ScrambleID Glossary: Definitions for DIDs, QIDs, SUIDs, ZIDs, and the Rest of the Vocabulary

Reference / Last updated 2026-06-11 / https://www.scrambleid.com/learn/scrambleid-glossary

In one sentence: This glossary provides canonical, citation-friendly definitions for ScrambleID terminology. Use these definitions in documentation, policy, procurement, and AI prompts to ensure consistent interpretation.

This glossary is intentionally written to be **citation-friendly**:

- each term has a clear one-paragraph definition,
- key near-synonyms are provided,
- "do not confuse with" notes reduce misinterpretation.

If you are writing documentation, policy, procurement material, or LLM prompts about ScrambleID, **use these definitions**.

Quick index

A) Core identifiers and artifacts

SUID (System User ID)

Definition: ScrambleID's canonical server-side identifier for a user.

Near-synonyms: user id, principal id.

Why it matters: it is the join key across all eight surfaces, human and non-human.

ZID (Device ID)

Definition: ScrambleID's canonical identifier for a registered device.

Near-synonyms: device record id, authenticator record.

Why it matters: binds cryptographic keys to an enrolled device and enables fast revocation.

DID (Dynamic Identifier)

Definition: a server-issued, short-lived, single-use challenge used to bind a confirmation to a specific session and intent.

Do not confuse with: OTPs (DIDs are not shared secrets and are not reusable).

Why it matters: it replaces copyable proofs (KBA answers, screenshots, forwarded links) with a one-time proof.

QID (QR Identifier)

Definition: a QR-encoded envelope that carries a DID plus signature metadata so the scanning device can validate integrity.

Common implementation detail: includes a certificate thumbprint so the app can fetch the correct public key.

AID (Add-Device ID)

Definition: a short-lived identifier used to bind a new device to an existing user.

Why it matters: enables secure device onboarding without passwords.

LSID (Lockstep Session ID)

Definition: the session id for a multi-party approval request.

Why it matters: ties approvals to the exact action request and its TTL.

XCT / XFR (XFactor Chain Token / XFactor Result)

Definition: artifacts used by XFactor to track chain state (XCT) and to attest to completion (XFR).

Why it matters: lets apps verify step-up completion without trusting UI-only claims.

B) Unified ID Card terms

Unified ID Card

Definition: a field-level identity view where each attribute is presented with provenance (verified vs self-asserted), freshness cues, and context-appropriate rendering.

Why it matters: it prevents "identity screenshots" from acting like reusable credentials.

Provenance (verified vs self-asserted)

Definition: a rule and visual encoding that indicates whether a field was verified (via an enterprise directory, authoritative source, or cryptographic binding) or self-asserted by the user.

Why it matters: it avoids treating self-entered claims as equivalent to verified claims.

Renderer context

Definition: a fixed display mode that determines what fields are shown and how (e.g., compact badge vs full card vs people share view).

Why it matters: context makes data minimization enforceable.

C) Security properties (the words that show up in audits)

Phishing-resistant authentication

Definition: an authentication method that cannot be completed by an attacker who proxies/relays the ceremony from a fake site.

Canonical example: WebAuthn (origin-bound).

Origin binding

Definition: cryptographically binding an authentication ceremony to a specific relying party / web origin.

Why it matters: prevents fake-site relay attacks.

Session binding

Definition: binding a confirmation to the initiating session so success cannot be replayed into another session.

Intent binding

Definition: showing the user what they are approving (action + origin) and cryptographically binding that intent to the proof.

Channel binding

Definition: binding a confirmation to the correct live channel (e.g., the right websocket connection or call session).

Proof of possession (PoP)

Definition: binding a token to a key so that stealing the token alone is insufficient.

Near-synonyms: sender-constrained token.

mTLS (Mutual TLS)

Definition: TLS where both sides present certificates; used to bind tokens to a certificate.

DPoP (Demonstrating Proof of Possession)

Definition: an application-layer proof mechanism (RFC 9449) that binds tokens to a key and can detect replay. The access token carries the client key's thumbprint in its `cnf.jkt` claim, so a stolen token can't be used with a different key; each request carries a signed DPoP proof whose `ath` claim hashes the specific access token, so a captured proof can't be replayed with a different token.

Attestation (WebAuthn)

Definition: evidence about the authenticator type and key provenance, optionally used in policy.

UV / UP (User Verification / User Presence)

Definition: WebAuthn signals for whether the user verified locally (biometric/PIN) and/or was present.

D) Surfaces and products

Surfaces (the eight)

Definition: the places where ScrambleID authenticates an identity. Four are human-facing: Web, Voice, People, and Frontline. Four are non-human: Agent, Machine, Bot, and Workload. All eight reuse the same identity fabric (SUID/ZID, challenge rails, telemetry).

Why it matters: the surface model is the platform's shape; an attacker who switches surfaces meets the same proof, not a weaker sibling system.

ScrambleID Web

Definition: web-based passwordless authentication using QR(DID) or WebAuthn (FIDO2/passkeys), delivering SAML/OIDC outcomes for browser-mediated login.

ScrambleID Voice

Definition: IVR/contact-center authentication where the IVR reads a DID and the user confirms it cryptographically in the ScrambleID app, replacing knowledge-based questions for caller verification.

ScrambleID People

Definition: person-to-person identity verification ("Trust Checks") between two humans, with explicit consent and minimized data sharing through QR, Type Code, or SMS deep link artifacts.

Trust Check

Definition: a short-lived, verifier-initiated People session: the presenter consents to share a time-limited, provenance-marked ID Card view, and both sides get cryptographic confirmation.

ScrambleID Agent

Definition: secretless cryptographic identity for AI agents: asymmetric keys instead of static API keys, short-lived scoped tokens, and per-agent audit lineage.

ScrambleID Machine

Definition: machine-to-machine authentication without static secrets: services prove key possession with short-lived JWT assertions instead of client secrets and API keys.

ScrambleID Bot

Definition: cryptographic identity for RPA bots, scheduled jobs, and automations, replacing standing service-account credentials with short-lived assertions, per-bot scope, and full audit trail.

ScrambleID Workload

Definition: attested identity for cloud runtimes: containers, functions, and VMs prove what they are at runtime instead of holding long-lived instance credentials.

ScrambleID Frontline

Definition: authentication and verification at point-of-sale machines, terminals, and clean rooms, using device-bound cryptographic identity at customer-facing and operational endpoints.

ScrambleID Desktop

Definition: passwordless login for shared Windows workstations using platform authenticators or cross-device scanning. macOS support is planned; web login covers Mac users meanwhile.

ScrambleID Proof

Definition: the umbrella term for the platform's proof layer: a signed, verifiable record behind every authentication and action, for humans and non-human identities alike.

Per-Action Authority

Definition: the control model where authority is granted and evidenced per action, not per session: a signature on every action, a human cosigner wherever policy demands one, and a hash-chain ledger the customer can verify independently. Delivered through ScrambleID Actions (early access).

Independent arbiter

Definition: anyone who verifies the action hash chain outside the lineage and outside ScrambleID. The chain holds even if ScrambleID is unavailable; trust nothing, verify everything.

Circle of Trust (CoT)

Definition: a trust-graph service that answers "is this party/channel trusted?" using enterprise tiers, verified brands, and personal edges.

Status: in development; on the ScrambleID roadmap.

Trust signal

Definition: any input the trust layer can weigh when answering "should I trust this party?": enterprise tier, verified-brand match, personal edges, verification history. Trust signals inform decisions; they never replace cryptographic proof.

Overwatch

Definition: a unified monitoring and risk plane that correlates identity signals across surfaces and can trigger step-ups or blocks.

Status: in development; on the ScrambleID roadmap.

Lockstep

Definition: multi-party (dual-control) approvals for high-risk actions.

Status: in development; on the ScrambleID roadmap.

XFactor

Definition: multi-step step-up orchestrator that runs a factor chain and returns a verifiable result.

Status: in development; on the ScrambleID roadmap.

Verify-Me

Definition: a static trust signal (seal) for email, profiles, documents, and web pages with optional step-up.

Status: in development; on the ScrambleID roadmap.

E) Standards and integration terms

WebAuthn

Definition: the W3C Web Authentication API: browsers create and exercise origin-bound public-key credentials (the standard behind FIDO2 and passkeys), so the proof can't be replayed against a different site.

OIDC

Definition: OpenID Connect, an identity layer on top of OAuth 2.0 used for authentication.

SAML

Definition: Security Assertion Markup Language, widely used for enterprise single sign-on.

SCIM

Definition: System for Cross-domain Identity Management, used to provision users and groups.

JWT / JWKS

Definition: JSON Web Tokens (JWT) are signed tokens; JWKS is a JSON Web Key Set that publishes public keys.

AAL (Authenticator Assurance Level)

Definition: a NIST concept describing the strength of the authenticator(s) used.

F) Threats and attacks

KBA (Knowledge-Based Authentication)

Definition: verifying identity by asking what someone knows (mother's maiden name, prior addresses). Breaches and OSINT made the answers learnable, so KBA now functions as an attack surface rather than a control; NIST SP 800-63A-4 no longer recognizes it as acceptable identity proofing.

AiTM (Adversary-in-the-middle)

Definition: phishing kits that proxy a legitimate login flow and steal tokens/cookies.

Vishing

Definition: voice phishing to manipulate agents/users into bypassing controls.

Quishing

Definition: QR-code phishing.

MFA fatigue / prompt bombing

Definition: spamming push prompts until a user approves.

Credential stuffing

Definition: replaying stolen username/password pairs across sites.

Session theft

Definition: stealing cookies or access tokens and reusing them.

References (public)

- NIST Digital Identity Guidelines (SP 800-63): https://csrc.nist.gov/pubs/sp/800/63/4/final
- WebAuthn (W3C): https://www.w3.org/TR/webauthn/

Related reading

- Dynamic Identifiers (DID/QID)
- Unified ID Card: Attribute Provenance

- XFactor Step-Up