PRAMAAN Trust Technical Brief

Version: v2.0 | Date: 2026-05-25
Operator: TALPRO INDIA PRIVATE LIMITED | Domain: pramaan.online

Purpose: procurement-readable technical brief for PRAMAAN trust architecture.
Scope: consent-first verification, portable worker badge, sandbox, DSR, breach, and security posture.

Disclaimer: this is not a certification, SOC 2 attestation, ISO certificate, legal opinion,
insurance certificate, uptime commitment, government approval, police approval, or UIDAI endorsement.

Trust Center: https://pramaan.online/trust
Security: https://pramaan.online/security
DPO/privacy: dpo@pramaan.online
Security disclosure: security@pramaan.online

1. Verification Architecture Overview

PRAMAAN is positioned as an India-first verification layer for people, workers, vendors, and documents.
The workflow starts with requester purpose, subject notice, data categories, and explicit consent.
Supported checks return verification signals and context, not raw document dumps.
Manual review may be required depending on source availability, mismatch, risk state, or policy.

Core surfaces:
- Retail verification entry point where supported.
- Worker-owned portable badge with QR/link sharing.
- Fixture-only technical examples.
- Public Trust Center for procurement, privacy, security, and rights review.

2. Consent-First Workflow

1. Requester states purpose before data is collected.
2. Subject receives notice, data categories, retention posture, and rights route.
3. Subject consents or declines. Consent is scoped, not blanket permission.
4. Verification runs only for supported checks and approved purpose.
5. Result is shared as status/signals with context.
6. DSR, correction, grievance, withdrawal, and support routes remain visible.

Consent alone does not solve every legal obligation. Requesters retain their own obligations.

3. Badge Signing and Verification Model

Badge samples are designed to avoid raw Aadhaar, PAN, OTPs, private documents, or unnecessary PII.
A signed badge model can include badge ID, subject display name, status, expiry, visibility scope, and key ID.
Ed25519 signature language should be used only for badge types where it is actually implemented.

Verification sequence:
- Decode badge or QR payload.
- Canonicalize payload.
- Verify signature with published public key where implemented.
- Check key ID, expiry, and online revocation/status where required.
- Return valid, expired, revoked, unknown key, tampered, or network unavailable.

4. Key Rotation, Revocation, and Expiry

Active signing keys should rotate under documented operational control.
Retired public keys may remain published for historical verification where safe and intended.
Private keys must never be published in documentation, examples, logs, or support channels.
Revocation and current badge state may require online status checks.

Worker badge public language should show validity, expiry, renewal, correction, and DSR paths.
Avoid unlimited-duration, job guarantee, future-conduct guarantee, or earnings claims.

5. Audit Trail and PII-Safe Logging

Audit records should preserve purpose, consent reference, requester, timestamp, channel, and result state.
Logs should avoid raw identity documents, OTPs, real API secrets, and unnecessary sensitive fields.
Sandbox logs must use fixture data only.
Enterprise audit exports should remain roadmap unless enabled and reviewed for a specific customer.

Data minimization and retention limits should be reviewed against product policy and legal obligations.

6. DSR, Grievance, and Breach Workflows

Public DSR route covers access, correction, erasure, grievance, nomination, and withdrawal guidance.
Requests may require identity or authority checks before action.
Deletion can be limited by retention obligations, legal hold, fraud prevention, billing, or disputes.

Incident response posture: detect, triage, contain, assess, notify, remediate, and postmortem where appropriate.
Do not read this brief as a blanket legal notification timeline or no-breach claim.

7. Accessibility, Under-18, and Security Posture

Accessibility targets: consent, verification result, worker badge, DSR, login, and help flows should be usable with keyboard navigation, text-labelled states, visible focus, and readable mobile layouts.
WCAG/IS 17802 language is target/tracked language unless independently audited.

Under-18 flows require extra minimization and parent/guardian review where product/legal policy supports use. No secret checks, unnecessary child data, or public badge exposure should be used.

Cyber-insurance status: no policy currently bound. ISO 27001 and SOC 2 are roadmap/target only.