SAFERSIM

CUSTOMER WHITE PAPER · JULY 2026

Enterprise identity, secured in the eSIM.

A user-held, hardware-backed trust layer for workforce login, certificates and high-security physical access.

SaferSIM turns the eUICC already inside the employee's phone into a reusable enterprise identity. Instead of adding another password store or authenticator app, the profile, private key, local approval and lifecycle remain bound to hardware that travels with the employee. An optional app can add richer interaction while the key stays in the eSIM.

Why the eSIM changes the identity model

USER-HELD IDENTITY	LOCAL AUTHORIZATION	ENTERPRISE LIFECYCLE
Profile, private key and consent remain hardware-protected with the employee.	Service, purpose and SaferSIM PIN are verified on the phone - no consumer app required.	Provision, rotate, suspend and revoke one reusable identity across access paths.

How a SaferSIM decision is created

1	**Request.** The enterprise service creates a fresh, purpose-bound challenge.
2	**Route.** The SaferSIM Server validates the relying party and routes the request to the employee's eSIM.
3	**Approve.** The employee sees the context and enters the SaferSIM PIN locally on the phone.
4	**Prove.** The eUICC returns a signed, replay-protected result to the IdP, application, VPN gateway or PACS.

LAYERED SECURITY MODEL

HTTPS interfaces support TLS 1.3. **The eUICC runtime channel** uses authenticated BIP/TCP with HMAC-SHA-256 and P-256 signatures. **Production provisioning** uses SCP03/AES or the provider-equivalent protected process; the pilot validates the final AEAD confidentiality profile on the selected eUICC and carrier combination.

One identity. From login to building access.

Deploy the highest-value workflow first, then extend the same hardware-backed profile across digital and physical access.

1 WORKFORCE ACCESS

SSO + optional VPN

The user sees service and purpose, enters the SaferSIM PIN and returns an eSIM-signed proof.

OIDC / SAML · optional RADIUS

Outcome: One approval path for office, home and mobile work.

2 CERTIFICATE LOGIN

Entra ID + managed PCs

The SaferSIM PC Connector routes the certificate challenge. The non-exportable eSIM key signs it.

Microsoft Entra ID · X.509

Outcome: No private key stored on the PC.

3 HIGH-SECURITY ACCESS

Badge/app + PIN + face

Identity, local PIN approval and independent face/liveness verification are bound into one assertion.

PACS adapter · biometric service

Outcome: The existing access system keeps the final decision.

High-security access: identity, intent and presence

HIGH-SECURITY FLOW

Four signals. One bound decision.

01 IDENTIFY
Badge, app or employee credential identifies the access request.

02 APPROVE
The user confirms the displayed context with the SaferSIM PIN on the phone.

03 VERIFY
An independent service performs face and liveness verification.

04 DECIDE
The eSIM binds the factors into a signed assertion; the PACS makes the final access decision.

Privacy by design

The optional biometric reference can remain non-exportable in the eSIM. Matching, liveness, consent and retention are validated for the customer's policy and jurisdiction.

SAFERSIM

TECHNICAL ARCHITECTURE

Designed to integrate. Built to preserve control.

SaferSIM adds a user-held hardware trust layer while the customer's IdP, VPN gateway, application or PACS remains authoritative.

End-to-end trust chain

1 RELYING PARTY

SSO, VPN, Entra ID, PC Connector or PACS

Creates a fresh request with service, purpose and policy context.

2 SAFERSIM SERVER

Validation, routing and lifecycle

Checks the customer and request, routes the challenge and retains auditable evidence.

3 PHONE + eUICC

Display, local PIN and non-exportable key

The user approves locally; the P-256 key signs the bound response inside the eSIM.

4 ENTERPRISE DECISION

IdP, gateway, application or PACS

Verifies the assertion and remains the final authorization point.

Channels, cryptography and explicit boundaries

INTERFACE	MECHANISM	SECURITY PROPERTY	SCOPE / BOUNDARY
Enterprise web / API	HTTPS with TLS 1.3	Confidentiality, server authentication and transport integrity	Applies to SaferSIM web and API endpoints.
eUICC runtime	BIP/TCP, HMAC-SHA-256 and P-256 signatures	Message authentication, integrity, replay protection and device proof	Pilot payload confidentiality is not assumed. The production AEAD profile is qualified per eUICC and MNO combination.
Profile provisioning	SCP03/AES or provider-equivalent protected process	Protected profile and key loading plus lifecycle operations	Provisioning path only; SCP03 is not described as the runtime channel.
Enterprise federation	X.509, OIDC, SAML, optional RADIUS and PACS adapter	Interoperability with the existing identity and access estate	SaferSIM adds hardware-bound approval; enterprise policy remains authoritative.

Standards, devices and lifecycle

eUICC, devices and standards

GSMA SGP.21/22/23/25 · eSA / SGP.07 · GlobalPlatform SCP03 · ETSI TS 102 223 · 3GPP TS 31.111 · SAS-UP / SAS-SM

Designed for supported Android and iOS eUICC devices. App-free approval is the core path; an optional app can add richer biometric interaction.

Keys, lifecycle and assurance

Non-exportable P-256 key · local SaferSIM PIN · fresh challenges · expiry and replay protection · provision, rotate, suspend and revoke

Certification evidence is checked for the selected eUICC platform, regional SKU, production site and provisioning provider; this is not a blanket SaferSIM product certification.

Production qualification is performed against the exact eUICC, regional device SKU, firmware, MNO and provisioning-provider combination selected for rollout.

RECOMMENDED PAID PILOT

8 weeks · 50 users · one primary integration · selected deployment devices

Acceptance covers completion rate, end-to-end response time, suspend/revoke lifecycle, audit evidence and user feedback. Exact eUICC, MNO, regional SKU, firmware and provisioning combinations are qualified before rollout.

Choose one workflow. SaferSIM delivers a fixed-price statement of work within five business days.

kratz@safersim.com · wulf@safersim.com · safersim.com

References: GSMA SGP.21/22/23/25 and SGP.07 · GlobalPlatform SCP03 Amendment D · ETSI TS 102 223 · 3GPP TS 31.111 · OpenID Connect Core 1.0 · OASIS SAML 2.0.