SIG ONE

August 2026 · v1.0

TECHNICAL WHITEPAPER

The Engineering of Passwordless Trust

How SIG ONE's BSA (Blockchain Secure Authentication) establishes trust with no stored secret — no passwords, no OTP, no tokens. This paper explains the four-layer trust chain.

Company **SigOne Co., Ltd.**

Site **www.sigone.net**

SUMMARY

BSA does not rely on stored secrets. It establishes trust with one-time material and keys that are created for each authentication and discarded immediately, and with distributed verification by randomly selected nodes. The one-way trust chain — Material (MIRC) → Key (OTAK) → Verification (MDV) → Ledger (Hybrid DLT) — is a pipeline in which each stage consumes the output of the previous stage and leaves nothing behind. There is no asset to steal and no single point to seize.

MIRC Material › **OTAK** Key › **MDV** Verification › **Hybrid DLT** Ledger

DESIGN RATIONALE · THE PROBLEM

Every authentication attack starts from two structural premises

Instead of blocking each attack technique one by one, BSA's design goal is to remove the common premises that make those techniques possible — from the structure itself.

VULNERABILITY 01

A fixed credential exists

As long as a fixed asset (password, key) that can be stored, reused, and stolen exists, the following attacks keep working.

ENABLED ATTACKS

Phishing · Credential stuffing · Password DB theft · MITM replay

VULNERABILITY 02

A single verification point exists

When verification is concentrated at one point, seizing that single point alone is enough to manipulate the entire authentication result.

ENABLED ATTACKS

Verification server breach · Insider tampering · Single point of failure (SPOF)

DESIGN PRINCIPLES

Leave no asset to steal · Trust no single point

PRINCIPLE 01

Leave no asset to steal

No fixed asset that can be stored, reused, or stolen is left behind. Material is randomly combined per request (MIRC), and keys are generated per request and discarded immediately (OTAK).

PRINCIPLE 02

Trust no single point

Verification and record-keeping are distributed so that seizing one point cannot determine the whole result. Judgment is made by the consensus of randomly selected nodes (MDV), and records are split across Public and Private chains (Hybrid DLT).

MECHANISM

The Four-Layer Trust Chain

Material → Key → Verification → Ledger. The output of each stage becomes the input of the next, and no stage passes a reusable asset forward.

LAYER 01 · MATERIAL **MIRC**

Randomly combines multiple identifiers into unpredictable material

Rather than a single secret, a subset is randomly selected and combined for each request from a set of different identifiers — ownership (registered device), device, location, knowledge/biometrics. Even for the same user, the material differs per request, so observation and reproduction do not hold.

What it leaves behind: **A stored fixed identifier combination**

LAYER 02 · KEY **OTAK**

Generates a one-time key per request and discards it right after authentication

The lifetime of the key is limited to a single request window. A key of 300+ characters passes through multi-stage encryption (generate → reduce → merge, encrypted at each step) and vanishes immediately after the result is returned. Even if stolen, no moment is left to use it.

What it leaves behind: **A reusable key**

LAYER 03 · VERIFICATION **MDV**

Verifies through the consensus of randomly selected multiple nodes

Verification authority is not placed in one location. Randomly selected nodes verify in parallel at the same time and judge by a predefined consensus rule. An attacker cannot designate the verification nodes in advance, and seizing one node cannot sway the result.

What it leaves behind: **A manipulable single verification point**

LAYER 04 · LEDGER **Hybrid DLT**

Public and Private chains split roles to preserve immutable records

The Public chain handles open verification and anonymity, while the Private chain handles authentication processing and immutable records — the two complement each other. The exposure or damage of one cannot replace the trust of the other, and the authentication fact remains as an immutable record for later cross-checking.

What it leaves behind: **A forgeable single ledger**

ASSURANCE

Structural defense against four threats

BSA's defense holds by structure, not by probability. For an attack to succeed, it would need an asset or a point that does not exist.

✔ Anti-forgery

To forge the material, an attacker must simultaneously match ownership, device, location, knowledge/biometrics and the random combination at that exact request moment. Obtaining one is useless if the rest and the timing combination do not match.

✔ Anti-reuse

The key's lifetime is only the single request window. By the time an attacker obtains the key it is already discarded, and the next request uses a different key. There is nothing to reuse.

✔ Anti-tampering

Verification is distributed across randomly selected nodes. No node can be designated in advance or decide the result alone, and partial seizure is nullified by consensus.

✔ Non-repudiation

Authentication results are preserved as immutable, transparent records on the Hybrid DLT, so the authentication fact can be cross-checked and proven afterward. Biometric originals and fixed passwords are never stored in the first place.

STANDARDS & CERTIFICATIONS

Already validated by the world's highest authorities

BSA is adopted as a UN-affiliated international standard and validated by international security certifications and a global award — which is why you don't need to validate it yourself.

- ✔ **ITU-T X.1284 · X.1286**
  Adopted as an ITU-T international standard (UN agency)
- ✔ **TTAK.KO-12.0411**
  Enacted as a national standard
- ✔ **Common Criteria EAL2**
  International Common Criteria certification
- ✔ **Patents · 8 countries**
  Core technology patents registered

Ready to start a technical review?

Detailed technical specifications — consensus thresholds, key length, cryptographic algorithms, entropy sources — are provided separately as a technical specification upon a security-review request.