Assuring Statistical Confidentiality and Security: RBI experience

Dr. Anil Kumar Sharma
(anilksharma@rbi.org.in)
Adviser
Department of Statistics & Information Management
Reserve Bank of India

Information Confidentiality & Security

- Core Principles of Information Security includes
  - **Data Confidentiality**: Preventing the disclosure of information to unauthorized individuals or systems. This is achieved through the process of **ENCRYPTION (non-readability) of Data while in transit or at rest**. **Data Masking** of confidential data is another way to protect confidential information.
  - **Data Integrity:** Ensuring the accuracy and consistency of data over its entire life-cycle. This means that **data cannot be modified in an unauthorized or undetected manner.**
  - **Data Availability:** Information must be available when it is needed. This means that the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly. **HIGH Availability (24X7).**
  - **Data Authenticity:** Ensuring authenticity of parties involved in the transaction. Some systems use **Digital/Electronic Signature Certificates** to ensure the authenticities of parties involved.
  - **Non-Repudiation**: In law, non-repudiation implies one's intention to fulfil their obligations to a contract. It also implies that one party of a transaction cannot deny having received a transaction nor can the other party deny having sent a transaction. **Cryptographic systems** can assist in non-repudiation efforts.

Various methods used for Authentication

- Two Factor Authentication includes
  - User name & password and One Time Password (OTP)
  - User name & password and Grid Card
  - User name & password and Hardware Key
  - User name & password and Digital signatures can be derived from Public Key Infrastructure (PKI) credentials held on a PC-connected smart token — or "soft" credentials held on the customer's PC — using suitable client software
  - User name & password and Message Authentication Code (MAC) — based on secret-key cryptography — or a digital signature — based on public-key cryptography.

Depending on the criticality of the system, any of the above method of authentication may be deployed.

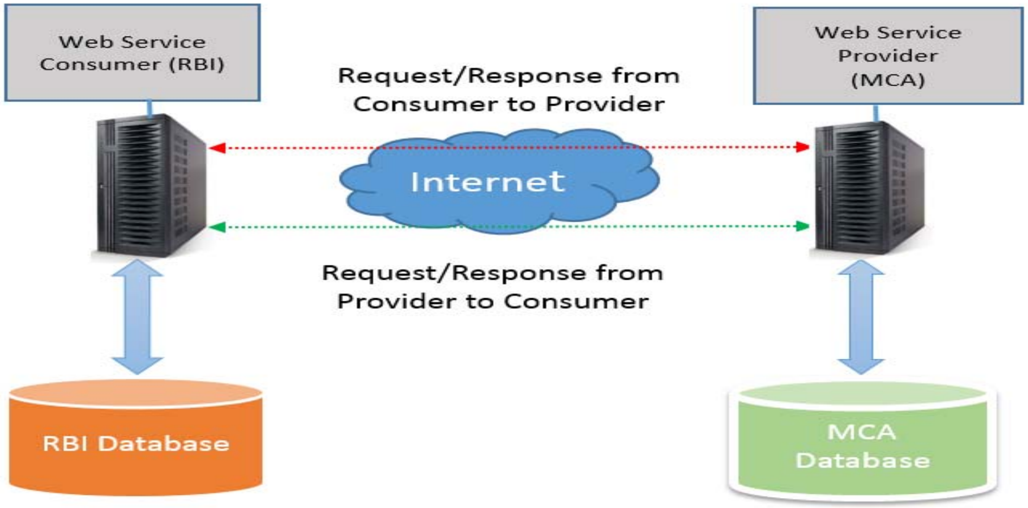
Use of Web Service APIs for Secured Data Transfer

- To enable the data exchange between RBI and MCA. Web service will be developed by MCA (by CDM Department of MCA) and hosted at their end. RBI will develop an application which will be hosted at Web server that will generate the data request and consume the Web service after proper authentication.
- Restful Web service will be created and consumed on both ends.
- As Consumer of Web service (provided by client in this case MCA) our Application will request Web service for Actual Data, Master Data and related files
- Data will be consumed in JSON format
- Data will be validated with the tracker information
- Error Log will be maintained
- After Consuming the Web service Acknowledgement will be send to Service provider
- The Channel of Data flow through the Web Service will be in Encrypted form

Use of Web Service APIs for Secured Data Transfer

- A web service is generally defined as ‘A software system designed to support interoperable machine-to-machine interaction over a network.’
- Web services allow you to expose the functionality of your existing code over the network
- Web services allow various applications to talk to each other and share data and services among themselves
- Web services are used to make the application platform and technology independent. (For example, a .NET or PHP application can talk to Java web services and vice versa.)

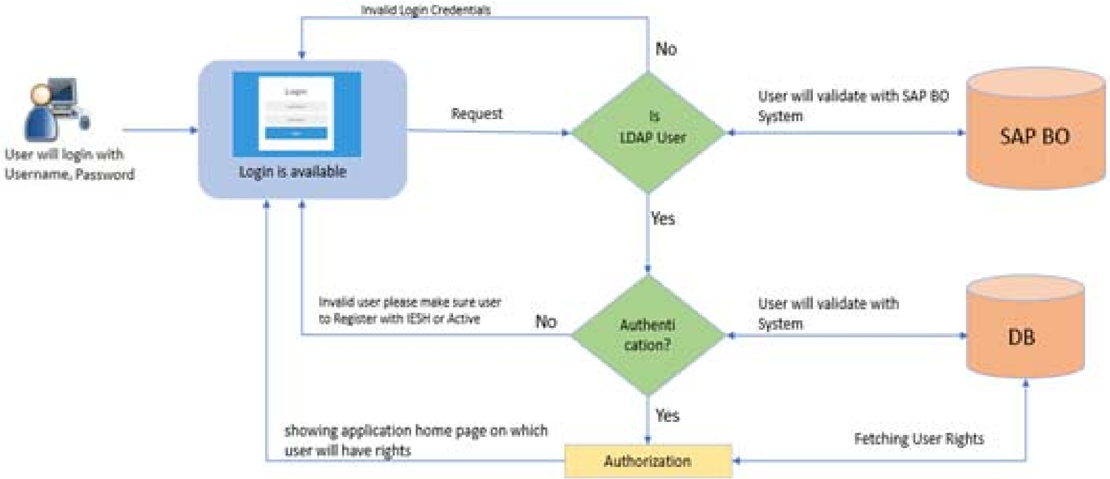
Use of Web Service APIs for Secured Data Transfer


Web Service Consumer (RBI)
Request/Response from Consumer to Provider
Web Service Provider (MCA)
Internet
Request/Response from Provider to Consumer
RBI Database
MCA Database

- IP’s for RBI will be whitelisted by MCA as a result access for the Web Service will be controlled and limited to just RBI users
- Secure algorithm will be used (SHA-256 or bCrypt) to encrypt the Web Service data.

Web Portal for Data Collection

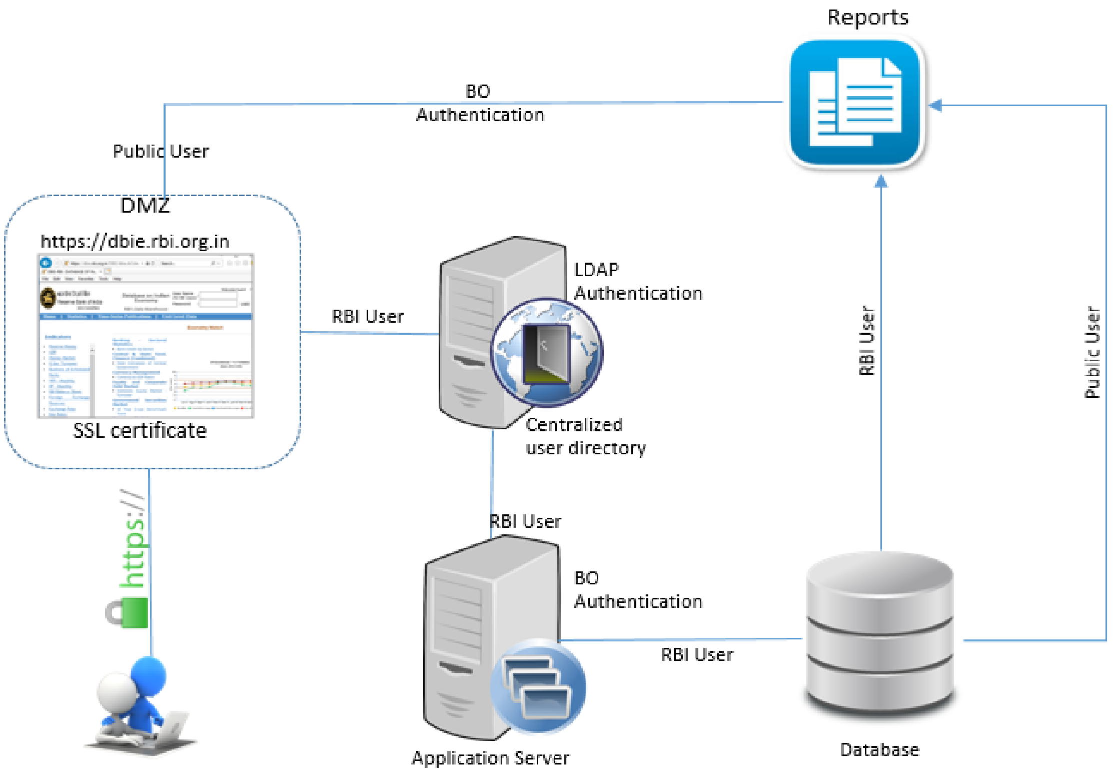
- The users are authenticated in the application by providing username and password. RBI user’s authentication will be performed by verifying their provided credentials with the application and their status in user master table in the database. However, outside user’s authentication will be performed by verifying their username and password from user master.
- Application has a Captcha and email OTP authentication facility


Invalid Login Credentials
No
User will login with Username, Password
Login is available
Request
Is LDAP User
User will validate with SAP BO System
SAP BO
Yes
Invalid user please make sure user to Register with IESH or Active
No
Authenti cation?
User will validate with System
DB
Yes
showing application home page on which user will have rights
Authorization
Fetching User Rights

User management and Access Control

- Access to confidential data requires proper authentication mechanism
- Confidential Data is accessible to the internal users of RBI with proper access rights defined at the application level.
- Currently, the authentication is being managed at two different levels for the internal users of RBI.
  - LDAP configuration and
  - Application level authentication.
- For each user (both internal and public), access levels are defined so that user can access the data.

User management and Access Control



Use of Secured website over Internet

- The DBIE can be accessed through the following url https://dbie.rbi.org.in using the web servers present in the Demilitarized Zone (DMZ).
- The SSL certificate is deployed to make sure that the communication is secure over the internet.

User security Management in RTGS

- All users of RTGS and PO are authenticated based on a digital certificate issued by Certifying Authority, a username and a secret password and user certificate serial number.
- The certificate is stored securely on token device along with the private and public keys.
- The user account definitions along with their passwords and certificate serial numbers are stored in the application main database.
- The passwords are stored only in an encrypted format.
- A password policy (i.e. minimum length, minimum complexity etc.) has been enforced to all users according to RBI internal regulations.
- The system also forces the users to periodically update their passwords, without reusing the same values.
- User Management is the responsibility of the admin of respective participants.
- RTGS uses Class III Signing and Encryption certificates with SHA2/RSA 2048 bits key for both SFMS-MI (Thick Client) and Web-API

Report on Enabling PKI in Payment System Applications

- RBI published its report on enabling Public Key Infrastructure (PKI) in Payment Systems in India in April 2014 https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=31054
- Major recommendations included were strengthening the security features in existing payment system applications and feasibility in implementing PKI in all payments system applications.
- All banks’ internet banking applications should mandatorily create authentication environment for password-based two-factor authentication as well as PKI-based system for authentication and transaction verification in online banking transaction.
- In online banking transactions, banks should provide the option to its customers for enabling PKI for its online banking transactions as optional feature for all customers.

PKI enabled Payment Systems in India

- Real Time Gross Settlement (RTGS)
- National Electronic Fund Transfer System (NEFT)
- Cheque Truncation System (CTS)
- Collateral Borrowing and Lending Obligation (CBLO)
- e-Kuber System (Core Banking Solution of RBI)
- Forex settlement system
- NACH system of NPCI

Non-PKI Payment Systems

- Non- MICR clearing systems
- ECS – Debit and Credit Clearings
- Credit Cards and Debit Cards Payment systems
- Mobile Payment Systems (IMPS)

Payment System During 2017-18	Volume (Million)	% to Total	Value (Rs. Billion)	% to Total
RTGS	124.4	0.78	1167125	46.18
CBLO, Forex and G-Sec (CCIL)	3.5	0.02	1074802	42.52
CTS	1111.9	6.70	74035	2.93
Retail Electronic Clearing (ECS, NEFT and NACH)	4457.3	28.05	183090	7.24
Paper Clearing (Non-MICR)	32.6	0.21	2442	0.09
Cards	4748.6	29.89	9191	0.36
Prepaid Payment Instruments (PPIs)	3459.0	21.77	1416	0.06
IMPS	1009.8	6.36	8925	0.35
Unified Payment Interface	915.2	5.76	1098	0.04
Total	15,888.5	100.00	2,527,539	100.00

Payment Systems Statistics

- About 98.87 per cent of total value of payment systems are being settled using PKI enabled payment systems
- However, only about 35.55 per cent of transactions (volume) are settled using PKI enabled payment systems
- About 30 per cent of transactions are card related payments and 22 per cent are PPIs related which are being settled without PKI enabled systems. However, these are low value transactions.
- The Reserve Bank of India in 2016 has instructed banks to shift from magnetic stripe based ATM and debit cards to EMV chip and Pin based model of cards to ensure protection of cards from cloning, skimming and other forms of frauds which can happen on a magnetic strip.
- Recently, RBI made **data localisation** as a mandatory requirement for foreign players who wants to operate in domestic payment space in India to take care of data privacy and security issues.

What level of security is needed?

- Implementation of information security **comes at a cost**.
- One has to ask **what level of security** should be implemented in a statistical system?
  - Encryption for **Data at Rest** or **Data in Transit** or **both**?
  - Electronic Signing versus OTP?
  - Whether both encryption and electronic signing is needed or not?

Thank You

Q&A