Glide identity

Glide Identity Trust Kit

Version:	**1.0**
Date of version:	**October 23th , 2025**
Approved By:	**Shai Sivan**
Confidentiality Level:	**Share with NDA**

Table of Contents

1 Executive Overview

At Glide Identity, security and privacy are not optional features, they are fundamental to our platform design and our culture.

We build identity verification and authentication systems that protect users, partners, and data through layered security controls and constant vigilance.

Our security philosophy is built on five pillars:

1. **Privacy by Design** – Every product decision considers data minimization and lawful processing.
2. **Defense in Depth** – Multiple layers of preventive and detective controls.
3. **Least-Privilege Access** – Employees and systems only access what they need.
4. **Continuous Monitoring** – Real-time detection, logging, and response.
5. **Transparency** – We openly share our practices, findings, and certifications.

2 Trust & Transparency Commitments

Glide Identity is committed to maintaining trust through transparency.

We continuously enhance our security posture and share updates openly with customers.

2.1 Our Commitments

- Annual third-party audits and certifications
- Regular updates to the Trust Kit and public Trust Center
- Timely communication of security events
- Security reviews embedded in every product release

2.2 Contact Channels

- Security: security@glideidentity.com
- Privacy: dpo@glideidentity.com
- Legal & Compliance: legal@glideidentity.com

3 Product Security

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.

3.1.1 Key Product 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).

3.1.2 AAL2 Compliance Status NIST SP 800-63 B-4

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

3.1.3 Attack Scenario Comparisons

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**

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**

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	**ATTACK SUCCESSFUL** **Complete credential theft**

	device 5. Victim unaware of 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**

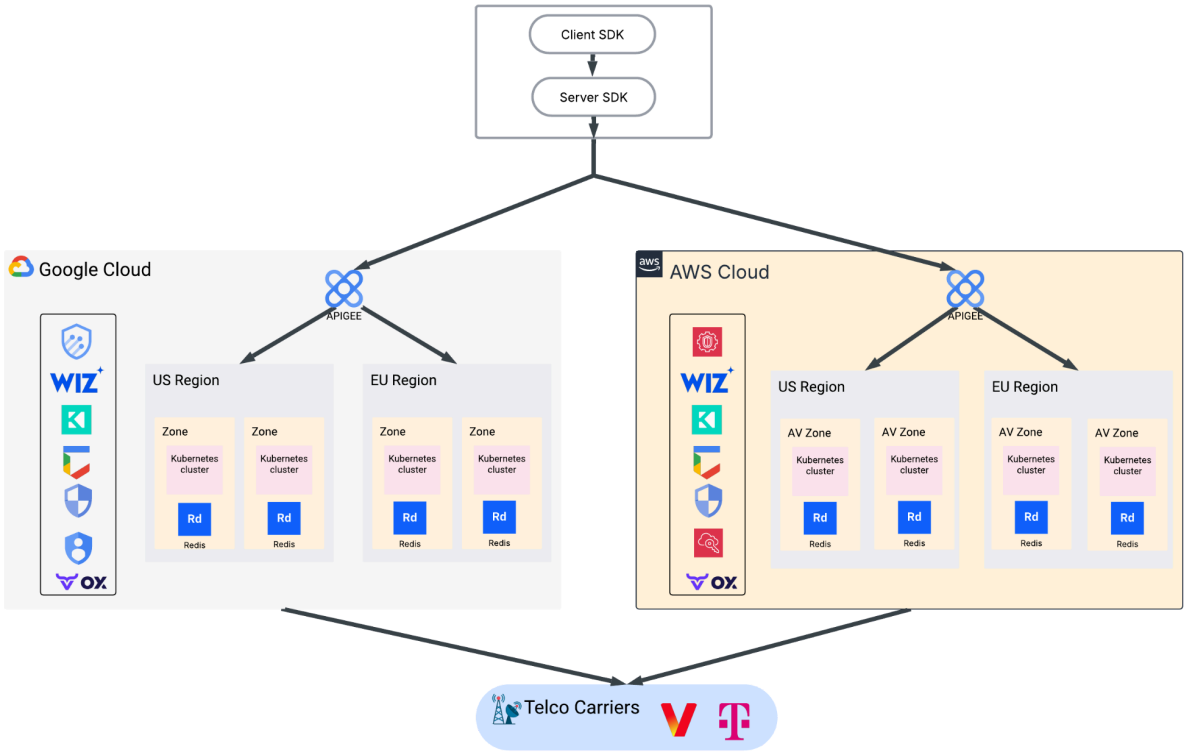
Scenario 4: Attacker on same network

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

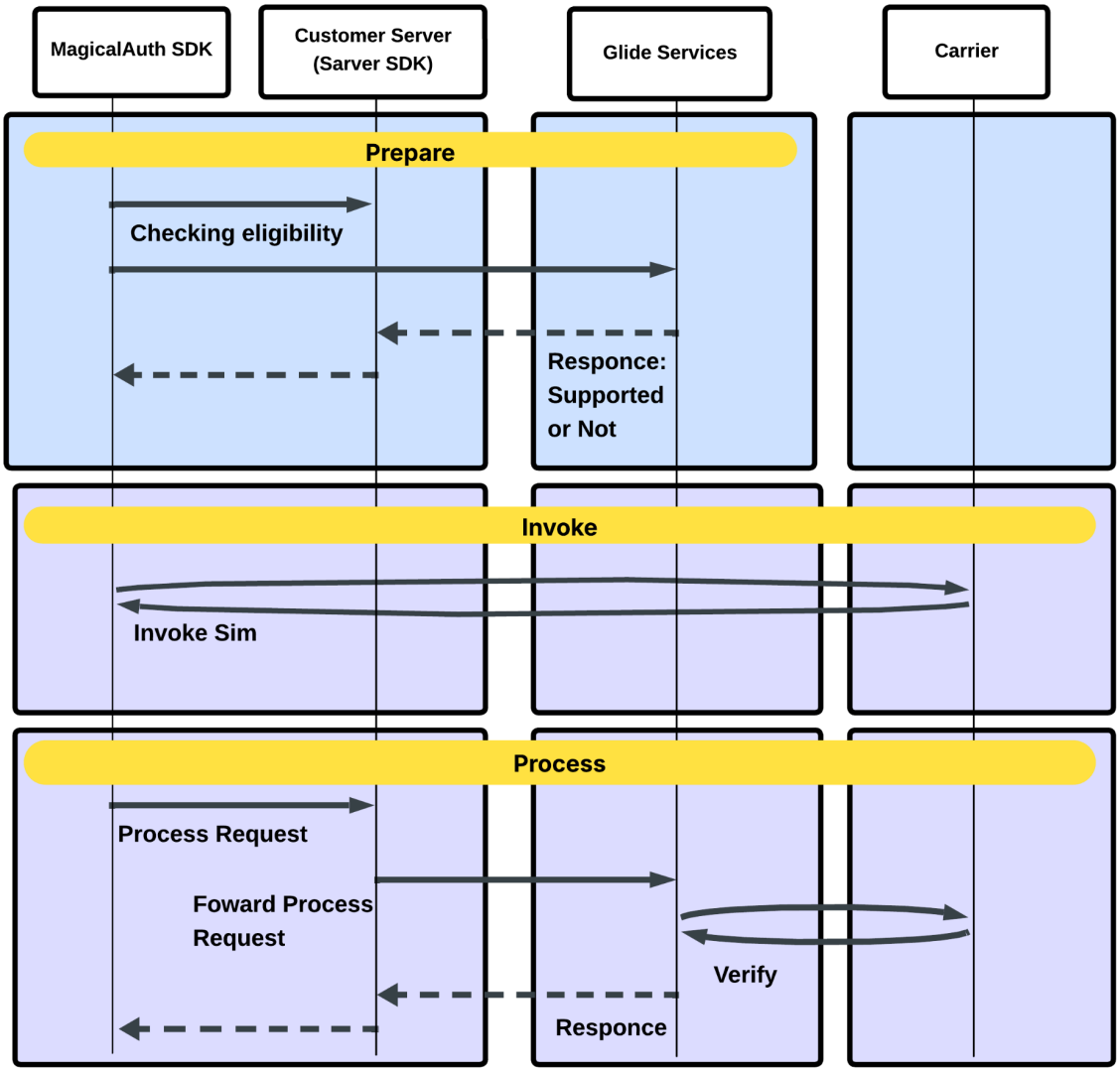
Method	Attack Flow	Result
Password + SMS OTP	1. User authenticates on public Wi-Fi 2. Attacker intercepts session cookie (if not secure) 3. Attacker replays session cookie 4. Access granted until session expires	VULNERABLE Depends on session security
SNA (Silent Network Auth)	1. SNA validates via carrier 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

4 Architecture & Data Flow

Glide Identity operates a multi-tenant, microservices-based platform hosted on Google Cloud Platform (GCP). Customer data flows securely through load-balanced endpoints, encrypted end-to-end. Each service runs in an isolated Google VPC with private subnets and service perimeter controls (VPC Service Controls) to protect against data exfiltration.



Network \ DFD Diagram



Verify \ Get Phone Number With Glide SDK Sequence Diagram

5 Authentication & Authorization

- Key base authentication for API request access
- MFA enforced for admin and privileged accounts
- Role-Based Access Control (RBAC) across all services
- Automatic session timeout and token expiry policies

6 Data Protection

Layer	Control
At Rest	AES-256 encryption using Akeyless CloudHSM (automated key rotation)
In Transit	TLS 1.2\3 with HSTS and Perfect Forward Secrecy
Secrets	Stored and rotated via Akeyless Secret Manager

7 Secure Development Lifecycle (SDLC)

- All code reviewed and tested prior to merge
- Code scanning (Such as Static and Dynamic) integrated into Glide pipelines
- Dependency scanning via OX Security and GitHub Dependabot
- Threat modeling integrated into design reviews

8 Compliance & Certifications

Framework	Status	Target	Scope
SOC 2 Type II	In progress	Q4 26	Platform, APIs, infrastructure
ISO 27001	Planned	Q1 26	ISMS across all business units
ISO 42001	Planned	Q1 26	Across all business units
ISO 22301	Planned	Q1 26	BSMS across all business units
ISO 27701	Planned	Q1 26	PSMS across all business units

GDPR	Compliant	—	EU personal data handling
CCPA	Compliant	—	US consumer data
Pen Tests	Ongoing	Annual	E2E across all Production

- Industry-specific certifications – FIDO certified.

8.1 External Validation - Pen Tests

Glide engages accredited cybersecurity firms not just on an annual basis but continuously throughout the year for penetration tests and security audits to test the resilience of our products and network.

Executives Summaries are available under NDA.

8.2 Policies

- AI Security Policy
- Information Handbook and Policy for Users
- Outsourcing Employees Policy
- Secure Development Policy
- Access Control and User Management Policy
- Asset Management Policy
- Change management Policy
- Cloud security Policy
- Data Collection, PII Mapping and Anonymization processes
- Disposal of Physical-Logical Information
- Encryption Management Policy
- External Party Management Policy
- Hardening Policy
- Incident Response Policy

- Information Classification Policy
- Information Security Awareness Program
- Information Security in HR
- Open Source Software Management Policy
- Password Policy
- Patch Management Policy
- Physical and Environmental Security Policy
- Risk Management Policy
- Secure Development Policy
- Web Applications Security Policy
- Secure Transfer of Information Policy
- Information Security Management System Policy (ISMS)
- Privacy Information Management System Policy (PIMS)
- Business Continuity Information Management System Policy (BIMS)

9 Privacy & Data Governance

9.1 Data Protection Approach

We design Glide Identity with privacy and compliance built in as core fundamentals in our product. Personal data is processed within GCP regions aligned with customer location and contractual obligations.

- Data Residency: Customers can request specific data residency. Default is us-central1 (Iowa). EU data is hosted in europe-west1 (Belgium) per GDPR requirements.
- Retention: Verification records are retained Hashed and secure.
- Access Logging: Managed through Cloud Audit Logs and Chronicle SIEM

9.2 Incident Response

- 24×7 on-call security team

- 4-hour SLA for high-severity incidents
- Root-cause analysis within 72 hours
- Customer notification occurs immediately upon detection of high-severity incidents, with detailed RCA provided within 72 hours.
- Threat Detection Incident response tool.

10 Infrastructure & Operations Security

10.1 Cloud Platform

Glide Identity is fully hosted on Google Cloud Platform (GCP), leveraging its security, compliance, and availability guarantees.

10.2 Key GCP Services Used

- Compute Engine and GKE (Kubernetes Engine) for container orchestration
- Cloud SQL and BigQuery for secure data processing
- Cloud Storage for encrypted object storage
- Cloud Armor and APIGEE for DDoS protection
- Identity-Aware Proxy (IAP) for internal access control
- VPC Service Controls for data exfiltration prevention

10.3 Network Security

- Isolated VPC networks with private subnets
- Strict firewall and IAM policies
- Cloud Armor edge protection (rate limiting, IP filtering, threat intelligence)
- Enforced TLS termination via Cloud Load Balancing

10.4 Operational Security

- Infrastructure as Code
- Change management enforced via triggers and approvals

- Continuous monitoring via Security Posture Management (CSPM), Data Security Posture Management (DSPM), Application Security Posture Management (ASPM), Threat Detection Incident Response (TDIR) and Chronicle SIEM
- Alerts routed to security on-call team

10.5 AI Security

- Glide Identity developed GAIA (Glide AI Agent) for secure AI use in company employees, where Glide Identity controls the Model garden approach used in AI tools for employee productivity.
- Continuous monitoring on dedicated AI GCP account with secure guardrails, such as Prompt security and DLP, and Privacy.
- GAIA was tested and validated by 3th party auditors (EY) as part of our SOC2 report with 18 controls.

10.6 Business Continuity & Disaster Recovery

- RTO: < 15 min RPO: < 5 Min
- Quarterly disaster recovery tests and tabletop exercises

11 Secure Engineering & Testing

- Engineers complete secure coding and OWASP training annually
- CI/CD pipeline runs automated static and dynamic scans
- Secrets scanning enforced via pre-commit and pipeline checks
- Regular third-party penetration testing and remediation follow-up
- Active vulnerability disclosure program and bug bounty
- Dependency management monitored continuously (CVSS flagged automatically)

12 Incident Response & Disclosure

12.1 Security Incident Response

Our Security team monitors the platform 24/7.

In case of a suspected breach or security incident, Glide initiates its formal Incident Response Plan (IRP) — including triage, containment, eradication, and post-incident review.

12.2 Reporting Security Issues

security@glideidentity.com

Reports are acknowledged within 24 hours with status updates until resolved.

13 Sub processors & Third-Party Vendors

We maintain a list of subprocessors and their security certifications in the Glide Trust Center.

All vendors undergo an annual risk and data-protection assessment.

Appendix A — Glossary

Term	Definition
Cloud KMS	Akeyless Cloud Key Management Service for encryption key lifecycle management
VPC	Virtual Private Cloud; isolated network environment for GCP workloads
Chronicle	Google Cloud's enterprise SIEM and security analytics platform
SOC 2 Type II	Independent audit of security, availability, and confidentiality controls
GDPR / CCPA	Data privacy regulations for EU and California residents
RTO / RPO	Recovery Time Objective / Recovery Point Objective for BCP/DR planning

Document Maintenance

This Security Kit is reviewed quarterly by Glide Identity's Security, Privacy, and Compliance teams.

The latest version and historical records are available in our Trust Center or under NDA upon request.