Digital Certificates in Payment Systems

Ops Payment System
State Bank Global IT Centre
CBD Belapur, Navi Mumbai

PAYMENT SYSTEM PRODUCTS

- RTGS
- NEFT

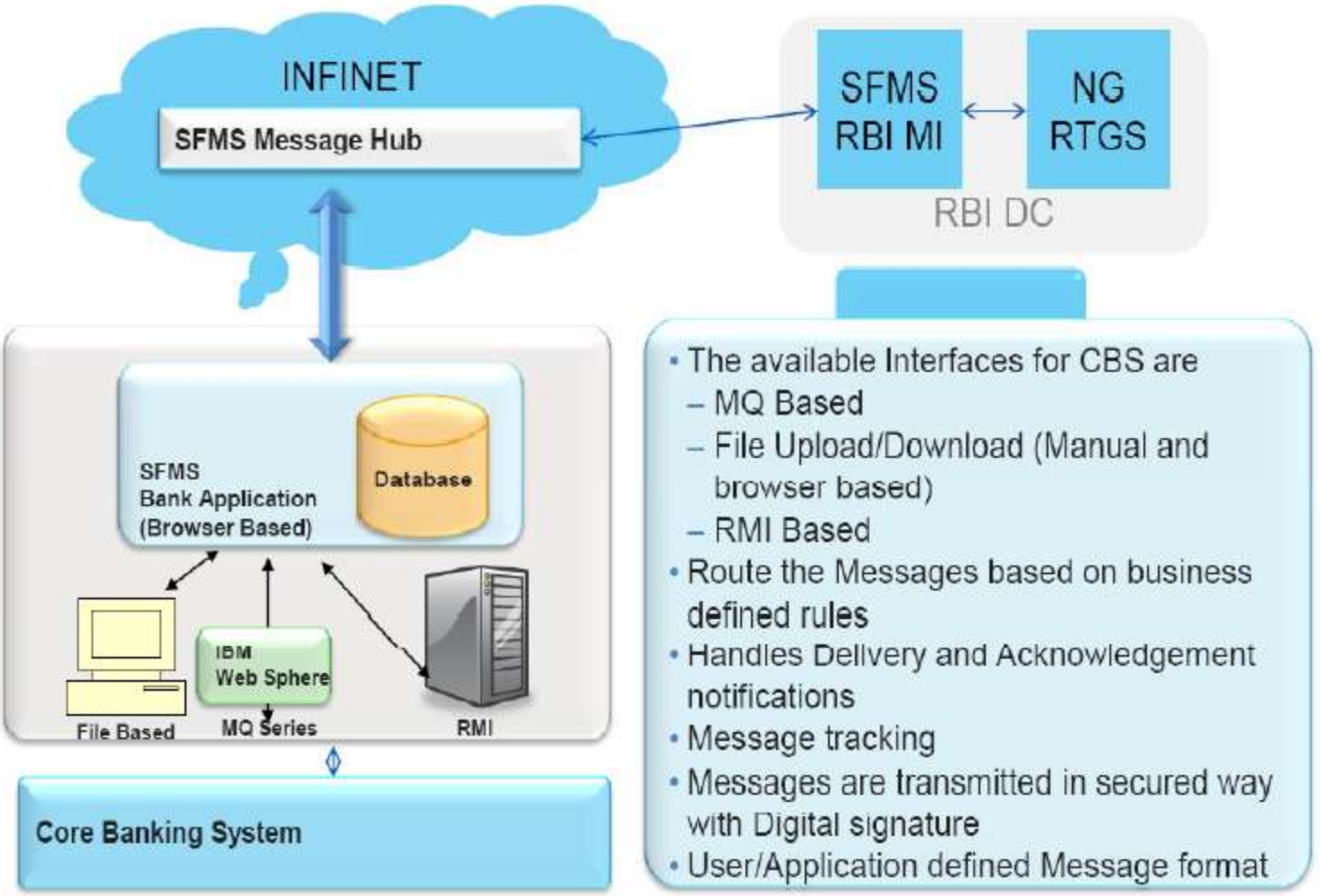
SFMS

- **Structured Financial Messaging System** (SFMS) is a secure messaging standard developed to serve as a platform for inter-bank applications.
- It is an Indian standard similar to SWIFT (Society for World-wide Interbank Financial Telecommunications) which is the international messaging system used for financial messaging globally.
- SFMS Application is used for RTGS and NEFT for its gateway systems to RBI/IDRBT.

SFMS Features

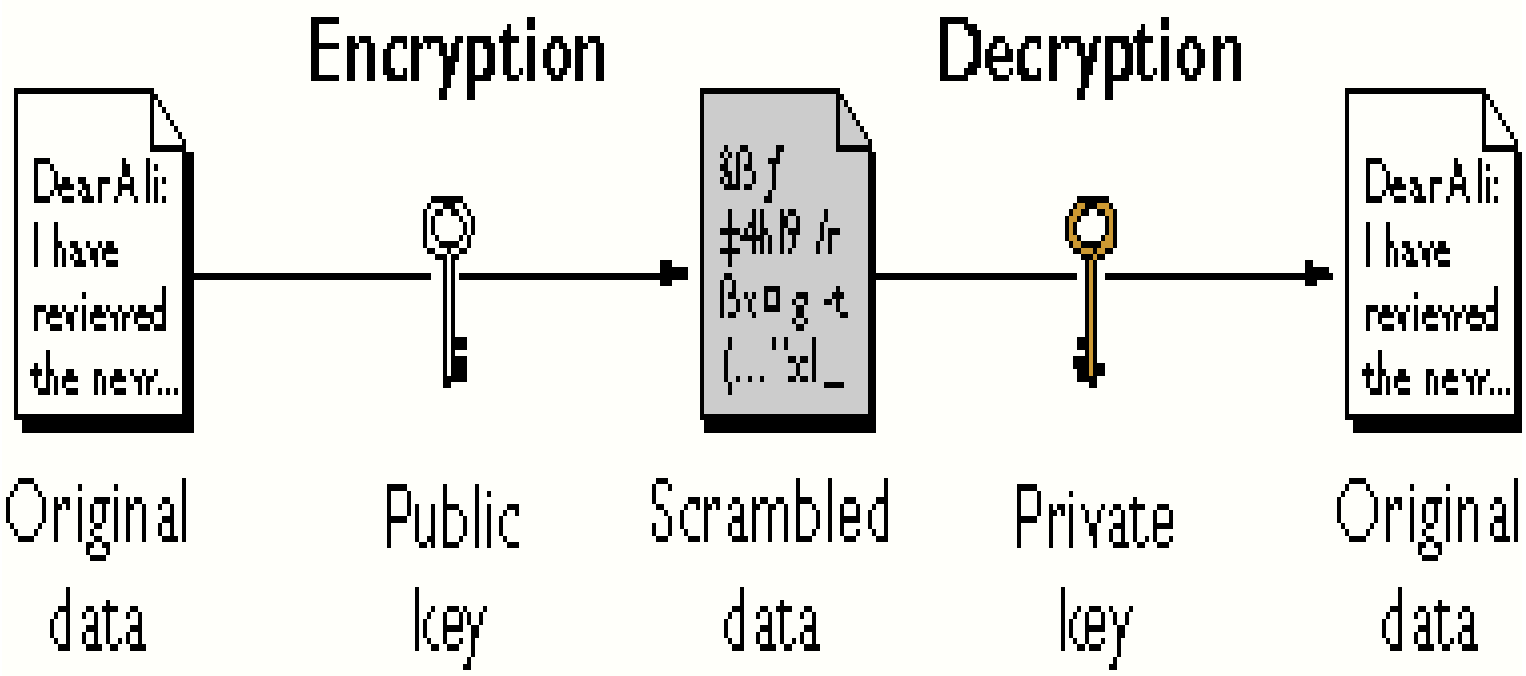
- RTGS Member's SFMS Server communicates with IDRBT Message Hub/RBI through INFINET (Indian Financial Network)
- Secured Communication
- Digitally signed & encrypted
- Specified message format
- Unique identification – Unique Transaction Reference (UTR) / Sequence Number (SN)
- Participants identified uniquely by IFSC(Indian financial system code)

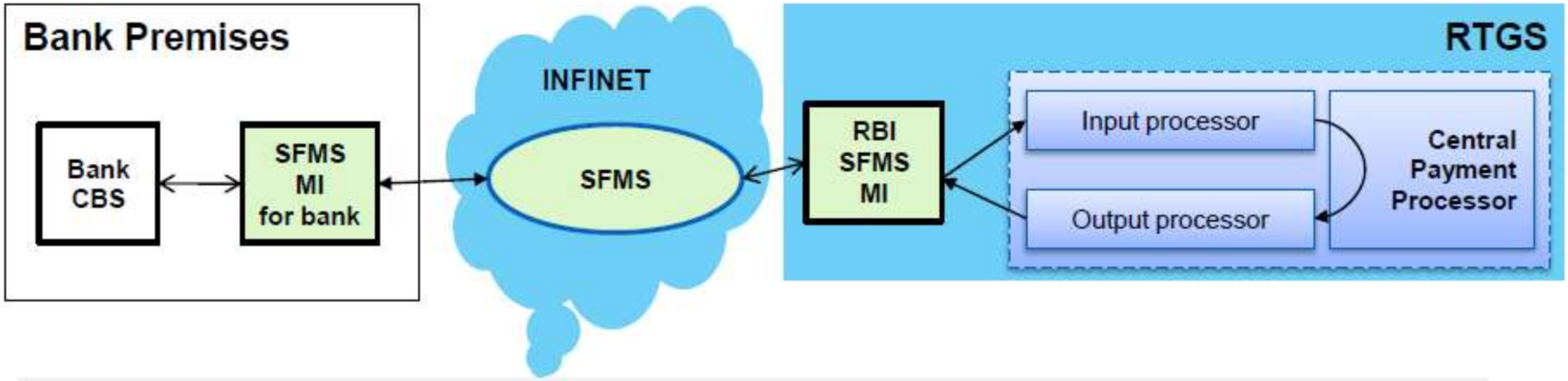
SFMS MI Application overview



- The available Interfaces for CBS are
  - MQ Based
  - File Upload/Download (Manual and browser based)
  - RMI Based
- Route the Messages based on business defined rules
- Handles Delivery and Acknowledgement notifications
- Message tracking
- Messages are transmitted in secured way with Digital signature
- User/Application defined Message format

Asymmetric Key Encryption or Public Key Encryption





- Full STP
- Horizontal scaling possible for parallel input and output processing
- Supports High Volume of transactions
- SFMS as the Messaging Service
- SFMS-MI Thick-client at the Banks Premises – enabling STP.

Security Overview – ISO messaging

SFMS Application should ensure

i) The messages received from banks should be digitally signed and verified at SFMS application end, even through the systems are in same network.

ii) The maker and checker authorization concept is enforced for all the messages which are not Digitally signed at Bank end.

iii) Node to node authentication, guarantees the message is from its rightful sender.

iv) Implementation(s) should be as per CCA guidelines

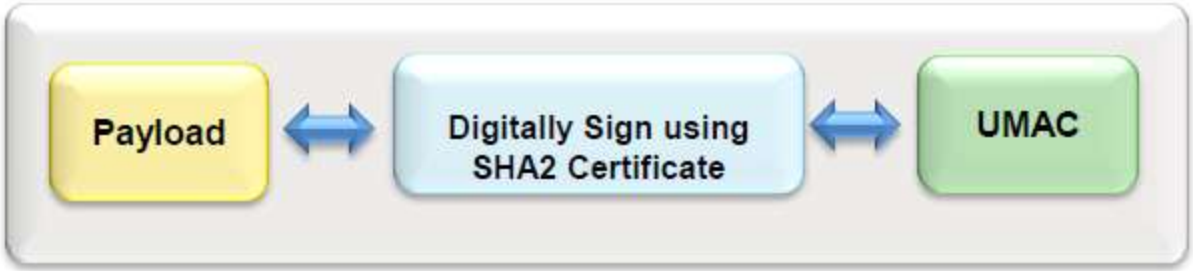
To achieve message End–to-End security

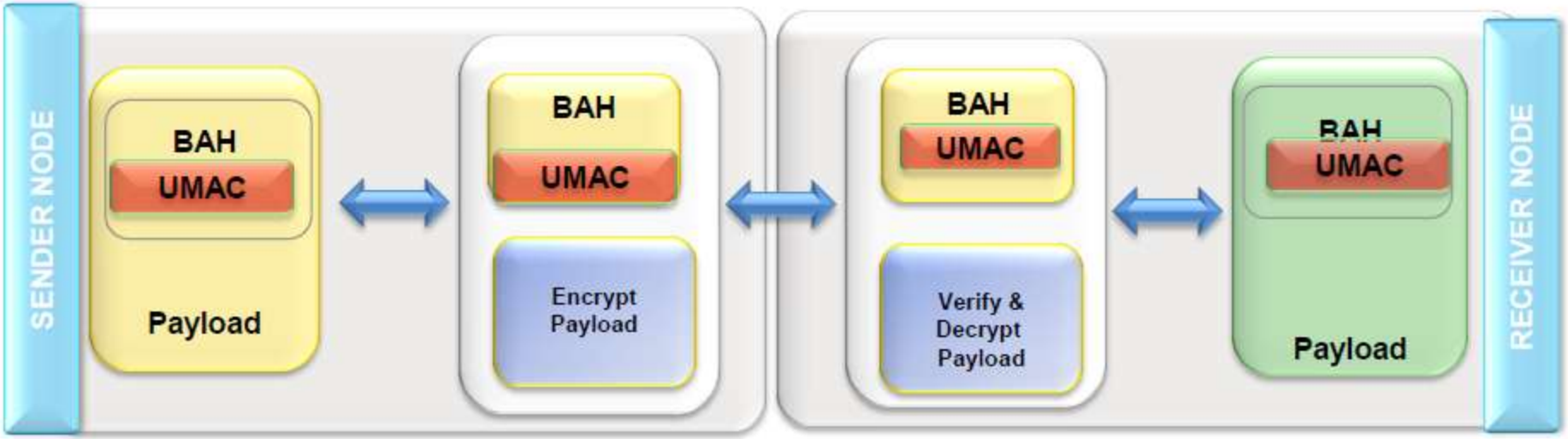
1. Authentication to identify the sender of the message.
2. Non-repudiation of the message guarantees that the sender has seen the message and therefore cannot deny having produced it.
3. End-to-end message integrity to guarantee that the message has not been modified during transit.
4. End-to-end message confidentiality to make the message unreadable to all except the receiver.

Security Framework – ISO Messaging layer

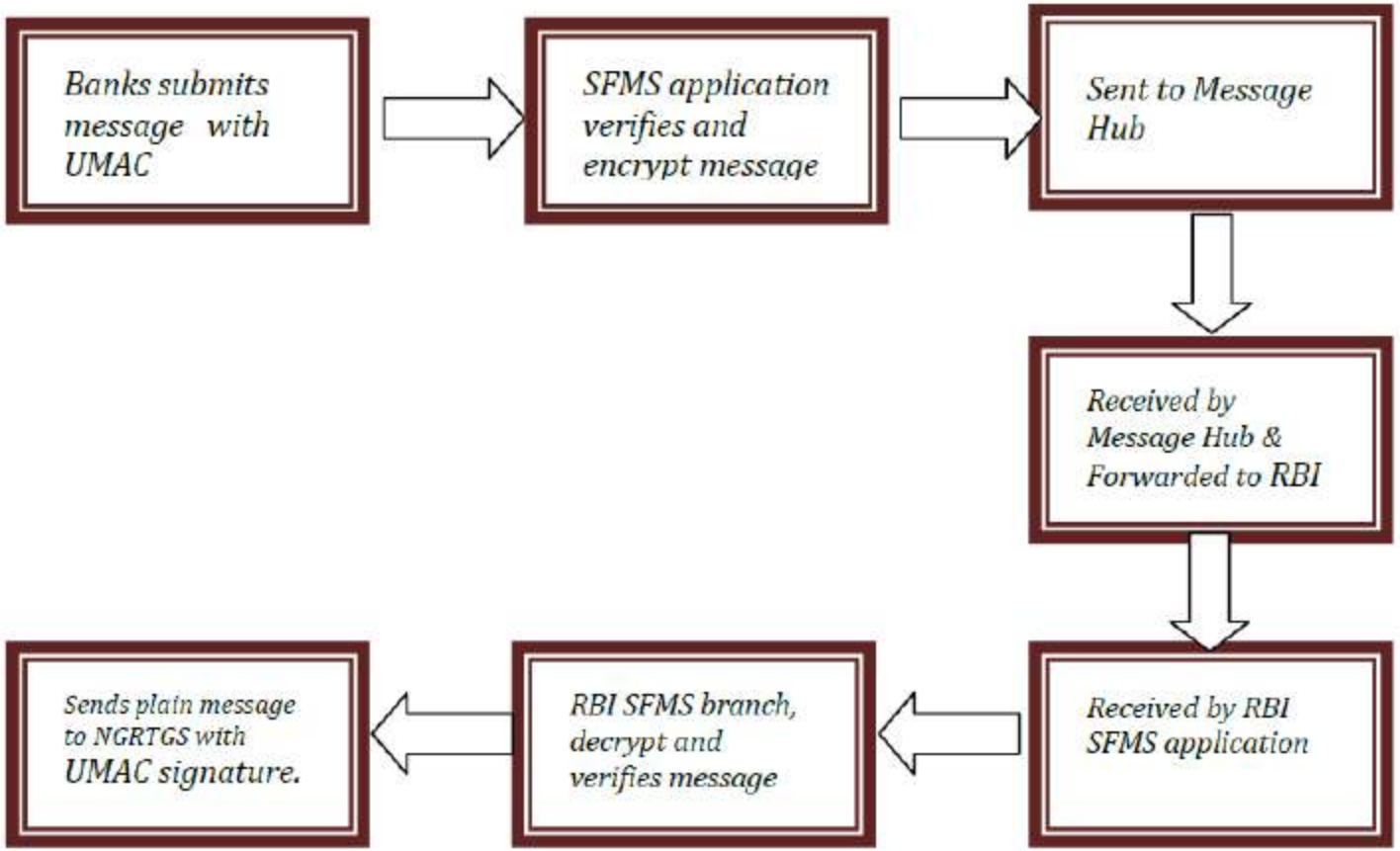
- The messages received from banks should be digitally signed and verified at SFMS application end, even through the systems are in same network
- The maker and checker authorization concept is enforced for all the messages which are not signed at Bank end.

The digital signing / verification procedures are followed as per the current SHA2 standards.





Secure messaging – SFMS over INFINET



SFMS Security – across components

MI Client OR MI Server access

- Only authorized users should be allowed access at Branch servers, through a Digital Certificate
- The user's certificate should be verified with respect to certificate expiry, revocation and access privileges while login into the MI server.

MI Server to messaging HUB

- Message confidentiality can be provided by encrypting the message at the MI with Next node public key.
- On receipt of message from MI, SFMS decrypts the message using private key
- Messaging HUB will not have any access to the contents of the messages. Messages will be stored at the HUB level in the encrypted format.

Messaging HUB to SFMS RBI MI

- The encrypted message will be decrypted by SFMS HUB and encrypted with next node public Key.

Security in SFMS MI

Thick Clients Security

- The messages are digitally signed using the certificates issued by IDRBT.
- The signature is included in the business application header (BAH) of the message and it covers the actual ISO message, excluding the BAH.
- The payload is encrypted through network till it reaches the destination node.
- The NG-RTGS verifies the signature of each message before it accepts the settlements.
- Then the signature is copied verbatim by the NG-RTGS to the outgoing message delivered to the receiving Participant after the settlement takes place so that the receiving institution can verify the authenticity of the payment.
- The NG-RTGS application will ensure that the owner of the certificate used to sign the incoming message is also the debited party indicated within the message's details.

- Thank You