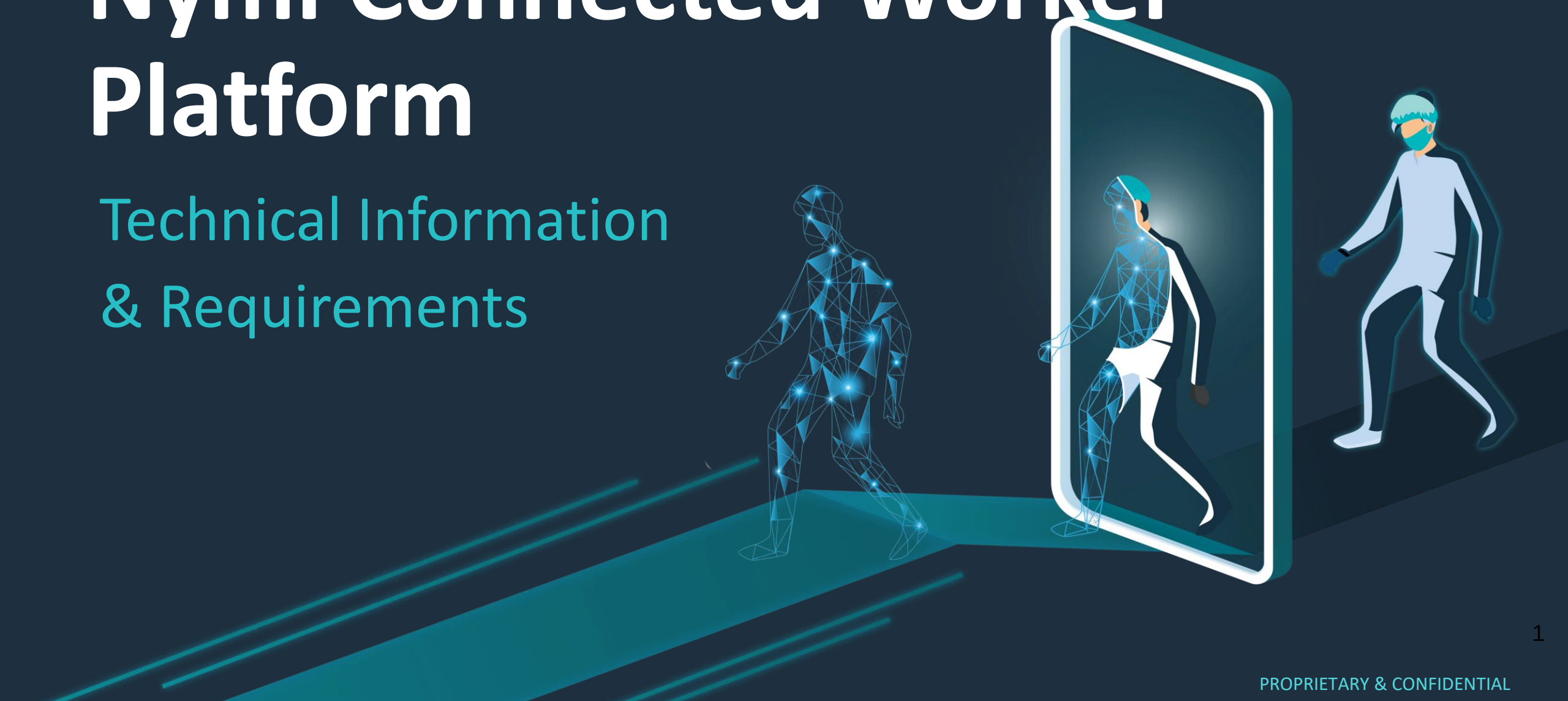
Nymi Connected Worker Platform

Technical Information & Requirements



PROPRIETARY & CONFIDENTIAL

Nymi Band Gen 3

Privacy by Design & Unmatched Security

Biometrics never leave the Nymi Band
GDPR Right to Forget
Multi-Factor Authentication (MFA)
Liveness Detection
Cryptographic Processor
Collusion Prevention

Password-less Physical & Logical Access

FIDO2, PIV, SDK, SSO, HID Seos

Health, Safety, & DX Information

Location
Presence
Activity
Liveness



NFC
A POWERFUL COMBINATION

Operational Technology (DX)

IP66- and IP67-rated (durable, clinically cleanable)
Functions under PPE (Personal Protection Equipment)
Hands-free
3+ Day Battery
Low-profile

2-Way Communications & Control

Display
Buttons
Haptic feedback (Vibration)
GDPR Right to Forget
Gestures
Secure NFC
Encrypted BLE

Use Cases

Location & Presence
- Presence Detection
- Geo-fencing
- Real-Time Location

Passwordless Office
- Login & SSO
- Walkaway Auto-lock

Passwordless Shop Floor & Labs
- Terminal Login
- App Login & eSign
- Presence

Handsfree Building Access
- Doors, Elevators, Printing, Vending & Payment



Health & Safety
- Social Distance Reminders
- Contact Tracing

Lone Worker Safety
- Motion/Liveness
- Two-way comms

Real World Data Points

Customer-Stated Value & Savings

Global Medical Device Manufacturer, signing with MES
20 seconds per signature

Global Pharmaceutical, Manufacturing - signing with 2 MES systems
6 Seconds

Global Pharmaceutical, Labs – logon and signing, various apps
5 Seconds

Global Pharmaceutical, Packaging – signing with MES
11 Seconds

Global Pharmaceutical, Manufacturing – signing with MES system
12 Seconds

Additional Benefits

Improved ergonomics and operator satisfaction – strong results from user surveys

Reduced "interruption" for operator – allows process to be more natural

Improved data integrity – removing friction, removes human attempts to by-pass

Increased security

Enablement of strategic initiatives:

- Digital Transformation
- Health and safety
- Social distancing

Customer ROI and Cost Metrics

Password Resets & Account Lockouts:

Average cost of **$420** per employee per year to manage password resets

Password resets represent **20-50%** of IT helpdesk service requests

Average time unproductive while waiting for password reset is **10 minutes to 2 hours**



$70: average help desk labor cost for a single password reset



Passwords are the root cause of over **80%** of data breaches

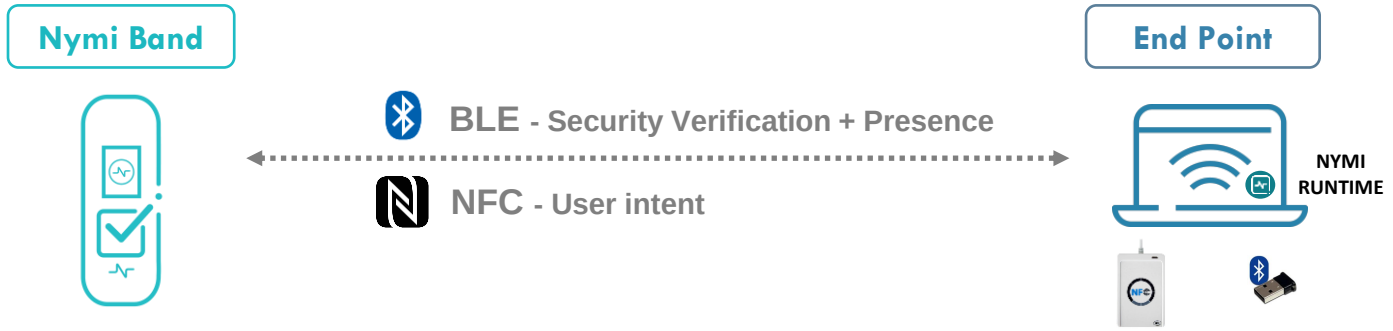
Operator Time Savings:

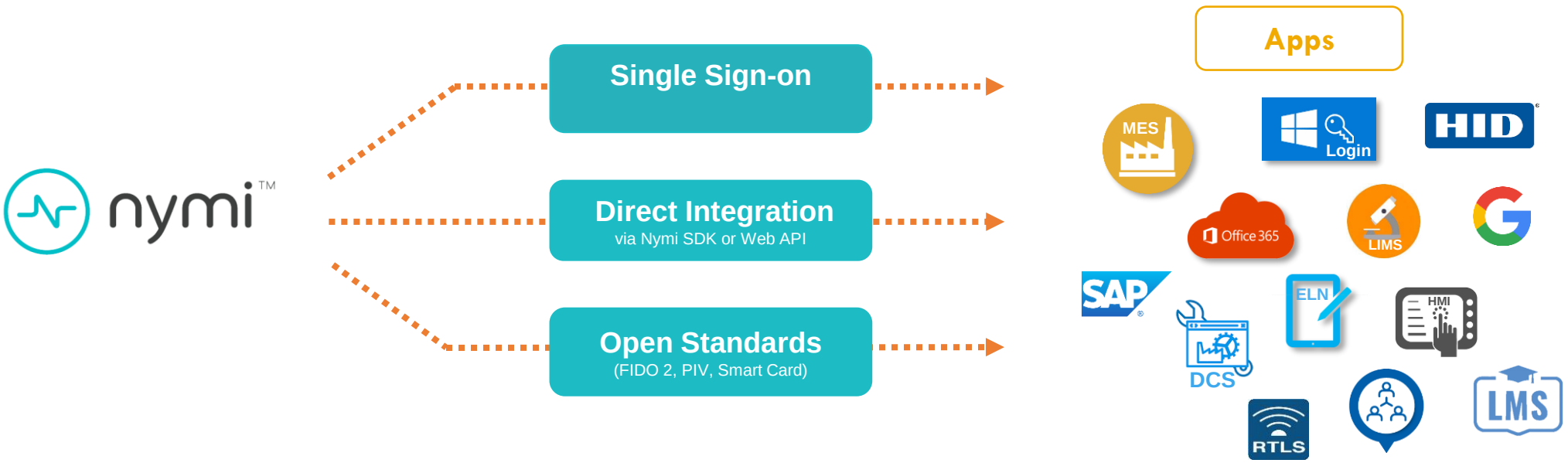
Average time saved per authentication	**10s**
Average authentications per day	**100**
Average shifts worked per year	**200**
Annual time savings per person	**55hrs**
Average hourly rate	**$40**

$2,200/year

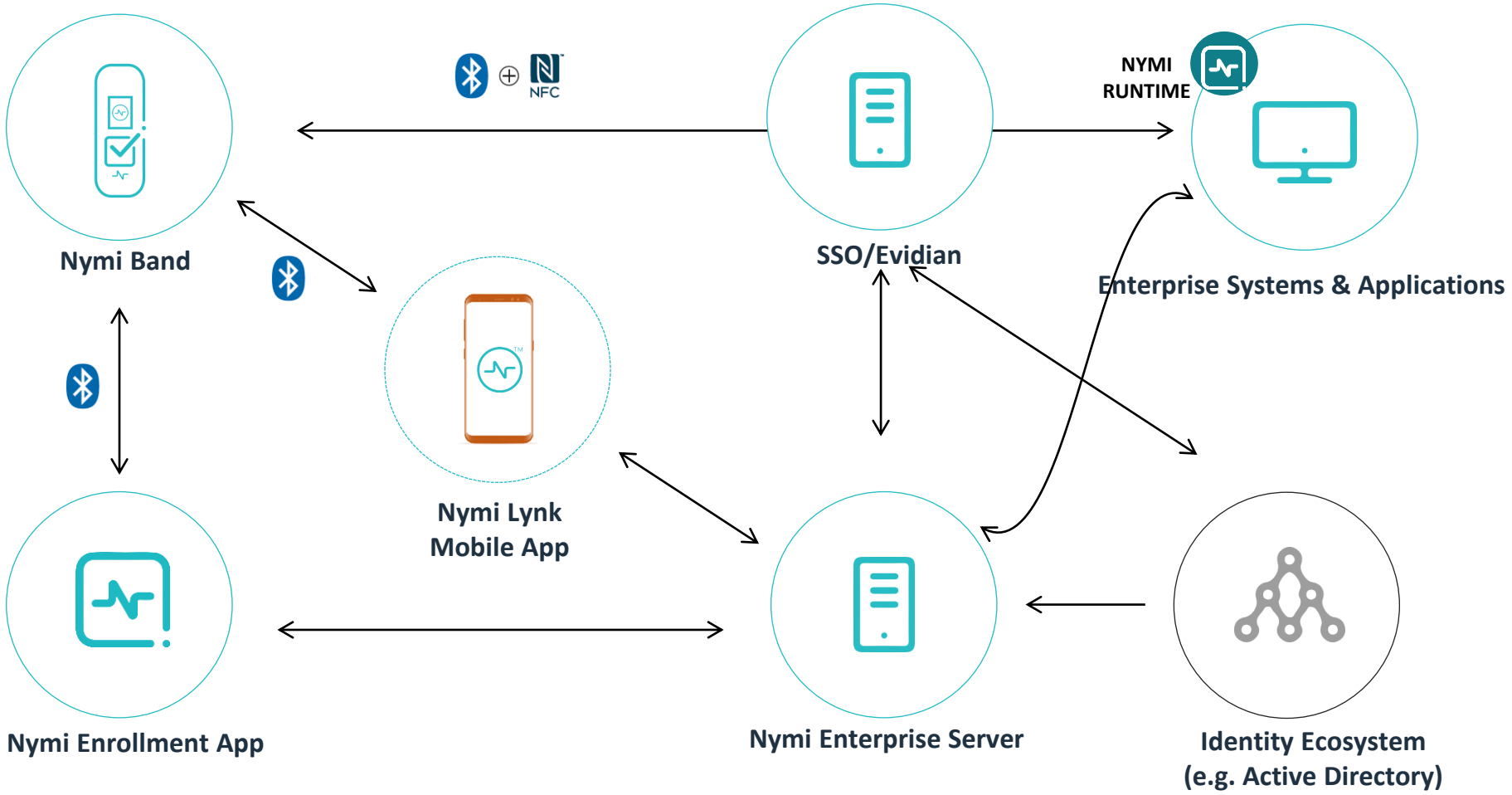
Average Savings per User

How Nymi Connects with Your Environment





Solution Architecture



Nymi Connected Worker Platform Components

- **Nymi Bands** are a biometrically-enabled wearable for digitizing the active worker. They are manufactured with unique cryptographic keys to ensure non-repudiation. They use secure NFC and encrypted BLE to communicate to the enrollment app and enterprise systems, sensors and applications, while using encrypted BLE to communicate with Nymi's My Digital Twin app.

- The **Nymi Enrollment App** is a Windows app for secure self-service enrollment of Nymi Bands.

- The **Nymi Enterprise Server** provides administration and enterprise services for the entire solution. This includes managing updates, backup and DR, scalability, security, policy management and integration with the enterprise identity system.

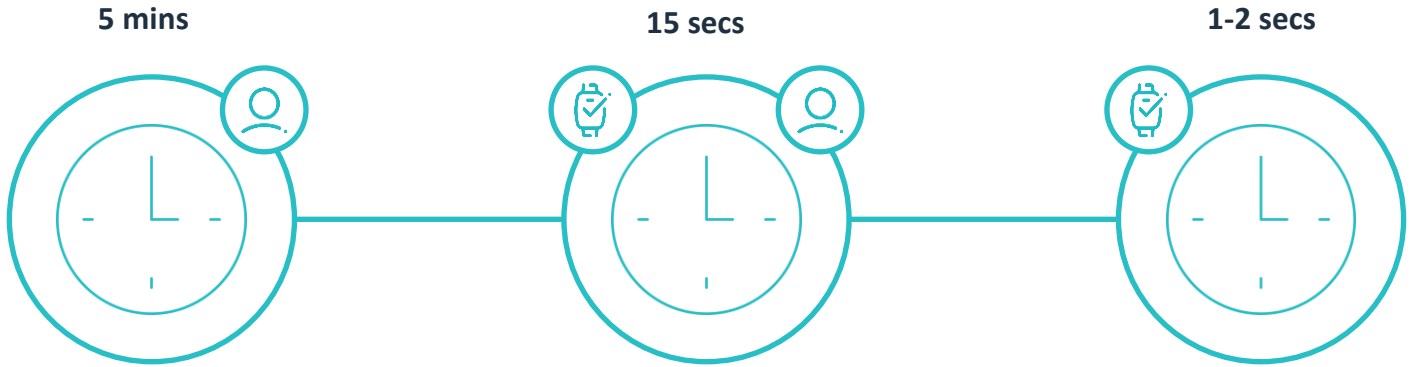
- The **Identity Ecosystem** provides the authoritative source for service personnel employees, partners and contractors that should be enabled in a system

- **Enterprise Systems and Applications** interact with the worker via secure BLE and NFC channels. Cryptographic certificates are used for authentication and signing. Integrations are enabled through a wide variety of standards, the Nymi API, and popular SSOs.

- The **Nymi Link App** provides the user with full control over their identity and privacy, enforces transparency in enterprise privacy policies and allows rich interaction with visualizations and apps.

Enrollment & Daily Use





Enrollment

One time

User Authenticates to Nymi Band

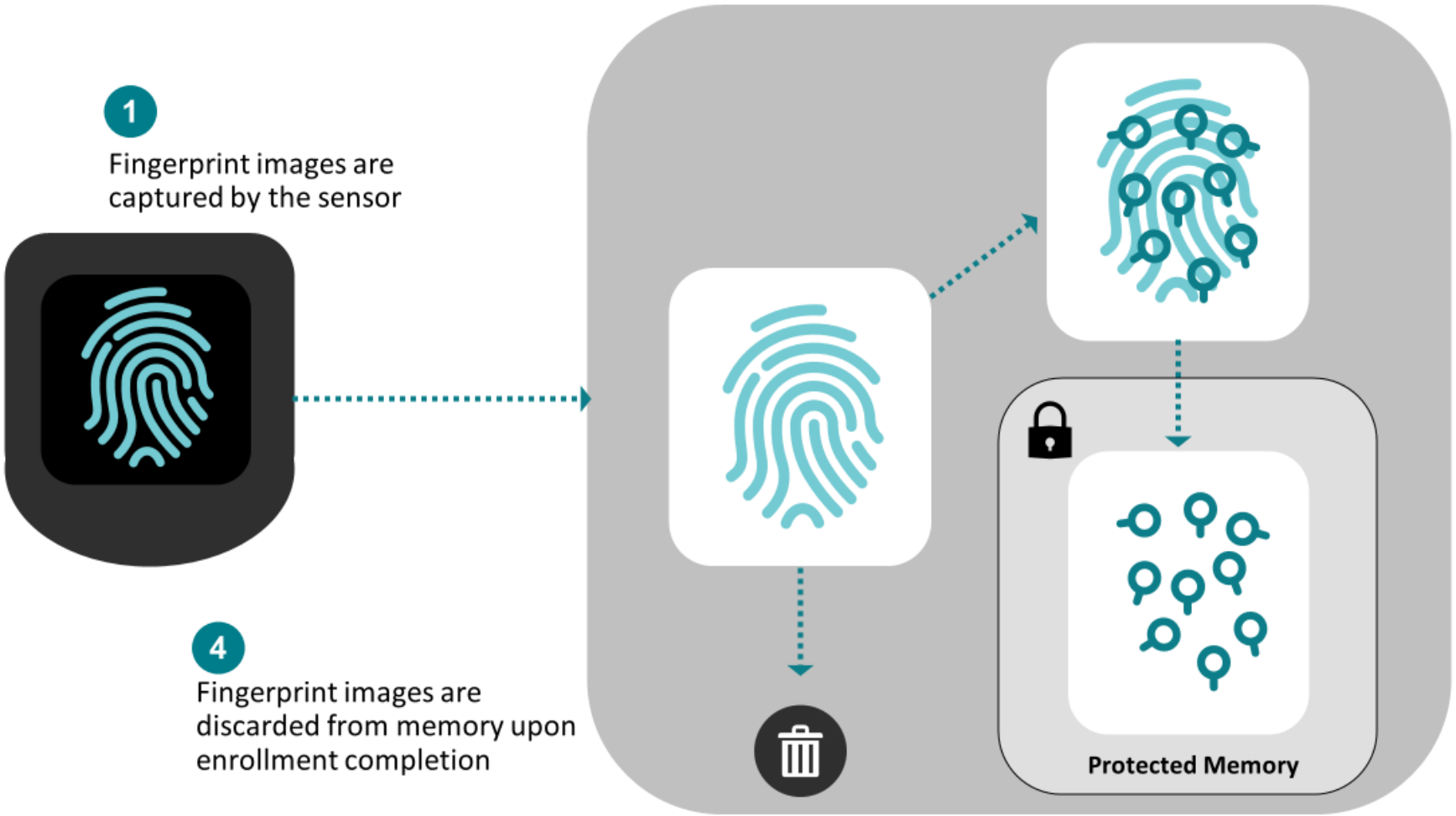
Once per shift

Open, Login, eSign

50-300 times per shift

Nymi Band™ Biometric Privacy

1 Fingerprint images are captured by the sensor



Cryptography

2 Unique features are extracted from images to create a mathematical template

3 Template is stored within protected memory and never transmitted; there is no mechanism to retrieve the template from the Nymi Band

4 Fingerprint images are discarded from memory upon enrollment completion

Biometrics is not used in the Nymi solution, outside of the Nymi Band.

A user's ECG template is not captured nor stored – the user's ECG is only compared against a generic human template.

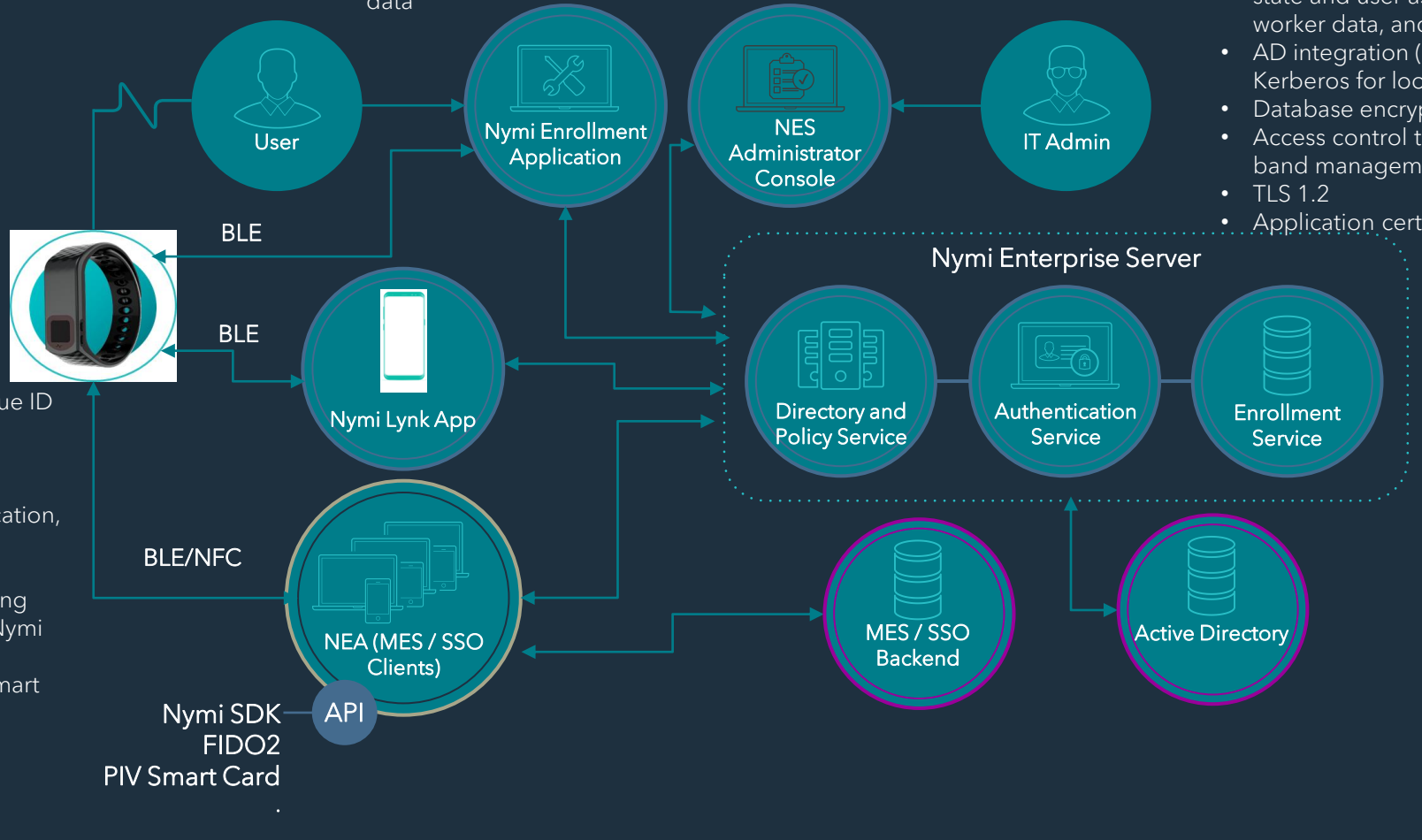
Security in Nymi Solution

- Biometric authentication required to unlock majority of functionalities
- Biometric never leaves the Nymi Band
- Secure storage with no external access
- Memory protection
- HardwaSecure boot / secure upgrade based on firmware signature
- re certificate burnt in at manufacturing time

- Orchestrate Nymi Band enrollment to bind Nymi Band, user (via biometric), and user's digital identities
- Does not process biometric data

- Facilitate system configuration and monitoring, and user and band management
- Access restricted to authorized IT admins

- Secure repository for Nymi Band identities, state and user assignments, policies, digital worker data, and audit logs
- AD integration (read-only) via LDAPS and Kerberos for lookup and user authentication
- Database encryption
- Access control to restrict data access and band management to authorized parties
- TLS 1.2
- Application certificate issuance



- NFC tap identifies device via unique ID then handover to secure BLE communication
- Nymi Security Protocol provides certificate-based mutual authentication, encryption and message integrity, equivalent to TLS 1.2
- BLE presence for OS session locking when user walks away / takes off Nymi Band
- NFC security via FIDO2 and PIV smart card protocols

BLE Specifications & Capabilities

BLE Communication is available on the Nymi Band

- Nymi Band BLE communication does not rely on Bluetooth security. All security is implemented in the Nymi-proprietary protocol layers.
  - The Nymi Security Protocol is modeled after TLS 1.2 and provides security for BLE communications with Nymi Bands.
  - Currently a USB Dongle is required to enable the NYMI Band to work on an endpoint
    - USB Slot needs to be available
    - Native Bluetooth being researched



NFC Specifications & Capabilities

NFC is available on the Nymi Band

- A typical use is to show user intent by tapping the Nymi Band on a NFC Reader
  - Intent to Login or Intent to provide an e-signature would require a tap on the NFC reader with a band (endpoints mainly)
  - Used widely in Pharma & Manufacturing where hundreds of authentications need to be done
  - On endpoints using NFC with the combination over BLE a tap would trigger the application on the endpoint t establish a secure session with the Nymi band
- For Physical Access similarly a “tap” would occur on the access reader to show intent by the user trying to access the room or building
  - Existing Access/Reader infrastructure may be supported, verification required
  - Readers need to have the necessary specs to be supported

nymi™

Recommended NFC Readers and Technical Specifications

In general, for a reader (endpoint) to be compatible with the Nymi Band, the following requirements must be met:

- **ISO14443A compatibility**
- **Operation frequency of 13.56MHz**
- **PC/SC compatibility**

Recommended Endpoint Readers

These readers are tested with every release. They are recommended to customers based on their superior performance.

Application	Model
General Use	HID Omnikey 5022

Supported Readers

These readers are tested with every release. They are suggested to customers if Nymi's recommended readers do not meet the particular needs of the customer.

Application	Model
General Use	ACS ACR122U
General Use / Cleanroom* *Silicone case req'd	Elatec TWN4 LEGIC NFC USB (P/N: T4DT-BB2BEL-NL)
Cleanroom / IPxx Rated / Single port BLE + NFC	Systec CONNECT BOX (using Elatec TWN4 MultiTech 3 module)

nymi™

Nymi Requirements at Endpoints

Software Requirements:

- ✓ Windows 10, 64-bit
- ✓ Windows 7, 32-bit & 64 –bit

Enrollment PC is needed if the User Terminals are not Windows 7/10 or a separate system is warranted for security/mgmt. purposes.

Hardware Requirements:

- ✓ 4GB RAM
- ✓ 5GB Free disk space
- ✓ 2 core CPU (recommended)
- ✓ 1-2 USB 2.0 ports
- ✓ Bluegiga BLED112 Bluetooth Low Energy (BLE) Dongle
- ✓ Nymi recommended NFC Reader

Installed on Endpoint:

- ✓ NBE/Nymi Runtime
- ✓ Evidian (EAM) Client (If Applicable)

nymi™

Nymi Requirements at Datacenter/Test Environment

Software Requirements

- ✓ Microsoft Windows Server 2012 R2 or Windows Server 2016
- ✓ Microsoft IIS
- ✓ Microsoft SQL Server 2012, 2016 or 2017
- ✓ Microsoft .NET Framework 4.8
- ✓ Read access to Domain Controller and Active Directory or other Authoritative Source

Hardware Requirements

1-5000 users:

- ✓ 4 Core CPU
- ✓ 8GB RAM
- ✓ 20GB free disk space

5000-10000:

- ✓ 4 Core CPU
- ✓ 16Gb RAM
- ✓ 40GB free disk space

Installed on Nymi server:

- ✓ Nymi Enterprise Server
- ✓ SQL Server Express (if no SQL DB to be used)
- ✓ Evidian Access Controller
- ✓ Proper Certificates (given by Nymi)

Changes to the Applications:

None

nymi™