Glide identity

Glide Identity Authentication System

NIST AAL2 Compliance Document

Version:	**0.2**
Date of version:	**October 17th , 2025**
Approved By:	**Eran Haggiag**
Confidentiality Level:	**Share with NDA**

Change Control

Date	Name	Version	Change description
13-10-2025	Shai Sivan	0.1	First Version
17-10-2025	Eran Haggaig	0.2	Approval

Table of Contents

1 introduction 3
1.1 Key Security Properties 3
2 AAL2 Compliance Status 3
3 Hardware Security Foundation 4
3.1 Private Key Storage Architecture 4
3.2 Physical SIM Cards 4
Security Properties: 4
• Private keys stored in tamper-resistant hardware separate from device CPU/memory 4
• Keys generated within SIM and never leave in plaintext 4
• Separate execution environment - only OS and carrier have controlled access 4
• Tamper-evident: Physical opening destroys keys 4
• Non-exportable: Even on rooted/jailbroken devices, keys remain protected 4
3.3 Key Security Guarantees 4
4 NIST 800-63B-4 AAL2 Compliance Mapping 5
4.1 AAL2 Requirements Summary 5
5 Comparison to Traditional Authentication 6
5.1 Traditional MFA vs. Glide Identity 6
6 Attack Scenario Comparisons 11
6.1 Scenario 1: Sophisticated Phishing Attack 11
6.2 Scenario 2: SIM Swap Attack 12
6.3 Scenario 3: Malware on User's Device 13
6.4 Scenario 4: Attacker on same network 14

1 introduction

Glide Identity provides a phishing-resistant, hardware-backed cryptographic authentication system that meets and exceeds NIST SP 800-63B-4 (July 2025) Authenticator Assurance Level 2 (AAL2) requirements.

1.1 Key Security Properties

- **Phishing Resistant:** Cryptographic challenge-response bound to verifier identity
- **Replay Resistant:** Single-use nonces with cryptographic binding
- **Hardware-Backed:** Private keys in tamper-resistant SIM/eSIM secure elements
- **Origin-Bound:** JWT/OIDC claim prevents relay attacks
- **Risk-Aware:** Real-time fraud signals integrated with authentication
- **Standards-Compliant:** NIST 800-63B-4 AAL2, OpenID4VP, GSMA TS.43(entitlement config spec).

2 AAL2 Compliance Status

Requirement	Status	Evidence
3.1.6.1: Approved cryptography	**COMPLIANT**	ES256, EAP-AKA', AES-128-GCM, SHA-256
3.1.6.1: Hardware-based key storage	**COMPLIANT**	SIM/eSIM secure elements, tamper-resistant
3.2.5: Phishing resistance	**COMPLIANT**	Verifier name binding (JWT/OIDC)
3.2.7: Replay resistance	**COMPLIANT**	Single-use nonces, server-side tracking

2.2.1: Multi-factor authentication	**COMPLIANT**	Cryptographic + biometric/other

3 Hardware Security Foundation

3.1 Private Key Storage Architecture

The security foundation of Glide Identity's authentication system is hardware-backed private key storage in tamper-resistant secure elements. This ensures keys can't be extracted, even by sophisticated attackers

3.2 Physical SIM Cards

Security Properties:

- Private keys stored in tamper-resistant hardware separate from device CPU/memory
- Keys generated within SIM and never leave in plaintext
- Separate execution environment - only OS and carrier have controlled access
- Tamper-evident: Physical opening destroys keys
- Non-exportable: Even on rooted/jailbroken devices, keys remain protected

3.3 Key Security Guarantees

Property	Physical SIM	iOS eSIM	Android eSIM
Key Storage Location	SIM hardware	Secure Enclave	eUICC + StrongBox
Key Extractability	Never	Never	Never
Tamper Protection	Physical destruction	Hardware + secure boot	TRE + attestation

Device Binding	SIM hardware	Secure Enclave	eUICC hardware
Rooted Device Protection	Yes	Yes	Yes (If StrongBox)

4 NIST 800-63B-4 AAL2 Compliance Mapping

4.1 AAL2 Requirements Summary

Requirement	NIST Reference	Status	Evidence
Multi-factor authentication	2.2.1	**COMPLIANT**	Single-factor cryptographic (SIM) + biometric/password
Approved cryptography	2.2.2	**COMPLIANT**	ES256, AES-128-GCM, SHA-256, FIPS approved
Replay resistance	2.2.2	**COMPLIANT**	Single-use nonces, challenge-response protocol
Authentication intent	2.2.2	**COMPLIANT**	consent required per auth
Authenticated protected channel	2.2.2	**COMPLIANT**	TLS 1.2+, mutual authentication

Phishing-resistant option	2.2.2	**COMPLIANT**	Passwordless cryptography
Reauthentication timeout	2.2.3	**COMPLIANT**	Configurable (≤ 24h and inactivity ≤ 1h recommended in AAL2)

5 Comparison to Traditional Authentication

5.1 Traditional MFA vs. Glide Identity

Aspect	Password + SMS OTP	Password + TOTP App	SNA (Silent Network Auth)	Glide Identity
Security				
Phishing Resistant	Both factors phishable	Both factors phishable	Partial - IP validation only	**Origin-bound cryptographic**
Replay Resistant	OTP time-limited (60s)	OTP time-limited (30s)	Session-based, time-limited	**Single-use nonces (10min)**
Hardware-Backed	Software-only	Software-only	SIM-based (passive check)	**SIM/eSIM secure element (active crypto)**

SIM Swap Protection	Vulnerable	Not affected by SIM swap	Detection only (carrier API)	**SIM Swap Detection**
Endpoint Compromise	Both factors stealable	TOTP secret exportable	Session hijacking possible	**Keys non-exportable**
Man-in-the-Middle	Vulnerable (relay attack)	Vulnerable (relay attack)	IP spoofing possible	**Origin binding Server side call**
Mobile Network Dependency	High (SMS delivery)	Low (offline TOTP)	High (carrier API required)	**No (Any internet connection)**
Privacy Protection	Phone# exposed to SMS gateway	No phone# exposure	Phone# + IP shared with carrier	**Encrypted** **(Hashed Optional)**
User Experience				
Authentication Time	3-60 seconds	Manual	3-20 seconds (silent check)	**<2s**
User Steps	4 steps (password + wait + code + submit)	3 steps (password + open app + code)	1-2 steps (may require consent prompt)	**1-2 steps (OS consent + optional biometrics)**

Device Required	Phone (SMS capable)	Phone with TOTP app	Phone (mobile data required)	**Phone (built-in SIM/eSIM + internet connection)**
Mobile Network Required	Yes (SMS delivery)	No (offline TOTP)	Yes (mobile data)	No (Any internet connection)
Error Rate	High (SMS delays, typos)	Medium (time sync issues)	Medium (network errors, timeouts)	**Low (99%+ success rate for supported carriers)**
User Friction	High (wait for SMS, manual entry)	Medium (app switching)	Low-Medium (background check, may prompt)	**Very Low (one-touch + optional biometric)**
Operational				
Carrier Integration	None (SMS only)	None required	Direct carrier API integration	**Direct network integration**
Deployment Complexity for carrier	Low (SMS gateway only)	Low (app-based)	Medium-High (carrier partnerships)	High (network integration)
Compliance				

NIST AAL2	Doesn't meet the new rev 4 phishing resistant option	Doesn't meet the new rev 4 phishing resistant option	Questionable - lacks cryptographic binding	**Compliant (phishing-resistant)**
PCI DSS	Accepted	Accepted	May not meet requirements	**Preferred (hardware-backed)**
GDPR Privacy	Phone# storage concerns	Compliant	Phone# + IP shared with 3rd party	**Privacy-preserving (E2E encrypted)**
Phishing-Resistant (3.2.5)	No	No	No (IP validation insufficient)	**Yes**
Hardware Authenticator (3.1.6)	No	No	No (SIM not used for crypto)	**Yes (SIM/eSIM secure element)**
Authentication Intent (3.2.8)	Partial (not OS dialog)	Partial (not OS dialog)	No (silent/passive)	**Yes**

6 Attack Scenario Comparisons

6.1 Scenario 1: Sophisticated Phishing Attack

Setup: Attacker creates phishing site (nike-secure-login.com), user receives email: "Your order requires verification"

Method	Attack Flow	Result
Password + SMS OTP	1. User enters password on phishing site → COMPROMISED 2. Phishing site relays to real Nike.com 3. User receives SMS OTP 4. User enters OTP on phishing site → COMPROMISED 5. Attacker relays OTP within validity window	**ATTACK SUCCESSFUL Full credential theft**
SNA (Silent Network Auth)	1. Phishing site initiates SNA check 2. SNA validates phone# via carrier API 3. Carrier checks SIM presence (passive) 4. IP address validated (can be spoofed via VPN/proxy) 5. Session token issued to phishing site 6. Attacker uses token on real site (session hijacking)	**ATTACK SUCCESSFUL IP validation insufficient**
Glide Identity	1. User clicks "Login with Phone" on phishing site 2. Chrome generates request with origin: "nike-secure-login.com" 3. Glide issues JWT with aud: "nike-secure-login.com" 4. User presents biometric (unaware of phishing) 5. VP generated with domain: "nike-secure-login.com" 6. VP proof cryptographically bound to phishing domain 7. Glide validates: Expected "nike.com" ≠ VP "nike-secure-login.com" 8. MISMATCH DETECTED	**ATTACK PREVENTED Origin binding blocks relay**

6.2 Scenario 2: SIM Swap Attack

Setup: Attacker socially engineers carrier to port victim's phone number to attacker's SIM

Method	Attack Flow	Result
Password + SMS OTP	1. Attacker has victim's password (previous breach) 2. Attacker attempts login with password 3. SMS OTP sent to victim's number (now attacker's SIM) 4. Attacker receives OTP on their device 5. Attacker enters OTP and completes authentication	**ATTACK SUCCESSFUL** **Full account takeover**
SNA (Silent Network Auth)	1. Attacker ports victim's number to their SIM 2. Attacker initiates SNA authentication 3. SNA checks with carrier API 4. Carrier reports: SIM swap detected (if checking enabled) 5. SNA returns risk signal: sim_swap = true 6. **BUT:** Phone number is now on attacker's device 7. **AND:** No cryptographic binding to victim 8. Session validation passes (depends on merchant policy)	**PARTIAL PROTECTION** **Detection only, policy-dependent**

Glide Identity	1. Attacker ports victim's number to their SIM 2. Glide calls telco API for verification 3. Telco returns: SIM swap detected, days_since_swap = 0 4. Glide returns risk signal: sim_swap.detected = true 5. PayPal policy: DENY (SIM swap < 7 days) 6. **Additionally:** Attacker's NEW SIM has NEW private key 7. **Original victim's private key** remains on old SIM 8. Attacker cannot generate valid signatures with victim's key 9. Even without risk signal, cryptographic auth would fail	**ATTACK PREVENTED** **Risk signal + crypto binding**

6.3 Scenario 3: Malware on User's Device

Setup: User downloads malicious app with keylogger, SMS reader, and network interceptor

Method	Attack Flow	Result
Password + SMS OTP	1. Malware keylogger captures password as user types 2. Malware SMS reader intercepts OTP 3. Attacker has both factors in real-time 4. Attacker can authenticate from any device 5. Victim unaware of credential theft	**ATTACK SUCCESSFUL** **Complete credential theft**
SNA (Silent Network Auth)	1. Malware intercepts SNA session token 2. SNA operates silently (no user prompt) 3. Malware can proxy authentication requests 4. Attacker uses session token for API calls 5. No cryptographic keys to protect 6. Victim completely unaware (silent authentication)	**ATTACK SUCCESSFUL** **Silent token theft**

Glide Identity	1. Malware attempts to export SIM private key 2. Key stored in secure element (Secure Enclave/StrongBox) 3. Secure element isolated from main OS and apps 4. No API exists to export keys (even with root access) 5. Malware can only proxy authentication (not steal credentials) 6. User must present biometric for EACH authentication 7. BiometricPrompt dialog visible to user (cannot be hidden) 8. User aware of authentication attempts	**ATTACK MITIGATED** **Keys secure, user aware**

6.4 Scenario 4: Attacker on same network

Setup: Attacker on same network (public Wi-Fi) attempts to intercept session

Method	Attack Flow	Result
Password + SMS OTP	1. User authenticates on public Wi-Fi 2. Attacker intercepts session cookie (if not secure) 3. Attacker replays session cookie 4. Access granted until session expires	VULNERABLE Depends on session security
SNA (Silent Network Auth)	1. SNA validates via carrier network (separate from Wi-Fi) 2. Session token issued over HTTPS 3. Attacker intercepts encrypted traffic 4. Cannot decrypt without session keys 5. BUT: No origin binding or device binding 6. Token usable from any IP if intercepted	PARTIAL PROTECTION TLS only, no device binding
Glide Identity	1. All traffic encrypted with TLS 1.2+ (PFS) 2. VP cryptographically bound to origin 3. Session bound to specific merchant (PayPal API key) 4. Nonce single-use, cannot be replayed 5. Even if traffic intercepted, cannot decrypt 6. Cannot use VP on different origin 7. Cannot reuse nonce for new session	ATTACK PREVENTED Multiple layers of protection