STATEMENT

eMudhra Statement on Recent Certificate Security Incident

Investigation ongoing Last updated: **30 October 2026**

First published: 20 October 2026

Updates are listed newest first.

Update 7 30 October 2026 LATEST

eMudhra Limited today announced the appointment of KPMG as its independent external reviewer following the incident that led to the distrust of select global TLS intermediate certificate authorities earlier this month. The appointment fulfills the commitment the company made in its press release of October 21, when it said an independent entity would examine the matter. KPMG is among the leading global networks of professional services firms.

The company said the review is intended to bring clarity on the incident and to help it address any issues arising from it, in keeping with its approach to governance and compliance.

Update 6 28 October 2026

Progress on Customer Transition from eMudhra TLS Certificates

This update follows Update 5 and gives more detail on where the customer transition stands.

Affected G3 certificates and the alternate G1 pathway

The roughly 30,800 certificates issued under the affected G3 hierarchies belong to a client ecosystem in the United States. We had already given this ecosystem an alternate issuance pathway through eMudhra's G1 RSA root, and they are now using that pathway.

Orderly transition out of the G1 TLS Roots

We have asked the browser and root-store programs for time so that the impacted client ecosystem in US can move over in an orderly way without disrupting its member institutions. We are in advanced discussions with leading SSL/TLS providers to support the move. We will keep working with our Client, these providers and the root programs until the transition is complete.

Voluntary wind-down of G1 issuance

G1 issuance is being used only to support this transition. As part of our voluntary wind-down of publicly trusted TLS services, eMudhra will stop issuing TLS certificates from G1 once the federation's transition is complete. A vast majority of our remaining TLS customers have already been transitioned to alternate TLS providers and we intend to complete this activity in the coming days.

Free migration to alternate providers for unaffected TLS customers

eMudhra immediately provided (and continues to provide) alternate options at no charges to all TLS customers who were using eMudhra TLS certificates without any additional

charges. We have already moved these customers to alternate providers at no cost to them, and our teams remain dedicated to support them through the switch.

Global eSignature (DSC, eSignature, eSign), and Enterprise Solutions business unaffected

None of eMudhra's Global Digital Signature Certificate (DSC) or eSign business is affected by this incident. They continue to run normally throughout and remain unaffected. Neither is there any impact to our enterprise solutions (emSigner, CertiNext, SecurePass, Privatrust). Where applicable, SaaS solutions provided by eMudhra also remain unaffected.

Continued investment in PKI and Identity

Discontinuing sale of publicly trusted TLS certificates does not change our long-term commitment to PKI and Digital Identity. eMudhra will keep investing in research and development across its eSignature, Identity, Privacy and PKI businesses, and will continue to expand the range of its offerings and its reach in several markets, including North America.

We remain committed to transparency, responsible remediation and continued cooperation with the global WebPKI community. We thank our customers, partners, and root store programs for their understanding as we work our way through this transition. Further updates will be published on this page as material developments occur.

A Note from eMudhra Leadership 26 October 2026

Last week, a security researcher reported that the private keys associated with eight of our emSign G3 intermediate TLS CAs were recoverable. They were right.

The flaw was ours. A script error resulted in issuing CA's with weak keys.

We want to apologise directly to our customers and to the broader WebPKI community, both of whom were entitled to expect better from us. Also to our partners, who have had to field questions that are ours to answer.

The affected intermediate CAs were revoked within 14 hours of our confirming the issue. Based on our investigation to date, the affected intermediates had not issued publicly trusted end-entity certificates, and there has been no compromise of our infrastructure or customer data.

Our digital-signature & eSign/eSignature in India, and Globally, along with all of our enterprise applications operate on separate infrastructure and were not impacted in any manner. We are already in the process of moving our impacted G3 customers and our broader non-impacted TLS customers to alternate certificates at no cost.

We will publish a full root-cause analysis through the CCADB process. It will explain what went wrong, why our controls failed to detect it, and the changes we are making as a result.

We are also commissioning an independent expert to review the incident and the procedures and controls followed by us. Nothing is more important in our business than the trust placed in us by our customers and the broader digital-trust ecosystem.

We will do all that is necessary to maintain that trust and confidence through our actions in the coming weeks.

eMudhra Leadership Team

Update 4 22 October 2026

Availability of Sectigo Certificates as an Alternate Option

eMudhra is making certificates issued by Sectigo available as an alternate option to all of our customers.

Our G1 root certificates remain active and continue to be fully supported. Despite this, we are offering Sectigo-issued certificates to give customers additional peace of mind and flexibility in managing their certificate deployments.

How to request a Sectigo certificate

- **Existing CertiNext users:** Submit your request directly through your CertiNext account.
- **All other customers:** Contact eMudhra Support at support@emudhra.com.
- **Customers in the USA:** Contact support@certinext.io.

Our support team will guide you through the process and help ensure a smooth experience for your environment.

We remain committed to the security, reliability, and continuity of the services our customers depend on.

Update 3 21 October 2026

An Update on Our Global TLS Intermediate CA Incident

What happened, who is affected, and what we are doing about it

On October 17, 2026, an independent security researcher reported that the keys of eight (out of several) eMudhra Global TLS intermediate Certificate Authorities (CAs) were cryptographically weak. We revoked all eight intermediates the following day. No certificates had been issued from any of them, our infrastructure was not compromised, and no data was breached.

We take this incident seriously. We believe an organization's character is shown in how it responds when something goes wrong, so this post sets out plainly what happened, who is affected, and what we are doing about it.

What happened

Eight intermediate (issuing) CAs in our Global TLS business were revoked because their published keys were weak. These intermediates sit under eMudhra's ECC root. As a consequence of the incident, the browser root programs have also distrusted that one ECC root.

To be clear about what was and was not affected:

- **Intermediate keys were revoked, not root keys.** The weakness was in the keys of the eight intermediates.
- **The root was distrusted by the root programs as a precaution.** To the best of our knowledge, no other roots or intermediates were generated using the flawed process.
- **Seven of the eight intermediates were never used in production.** The one that was in production had not issued a single certificate.

The key sequence of events:

- **April 30, 2025:** The eight intermediates were created in a Key Generation Ceremony.
- **Mid-2025:** The hierarchy was included in browser trust lists. It has since passed two independent audit cycles.
- **October 17, 2026 (late evening, India time):** We were made aware of the issue. The researcher notified Apple, Google, Microsoft and Mozilla at the same time.
- **October 18, 2026:** We revoked all eight intermediates.

How it happened

The keys were generated on FIPS 140-2 Level 3 certified Hardware Security Modules (HSMs). Suggestions that HSMs were not used are incorrect. The problem was a flaw in one step of the ceremony procedure, not the absence of HSMs.

During the ceremony, a key wrap/unwrap step produced a second, weak set of keys alongside the original strong keys. The weak keys were the ones published to the browser root stores. The issue went undetected for about 18 months, through two independent audit cycles. The researcher was able to reverse-engineer the weak keys, reportedly with the help of AI-assisted tooling.

We have not yet confirmed the exact root cause. We will publish it in full once our investigation is complete. We are not aware of any evidence that the weak keys were recovered or exploited by anyone before the issue was disclosed.

What is the actual impact

The impact is limited to TLS certificates chaining to the distrusted ECC root, and it is contained to a single customer ecosystem in the United States.

- **The revoked intermediates themselves have no customer impact.** They never issued a certificate, so no certificate in use anywhere relied on them.
- **The distrust of the ECC root affects one customer ecosystem in the United States.** Certificates from that hierarchy are being replaced, and we are working directly with this customer on a transition plan.
- **The majority of TLS certificates we have issued are unaffected,** because they chain to other trusted hierarchies.

There is no impact whatsoever on:

- **Our digital signature and eSign services, in India or anywhere else in the world**
- **emSigner**
- **CertiNext**
- **emCA**
- **Privatrust**
- **SecurePass**

These products and services run on separate infrastructure and continue to operate normally. Customers using them do not need to take any action.

How we are handling it

Our first priority is making sure the affected customer's services keep running without disruption.

- **Replacement certificates.** We are issuing fresh certificates to the affected customer ecosystem from an alternate, independently operated, publicly trusted CA hierarchy.

- **Working with the root programs.** We are cooperating fully with Apple, Google, Microsoft and Mozilla.
- **Clear communication.** We have notified affected customers and partners directly. We are also making sure every customer knows exactly what is and is not affected: all of our enterprise applications, the majority of our TLS certificates, and all of our digital signature and eSign services remain unaffected.

What we are putting in place

CA redundancy for all Enterprise TLS customers. We are offering every Enterprise TLS customer certificates from an additional publicly trusted CA. If one hierarchy ever has a problem, customers can switch without interrupting their business. Keeping our customers running is one of our top priorities.

A full review of our key generation process. We are reviewing every step of our Key Generation Ceremonies, starting with the wrap/unwrap step that caused this incident. We intend to deeply study how we can enhance the governance around our processes, and adopt AI based tooling in addition to other conventional means available to mitigate such occurences.

Our commitment

We acknowledge this incident and take full responsibility for it. Trust is the foundation of everything we do, and we intend to earn it back through action.

- **Transparency with the WebPKI community.** We will keep working in good faith with the root programs and the CA/Browser Forum, and publish our root cause and investigation findings openly.

- **Full support for the affected customer.** We are working closely with the one affected customer ecosystem in the United States to make sure they receive our utmost support throughout the transition.
- **Reducing risk for every TLS customer.** We will work proactively with our unaffected TLS customers to put measures such as CA redundancy in place, so that no single event can disrupt their business.

We thank the independent researcher who reported this issue responsibly, and our customers and partners for their trust.

Update 2 20 October 2026

eMudhra is actively investigating a security incident involving a specific set of intermediate CA certificates created as part of a Key Generation Ceremony (KGC) conducted in April 2025 within its public trust infrastructure.

The incident is limited to these specific intermediate CA certificates and does not affect eMudhra's root CA private keys or other intermediate CAs.

Importantly, none of the affected intermediate CAs were deployed in production, with the exception of one. Furthermore, none of these intermediate CAs, including the one deployed in production, have issued any end-entity certificates. This has been confirmed through our internal analysis and corroborated by publicly available Certificate Transparency records on crt.sh.

Upon becoming aware of the incident, eMudhra initiated its incident response procedures, took measures to contain the affected certificates, and began working closely with browser and root-store operators to safeguard users and maintain the integrity of the broader WebPKI ecosystem.

We are conducting a thorough investigation into the circumstances surrounding the incident and reviewing our security controls and operational procedures to identify and implement any necessary improvements.

The security and integrity of our trust services remain our highest priority. We are committed to transparency, adherence to industry standards, and continued collaboration with the global WebPKI community.

To avoid any misunderstanding, the removal of our Root CA's C1 and C3 with Mozilla was a voluntary and planned activity and does not pertain to this security incident.

We will provide further updates as our investigation progresses and additional findings are confirmed.

Update 1 20 October 2026

On 20 October 2026, Mozilla published a post on its Security Blog regarding eMudhra intermediate certificates. According to Mozilla:

- On 17 October 2026 at 20:06 UTC, Mozilla received a report that private keys associated with eight eMudhra intermediate certificates had been compromised.
- Mozilla blocked the affected certificates in Firefox through OneCRL, its centralised list of revoked certificates. By

22:59 UTC the same day, the update had reached all Firefox users with standard configurations, without requiring them to update or restart Firefox.

- Mozilla released Firefox 158.0.1 (Desktop and Android), Firefox ESR 115.43.1 and Firefox ESR 153.5.1 to extend this protection to users whose custom settings may have prevented the OneCRL update.
- Mozilla is updating the trusted certificate list in NSS (NSS 3.131.1) to remove the root certificate that signed the affected intermediates, to protect other applications that use Mozilla's trust store but do not receive OneCRL updates.