



SyberKey for Telecommunications

Human Verified Identity for the Digital Telecom Ecosystem

One Platform. One Identity. Unlimited Trusted Transactions.

Telecommunications providers are rapidly transforming into digital service providers.

Beyond connectivity, today's operators deliver:

- Consumer mobile services
- Enterprise networking
- Cloud services
- Identity services
- Financial services
- IoT
- eSIM management
- Customer self-service
- Digital onboarding
- AI-enabled customer support
- Enterprise security services

Every one of these services depends on one critical element:

Trusted digital identity.

SyberKey provides a modern identity platform that replaces traditional authentication methods with continuous human verification using live biometrics and cryptographic trust.

The result is stronger security, better customer experience, lower operational cost, and a future-ready identity foundation.

Why Telecommunications Needs a New Identity Model

Telecommunications providers face increasing challenges including:

- Account takeover fraud
- SIM swap attacks
- Password theft
- OTP interception
- Call centre impersonation
- Dealer fraud
- Identity theft
- Insider threats
- AI-generated fraud
- Regulatory compliance
- Enterprise customer security

Traditional authentication methods were never designed for today's threat landscape.

The SyberKey Platform

SyberKey delivers an identity-first authentication platform built around a verified digital human identity.

Instead of relying primarily on passwords or one-time codes, SyberKey continuously verifies that the authorised human is performing the transaction.

The platform can integrate with existing telecom infrastructure without requiring replacement of current systems.

Core Capabilities

OneBioID

A single trusted digital identity used across customer, employee and partner ecosystems.

Live Biometric Authentication

Human presence verified in real time.

No reusable biometric templates.

No static credentials.

Passwordless Authentication

Eliminates dependency on passwords.

Reduces credential theft.

Improves customer experience.

No OTP Dependency

Removes reliance on SMS or email OTPs.

Eliminates one of the largest attack vectors affecting telecommunications providers.

Adaptive Authentication

Authentication dynamically adjusts according to:

- user behaviour
- device
- location
- transaction type
- risk profile

Zero Trust Identity

Every request is verified.

No implicit trust.

Continuous verification.

Decentralised Architecture

Works with existing enterprise identity systems.

No large-scale replacement projects.

API-based deployment.

PQ-Ready

Designed to support post-quantum cryptographic evolution.

Helps future-proof long-term identity infrastructure.

Verified Actions

Identity can be attached to important business actions, creating trusted, auditable human verification.

Examples include:

- account changes
- SIM replacement
- enterprise approvals
- financial transactions
- service activation
- administrator actions

FingerSign

Biometrically verified electronic signatures for customer agreements and enterprise workflows.

VerifiedBioMail

Trusted identity attached to email communications for sensitive telecom workflows.

AI Agent Identity

Creates verified identity for AI agents operating within telecom environments.

Every AI action can be linked back to an authorised human owner.

AI Airlock

Allows telecommunications organisations to safely deploy AI while maintaining governance, identity and human accountability.

CAM

Continuous Authentication Management.

Identity assurance throughout an entire user session.

Not simply at login.

CPE

Continuous Policy Engine.

Dynamic enforcement of security policies based on:

- identity
- risk
- behaviour
- context

Telecommunications Use Cases

Customer Digital Identity

Secure customer identity throughout the customer lifecycle.

Examples:

- new customer onboarding
- account login
- account recovery
- service changes

- mobile app authentication
- digital self-service

SIM Swap Protection

One of the industry's biggest fraud problems.

Instead of relying on passwords or OTP verification, SyberKey can require verified human authentication before high-risk SIM replacement.

Customer Account Recovery

Replace knowledge-based questions and SMS verification with trusted biometric identity verification.

Faster.

More secure.

Lower fraud.

Enterprise Telecom Customers

Large enterprise customers increasingly require stronger identity controls.

SyberKey can secure:

- enterprise portals
- VPN access
- network management
- privileged access
- administrator approval
- remote workforce authentication

Dealer and Retail Networks

Secure thousands of authorised dealers using verified identity.

Protect against:

- fraudulent activations

- unauthorised SIM issuance
- identity fraud
- insider abuse

Workforce Identity

Employees access hundreds of internal systems.

SyberKey provides:

- passwordless login
- privileged access protection
- adaptive authentication
- continuous identity verification

Call Centre Identity Verification

Reduce customer friction while improving fraud protection.

Instead of multiple security questions, customer identity can be verified using trusted live authentication.

eSIM Provisioning

Secure identity verification before:

- issuing eSIMs
- transferring services
- changing ownership

Enterprise VPN Access

Modern passwordless authentication for:

- network engineers
- administrators
- field technicians

- contractors

API Security

Protect API access using verified digital identity rather than only static API credentials.

AI Customer Service

As telecom providers increasingly deploy AI assistants, SyberKey enables:

- verified AI identity
- human accountability
- secure AI actions
- trusted automation

Telecom Financial Services

Many operators now provide:

- digital wallets
- payments
- lending
- insurance
- remittance

SyberKey strengthens customer identity throughout financial transactions.

IoT Identity

Secure authentication for connected devices using identity policies managed through the SyberKey platform.

Example Customer Journey

Traditional Model

Password



OTP



Login



Trust Session



Risk increases over time

SyberKey Model

Live Human Verification



Verified Digital Identity



Adaptive Authentication



Continuous Authentication



Continuous Policy Enforcement



Verified Action



Full Audit Trail

Business Benefits

Better Customer Experience

- Faster login

- Reduced authentication friction
- Passwordless access
- Fewer support calls

Lower Fraud

- Reduced SIM swap fraud
- Reduced account takeover
- Reduced impersonation
- Stronger identity assurance

Lower Operating Cost

- Reduced password reset costs
- Reduced OTP costs
- Lower fraud investigation costs
- Faster onboarding

Stronger Compliance

Supports identity assurance across regulated telecommunications environments.

Future Ready

Designed for:

- AI adoption
- Post-Quantum security
- Zero Trust
- Digital identity regulations

Integration

SyberKey is designed for rapid deployment through APIs.

The platform complements existing investments including:

- IAM platforms
- Customer Identity systems
- SSO
- PAM
- CRM
- Mobile applications
- Customer portals
- Network management platforms
- Dealer systems
- Billing platforms
- Contact centre platforms

No large infrastructure replacement is required.

Why SyberKey

Unlike traditional authentication vendors, SyberKey is built around verified human identity rather than credentials.

Key Differentiators

- ✓ Live biometric human verification
- ✓ Passwordless architecture
- ✓ No OTP dependency
- ✓ No special hardware required
- ✓ API-first integration
- ✓ Low integration cost
- ✓ Decentralised identity model
- ✓ Continuous Authentication Management (CAM)
- ✓ Continuous Policy Engine (CPE)

- ✓ Verified Actions with end-to-end auditability
- ✓ AI Agent Identity for trusted autonomous operations
- ✓ AI Airlock for sovereign and governed AI deployment
- ✓ PQ-ready architecture for future cryptographic resilience
- ✓ Scalable across consumer, enterprise and partner ecosystems

Strategic Value for Telecommunications Providers

SyberKey enables telecommunications providers to evolve from simply authenticating users to establishing trusted digital identity across every customer, employee, partner, device and AI interaction.

By replacing legacy authentication methods with continuous human verification, telecom operators can reduce fraud, simplify customer experiences, strengthen regulatory compliance, and create new trusted digital services on a future-ready identity platform.

SyberKey delivers a single, scalable identity layer that helps telecommunications providers protect people, secure networks, enable AI safely, and build the next generation of trusted digital communications.