emudhra
Trust Delivered

# emCA – eMudhra Certifying Authority Suite

## Issuing and managing digital signatures has never been easier!

As your Enterprise crosses the Digital chasm and adopts Cloud, Mobility, how do you ensure that your digital assets are protected and your customers data is protected. Adopt the power of eMudhra PKI suite of solutions that use digital certificates to create a secure digital identity and transaction management platform!

emCA powers eMudhra's Certifying Authority operations which issue over 12 million end user Certificates yearly (3x global volume of SSL's issued).

eMudhra's solutions are trusted by several large Banks, Government, Financial Institutions globally who use Digital Signatures to put advanced security for their physical, mobile, logical access to applications.

## emCA addresses the need of the hour – mitigating risk for enterprise and it's end users while keeping it simple

**Deploying PKI is Simple**
With customers, employees, suppliers accessing applications across web, desktop, mobile and cloud; Enterprises have to constantly worry about newer threat dimensions. emCA allows for a quick deployment of both On-Premise and Managed PKI to ensure your threats are mitigated.

**Bring all your signing and encryption needs under one roof**
Flexibility of PKI allows for both signing and encryption of data in a media-neutral manner to ensure non-tampering and confidentiality. Complexity is managed by design while ensuring ease of use for end users.

**Username/Passwords are inadequate**
Ensure integrity and legal-non-repudiation using PKI – The basis of legal non-repudiation for online transactions is dependent on integrity, confidentiality and traceability of transactions to a strong identity. The architecture of PKI ensures the above thereby providing legal validity and non-repudiation to online transactions.

emCA

eservices@emudhra.com
**http://www.emudhra.com/products/pki/emca.html**

**Product Benefits**

- On premise / Cloud Deployment as Managed PKI
- Cost effective deployment
- Comprehensive Certificate Lifecycle Management
- Elliptic Key Cryptography Support
- Mobility enabled for leveraging mobile certificate options
- Platform agnostic – deployed across Solaris/Window server/Red Hat Enterprise/Linux/AI
- API's for easy provisioning of Certificates

## Key Features

- Highly Scalable
- Provides keys and certificates for software such as browsers, and Web servers, for tokens, devices, things etc
- Support for Key Archiving and Recovery
- Certificates generated by emCA comply with global
- Digital Signature Certificate Standards - X.509 v3 standards
- Integrating with Leading HSM manufacturers – Thales/Safenet
- M out of N access control mechanism
- Digital signature based authentication for Login Authentication
- OCSP/CRL Module
- Timestamping Module
- RA/CA Module

Whether your Enterprise is deploying a new Certifying Authority or migrating from an existing solution, emCA can seamlessly handle your Certifying Authority operations with a host of features that will help you scale your trusted network as it grows.

## emAS offers a holistic deployment of a trusted PKI network for your Enterprise

**Plug-n-Play** - Quick deployment of both On-Premise / Managed PKI.

**Multiple credentials under one single platform** – A variety of strong authentication options allows users or administrators to ensure easy and seamless multifactor authentication based on risk profiling of users.

**IoT Ready -** eMCA is capable of issuing device certificates and supports relevant protocols.

**Simplified RA Module -** Simplified and intuitive RA dashboard where you can finish any activity in 3 simple steps.

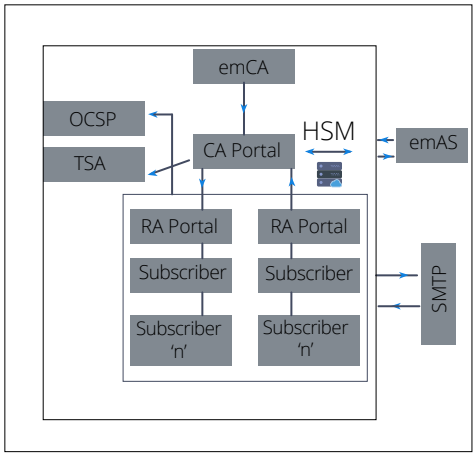
**Integrations with emAS** – Strong Authentication Platform – emAS, eMudhra Authentication Server can be integrated with emCA to ensure validation of digitally signed documents in accordance with key policies.

## emCA powers Identity Management Needs for Secure Digital Transformation

**Device Certificates for even more security** – Deploy device certificates on mobile devices for authentication of devices and signing of data for communication in a network and ensure no intrusion takes place.

**Certificate deployment on embedded devices –** eMudhra's R&D efforts have resulted in the ability to issue/manage digital signature certificates to embedded devices ("Things") and ensure your IoT network is safe and secure.

**Legal Non-Repudiation is driven by need for government licensed/accredited CA's** - emCA powers eMudhra's service which helps people digitally sign documents on the fly using their National ID.



emudhra
Trust Delivered

# DATA SHEET

## Technical Specs

### emCA

emCA is a complete package of Certificate Manager and associated components which is the backbone of Public Key Infrastructure (PKI), a framework for securing enterprise applications. emCA is a robust, standards compliant, fully scalable policy driven certificate manager with support for commercial strength of popular keypair algorithms.

| Components | Hardware specification | Software specification |
|---|---|---|
| eM Certificate manager<br>eM Certificate Controller<br>eM Key Generation system<br>eM Administration Module<br>eM CRL Manager<br>eM OCSP Responder<br>eM Time Stamp Server<br>eM OCSP Client<br>eM TS Client<br>eM Key Archiving Module<br>eM Log/Config Module | 2*Quad Core Processors<br><br>16 GB RAM<br><br>1 TB SAS HDD<br><br>Integrated APP & DB server | Apache/Tomcat<br><br>Oracle: 10g+/SQL<br><br>Windows Server 2012+<br><br>JRE 1.6 or above |

**Key-pair generation-**
Can be done using traditional algorithms as well as elliptical curve algorithms to enable high performance.

**emCA service-**
It's built using Java platform. Comes with desktop utility that supports offline certificate creation where required.

**Algorithms used-**
MD5, SHA-1, SHA-2 Family, MAC, HMAC, RSA Signing, ECDSA, RC2, RC4, RC5, Triple DES EDE, AES

---

### RA/CA Portal

RA/CA portal is web based workflow application that enables organisation seamlessly issuance of digital signatures to end users on approval by RA as well as CA. The application also allows end users to download digital signature on to the crypto token directly.

The CA/RA Portal is meant for processing the digital signature certificate requests put forth by the subscriber.

**Subscriber:**
The end entity who requires digital signature certificate from the Certifying Authority.

**Registration Authority:**
The entity identified by Certifying Authority to validate the subscriber credentials and forward the application to CA for final approval.

**Certifying Authority:**
Enterprise CA/Licensed CA who is given the authority to issue digital signature certificate to the end entity. This can be a private entity using PKI for their own internal purpose

| Components | Hardware specification | Software specification |
|---|---|---|
| eM CA Management System | 2*Quad Core Processors | IIS 7.5 or above |
| eM RA Management System | 8 GB RAM | Windows Server 2012+ |
| eM User Enrollment | 500 GB SAS HDD | JRE 1.6 or above |
| eM Click Certificate Downloader | Webserver | |

## Functional Module includes

**eMudhra Authentication Server -**
To authenticate, verify digital signature certificates on a real time basis.

**Configuration Module -**
Signature, Encryption & HSM

**CRL -**
Ability to publish Certificate Revocation List

**OCSP (Server and Client) -**
Online Certificate Status Protocol to check status of Certificates

**Time Stamping Server -**
Ability to provide a reliable time source for Digital Signatures

**Certificate Lifecycle Management Module -**

Certificate Issuance | Certificate Revocation | Certificate Renewal | Certificate Expiry | Certificate Retrieval

## High Availability & Scalability

emCA solution ensures the security and scalability of e-transactions by providing a flexible, scalable system for managing digital identities. Establishing the trust carried by digital certificates and managing the use of keys and certificates are critical to proper deployment and maintenance of e-business applications. This is done by automating and centralizing the management of cryptographic keys and digital certificates.

emCA is capable of scaling from digital certificate deployment of small enterprises, to managing millions of certificates with a proven ability to issue certificates at very high rates.

## 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 using advanced encryption standards that are global (AES 256).

## Compliance with PKI Standards

emCA complies with established PKI standards for certificates, revocation lists, smart cards and certificate management interfaces.

Supports FIPS- 140-2 Level 3 certified HSM and Crypto tokens of various vendors. Also supports smartcards and server-side signing scenarios.

| Component | OEM |
|---|---|
| HSM | ➢ Safenet<br>➢ Thales |
| Crypto Token | ➢ Safenet<br>➢ Watchdata<br>➢ G&D<br>➢ Feitian |

## Applicable Industries

Enterprises, State Departments, Defence, and other Public/Private sectors.

## Benefits

- Scalable application
- Provides keys and certificates for software such as browsers, and Web servers, for tokens, etc
- Support for key archiving and recovery
- Certificates generated by emCA comply with the X.509 v3 standards.
- HSM provides highest security to the private keys which is required for digital signatures
- Offers high levels of interoperability to benefit customers leverage existing investments
- M out of N access control mechanisms incorporated
- Digital signature based authentication is applied for login access

emCA benefits the enterprise in issuance and management of digital signature certificates as per the global standards

emCA manages the entire life cycle of digital signature certificates.

The digital certificate issued to the user using emCA conforms to following:

- Confidentiality
- Authentication
- Data Integrity
- Non-Repudiation

**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 issues over 15 million digital signature certificates yearly, serves over 10 million customers who use eMudhra's authentication platforms and has partnered with over 100 large Enterprises such as Banks, Financial Services companies and several Government agencies in India to implement digital security and analytics solutions.