emudhra
Trust Delivered

CASE STUDY

Bank Uses Digital Signature Certificates

Bank Uses Digital Signature Certificates

Intergration of DSC for Login and Transaction Signing Ensuring Convenience to Customers

Industry
Banking

Business Situation
ICICI Bank has in place a successfully running Internet Banking Application for both retail as well as corporate customers. The RBI through their Information Security Guidelines 2011, recommended usage of Digital Signature Certificates based on login and transaction signing.

Approach
Issuance of Digital Signature Certificates: eMudhra being a licensed Certifying Authority, issued digital signature certificates to the customers of the bank. eMudhra has created a white labeled alliance page specifically for the Bank through which customers are allowed to post certificate requests

Key Highlights
PKI setup with minimum modifications to the Bank's application and database

Authentication Server components installed in the Bank's web server and database is modified to store user login Information

Minimal modifications to the user interface to accept DSC data in addition to User ID and passwords

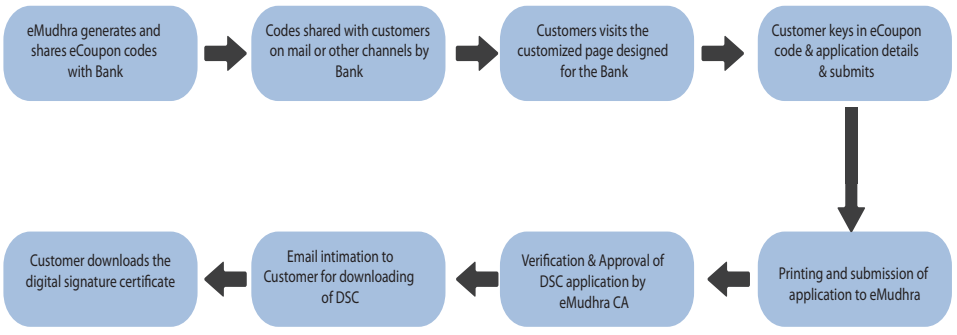
Real time certificate validation with OCSP and no other sharing of sensitive data between Bank and eMudhra

eMudhra carried out KYC, as per CCA guidelines, before issuing the DSC

Background

In India, retail and corporate banking is where the maximum frauds take place. According to the Association of Certified Fraud Examiners, the Indian banking sector has witnessed frauds of over Rs 8,646 crore in 2012-13, up from Rs 2,038 crore in 2009-10. Furthermore, 25% of the banks said that they face over 100 frauds a year. Majority of these could be attributed to the use of electronic payment and delivery channels for transaction. Thus there is a need to make electronic payments more robust and secure in order to protect information from unauthorized access, use, disclosure, disruption, modification, perusal, recording or destruction.

The RBI has mandated that internet banking applications should necessarily create an authentication environment for password-based two-factor authentication as well as a PKI-based system for authentication and transaction verification. PKI will enable users of a basically unsecure public network such as the Internet to securely and privately exchange data and money through the use of a public and a private cryptographic key pair.



Digital Signature Technology

The Digital Signature Technology works on the Public Key Infrastructure framework which uses a Cryptographic Key Pair – Private and Public Key for secure access and transmission of Information. Digital Signatures are generated by the issuer for the client in a secure device.

Benefits to the Bank

PKI technology in tandem with 2FA is a fool-proof solution against MITM (man-in-the-middle) and MITB (man-in-the-browser) attacks.

DSC ensures integrity and confidentiality of information since data is now impervious to phishing and hacking attacks.

DSC is issued by the Bank through a licensed certifying authority, hence it is legally valid.

The DSC identifies the user uniquely and therefore the user is subject to the attendant legal implications and non repudiation of data exchanged using the DSC.

Increased online transactions decreases demand on the Bank's physical assets due to reduced footfall at Branches.

Benefits to Customers

Benefits of a Paperless Office – With the introduction of DSCs, office space occupied by paper documents has reduced by 40%.

Relief from the manual process - Automation of basic manual processes helped increase the efficiency and productivity of employees. Employees could process more number of transactions compared to manual process. The time and effort spend by the officials for issuing delivery notes is drastically reduced.

Solution

eMudhra's solution for ICICI Bank involved setting up a PKI platform, initially for their existing corporate customer base, with a facility to scale up to include retail, NRI and HNI customers. eMudhra, with its Class 3 DSC crypto token provides 2048 bit security. The data is in an encrypted format through secure socket layer (SSL) connected to the server.

Authentication of the account holder is done by the bank first and verification of the DSC used by the account holder for login and authentication is done by the bank through the authentication system provided by eMudhra. The entire integration and execution exercise requires only minimal changes, thereby allowing the Bank to release value-added services to its corporate customers in a significantly short turnaround time.

Products and Services Used

For enabling the banking system to accept Digital Signature Certificates, eMudhra has provided the following products and services:

emAS (eMudhra Authentication Server)

emAS is typically used for login authentication as well as authenticating electronic transactions before they are considered by the respective core business applications. For example, an online fund request initiated by a bank's customer will first get authenticated in emAS before it gets processed through internet banking or core banking system.

Digital Signature Certificates

eMudhra being a licensed Certifying Authority in India issues legally valid Digital Signature Certificates. The same being accepted by large number of Government departments, corporates and BFSI segments.

About eMudhra:

Much like the name, which is an embodiment of the seal of authenticity in the electronic or digital world, eMudhra is a cyber security solutions company and a trust service provider that is focused on accelerating the world's transition to a secure integrated digital society. With presence in 5 continents and a global delivery center in Bengaluru, India, eMudhra is empowering secure digital transformation of over 45 global banks, several Fortune 100 customers and thousands of SMEs.