

GENERAL STUDIES III

eMudhra Certificates UPSC 2026: Complete Notes

Faculty/Author: Faculty Editorial Board**Date:** 22 October 2026**Platform:** Civil Service Gurukul Research Wing**Reading Time:** 5 Mins

In October 2026, Google, Mozilla and other major technology providers responded to a critical cryptographic weakness affecting eight intermediate certification authority certificates associated with eMudhra's global web trust services. The problem originated in a April 2025 key-generation process and highlighted vulnerabilities in Public Key Infrastructure (PKI), digital certificates and browser trust. These original Civil Service Gurukul notes explain asymmetric encryption, certificate authorities, HTTPS/TLS, the trust chain, CERT-In's response, India's digital signature framework, cybersecurity governance, UPSC Prelims MCQ and a GS Paper 3 Mains model answer.

CIVIL SERVICE GURUKUL | PRELIMS IN FOCUS

Understand why major browsers blocked eMudhra certificates, how digital certificates establish website trust, the role of

8

Affected intermediate CA certificates

17 Oct

Vulnerability disclosure in 2026

PKI

Public Key Infrastructure

CERT-In

Indian cybersecurity response agency

1. Why Are eMudhra Digital Certificates in the News?

Modern internet services rely on an invisible but essential infrastructure of cryptographic keys and digital certificates.

Whenever users access an HTTPS-enabled website, their browser must determine whether the server presenting the certificate can be trusted.

In October 2026, a serious cryptographic weakness was identified in eight intermediate Certification Authority certificates associated with eMudhra's global digital certificate operations.

The affected private keys were generated with insufficient randomness during an April 2025 key-generation process.

This made the keys susceptible to reconstruction, potentially allowing attackers to issue fraudulent certificates that appeared to come from a trusted authority.

Google and Mozilla acted rapidly to prevent their browsers from trusting the affected certificate keys.

India's Computer Emergency Response Team also issued a cybersecurity advisory on 21 October 2026.

UPSC significance: The incident provides a practical case study for understanding asymmetric cryptography, PKI, digital trust, certificate authorities, cybersecurity regulation and critical digital infrastructure.

2. UPSC Syllabus Mapping

Paper	Relevant area
Prelims GS I	Science and technology developments, cybersecurity and current affairs
GS Paper III	Developments in information, technology and cyber security
GS Paper III	Challenges to internal security through communication networks
GS Paper II	Regulatory governance and responsibilities of public institutions
GS Paper IV	Accountability, institutional trust and responsible disclosure

Contents of This UPSC Guide

1. What are digital certificates?
2. Public Key Infrastructure
3. Asymmetric cryptography
4. The eMudhra incident explained
5. Timeline of events
6. Potential cybersecurity risks
7. Browser and CERT-In responses
8. India's digital trust regulations
9. SSL, TLS, signatures and hashing
10. Governance lessons and way forward
11. UPSC Prelims questions

12. UPSC Mains model answer

13. Frequently asked questions

3. What Is a Digital Certificate?

A digital certificate is an electronic credential used to associate a public key with an identified entity, such as a website or software publisher.

It is normally issued and digitally signed by a trusted Certification Authority, commonly abbreviated as CA.

Important information in a certificate

- The entity or subject identified by the certificate.
- The public key associated with that entity.
- The certificate issuer.
- The validity period.
- The digital signature of the issuing authority.
- Permitted certificate uses and technical extensions.

Example: Visiting an HTTPS website

Suppose a user opens a banking website. The browser receives a certificate associated with the website's domain.

The browser then checks whether the certificate is valid, matches the website address and links to a trusted authority.

A successful validation helps establish an authenticated encrypted connection.

Prelims trap: An HTTPS padlock indicates an authenticated, encrypted connection to the named site. It does not guarantee that the website's content is truthful, safe or free from fraud.

4. What Is Public Key Infrastructure (PKI)?

Public Key Infrastructure is a framework of technologies, institutions, rules and procedures that supports digital certificate issuance, validation and revocation.

The chain of trust

Root Certification Authority

?

Intermediate Certification Authority



Website or End-Entity Certificate

Root Certification Authority

A root CA is a high-trust authority whose certificate may be included in a browser or operating system's trusted root store.

Intermediate Certification Authority

An intermediate CA is authorised through a certificate chain and may issue other certificates, subject to relevant technical constraints.

End-Entity Certificate

An end-entity certificate is used by a particular website, service or software publisher rather than to issue further CA certificates.

Why intermediate authorities matter

If an intermediate CA's private key is compromised, an attacker may be able to create certificates appearing to be issued by that CA.

The practical consequences depend on trust status, certificate constraints and security checks.

Exam memory trick: Root CA ? Intermediate CA ? End-Entity Certificate. Trust is checked through a cryptographically verified certificate chain.

5. Asymmetric Cryptography and Cryptographic Entropy

Asymmetric cryptography uses two mathematically related keys: a public key and a private key.

Public key	Private key
May be distributed openly.	Must be protected against unauthorised access.
Can verify signatures created by the associated private key.	Can create digital signatures.
Can support certain encryption or key-establishment operations.	Can support corresponding decryption or key-establishment operations.

What is cryptographic entropy?

Entropy, in the context of cryptographic key generation, refers to the unpredictability or randomness available to the key-generation process.

A key generated with insufficient unpredictability may be vulnerable to guessing or mathematical recovery.

Such weaknesses can undermine the security of even well-established cryptographic algorithms.

Why key length alone is insufficient

A system may use a recognised cryptographic algorithm while still producing vulnerable keys if implementation or randomness generation fails.

Therefore, cryptographic security requires correct algorithms, secure implementations, proper key handling and reliable operational controls.

6. eMudhra Certificate Incident: What Went Wrong?

The reported weakness affected eight intermediate CA certificates associated with eMudhra's global web trust infrastructure.

Six were intended for website authentication functions, while two were associated with code signing.

According to the public disclosures, a problem arose during a key-generation ceremony on 30 April 2025.

Weak keys were generated and associated with the affected intermediate CA certificates.

The weakness allowed recovery of private keys that should have remained secret.

Why is this serious?

Intermediate CA keys occupy a highly trusted position in certificate issuance.

If their private keys can be reconstructed, an unauthorised person could potentially create certificates that appear to come from a legitimate issuing authority.

Important clarification: A discovered cryptographic weakness is not, by itself, proof that users' personal information was stolen. eMudhra stated that there was no infrastructure intrusion or data breach identified.

7. Timeline of the October 2026 Incident

Date	Development
30 April 2025	Key-generation ceremony later identified as the origin of the weak keys.
17 October 2026	Security researchers reported the affected intermediate CA certificates to browser trust operators.
17 October 2026	Chrome and Firefox implemented rapid blocking protections.
20 October 2026	Public disclosures explained the certificate weakness and emergency response.
21 October 2026	CERT-In issued an advisory, and eMudhra published an additional public statement.
22 October 2026	The incident became a significant Indian cybersecurity current-affairs topic.

The incident demonstrates that weaknesses introduced during certificate generation may remain undiscovered until independent testing or research exposes them.

8. Cybersecurity Risks Associated with Compromised CA Keys

Website impersonation

Fraudulent certificates could potentially be used to make an attacker-controlled service appear associated with a legitimate domain.

Man-in-the-middle attacks

An attacker positioned to intercept network traffic might attempt to impersonate a trusted endpoint using forged certificates.

Malicious software signing

Compromised code-signing CA keys could potentially let malicious software appear to have a legitimate publisher signature.

Loss of public trust

Certificate incidents can undermine confidence in security infrastructure, even when there is no confirmed successful attack on end users.

Important distinction: A potential attack capability does not establish that the attack was actually carried out.

9. How Did Google, Mozilla and CERT-In Respond?

Google Chrome

Google used its CRLSet-based blocking mechanism to distrust keys associated with the affected intermediate certificates.

The emergency protection was designed to reach users without requiring a browser restart.

Mozilla Firefox

Mozilla used OneCRL, its centralised certificate revocation mechanism, to block affected certificates.

Further measures addressed related root-trust concerns across software that relies on Mozilla's trust store.

CERT-In

The Indian Computer Emergency Response Team issued guidance on the compromise of eMudhra intermediate CA certificates.

Relevant advice included updating browsers and operating systems, checking affected certificate chains and strengthening cryptographic key management.

Good security practices

- Keep browsers and operating systems updated.
- Do not bypass invalid-certificate warnings.
- Replace certificates relying on distrusted chains.
- Maintain current trusted root stores.
- Monitor Certificate Transparency records.
- Use secure and auditable key-generation procedures.
- Maintain effective incident-response processes.

10. India's Digital Signature and Cybersecurity Framework

Information Technology Act, 2000

The Information Technology Act, 2000 provides a framework for legally recognised electronic records, electronic signatures and specified cyber-related matters.

Controller of Certifying Authorities

The Controller of Certifying Authorities, or CCA, regulates licensed Certifying Authorities issuing Digital Signature Certificates in India.

It operates within the legal framework established under the Information Technology Act.

CERT-In

CERT-In is India's national agency for specified cybersecurity incident response functions, including advisories and security coordination.

It operates under the Ministry of Electronics and Information Technology.

Why the distinction matters

eMudhra operates different kinds of trust services.

The October incident concerned its international web-certificate infrastructure, not the separate Indian DSC and eSign services regulated by CCA.

Critical UPSC fact: CCA and CERT-In are different institutions with different functions. CCA regulates specified electronic signature certification services; CERT-In coordinates designated cybersecurity incident-response activities.

11. Important Technical Terms for UPSC

Term	Meaning
HTTPS	HTTP communication protected using TLS.
TLS	Protocol supporting authenticated and encrypted network communications.
SSL	Older predecessor to TLS; the term remains common in casual usage.
Digital signature	Cryptographic mechanism for verifying origin and integrity under specified conditions.
Hash function	Transforms input data into a fixed-length digest; secure hashes are designed to resist collisions and inversion.
Root CA	High-trust certificate authority represented in trust stores.
Intermediate CA	Authority authorised through a certificate chain to issue specified certificates.
Certificate revocation	Withdrawal of a certificate's validity or trust before normal expiry.
Code signing	Use of digital signatures to authenticate software publisher identity and help detect tampering.
Certificate Transparency	Public logging system designed to improve visibility of certificate issuance.

Encryption versus digital signature

Encryption primarily protects confidentiality by restricting who can read information.

A digital signature supports authenticity and integrity by allowing verification that data was signed using the corresponding private key.

They are related cryptographic applications, but they do not perform identical functions.

12. Governance Lessons and the Way Forward

Secure key-generation processes

Certification Authorities should implement independently reviewed key-generation procedures with robust randomness and documented operational controls.

Independent security audits

Audit programmes should test technical controls and key-management processes rather than relying only on documentation.

Rapid trust withdrawal

Browser operators need mechanisms to block compromised certificate keys quickly and reliably.

Responsible disclosure

Researchers, certificate issuers and browser vendors should coordinate to protect users without unnecessary delay.

Clear public communication

Authorities should distinguish verified technical vulnerabilities from unconfirmed claims of data theft or service compromise.

Institutional coordination

Global trust-store operators and national cybersecurity authorities should cooperate during major digital trust incidents.

13. UPSC Prelims Practice MCQs**Question 1**

A digital certificate primarily associates:

- (a) A public key with an identified entity
- (b) A private password with a physical address
- (c) A biometric record with a tax return
- (d) A computer's IP address with its electricity consumption

Correct answer: (a).

Digital certificates help establish authenticated associations between public keys and identified entities.

Question 2

With reference to Public Key Infrastructure, consider the statements:

1. A root CA may provide a trust anchor for validating certificate chains.

2. An intermediate CA may issue end-entity certificates.
3. A compromised intermediate CA private key can create certificate-forgery risks.

Select the correct answer:

- (a) 1 only
- (b) 1 and 2 only
- (c) 2 and 3 only
- (d) 1, 2 and 3

Correct answer: (d).

All three statements accurately describe the PKI trust hierarchy and associated security risks.

Question 3

The October 2026 eMudhra certificate incident primarily involved:

- (a) A shortage of cloud server storage
- (b) Weak cryptographic private keys
- (c) A nationwide UPI server shutdown
- (d) Satellite navigation interference

Correct answer: (b).

The weakness arose from insufficient randomness in the generation of certain intermediate CA keys.

Question 4

Which organisation regulates licensed Digital Signature Certificate authorities in India?

- (a) Election Commission of India
- (b) Controller of Certifying Authorities
- (c) Securities and Exchange Board of India
- (d) National Payments Corporation of India

Correct answer: (b).

CCA operates under India's Information Technology Act framework.

Question 5

Which statement best distinguishes encryption from a digital signature?

- (a) Encryption supports confidentiality, while digital signatures support authenticity and integrity.
- (b) Digital signatures are used only for storing passwords.
- (c) Encryption necessarily proves the physical identity of a sender.
- (d) Digital signatures eliminate the need for any cryptographic keys.

Correct answer: (a).

Their security objectives differ, even though both use cryptographic techniques.

Question 6

With reference to the October 2026 eMudhra incident, consider the statements:

1. Eight intermediate CA certificates were affected.
2. The problem related to the company's international web trust services.
3. The incident established that India's entire digital signature infrastructure had been compromised.

Which statements are correct?

- (a) 1 only
- (b) 1 and 2 only
- (c) 2 and 3 only
- (d) 1, 2 and 3

Correct answer: (b).

The separate Indian DSC and eSign operations were reported as unaffected.

14. UPSC Mains Practice Question and Model Answer

GS Paper 3 | 15 Marks | 250 Words

"Public Key Infrastructure is essential for trusted digital governance, but failures in cryptographic key management can create systemic cybersecurity risks." Explain with reference to the eMudhra certificate incident of 2026.

Model Answer

Public Key Infrastructure is a framework of digital certificates, cryptographic keys, trusted authorities and verification procedures that supports secure electronic communication. It is central to online banking, e-governance and authenticated internet services.

Incident: In October 2026, eight intermediate CA certificates associated with eMudhra's international web trust services were found to have weak private keys. The weakness originated in a 2025 key-generation process.

Risks: Compromised certificate authority keys could potentially enable forged website certificates, website impersonation and malicious software signing. Such weaknesses could undermine trust across multiple applications.

Institutional response: Google and Mozilla rapidly blocked affected certificate keys, while CERT-In issued a cybersecurity advisory. The response demonstrated the importance of international coordination.

Way forward: Certification Authorities need robust key-generation practices, independent security testing, effective audits, rapid revocation mechanisms and transparent incident reporting. Governments should support institutional capacity and public awareness.

Conclusion: Digital public trust depends not merely on strong cryptographic algorithms but also on secure implementation, regulatory oversight and responsive governance.

15. Frequently Asked Questions

What happened to eMudhra certificates in October 2026?

Eight intermediate CA certificates were found to have weak private keys, leading major browsers to block affected trust chains.

What is PKI?

Public Key Infrastructure is a framework for issuing, managing and validating digital certificates and cryptographic identities.

What is an intermediate Certification Authority?

It is a certificate authority authorised through a trust chain to issue specified certificates.

What caused the eMudhra vulnerability?

Insufficient cryptographic randomness during a key-generation process in April 2025.

What is HTTPS?

HTTPS is HTTP protected by Transport Layer Security, providing encrypted and authenticated communication.

What is CERT-In?

The Indian Computer Emergency Response Team is a national cybersecurity incident-response agency under MeitY.

Were Indian DSC and eSign services affected?

CERT-In and eMudhra stated that the separate Indian DSC and eSign operations were not affected.

Was a data breach confirmed?

The public disclosures did not establish that the weak keys had been used to steal users' information.

16. Conclusion: Digital Trust Depends on Secure Implementation

The eMudhra certificate incident of October 2026 demonstrates how a weakness in cryptographic key generation can threaten internet trust infrastructure.

It also shows the importance of rapid response by browser vendors, cybersecurity authorities and certificate issuers.

For India, the episode reinforces the need for resilient digital infrastructure, strong technical standards and institutional accountability.

For UPSC aspirants, the central lesson is that cybersecurity is both a technological issue and a governance challenge.

Civil Service Gurukul

Prepare with original current affairs notes, concept explanations, Prelims MCQs, Mains model answers and syllabus-linked learning resources.

[Visit Civil Service Gurukul](#)[Contact Civil Service Gurukul](#)

Website: www.civilservicegurukul.com

Mobile: +91 9911020626

Email: info@civilservicegurukul.com

Educational disclaimer: This original UPSC article was prepared on 22 October 2026. Cybersecurity investigations may evolve as new technical evidence emerges. The discussion distinguishes verified vulnerabilities from hypothetical attacks and does not claim that a confirmed user-data breach occurred.

CIVIL SERVICE GURUKUL

UPSC Prelims | UPSC Mains | Cybersecurity | Science & Technology

CIVIL SERVICE GURUKUL

UPSC Preparation • Current Affairs • Mentorship • Test Series

Website: www.civilservicegurukul.com • Email: info@civilservicegurukul.com • Mobile: +91 9911020626