emudhra
Trust Delivered

emCA

emCA: End-to-end PKI Management Suite

fido ALLIANCE MEMBER

CAB CA/BROWSER FORUM

Webtrust Accredited

AATL

CLOUD SIGNATURE CONSORTIUM

Asia PKI Consortium

Today, companies are deploying billions of Internet-connected devices into mission-critical systems. Such kind of mass deployments are resulting in security risks with implications that grow with the number of deployed devices.

PKI is the leading choice for providing information and communication security in such a challenging environment. Hence why not make PKI a part of your IT infrastructure by utilizing emCA — eMudhra's PKI powered digital certificate issuance and management solution. Built exclusively to provide trust and control, emCA is a robust, standards compliant, fully scalable, policy driven PKI solution designed to provide unparalleled security services, which include authentication of user and device, data security, integrity and verification.

12+ Years as a Public Certifying Authority

eMudhra has been a Public Certifying Authority under the Indian root for more than 12 years. The company is also a CA under the Mauritian root and a certified Cross Certification Service Provider under the UAE root. In addition, we are powering local TSPs across the globe through our globally accredited emSign root. That's a lot of audits, documentation, and compliance, which we manage on a regular basis.

A Pioneer, Not a Follower

We take pride in being a thought leader in our space. From National ID based one-time-use eSign, to Cloud PKI for mobility, we are constantly thinking what's next. We ensure that we focus equally on convenience of PKI as we do on security to ensure quick adoption and effective Digital Transformation

50 million trusted public signatures issued, WebTrust accredited, EAL 4+ CC compliant, ISO/CMMI certified. Experience you can trust.

End-to-end Consulting

PKI is our bread and butter. Having done it every day for 12+ years at a retail level and a B2B level, we're quite aware of how it works, what the typical issues are, and how best the processes can be streamlined. Leveraging the same expertise and experience, we offer end-to-end consulting services—from deploying PKI infrastructure to enabling successful WebTrust audits, planning Data Centers, determining levels of Assurance and sometimes, even working closely with you to create bespoke scenarios and implementing custom built solutions.

Superior Product Capability

emCA has been built keeping in mind our needs as a public CA, and our learning from venturing out into the Enterprise, IoT, and Blockchain world. As a result, our CA system is robust, scalable, and works in IoT, Blockchain, and network security ecosystems quite effectively in addition to conventional use cases.

Support for a Wide Variety of Use Cases

Out of the box emCA supports issuance of Digital Signature Certificates to user, server, network device, mobile phone, TPM (Trusted Platform Module), Trusted Execution Environment (Strong Box), IoT device, etc.

Other Key Highlights

- Ability to issue certificates to smart devices in IoT ecosystem
- Support for Mobile PKI – Secure generation of key-pair, certificate attestation, signing, encryption/decryption
- Cross-certification to establish trust relationships between multiple CAs
- Encryption of sensitive data using AES key that can be securely stored on HSM
- Tool to detect modification of Certificate Manager Binaries
- Provision to define automatic and manual backup of entire application within the application
- Provision to restore application through backup files done using application itself
- Comprehensive enrolment system to manage approval of certificate requests including video verification, token inventory management, etc.

Benefits

- Cost effective solution
- Faster deployment
- Better management of RA's
- Superior support
- Easy migration
- Ability to provide managed services
- Used in Webtrust compliant deployments

Key Projects

- Aadhaar eSign - eMudhra developed and deployed at scale national ID based signing
- emCA is used extensively in the world's second largest armed forces
- Mauritius Root PKI - eMudhra set up the Root PKI and issuing CA for Mauritius
- eMudhra Public CA - eMudhra's Public CA runs on emCA Suite and supports a 13,000 large re-seller network
- World's largest outsourcing company used emCA for signing and management of Employment Eligibility (I-9) Forms in the US
- emCA is used to issue Digital Signature Certificates to electronic voting machines
- emCA supported IoT deployment for a large diesel generator manufacturing company
- emCA Certificate Manager & OCSP is used by a large digital payment and transactional solutions provider with operations across the globe for provisioning of IoT certificates for smart meters embedded at source to power several large scale requirements
- eMudhra assisted a reputed telecommunications company in the APAC region for setting up Public In-country TSP and issuing digital certificates at scale

Technical Details

- **Minimum Hardware**
  Processor: Quad core Processors
  RAM: 16 GB
  HDD: 1 TB SAS HDD
  (Integrated App & DB Server)
- **Recommended hardware**
  Processor: 2 * Quad core Processors
  RAM: 32 GB
  HDD: 1 TB SAS HDD
  (Integrated App & DB Server)
- **OS Compatibility**
  Windows Server 2008+ Enterprise, RHEL 5+, AIX 7+, Suse 12+ and Solaris 10+
- **Application Server**
  Apache Tomcat 7+, JBoss 7+, Web Sphere 8+, Web Logic 12+
- **DB Compatibility**
  Oracle 10g+, SQL Server 2008+, MySQL 5+, DB2 9+, Postgre 9+
- **Algorithms & Standards**
  MAC, HMAC, Triple DES, AES 256
  X.509 v3, PKIX, XAdES, PAdES, CRL v2
- **Java**
  Oracle JDK 1.8+
- **Protocols**
  SCEP, CMP, OWASP, HTTP, HTTPS, SMTP, FTP, WSS, LDAP
- **RFC's**
  RFC 6960, RFC 6962, RFC 5273, RFC 4210, RFC 3161, RFC 4998 ERS, RFC 4810
- **Web Services**
  SOAP, REST
- **Signature Algorithms**
  SHA1WithRSA
  SHA256WithRSA
  SHA384WithRSA
  SHA512WithRSA
  SHA1WithECDSA
  SHA256WithECDSA
  SHA384WithECDSA
  SHA512WithECDSA
- **Key Algorithms**
  DSA-1024
  RSA-1024
  RSA-2048
  RSA-3072
  RSA-4096
  RSA-8192
  ECDSA secp-192
  ECDSA secp-256
  ECDSA secp-384
  ECDSA secp-521
  ECDSA brainpoolP256r1
  ECDSA brainpoolP384r1
  ECDSA brainpoolP521r1
  prime192v1
  prime256v1
- **Security Compliance**
  EAL 4+ Common Criteria Compliant
  WebTrust Compliant
- **Management and Monitoring**
  Uses m out of n authentication
  Support segregation of duties
  Secure Audit Logging
- **Support for HSM**
  Thales
  Safenet
  Cavium
  Ultimaco

Key Modules

- Certificate Lifecycle Management
- Online Certificate Status Protocol Responder
- Timestamping Authority
- Validation Server
- API Gateway
- Web Socket
- CRL Manager
- Key Archival
- Tamper Proof Logging
- emClick Certificate Download App
- Auto Enrollment
- Subscriber Portal
- Inventory Management Portal
- Registration Management Portal
- Certifying Authority Portal
- OSCP and Timestamping Client
- Mail Notification for Certificate Expiry
- Certificate Template Creation
- Certificate, Keys & CRL Templates Management

About eMudhra:

As the world goes Digital, security is ever more crucial to protect identities, data, and enable trust in a digital society. eMudhra focuses on SECURE Digital Transformation to enable organizations to progress and evolve without sacrificing “Trust,” which matters most in our society. With an end-to-end stack around trust services, PKI, Paperless transformation, and Digital Authentication, eMudhra is optimally placed to aid digital journeys where identity assertion is critical.

eMudhra chairs the Asia PKI Consortium, is a board member of the Cloud Signature Consortium and a member of the CA Browser Forum. Having been in business for over 12 years and built a reach that spans more than 50 countries, eMudhra is deeply committed to bringing change and helping societies across not just go digital but go digital in a secure way.

Email: eservices@emudhra.com
Web: www.emudhra.com