NPCI/2026-27/BBPS/017 22nd October 2026

To

All Operating Units
Bharat Bill Payment System,
NPCI Bharat BillPay Ltd.

Dear Sir/Madam,

Subject: Advisory on Security Incident Involving eMudhra Intermediate Certificate Authorities and Recommended Actions

1. Background

With reference to the Cert-IN advisory CIAD-2026-0050 dated October 21, 20262, NBBL would like to draw the attention of all participants to a recently reported security incident involving certain intermediate Certificate Authorities (CAs) operated under the eMudhra/emSign ecosystem.

As per publicly available information and disclosures made by eMudhra, weaknesses in the cryptographic key-generation process resulted in the compromise of private keys associated with certain intermediate CA certificates. The affected certificates have since been revoked by eMudhra and corresponding trust actions have been initiated by major technology providers including Google, Microsoft, Apple, and Mozilla.

At present, there is no publicly confirmed evidence of malicious exploitation of the affected certificates. However, considering the critical role of digital certificates in establishing trust, authentication, encryption and software integrity, the incident warrants immediate review and preventive action by all ecosystem participants.

Potential Impact to Ecosystem

Participants using eMudhra-issued certificates may face the following risks:

1. Potential acceptance of forged or fraudulent certificates by systems not performing adequate certificate validation.
2. Exposure to man-in-the-middle (MITM) attacks against websites, APIs, applications or communication channels.
3. Authentication failures due to revocation of affected certificates.
4. Service disruption arising from certificate trust-chain validation failures.
5. Risks associated with software or applications signed using impacted code-signing certificate chains.
6. Potential impact on internet-facing services, partner integrations, VPNs, APIs, mobile applications and mutual TLS (mTLS) implementations.

Although no compromise has currently been identified within NBBL's environment, all participants are advised to assess their exposure on priority. If ASPs/TSPs/Third-parties host Production, DR, UAT, or cloud environments on behalf of participants, the participants must communicate this advisory to their respective hosting partners and ensure that all prescribed recommendations and actions are duly implemented and complied with by the ASPs/TSPs/Third-parties.

Actions Required from Participants

A. Immediate Certificate Inventory and Assessment

Participants shall:

1. Identify all digital certificates issued by eMudhra/emSign across production, DR, UAT and cloud environments that connects to BBPS ecosystem.
2. If participants identify that a TLS certificate in use has been compromised, the same shall be reported to NBBL immediately through the designated Relationship Manager (RM).
3. Identify dependencies on affected intermediate CA certificates and related trust chains.
4. Assess exposure across third-party service providers and outsourced technology environments.

B. Certificate Replacement

Participants shall:

1. Replace their eMudhra certificates on priority wherever dependency exists.
2. Prefer issuance of replacement certificates from unaffected and trusted certificate hierarchies.
3. Ensure that certificate renewals and reissuance activities are completed without service disruption.

C. Threat Hunting and Monitoring

Participants shall:

1. Review security logs for unusual certificate-related activities.
2. Monitor authentication failures and certificate validation errors.
3. Investigate suspicious TLS sessions or anomalies involving certificate trust chains.
4. Review EDR, SIEM, proxy and network-security tool alerts for indicators of misuse.

D. Third-Party Risk Management

Participants shall:

1. Assess exposure across Technology Service Providers (TSPs), Application Service Providers (ASPs), Cloud Service Providers (CSPs) and other critical vendors.
2. Obtain confirmation from critical third parties regarding assessment and remediation activities.
3. Ensure vendors undertake equivalent security measures.

E. Business Continuity Preparedness

Participants shall:

1. Validate fallback arrangements for certificate replacement activities.
2. Assess concentration risk associated with dependency on a single Certificate Authority.
3. Consider certificate authority diversification strategies for critical services.
4. Update incident response and business continuity procedures where required.

Reporting Requirements

Any suspected exploitation, service disruption, security incident, or compromise related to this advisory must be reported to NBBL immediately in accordance with applicable NBBL cybersecurity incident reporting requirements and to CERT-In as applicable.

Yours Sincerely,

Sd/-
Noopur Chaturvedi
MD & CEO
NPCI Bharat BillPay Ltd.