Your supplier can revoke your certificate in 14 hours

5 November 2026 | Strategic Intelligence Division | Security

eMudhra revoked eight weak intermediates within 14 hours of confirming the defect. Two independent audit cycles had passed over them across about 18 months. Mozilla blocked them for every standard Firefox user by 22:59 UTC on 17 October 2026, and the distrust stopped at browsers: a Java runtime keeps trusting the key until its own trust store is updated. The remedy was to leave the business.

KEY POINTS

1. The cost that lands on you is not the certificate. eMudhra is replacing certificates free of charge from partners including Sectigo, and the work is the trust stores inside your own estate.
2. Mozilla closed this in 2 hours 53 minutes. A Java runtime, an operating system store, a container image and a certificate uploaded into an application each keep trusting the key until their own owner updates them.
3. Two independent audit cycles passed over the hierarchy while the published intermediates were the weak ones, so an audit opinion is not evidence about the key a supplier shipped.
4. The supplier's remedy was exit: global SSL/TLS is about 1 per cent of consolidated revenue, ICRA retained A (Stable) and A1, and G1 issuance now ends only when a federation the releases do not name completes its migration.
5. The second certificate authority is now a line you can demand, because eMudhra offered Sectigo to every TLS customer at no additional cost, including the ones the incident never touched.

2 h 53 min
Report received by Mozilla to every standard Firefox user blocked

14 hours
Revocation of all eight intermediates, from confirmation

about 18 months
Weak keys in published trust lists, through two audit cycles

30,800
G3 certificates in the one affected client ecosystem

Source: eMudhra, Statement on Recent Certificate Security Incident, first published 20 October 2026 and updated 30 October 2026, quoting Mozilla's 20:06 and 22:59 UTC timings of 17 October 2026 and its own "about 18 months" and "within 14 hours of our confirming the issue"; Update 6 of 28 October 2026 for the 30,800 certificates. Mosaic Singularity analysis, November 2026: 20:06 to 22:59 UTC is 2 hours 53 minutes.

Its own Statement on Recent Certificate Security Incident, first published on 20 October 2026, sets out every assurance that had passed. The eight intermediates were created in a key generation ceremony on 30 April 2025, their keys were generated on FIPS 140-2 Level 3 certified hardware security modules, the hierarchy entered browser trust lists in mid-2025, and it has since passed two independent audit cycles. The published intermediates were the weak ones throughout, and an outside researcher found them on 17 October 2026. Five days later the board decided to withdraw from the global SSL/TLS certificate business, and gave as its reasons the cost and complexity of the line, the free certificates large entities already issue, and scrutiny it called out of proportion. This reaches you if your certificate estate is single-CA, or if the servers, build agents and container images behind it keep trust stores of their own, because that is the part of this neither the browser vendors nor the certificate authority can close for you.

The distrust reached Firefox by 22:59 UTC and stopped at the estate boundary

Mozilla received the report at 20:06 UTC on 17 October 2026. "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." Chrome blocked the affected intermediates within hours as well, followed by Apple and Microsoft, on the sequence ICRA records and eMudhra reproduces. Distrust is a root program's decision, not the certificate authority's and not the buyer's, and four of them made it inside a working day.

The same speed is not available inside an estate. JetBrains told its TeamCity customers on 3 November 2026 that "Software with its own trust store, such as a Java runtime, keeps trusting the compromised certificates until that trust store is updated", and that its own health report for the affected roots covers server nodes only: "The health report does not check agents."

Six trust stores, two owners, and one of them acted without being asked

Where the trust sits	Who closes it	What that takes
Mozilla's OneCRL, which Firefox reads	Mozilla	Nothing. Every standard configuration by 22:59 UTC on 17 October 2026, without a restart.
Chrome, Apple and Microsoft platforms	Those vendors	Install the vendor update. ICRA records Chrome and Firefox blocking within hours, followed by Apple and Microsoft.
Java runtime on a server node or a build agent	Platform team	A runtime build carrying the fix, for example Amazon Corretto 21.0.13.0.11 or later, then a restart of each node or agent.
Certificates uploaded into an application	Application owner	Delete or replace them. Updating the runtime does not remove uploaded certificates.
Container images and custom builds	Build team	Rebuild the image with an updated store and recreate the containers.
Operating system store, Git and MinGit, Python certifi, Node.js	Platform team	A separate update for each, from each vendor, on each image.

Source: Mozilla's timings as quoted by eMudhra, Statement on Recent Certificate Security Incident, Update 1, 20 October 2026; ICRA's sequence as reproduced in eMudhra's release of 23 October 2026; rows three to six are the stores JetBrains names in its TeamCity advisory of 3 November 2026, which states that "Updating Java does not remove uploaded certificates" and that "The health report does not check agents".

Count them as the unit of this problem: one trust store, one owner, one update. The question to carry into your own estate is how many of the places above you can name an owner for, because the certificate authority's remedy reaches none of them, and the revocation that began this arrived 14 hours after the supplier confirmed the defect.

Two independent audit cycles passed over a hierarchy whose published keys were weak

The supplier's own account is the evidence, and it is worth reading at the level of the ceremony. "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 leadership note of 26 October 2026 is shorter: "A script error resulted in issuing CA's with weak keys."

The hardware was not the failure, and the supplier says so. "The keys were generated on FIPS 140-2 Level 3 certified Hardware Security Modules (HSMs)." And: "The problem was a flaw in one step of the ceremony procedure, not the absence of HSMs." There was no breach of its infrastructure and no customer data lost, in the supplier's account. The eight intermediates "had not issued publicly trusted end-entity certificates", seven

were never used in production, and the one that was in production "had not issued a single certificate". What was lost was not data. It was about 18 months in which the published key was the weak one, and a certificate estate that then had to move inside a window four root programs set.

What a buyer can ask for instead of an audit opinion

The question a certificate buyer can put to a supplier is therefore narrow and answerable: what can you show me about the key that signs my certificate? Not the audit opinion, which passed twice while the published keys were weak. The ceremony record, the wrap and unwrap procedure, the key that was actually published to the root stores, and the name of whoever checked it. A supplier that cannot produce those has sold an assurance about a process, not about the artefact your customers' browsers were trusting.

The remedy was exit from a business worth about 1 per cent of revenue

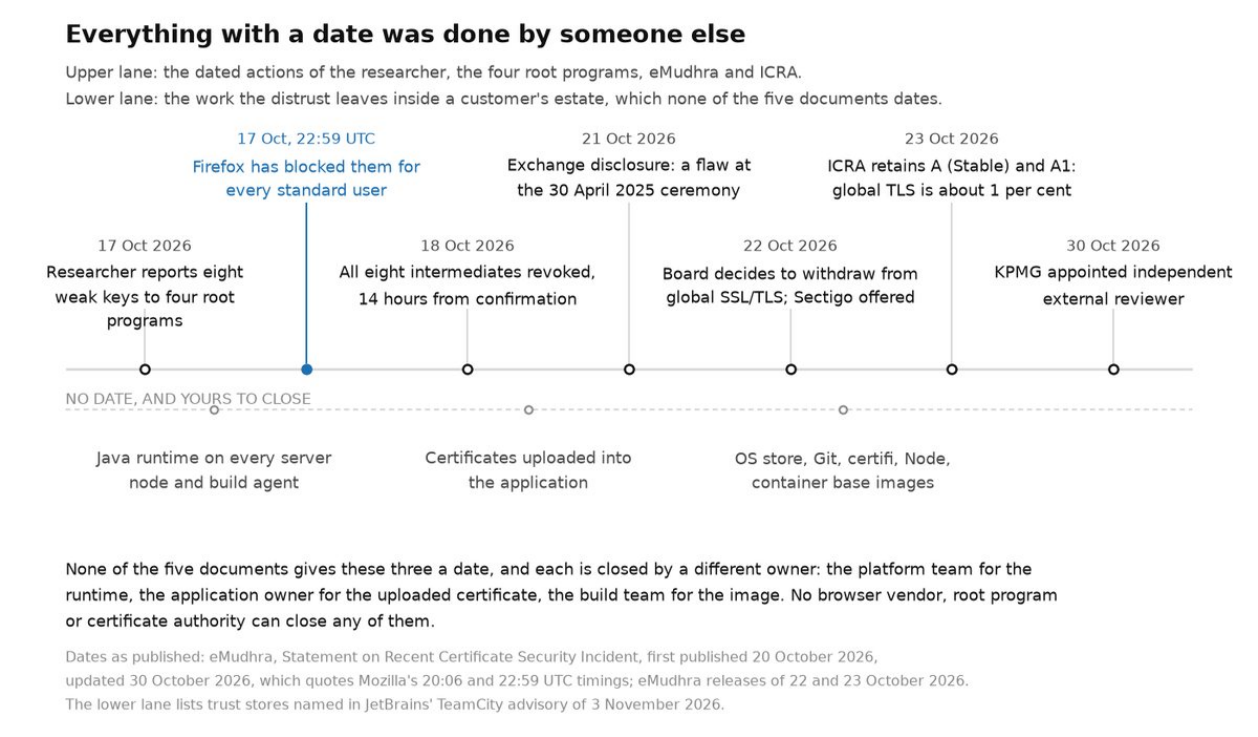
On 22 October 2026 eMudhra's board "decided to voluntarily withdraw from the global SSL/TLS certificate business". The chairman's reasons are in the release: rising data sovereignty and compliance requirements, complexity and cost, "some of the large entities issue the SSL/TLS free of cost", and "the level of social media amplification around this incident has brought scrutiny that is out of proportion to SSL/TLS's place in our business". ICRA retained the ratings the next day, 23 October 2026, "[ICRA]A (Stable)/[ICRA]A1 on Rs 35 crore of eMudhra Limited's unallocated limits", and recorded that "The global TLS business contributes only about 1 per cent of consolidated revenue." For a supplier that arithmetic makes leaving rational. For a buyer it means the party that sold the assurance is winding the line down on a timetable that ends with somebody else's migration.

That timetable is the part to watch, because it is the one deadline in the five documents that nobody has set. G1 issuance "is being used only to support this transition", and eMudhra "will stop issuing TLS certificates from G1 once the federation's transition is complete". No date appears anywhere, and the federation is not named.

The winner is named in the loser's own statement

The winner is Sectigo, and the offer went wider than the incident. On 22 October 2026 eMudhra said it was "making certificates issued by Sectigo available as an alternate option to all of our customers". By 26 October 2026 the terms were "at no additional cost, including to customers whose existing certificates are completely unaffected by the incident", which that release calls "a proactive CA redundancy measure, rather than a remediation requirement for customers in the region". A competitor's certificate, at zero, to the entire installed base, while the chairman explains that large entities already issue SSL/TLS free of cost: that is where the margin in this line had gone.

The durable gain is not Sectigo's book. It is the requirement the incident has made ordinary, and eMudhra wrote it down on 21 October 2026: "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." That sentence is now the benchmark for the next renewal, including with a different supplier: two independently operated authorities in the estate, switchable without interrupting service. The buyer who does not ask for it has accepted single-CA risk on terms nobody offered them.



Upper lane: every dated act in the record, all of them by the researcher, four root programs, eMudhra or ICRA. Lower lane: the trust stores the distrust leaves open, none of which any of the five documents dates. Source: eMudhra, Statement on Recent Certificate Security Incident, first published 20 October 2026 and updated 30 October 2026, including Mozilla's 20:06 and 22:59 UTC timings; eMudhra releases of 22 and 23 October 2026; the lower lane is the store list in JetBrains' TeamCity advisory of 3 November 2026.

Two things are promised and neither carries a date

KPMG was appointed "independent external reviewer" on 30 October 2026, and the supplier has committed to "a full root-cause analysis through the CCADB process", which "will explain what went wrong, why our controls failed to detect it, and the changes we are making as a result". It has not been published, and eMudhra states plainly that "We have not yet confirmed the exact root cause." Until it appears, no buyer can test the ceremony against an audit standard, which is why the contractual right to the ceremony record is worth more than the promise of a report. One nearby fact is a different event: the removal of eMudhra's Root CA's C1 and C3 with Mozilla "was a voluntary and planned activity and does not pertain to this security incident".



Illustrative photograph, generated for this article. It is not a photograph of any company, site or event named here.

What the CISO signs, and by when

• CISO, with the head of PKI: inventory every trust store the company operates that is not a browser, meaning each Java runtime on a server node and on a build agent, the operating system store, container base images, Git and MinGit, Python's certifi, Node.js, and every certificate uploaded into an application. JetBrains' advisory of 3 November 2026 is a usable template, because it names the places inside one product and states that the health report checks server nodes only. By 31 December 2026, ahead of the renewal.

• General Counsel: read the certificate terms for the four things this incident tested, and take them into the renewal. How much notice the supplier must give before revoking. Whether re-issue is free and by when. Whether a revocation shortens the term already paid for. Whether the supplier must publish a root-cause analysis. eMudhra gives 14 hours from confirmation and has promised a CCADB report, so both are now fair to ask of anyone. By 31 December 2026.

• CIO: make dual issuance a standing certificate requirement, two independently operated authorities per externally facing service, with a written switch path. The supplier offered exactly that to every TLS customer at no additional cost on 21 and 26 October 2026, so the licence cost of the requirement is zero and the argument is about the switch path, not the price. By 31 December 2026.

• COO: name the services that stop if a hierarchy we use is revoked or distrusted inside a working day, and pre-approve the re-issue runbook and the change window that goes with it. JetBrains' caution that "Removing AAA Certificate Services can disrupt unaffected services" is the shape of the blast radius: the fix can break connections that were working. By 31 December 2026.

The questions a board should put to management before 31 December 2026

- How many trust stores do we operate, and who is the named owner of each one?
- Which externally facing services are single-CA at present, and what would re-issuing them inside 14 hours cost in hours and in downtime?
- What does our certificate contract require the supplier to give us before it revokes, and does it require a published root-cause analysis?
- At the last renewal we accepted something as evidence of key integrity. Was it an audit opinion, and what else were we offered?
- If a root program distrusted one of our hierarchies without warning, who decides to re-issue, and who tells the customer?

What to watch, and when

- 31 December 2026: eMudhra's root-cause analysis through the CCADB process. If it names a ceremony control that an existing audit standard already tests, and says the audits should have caught it, then the reading that an audit opinion is not evidence about the published key fails, and this piece is wrong at its centre. If it names a step no audit covers, the reading holds and the ceremony record is the thing to buy.
- 31 December 2026, in your own estate: whether any runtime, image or uploaded certificate still trusts the affected roots. A clean result at every node retires this piece for you and leaves only the 14-hour notice to carry into the contract.
- 31 March 2027: whether G1 issuance has stopped. eMudhra tied it to "the federation's transition" and gave no date, so issuance continuing past the first quarter of 2027 means the wind-down is slower than the release implies.

- eMudhra, "Statement on Recent Certificate Security Incident", first published 20 October 2026, last updated 30 October 2026.
- eMudhra, "eMudhra to Exit global SSL/TLS Certificate Business", 22 October 2026.
- eMudhra, "ICRA retains eMudhra ratings after TLS certificate incident, notes exit from global business", 23 October 2026.
- eMudhra, "eMudhra Confirms No Impact to Customers or Services Across the Middle East and Africa Following Global TLS Incident", 26 October 2026.
- JetBrains, "The eMudhra Certificate Authority Compromise: What It Means for TeamCity", 3 November 2026.