nymi™ | WHITEPAPER

Zero-Trust Made Practical for the Modern Workforce

Security on the Nymi Connected Worker Platform

Table of Contents

Revision History

Version	Date	Summary of Changes
3.2	November 20, 2023	Editorial changes
3.1	August 22, 2022	Updated for design and proprietary changes
3.0	April 26, 2021	Updated for CWP 1.1 Release
2.2	April 2, 2021	Updated for NEE 3.3 Release
2.1	February 24, 2021	Clarification on protection of user biometric data (Section 2.3.1)
2.0	September 18, 2020	Updated for NEE 3.2.0 to include Evidian smart card integration
1.0	September 26, 2019	Initial version for NEE 2.4.0

Acronyms

Acronym	Definition
AD	(Microsoft) Active Directory
AD LDS	Active Directory Lightweight Directory Service
AES	Advanced Encryption Standard
API	Application Programming Interface
BLE	Bluetooth Low Energy
CA	Certificate Authority
CAPI	Microsoft Cryptographic API
CBC	Cipher Block Chaining
CMAC	Cipher-based Message Authentication Code
CNG	Microsoft Cryptographic API Next Generation
CSR	Certificate Signing Request
DLL	Dynamically-Linked Library
ECDH	Elliptic Curve Diffie Hellman
ECDSA	Elliptic Curve Digital Signature Algorithm
ECG	Electrocardiogram

Acronym	Definition
ES	Enrollment Service
GCM	Galois Counter Mode
HMAC	Hash-Based Message Authentication Code
IIS	Internet Information Service
JTAG	Joint Test Action Group
L1	Level 1
L2	Level 2
LDAP	Light Directory Access Protocol
LDAPS	Secure Light Directory Access Protocol
MAC	Medium Access Control
MCU	Micro-Controller Unit
NAPI	Nymi API
NBA	Nymi Band Application
NBE	Nymi Bluetooth Endpoint
NEA	Nymi-Enabled Application

Acronym	Definition
NES	Nymi Enterprise Server
NFC	Near Field Communication
NTS	Nymi Token Service
NTLM	NT LAN Manager
OTP	One-Time Password
PKCS	Public Key Cryptographic Standard
RSA	Rivest, Shamir and Adelman
SDK	Software Development Kit
SHA	Secure Hash Algorithm
TLS	Transport Layer Security
UI	User Interface
UID	Unique ID

1.0 Scope

This document describes the security architecture of the Connected Worker Platform (CWP), and how the Nymi solution provides always-on authentication, while protecting sensitive information and personal information.

Security features described in this version of the document are implemented in all current Connected Worker Platform Releases, unless otherwise stated.

1.1 Intended Audience

The intended audience for this document is current and prospective Nymi customers, and anybody who needs to understand and review the security architecture of the Connected Worker Platform.

1.2 Organization of the Document

The organization of the remainder of this document is as follows:

- Section 2 provides an introduction to the system components, concepts, and terminologies.
- Section 3 describes the core aspects of the CWP security architecture.
- Section 4 provides in-depth security analysis of the most common use cases involving CWP, and discusses how the solution safeguards the security of enterprise assets, and the security and privacy of personal data.

2.0 System Overview

2.1 High Level Description

The Nymi Connected Worker Platform connects people with their workplace technologies in one authentication. The Connected Worker Platform supports numerous use cases and digital systems integrations to converge point solutions into a single offering that is safe, secure, and simple.

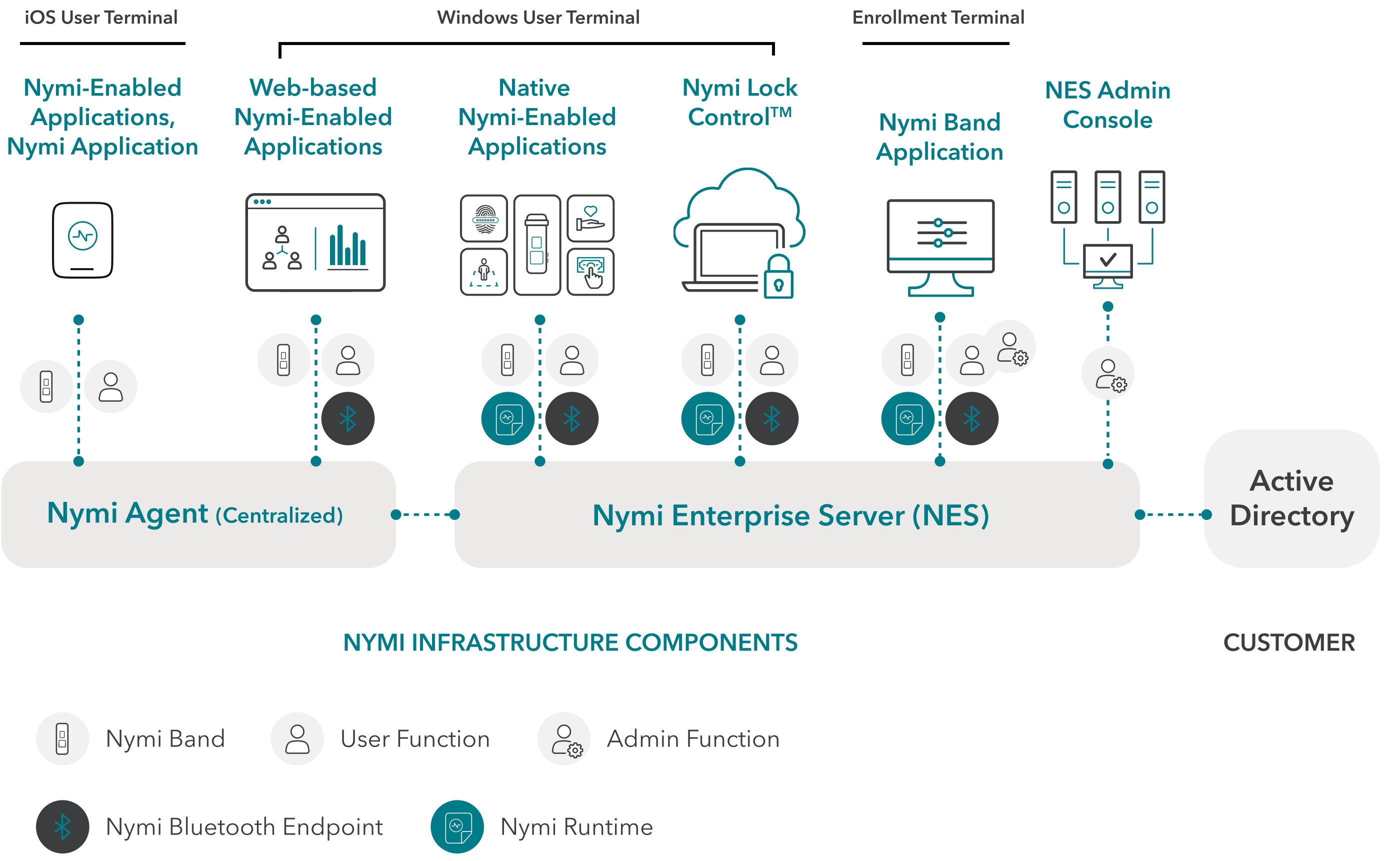
The Connected Worker Platform consists of both hardware and software components. The Nymi Band is a wearable device that allows wireless communication between users and digital systems. On-device biometrics ensure the identity of the user while integrated sensors convey information about the individual and their environment. Combined with supporting software, the Connected Worker Platform addresses numerous use cases. These include, but are not limited to:

- Physical Access
- Passwordless Windows Login
- Manufacturing Execution System (MES) Signing with Biometrics

- Automatic Terminal Locking through Presence (ie, Nymi Lock Control)
- Secure Printing
- Smart Distancing and Contact Tracing

The goal of the Connected Worker Platform is to simplify the connection of workers to the digital workspace found in modern organizations. When the barriers to secure digital work are removed, people can focus on what they do best and become more valuable assets to their business.

2.2 Ecosystem Diagram



2.3 Nymi Component Description

2.3.1 Nymi Band™ 3.0

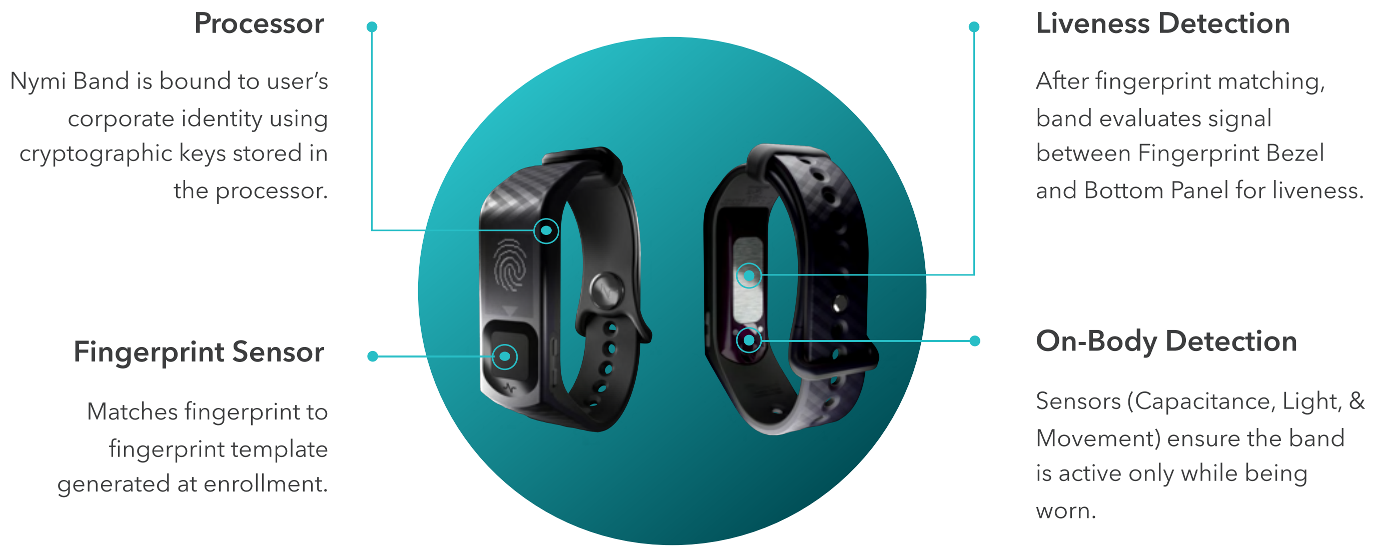
The Nymi Band 3.0 is the wearable component that acts as a secure cryptographic key chain for the user. Biometrics provide strong user authentication. An OLED display and buttons provide the user interface.

Nymi Band 3.0 supports three modes of integration with a wide range of applications, operating systems, and middleware (all referred to as "applications" in the rest of this document):

- Nymi-Enabled Applications (NEAs) integrate with Nymi Bands by using the Nymi API. In this mode of integration, the Nymi Bands communicate securely with the Nymi SDK Runtime and the NEA, over Bluetooth Low Energy (BLE) and Near Field Communications (NFC) protocols.
- Applications can integrate with Nymi Bands by using FIDO U2F or FIDO 2.0 securely over the NFC protocol.

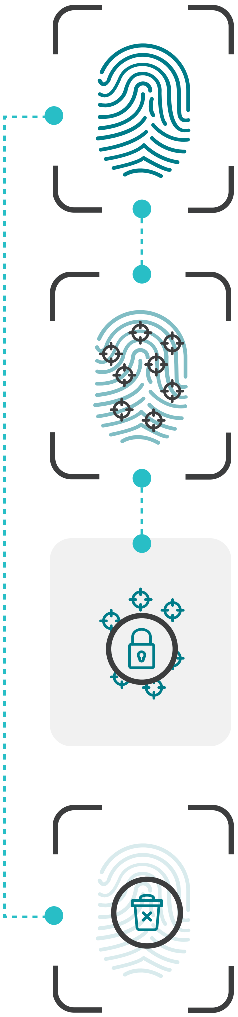
Nymi Band is engineered with superior security and privacy as key requirements. The following focuses on how the Nymi Band keeps the user's biometrics data secure, thus safeguarding the user's privacy.

The user is authenticated on their Nymi Band through biometrics, and the biometrics data (fingerprint and ECG signals) never leaves the Nymi Band. The ECG signal is only used to verify "liveness" of the fingerprint and not used for authentication.


Processor
Nymi Band is bound to user's corporate identity using cryptographic keys stored in the processor.
Fingerprint Sensor
Matches fingerprint to fingerprint template generated at enrollment.
Liveness Detection
After fingerprint matching, band evaluates signal between Fingerprint Bezel and Bottom Panel for liveness.
On-Body Detection
Sensors (Capacitance, Light, & Movement) ensure the band is active only while being worn.

During user enrollment, fingerprint images are captured on the Nymi Band and converted into a mathematical template of unique features found on the fingerprint. Once enrollment is complete the images are discarded. Only the fingerprint template is stored and in a protected memory region of the Nymi Band's microcontroller (MCU).

Please refer to the following diagram:



1. Fingerprint images are captured by the sensor and sent to the MCU

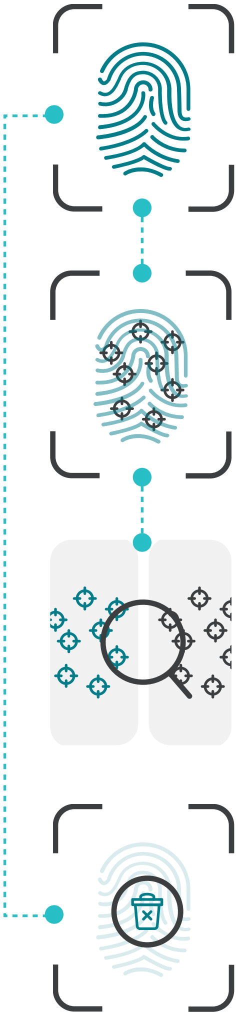
2. Unique features are extracted from fingerprint images to create a mathematical template

3. Fingerprint template is stored within protected memory on the MCU and is never transmitted outside the MCU

4. Fingerprint images are discarded from memory upon enrollment completion

During authentication, the user's fingerprint image is matched against the fingerprint template that is stored on the MCU. The fingerprint image is discarded after authentication.

Please refer to the following diagram:



1. A fingerprint image is analyzed by the sensor and sent to the MCU

2. Unique features are extracted from the incoming fingerprint image

3. Features are compared against the stored template to determine if they match

4. Fingerprint image is discarded from memory upon match completion

The fingerprint template, cryptographic keys and certificates are considered sensitive data and design measures are in place to safeguard them:

- The physical access ports to the MCU (USB, serial and JTAG) are disabled by design, during manufacturing, which prevents subsequent access.
- Sensitive data is stored in protected memory inside the MCU. This memory cannot be read by an external entity outside the MCU, and can only be accessed by the firmware that is running on the MCU.
- The only method to load firmware onto a Nymi Band is via the bootloader over the Bluetooth interface. Nymi Band firmware is encrypted and digitally signed. The firmware digital signature is verified after it is uploaded to the Nymi Band (secure upgrade), and is again verified every time the Nymi Band starts up (secure boot). Malicious firmware that attempts to read the protected memory cannot be loaded into or executed on the Nymi Band, as it lacks the required digital signature.
- The bootloader, along with the cryptographic keys used by the secure upgrade and secure boot processes, are protected by read-only memory regions and a memory firewall.

At any time, the user may perform a “Delete User Data'' operation, to permanently erase all sensitive user data, including the user’s fingerprint template, on their Nymi Band.[1]

2.3.2 Nymi Enterprise Server (NES)

Nymi Enterprise Server (NES) handles centralized functionalities that are required for the deployment, operations, and management of the Nymi Bands and other Nymi software components. NES has the following main functionalities:

1. Allows storage and retrieval of information that is necessary for usage and management of Nymi Bands, for example, Nymi Band to Nymi User mapping, and dissemination of the NES security policy, through the NES Directory and Policy Service.
2. Issues authentication tokens to NEAs, through the NES Enrollment Service and the Nymi Token Service (NTS).
3. Allows user authentication to Active Directory during Nymi Band enrollment.
4. Supports Nymi Band management and NES security policy configuration through the NES Administrator Console.

NES makes use of Microsoft Internet Information Service (IIS), and Microsoft SQL Server.

[1] As the protected memory is inaccessible from outside the Nymi Band, it is impossible for a user to verify directly that their fingerprint template has indeed been deleted. Instead, the user can rely on Nymi’s design process and external audits, to confirm that the “Delete User Data'' operation is performing as intended.

2.3.3 Nymi Band Application (NBA)

Nymi Band Application (NBA) is a Windows desktop application that allows users to enroll their Nymi Band. From an architecture perspective, NBA is an NEA with special management privileges.

NBA performs the following functions:

- Orchestrates user authentication, Nymi Band authentication, enrollment of a fingerprint template and other authentication credentials.
- Provides the necessary information to NES, which NES stores in a SQL database, to support subsequent management and operation of Nymi Bands.

2.3.4 Nymi Lock Control™

Nymi Lock Control is an application that provides users with the ability to manage access to a Windows machine, without typing a username and password. Nymi Lock Control verifies user access through Active Directory.

When you install Nymi Lock Control on a user terminal, the following functionality is supported:

- Unlocking or logging into a terminal by tapping an authenticated Nymi Band on an NFC reader or a Bluetooth adaptor that is attached to the terminal.
- Unlocking or logging into a terminal by placing an authenticated Nymi Band within the range of the Bluetooth adapter, and clicking the Submit button on the Nymi Credential Provider Login screen.
- Automatically unlocking or logging into a terminal by placing an authenticated Nymi Band within range of the Bluetooth adapter and tapping their keyboard.
- Locking the user terminal when the authenticated user is not within the Bluetooth range of the terminal or when the user removes their Nymi Band.
- Preventing a user terminal from locking by keeping an authenticated Nymi Band within Bluetooth range.

2.3.5 Nymi-Enabled Applications (NEAs)

Nymi provides an SDK that allows developers to build Nymi-Enabled Applications (NEAs). When the NEA is integrated with the Connected Worker Platform, the solution can perform tasks such as application login and electronic signatures.

NEAs can be a web application or native application that makes use of the Nymi Band's security functions.

2.3.6 Nymi SDK

The Nymi SDK serves two purposes:

- Provides access to the Nymi API (via either a C language interface or a Websocket interface), which enables developers to create NEAs.

- Provides the Nymi Runtime, which includes the Nymi Agent and Nymi Bluetooth Endpoint (NBE) services that communicates with Nymi Bands via the Nymi Security Protocol.

Nymi SDK contains three components: Nymi Agent, Nymi Bluetooth Endpoint (NBE), and Nymi API (NAPI) DLL:

- Nymi Agent facilitates communication between NEAs and the Nymi Bands, and maintains knowledge of Nymi Band presence and authentication states. In addition, it provides access to the Nymi API via the websocket interface.

- NBE provides local BLE communications with Nymi Bands through the Nymi-provided Bluegiga dongle. NBE also detects NFC taps and reads the NFC Unique Identifier (UID) from detected Nymi Bands.

- NAPI DLL provides NEAs access to Nymi Band functionalities via the Nymi API C interface. It also manages NEA certificates and allows secure communications with Nymi Bands via the Nymi Security Protocol.

The Nymi Agent may be deployed either locally or centrally:

- Deploy a local Nymi Agent when an NEA that is using the Nymi API C Interface (via the NAPI DLL component) is running locally. In this scenario, the Nymi Agent runs on the same machine as the Nymi Bluetooth Endpoint, the BLE Adapter and the NFC reader).

- Deploy a centralized Nymi Agent in the following situations:

  a. When the NEA runs on a different machine from the NBE, BLE adapter, and NFC reader. For example, the NEA may run on a centralized Citrix / RDP server, while the NBE, BLE adapter, and NFC reader are on terminals running Citrix / RDP clients.

  b. When the NEA uses the Nymi API WebSocket Interface.

The different deployment options discussed previously can co-exist, for example, electronic signature operations on an MES can rely on a centralized Nymi Agent deployment, while NBA and Lock Control rely on a local Nymi Agent deployment. However, note that on each workstation machine, only one NBE instance can exist, and you can configure NBE to use the local Nymi Agent or the centralized Nymi Agent, but not both simultaneously.

2.3.7 Nymi Contact Tracing Services (CTS) and Contact Tracing Collection Agent (CTCA)

Nymi Contract Tracing Services (CTS) are the core of the contact tracing feature on the Connected Worker Platform, and are responsible for the collection, processing, storage, and presentation of the contact tracing data. The CTS consist of the following components:

- CT Consumer Service
- Apache Kafka
- CT Dashboard / CT API Service

Raw contact tracing data is generated by Nymi Bands, collected by the Contact Tracing Collection Agent (CTCA). and processed by the CT Consumer service, using Apache Kafka as the data pipeline. The Contact Tracing data is stored in a Microsoft SQL Server database.

The CT Dashboard / CT API Service allows authorized administrators to access and visualize the contact tracing data via any supported web browsers. The CT Dashboard / CT API are powered by Node.js Express.

All CTS components are deployed via containers, orchestrated via Kubernetes.

2.4 Evidian Integration with the Connected Worker Platform

Evidian is an enterprise single sign-on (SSO) middleware. Evidian supports passwordless Windows logon, application sign-in, and electronic signature, with legacy applications and OS environments that only support username and password.

In an Evidian integration with the Nymi Connected Worker Platform, a user's password vault is secured by the user's Nymi Band. SSO operations are possible only after the user wears and authenticates their Nymi Band, for example, by using their fingerprint.

Evidian integration is based on the general architecture described in Section 2.2 Ecosystem Diagram and Section 2.3 Nymi Component Description. The Evidian Access Management Client is the Nymi-Enabled Application in the architecture and it can be deployed on Citrix / RDP servers that communicate with a centralized Nymi Agent.

The Nymi Connected Worker Platform supports simultaneous Nymi Band enrollment to both NES and to Evidian.

Evidian integration involves a few additional components described in the following subsections.

2.4.1 Evidian Access Management Client

The Evidian Access Management (EAM) Client performs Windows login / unlock / lock, application login (SSO), and e-signature operations by using Nymi Bands as authenticators. The following modes of integration are supported:

- Wearable: Utilizes NFC taps for intent, followed by Nymi Security Protocol over BLE for authentication. From the Nymi architecture perspective, the EAM Client is an NEA. This is the default mode of integration.
- RFID badge: Utilizes the NFC Unique Identifier (UID) only, without the use of the Nymi Security Protocol over BLE. The RFID mode offers a simpler way of deploying the Evidian solution, and is also useful in situations where only one USB port is available on the client devices.

The EAM Client invokes the NBA to perform the Nymi Band enrollment operations.

2.4.2 Evidian Access Management Controller

The Evidian Access Management (EAM) Controller is responsible for overall management of authenticators, users, and SSO credentials. During Nymi Band enrollment, Nymi Band information (e.g., NFC UID, BLE MAC address, cryptographic key identifiers, etc.) are provided by the NBA to the EAM Controller, which stores the data in the LDAP Directory.

2.4.3 LDAP Directory

The Evidian solution stores users, authenticators, and SSO data in an LDAP directory by using either Active Directory (through AD schema extension), or a standalone instance of AD Lightweight Directory Service (AD LDS).

3.0 Connected Worker Platform Security Architecture

This section describes a few key components of the Connected Worker Platform security architecture from a system perspective.

3.1 Cryptographic Algorithms and Security Protocols

Cryptographic algorithms are used in many areas of the Connected Worker Platform to provide the following security functions:

- Authentication (of Nymi Bands, NEAs, and other Nymi components)
- Data encryption (in communication protocols and storage)
- Message authentication code
- Code signing in firmware

The following table summarizes the cryptographic protocols and key strengths that are used in various features of the Connected Worker Platform. All protocols and key strengths that are used meet the requirements for modern cryptography usage, and specifically the US National Institute of Science and Technology (NIST) requirements and recommendations.

Feature	Cryptographic Algorithm
Nymi Security Protocol over BLE	ECDSA / P-256 (certificate authentication) ECDH / P-256 and HMAC-SHA256 (key agreement) AES-GCM 128-bit (session encryption and message authenticity)
Credential protection	RSA 2048-bit AES-CBC 256-bit
Firmware protection	ECDSA / P-256 (firmware code signing) AES-CBC (firmware binary encryption)
FIDO2	ECDSA / P-256 (authentication) HMAC-SHA256 (HMAC secret extension)
Time-based One Time Password (RFC 6238)	HMAC-SHA1

Communications in IT environments (e.g., NES admin console access, NES web service API access, websocket connections) are secured by using TLS. Nymi recommends that you harden server environments to only use TLS 1.2 or above with modern cipher suites that are considered secure.

The Nymi Band and the Nymi SDK secure BLE communications by using the Nymi Security Protocol, which is further discussed in Section 3.4.1.

3.2 Nymi Band Security

3.2.1 User Authentication

3.2.1.1 Nymi Band Authentication States

After the user enrolls a Nymi Band, the Nymi Band operates in one of two authentication states: authenticated, or unauthenticated. In the unauthenticated state, the Nymi Band is limited to user authentication and band management functions. End-user security functions like assertion of user identity, NFC taps for intent, and creating additional credentials, are not available until the Nymi Band goes into the authenticated state through biometric authentication or Corporate Credentials Authentication.

3.2.1.2 Nymi Biometric Authentication

Biometric authentication on the Nymi Band by default uses fingerprint only. The electrocardiogram (ECG) sensors on the band may be utilized for liveness detection to provide an additional level of assurance during authentication that the provided fingerprint is from a live person, and that the Nymi Band is on the body of the user who is attempting fingerprint authentication (instead of being worn by a different user than the one performing the fingerprint authentication).

Biometric authentication enrollment happens during Nymi Band enrollment. After the user supplies fingerprint samples, the Nymi Band constructs and stores a fingerprint template, which never leaves the Nymi Band.

After the user successfully authenticates by using biometric authentication, the Nymi Band continuously performs On-Body Detection, i.e., verifies that the Nymi Band is still on the user's body by using a combination of different sensors. Once the Nymi Band determines that it is off-body, the Nymi Band transitions to the unauthenticated state.

3.2.1.3 Corporate Credentials Authentication

Corporate Credentials Authentication allows a user to authenticate to a Nymi Band using their AD username and password. Corporate Credentials Authentication is disabled by default within the NES Policy.

Corporate Credentials Authentication setup occurs during Nymi Band enrollment. NES generates an ECDSA key pair and passes the public key portion to NBA, which passes the public key portion to the Nymi Band. The private key stays on NES.

NBA and NES together perform Corporate Credentials Authentication. First, the user authenticates to NES by logging into NBA with their AD credentials. NBA then retrieves a nonce from the Nymi Band, and sends a request to NES to sign the nonce with the Corporate Credentials Authentication private key. NES enforces that the user is the only party that has the privilege to request a signature by using the Corporate Credential Authentication private key. NBA then passes the signature to the Nymi Band. If the signature verification succeeds, the Nymi Band transitions to the authenticated state.

On-Body Detection after authentication by using Corporate Credential Authentication works the same way as after authentication by using biometric authentication.

3.2.1.4 Configuration of Authentication Methods

The NES Administrator can configure the authentication methods that are allowed (biometric authentication, Corporate Credentials Authentication, or both) by using the NES Administrator Console. Based on the configuration, NBA controls the enrollment process and instructs the Nymi Band to perform fingerprint enrollment and/or Corporate Credentials Authentication enrollment. At least one authentication method must be enrolled on a Nymi Band.

Biometric authentication offers improved assurance that the user performing fingerprint authentication is the same user wearing the band, while Corporate Credentials Authentication provides a convenient backup mode of authentication. NES Administrators need to consider the specific security and usability requirements in their environments and configure the allowed authentication methods accordingly.

3.2.2 Public Key Infrastructure

PKI certificates are used for mutual authentication between Nymi Bands and NEAs. The use of certificates enhances security by eliminating the need for key sharing to support multiple-terminal operations (large number of NEAs being able to authenticate to a Nymi Band), and permits offline operations of NEAs. There are two types of end-entity certificates:

- Nymi Band certificate: authenticates a Nymi Band to an NEA and resides on a Nymi Band. During manufacturing, each Nymi Band generates a unique key pair, and the Nymi Band PKI issues a certificate to the Nymi Band.

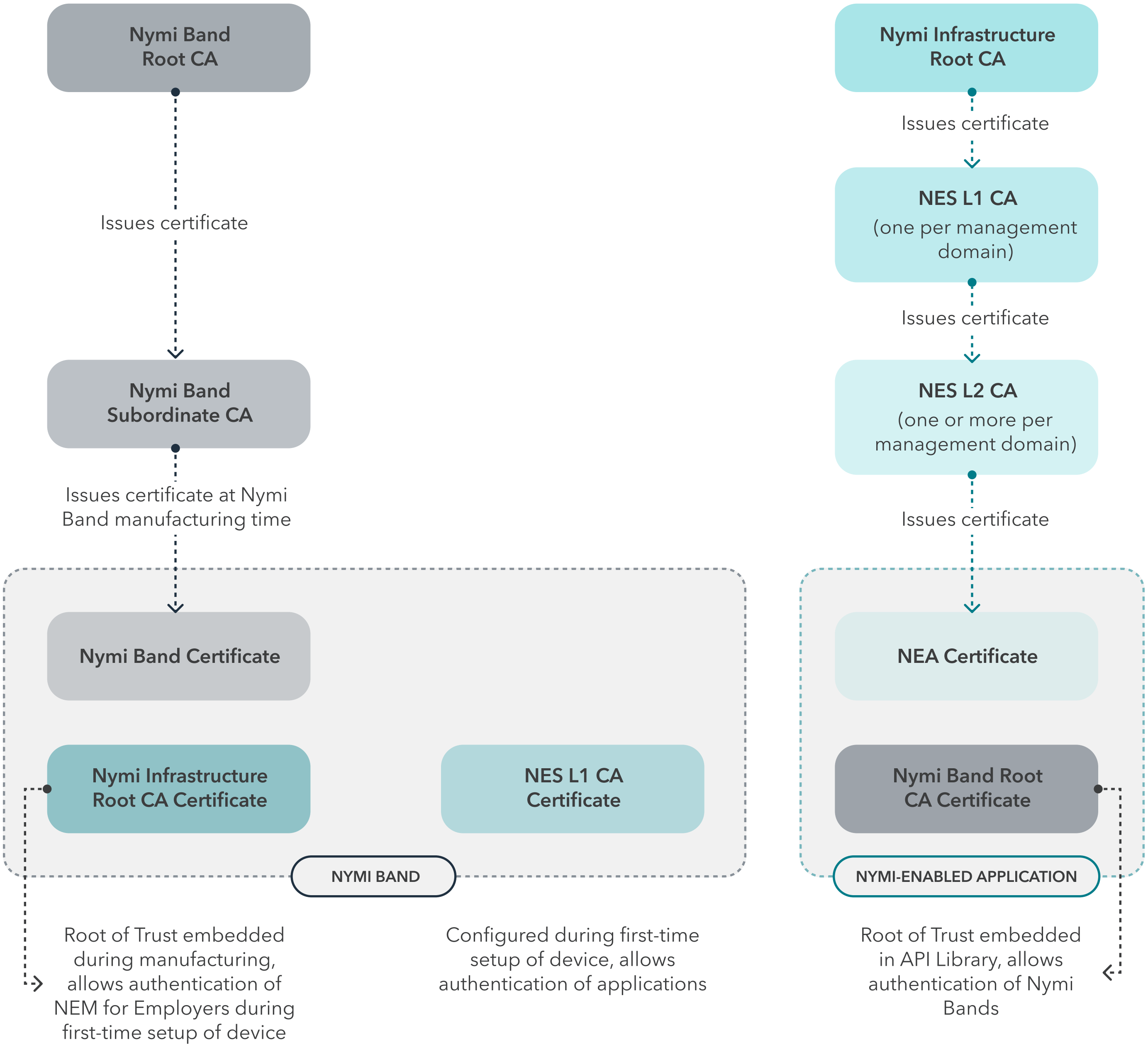
- NEA certificate: authenticates an NEA to the Nymi Band and is installed by the SDK on the NEA machine. Different instances of the same NEA that run on different machines, each have their own key pair and NEA certificate. NEA certificates are issued by NES at the first-time launch of an NEA.

All certificates that are described in this section are used only for communications between Nymi Bands and Nymi-enabled Applications. Specifically, NES requires a server certificate, which is unrelated to the Nymi Band certificate and NEA certificate discussed here. The NES certificate is a regular TLS server certificate, similar to other certificates that are used in an IT environment, which are issued by a trusted public PKI or the enterprise PKI, and are not issued by the Nymi Band and Nymi Infrastructure PKI.

Two public key infrastructures (PKIs) issue certificates for the Nymi solution:

- A Nymi Band PKI issues Nymi Band certificates.
- A Nymi Infrastructure PKI issues NEA certificates. Specifically, the NES Level 2 (L2) CA in this PKI issues NEA certificates by using the Nymi Token Service (NTS)

The following diagram depicts the PKI hierarchy.


Nymi Band Root CA
Issues certificate
Nymi Band Subordinate CA
Issues certificate at Nymi Band manufacturing time
Nymi Band Certificate
Nymi Infrastructure Root CA Certificate
NES L1 CA Certificate
NYMI BAND
Root of Trust embedded during manufacturing, allows authentication of NEM for Employers during first-time setup of device
Configured during first-time setup of device, allows authentication of applications
Nymi Infrastructure Root CA
Issues certificate
NES L1 CA (one per management domain)
Issues certificate
NES L2 CA (one or more per management domain)
Issues certificate
NEA Certificate
Nymi Band Root CA Certificate
NYMI-ENABLED APPLICATION
Root of Trust embedded in API Library, allows authentication of Nymi Bands

3.2.2.1 Bind to Enterprise

During initial enrollment of a Nymi Band, NBA initiates the “bind to enterprise” operation, during which the NBA loads the NES Level 1 CA certificate into the Nymi Band. After binding, the following results occur:

- Only NEAs with certificates chaining back to the NES L1 CA can perform authentication and secure access with the Nymi Band.
- Only NBA / NES with certificates chaining back to the NES Level 1 CA can manage the Nymi Band (e.g., configuration, external authentication).

3.2.2.2 Certificate Enrollment

Nymi Band certificate enrollment is performed during manufacturing. The Nymi Band generates a Nymi Band key pair and stores it in the on-band secure storage, and then generates a PKCS #10 Certificate Signing Request (CSR) that is signed by the Nymi Band private key. The CSR is then retrieved from the Nymi Band and sent to the Nymi Band Subordinate CA. The CA verifies the CSR, signs the certificate, and returns it to the Nymi Band for secure storage. The Nymi Band private key never leaves the Nymi Band.

NEA certificate enrollment is performed during first-time execution of the NEA. Key generation and CSR creation are performed in a similar fashion as in Nymi Band certificate enrollment. NES Enrollment Service and NTS performs additional authentication of the CSR origination point by using AD credentials, verification of CSR subject, and authorization of the CSR using a challenge password.

3.2.2.3 Root-of-trust provisioning on Nymi Band and NAPI DLL

During manufacturing, the Nymi Infrastructure Root CA certificate is loaded onto each Nymi Band. This allows the Nymi Band to authenticate any NEA with a valid NEA certificate that is issued by the Nymi Infrastructure PKI.

On the NAPI DLL side, the Nymi Band Root CA certificate is embedded into the library. This allows the NAPI DLL to authenticate any Nymi Band that has a valid Nymi Band certificate. The Nymi API websocket interface of Nymi Agent similarly has an embedded Nymi Band Root CA certificate.

3.2.3 BLE Communication Security

The Nymi Band and the NAPI DLL are the two end points of all Nymi Band communications over BLE. Nymi Band BLE communication does not rely on Bluetooth security. All security is implemented in the Nymi-proprietary protocol layers.

3.2.3.1 Nymi Security Protocol

The Nymi Security Protocol is modeled after TLS 1.2 and provides security for BLE communications with Nymi Bands.

The first phase of setting up a BLE secure session is called "Validation", and it is akin to TLS handshake. Validation involves the NEA and Nymi Band performing mutual authentication by using the NEA certificate and Nymi Band certificate, and establishing a session key by using Elliptic Curve Diffie Hellman (ECDH) with ephemeral keys to achieve perfect forward secrecy.

After the successful completion of the Validation phase, secure data transfers can happen between the Nymi Band and the NEA. The use of AES-GCM ensures security by providing message encryption, message origin authentication, tamper detection, and (with the inclusion of a message sequence number) replay protection.

3.2.3.2 Presence

The purpose of presence advertising is to announce the presence of a Nymi Band to nearby NEAs. Presence advertising uses BLE advertising packets that are sent by Nymi Bands and received by NBEs, and informs NEAs about the presence of a Nymi Band, and the authentication state of the band.

The NAPI DLL reports the state presence of a Nymi Band to NEAs. A Nymi Band can be in one of the following states:

- Absent (NAPI has not heard from this Nymi Band for a certain period of time, or the Nymi Band has been taken off-body)
- Unauthenticated (Nymi Band is bound to enterprise, but in unauthenticated state)
- Weak (Nymi Band is in authenticated state)[2]

Each BLE advertising packet contains the following fields:

- BLE MAC address of the Nymi Band
- Flags indicating device states, e.g., whether it is in the authenticated state, and whether it can accept connection requests.

In cases that require the highest assurance of user / band presence , an NEA can use the `assert_identity` API call as a point-in-time authentication without the risk of replay, as presented by the BLE advertisement.

3.2.4 NFC

Nymi Band supports a number of features over NFC.

[2] A "strong" presence state, where the Nymi Band is in authenticated state and a cryptographic message authentication code is used to limit replay of this information, is a roadmap item.

3.2.4.1 FIDO 2.0 / U2F

The Nymi Band supports FIDO 2.0 and Universal Two-Factor (U2F) authenticator functionalities over NFC. FIDO 2.0 / U2F relying parties (RPs) can create an asymmetric authentication key pair that is scoped to the RP, and then can subsequently perform authentication using the key pair, using the FIDO2 `authenticatorMakeCredential` and `authenticatorGetAssertion` operations. FIDO 2.0 and U2F support ECDSA algorithm with P-256 curves.

Enrollment of FIDO 2.0 / U2F credentials are performed after the Nymi Band enrollment process.

The FIDO protocol is inherently secure by virtue of the protocol design:

- Authentication makes use of public key cryptography via a challenge-response mechanism. The private key is never shared outside of the authenticator.
- Where a symmetric key needs to be retrieved from the authenticator (using the FIDO2 HMAC Secret extension), the key retrieval is protected for confidentiality and integrity by a secure session.

The FIDO implementation in Nymi Bands does not require (nor does it support) the use of a PIN for user verification. Instead, fingerprint authentication and On-Body Detection provide the necessary user intent and user authentication.

3.2.4.2 NFC UID

The Nymi Band also supports the retrieval of an ISO 14443 Unique Identifier (UID) over NFC. Retrieval of the NFC UID supports use cases such as the implementation of NFC tap for user intent. For example, a user can tap the Nymi Band on an NFC reader to indicate the intent to unlock a computer. The tap triggers the NEA to establish a secure session with the Nymi Band over BLE and the NEA uses the stored cryptographic material for unlocking purposes.

3.3 IT Integration and Security

3.3.1 Active Directory Integration

The Nymi Connected Worker Platform is designed for seamless integration into Active Directory (AD) environments. AD is used in a number of scenarios:

- For authentication of users by the NBA to enable user management of Nymi Bands (e.g., Nymi Band enrollment).
- For user authentication and authorization during access to the NES Administrator Console.
- For user authentication and authorization during access to the Contact Tracing Dashboard.
- For verification of user status (e.g., is a user account still active in AD) after an `assert_identity` operation.

- For client authentication when the NAPI DLL needs to access NES for privileged operations.

The Connected Worker Platform integration with AD is limited to performing authentication of users and computers (via Kerberos, NTLM, or LDAPS), and looking up user status and group membership (via LDAP and LDAPS). You can integrate an NES instance into one or more Active Directory domains and forests. (The Contact Tracing Dashboard currently supports integration with a single AD domain.)

Specifically, the Nymi Connected Worker Platform does not write to AD.

3.3.2 Authentication and Authorization

3.3.2.1 NES Administrator Console Access

NES provides a secure web-based application to manage users, Nymi Bands, and applications policies. Access to perform administrative functions in NES is granted when a user that has the NES Admin privilege logs into the application. The NES Admin privilege is based on membership in the Active Directory group that was specified during NES deployment.

3.3.2.2 NES API Access

Access to the privileged NES API requires either domain membership (user or computer), or NES Admin privilege, depending on the particular API and the scope of the operation.

Authentication is performed over Kerberos (with fallback to NTLM), or via domain username / password in the case when an administrator logs in via the NES Administrator Console. Once authenticated, an authentication token is issued by NES to the requesting entity for authorizing subsequent access.

3.3.2.3 NBA Access

NBA access requires user login by using their Active Directory domain user credentials.

3.3.2.4 Contact Tracing Dashboard / API Access

Contact Tracing Dashboard / API Access is restricted to authorized individual based on membership in the appropriate Active Directory groups that are specified at the time of deploying the Contact Tracing Services.

Dashboard user authenticates to the Contact Tracing Dashboard using their Active Directory domain user credentials.

3.3.2.5 Contact Tracing Services Access

The Contract Tracing Services are based on Apache Kafka, and has the following security features:

- Access control to Kafka is enforced via user accounts.
- Authentication is performed using the SASL-SSL protocol.

- Kafka user credentials on CTCAs are encrypted via RSA encryption.

- Kafka user credentials and TLS private key on the CTS are protected via Kubernetes secrets encrypted at rest using AES encryption. For AWS-based deployment, AWS KMS can optionally be used for further protection.

3.3.2.6 Microsoft SQL Server Access

Access to Microsoft SQL Server by NES is authorized through appropriate Active Directory user accounts or SQL Server user accounts.

Access to Microsoft SQL Server by the Contact Tracing Services is authorized through appropriate SQL Server user accounts.

3.3.3 Network Port Usage

The table below summarizes the default network port usage in the Nymi solution. This is in addition to any ports required for a standard Windows Active Directory environment. IT administrators may customize the ports based on deployment needs. In some cases, changes to the default port is mandatory (e.g., when the Nymi Agent and NES are co-located on the same server).

If load balancers are used, firewall rules should be adjusted based on the load balancer configuration.

Source	Destination	Port and Protocol	Application Protocol	Note
NBA	NES	443/TCP 80/TCP	HTTPS HTTP	1
NEA with Nymi API DLL	NES	443/TCP 80/TCP	HTTPS HTTP	1
Nymi Agent (centralized)	NES	443/TCP 80/TCP	HTTPS HTTP	1
NES Admin Console **NES** (Browser)	NES	443/TCP 80/TCP	HTTPS HTTP	1
CTCA	NES	443/TCP 80/TCP	HTTPS HTTP	1

Source	Destination	Port and Protocol	Application Protocol	Note
NEA with Nymi API DLL (RDP / Citrix deployment)	Nymi Agent (centralized)	9120/TCP 443/TCP	HTTP (WebSocket) HTTPS (WebSocket)	2
CTCA (RDP / Citrix deployment)	Nymi Agent (centralized)	9120/TCP 443/TCP	HTTP (WebSocket) HTTPS (WebSocket)	2
Nymi Bluetooth Endpoint	Nymi Agent (centralized)	9120/TCP 443/TCP	HTTP (WebSocket) HTTPS (WebSocket)	2
NEA using Websocket API	Nymi Agent (centralized)	80/TCP 443/TCP	HTTP (WebSocket) HTTPS (WebSocket)	3
NES	NES	389/TCP 636/TCP	LDAP LDAPS	4
NES	Domain Controller	1433/TCP	MS SQL	
EAM Client	MS SQL Server	55000/TCP	LDAP	5
EAM Client	EAM Controller (AD LDS)	389/TCP	LDAP	6
EAM Client	Domain Controller	3644/TCP	SSPI to EAM Security Service	
CTCA	EAM Controller	9092/TCP	TLS	
Kafka (Load Balancer)	Kafka (Load Balancer)	30090-30094/ TCP	TLS	8

Source	Destination	Port and Protocol	Application Protocol	Note
CT Consumer	NES	443/TCP 80/TCP	HTTPS HTTP	1
CT Consumer	MS SQL Server	1433/TCP	MS SQL	
CT Dashboard (Browser)	CT Dashboard (Load Balancer)	443/TCP	HTTPS	
CT Dashboard (Load Balancer)	CT Dashboard service	31443/TCP	HTTPS	
CT Dashboard / API Service	MS SQL Server	1433/TCP	MS SQL	
CT Dashboard / API Service	Domain Controller	636/TCP 389/TCP	LDAPS LDAP	7
Kubernetes nodes	Kubernetes apiserver	6443/TCP	HTTPS	
Web client Browser	Kubernetes dashboard	443/TCP	HTTPS	
Kubernetes nodes	Kubernetes etcd cluster	2379-2380/ TCP	etcd protocol	
Kubernetes control plane	Kubernetes worker nodes	10250/TCP	Communication with kubelet	
Kubernetes control plane	Kubernetes worker nodes	10255/TCP	Communication with kubelet (read-only)	

Source	Destination	Port and Protocol	Application Protocol	Note
Kubernetes control plane	Kubernetes nodes	10256/TCP	Health check	
Kubernetes nodes	Kubernetes nodes	179/TCP	BGP for pod-to-pod 9 networking	9
Kubernetes nodes	Kubernetes nodes	9500/TCP	Longhorn Container 10 Storage Interface	10
Kubernetes nodes **Kubernetes control plane**	Kubernetes control plane	53/TCP 53/UDP	DNS	

1. HTTPS is the default.
2. HTTP is the default, but Nymi recommends the use of HTTPS. The websocket interfaces on the Nymi Agent for Nymi API DLL and NBE only support HTTP. Use a TLS gateway in front of the Nymi Agent to enable HTTPS support. On the other hand, Nymi API DLL and NBE can be configured to use HTTPS natively.
3. HTTP is the default, but Nymi recommends the use of HTTPS. The websocket interface on the Nymi Agent for the Websocket API supports HTTPS natively (unlike note 2 above).
4. LDAP is the default.
5. For Evidian deployments that use dedicated AD LDS instances.
6. For Evidian deployments that use LDAP schema extension on the Active Directory domain controller.
7. Use of LDAPS is highly recommended unless the traffic is over a trusted network.
8. For a three-node cluster. More ports will be needed for additional nodes.
9. Only required for multi-network Kubernetes clusters (for site-to-site failover)
10. Only required for self-managed Kubernetes deployments.

4.0 Nymi Band Use Cases and Security Analysis

This section discusses the major use cases of the Nymi solution with specific focus on how the solution protects the security and privacy of corporate assets and user data.

4.1 Assert Identity

Assert Identity provides a mechanism for NEAs, e.g., Manufacturing Execution Systems (MESs), to confirm the identity of a user cryptographically, and optionally to confirm the account status of a user in Active Directory. Assert Identity is a passwordless way to perform electronic signatures that provides improved compliance and productivity.

The NEA monitors the intent of a user to authenticate (typically an NFC tap) through direct interaction with the NFC reader, or through the Nymi API. The NEA then uses the `lookup` operation to resolve the Nymi BandID, followed by the `assert_identity` operation to initiate an authentication with the Nymi Band and retrieve the user ID. NES administrators can configure the active policy in the NES Administrators Console to allow AD queries about the user status (i.e., is the user account active, inactive, or locked, and has the password expired) and to cache the information for a specified duration.

4.1.1 Authentication

The `assert_identity` operation removes the need for password authentication, and replaces it with certificate authentication by using the Nymi Band certificate.

The NFC tap and `assert_identity` operation can proceed only when the Nymi Band has authenticated the user and is on-body.

The user status check provides the NEA with information on whether the user has an inactive or locked account, so that the NEA can act accordingly.

4.1.2 Protection of Sensitive Data

No sensitive data is exchanged between the Nymi Band and Nymi SDK, as the authentication is performed using public key cryptography.

The Nymi SDK retrieves user identity and account status from NES / AD, and provides the information to the NEA. This information is protected in transit over the network via TLS (including Nymi API Websocket interface access, if the Nymi API Websocket interface is enabled with TLS).

4.2 FIDO 2.0

Nymi Bands support FIDO 2.0 and FIDO Universal Two-Factor (U2F) authenticator functionalities over NFC. This allows Nymi Bands to be integrated using standard protocols with any web applications and services that support FIDO 2.0 or U2F authentication, and a browser that supports the protocols over NFC, e.g., Microsoft Edge.

4.2.1 Authentication

FIDO 2.0 removes the need for password authentication. The user's Nymi Band is authenticated by using the FIDO 2.0 credentials that are created by the FIDO 2.0 relying party.

FIDO 2.0 operations, including creating new credentials and authenticating against a relying party, can proceed only when the Nymi Band has authenticated the user and is on-body.

4.2.2 Protection of Sensitive Data

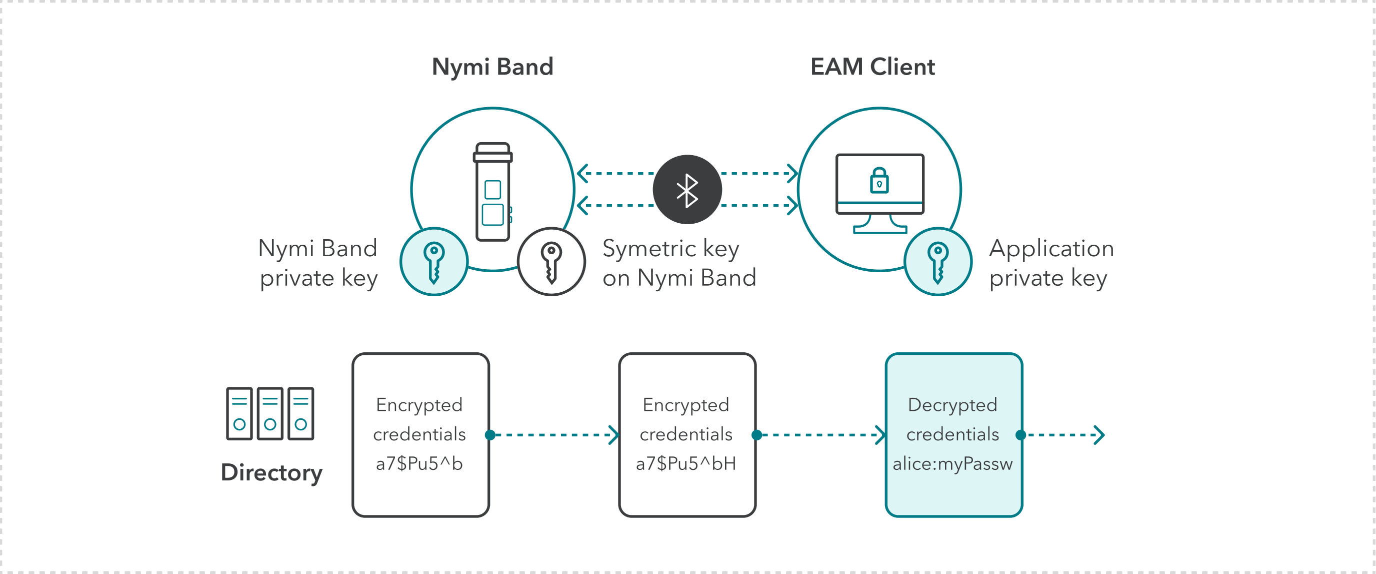
FIDO 2.0 private keys never leave the Nymi Band, as the authentication is performed using public key cryptography.

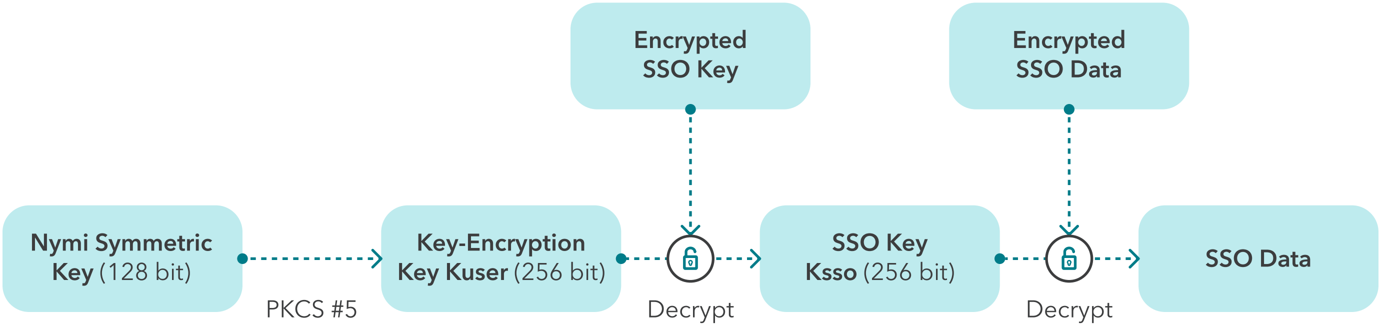
User identity is included only in the FIDO 2.0 `authenticatorMakeCredential` message when enrolling credentials against a new relying party. During subsequent authentication, user identity is not revealed in the `authenticatorGetAssertion` message.

4.3 Evidian Integration (Wearable)

The Evidian SSO solution manages windows logon, application logon and e-signature, often involving multiple user accounts and passwords, with a single means of authentication, for example using the Nymi Band as a strong, two-factor biometric authenticator.

4.3.1 Authentication


Nymi Band
EAM Client
Nymi Band private key
Symetric key on Nymi Band
Application private key
Directory
Encrypted credentials a7$Pu5^b
Encrypted credentials a7$Pu5^bH
Decrypted credentials alice:myPassw



SSO Data (username / password) is encrypted via a split-secret scheme.

- SSO Data encrypted by an AES-256 key Ksso stored in LDAP.
- Ksso encrypted by an AES-256 Key-Encryption Key (Kuser), generated using the Nymi Symmetric Key (128 bit) and PKCS#5 PBKDF2.

4.3.2 Protection of Sensitive Data

- All SSO Data (username and encrypted password) that is sent over the network is encrypted; sensitive data is never transmitted in clear text.
- All sensitive information (SSO Data and Keys) is stored encrypted.
- Key and Password are decrypted only at time of use, and remain in clear text in memory only for as long as needed, and deleted after completion of Windows / SSO login.
- Encrypted SSO Data and SSO Keys are protected via LDAP access control.
- Nymi Symmetric Key is transmitted over a secure BLE session by using the Nymi Security Protocol

  a. BLE secure session provides mutual authentication, encryption, and message integrity.
  b. Secure session is implemented in the application layer, and does not rely on Bluetooth security.
  c. Protocol closely resembles TLS 1.2 with equivalent security as the cipher suite TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256.

- Nymi Symmetric Key is only accessible by EAM Clients that possess valid certificates and private keys

  a. Certificates issued by NES under Nymi PKI
  b. Can only be retrieved after the user has authenticated to the band