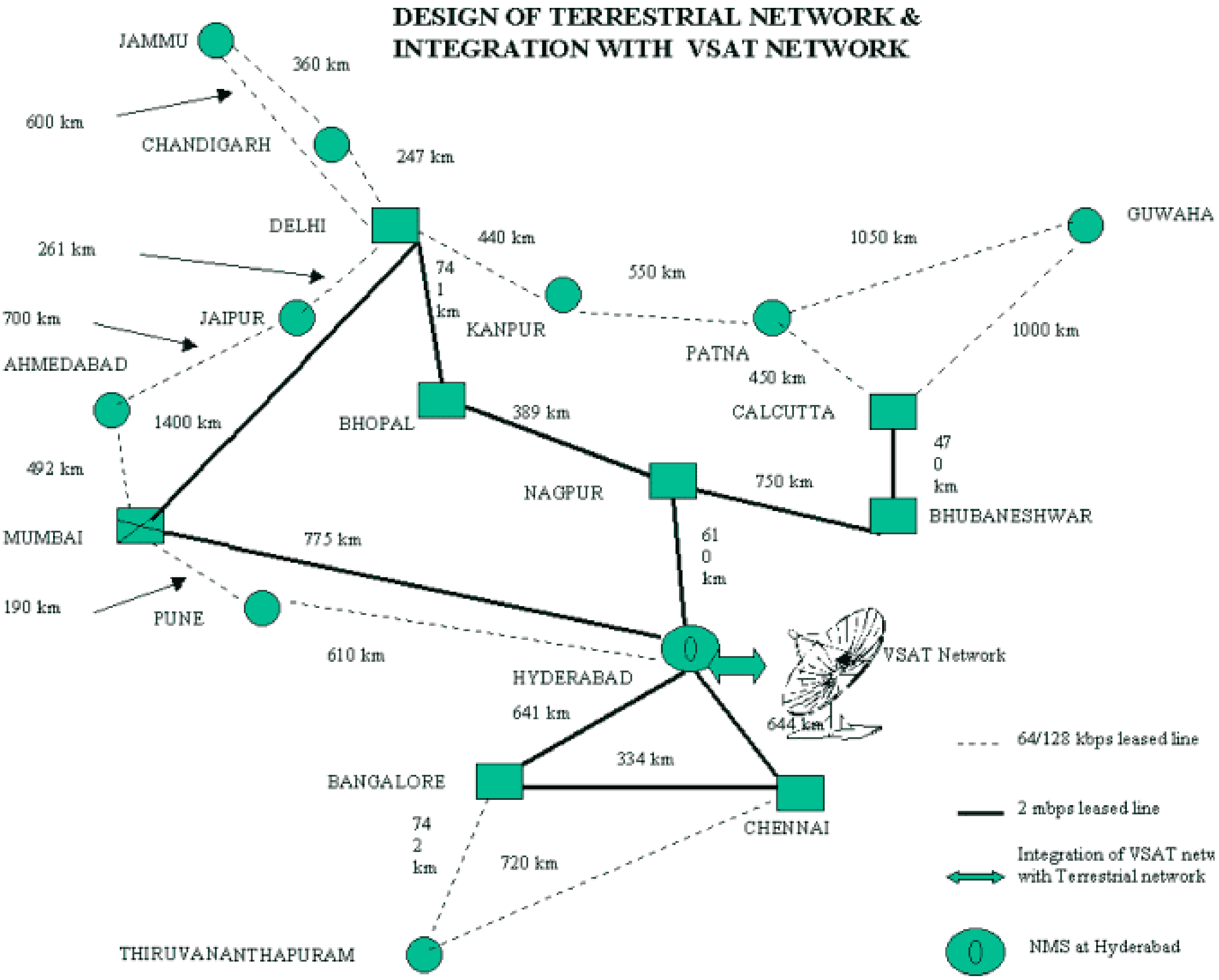
4. A satellite based Network using VSAT technology has several advantages some of which are worth noting

- VSATs provide an enabling technology in rapidly building a reliable communication backbone
- Consistent network response/performance
- Besides providing communication channels of high quality and availability, VSATs can be installed and operated in widely dispersed locations irrespective of the distance and terrain
- Low cost of maintenance - There are three points of failure viz., satellite, Hub and VSATs. Location of problem is comparatively easy from Network Management System (NMS). In terrestrial lines, the problem can be anywhere along the transmission path and hence is difficult to locate and repair.
- The INFINET network based on VSAT is configured and monitored through NMS providing easy centralised control and monitoring of every single site.
- Uptime is very high
- Distance insensitivity - Cost of a link in a VSAT based Network is not sensitive to distance
- Better price performance. If the number of sites to be covered in the network is large and highly dispersed geographically, significant cost savings over terrestrial alternatives can be expected
- The Network is entirely under the control of owner organisation and is independent of intermediary agencies (e.g., DoT) once the necessary approvals and satellite resources are obtained
- Broadcast transmission capacity of satellites enables signals to be sent to a wide geographic area. In countries with hostile terrain and little existing infrastructure, satellites are an attractive idea.

As in the case of any media, there are some aspects of concern relating to a satellite based VSAT network. These are:

- Broadcast aspect of satellite communications may present security problems, since all stations under the satellite antenna can receive the broadcasts. Consequently transmissions are encrypted for satellite channels.
- Propagation delay - affects commercial standard voice communication
- Interference sensitive - Radio frequency link in a VSAT based network is subject to interference as a result of small earth station size.

Annexure - 2
(Para 2.1.3)
Figure - 1



DESIGN OF TERRESTRIAL NETWORK & INTEGRATION WITH VSAT NETWORK

Annexure - 2
(Para 2.1.3)
Figure - 2

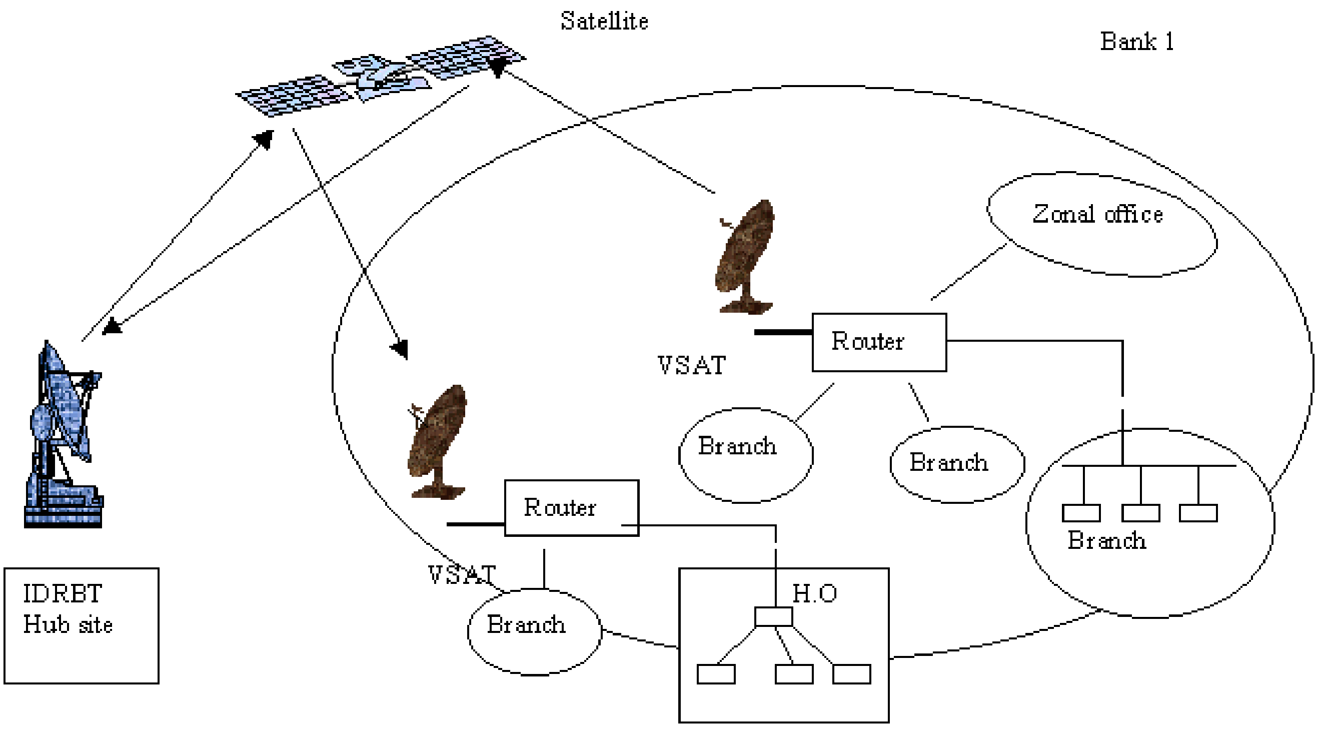
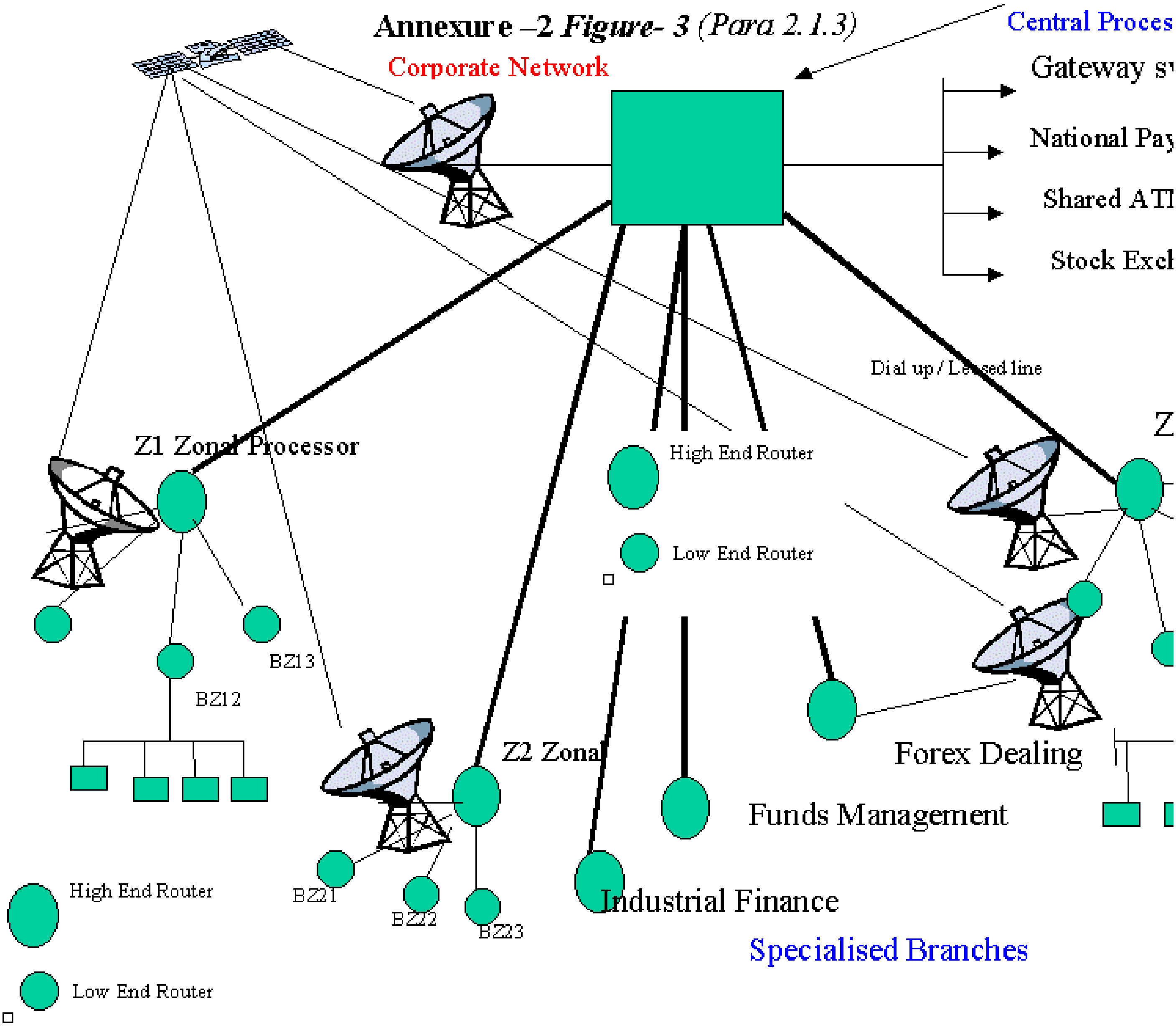
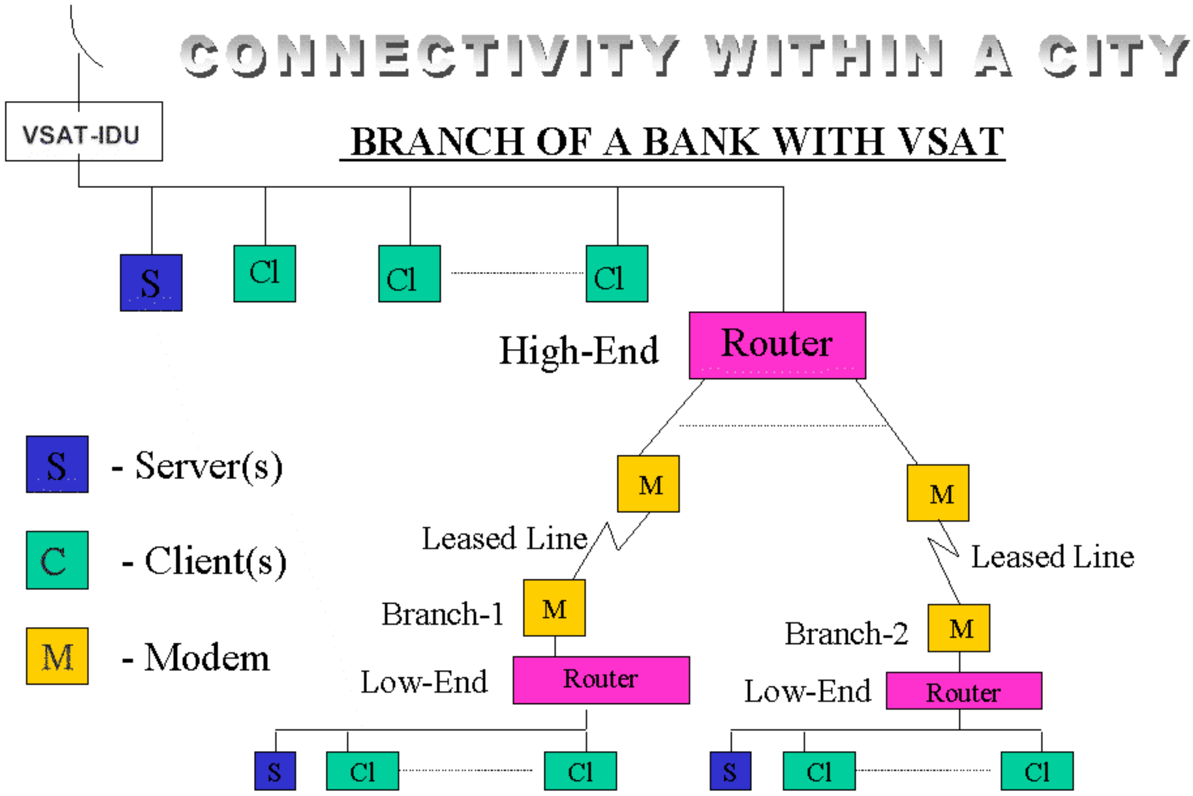


Figure - 3

Annexure –2 ***Figure- 3*** *(Para 2.1.3)*



Annexure - 2
(Para 2.1.3
Figure - 4



Annexure 3
(Para 2.2.1)

Access modes in the VSAT based INFINET

Aloha Mode - In contention mode. It is good for data transactions involving small messages occurring at random, and often long intervals (bursty type of traffic). This mode gives the fastest overall response time, but the finite probability of collision means that there will be occasional instances of increased delay e.g., ATM type of applications, short queries (like balance enquiry).
Transaction Reservation – Non-contention mode. It is most suitable for messages which are large but of a limited duration (a few seconds). Remote VSATs request the hub for capacity to transfer a specific volume of data, typically some thousands of bytes, at a predefined data rate. The hub identifies a sequence of frames with available capacity and responds with a command to generate bursts in those frames. The last burst of the sequence includes a piggyback request for further capacity if required. Of the three access methods, the transaction reservation carries the highest volume of traffic. E.g., small file transfer

Stream Mode – Non-contention mode. It is most suitable for transactions comprising messages that are long and of long duration. The set-up time for the mode is 1 – 2 seconds, but once established there is no further set-up delay. E.g., Voice and large file transfer

There is also a hybrid access method called Flexi-route. In this case, a particular port is configured with a threshold limit (so many Kilo bytes). If the threshold limit is reached for a transaction, then there is automatic switching to stream mode.

Annexure - 4
(Para 2.5.1)

Applications Architecture

Part I - Intra-bank Application

(a) Funds transfer and payment messages (Intra-bank)
(b) Banks owned ATM/credit card, debit card and other applications on the Corporate network
(c) Inter Branch Reconciliation (IBR)
(d) Quick disposal of loan / investment proposal
(e) Forex information from branches to the office dealing in Forex
(f) Fund information from clearing centers to the fund management office for optimal allocation of funds
(g) Cash Management Product
(h) Treasury Management (TM)
(i) Any Branch Banking
(j) Asset Liability Management (ALM)
(k) E-mail (e-mail can replace the telephone / telex / facsimile, etc.), and Collaborative Environment Applications
(l) Software distribution in the bank
(m) Organizational bulletin boards may contain the following
- Circulars
- News letters, Phone and address directories
- Undesirable parties
- hot list / warning bulletins
- missing security items
- confidential circular on attempted frauds

(n) Human Resources Development and Personnel Administration
(o) Auditing and Inspecting computerised branches using the network
(p) Organizational / Customers data base may include
- Statutory returns
- Control returns
- Standardized returns
- Adhoc reports

(q) Banks : corporate customers connectivity

(r) Management Information Systems

- Borrower's profile
- Branch profile
- Employees analysis
- Products / services profile
- Business profile of branches

(s) Apart from providing efficient service to customers the financial network will also fulfill the following objectives:

- timely information to top management
- helping in development of new products
- speedy communication among branches and to the controlling offices

Many of the above applications could be implemented as part of a bank's Intranet.

Part II - **Inter-bank Applications**

(a) Electronic Funds Transfer (EFT)

- Retail EFT (Small value credit transfer) on net settlement basis
- Wholesale EFT (Large value credit transfers) on Real Time Gross Settlement (RTGS) basis for time critical payments.

(b) Clearing and settlement systems for securities – Delivery vs. Payment (DVP): The final delivery of securities will occur if and only if final payment occurs.

(c) Transferring balances from net settlement systems to RTGS Server at periodic intervals. The net obligations   could be from:

- Local paper-based clearing
- Inter-city paper-based clearing (including TT discounting facilities)
- Bulk payments - ECS(Debit, Credit, RAPID) including inter-city
- Shared ATM networks
- Smart cards and other pre-paid/pre-authorised debit cards
- Debt Market clearing including derivatives

(d) Exchange of Defaulting Borrowers' list among RBI and banks

(e) EDI services to the extent they pertain to payment cycle of EDI

(f) Consolidation of current account balances from the existing DAD applications synchronously / asynchronously to facilitate balance enquiry by banks on all India/centre-wise basis and if necessary to activate transfer of funds among DADs at different centres.

(g) Currency chest accounting

(h) Reporting of Government account transactions (Central and State Governments)

(i) Reporting of BSR, R-Returns etc. to RBI

(j) Asset Liability Management (for reporting to RBI)

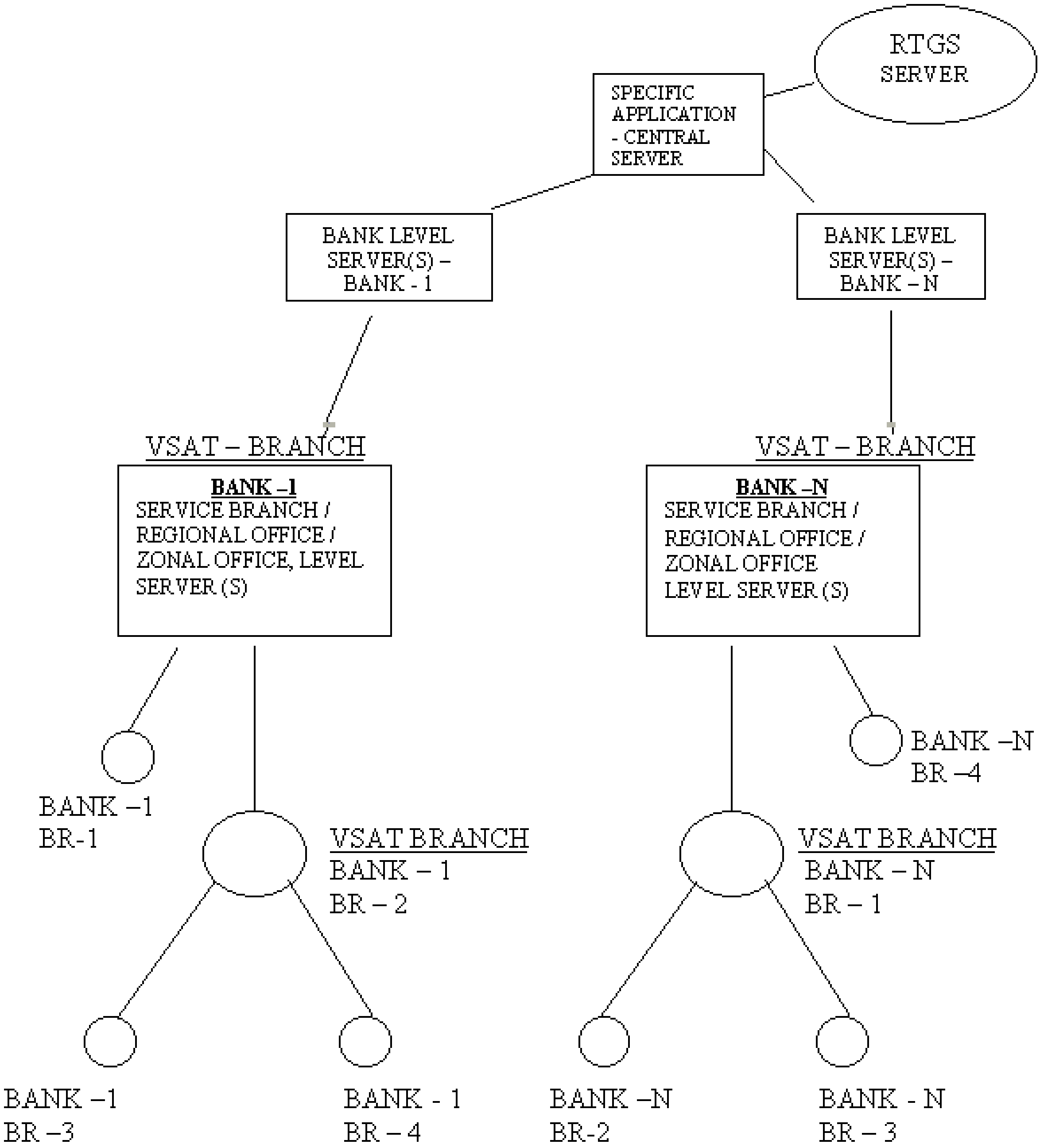
(k) Intranet in RBI to enable banks to get circulars, press releases etc.

(l) Reporting of Section 42 Data as per the RBI Act, 1934 to the RBI

(m) Returns to be submitted by the banks to Department of Banking Supervision (DBS) for off-site supervision and monitoring.

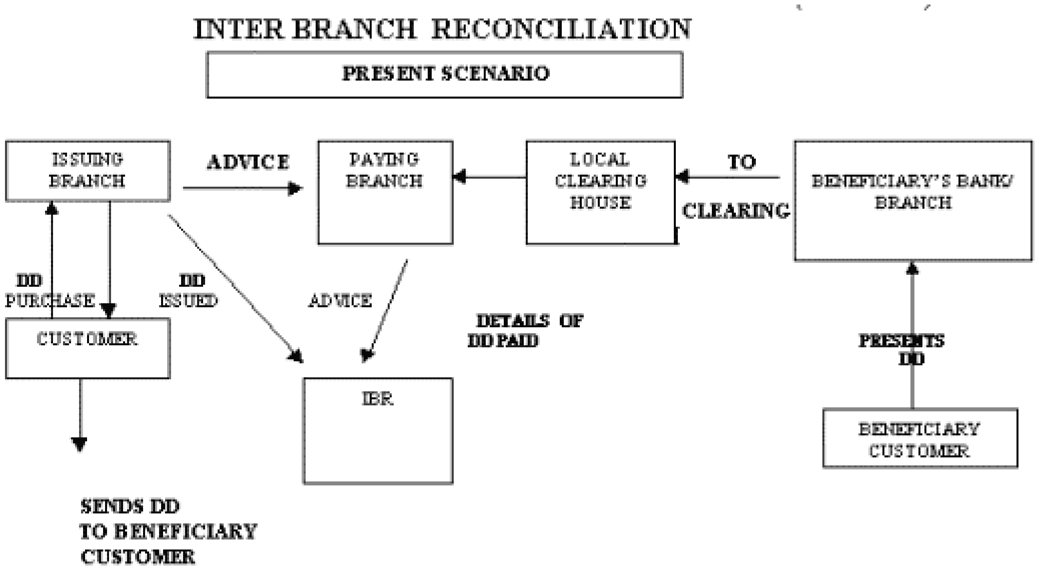
Annexure - 5
(Para 2.5.4)

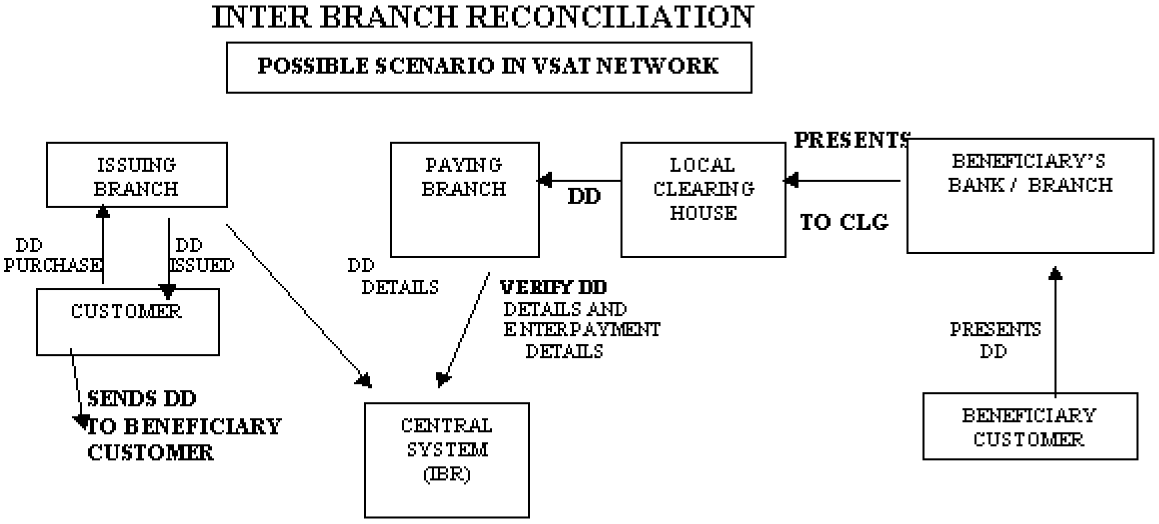
SCHEMATIC APPLICATION ARCHITECHTURE



- Communication link can be through satellite using VSATs or leased line link to a VSAT Branch within a city.
  Central Servers of various application systems, RTGS server and Bank Level Servers should ideally be linked to Hub Site via backhaul links.

Annexure - 6
(Para 2.5.5

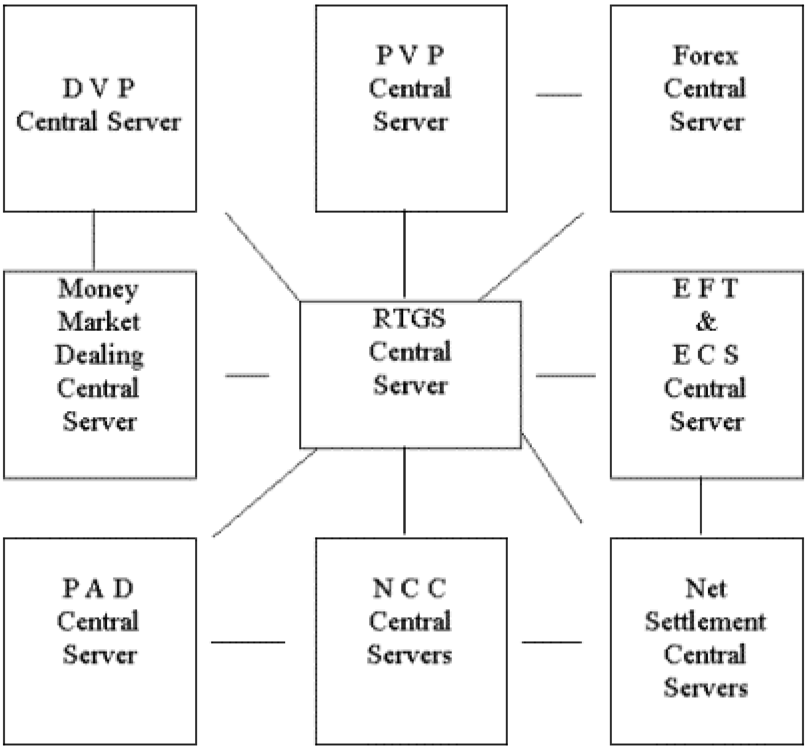




Note: Though the schematic is for a centralised set up, the same can be extended to a decentralised set up.

Annexure - 7
(Para 2.5.7)

SETTLEMENT SERVER ARCHITECTURE



Annexure 8
(Para 3.1.3)

Standards for Security

The Intranet will initially have database services and as time progresses will have to support voice and video based applications. Eventually, this corporate network will be a true multi-media application network with TCP/IP as the communication protocol. The three choices for the Intranet design are:

- **fully open**: public domain, formal and consensus standards
- **semi-open** : published API with significant industry usage
- **closed** : proprietary or little used API

The Committee recommends fully open systems because of the following reasons:

- Guaranteed Interoperability between products
- Wide vendor choice.

In this project it is important to implement initially a prototype to test performance and inter-operability before deploying on the corporate network.

Most of the banks would like to implement a Web Server which can be accessed from their locations. Designing and implementing a Web Server is a complex task and some of the aspects to be considered are given below:

* Performance

- Consistent throughputs for multiple connections

  - ➡ Maximum number of connections
  - ➡ Admission Control
  - ➡ Good backplane throughputs
  - ➡ multithreading

* Security

- Good data security to host and transfer sensitive data

  - ➡ Access Control
  - ➡ Proxy Servers
  - ➡ Transaction Security

* Service Integration

- Integrating various services into a common frontend - the Web client

  - ➡ SQL Databases
  - ➡ Other custom applications
  - ➡ inbuilt indexing and search engines

* Administration & Management

  - ➡ Remote Administration
  - ➡ Configuration Control Delegation
  - ➡ Automated site map generation and link (URL) verification

The corporate network of the banks will have different types of connectivity mechanisms viz., dial-up and leased line modems, analog and digital modems, voice / data multiplexers and TCP/IP routers. These inter-networking equipment will have to meet the current and future needs. Some of the important specifications that need to be considered are given below:

- Concurrent bridging and Routing
- IP/IPX support
- Bandwidth on demand
- and Frame relay support
- SLIP and PPP support
- RIP v2 and OSPF

- NAT VLSM and CIDR support
- Call back security
- Policy based routing
- Access control list
- Authentication service for remote dial in
- Traffic shaping

Annexure 9
(Para 3.2.2)

Security Standards for Financial Applications

A. Bureau of Indian Standards

Sr. No.	BIS Standard No.	Title
1.	IS 14356:1996	Guide for Protection of Information Resources
2.	IS 14357:1996	Code of Practice for Information Security Management

B. International Standardization Organization

1. Banking and Financial Services

Sr. No.	ISO Standard No.	Title
1.	ISO 8730 : 1990	Banking – Requirement for Message Authentication (Wholesale)
2.	ISO 8731 (Part 1) : 1987	Banking – Approved Algorithms for Message Authentication – Part 1 : DEA
3.	ISO 8731 (Part 2) : 1987	Banking – Approved Algorithms for Message Authentication – Part 2 : Message Authentication Algorithm
4.	ISO 8732 : 1988	Banking – Key Management (Wholesale)
5.	ISO 9564 (Part 1) : 1991	Banking Personal Identification Number Management and Security – Part 1 : PIN Protection Principles and Techniques
6.	ISO 9564 (Part 2) : 1991	Banking Personal Identification Number Management and Security – Part 2 : Approved Algorithm(s) for PIN Encipherment
7.	ISO 9807 : 1991	Banking and Related Financial Services – Requirements for Message Authentication (Retail)
8.	ISO 9992 (Part 1) : 1990	Financial Transaction Cards – Messages between the Integrated Circuit Card and the Card Accepting Device, Part – 1: Concept and Structures
9.	ISO 9992 (Part 2) : 1990	Financial Transaction Cards – Messages between the Integrated Circuit Card and the Card Accepting Device, Part – 2: Functions, Messages (Commands and Responses), Data Elements and Structures
10.	ISO 9992 (Part 4) : 1990	Financial Transaction Cards – Messages between the Integrated Circuit Card and the Card Accepting Device, Part – 4: Common

Sr. No.	ISO Standard No.	Title
		Data for Interchange
11.	ISO 10126 (Part 1) : 1991	Banking – Procedure for Message Encipherment (Wholesale) - Part 1: General Principles
12.	ISO 10126 (Part 2) : 1991	Banking – Procedure for Message Encipherment (Wholesale) - Part 2: DEA Algorithm
13.	ISO 10202 (Part 1) : 1991	Financial Transaction Cards – Security Architecture of Financial Transaction Systems using Integrated Circuit Cards – Part 1 : Card Life Cycle
14.	ISO 10202 (Part 2) : 1996	Financial Transaction Cards – Security Architecture of Financial Transaction Systems using Integrated Circuit Cards – Part 2 : Transaction Process
15.	ISO DIS 10202 (Part 3) : 1996	Financial Transaction Cards – Security Architecture of Financial Transaction Systems using Integrated Circuit Cards – Part 3 : Cryptographic Key Relationships
16.	ISO 10202 (Part 4) : 1996	Financial Transaction Cards – Security Architecture of Financial Transaction Systems using Integrated Circuit Cards – Part 4 : Secure Application Module
17.	ISO DIS 10202 (Part 5) : 1996	Financial Transaction Cards – Security Architecture of Financial Transaction Systems using Integrated Circuit Cards – Part 5 : Use of Algorithms
18.	ISO 10202 (Part 6) : 1994	Financial Transaction Cards – Security Architecture of Financial Transaction Systems using Integrated Circuit Cards – Part 6 : Card Holder Verification
19.	ISO DIS 10202 (Part 7) : 1994	Financial Transaction Cards – Security Architecture of Financial Transaction Systems using Integrated Circuit Cards – Part 7 : Key Management
20.	ISO 10202 (Part 8) : 1994	Financial Transaction Cards – Security Architecture of Financial Transaction Systems using Integrated Circuit Cards – Part 8 : General Principles and Overview
21.	ISO 11131 : 1992	Banking and Related Financial Services – Sign-on Authentication
22.	ISO 11166 (Part 1) : 1994	Banking – Key Management by Means of Asymmetric Algorithms – Part 1 : Principles, Procedures, and Formats
23.	ISO 11166 (Part 2) : 1994	Banking – Key Management by Means of Asymmetric Algorithms – Part 2 : Approved Algorithms using the RSA Cryptosystem
24.	ISO 11568 (Part 1) : 1994	Banking Key Management (Retail) – Part 1 : Introduction to Key Management
25.	ISO 11568 (Part 2) : 1994	Banking Key Management (Retail) – Part 2 : Key Management Techniques Symmetric Ciphers
26.	ISO 11568 (Part 3) : 1994	Banking Key Management (Retail) – Part 3 : Key Life Cycle for Symmetric Ciphers
27.	ISO DIS 11568 (Part 4) :	Banking Key Management (Retail) – Part 4 : Key Management Techniques using Public Key Cryptography

Sr. No.	ISO Standard No.	Title
28.	ISO DIS 11568 (Part 5) :	Banking Key Management (Retail) – Part 5 : Key Life Cycle for Public Key Cryptosystems
29.	ISO DIS 11568 (Part 6) :	Banking Key Management (Retail) – Part 6 : Key Management Schemes
30.	ISO DIS 13491 – 1 :	Banking – Secure Cryptographic Devices (Retail) Part 1 : Concepts, Characteristics, Management & Compliance
31.	ISO DIS 13492	Banking – Key Management Related Data Elements (Retail)
32.	ISO/TR 13569 : 1997	Banking and Related Services – Information Security Guidelines

2. Information Technology

Sr. No.	ISO Standard No.	Title
1.	ISO 7498 – 2	Information System Processing – Open Systems Interconnection – Basic Reference Model
2.	ISO 8372:1987	Information Processing -- Modes of operation for a 64-bit Block Cipher Algorithm
3.	ISO 9160:1988	Information Processing -- Data Encipherment -- Physical Layer Interoperability Requirements
4.	ISO 9735	UN/EDIFACT
5.	ISO/IEC 9796:1991	Information Technology -- Security Techniques -- Digital Signature Scheme giving Message Recovery
6.	ISO/IEC 9796-2:1997	Information Technology -- Security Techniques -- Digital Signature Schemes giving Message Recovery -- Part 2: Mechanisms using a Hash-function
7.	ISO/IEC WD 9796-3:1997	Information Technology -- Security Techniques -- Digital Signature Schemes giving Message Recovery -- Part 3: Mechanisms using a Check Function
8.	ISO/IEC WD 9796-4:1997	Information Technology -- Security Techniques -- Digital Signature Schemes giving Message Recovery -- Part 4: Discrete Logarithm based Mechanisms
9.	ISO/IEC 9797:1994	Information Technology -- Security Techniques -- Data Integrity Mechanism using a Cryptographic Check Function employing a Block Cipher Algorithm
10.	ISO/IEC 9798-1:1997	Information Technology -- Security Techniques -- Entity Authentication -- Part 1: General
11.	ISO/IEC 9798-2:1994	Information Technology -- Security Techniques -- Entity Authentication -- Part 2: Mechanisms using Symmetric Encipherment Algorithms
12.	ISO/IEC 9798-3:1993	Information Technology -- Security Techniques -- Entity Authentication Mechanisms - - Part 3: Entity Authentication using a Public Key Algorithm
13.	ISO/IEC 9798-	Information Technology -- Security Techniques -- Entity

Sr. No.	ISO Standard No.	Title
	4:1995	Authentication -- Part 4: Mechanisms using a Cryptographic Check Function
14.	ISO/IEC DIS 9798-5	Information Technology -- Security Techniques -- Entity Authentication -- Part 5: Mechanisms using Zero Knowledge Techniques
15.	ISO/IEC 9979:1991	Data Cryptographic Techniques -- Procedures for the Registration of Cryptographic Algorithms
16.	ISO/IEC DIS 9979	Information Technology -- Security Techniques -- Procedures for the Registration of Cryptographic Algorithms (Revision of ISO/IEC 9979:1991)
17.	ISO/IEC 10116:1997	Information Technology -- Security Techniques -- Modes of Operation for an n-bit Block Cipher
18.	ISO/IEC 10118-1:1994	Information Technology -- Security Techniques -- Hash-functions -- Part 1: General
19.	ISO/IEC 10118-2:1994	Information Technology -- Security Techniques -- Hash-functions -- Part 2: Hash-functions using an n-bit Block Cipher Algorithm
20.	ISO/IEC DIS 10118-3	Information Technology -- Security Techniques -- Hash-functions -- Part 3: Dedicated Hash-functions
21.	ISO/IEC DIS 10118-4	Information Technology -- Security Techniques -- Hash-functions -- Part 4: Hash-functions using Modular Arithmetic
22.	ISO/IEC 11770-1:1996	Information Technology -- Security Techniques -- Key Management -- Part 1: Framework
23.	ISO/IEC 11770-2:1996	Information Technology -- Security Techniques -- Key Management -- Part 2: Mechanisms using Symmetric Techniques
24.	ISO/IEC DIS 11770-3	Information Technology – Security Techniques -- Key Management -- Part 3: Mechanisms using Asymmetric Techniques
25.	ISO/IEC TR 13335-1: 1996	Information Technology – Guidelines for the Management of IT Security (GMITS) -- Part 1: Concepts and Models for IT Security
26.	ISO/IEC TR 13335-2 : 1997	Information Technology (GMITS) -- Guidelines for the Management of IT Security (GMITS) -- Part 2: Managing and Planning IT Security
27.	ISO/IEC DTR 13335-3	Information Technology -- Guidelines for the Management of IT Security -- Part 3: Techniques for the Management of IT Security
28.	ISO/IEC WD 13335-4 : 1996	Information Technology -- Guidelines for the Management of IT Security (GMITS) -- Part 4: Baseline Approach
29.	ISO/IEC WD 13335-5 : 1996	Information Technology -- Guidelines for the Management of IT Security (GMITS) -- Part 5:

Sr. No.	ISO Standard No.	Title
		Application of IT Security Services and Mechanisms
30.	ISO/IEC 13888-1:1997	Information Technology -- Security Techniques -- Non-repudiation -- Part 1: General
31.	ISO/IEC DIS 13888-2	Information Technology -- Security Techniques -- Non-repudiation -- Part 2: Mechanisms using Symmetric Techniques
32.	ISO/IEC 13888 -3: 1997	Information Technology -- Security Techniques -- Non-repudiation -- Part 3: Mechanisms using Asymmetric Techniques
33.	ISO/IEC WD 14516-1 : 1995	Guidelines on use and Management of Trusted Third-Party Services – Part 1 : General Model
34.	ISO/IEC WD 14516-2 : 1996	Guidelines on use and Management of Trusted Third-Party Services – Part 2 : Technical Aspects
35.	ISO/IEC DIS 14888-1	Information Technology -- Security Techniques -- Digital Signatures with Appendix -- Part 1: General
36.	ISO/IEC DIS 14888-2	Information Technology -- Security Techniques -- Digital Signature with Appendix -- Part 2: Identity-based Mechanisms
37.	ISO/IEC DIS 14888-3	Information Technology -- Security Techniques -- Digital Signature with Appendix -- Part 3: Certificate-based Mechanisms
38.	ISO/IEC DIS 14980	Information Technology -- Code of Practice for Information Security Management
39.	ISO/IEC CD 15408-1 : 1996	Evaluation Criteria for IT Security – Part 1 : Introduction and General Model
40.	ISO/IEC CD 15408-2 : 1996	Evaluation Criteria for IT Security – Part 1 : Security Functional Requirements
41.	ISO/IEC CD 15408-3 : 1996	Evaluation Criteria for IT Security – Part 3 : Security Assurance Requirements

C. American National Standards Institute (ANSI)

1. Information Processing Systems

Sr. No.	ANSI Standard No.	Title
1.	ANSI X3.92	Data Encryption Algorithm (DEA)
2.	ANSI X3.105	Information Systems - Data Link Encryption
3.	ANSI X3.106	Data Encryption Algorithm - Modes of Operations

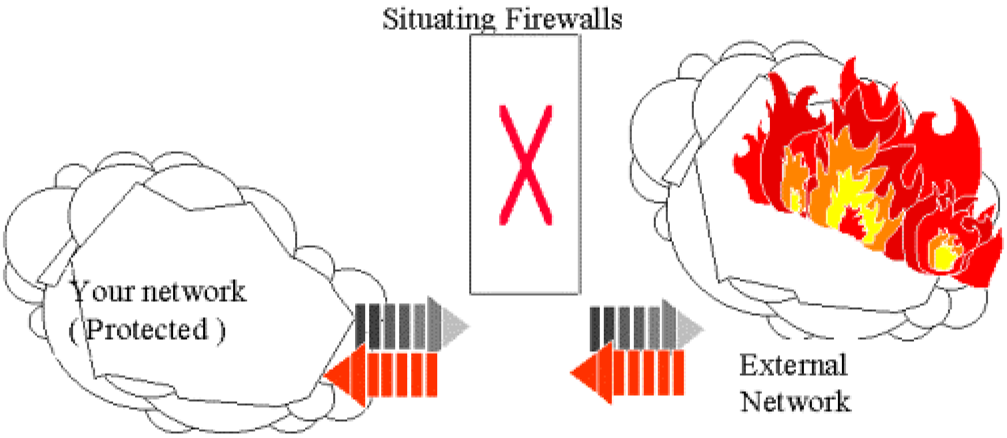
2. Financial Services

Sr. No.	ANSI Standard No.	Title
1.	ANSI X9.8	Personal Information Number (PIN) Management and Security
2.	ANSI X9.9	Financial Institution Message Authentication (Wholesale)
3.	ANSI X9.17	Financial Institution Key Management (Wholesale)
4.	ANSI X9.19	Financial Institution Retail Message Authentication
5.	ANSI X9.23	Financial Institution Message Encryption (Wholesale)
6.	ANSI X9.24	Retail key Management
7.	ANSI X9.26	Financial Institution Sign-on Authentication for Wholesale Financial Transactions
8.	ANSI X9.28	Financial Institution Multiple Center Key Management (Wholesale)
9.	ANSI X9.30:	Public Key Cryptography for Financial Services Industry: Part 1: Digital Signature Algorithm
10.		Public Key Cryptography for Financial Services Industry: Part 2: Secure Hash Algorithm
11.		Part 3: Certificate Management for DSA
12.	ANSI X9.31	Part 1: RSA Signature Standard
13.		Part 2: MD2, MD5, SHA, MDC-2
14.		Part 3: Certificate Management
15.	ANSI X9.41 DRAFT	Security Services Management for Financial Industry
16.	ANSI X9.42	Public Key Cryptography for the Financial Services Industry : Management of Symmetric Algorithm Key using Diffie-Hellman
17.	ANSI X9.44	Public Key Cryptography using Reversible Algorithm for the Financial Services Industry: Transport of Symmetric Algorithm keys using RSA
18.	ANSI X9.52	Triple DES
19.	ANSI X9.55 DRAFT	Public Key Cryptography for the Financial Services Industry, Extensions to Public Key Certificates and Certificate Revocation Lists
20.	ANSI X9.57	Public Key Cryptography for the Financial Services Industry: Certificate Management
21.	ANSI X9.62	The Elliptic Curve Digital Signature Algorithm (ECDSA)
22.	ANSI X9.63	The Elliptic Curve Key Agreement and Transport Protocols

3. Electronic Business Data Interchange

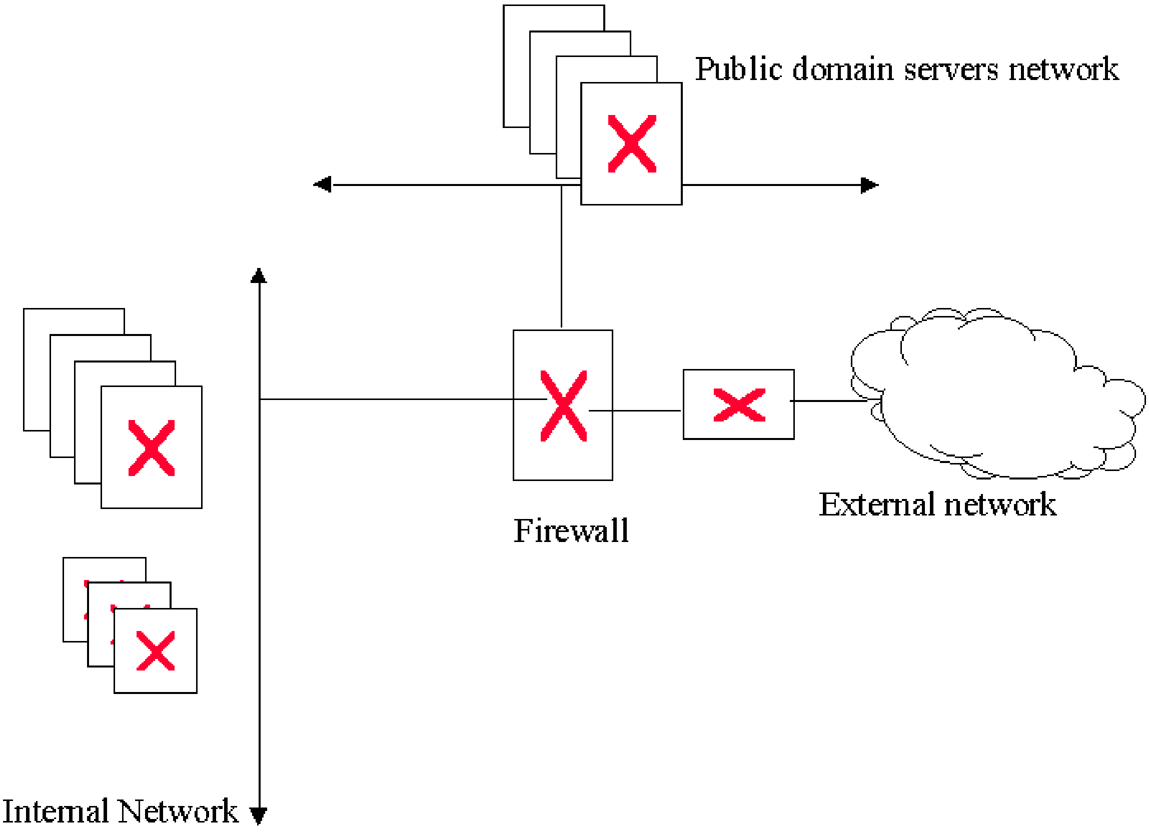
Sr. No.	ANSI Standard No.	Title
1.	ANSI X12.58	X12: Electronic Business Data Interchange : EDI Security Structures

Annexure - 10
(Para 3.2.8)



<u>**Annexure - 11**</u>
(Para 3.2.8)

A Typical Firewall Configuration



<u>**Annexure 12**</u>
<u>*(Para 3.3.1)*</u>

Standards for Message Formats

1. Coding System for banks and financial institutions

For identifying bank branches there are different coding systems in existence viz., individual bank coding system, uniform code for banks for reporting to RBI, MICR code etc. The numbering pattern used by the RBI for MICR cheque processing and uniform code for reporting to RBI would not be adequate to cover all districts / centres and branches when the number of districts / centres and branches exceeds 999 and 9999 respectively.

The Sub-Group had recommended 11 digit coding pattern for Indian Financial Code System (IFSC). The first four characters would be for bank – same code as in SWIFT, fifth character to be zero – reserved for future use, and last six characters for branch code – banks can use the existing codes with no white spaces (zeros prefixed).

Suitable interfaces have to be in place to map the incoming and outgoing SWIFT messages on INFINET. For effectively using the IFSC for national routing of financial transactions which could be included in all SWIFT international messages would necessitate use of a routing symbol, //IN, as suggested by the Sub-Group.

2. Central Body for Directory Maintenance

The Sub-Group recommended a central location for IFSC directory maintenance and necessary information to be broadcasted for individual banks to update their databases.
The Sub-Group had recommended that the secretariat of the VSAT User Group in RBI would be responsible for maintaining the directory of bank branches.

3. Coding System for Country and Currency

For carrying out international transactions, the banks are already using SWIFT. The Indian transactor would also need to maintain accounts in multiple currencies, at some point of time in future.
The Sub-Group recommended that the ISO standard being used by SWIFT for coding country and currency may be adopted by the Indian Banking and Financial system (2 character alphabetic code for country and 3 character alphabetic code for currency).

4. Need for Working Group on an on-going basis

The Sub-Group had suggested forming a Working Group to work on an on-going basis for offering new products and services. The working group would also be responsible for development of message formats, review / modifications of the existing formats and development of message types for new applications / transactions.
The Sub-Group had recommended establishing a working group which would be entrusted with the task of studying and recommending the message types for all applications on an on-going basis.

5. Agency to Act as Depository for Message formats

New bank / branches and financial institutions who join the network need to be given full support to implement applications on the INFINET.

The Sub-Group had recommended that the Secretariat of VSAT Users’ Group may act as a depository for all standard message formats and interface with the banks as regards implementation of the message formats.

5. Interface between the banks’ application and INFINET

The INFINET is an IP network and it is desirable that all applications are implemented over the TCP/IP network.

Annexure 13
(Para 3.4.6)

Standards for System Software

1. Requirements for the TP Monitor

Essential :

- Support for Two-Phase Commit Processing
- Support for XA Compliant and all leading Relational Data Base Management Systems (RDBMSs)
- Support diversity of platforms, both hardware and operating system
- Support for TCP/IP
- Distributed Transaction Management
- Recoverable Transaction Queuing
- Fault tolerant
- Handle System failures and Network outages
- Integrated TP and Messaging System providing APIs
- Messaging Systems : Guaranteed delivery and in-order delivery
- Message Sensitive Routing
- Data Marshalling
- Provide Security and Authentication facilities
- Audit Services
- Interface to third party Messaging Software

Desirable :

- Load balancing capability whereby additional application servers can be fired, Messages can be routed to specific servers, etc.
- Facility for Message priority settings
- Support for GUI-based Monitoring
- Operate in low-bandwidth also
- Compliance with full X/Open, CORBA. OLE/Active-X Standards -
- Support of JAVA, JAVA Beans etc.
- Permit Application specific or RBI recommended Security, Encryption/Decryption, Authentication, Non-repudiation, Certification interfacing
- Support "Thin" Clients to participate in two-phase commit transactions and Messaging Services.
- Time-based Messaging - Message Delivery
- Automatic Software Distribution
- Global Time Service Facility
- Process management - including starting processes, registering processes, balancing workloads among processes, and so on.
- Configuration, installation, and monitoring of transaction processing systems.
- Standard Client/Server Application Development Tools

- World Wide Web Interface

2. Requirements for the Messaging and Queuing Products

Essential :

- Support diversity of platforms, both hardware and Operating Systems.
- Message Sensitive Routing
- Fault tolerant
- Handle System failures and Network outages
- Integrated Messaging System providing APIs
- Support for TCP/IP
- Messaging Systems : Guaranteed delivery and in-order delivery, Non duplication
- Data Marshalling
- Provide Security and Authentication facilities
- Audit Services
- Interface to third party Messaging Software as well as TP Monitors
- Support for Triggers to initiate applications.
- Message prioritisation facility
- Comprehensive Queue Management facility
-

Desirable :

- Load balancing capability whereby additional application servers can be fired, Messages can be routed to specific servers, etc.
- Support for GUI-based Monitoring
- Operate in low-bandwidth also
- Support of JAVA, JAVA Beans etc.
- Permit Application specific or RBI recommended Security, Encryption/Decryption, Authentication, Non-repudiation, Certification interfacing
- Support "Thin" Clients to participate in Messaging Services.
- Time-based Messaging - Message Delivery
- Automatic Software Distribution
- Global Time Service Facility
- Process management - including starting processes, registering processes, balancing workloads among processes, and so on.
- GUI based tools for configuration, installation and monitoring of message processing systems
- Standard Client/Server Application Development Tools
- World Wide Web Interface

Annexure 14

(Para 4.3.9)

Guidelines for a Healthy Outsourcing Strategy

1. Version control of the software offered by the vendor should be ensured by the bank. Bug clearance in a given version should be done first. The end-users' requirement should be specifically spelt out and given. Any enhancement required by the bank should be undertaken only in the subsequent versions. Version control thus can be successfully ensured across different branches for a given vendor within a bank.

2. The terms of keeping the source code of the software in ESCROW arrangement should be spelt out as follows:

- The sources of software (version x, say) will be recompiled in the presence of designated bank official (s) and the representative of the software vendor/firm.

- The compiled programmes should be loaded at the pilot site, tested and certified for being the same version (version x) e.g. Y2K compliant version of software.

- On completion of testing, the source code should be copied into DAT/Optical Disc (any other mutually agreed media), sealed in the presence of the authorised persons.

- The sealed package containing the source should be kept in the joint custody of the bank and the vendor at mutually agreed branch of the bank and this sealed cover containing the source code should be deliverable only against the joint signatures of the authorised signatory of the vendor company and the bank.

- In cases where a vendor company ceases to exist without any assignees or successors, the bank will have the right to open the seal cover and use the source code for its use giving written notice to the vendor company at its last known address.

- Proper safe custody of the packet in safe deposit should be the responsibility of the bank.

- Software vendor should have the right of inspection of the same code in sealed condition at any time.

3. The bank should ensure that the software license and the professional services should include the following details:

- Licence copy of the object code of the software, the customisation and implementation of the software, training to branch staff, operation staff and EDP staff.

- If the vendor company brings out a higher version / releases , newer operating systems or database management systems than the present one, the same should be available at no extra cost to the bank, if similar arrangement is enjoyed by the vendor with the parent partner of the Operating Systems (OS) / RDBMS.

- The Vendor should study the functioning of branch / office where software is being provided and suggest hardware sizing, various peripherals, other interfaces such as signature verification facility, MICR, Tele banking or any other Hi-Tech facility to enhance customer satisfaction. The Vendor company should undertake project management and have joint responsibility with the bank for completion of the project which includes necessary controls, tuning, etc. Old version of any software should be discontinued by the vendor only after obtaining the consent from the bank management. If the bank desires to continue with the old versions, the vendor should provide such a version under an ESCROW arrangement as specified above. The maintenance of the old version, however, would become the responsibility of the bank officials, as vendor may not be interested in supporting the old version for maintenance.

- The vendor company will take full responsibility of master creation at a mutually agreed cost and its smooth functioning after installation of the software. As a part of the offer, the vendor company should deliver copies of the users manuals and operation manuals.

- In addition the vendor company should provide one source code copy of complete software ordered under the purchase order on magnetic media for backup purposes.

- The entire software duly customised should carry the warranty period of minimum of 12 months from the date of the installation of the customised software. Such warranty should protect the bank fully against all software bugs, faulty programming and provide free maintenance during this period.

- The vendor company should provide software maintenance services starting from the date of completion of the warranty period on annual basis preferably at not more than 10 percent per annum. The vendor company should carry out debugging as may be required in smooth running of the software and changes that must be necessary from the security angle during AMC. Database administration and tuning should be integral part of software maintenance and should be done periodically as may be mutually agreed to.

- The time frame indicating the schedule of implementation plan should be drawn by the vendor company in consultation with the Computer Policy and Planning Department (CPPD) of the bank. In case of delay in customisation / implementation beyond a stipulated period, the vendor company should pay the bank damages on mutually agreed terms per day from the first day of such delay till the completion of the project.

- The vendor company should advise the bank about composition of the project team with the view to ensuring smooth implementation of the project and it is very much desirable that the team identified should continue till the completion of the project. The bank should enter into ESCROW arrangement with the vendor company as specified above.

4. The availability of IT / IS education training support from the Vendor needs to be stressed. Banks should ensure IT culture and awareness is well spread through such support systems, as it is prerequisite for successfully adding to the customer service and providing value addition in business decisions.

<u>Annexure 15</u>
(Para 6.1.1)

Data Warehousing and Data Mining

1 What is Data Warehouse ?

1.1 Data warehousing means a central repository of all critical data, which help managers to take decisions, based on authentic information. Building a data warehouse is not an easy task. The type of data to be kept in a data warehouse is a pivotal issue to be examined by the banks/financial institutions, since this exercise involves a lengthy and tedious process of consolidating all back end data from different databases.

1.2 Data warehousing at the most fundamental level is a staging area for decision support information. It collects raw data from various applications in an organizations' operational systems, integrates the data into a logical and uniform model of business subject areas. It stores the information in a manner that is accessible and understandable to all decisions makers and delivers information to decision-makers across the organizations through various query and reporting tools.

1.3 It is difficult to utilize the core operational data for decision making. A warehouse overcomes this restriction by adopting a different technology / method for organisation, structure, access of data.

2 **Data "Populated" on to a Data Warehouse** :

2.1 There are two high level categories of data populated on to a data warehouse environment and these are defined by source :

@ Internal Data
@ External Data

Internal Data :

$ Data belonging to and generated by the enterprise
$ Generated by operational transaction Systems
$ Described activities happening inside the enterprise

External Data :

# May be obtained or purchased by the enterprise.
# Describes activities happening outside the enterprise.
# The purpose of analysing external data is recognise opportunities, visualise threats, and identify synergies.

3 The Structure of the Data Warehouse :

3.1 Data warehouses have a distinct structure. There are different levels of summarisation and details that demarcate the data warehouse. The different components of data warehouse are :

- Meta Data
- Current Detail Data

* Older Detail Data
* Summarised Data

3.2 **Meta Data** can be classified into two categories :

# Technical Meta Data
# Information about data sources
# Transformation description
# Warehouse object and data structure definitions
# Rules to perform data clean up and data enhancement
# Data mapping
# Access Meta Data
# Business Meta Data
# Subject areas and information object type
# Internet Homepages
# Other information to support all data warehousing components
# Data warehouse operational information

3.3 The **Current Detail Data** is the major concern because
(a) It reflects the most recent happenings
(b) It is voluminous
(c) It is always stored on a disk which is easy to access by anyone.

3.4 **Older Data** is data that is frequently accessed and is stored at a level of detail consistent with current detailed data. While not mandatory that it be stored on an alternate storage medium, because of the anticipated large volume of data coupled with infrequent access of the data, the storage medium for older data is usually removable storage such as automatic tape library.

3.5 The **Summarised Data** is of two type, according to the processing need and storage. These are :

- **Lightly Summarised Data** is data that it is distilled from the current detailed level. This level of the data warehouse is almost always stored on disk storage.
- **Highly Summarised Data** is compact and easily accessible.

4 Access Tools :

4.1 The following are the front-end tools for user interaction. They support both dynamic and pre-planned analysis. They use Meta Data for accessing the warehouse. They can be classified into five main groups:
* Data query and Reporting Tools
* Application Development Tools
* Executive Information Systems Tools
* On-line Analytical Processing Tools
* Data Mining Tools

4.2 **On-line Analytical Application (OLAP) :**

4.2.1 Since, Data warehouse has to cater to ad-hoc and complex queries, it uses a special type of architecture called "Multi Dimensional Data Bases (MDDB)" which can be implemented using relational technology with stars schema.

4.2.2 Multi dimensional data may recite in spreadsheets, relational databases, or legacy data managers. The data-access and analysis tools must be able to take enterprise data from a variety of sources and give work groups the accessibility, power, and flexibility the need to view it in every conceivable way. Only multidimensional analysis provides a clear picture of the business at any given time. OLAP is the answer.

4.2.3 Characteristics of OLAP :

+ The ability to scale large volumes of data and large number of concurrent users.
+ Provides fast, interactive response time.
+ Provides for analysing time series.
+ Supports `What If' analysis and planning in a multi user "read-write" environment
+ Robust data access security and user management.
+ Availability of a wide variety of viewing and analysis tools and support different user community

5. Data Mining :

5.1. The use of large databases (Data Warehouse) to store customer information created the need to leverage the information for better customer service and competitive advantages in the ever-changing market place.

5.2 Data Mining is the process of extracting hidden information from databases. Data Mining also helps in predicting future trends and behavior allowing business to make pro-active and knowledge driven decision.

5.3 Data mining is often viewed as a corollary to Data Warehousing because of the necessity to integrate and derive new information that transactional systems do not provide.

5.4 Data Warehousing allows building the Data Mountain. Data Mining allow shifting the mountain down to the level of essential information that is useful to the business. The metaphor here is that some nugget of gold hidden in the mountain of data and Data Mining can find the gold which would otherwise be too costly or too difficult to find without Data Mining tools.

5.5 Data Mining Techniques :

**** Classification :***

This technique is used to classify database records into a number of redefined classes based on certain criteria. For example, a bank wants to classify its customer records as good, medium, or poor risk based on the attributes income, and age. A generated rule could be that a customer in the age group between 50 and 60 with an income greater than Rs.50,000 are a good credit risk.

**** Clustering and Segmentation :***

This technique is used to segment the database into different clusters, based on a set of attributes. Records with similar attributes are in the same cluster. For example, retailers want to know where similarities exist in their customer base so that they can create and understand their target market better.

*** Association Rules:***
These techniques are often used for market basket analysis and discover rules that are hidden between the attributes. For example, 60% of all customers that buy diapers also buy beer on Friday afternoon. The percentage of occurrence is the confidence factor.

*** Sequencing :***
This technique helps identify patterns in times series. This is useful for stock market predictions or for catalogue companies. For example, they might discover that buyers of today buy learning software for children five years later.

*** Decision Tree :***
It is a predictive model that can be perceived as a tree. Each branch of the tree is a classification question and the leaves are the partitions with their classifications.

*** Neural Networks :***
Neural networks try to stimulate the human brain. The nodes of the neural networks are connected and every connection has a weight. The difference between the output and the training output is called the error and is "Back-Propagated" through the net. The weights are adjusted according to the error.
Neural networks can handle noise in the data and are good for most of the problems, but the knowledge cannot be analysed like for the decision trees. Therefore, neural networks can be pursued as a black box only.

***** Genetic Algorithms :***
Genetic algorithms stimulate the biological evolution. The attributes are coded like the DNA. A lot of individuals are generated and from generation to generation they change their DNA with operators like mutation and crossover. The survival of the fittest principle selects only individuals that are better than the generation before.

*** Rule Induction (Association Rules) :***
All possible patterns in the database are systematically pulled out and then the accuracy (confidence) and the coverage (support) are calculated. The rules are easy to understand.

6. Select Internet Websites for further information on Data Warehousing and Data Mining

1. http://www.cait.wustl.edu/papers/presume
2. http://www.ecst.csuchico.edu-tatianam/csci 374/dataware.html
3. http://www.digital.com/info/liO1sc/li01schm.htm
4. http://www.fis.www.com/banking.htm
5. http://www.fis.www.com.peoplesbnk.htm
6. http://www.microstrategy.com/dw dossier/vol3 num1/banking.htm

7. http://ftp.ncr.com/product/financial/product/ifs/cc/cc/htm
8. http://www.software.ibm.com/data/solution/customer/siam/siam.htm
9. http://www.software.ib.com/data/solution/customer/korea-hb/korea-hb.html
10. http://www.sybase.com/inc/success/bomhtml
11. http://www.techmall.com./techdocs/np980701-3.html
12. http://www.data-warehouse.com/index.html
13. http://www.dmdirect/issue1.3/article2.htm

7. Select Bibliography on Data Warehousing and Data Mining

1. ***Data Warehousing & Data Mining Technology: An Overview*** by Prof.S.Chandrasekhar, Senior Professor and Executive Director, FORE School of Management, New Delhi

2. ***Data Warehousing - Concept, Technologies, Implementations, and Management*** by Dr.Harry Singh, Ph.D.Prentice Hall PTR, Upper Saddle River, New Jersey 07458

3. ***Data Warehousing for Dummies*** by Alan R.Simon, Comdex Computer Publishing (A Division of Pustak Mahal), New Delhi 110 002.

Annexure 16
(Para 7.4.2)

Extract from Proposed Electronic Commerce Bill , 1999

(Sections 9, 10, 11, 12 and 14)

9. Original Record

(a) Where a rule of law requires a record to be presented or retained in its original form, that requirement is met by an electronic record or otherwise; and

(i)there exists reliable assurance as to the integrity of the record from the time where it was first generated in its final form is an electronic record or otherwise; and
(ii)where it is required that a record be presented, that the record is capable of being displayed to the person to whom it is being presented.

(b) Subsection (a) applied whether the requirement referred to therein is in the form of an obligation or whether the law simply provides consequences for the record not being presented or retained in its original form.

(c) For the purposes of subsection (a)(i) :

(i) the criteria for assessing integrity shall be whether the information has remained complete and unaltered, apart from the addition of any endorsement and any change which arises in the normal course of communication, storage and display; and
(ii) the standard of reliability required shall be assessed in light of the purpose for which the information was generated and in light of all the relevant circumstances.

10. **Admissibility and Evidentiary Weight of Electronic Records and Electronic Signatures**

(a) Nothing in the Indian Evidence Act, 1872 or any rules made under this Act shall apply in any legal proceedings so as to deny the admissibility of an electronic record or an electronic signature into evidence :

(i) on the sole ground that it is an electronic record or an electronic signature; or
(ii) on the grounds that it is not in its original form or is not an original.

(b) Information in the form of an electronic record shall be given due evidentiary weight without regard to the fact that it is an electronic record. In assessing the evidentiary weight of an electronic record or an electronic signature, and shall be given to :

(i) the reliability of the manner in which it was generated, stored or communicated;
(ii) the reliability of the manner in which its integrity was maintained;
(iii) the manner in which its originator was identified or the electronic record was signed; and
(iv) any other factor that may be relevant.

(c) Nothing in this section shall be construed to affect the provisions of Section 4 of this Act.

11. Retention of Electronic Records

(a) Where any law for the time being in force requires that certain documents,, records or information be retained, whether permanently or for a specified period, that requirement is satisfied by retaining them in the form of electronic records if the following conditions are fulfilled.

(i) the electronic record and the information contained therein remains accessible so as to be usable for subsequent reference;
(ii) the electronic record is retained in the format in which it was originally generated, sent or received, or in a format which can be demonstrated to represent accurately the information originally generated, sent or received; and
(iii) such information as enables the identification of the origin and destination of an electronic record and the date and time when it was sent or received, if any, is retained.

(b) An obligation to retain documents, records or information in accordance with subsection (a) shall not extend to any data the sole purpose of which is to enable the record to be sent or received.

(c) It shall be lawful for a person to satisfy the retention requirement referred to in Section 11(a) by using the services of any other person, if the conditions in Sections 11(a)(I) through (iii) are complied with.

(d) Nothing in this section shall preclude any department or ministry of the Central Government, State Government or a statutory corporation under Central or State Government from specifying additional requirements for the retention of electronic records that are subject to its jurisdiction.

12. Secure Electronic Record.

(a) For the purposes of this Section 12 and of Section 13, whether a security procedure agreed to by the parties involved has seen applied to an electronic record in a trustworthy manner and has been relied upon reasonably and in good faith by the relying party to verify that the electronic record has not been altered since a specified point of time, such record shall be treated as a secure electronic record from such specified point of time to the time of verification.

(b) For the purposes of this Section 12 and of Section 13, whether a security procedure is commercially reasonable shall be determined in light of the procedure used and the commercial circumstances prevailing at the time the procedure was used, including :

(i) the nature of the transaction;
(ii) the sophistication of the parties;
(iii) the volume of similar transactions engaged in by the parties involved;
(iv) the availability of alternatives offered to but rejected by any party;
(v) the cost of alternative procedures; and
(vi) the procedure in general use for similar types of transactions.

(c) Whether reliance on a security procedure was reasonable and in good faith shall be determined in light of all the circumstances known to the relying party at the time of the reliance, with regard to;

(i) the information that the relying party knew or should have known of at the time of reliance that would suggest that reliance was or was not reasonable;
(ii) the value or importance of the electronic record, if known :
(iii) any course of dealing between the relying party and the purported sender and the available indications of reliability or unreliability apart from the security procedure;
(iv) any usage of trade, particularly trade conducted by trustworthy systems or other computer-based means; and
(v) whether the verification was performed with the assistance of an independent third party

14. Presumptions Relating to Secure Electronic Records and Signatures.

(a) In any civil proceedings involving a secure electronic record, it shall be presumed, unless the contrary is proved, that the electronic record has not been altered since the specific point of time to which the secure status relates.

(b) In any civil proceedings involving a secure electronic signature, the following shall be presumed unless the contrary is proved.

(i) the secure electronic signature is the signature of the person to whom it correlates: and
(ii) the secure electronic signature was affixed by that person with the intention of signing or approving the electronic record.

(c) In the absence of a secure electronic record or a secure electronic signature, nothing in this Part shall create any presumption relating to the authenticity and integrity of the electronic record or an electronic signature.

(d) The effect of presumptions provided in this section is to place on the party challenging the integrity of a secure electronic record or challenging the genuineness of a secure electronic signature both the burden of going forward with evidence to rebut the presumption and the burden of persuading the trier of fact that the nonexistence of the presumed fact is more probable than its existence.

(e) For the purposes of this section :
(i) "secure electronic record" means an electronic record treated as a secure electronic record by virtue of Sections 12 or 21: and
(ii) "secure electronic signature" means an electronic signature treated as a secure electronic signature by virtue of Sections 13 or 22

Annexure 17
(Para 8.1.3)

Technology plan

Technology planning in banks has hitherto emphasised quantitative aspects. Banks should move away to a qualitative approach. An Information Technology Plan should be drawn up which reflects the business strategies of the bank over a three year period. The plan could comprise the following elements:

(a) Overview of business strategies: This should cover the broad business goals in both wholesale and retail banking arena and the specific strategies proposed to achieve the business goals.

(b) Overview of the technology environment in the bank and in the industry: This should contain a summary of the existing technology in the bank, indicate key technology trends and any changes to the technology platforms which would be needed as a result, viz., a) obsolescence of existing technology platforms, b) the need to conform to emerging technology standards, and c) other issues like Y2K/ Euro compliance.

(c) Recommendations regarding the technology projects proposed for achieving the business strategies in the respective segments: For example, if one of the goals of retail banking strategy is to improve customer service delivery channels in metro cities, the plan should detail the strategy for installing technology such as in-branch / off-site ATMs, Telephone Banking etc. The services to be offered through these channels, the technical linkages needed should also be detailed.

(d) A technology architecture : The aim of the architecture document would be to offer a technical framework within which all projects can be fitted to ensure inter-operability and consistency of processing. The document should indicate the technologies proposed for each project, the inter-dependencies among projects, the common middleware, if any, proposed for linking the various dependent projects and interim solutions proposed pending the availability of the final technology elements.

(e) Project costs: An estimation of the project costs should be made so that plan budgets can be drawn. The costs should be divided into discretionary and non-discretionary expenditure. Non-discretionary costs would include those relating to hardware / software maintenance, infrastructure charges, routine software enhancements, staff costs etc. The discretionary costs would include those relating to the new technology projects.

(f) The phasewise implementation schedule: The project priorities should be fixed based on the business priorities, the availability of technical skills, staff and financial resources.

Annexure 18
(Para 1.5.5)

ABBREVIATIONS

ACRONYM	**DETAILS**
ACH	Automated Clearing House
ALM	Asset Liability Management
ALPM	Advanced Ledger Posting Machine
AMC	Annual Maintenance Contract
API	Application Programming Interface
ATM	Automatic Teller Machines
BSR	Basic Statistical Returns
CAS	Central Accounts Section, RBI, Nagpur
CBDT	Central Board of Direct Taxes
CIDR	Classless Inter Domain Routing
COMET	Computerised Message Transfer

CPPD	Computer Policy and Planning Department
CUG	Closed User Group
DAD	Deposit Accounts Department
DAMA	Demand Assigned Multiple Access
DAT	Digital Audio Tape
DBA	Data Base Administrator
DBMS	Data Base Management System
DBS	Department of Banking Supervision
DD	Demand Draft
DDO	Drawing and Disbursement Officer
DES	Data Encryption Standard
DIT	Department of Information Technology
DNS	Domain Name System
DoT	Department of Telecommunication
DRDO	Defense Research and Development Organisation
DSS	Decision Supports System
DvP	Delivery Versus Payment
ECS	Electronic Clearing Services
EDP	Electronic Data Processing
EDI	Electronic Data Intechange
EFT	Electronic Funds Transfer
EFTPOS	Electronic Funds Transfer at Point of Sale
EMV	Europay, Master card, Visa
FI	Financial Institution
FPB	Focal Point Branch
FTP	File Transfer Protocol
GAD	Government Accounts Dept, State Bank of India

GUI	Graphical User Interface
HO	Head Office
HPA	High Power Amplifier
HR	Human Resources
HRD	Human Resource Development
IBA	Indian Banks’ Association
IBR	Inter Branch Reconciliation
ICMP	Internet Control Message Protocol
IDMC	Internal Debt Management Cell
IDRBT	Institute for Development and Research in Banking Technology
IDU	Indoor Unit
IFSC	Indian Financial Code System
IIT	Indian Institute of Technology
INFINET	INdian Financial NETwork
IP	Internet Protocol
IPX	Internet Protocol Exchange
IS	Information System
ISDN	Integrated Services Digital Network
ISO	International Standard Organisation
IT	Information Technology
Kbps	Kilo bits per second
LAN	Local Area Network
LNA	Low Noise Amplifier
LVTS	Large Value Transfer System
Mbps	Mega bits per second
MICR	Magnetic Ink Character Recognition
MIS	Management Information System

MOU	Memorandum of Understanding
MT	Message Transfer
NAT	Network Address Translator
NBFC	Non-Banking Financial Companies
NCC	National Clearing Centre / Cell
NCST	National Council for Software Technology
NIBM	National Institute of Bank Management
NMS	Network Management System
NPA	Non Performing Asset
NRI	Non-Resident Indians
OLTP	On-line Transaction Processing
OS	Operating System
OSMOS	Offsite Surveillance and Monitoring System
OSPF	Open Shortest Path First
PAD	Public Accounts Department
PAO	Pay and Accounts Officer
PC	Personal Computer
PPP	Point to Point Protocol
PSTN	Public Switched Telephone Network
PVP	Payment Versus Payment
QoS	Quality of Service
RAPID	Receipt and Payment Instruments/Documents
RBI	Reserve Bank of India
RDBMS	Relational Data Base Management Systems
RF	Radio Frequency
RIP	Router Information Protocol
RPC	Remote Procedure Call

RSA	Rivest Shamir Adleman
RTGS	Real Time Gross Settlement
SBI	State Bank of India
SCPC	Single Channel Per Carrier
SDLC	Synchronous Data Link Control
SET	Secured Electronic Transaction
SLIP	Serial Line Internet Protocol
SQL	Structured Query Language
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TBA	Total Branch Automation
TCP	Transmission Control Protocol
TDM	Time Division Multiplexing
TDMA	Time Division Multiple Access
TFTP	Trivial File Transfer Protocol
TM	Treasury Management
TP Monitor	Transaction Processing Monitor
TT	Telegraphic Transfer
TTL	Time To Live
UDP	User Datagram Protocol
UN/EDIFACT	United Nations Electronic Data Interchange Financial and Commercial Telecommunication
UPS	Uninterrupted Power Supply
URL	Uniform Resource Locator
VLSM	Variable Length Subnet Masking
VSAT	Very Small Aperture Terminal
WAN	Wide Area Network
Y2K	Year 2000