Product Overview

Technical Whitepaper



(303) 888-4360

Sales@tssgroupllc.com

www.tssgroupllc.com

Table of Contents

Executive Summary 3

Paradigm Shift: From Point-in-Time Login to Continuous Protection 4

Core Capabilities of Proximia Connect 6

Attack Vectors Mitigated by Proximia's Architecture 7

Downstream Impact: Alleviating the Hidden Complexity of Daily Access 8

XiFi™ for Complete Device Flexibility 9

Persistent Authentication Explained 10

Device-Bound Identity and Wearable Tech 11

Proximity, Presence & Mutual Trust 12

Passwordless Access & Legacy System Integration 13

NFC, BLE, and UWB: How They Work Together 14

Deployment Models 15

Tech Stack 16

Analytics & Insight Engine 18

Security & Compliance 19

Frequently Asked Questions (FAQs) 20

© Proximia, all rights reserved.

Executive Summary

Proximia Connect is redefining what it means to authenticate. Unlike traditional Identity and Access Management (IAM) platforms that validate identity once at login, Proximia delivers persistent, presence-aware authentication that protects the user continuously—across every session, device, app, physical and digital checkpoint.

This breakthrough lies in a simple shift: the persistence of a user's biometric identity. Once biometrically authenticated, identity is bound to a trusted device with wear detection. That device becomes the key—enabling a secure walk-up-and-work experience that eliminates friction.

Every login event—whether at a computer, a physical doorway, or a downstream legacy system—is protected invisibly. For mid-sized enterprises, where users may encounter 20–35 login points daily, Proximia replaces friction with flow—eliminating traditional MFA entirely. No more QR codes, authenticator apps, or interruptions—just seamless, persistent validation through proximity and trust.

This isn't just a usability enhancement—it's a structural rethinking of how identity travels with the user. By merging persistent identity with proximity and mutual trust, Proximia unifies fragmented security stacks and brings Zero Trust principles to life.

This represents more than a product—it's a new category of IAM.



© Proximia, all rights reserved.

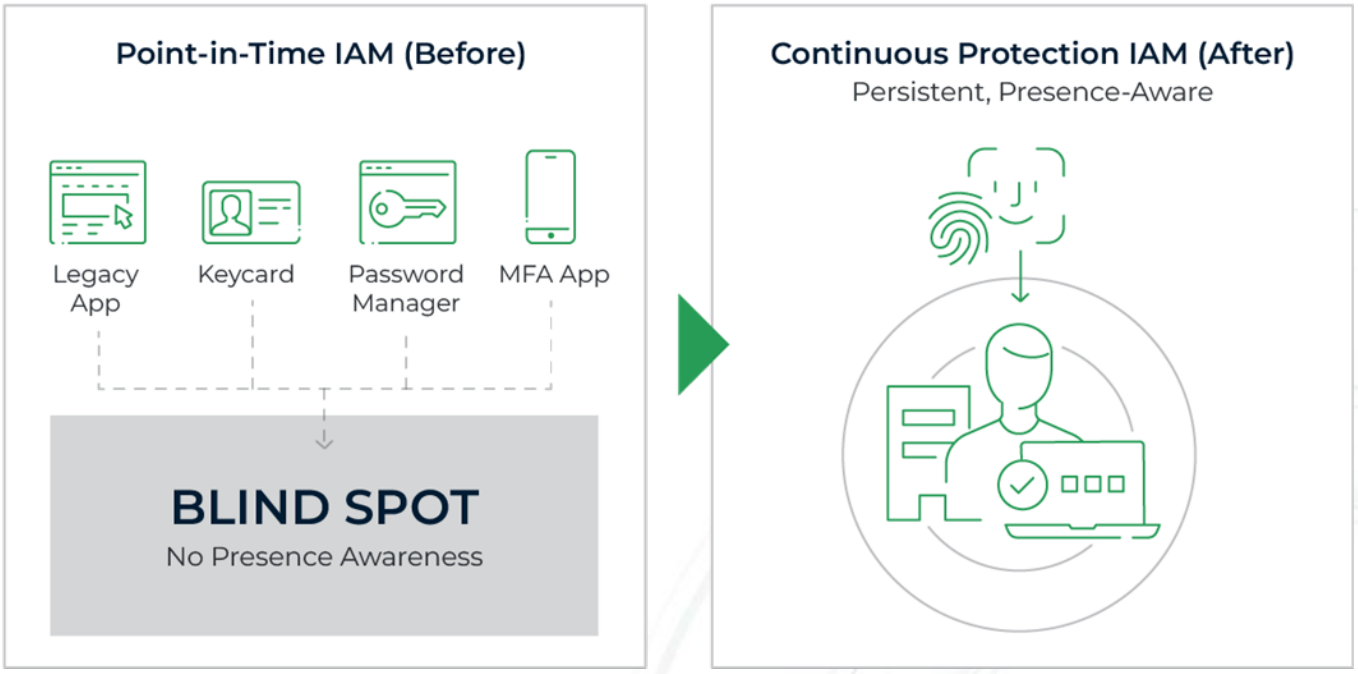
Paradigm Shift: From Point-in-Time Login to Continuous Protection

Identity and access management (IAM) hasn't kept pace with how people work—or how threats evolve. Today's architecture remains largely static: a fragmented patchwork of MFA apps for cloud access, password managers for legacy systems, and entry cards for physical spaces. This brittle stack can't adapt to dynamic environments like IoT—and worse, it's blind to the question that matters most: is the right person still there after access is granted?

Even organizations embracing Zero Trust remain tethered to point-in-time logic. MFA and SSO may determine where access begins—but not who remains present once it does.

The Limitations of Today's IAM Landscape

- **Static Architecture:** Designed for fixed logins, not dynamic user and device behavior—especially problematic in IoT and hybrid environments
- **Fragmentation:** No unified identity layer across physical, digital, and legacy systems
- **Blind Spots:** Trust is assumed after login, with no ongoing awareness of presence or proximity
- **Friction:** MFA slows productivity and is frequently avoided, misconfigured, or inconsistently enforced
- **Unusable Data:** Static systems produce limited and outdated access signals, making real-time decisioning and AI threat response nearly impossible



© Proximia, all rights reserved.

Proximia's Breakthrough: Persistent, Presence-Aware Authentication

Proximia introduces an identity model that binds the user to a secure wearable or smart badge - persisting biometric authentication. From that moment forward, identity is no longer a credential—it's a continuously enforced state.

This presence-aware framework enables:

- **Always-on Authentication:** Identity is verified not only at login, but throughout the session—automatically revoking access if proximity is lost or trust is broken
- **Seamless Access Flow:** Users move across workstations, cloud apps, physical spaces, and legacy terminals without repeated logins or prompts
- **Mutual Trust Architecture:** Devices and users verify each other continuously using mutual Transport Layer Security (mTLS), certificate exchange, and biometric integrity—delivering bidirectional authentication not just at the edge, but in-session

Under the hood, Proximia unifies identity, proximity, and trust into a composable, Zero Trust-aligned architecture that supports:

- Passwordless access for both modern and legacy systems
- Offline authentication for air-gapped environments
- Centralized policy enforcement with distributed presence validation

From Point-in-Time to Continuous Protection

This isn't just a more secure login. It's an entirely new model for identity—stateful, wearable, and persistent. This is how Zero Trust becomes usable—and enforceable.

This framework not only eliminates passwords and MFA fatigue but establishes real-time confidence that the correct user is present and trusted. It aligns directly with the NSA's Zero Trust Pillars and NIST SP 800-207.

Proximia is the first product to deliver this level of continuity in a form factor users can wear, carry, and forget about.



© Proximia, all rights reserved.

Core Capabilities of Proximia Connect



Persistent authentication of biometric identity



Biometric identity capture via modern standards – no vendor lock-in



Device-bound trust—users become the key



Live proximity sensing for real-time presence detection



Wear detection to ensure authentication is active only when devices are worn



Mutual trust model (user ↔ device verification)



Auto-lock on presence loss or proximity parameter breach



AI Insight Engine for anomaly detection and behavioral analytics



Unified access to digital, physical, and legacy systems



Mobile app with passkey orchestration



Passwordless access—across entire ecosystem



Credential vault with dynamic password rotation for legacy apps



Offline access controls and FIDO2 compatibility

© Proximia, all rights reserved.

Attack Vectors Mitigated by Proximia's Architecture

Threat Category	Mitigated Risk & Proximia Response
Credential-Based Attacks	• Eliminates passwords, neutralizing phishing, credential theft, replay attacks, and credential stuffing • Uses ephemeral, rotating tokens to prevent reuse or interception from infostealers or leaked credential databases • Credential injection prevents keylogging and shoulder surfing
Session & Access Exploits	• Session hijacking is prevented by automatic revocation on proximity loss or wearable removal • Per-user proximity ensures shared devices are secure in environments like kiosks or meeting rooms • Prevents proximity spoofing with encrypted BLE, wear detection, MAC rotation, and future UWB support
Insider Threats & Physical Risks	• Stolen badges are useless without biometric and wear validation • Dynamic credential injection blocks reuse, sharing, or extraction of passwords
Offline & Air-Gapped Environments	• Local passkey validation ensures secure access without internet • Maintains Zero Trust enforcement even in disconnected environments
Visibility & Compliance Gaps	• Real-time session logs, proximity tracking, and wear status auditing ensure traceability • Encrypted logs with export-ready reporting support SOC 2, HIPAA, CJIS, ISO 27001 compliance

© Proximia, all rights reserved.

Downstream Impact: Alleviating the Hidden Complexity of Daily Access

Most users interact with **20–35 systems or devices daily**, including:

- Web-based applications with non-SSO logins
- Legacy applications requiring authentication
- Shared workstations or kiosks (e.g., in healthcare, courtrooms, control centers)
- Physical access points
- Virtual desktops or secure terminal servers
- Air-gapped or offline systems that bypass SSO
- Elimination of complexity results in significantly lower energy consumption

Each of these presents a separate trust challenge—often requiring a new MFA prompt, password entry, or physical badge tap. The result is **repeated interruptions**, lost time, and inconsistent enforcement.

Scenario	Traditional Workflow	With Proximia
Return from break	MFA prompt or password reentry	Walk-up unlock via presence
Move between shared PCs	Reauthenticate + credential conflict	Auto-switch based on trusted wearable
Legacy app access	Password entry or static MFA	Credential injected securely
Badge Entry	Quick to use, but completely unprotected	Quick to use, plus identity-bound with wear detection

Security & Productivity ROI

- **20–30** minutes saved per user per day in high-friction environments
- **55%** of help desk tickets relate to passwords
- **85%** of breaches involve human error
- **91%** of phishing attacks target credentials
- **$70-$120** average spend on each password reset

Proximia doesn't just streamline access—it **reshapes the daily user experience** while hardening your security posture across every system, every time.

© Proximia, all rights reserved.

XiFi™ for Complete Device Flexibility

Proximia's patent-pending platform XiFi delivers a device-agnostic approach to authentication by allowing Proximia Connect to work seamlessly with the devices chosen by users—phones, wearables, workstations, tags, and more. It also streams real-time location and proximity data from those devices, enabling intelligent, context-aware Zero Trust access decisions without lock-in or system overhauls.

- **Device Agnostic:** Use any mix of phones, biometric readers, wearables, tags, or workstations—your ecosystem, your choice
- **Location-Driven Intelligence:** Streams real-time, meshed location data to inform access and trust decisions
- **Built to Evolve:** Adapts with your stack—no vendor lock-in, no new hardware required
- **Multi-Protocol Support:** Compatible with BLE, RFID, GPS, NFC, UWB, and more
- **Flexible Deployment:** Works across public cloud, private cloud, or on-prem—no infrastructure overhaul needed

XiFi™ by PROXIMIA



© Proximia, all rights reserved.

Persistent Authentication Explained

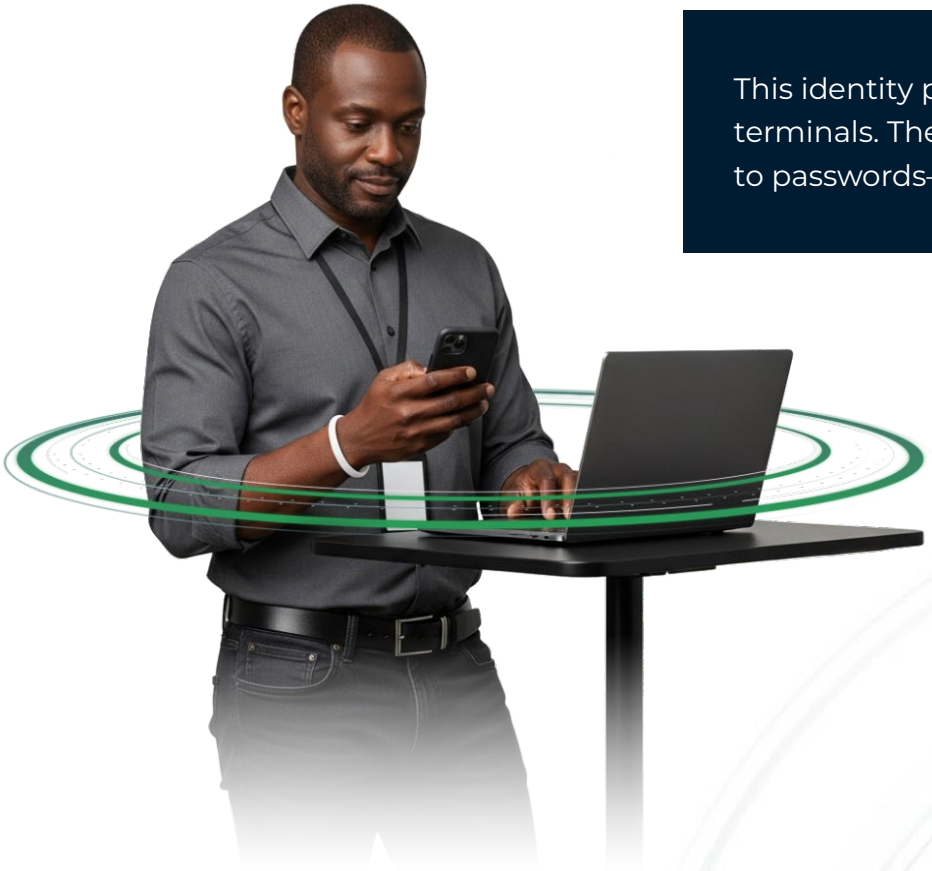
Once a user is verified through biometrics, their identity is securely bound to a trusted device—enabling persistent authentication continuously protected by real-time proximity, wear detection, and mutual trust.

Current Options Include:

- **Android/iOS:** Native biometric platform APIs (e.g., Face ID, fingerprint)
- **Windows:** Proximia's proprietary facial recognition system, using a webcam or attached camera for biometric login (NIST-compliant)
- **Future:** Biometric device agnostic via XiFi engine

Once verified, identity is bound to a wearable device. From this point on:

- **Wear detection** ensures the device is actively being worn
- **Proximity** ensures the user is near the device they're accessing
- **Re-validation** periodically occurs based on policy or device type



This identity persists across sessions and terminals. There's no user managed fallback to passwords—even for legacy apps.

© Proximia, all rights reserved.

Device-Bound Identity and Wearable Tech

Proximia's device form factors include:

- Smart badges (with NFC + BLE + future UWB)
- Wearable bands with IMU sensors and optional biometric pulse detection
- NFC-enabled phone apps that behave as smart wearables



Why wear detection matters:

Traditional proximity cards offer no assurance of who is carrying them. With Proximia, NFC door access only works when biometric trust is active on the wearable. Simply stealing or borrowing a badge will not permit access.



Wear detection uses:

- IMU sensors
- Machine learning pattern recognition
- Planned UWB radar (e.g., heartbeat sensing)

Competitors haven't successfully deployed wear detection due to OS limitations or precision challenges. Proximia designed custom firmware to address this directly.

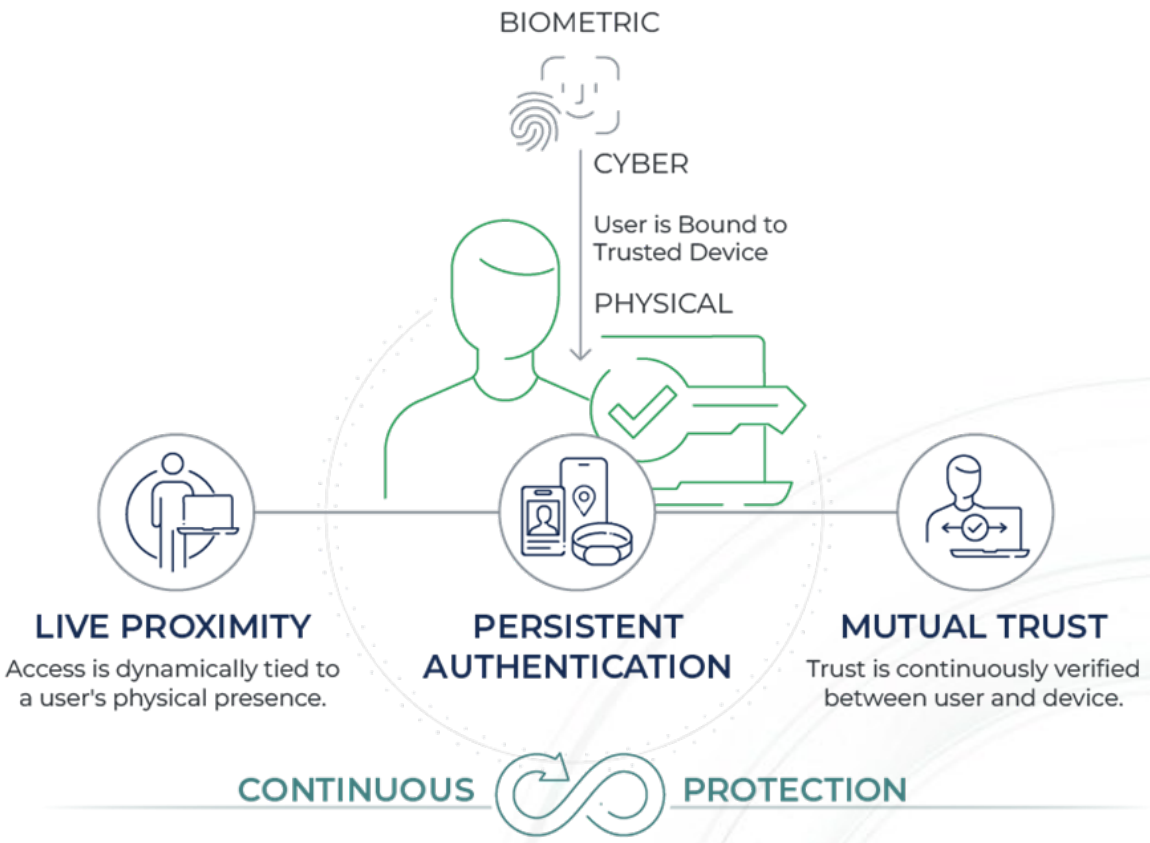
© Proximia, all rights reserved.

Proximity, Presence & Mutual Trust

Presence is more than proximity—it's about proving the right user is still actively engaging with the system. Proximia verifies this in real-time using multiple dimensions:

- **Proximity sensing:** Uses Bluetooth Low Energy (BLE) to measure distance between user and device. BLE is broadly supported and serves as the current default
- **Next-gen UWB roadmap:** For environments requiring more granular accuracy, Proximia's devices are UWB-ready, offering millimeter-level precision for directional sensing
- **Wear detection:** Ensures the device is being worn—not just nearby—by using IMUs and planned UWB heartbeat sensing
- **Mutual trust model:** Proximia doesn't just authenticate the user; the device must prove it is trusted as well. Bidirectional authentication (mTLS, certificate exchange) ensures that both ends of the session are continuously verified

This mutual, presence-aware trust model goes beyond login events. It enables real-time session monitoring, auto-lock on removal or walk-away, and policy-based revalidation—creating a constantly protected state.

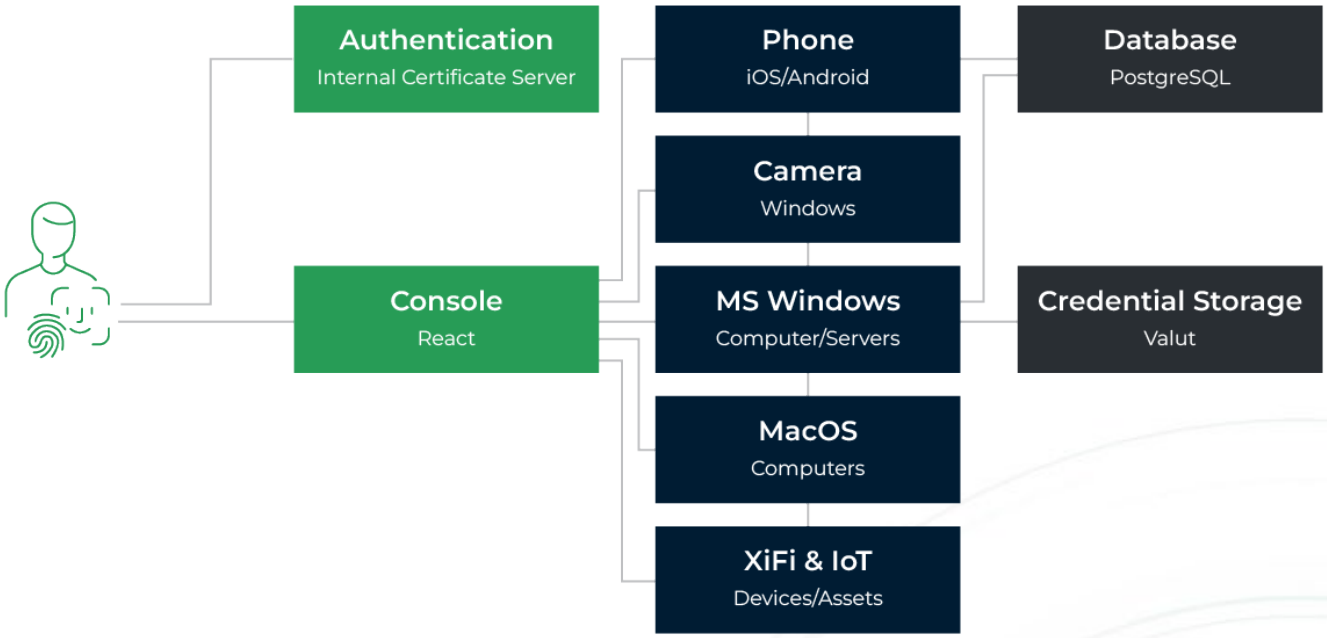


© Proximia, all rights reserved.

Passwordless Access & Legacy System Integration

Proximia fully eliminates passwords from the end-user experience—even for legacy systems and apps that lack modern SSO capabilities.

- **Users never know or see passwords:** Credentials are created and rotated automatically, and injected on the user's behalf
- **Legacy system support:** Web apps, desktop apps, and green-screen terminals are all supported via credential vaulting and injection
- **Credential obfuscation:** Admins assign and manage credentials from a central console; users are unable to extract or share them
- **FIDO2 & passkey orchestration:** Proximia acts as a roaming authenticator—no separate hardware keys, e.g., required
- **Offline authentication:** Proximia supports offline login through secure wireless FIDO2 authentication. Passkeys can be stored locally on trusted device, allowing users to authenticate even without internet or backend access



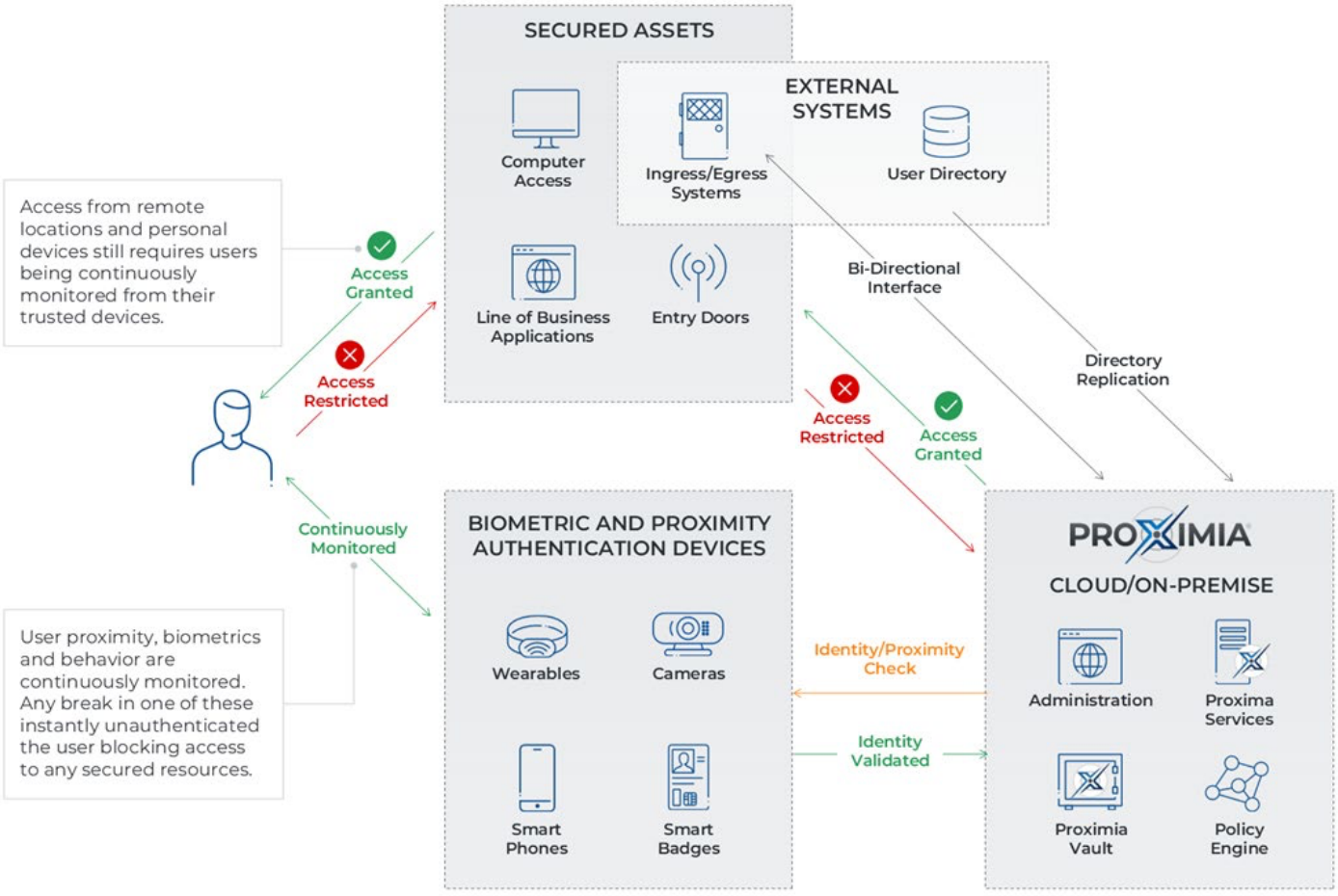
© Proximia, all rights reserved.

NFC, BLE, and UWB: How They Work Together

Proximia blends three key wireless technologies to deliver seamless, secure access:

- **BLE (Bluetooth Low Energy):** Used for live proximity sensing, BLE offers the best balance of battery life and range today. It's the most common denominator across mobile and desktop ecosystems, making it the ideal starting point for scalable enterprise deployment. BLE enables immediate compatibility with a wide range of devices while laying the foundation for more advanced capabilities.
- **NFC (Near Field Communication):** Used for secure tap-based access—especially at physical door readers. NFC functionality is only enabled when a user has been verified and persisted to their badge or device. This prevents lost or stolen cards from being misused.
- **UWB (Ultra-Wideband):** Future capability that offers millimeter-level distance and direction sensing. UWB allows for far more precise presence verification than BLE. Proximia devices are UWB-ready, and future firmware updates will enable directional sensing, heartbeat detection, and fine-grain location awareness.

Together, these technologies allow Proximia to secure access invisibly, without relying on cumbersome tap-ins or re-authentication. Each protocol plays a role in securing sessions, validating presence, and enhancing both digital and physical access.



© Proximia, all rights reserved.

Deployment Models

Proximia Connect is designed to support a range of enterprise deployment needs, from cloud-native environments to secure, disconnected installations. Supported models include:

- **Cloud-Hosted (SaaS):** Fully managed by Proximia, ideal for fast onboarding and minimal IT overhead. Includes automatic updates and cloud analytics.
- **Hybrid Deployment:** Cloud console with on-premise components. Useful for environments with strict access policies for certain applications or physical infrastructure.
- **On-Premise:** All services—including orchestration, credential vaulting, and analytics—deployed within the customer's data center. Supports regulated industries and air-gapped environments.
- **Air-Gapped / Disconnected Sites:** Designed for court systems, defense, utilities, and critical infrastructure. Authentication works without an internet connection via local validation and secure passkey storage.

Each model supports remote device management, policy enforcement, and real-time alerting.



© Proximia, all rights reserved.

Tech Stack

Proximia Connect is built using a modern, scalable, and secure technology stack optimized for speed, cross-platform compatibility, and compliance with enterprise-grade security standards.

Core Technologies

Backend Services:

- Scalable TypeScript backend powered by NestJS (Node.js) with modular, maintainable architecture
- Supports **REST APIs** for extensible integration with enterprise IAM platforms, SIEMs, and access management tools
- Uses **PostgreSQL** as a relational database engine for fast, reliable structured data storage across policy and admin layers

Frontend Console:

- Developed in **React** with **TypeScript** for administrative interfaces
- Built for responsiveness and compatibility with desktop and tablet environments
- Includes embedded **Role-Based Access Control (RBAC)** to manage delegation across teams

Mobile App (iOS/Android):

- Built natively using **Swift** and **Kotlin**, allowing deep integration with platform biometrics, secure elements, and background BLE/UWB scanning
- **FIDO2** authentication support via **WebAuthn** and native platform authenticators (e.g., Apple Face ID, Android biometrics)
- Secure element access ensures credential security and offline functionality for disconnected environments

Wearable Firmware:

- Written in **C/C++** for ultra-low-power MCU chips
- Integrated with custom drivers for **BLE** and **UWB** to support persistent proximity and directional sensing
- Interfaces with onboard sensors: **IMU, pulse detection, ambient light**, and **NFC antenna**
- Includes support for **MAC address rotation and out of band BLE communications** to strengthen BLE security and remove potential man in the middle attacks

Cloud Infrastructure:

- Hosted on **Azure**, leveraging **EC2**, **Lambda**, and **DynamoDB** for distributed orchestration
- Uses **Azure Key Vault** for encryption key management and **CloudWatch** for observability and alerting
- Infrastructure-as-Code via **Terraform** and container orchestration using **Kubernetes (EKS)**

Security & Compliance:

- Enforces **TLS 1.3** and **mTLS** between all services
- No raw biometric images are stored—only encrypted, tokenized biometric trust signals
- Aligned with **NIST 800-207** Zero Trust architecture and built toward **SOC 2, CJIS, HIPAA**, and **FIPS 140-3** certification readiness

© Proximia, all rights reserved.

Extended Capabilities

Identity Federation & SSO:

Integrates with **Keycloak** for support of **OpenID Connect, OAuth 2.0, SAML, LDAP**, and **Azure AD/Entra**—enabling compatibility with common enterprise IAM systems.

Observability & Logging:

Uses **Grafana, Prometheus, Wazuh,** and **Loki** to monitor system health, performance, and authentication behavior while aggregating logs for security and compliance auditing.

Zero Trust Remote Access:

Supports **OpenZiti** for secure remote tunneling and Zero Trust enforcement across distributed or unmanaged endpoints.

Smart Card & CAC/PIV Integration:

Supports **ActivID** for environments requiring **CAC/PIV smart card compatibility**, particularly in federal and defense deployments.

Web Delivery & Static Hosting:

Select assets are deployed via **Vercel**, providing scalable, high-performance web hosting and edge delivery for admin portals and related UI components.



Why This Stack?

- Native mobile and firmware development allows direct access to biometric, BLE, and UWB capabilities—unavailable through OS-constrained platforms
- **Azure-native architecture** provides geographic data control, horizontal scaling, and cryptographic robustness required by enterprise and government clients
- Use of **Keycloak, Prometheus**, and **OpenZiti** signals enterprise-grade readiness for integration, observability, and Zero Trust compliance
- The combination of platform-native biometrics, real-time proximity, and multi-layered verification creates a secure, persistent authentication system aligned with both operational efficiency and regulatory standards

Analytics & Insight Engine

The Proximia Connect roadmap includes a built-in AI-powered analytics engine designed to give administrators deep visibility into authentication behaviors, user activity, and real-time trust posture—without compromising user privacy.

Key Capabilities:

Anomaly Detection
Continuously monitors authentication patterns across users and devices. Detects anomalies such as:

- Unusual login times or locations
- Unexpected session durations
- Suspicious credential injection patterns
- Inconsistent wear detection events

Trust Timeline
Visual audit trail that shows how trust was established, maintained, or revoked throughout a session. Includes proximity logs, biometric verifications, and device-level integrity checks.

Behavioral Insights
Identifies patterns in user movement, frequency of access, and dormant accounts. Surfaces risk signals like:

- Infrequent wear but frequent access
- Devices left near shared terminals
- Users bypassing physical checkpoints

Policy Optimization
Leverages machine learning to recommend adjustments in authentication policies, lockout thresholds, and revalidation timing based on real-world usage data.

Compliance Reporting
Easy export of detailed logs for audits and regulatory requirements (e.g., HIPAA, CJIS, SOC 2). Supports role-based access for security, HR, and compliance officers.

Privacy-by-Design
No biometric images or raw inputs are stored. All analytics are derived from tokenized trust signals and session metadata.



Why It Matters

Security is no longer just about access—it's about visibility.
Proximia's analytics engine will provide teams the insight needed to:

- Proactively spot insider threats and credential misuse
- Reduce IT support overhead by identifying systemic access friction
- Ensure users are adhering to policies—without surveillance or disruption
- Prove compliance with Zero Trust mandates and audit requirements

© Proximia, all rights reserved.

Security & Compliance

Proximia Connect is engineered from the ground up to meet the most rigorous security and compliance standards across public and private sectors. Its architecture and policies are aligned with Zero Trust principles and follow the latest NIST, NSA, and industry best practices.

Zero Trust by Design

- Built to support full alignment with **NIST SP 800-207**
- Maps directly to the **7 Pillars of Zero Trust** (NSA), including Identity, Devices, Network, Applications, Data, Visibility, and Automation
- No implicit trust—every access decision is verified in real time, continuously

Cryptographic Safeguards

- All data in transit is encrypted with TLS 1.3
- All local storage is encrypted using ChaCha20 ciphers
- Credential injection uses ephemeral, rotating secrets
- Certificate-based mutual authentication ensures trust between users and devices

Biometric Privacy

- Proximia never stores raw biometric images (fingerprint, face, etc.)
- For Android and iOS, biometric validation is handled by the OS and Proximia has no access to the underlying data
- For Windows, biometric capture is performed only when using Proximia's own software, and data is used strictly for local verification and then discarded
- In all cases, biometric data is never transmitted or stored beyond the moment of use

Credential & Vault Security

- Admin-managed credential vault with role-based permissions
- Supports dynamic credential rotation for downstream systems
- Credentials are never shown or accessible to users

Audit & Logging

- Immutable audit trails
- Full session-level logging including proximity, wear detection, access timestamps, and credential injections
- Exportable reports for SOC 2, CJIS, HIPAA, and ISO 27001 compliance audits

Platform Certifications (Planned or In Progress)

- SOC 2 Type II
- FIPS 140-3 compliance for cryptographic modules
- HIPAA-readiness for healthcare deployments
- CJIS alignment for law enforcement and judicial agencies

Organizational Security

- Full RBAC enforcement in admin console
- Device enrollment and deprovisioning policies
- Alerts for anomalies, wear removal, or proximity loss
- Optional policy enforcement based on location, time-of-day, or terminal type

Proximia's security model is not an afterthought—it is foundational to how trust is established, preserved, and revoked. For security-conscious organizations, it delivers a platform that satisfies both operational efficiency and regulatory confidence.

© Proximia, all rights reserved.

Frequently Asked Questions (FAQs)

Q1: How is Proximia different from standard passwordless authentication solutions like FIDO2 or passkeys?
A: Most passwordless solutions authenticate a user once—Proximia goes further. We bind identity to a wearable or smart device and verify presence continuously. This provides session persistence, walk-up access, and dynamic trust revocation without repeated prompts.

Q2: What happens if a user removes the wearable or steps away from a terminal?
A: The system detects loss of proximity or wear status and immediately locks access. Depending on admin policy, re-authentication or supervised reentry may be required before access resumes.

Q3: Can Proximia work in environments without internet access?
A: Yes. Our offline mode supports authentication even in air-gapped or disconnected environments, using locally stored passkeys, biometric validation, and wear detection.

Q4: How does Proximia secure legacy systems that don't support modern SSO or MFA?
A: Proximia uses a secure credential vault combined with credential injection technology to bridge the gap. For legacy systems that still require usernames and passwords, credentials are managed centrally by administrators—but never exposed. Admins can reset passwords when needed, but they can't see or retrieve them. Users also never see or enter their credentials in legacy systems. Instead, once presence is verified, Proximia silently injects the necessary credentials into the legacy system.

Q5: What kind of wearables does Proximia support?
A: Proximia supports a wide range of wearables thanks to XiFi, our flexible, device-agnostic platform. This includes custom smart badges, NFC-capable wearables, and mobile devices that act as secure tokens. All wearables require biometric activation and wear detection before becoming valid access tools. XiFi ensures compatibility with your chosen devices today and adapts to emerging technologies—like UWB—for even greater precision and security in the future.

Q6: What kind of biometric data does Proximia store?
A: None. Proximia never stores or transmits biometric images. On iOS and Android, we leverage each platform's native biometric APIs (e.g., Face ID, fingerprint) to validate the user—Proximia has no access to this data. On Windows, when using Proximia's own software for biometric capture, data is processed locally and discarded immediately after validation. In all cases, biometric verification is ephemeral and privacy-preserving.

Q7: How does Proximia use Bluetooth Low Energy (BLE), and is it secure and accurate enough for Zero Trust authentication?
A: BLE is the most widely supported proximity protocol across mobile and desktop ecosystems, making it the best foundation for scalable enterprise deployment. Proximia uses BLE to enable real-time presence detection—but never in isolation.

To ensure both security and precision, BLE is combined with biometric verification, wear detection, encrypted out-of-band token exchange, and MAC address rotation. This layered approach mitigates known

© Proximia, all rights reserved.

BLE limitations like spoofing or interference and aligns with Zero Trust principles by validating not just proximity, but identity, intent, and session continuity.

Proximia's architecture is also built to evolve: UWB (Ultra-Wideband) integration is already underway for even greater directional accuracy and location fidelity in the future.

Q8: How does Proximia help with regulatory compliance (e.g., HIPAA, CJIS, SOC 2)?
A: Our architecture includes encrypted audit logs, role-based access, dynamic credential management, and full session traceability—supporting compliance across multiple regulatory frameworks.

Q9: What integrations are supported?
A: Proximia integrates with physical access control systems, legacy desktop software, SSO platforms, and IAM tools via REST/gRPC APIs. We also support shared terminals and mixed OS environments.

Q10: What happens during a security incident or device loss?
A: Proximia supports user and device deprovisioning. All sessions can be terminated, credentials revoked, and access immediately blocked across all Proximia devices and legacy applications.

Q11: Can Proximia co-exist with existing IAM systems or replace them?
A: Both. Proximia can serve as a drop-in enhancement to your current stack or operate as a complete IAM replacement. We work alongside traditional systems while extending Zero Trust enforcement to every layer.

© Proximia, all rights reserved.