

Secure Banking using Digital Signatures

eMudhra helps large Banks in India secure login authentication and fund transfers using Digital Signatures

Industry

Banking

Banking Security

With increasing transactions going through mobile and the internet, the Banking regulator - Reserve Bank of India felt the need to comprehensively enhance security measures in Online banking to enhance privacy, confidentiality, authenticity and legal non-repudiation wherever required.

Business Need

Enabling two factor and multi factor authentication for Online Banking using Digital Signatures, One Time Passwords etc based on risk assessment of transactions.

Approach

Deploy an integrated solution for multi factor authentication including Digital Signatures to allow customers to securely login and conduct online transactions.

**Background**

The Banking regulator in India and the Central Bank – Reserve Bank of India came out with a detailed study on enabling Public Key Infrastructure and Digital Signature in the Banking System. The report highlighted that the interbank clearing for electronic payment systems used PKI and this constituted over 90% in terms of value of transactions in the year 2012-13.

With increasing cyber frauds, the Reserve Bank of India therefore felt the need to extend Digital Signature usage to end customers of Corporate and Retail Internet Banking as Digital Signatures offer very high security, enable risk containment and provide legal non-repudiation.

Business Requirement

Enhance the security of online Banking transactions and electronic payment systems. Banks must create an authentication environment for password based two factor authentication as well as PKI based system for authentication and transaction verification. Customers must be informed of risks, existing security measures and given a choice of different methods of authentication to be able to select a system that matches their security requirements *.

* Source – RBI Report of the Group for Enabling PKI in Payment Systems, January 2014

Technologies Used

Languages : JAVA(JDK 1.6+)

APIs: JCA, Bouncy Castle, XML Dig Sign, Apache XML Security Communities.

Frameworks: Spring 2.5, Hibernate 3.0

Web service protocols: SOAP/HTTP, WSDL

Cryptographic Standards: PKCS#1, PKCS#7, PKCS#11, PKCS#12, CMS, X.509 Certificate and CRL

Algorithm Standards: RSA, AES, SHA-256



Benefits

Banks have reaped significant benefits by implementing digital signature based authentication and fund transfers.

These include -

- Legal non-repudiation thereby reducing frauds
- Enabling enhanced security through the full chain of electronic payments from initiation to settlement
- Offering anywhere, anytime filing of forms for customer onboarding, service requests
- Faster turnaround time, increased employees efficiency, productivity and transparency
- Meeting compliance & regulatory requirements

Solution

eMudhra being a Licensed Certifying Authority in India and also PKI solution provider implemented emAS – eMudhra Authentication Server to enable Digital Signature based login and fund transfer.

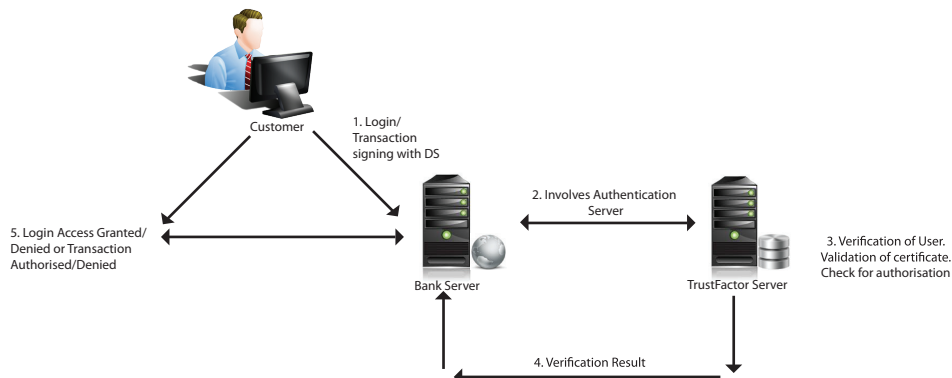
emAS is a plug and play authentication server that is implemented in over 23 banks in India across a variety of core banking/ internet banking applications.

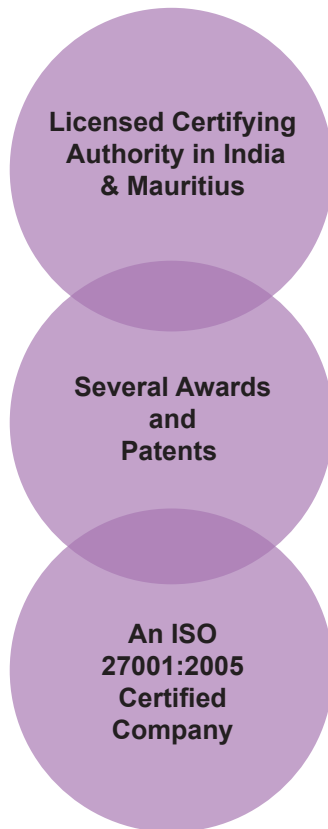
emAS works on top of the Internet Banking platform to provide digital signature signing and authentication. It works with leading core banking platforms such as Finacle, Flexcube, Bancs etc.

The emAS solution provides following broad modules:

- **emAS** – To authenticate, verify digital signature certificates on a real time basis.
- **Configuration Module-** Signature, Encryption & HSM
- **Hardware Security Module** - FIPS-2 level 3 certified physical computing device that safeguards and manages digital keys for strong authentication and provides crypto processing.
- **emCA – Certificate Lifecycle Management**
 - **Certificate Issuance** - To manage the issuance, revocation of Digital Signature certificates
 - **Certificate Download** - For downloading digital certificate from Certifying Authority (CA) as a soft or crypto token
 - **Certificate Registration** - To allow the customer to register their digital signature on the Banking application

emAS – Transaction Workflow





About eMudhra

eMudhra is a technology and digital identity and transaction management company providing solutions which ease financial and statutory needs of consumers. eMudhra was established in 2008 and is a Certifying Authority in India and Mauritius to issue Digital Signature Certificates.

eMudhra's current enterprise and consumer solutions include Digital Signature Certificates, emSigner – Paperless Office Solution, emAS – secure multifactor authentication for banks, emCA for Digital Signature issuance and management and Prism – Voice of Customer Analytics using Semantics.

eMudhra is a market leader in India and has worked with large Banks, Financial Services companies and several Government agencies in India to implement Digital Signature based solutions which include secure access and paperless workflows.

eMudhra won the e-Asia award, an award given by AFACT (A United Nations body) for implementing Digital Signatures based on India's National ID – AADHAAR to bridge Digital Divide.