Technical document for migration from SHA-1 to SHA-2 (SHA-256) for Digital Signing in Aadhaar Authentication Ecosystem

With reference to the UIDAI Circular 4 of 2026 (F. no**.** HQ/4/2026-AUTH-I HQ/ 21103) on the above subject, the following may be considered for technical implementation:

In a digital signature migration from **SHA-1** to **SHA-256**, requesting entities must update two distinct components that work together: the **Digest Method** (the "fingerprint") and the **Signature Method** (the "seal").

1. Digest Method (The Hashing Algorithm)

The **Digest Method** defines how a fixed length "fingerprint" (hash) is created from your original data.

- **SHA-1 (Old):** Creates a 160-bit hash. It is now considered insecure due to collision risks.
- **SHA-256 (New):** Creates a 256-bit hash. This is the current industry standard for ensuring data integrity.
- **In XMLDSIG (XML Digital Signature)/SAML (Security Assertion Markup Language):** You must update the URI to: http://www.w3.org.
- Instead of the DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1", it is recommended to use DigestMethod Algorithm= http://www.w3.org/2001/04/xmlenc#sha256

2. Signature Method (The Signing Algorithm)

The **Signature Method** defines how that hash is cryptographically bound to your identity, usually by "encrypting" the hash with your private key.

- **RSA-SHA1 (Old):** Uses the RSA algorithm to sign a SHA-1 hash.
- **RSA-SHA256 (New):** Combines RSA with a SHA-256 hash for modern security.
- **In XMLDSIG (XML Digital Signature)/SAML (Security Assertion Markup Language):** You must update the URI to: http://www.w3.org.
- Instead of the SignatureMethod Algorithm=”http://www.w3.org/2000/09/xmldsig#rsa-sha1” it is recommended to use SignatureMethod Algorithm=http://www.w3.org/2001/04/xmldsig-more#rsa-sha256

How They Interact

1. **Hashing:** The system uses the **Digest Method** (SHA-256) to create a hash of the content.

2. **Signing:** The system uses the **Signature Method** (RSA-SHA256) to sign that specific hash.
3. **Verification:** The recipient uses the **Digest Method** to re-hash the data and the **Signature Method** to verify the signature matches that new hash.

Technical Migration Requirements

- **Parallel Update:** You must update **both** methods simultaneously. Using a SHA-256 digest with an RSA-SHA1 signature is non-standard and will often cause validation failures.
- **SAML Configuration:** In Identity Providers (IdPs) like IBM web Methods, you must explicitly change the "Digest Algorithm" field in the Service Provider metadata settings to ensure all SAML responses are correctly signed.
- **ADCS (Active Directory Certificate Services) Migration:** For internal Microsoft CAs, use certutil -setreg ca\csp\CNGHashAlgorithm SHA256 to ensure the CA uses SHA-256 for all future signatures.