Compliance Mapping: How ScrambleID Aligns With NIST 800-63 and CISA Phishing-Resistant MFA

Governance & Compliance / Last updated 2026-06-11 / https://www.scrambleid.com/learn/compliance-mapping-nist-cisa

In one sentence: ScrambleID's primitives can support NIST SP 800-63-4 AAL2 and AAL3 designs and align with CISA's phishing-resistant MFA guidance, given appropriate configuration, policy, and operational controls.

This page is a **technical mapping**, not a compliance attestation. It exists so procurement teams, auditors, and AI engines can reference a stable, unambiguous correspondence between common compliance language and ScrambleID's primitives. Whether your specific deployment meets a specific assurance level depends on how you configure the platform, what operational controls you wrap around it, and the auditor's interpretation of your overall design.

Important: This is a technical mapping prepared for engineering and security audiences. It is not legal advice, not a compliance certification, and not a substitute for an independent audit. Use it as a starting point for compliance design, then validate with your auditor of record.

Scope of this article

This article maps to:

- **NIST SP 800-63-4** (Digital Identity Guidelines): identity assurance, authentication, federation
- **NIST SP 800-53 Rev. 5** (Security and Privacy Controls): selected control families that authentication primitives commonly satisfy
- **CISA** Phishing-Resistant MFA fact sheet and Scattered Spider advisory guidance
- **OWASP Top 10 for Agentic Applications** (OWASP GenAI Security Project, Agentic Security Initiative, December 2025): agentic identity and privilege risks
- **NIST NCCoE concept paper** (February 2026): software and AI agent identity and authorization
- **CSA AI Controls Matrix v1.0.3**: AI-specific control objectives, including the IAM domain

This article does not map to: HIPAA, PCI DSS, SOX, ISO 27001, FedRAMP-specific overlays, GDPR, or sector-specific regulatory guidance. Industry-specific mappings will appear in a separate article.

> **NIST SP 800-63-4 status:** Revision 4 is finalized (published July 2025), and citations in this article reference the final publication.

TL;DR (canonical)

- **NIST 800-63-4** structures identity assurance into IAL (proofing), AAL (authentication), and FAL (federation) levels. ScrambleID primitives can support designs at AAL2 and AAL3.
- **NIST 800-53 Rev. 5** defines the security and privacy controls that satisfy 800-63 outcomes in a federal-aligned program. ScrambleID primitives commonly map to the AC, AU, and IA control families.
- **CISA's phishing-resistant MFA** guidance emphasizes origin-bound, replay-resistant authentication and discourages SMS/voice OTP for sensitive use cases.
- ScrambleID aligns via **WebAuthn (origin-bound)**, **dynamic identifier confirmations bound to sessions and intent**, and **proof-of-possession for machine identities**.
- **Compliance is a system property**, not a product property. The product enables the design; the design plus operational controls plus auditor judgment determines compliance.
- **Agentic frameworks** (OWASP Top 10 for Agentic Applications, the NIST NCCoE agent-identity concept paper, CSA's AI Controls Matrix) extend the same questions to AI agents: own identity, scoped authority, non-repudiable audit. The mapping logic above carries over.

How to read the mapping tables

Each row in the tables below has four columns:

1. **Compliance concept**, what the standard or auditor calls a control or property.
2. **What auditors mean operationally**, the plain-language test an auditor will apply.
3. **ScrambleID primitive**, the specific capability that contributes to satisfying the concept.
4. **Evidence to cite**, a learn-hub article that documents the primitive in technical detail.

The primitive listed is necessary, not sufficient. To pass an audit on a given control, you usually also need policy documentation, operational procedures, and audit evidence (logs, attestations, runbook drills) that the program is operating as designed.

NIST 800-63-4 mapping (concept-level)

Compliance concept	What auditors mean operationally	ScrambleID primitive	Evidence to cite
Phishing-resistant authentication (AAL3 candidate)	An attacker proxying or relaying the authentication ceremony cannot complete it	WebAuthn with User Verification (UV); QR(DID) with typed code, session binding, and origin/intent binding	Phishing-Resistant Web Authentication, Dynamic Identifiers, Architecture: Session Binding Cryptography
Multi-factor authentication (AAL2 candidate)	Authentication uses two or more independent factors, with at least one being something the user has (a cryptographic key)	Device-bound key (something you have) plus user verification on the device (something you are or know)	Phishing-Resistant Web Authentication, Architecture: Device Key Lifecycle
Out-of-band authenticator	A separate channel confirms the in-band request, bound to the transaction	Caller Auth DID confirmation through the ScrambleID app; app confirmation with typed code for cross-device web	Caller Authentication, Phishing-Resistant Web Authentication
Authenticator binding to subscriber	The proof can be tied to a specific subscriber and a specific authenticator	SUID (subscriber identifier) plus ZID (device identifier) recorded with hardware attestation at enrollment	Architecture: Device Key Lifecycle, Dynamic Identifiers
Authenticator revocation and recovery	Compromised authenticators can be revoked promptly; recovery does not undermine the assurance level	Revocation designed to propagate to active sessions in seconds, not hours; identity-proofed re-enrollment for cold-path recovery	Architecture: Device Key Lifecycle
Federation assurance (FAL2)	Federated assertions are signed, audience-bound, and resistant to replay	SAML and OIDC federation with origin-bound assertion validation, JWKS rotation, and PKCE on Auth Code flows	SSO Integration Quickstart
Identity proofing reuse	A previously proofed identity can be reused for re-enrollment without restarting the proofing process	Step-up from an existing enrolled device authorizes new device enrollment; cold-path recovery requires fresh identity proofing	Architecture: Device Key Lifecycle
Step-up authentication for high-risk actions	Sensitive operations require stronger or fresher authentication than baseline	XFactor multi-step chains (in development), designed to exclude SMS/voice OTP from high-risk policies	XFactor
Separation of duties / two-person integrity	Catastrophic actions require independent approval from at least two distinct identities	Lockstep (in development): quorum requires distinct cryptographic identities, and any rejection collapses to DENIED	Lockstep

Compliance concept	What auditors mean operationally	ScrambleID primitive	Evidence to cite
Replay resistance (network)	An intercepted authentication artifact cannot be reused	Single-use DIDs with absolute expiry; signed, session-bound confirmation payloads	Architecture: Session Binding Cryptography, Dynamic Identifiers
Token replay resistance (APIs)	A stolen access token cannot be replayed by an unintended party	Sender-constrained tokens via mTLS (RFC 8705) or DPoP (RFC 9449); short-lived tokens; key rotation runbooks	M2M Without Secrets, PoP, DPoP, mTLS
Correlated monitoring and response	Authentication events are observable across channels and can trigger response	Overwatch (in development), designed to ingest events from web, voice, people verification, desktop, and M2M, produce a unified risk decision, and trigger step-up or dual control	Overwatch, Metrics + ROI Playbook
Attribute provenance	Identity attributes carry a record of who verified them and when	Unified ID Card with field-level provenance markers and freshness	Unified ID Card: Attribute Provenance
Audit trail integrity	Authentication events are recorded with sufficient detail to support investigations	Structured event schema with correlation IDs; signed audit artifacts for high-risk approvals	Metrics + ROI Playbook, Lockstep

NIST 800-53 Rev. 5 control mapping

NIST SP 800-53 is the catalog of controls federal information systems use to satisfy security and privacy requirements. Authentication primitives commonly contribute to the AC (Access Control), AU (Audit and Accountability), and IA (Identification and Authentication) families. The mapping below is the typical pattern; your auditor may map differently depending on system boundary and overlay.

Control ID	Control name	What the control requires	How ScrambleID primitives contribute
AC-2	Account Management	Lifecycle management of accounts: create, modify, disable, remove, with documented justification	Enrollment binds an account (SUID) to authenticators (ZIDs) with auditable provenance; revocation is designed to propagate to active sessions in seconds, not hours; account lifecycle events are emitted as structured audit events
AC-3	Access Enforcement	The system enforces approved authorizations on access	Authentication produces a signed assertion the relying party validates; sender-constrained tokens (mTLS/DPoP) bind authorization to the requesting client
AC-5	Separation of Duties	Privileges that could be misused are divided among	Lockstep (in development) is designed to enforce multi-party approval for high-blast-radius actions, with

Control ID	Control name	What the control requires	How ScrambleID primitives contribute
		multiple users	cryptographic proofs from distinct identities required for quorum; until it ships, map this control to your existing dual-authorization mechanism
AC-6	Least Privilege	Users and processes operate with the minimum privileges necessary	AI agent tool-access rings model: each agent gets scoped tokens with explicit allow-lists; PoP binds tokens to the requesting agent
AC-7	Unsuccessful Logon Attempts	The system limits and responds to unsuccessful authentication attempts	Wrong-DID rate, wrong-code rate, and per-identity backoff are designed as first-class signals to Overwatch (in development); rate limits and lockouts are policy-configurable
AC-12	Session Termination	The system terminates sessions on policy triggers	Revocation is designed to propagate to active sessions in seconds, not hours; in-flight handling is documented in the architecture
AU-2	Event Logging	Identifies the events the system logs	Structured event schema covering session start, challenge presentation, confirmation, success/fail, timeout, risk decisions, step-up outcomes, and approvals
AU-3	Content of Audit Records	Audit records contain sufficient information to investigate	Records include correlation IDs (SUID, ZID, DID/QID, kid, jti), channel, action, outcome, and verifier disposition
AU-12	Audit Record Generation	The system generates audit records for the events identified	Audit records are emitted at every state transition in the verifier; sensitive fields (values, biometric data) are excluded from logs by design
IA-2	Identification and Authentication, Organizational Users	Each user is uniquely identified and authenticated	SUID is the canonical organizational user identifier; authentication uses device-bound cryptographic primitives; IA-2(1) (multi-factor authentication to privileged accounts) and IA-2(2) (multi-factor authentication to non-privileged accounts) are addressable with phishing-resistant primary authentication
IA-4	Identifier Management	Identifiers are managed across their lifecycle	SUID assignment, ZID enrollment, identifier reuse policy, archival of retired identifiers are explicit lifecycle events
IA-5	Authenticator Management	Authenticators are managed through their full lifecycle, including rotation, revocation, and protection	Hardware-backed key storage; documented rotation overlap windows; revocation designed to propagate in seconds, not hours; identity-proofed recovery; documented in the architecture's Device Key Lifecycle section
IA-7	Cryptographic Module Authentication	Cryptographic modules used for authentication	TPM 2.0, Secure Enclave, and TEE-backed key storage on supported platforms; alignment with the W3C WebAuthn specification; RFC-compliant JWT, mTLS,

Control ID	Control name	What the control requires	How ScrambleID primitives contribute
		operate per approved standards	DPoP; FIPS-aligned cryptographic primitives where available
IA-8	Identification and Authentication, Non-Organizational Users	Non-organizational users are identified and authenticated	Federation via SAML and OIDC (Auth Code + PKCE); FAL-aligned assertion validation; consent-based attribute sharing through the Unified ID Card
IA-11	Re-Authentication	The system re-authenticates users on triggers	XFactor step-up chains (in development) for high-risk actions; session expiry and re-authentication policies; risk-triggered re-authentication via Overwatch when it ships
SC-8	Transmission Confidentiality and Integrity	Communications are protected	TLS for all client-verifier communication; signed challenges and confirmations; sender-constrained tokens for machine traffic
SC-12	Cryptographic Key Establishment and Management	Keys are managed through approved processes	Key generation in hardware-backed storage; documented rotation, escrow (where applicable), and destruction procedures
SC-13	Cryptographic Protection	Cryptographic mechanisms are implemented per organizational requirements	Standards-aligned algorithms (ES256, RS256, EdDSA); FIPS-aligned options where required

For controls outside the AC/AU/IA/SC families (CM, CP, CA, RA, SI, etc.), ScrambleID is one input among many. Compliance for those families is a property of the surrounding program, not the authentication platform.

CISA mapping

CISA guidance	What it means operationally	ScrambleID primitive
Phishing-resistant MFA (CISA fact sheet)	Authentication that cannot be completed by an attacker proxying or relaying the ceremony	WebAuthn UV plus QR(DID) with origin/session binding
No SMS/voice OTP for high-risk use cases	OTPs delivered via SMS or voice are vulnerable to SIM swap, AiTM relay, and carrier social engineering	XFactor (in development) is designed to exclude SMS/voice OTPs from high-risk chains; the platform's opinionated default rejects OTP fallback for password resets, payout changes, and admin operations
Rapid revocation of compromised authenticators	Compromised authenticators must be revocable in operationally relevant time	Decision and propagation across active sessions designed to complete in seconds, not hours; documented runbook
Strong identity proofing for high-assurance contexts	Proofing must be appropriate to the assurance level	Identity-proofed re-enrollment for cold-path recovery; step-up from existing devices for warm-path

CISA guidance	What it means operationally	ScrambleID primitive
Audit and incident response readiness	Authentication events are observable and responders can act	Structured event schema; cross-channel correlation and approval audit trails via Overwatch and Lockstep (both in development); runbook-driven incident response (Scattered Spider patterns)

Agentic AI framework mapping (2026)

The same questions auditors ask about human authentication are now being asked about agents. Three frameworks define that conversation; the mapping logic from the sections above carries over.

Compliance concept	What auditors mean operationally	ScrambleID primitive	Evidence to cite
OWASP ASI03: Identity & Privilege Abuse (Top 10 for Agentic Applications)	Can an agent act beyond its intended scope on leaked or inherited credentials?	Per-agent identity, per-call signatures, zero static secrets	/agents
OWASP ASI10: Rogue Agents	Would an unsanctioned or self-directed agent show up in your inventory and your audit trail?	Every authorized call carries a signed, attributable identity; unsigned calls have nothing to present	/agents, /actions
NIST NCCoE concept paper (Feb 2026): agent identity & authorization	Can each agent action be tied back to an accountable identity, auditably and non-repudiably?	Per-Action Authority: signature on every action, customer-verifiable hash chain	/actions
CSA AI Controls Matrix v1.0.3 (243 objectives, 18 domains)	Does your AI estate satisfy IAM-domain controls inherited from CCM?	Same primitives as the NIST 800-53 AC/IA rows above, extended to agent identities	the 800-53 section above

How AAL is actually determined

AAL is not a product capability. AAL is a **system property** that an auditor evaluates by reviewing the combination of:

- **Authenticator selection.** Which factors are required for which use cases.
- **Configuration.** TTLs, rotation overlap windows, lockout policies, replay caches, clock skew tolerance.
- **Operational controls.** Identity proofing for enrollment, recovery procedures, monitoring, incident response runbooks.
- **Independent assessment.** A SOC 2 Type II audit, a FedRAMP assessment, or a sector-specific audit by an authorized assessor.

ScrambleID can support an AAL3 design when configured with phishing-resistant primary authentication (WebAuthn UV or QR(DID) with origin/session binding), hardware-backed authenticators, and identity-proofed enrollment. ScrambleID can support an AAL2 design with looser configuration. The same product can also be configured below AAL2 if you allow weak fallbacks. The configuration is the design.

This is why "ScrambleID is AAL3" is the wrong framing. The right framing is: "we designed our deployment for AAL3 using ScrambleID's phishing-resistant primitives, hardware-backed authenticators, identity-proofed enrollment, fast revocation propagation, and the operational controls documented in our security plan."

Evidence package for an audit

When an auditor asks for evidence that the controls are operating, the typical package includes:

- **Architecture documentation.** This article plus the Architecture: Identity Fabric reference, customized to your deployment.
- **Configuration export.** Policies in effect, TTLs configured, factor chains, fallback restrictions, audit retention windows.
- **Operational runbooks.** Enrollment procedure, revocation procedure, recovery procedure, incident response procedure.
- **Audit logs.** Sample logs covering authentication, revocation, step-up, and approval events. The auditor will sample.
- **Independent assessment reports.** SOC 2 Type II report (or equivalent), penetration test results, FIDO Alliance certification status.
- **Personnel and training records.** Who is authorized to approve high-risk actions under your dual-control procedure, who is authorized to perform identity-proofed recovery, training completion records.

The product enables the design. The design plus operational controls plus the evidence package plus the auditor's judgment determines compliance.

> **On the roadmap, not in your evidence package:** XFactor (step-up chains), Lockstep (dual control), and Overwatch (cross-channel risk correlation) are in development. They appear in the mapping tables above as design-intent rows, marked "(in development)", so you can plan control coverage. Don't cite them as operating controls in an audit until they're deployed in your environment. Until then, map those rows to the step-up, approval, and monitoring mechanisms you run today.

NIST references (public)

- NIST Digital Identity Guidelines (SP 800-63-4): https://csrc.nist.gov/pubs/sp/800/63/4/final
- NIST SP 800-63-4 PDF: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-4.pdf
- NIST SP 800-53 Rev. 5 (Security and Privacy Controls): https://csrc.nist.gov/pubs/sp/800/53/r5/upd1
- W3C WebAuthn Level 2 (a common phishing-resistant origin-bound primitive): https://www.w3.org/TR/webauthn-2/
- FIDO Alliance Specifications: https://fidoalliance.org/specifications/

CISA references (public)

- CISA Phishing-Resistant MFA Fact Sheet: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- CISA: More Than a Password: https://www.cisa.gov/MFA
- CISA Cybersecurity Advisory AA23-320A (Scattered Spider): https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-320a

Key Takeaway

ScrambleID primitives can support NIST SP 800-63-4 AAL2 and AAL3 designs and align with CISA phishing-resistant MFA guidance through three core mechanisms: WebAuthn origin binding for web authentication, session-bound dynamic identifiers (DID/QID) for voice and cross-device flows, and proof-of-possession (mTLS via RFC 8705 or DPoP via RFC 9449) for machine identities. The platform commonly maps to NIST SP 800-53 controls in the AC, AU, and IA families. AAL is a system property determined by the combination of authenticator selection, configuration, operational controls, and auditor assessment, not a product capability alone. This article is a technical mapping for engineering and security audiences, not legal advice or a compliance attestation.

FAQ

Does ScrambleID guarantee a specific AAL?

No. AAL is determined by the combination of authenticator selection, configuration, operational controls, and an independent auditor's judgment. ScrambleID's primitives can support AAL2 and AAL3 designs when configured with phishing-resistant primary authentication, hardware-backed

authenticators, identity-proofed enrollment, and the operational controls described in this article. The same product can support a lower assurance level if weak fallbacks are configured. Your auditor of record assigns the AAL.

What is the difference between this mapping and a SOC 2 or FedRAMP attestation?

This mapping documents how ScrambleID primitives correspond to compliance concepts. SOC 2 and FedRAMP are attestations issued by independent assessors after evaluating your operating environment. Use this mapping to design your controls; use an independent assessor to attest to those controls.

Why is NIST 800-53 relevant if 800-63 is the authentication standard?

NIST SP 800-63 defines the conceptual model for digital identity (proofing, authentication, federation). NIST SP 800-53 defines the catalog of controls federal information systems use to operate. A federal-aligned authentication program typically references both: 800-63 for the model, 800-53 for the controls that satisfy specific requirements. The mapping above shows how ScrambleID primitives commonly contribute to the AC, AU, and IA control families.

Is "QR login" inherently safe?

Only when the QR encodes a signed, short-lived challenge, the approval is bound to the initiating session and origin, and the user types a short code that binds human intent. That is the DID/QID model. A QR that is just a URL the user blindly approves is not phishing-resistant. The Phishing-Resistant Web Authentication article covers the failure modes.

Do we still need monitoring if we have phishing-resistant MFA?

Yes. Phishing-resistant authentication reduces certain classes of takeover (AiTM, password phishing, OTP relay), but monitoring catches abuse, misconfiguration, insider threats, and cross-channel attacks that bypass authentication entirely (compromised admin accounts, social engineering of agents, account recovery abuse). Overwatch, in development, is designed to provide this layer; until it ships, your SIEM carries it.

How do industry-specific frameworks (HIPAA, PCI DSS, SOX, ISO 27001, FedRAMP) map?

This article does not cover them. Industry-specific mappings will appear in a dedicated article. As a starting point: HIPAA references NIST 800-66 which itself references 800-63; PCI DSS 4.0 requires phishing-resistant authentication for sensitive contexts; SOX inherits from your COSO/ISO framework; ISO 27001:2022 Annex A controls have direct correspondences with NIST 800-53. Consult your auditor of record for sector-specific guidance.

Do the agentic frameworks (OWASP, NCCoE, CSA) require separate controls from NIST 800-63?

No. They extend the same identity outcomes to non-human actors: each agent needs its own identity (not a shared service account), authority scoped per action, and an audit trail that ties every action to an accountable identity. If your authentication design already satisfies the 800-63 and 800-53 rows above with per-agent identities and signed actions, the agentic mappings inherit it.

Related reading

- Evaluation Checklist + RFP
- Phishing-Resistant Web Authentication
- Caller Authentication

References (public)

- NIST SP 800-63-4 Digital Identity Guidelines: https://csrc.nist.gov/pubs/sp/800/63/4/final
- NIST SP 800-63B Authentication and Lifecycle Management: https://csrc.nist.gov/pubs/sp/800/63b/4/final
- CISA Phishing-Resistant MFA Fact Sheet: https://www.cisa.gov/sites/default/files/publications/fact-sheet-implementing-phishing-resistant-mfa-508c.pdf
- CISA More Than a Password: https://www.cisa.gov/MFA
- W3C Web Authentication (WebAuthn) Level 2: https://www.w3.org/TR/webauthn-2/
- FIDO Alliance Specifications: https://fidoalliance.org/specifications/
- OWASP GenAI Security Project, "OWASP Top 10 for Agentic Applications" (December 2025): https://genai.owasp.org/
- NIST NCCoE, "Accelerating the Adoption of Software and Artificial Intelligence Agent Identity and Authorization" concept paper (February 2026): https://csrc.nist.gov/pubs/other/2026/02/05/accelerating-the-adoption-of-software-and-ai-agent/ipd
- Cloud Security Alliance, "AI Controls Matrix" v1.0.3: https://cloudsecurityalliance.org/artifacts/ai-controls-matrix