

Passwordless and Multi-Factor Authentication with Biometrics (FIDO2)

Biometric Hardware as the Foundation of Zero-Trust Security

For security architects, CISOs, identity engineers and system integrators.

Contents

A roadmap of the argument, from threat model to deployment.

	Executive Summary	3
01	The Problem: Why Passwords and Legacy MFA Fail	4
02	FIDO2 Architecture in Depth	5
03	Biometric Engineering: What Determines Real-World Security	8
04	Biometric Hardware as the Root of Trust in Zero Trust	11
05	Threat Model and Mitigations	13
06	Privacy and Regulatory Alignment	14
07	The Indian Context: FIDO2 and Aadhaar Authentication Side by Side	15
08	Deployment Guidance for Experts	16
09	Where Mantra Softech Can Support	17
10	Illustrative Use Cases	19
11	Challenges and Future Directions	19
12	Conclusion and Recommendations	21
	Glossary	22
	References and Further Reading	22

SUMMARY

Executive Summary

Passwords remain the weakest link in enterprise and public-sector security. They are phished, reused, stuffed, leaked and socially engineered, and even one-time passwords delivered by SMS can be intercepted or relayed. At the same time, zero-trust architecture requires that every access request be authenticated and authorised continuously, based on strong evidence of who or what is making it.

FIDO2, the combination of the W3C WebAuthn API and the FIDO Alliance CTAP2 protocol, offers a standards-based answer: public-key cryptography bound to a specific origin, unlocked locally by a user-verification gesture such as a fingerprint. No shared secret travels over the network and none is stored on the server. Phishing resistance is built into the protocol rather than depending on user vigilance.

This paper argues three points:

1**Biometrics verify locally**

Biometrics are best used as a local user-verification factor, not as a centrally stored credential. In FIDO2 the template never leaves the authenticator; the server only verifies a signature.

2**Hardware sets the trust**

Trust in the whole chain depends on sensor quality, presentation attack detection, secure matching, key protection and attestation. Software-only approaches inherit the weaknesses of the host.

3**India needs a bridge**

Organisations need FIDO2 for workforce and consumer login, and Aadhaar authentication through certified Registered Devices for proofing and regulated services. Certified-hardware vendors such as Mantra Softech can support both.

The paper covers the threat landscape, FIDO2 architecture, biometric engineering considerations, a zero-trust reference architecture, regulatory alignment (NIST, DPDP Act 2023, UIDAI), deployment guidance, and the capabilities Mantra can support.

SECTION 01

The Problem: Why Passwords and Legacy MFA Fail

1.1 Structural weaknesses of passwords

A password is a shared secret. Whoever knows it can authenticate, and the server must hold something derived from it. This creates failure modes that cannot be fixed by policy alone:

- **Phishing and adversary-in-the-middle (AiTM) proxies** harvest passwords and session cookies in real time.
- **Credential stuffing** exploits password reuse across services.
- **Server-side breaches** expose hashed secrets that can be cracked offline.
- **Helpdesk and recovery abuse:** reset workflows become the real attack surface.
- **Cost:** password resets are a persistent drain on IT support.

Industry breach analyses consistently list stolen or misused credentials among the leading initial access vectors, and the pattern holds across sectors.

1.2 The limits of first-generation MFA

Factor	Main weakness
SMS OTP	SIM swap, SS7 interception, social engineering, malware reading messages
Email OTP	Only as strong as the mailbox
TOTP apps	Phishable; the user can be tricked into typing the code into a fake site
Push approval	MFA fatigue (prompt bombing) and accidental approvals
Knowledge questions	Publicly discoverable or guessable

These methods add friction but not **phishing resistance**. Attackers have adapted with real-time relay kits that capture both password and OTP and replay them instantly.

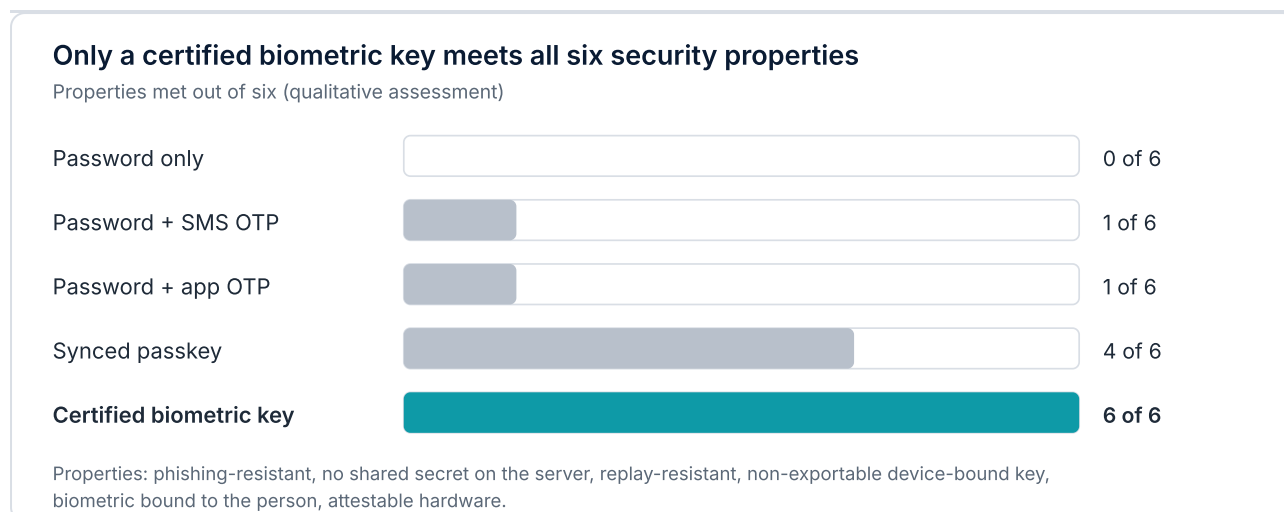


Figure 1. Author's qualitative assessment against six properties. OTP-based methods add friction but meet only the replay property; synced passkeys close most gaps, and certified hardware adds a non-exportable key and provable provenance.

1.3 Why biometrics alone, as traditionally deployed, are not the answer

Centralised biometric databases create a high-value, irrevocable target: a leaked fingerprint template cannot be reset like a password. Server-side matching also means biometric data crosses networks and sits in storage. FIDO2 avoids this by design, which is the key architectural insight of this paper.

SECTION 02

FIDO2 Architecture in Depth

2.1 Components

- **Relying Party (RP):** the application or identity provider requiring authentication.
- **WebAuthn client:** the browser or OS API exposing `navigator.credentials.create()` and `.get()`.
- **Authenticator:** the device that creates and uses credentials. It may be a *platform* authenticator (built into a laptop or phone) or a *roaming* authenticator (USB, NFC or BLE security key, possibly with a fingerprint sensor).
- **CTAP2:** the protocol between the client and a roaming authenticator.

2.2 Registration and authentication flow

REGISTRATION

1. The RP sends a challenge, its identifier (RP ID) and user information.
2. The client passes the request to the authenticator along with the origin.
3. The authenticator performs **user verification** (for example a fingerprint match) and generates a new key pair scoped to the RP ID.
4. The private key stays inside the authenticator. The public key, credential ID and an optional **attestation statement** go to the RP.

AUTHENTICATION

1. The RP sends a fresh challenge.

2. The authenticator verifies the user locally (biometric or PIN), finds the credential for that RP ID and signs the challenge plus client data and a signature counter.
3. The RP verifies the signature with the stored public key, checks the origin, challenge and flags, and grants access.

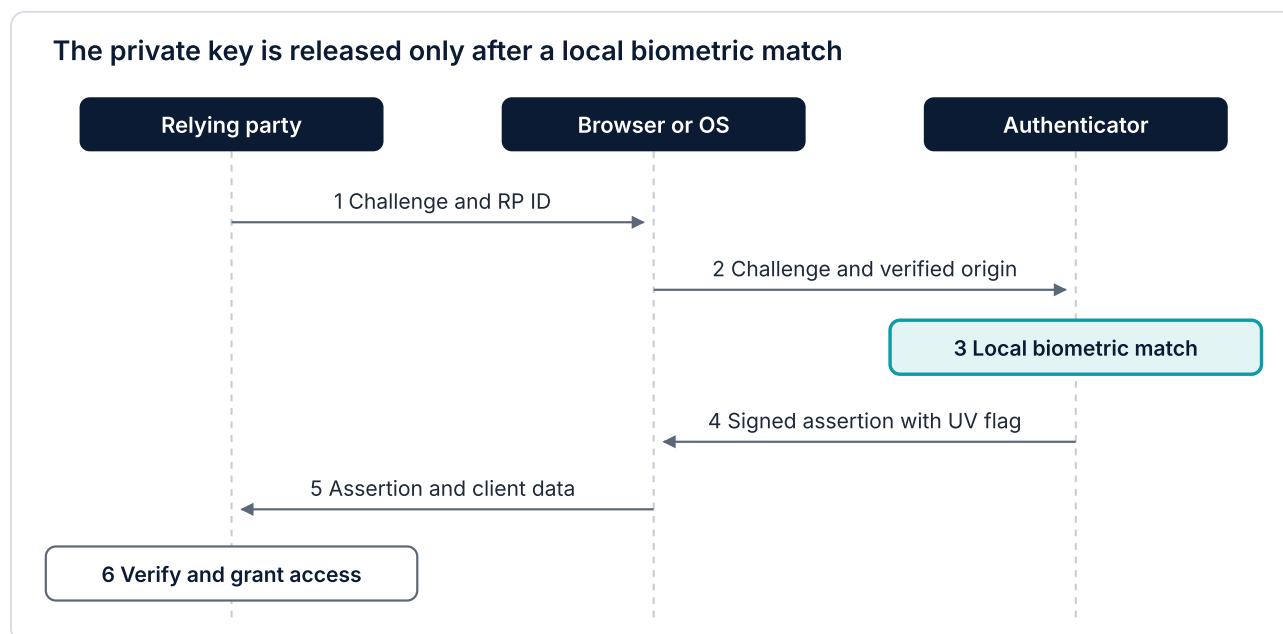


Figure 2. FIDO2 authentication sequence: six steps, three parties. The relying party never sees the biometric; it receives only a signature, which it checks against the public key stored at registration.

2.3 Why this is phishing-resistant

- Credentials are **scoped to the RP ID**. A look-alike domain gets no valid assertion because the browser reports the real origin and the authenticator holds no key for the fake one.
- Every assertion is bound to a **single-use challenge**, defeating replay.
- There is **no shared secret** to steal from the server. A breach exposes only public keys.
- The user cannot be tricked into "typing" the credential anywhere.

2.4 User presence versus user verification

FIDO distinguishes two flags that architects must set deliberately:

- **User Presence (UP):** a person touched the device. This proves presence, not identity.
- **User Verification (UV):** the authenticator verified *who* the person is, through a biometric or PIN.

DESIGN RULE

For high-assurance flows, the RP should set `userVerification: "required"` and check the UV flag server-side. Treating UP as equivalent to UV is a common design error.

2.5 Passkeys, discoverable credentials and sync

Passkeys are FIDO credentials that are discoverable (resident) and, in many consumer implementations, synchronised across a user's devices by a platform provider. Two policy models exist:

Model	Characteristics	Typical use
Synced passkeys	Convenient, recoverable, tied to an ecosystem account	Consumers, low to medium assurance
Device-bound passkeys	Private key never leaves the hardware; attestation proves the model	Workforce, privileged access, regulated environments

Zero-trust programmes with strict assurance needs usually favour **device-bound credentials on certified hardware**, using attestation to enforce which authenticators are acceptable.

Table 1. Authenticator options compared

Authenticator type	Where the private key lives	User verification	Attestation	Assurance ceiling	Best fit
Synced passkey	Platform credential manager, synced across devices	Device unlock (biometric or PIN)	Limited or none	AAL2	Consumers, general SaaS
Device-bound platform authenticator	TPM or secure enclave in the endpoint	OS biometric (fingerprint, face)	Available; varies by vendor	AAL2, higher with certified hardware	Managed laptops and phones
Roaming security key (PIN)	Secure element in the key	PIN only	Yes	AAL3	Administrators, shared workstations
Roaming biometric security key	Secure element in the key	Match-on-device fingerprint	Yes	AAL3	Privileged users, BFSI, government, shared workstations
Smart card or PKI token	Secure element in the card	PIN, or match-on-card where supported	Via certificate chain	AAL3	Legacy PKI estates, government

2.6 Attestation

Attestation lets the authenticator prove its make and model to the RP. Combined with the FIDO Metadata Service (MDS), the RP can accept only authenticators of a known certification level, reject known-vulnerable models and apply different policies by device class. This is the point where **hardware provenance becomes a security control**.

SECTION 03

Biometric Engineering: What Determines Real-World Security

A FIDO2 flow is only as strong as the user-verification step feeding it. Experts should evaluate the following layers.

3.1 Sensor and capture quality

- **Modality:** capacitive and optical fingerprint, multispectral, iris, face (2D, IR, 3D), palm vein.
- **Resolution and area:** fingerprint capture at 500 dpi with sufficient sensing area underpins both accuracy and interoperability with standards such as ISO/IEC 19794 and ANSI/NIST-ITL formats.
- **Image quality scoring** (for example NFIQ 2 for fingerprints) rejects poor captures before they degrade matching.
- **Environmental robustness:** dry, wet or worn fingers, ambient light for face and iris, sensor ageing and contamination.

3.2 Matching performance

Two error rates drive the security and usability trade-off:

- **False Accept Rate (FAR):** an impostor is accepted. Governs security.
- **False Reject Rate (FRR):** a genuine user is rejected. Governs usability and support cost.

Testing should follow ISO/IEC 19795 principles and be run on populations that resemble the deployment. Fingerprint performance on manual labourers, elderly users or users in dusty field conditions differs markedly from office use.

3.3 Presentation Attack Detection (PAD)

Spoofing with gelatin, silicone or printed artefacts (fingerprint), photos, replay video or masks (face) and now **deepfake injection attacks** is the principal threat to biometric user verification. PAD should be evaluated per ISO/IEC 30107-3, with metrics such as APCER and BPCER. Design points:

- Hardware-assisted liveness (optical or electrical signals, IR, multispectral) is stronger than purely software heuristics.
- **Injection attacks** (feeding synthetic data in place of the sensor signal) require a trusted capture path: signed sensor data, secure channels and device-level integrity, not only liveness at the image level.

3.4 Where matching happens

Architecture	Template location	Security property
Match-on-host	Host OS storage	Depends on the OS and drivers; larger attack surface
Match-in-TEE / secure enclave	Isolated environment on host	Strong when the TEE is hardened
Match-on-sensor / match-on-card	Inside the sensor or secure element	Template and decision never leave the device; best for portable authenticators

For roaming authenticators, **match-on-device** with a secure element is the strongest option: the template is stored in tamper-resistant memory, the matching decision is made inside it, and the key release is gated by that decision.

3.5 Key protection and anti-hammering

- Private keys held in a **secure element** or equivalent, non-exportable.
- **Retry limits** with lockout and PIN fallback to resist brute-force or hill-climbing attacks.
- Secure firmware update with signed images, and rollback protection.
- Side-channel and fault-injection resistance for high-assurance tiers.

3.6 Certification landscape

Experts should map their requirements to recognised programmes:

- **FIDO Alliance** functional certification, authenticator certification levels and **Biometric Component Certification** for the biometric subsystem.
- **ISO/IEC 30107-3** PAD testing from accredited laboratories.
- **Common Criteria** and FIPS 140 validations for secure elements and cryptographic modules.
- In India, **STQC** certification of biometric devices and **UIDAI Registered Device** certification for Aadhaar use (Section 7).

Table 2. Certification evidence to request from a biometric hardware vendor

Standard or programme	What it covers	What to ask the vendor for
FIDO Alliance authenticator certification	Protocol conformance, interoperability, authenticator security level	Certificate number and level; AAGUID listed in the FIDO Metadata Service
FIDO Biometric Component Certification	Accuracy and PAD of the biometric subsystem	Certificate for the exact sensor and algorithm version shipped
ISO/IEC 30107-3	PAD testing and reporting (APCER, BPCER)	Accredited laboratory report covering the attack types relevant to you
ISO/IEC 19795	Methodology for biometric performance testing (FAR, FRR)	Test protocol, population and results
Common Criteria or FIPS 140	Security of secure elements and cryptographic modules	Certificate whose scope matches the chip actually used
STQC certification	Indian testing and certification of biometric devices	Certificate valid for the model and firmware version
UIDAI Registered Device certification	Aadhaar-ready devices that sign and encrypt data at capture	Current RD certificate and RD service version
NIST SP 800-63B AAL3	Assurance level for hardware-based multi-factor cryptographic authenticators	Mapping of the authenticator to AAL3 requirements

SECTION 04

Biometric Hardware as the Root of Trust in Zero Trust

4.1 Zero-trust principles in brief

NIST SP 800-207 describes zero trust as a shift from perimeter-based trust to continuous, per-request verification of identity, device posture and context. Three tenets bear directly on authentication:

1. No implicit trust based on network location.
2. Access is granted per session with the least privilege needed.
3. Authentication and authorisation are dynamic and strictly enforced before access.

4.2 Why identity assurance needs a hardware anchor

A zero-trust policy engine is only as good as the signals it receives. If the "user is verified" signal comes from a phishable password or a spoofable software check, every downstream control inherits that weakness.

Certified biometric hardware contributes four properties:

- **Possession:** a private key bound to a physical device that cannot be copied.
- **Inherence:** a biometric match that links the device to the person present, not just whoever holds it.
- **Provenance:** attestation proving the authenticator's model and certification state.
- **Integrity:** tamper resistance and signed firmware, so the signal is trustworthy.

This maps to NIST SP 800-63B **Authenticator Assurance Level 3 (AAL3)**, which requires a hardware-based, verifier-impersonation-resistant authenticator with a multi-factor cryptographic device. FIDO2 roaming authenticators with user verification are a principal route to AAL3.

4.3 Reference architecture

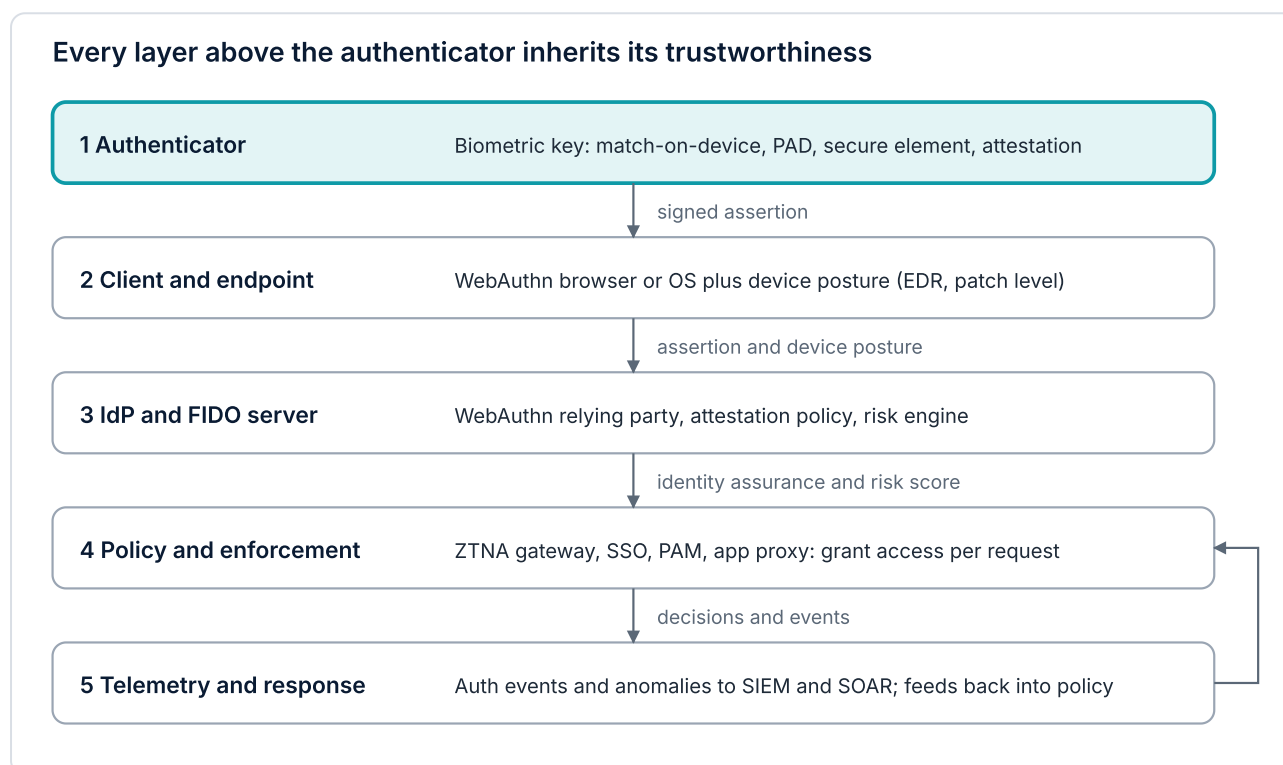


Figure 3. Zero-trust reference architecture: five layers and one feedback loop. The highlighted layer is the root of trust; if it can be spoofed or cloned, the policy engine acts on a false signal.

- **Layer 1, Authenticator:** biometric security key or reader with match-on-device, PAD and secure element; platform authenticators for managed endpoints.
- **Layer 2, Client and endpoint:** WebAuthn-capable browsers and OS, plus endpoint posture signals (managed device, patch level, EDR state).
- **Layer 3, Identity provider and FIDO server:** WebAuthn RP implementation, MDS integration, attestation policy, credential lifecycle management, risk engine.
- **Layer 4, Policy decision and enforcement:** the policy engine combines authenticator class, UV flag, device posture, location, time and resource sensitivity. Enforcement points include ZTNA gateways, SaaS SSO, VPN replacement, privileged access management and application proxies.
- **Layer 5, Telemetry and response:** authentication events, attestation anomalies, signature-counter irregularities and lockouts feed SIEM and SOAR for continuous evaluation.

4.4 Step-up and continuous authentication

Zero trust is not a single login. Practical patterns:

- **Session login** with a platform passkey for ordinary resources.
- **Step-up** to a certified hardware biometric authenticator for sensitive actions: privileged console access, payment approval, code signing, production deployment.
- **Transaction binding** where the signed assertion covers transaction details, giving non-repudiation.
- **Re-verification** triggered by risk signals such as new device, impossible travel or anomalous behaviour.

SECTION 05

Threat Model and Mitigations

Threat	Passwords + OTP	FIDO2 with biometric hardware
Phishing / AiTM	Vulnerable	Resistant through origin binding
Credential stuffing	Vulnerable	Not applicable; unique key per RP
Server database breach	Hashes exposed	Public keys only
Remote malware keylogging	Vulnerable	No secret typed
Replay	Partly mitigated	Single-use challenge
SIM swap	Vulnerable (SMS)	Not applicable
Stolen device	Depends	Biometric or PIN required; lockout
Spoofed fingerprint / face	Not applicable	Mitigated by PAD, hardware liveness
Injection / deepfake attack	Not applicable	Mitigated by trusted capture path and signed sensor data
Helpdesk social engineering	Vulnerable	Reduced; requires strong recovery design
Insider credential sharing	Easy	Hard; biometric binds credential to person

RESIDUAL RISKS EXPERTS MUST STILL ADDRESS

- **Account recovery** is the new weak point. Recovery should require a second registered authenticator or an identity-proving process of comparable strength, never a fallback to SMS or email alone.
- **Enrolment integrity**: a credential registered by an attacker is a valid credential. Bind enrolment to verified identity, ideally in person or via strong proofing.
- **Biometric bypass by coercion** remains possible; high-risk roles may need duress mechanisms or dual control.
- **Supply chain**: use attestation, verified firmware provenance and certified hardware.
- **Lifecycle**: lost, stolen or retired authenticators need prompt revocation.

SECTION 06

Privacy and Regulatory Alignment

6.1 Privacy by design in FIDO2

FIDO2 supports data minimisation structurally:

- Biometric templates stay on the authenticator and are never shared with the RP.
- Credentials are unique per RP, preventing cross-service tracking.
- Attestation can be batch-based so individual devices are not uniquely identifiable by default.

6.2 India: Digital Personal Data Protection Act, 2023

Biometric data is personal data under the DPDP Act, and processing requires lawful grounds, typically consent for workforce and consumer flows, along with notice, purpose limitation, security safeguards and breach notification duties for the Data Fiduciary. Architectures that keep templates on the device reduce the data held by the fiduciary and therefore the compliance burden and breach impact. Organisations should confirm rules and timelines with legal counsel, as subordinate rules and enforcement details continue to evolve.

6.3 Other frameworks to map

- **NIST SP 800-63B** for assurance levels and **SP 800-207** for zero trust.
- **RBI** guidance on authentication for digital payments and the move away from SMS-only factors.
- **CERT-In** directions on incident reporting and security practice.
- **ISO/IEC 27001** controls for access management.
- **ISO/IEC 24745** on biometric information protection and **ISO/IEC 30107** for PAD.

SECTION 07

The Indian Context: FIDO2 and Aadhaar Authentication Side by Side

India's identity infrastructure has a distinct model that technical teams must understand and not conflate with FIDO2.

Aspect	FIDO2 / WebAuthn	Aadhaar biometric authentication
Purpose	Authenticate a returning user to a service	Verify a resident against the national identity record
Biometric matching	Local, on the authenticator	Server-side at the UIDAI central repository
Biometric leaves device	No	Yes, encrypted and signed at capture
Credential	Key pair per service	Aadhaar number with live biometric or OTP
Hardware trust	Attestation and certification	UIDAI-certified Registered Device with signing at capture
Best fit	Workforce SSO, enterprise, consumer login	e-KYC, identity proofing, subsidy and regulated services

These models are **complementary**:

- **Aadhaar authentication** is excellent for *proofing who a person is* at onboarding.
- **FIDO2** is excellent for *proving it is the same person* on every subsequent login.

A strong combined pattern: verify the user's identity once using an Aadhaar-registered biometric device during enrolment or KYC, then issue and bind a device-bound FIDO2 credential to that verified identity for all later authentication. This closes the enrolment-integrity gap noted in Section 5.

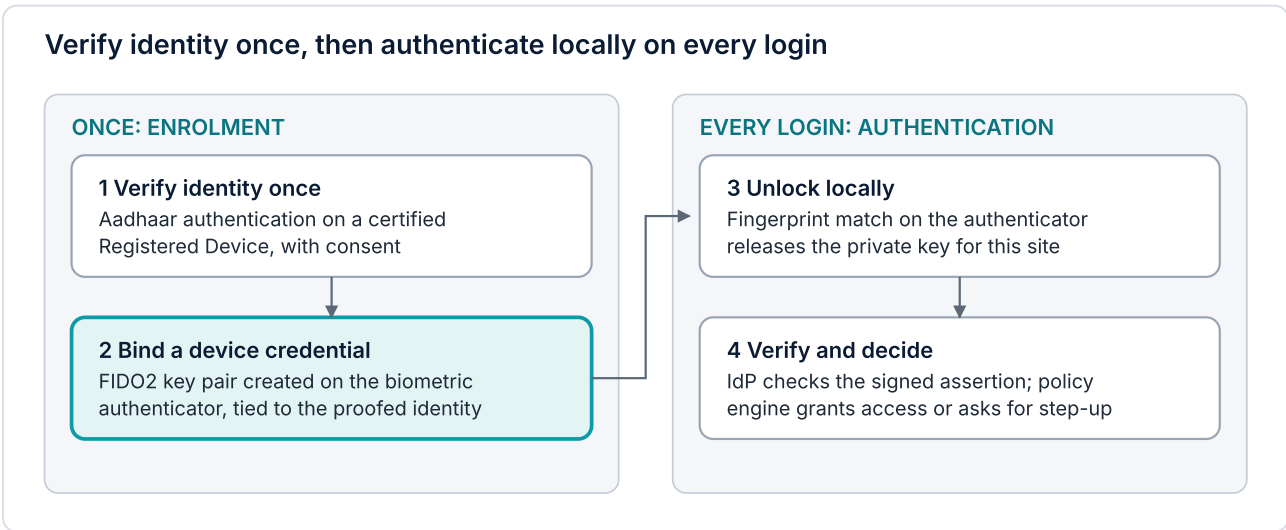


Figure 4. Aadhaar proofing bound to a FIDO2 credential: two phases, four steps. The national identity check happens once at enrolment; every later login is a local match and a signature, with no biometric sent to the server.

UIDAI's Registered Device model is itself an instructive case for hardware trust: certified devices sign and encrypt biometric data at capture, so downstream systems can rely on its origin and integrity. The same engineering principle of a trusted capture path underlies strong FIDO2 user verification.

SECTION 08

Deployment Guidance for Experts

8.1 Phased roadmap

Phase	Focus
Phase 0: Assess 4 to 6 weeks	Inventory applications, identity providers, protocols (SAML, OIDC, RADIUS, Kerberos, legacy LDAP) and user populations. Classify resources by sensitivity and map to assurance levels.
Phase 1: Pilot 6 to 10 weeks	Select high-risk groups such as administrators, finance and developers. Deploy certified biometric authenticators, enforce UV and attestation policy, and design recovery.
Phase 2: Scale	Extend to the workforce with a mix of platform passkeys and hardware authenticators. Introduce conditional access and step-up policies.
Phase 3: Eliminate passwords	Remove password and SMS fallbacks for covered applications. Move legacy apps behind a proxy or identity-aware gateway where native support is absent.
Phase 4: Optimise	Continuous risk-based policy, automated lifecycle management, red-team testing of recovery and enrolment flows.

8.2 Key design decisions

- **Authenticator mix:** which populations get hardware biometric keys, which get platform passkeys.
- **Attestation policy:** allow-list by AAGUID and certification level through MDS.
- **Recovery model:** two authenticators per user, supervised re-enrolment, manager or HR-backed proofing.
- **Shared and kiosk environments:** shop-floor, factory and healthcare settings where users share workstations. Roaming biometric authenticators or reader-based flows suit these better than personal phones.
- **Offline and low-connectivity operation:** relevant for field deployments.
- **Legacy integration:** bridge through an IdP that fronts older systems with SAML or OIDC.

8.3 Metrics to track

- Percentage of authentications that are phishing-resistant
- Password reset ticket volume
- Authentication success rate and time to authenticate
- FRR per population segment
- Share of privileged sessions using hardware-bound credentials
- Recovery events and their verification outcomes

8.4 Common pitfalls

- Leaving SMS or email fallback enabled, which negates phishing resistance.
- Setting only user presence and not requiring user verification.
- Skipping attestation checks and accepting any authenticator.
- Under-designing recovery and enrolment.
- Not testing biometrics on the real user population.

SECTION 09

Where Mantra Softech Can Support

CAPABILITIES MAPPED TO THIS ARCHITECTURE

Mantra Softech is an Indian biometric and identity-technology company with long experience in certified biometric capture hardware and Aadhaar-ecosystem deployments. The following capabilities map to the architecture above. **Product specifications and certifications should be confirmed against current Mantra datasheets and certificates at the time of deployment.**

9.1 Established strengths

Capability	Relevance to this architecture
Fingerprint and iris scanners with STQC and UIDAI Registered Device certification (the MFS and MIS device families, among others)	Trusted capture path for identity proofing and e-KYC; the enrolment anchor for binding strong credentials to verified people
Registered Device (RD) service software and SDKs for Windows, Android and Linux	Secure integration of capture hardware into banking, government and enterprise applications
Biometric attendance, access control and time-and-attendance systems	Physical and logical access convergence; workforce identity in factories, campuses and offices
Experience with large-scale, field-hardened deployments	Practical knowledge of sensor performance on diverse, real-world user populations
Local manufacturing, support and integration ecosystem	Supply-chain assurance, faster support and alignment with Indian compliance needs

9.2 Proposed solution blueprint: biometric-secured FIDO2 for the Indian enterprise

Building on these foundations, Mantra can position and develop the following offerings.

1

Biometric FIDO2 roaming authenticator (USB and NFC)

A security key with an integrated fingerprint sensor performing match-on-device within a secure element, with hardware PAD, CTAP2 support, attestation, and a target of FIDO Alliance functional and biometric component certification. Designed for privileged users, BFSI operations and government officers who require AAL3-class assurance.

2

"Verify once, bind forever" enrolment service

A workflow in which a person is identity-proofed using a Mantra Registered Device through Aadhaar authentication (with consent, within applicable law), after which a FIDO2 credential is issued and bound to that verified identity. This addresses the enrolment-integrity weakness and gives regulated entities an auditable chain from national identity to daily login.

3

Shared-workstation and shop-floor authentication

Biometric reader-based login for environments where users do not carry personal devices: manufacturing, hospitals, retail and call centres. Fast tap-and-touch authentication through FIDO2-compatible readers integrated with the enterprise IdP.

4

Authentication gateway and integration SDKs

A lightweight FIDO2/WebAuthn relying-party service and connectors for common IdPs (OIDC, SAML), RADIUS and legacy applications, so customers can adopt passwordless without re-platforming. Includes attestation policy management using the FIDO Metadata Service.

5

Unified physical and logical access

One biometric credential for door access, workstation login and application SSO, with unified audit logs and centralised revocation when an employee leaves.

6

Lifecycle and recovery tooling

Authenticator inventory, issuance, revocation, supervised re-enrolment and dual-authenticator enforcement, with telemetry exportable to SIEM platforms.

7

Advanced PAD and anti-injection roadmap

Multi-modal and hardware-assisted liveness, signed sensor data and device-integrity checks to counter spoofing and deepfake injection, aligned with ISO/IEC 30107-3 testing.

STATUS NOTE

These seven offerings are positioning proposals built on Mantra's existing strengths. They are not announced products; confirm current availability, specifications and certifications with Mantra before external publication.

9.3 Differentiators

- **Dual competence:** certified Aadhaar-ecosystem capture hardware and a path to global FIDO2 interoperability.
- **Privacy by architecture:** templates stay on the device, supporting DPDP Act obligations.
- **Field realism:** sensor design informed by Indian conditions such as varied fingerprint quality, heat, dust and high-volume use.
- **Cost and availability:** domestic manufacturing and support can lower total cost of ownership relative to imported alternatives.

9.4 Target sectors

BFSI and payments, government and e-governance, defence and critical infrastructure, healthcare, manufacturing, IT services and BPO, education and large enterprises with shared or distributed workforces.

SECTION 10

Illustrative Use Cases

USE CASE A

Bank branch and back-office

Tellers and operations staff authenticate with a biometric key at login and again for high-value transaction approvals. Customer onboarding uses an Aadhaar-registered device for e-KYC. Privileged database access requires step-up to a device-bound credential.

Outcome: phishing-resistant access, non-repudiable approvals and fewer password-reset tickets.

USE CASE B

Government e-office

Officers sign files and approve orders using biometric hardware authenticators bound to their verified identity. Attested devices only; audit trail for every signed action.

Outcome: stronger accountability and reduced credential sharing.

USE CASE C

Manufacturing and shop floor

Shared terminals use reader-based biometric login with FIDO2 behind the scenes. The same credential logs attendance and opens controlled areas.

Outcome: faster login for gloved or hurried workers, accurate records and unified revocation.

USE CASE D

DevSecOps and code signing

Engineers must present a hardware biometric authenticator to merge to protected branches and sign releases.

Outcome: protection against stolen tokens and supply-chain compromise.

SECTION 11

Challenges and Future Directions

- **Deepfakes and injection attacks** will push the industry toward signed, hardware-rooted capture and multi-signal liveness.

-
- **Passkey interoperability and portability** standards continue to evolve; organisations should track FIDO Alliance work on credential exchange.
 - **Post-quantum cryptography:** today's FIDO2 relies on elliptic-curve and RSA signatures. Authenticator vendors should plan crypto-agility and migration paths as post-quantum algorithms are standardised.
 - **Decentralised and verifiable credentials** may combine with FIDO2 to give users portable, privacy-preserving identity.
 - **Continuous and behavioural signals** will complement, not replace, strong hardware authentication.
 - **Inclusion:** designs must accommodate users with worn fingerprints, disabilities or limited digital literacy through multi-modal options and well-designed fallbacks.

SECTION 12

Conclusion and Recommendations

Passwordless authentication based on FIDO2 is the most practical route to phishing-resistant, privacy-preserving, zero-trust-compatible identity today. Its strength depends on the quality of the hardware that performs user verification and protects keys.

Recommendations for security leaders

- 1 **Make phishing-resistant authentication the target state** for all privileged and sensitive access first, then expand.
- 2 **Require user verification and attestation** in policy; do not accept presence-only or unattested authenticators for high-assurance use.
- 3 **Prefer match-on-device biometrics with hardware PAD** and certified components for roaming authenticators.
- 4 **Invest as much in enrolment and recovery as in login**, since attackers will target them next.
- 5 **Combine national identity proofing with FIDO2** in India: verify once with certified Registered Devices, then authenticate daily with device-bound credentials.
- 6 **Choose vendors with certified hardware, transparent security architecture and field-proven deployments**, and verify certifications independently.

Biometric hardware is not merely a convenience layer. Properly engineered, it is the root of trust that makes every other zero-trust decision believable.

APPENDIX

Glossary

AAGUID	Identifier of an authenticator model, used with attestation and the FIDO Metadata Service.
AAL3	NIST's highest authenticator assurance level.
APCER / BPCER	Attack presentation and bona fide presentation classification error rates used in PAD testing.
CTAP2	Client to Authenticator Protocol.
FAR / FRR	False Accept Rate / False Reject Rate.
MDS	FIDO Metadata Service.
PAD	Presentation Attack Detection.
RP	Relying Party.
TEE	Trusted Execution Environment.
UP / UV	User Presence / User Verification.
WebAuthn	W3C Web Authentication API.

APPENDIX

References and Further Reading

1. W3C, *Web Authentication: An API for accessing Public Key Credentials* (WebAuthn).
2. FIDO Alliance, *Client to Authenticator Protocol (CTAP2)* and certification programme documentation.
3. NIST SP 800-63B, *Digital Identity Guidelines: Authentication and Lifecycle Management*.
4. NIST SP 800-207, *Zero Trust Architecture*.
5. ISO/IEC 30107-3, *Biometric presentation attack detection: Testing and reporting*.
6. ISO/IEC 19795, *Biometric performance testing and reporting*.
7. ISO/IEC 24745, *Biometric information protection*.
8. UIDAI, *Aadhaar Authentication API and Registered Device specifications*.
9. Government of India, *Digital Personal Data Protection Act, 2023*.
10. Mantra Softech, product datasheets and certification documents (confirm current versions before publication).

Standards, regulations and product certifications evolve. Verify current versions, Mantra product specifications and regulatory status before external publication.