STUDY NOTES · BASIC CONCEPT

What is eMudhra? What is a Digital certificate? What Is Public Key Infrastructure (PKI)?

Defence & Security

23 Oct 2026

What does eMudhra do?

eMudhra is an Indian digital trust and cybersecurity company that provides services related to digital signatures, digital identity, electronic authentication and website security.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT

eMudhra emSigner Pricing 2026

eMudhra is an Indian digital-security company that provides digital signature services and digital certificates.

Its services help individuals, businesses and organisations authenticate identities, sign documents electronically and secure digital communications.

Service	Purpose
Digital Signature Certificates (DSCs)	Authenticate electronic documents and support legally recognised digital signing
eSign services	Enable electronic signing of documents through supported digital authentication processes
SSL/TLS certificates	Help authenticate websites and secure connections using HTTPS

Service	Purpose
Public Key Infrastructure (PKI)	Establish trust between digital identities and cryptographic keys
Identity and access management	Help organisations manage and verify users' access to digital systems

Why is eMudhra important?

eMudhra operates in the digital trust ecosystem. This ecosystem enables people and organisations to trust the identity of websites, users and electronic documents.

For example, when you visit a website using HTTPS, a TLS certificate helps your browser verify the website's identity and establish a secure connection.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT

What is its connection with the cybersecurity incident?

The incident discussed in the news concerned weaknesses in certain intermediate certificate authorities associated with eMudhra's international website-security business. Such weaknesses can potentially undermine trust in website certificates.

In October 2026, eight intermediate Certificate Authority (CA) certificates associated with eMudhra’s international website-security business were reported to have weak cryptographic private keys due to insufficient randomness during key generation.

Potential risks included fraudulent certificate issuance, website impersonation and man-in-the-middle attacks. However, no confirmed malicious exploitation or data breach was established. The company and authorities stated that India’s regulated Digital Signature Certificate (DSC) and eSign services remained unaffected.

What Is Public Key Infrastructure (PKI)?

Public Key Infrastructure (PKI) is a framework of technologies, rules and institutions used to establish trust in digital identities and electronic communications.

PKI uses two cryptographic keys:

1. Public key: Shared openly and used for verification or encryption, depending on the protocol.
2. Private key: Kept secret and used for digital signing or decryption, depending on the cryptographic system.
3. A digital certificate links an identity or website domain with a public key. A trusted Certificate Authority digitally signs the certificate to establish this association.
4. The certificate chain generally consists of:
5. Root Certificate Authority → Intermediate Certificate Authority → Website or Software Certificate → Verification by Browser or Operating System.
6. If an intermediate CA's private key is compromised, an attacker may be able to issue fraudulent certificates within its permitted scope.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT

What Is a Digital Certificate?

A digital certificate is an electronic credential that establishes a verifiable association between an identity and a public key.

Major types include:

1. TLS Certificate: Authenticates websites and enables secure HTTPS connections.
2. Digital Signature Certificate (DSC): Supports electronic signing and identity verification.
3. Code-Signing Certificate: Helps verify software publishers and software integrity.
4. Intermediate CA Certificate: Authorises a subordinate authority to issue certificates.
5. Root CA Certificate: Acts as a trust anchor in a browser or operating system's trust store.

These certificates serve different purposes. A problem affecting international website-security certificates does not automatically mean that all digital-signature products or government services provided by the same company are compromised.

Why Is Cryptographic Randomness Important?

Cryptographic systems depend on keys that are extremely difficult to predict or recover.

Private keys must be generated using secure cryptographic random-number generation methods. If a key is weak or predictable, an attacker may recover it and misuse the authority’s signing power.

The eMudhra incident highlighted a key-generation weakness. It did not, by itself, establish that the underlying cryptographic algorithm was broken.

What Is a Man-in-the-Middle Attack?

A man-in-the-middle (MitM) attack occurs when an attacker positions themselves between two communicating parties and attempts to intercept or alter their communication without their knowledge.

A fraudulent certificate may help an attacker impersonate a legitimate website. If the attacker can also defeat or bypass the relevant security checks, sensitive information such as login credentials may be exposed.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT

However, a weak certificate key does not automatically mean that encrypted traffic has been intercepted. Actual exploitation depends on the circumstances and the effectiveness of security controls.

Role of Important Cybersecurity Institutions

1. CERT-In: India's national agency for responding to cybersecurity incidents. It issues alerts, advisories and mitigation guidance.
2. Controller of Certifying Authorities (CCA): Regulates licensed Certifying Authorities under India's Information Technology Act framework.
3. Ministry of Electronics and Information Technology (MeitY): Formulates and implements policies concerning electronics, information technology and related digital infrastructure.
4. Browser and Operating-System Providers: Maintain trust stores and deploy protections against untrusted or revoked certificates.

5. Independent Auditors: Examine security controls and compliance with applicable standards.
6. Regulatory oversight of domestic DSC services must be distinguished from the management of international browser-trusted TLS certificates.

Why Are Security Audits Important?

Security audits examine whether organisations follow appropriate policies, technical controls and operational procedures.

They may identify weaknesses in cryptographic key management, access controls, software implementation and incident response.

However, an audit cannot guarantee absolute security. Its effectiveness depends on its scope, methodology, frequency, independence and ability to detect implementation errors.

The eMudhra incident raises questions about whether existing controls adequately detected the weak keys. Such questions require investigation rather than an assumption that all audits or regulators failed.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT

Measures to Strengthen India's Digital Trust Ecosystem

1. Secure Key Generation: Use validated cryptographic random-number generation and appropriate secure hardware.
2. Independent Audits: Conduct risk-based audits and verify the actual implementation of security controls.
3. Certificate Management: Maintain certificate inventories, revoke compromised certificates quickly and replace affected certificates.
4. Continuous Monitoring: Conduct regular vulnerability assessments and monitor suspicious certificate issuance.
5. Incident Response: Strengthen coordination among CERT-In, regulators, technology providers and affected organisations.
6. Transparency and Accountability: Require timely incident reporting, root-cause analysis and corrective action.
7. System Resilience: Identify legacy systems that cannot receive timely security updates and establish appropriate mitigation plans.

8. User Awareness: Educate users about certificate warnings and discourage bypassing browser security checks.

UPSC Examination Relevance

1. PKI establishes trust in digital identities and communications.
2. A private key must remain secret and be generated securely.
3. Certificate Authorities issue digital certificates within a trust hierarchy.
4. Encryption primarily provides confidentiality.
5. Digital signatures support authenticity and integrity.
6. CERT-In responds to cybersecurity incidents.
7. CCA regulates licensed Certifying Authorities under the applicable Indian framework.

BECOME IAS
AI-Powered UPSC Preparation by ZINKPOT