Nymi Configuration Specifications

Nymi Enterprise Edition
3.3
2021-02-17

Contents

Introduction

Based upon the type of system (e.g., configurable or custom), configuration and design specifications provide a detailed, technical expansion of the Functional Specification (FS) (see Appendix D2).

The specifications outlined in this document explain how the system will do what is defined in the FS. This information provides the basis for subsequent configuration management.

This document is the Configuration Specifications (CS) for a solution in which user authentication for login and electronic signatures is based on biometrics instead of usernames and passwords.

Software Design

`Nymi Enterprise Edition` is a Category 4 product under GAMP and defined as a configured product. Software Design specifications are required for custom applications. This is not normally required for configurable products, where software design is normally reviewed or evaluated as part of supplier assessment.

Nymi's software is developed and validated based on internal processes, outlined in 10014 - Software Development Life Cycle and 10009-Verification and Validation.

Nymi Enterprise Edition with Evidian Access Management Solution

There are several supported deployment configurations in the Nymi-Evidian solution.

The Nymi Band supports three authentication methods in an Evidian environment:

- Wearable (NFC with Bluetooth)—During communications, tapping the Nymi Band on an NFC reader initiates the authentication, and then the Nymi Band is cryptographically authenticated over Bluetooth. This is the default authentication method.
- Smart Card (NFC-only)-—During communications, the Nymi Band is cryptographically authenticated over NFC.
- RFID-only—During communications, the Nymi Band is identified by using only the NFC UID without cryptographic authentication.

Nymi provides you with one or more *TokenManagerStructure.xml* files, based on your configuration needs. The *TokenManagerStructure.xml* file defines the supported authentication types and modules that implement the authentication modules. The contents of the TokenManagerStructure file are loaded on the EAM Controller and the default configuration is pushed by the EAM Controller to the EAM Clients. To override the default authentication method on a terminal, place a different version of the TokenManagerStructure file locally on the terminal.

The *TokenManagerStructure* file for the Nymi Band as a Wearable device differs from the *TokenManagerStructure* for the Nymi Band a smart card or as an RFID-only device.

There are several supported deployment configurations in the Nymi-Evidian solution.

- Nymi Band configured as a wearable device
- Nymi Band configured as an RFID-only device
- Nymi Band configured as a secure NFC device
- Nymi Band configured as a mixed use device

Note: This document is specific to an Evidian configuration that uses Active Directory Lightweight Directory Services to provide data storage and retrieval support for directory-enabled applications.

Environment Configuration

The section outlines the configuration requirements for the enrollment terminal and the user terminals. Refer to the Nymi Enterprise Edition Deployment Guide for details about NES requirements and the Nymi Enterprise Edition Administration Guide for information about supported NFC readers.

User Terminal Requirements

The user terminal is a Windows 7 or Windows 10 machine that operators use to perform MES authentication tasks. User terminals include local machines as well as machines that are connected to remotely through an RDP session or on a Citrix server.

The user terminal requirements differ depending on the type of user terminal:

User Terminal Type	Requirements
Local Wearable User Terminal	• `Nymi Bluetooth Endpoint` and the `Nymi Agent` software to support MES operations. • Evidian Enterprise Access Management (EAM) Client, with a valid Evidian license file • Nymi-supported NFC Reader • BLE Adapter (BLED112)
Remote Wearable User Terminal	• `Nymi Bluetooth Endpoint` software to support MES operations. • EAM Client on the Citrix server or remote session host, with a valid Evidian license file. • Centralized Nymi agent.
Local Smart Card User Terminal	• Nymi-provided OpenSC software • EAM Client, with a valid Evidian license file • Nymi-supported NFC Reader.
Local RFID-only User Terminal	• Evidian Enterprise Access Management (EAM) Client, with a valid Evidian license file • Nymi-supported NFC Reader.

Network Requirements

User Terminals require a connection to the enterprise domain and bidirectional communication through the following firewall ports:

- For an ADLDS configuration, The user terminal communicates with the ADLDS server on default port 55000.
- For a centralized `Nymi Agent`, the EAM client communicates with the `Nymi Agent` machine on default port 9120.
- For communications between the EAM Client and EAM Controller, communication occurs on port 3644.

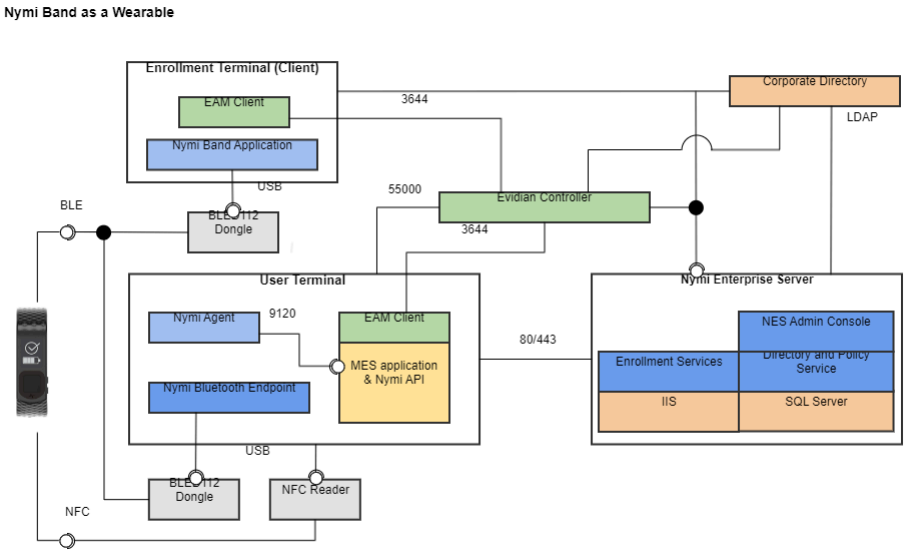
Enrollment Terminal Requirements

- Evidian License File
- Evidian Nymi Band Application
- EAM Client
- Domain Admin access or Directory Admin Access
- Connection to the enterprise domain
- BLE Adapter (BLED112)

- Bidirectional communication ports open on the firewall.
  - For an ADLDS configuration, The enrollment terminal communicates with the ADLDS server on default port 55000.
  - For a centralized `Nymi Agent`, the enrollment terminal communicates with the `Nymi Agent` machine on default port 9120.
  - For management of access points from the EAM Console, communications occurs on port 3644.
- For Nymi Band Smart Card environments also require the OpenSC software and a Nymi-supported NFC reader.

Nymi-Evidian Architecture - Wearable Device

The following image represents the components in a Nymi-Evidian solution where the Nymi Band is used as a wearable device.



Enrollment Terminal

The Windows 7 64-bit or Windows 10 machine where users enroll their Nymi Band.

User Terminal

The workstation on which you install Nymi components and the Evidian Access Manager (EAM) client.

Nymi Band Application

A native Windows application that is used to register biometric, employee ID, and Nymi Band with the enterprise. The Evidian version of the `Nymi Band Application` integrates directly to the Evidian ecosystem and facilitates communication between NES and the Nymi Bands. The Nymi Enterprise Edition Administration Guide provides more information about the `Nymi Band Application`.

Enterprise Access Management Client	The client-side Evidian software that provides users with a single sign-on (SSO) experience at the user terminal.
Nymi Enterprise Server	Management software for the Nymi Bands within the Nymi ecosystem. Nymi Enterprise Server (NES) ensures the validity of the hardware in the system. NES includes the `NES Administrator Console`, a web application that administrators can use to manage the Nymi Bands within the ecosystem. NES includes: • Enrollment Service - Authenticates, validates, and authorizes certificate requests from requesters, such as the `Nymi Band Application` and Nymi-enabled Application(NEAs. • Directory and Policy Service - Maintains the NES database, and provides the IIS web service that allows the `NES Administrator Console` to access the NES database. • Authentication Service - Provides authentication and authorization support for domain users and computers. The service currently uses an Active Directory (LDAP) interface.
Evidian Enterprise Access Management Controller	Evidian Enterprise Access Management (EAM Controller) allows centralization of User Access policy definition and audit events. Includes Evidian Enterprise SSO software that provides agile single sign-on (SSO). The EAM Console application provides the interface to perform management activities.
Corporate Directory	A server such as Windows domain controller that provides authentication services, such as Active Directory.
NFC Reader	Captures the NFC UID of the Nymi Band, which is used when an operator performs and SSO authentication event.
BLE112 Dongle	Nymi Band uses Bluetooth Low Energy (BLE) to interact with external components and services. Nymi Band BLE communication does not rely on Bluetooth security. All security is implemented using strong, standard-based cryptography. A BLE dongle (adapter) is required on the enrollment terminal and user terminals.

Configurations

A `Nymi Enterprise Edition` environment requires a minimum of two computer systems, a Windows server on which the NES software is installed and a Windows network terminal on which to install the Nymi Band Application.

The following table summarizes the configuration specifications and related user specifications for configuration requirements.

Table 1: Configuration specifications for configurations

URS #	FS #	Functional Specification	CS #	Configuration Specification
URS-001	FS-CFG-01	The server-side components can be installed on bare metal within the customer's environment (Supported Operating Systems: Windows Server 2012 R2, Windows Server 2016)	n/a	n/a
URS-029	FS-CFG-02	Create a document that describes the steps to deploy Nymi Agent so that it can achieve 99.9% availability	CS-CFG-02	This information is covered in the Nymi Enterprise Edition Deployment Guide.
URS-003	FS-CFG-03	Nymi Enterprise Edition shall be deployable in a way that allows a user's Nymi Band to be enrolled once and able to authenticate to systems in multiple domains.	CS-CFG-03	During NES deployment on the `Enterprise` window, there exists the option to specify multiple domains on which an which a user can use an authenticated Nymi Band.
URS-003	FS-CFG-04	NES shall require only one AD account for all domains for which there are trust relationships (requires two way trust between domains).	CS-CFG-04	The user account that is specified during NES deployment on the `Enterprise` window, in the **`Domain`** table must be a member of one of the domains in the trust.

URS #	FS #	Functional Specification	CS #	Configuration Specification
URS-002	FS-CFG-010	NES and the Nymi Agent are installable on a virtual machine that has connectivity with required components, such as a Domain Controller and AD server. The NES server and Nymi Agent must also have connectivity and access to the user terminals. The Nymi Agent can qualify as a server side component and you can deploy Nymi Agent on a VM.	CS-CFG-010	This functionality is qualified as part of the Product verification and validation testing performed by Nymi.
URS-011	FS-DAT-002	Backup and restore procedures for database protection follow corporate policies.	CS-DAT-002	Configure SQL backups in accordance to corporate policies
URS-027 URS-028	FS-SAF-005	Evidian maintains an audit log of Nymi Band user assignments	CS-SAF-005	Evidian stores audit information in Evidian's SQL sever database.
URS-030 URS-039	FS-APP-001	The `Nymi Band Application` is a graphical user interface that allows users to enroll a Nymi Band and authenticate their Nymi Band using corporate credentials.	DS-APP-001	After a user logs in to the Nymi Band Application with a valid AD username and password, the application provides users with step-by-step instructions to enroll their Nymi Band. After users have enrolled their Nymi Band, they can use the Nymi Band Application to authenticate the Nymi Band by their Active Directory username and password if active policy on NES is configured to support corporate credential authentication.

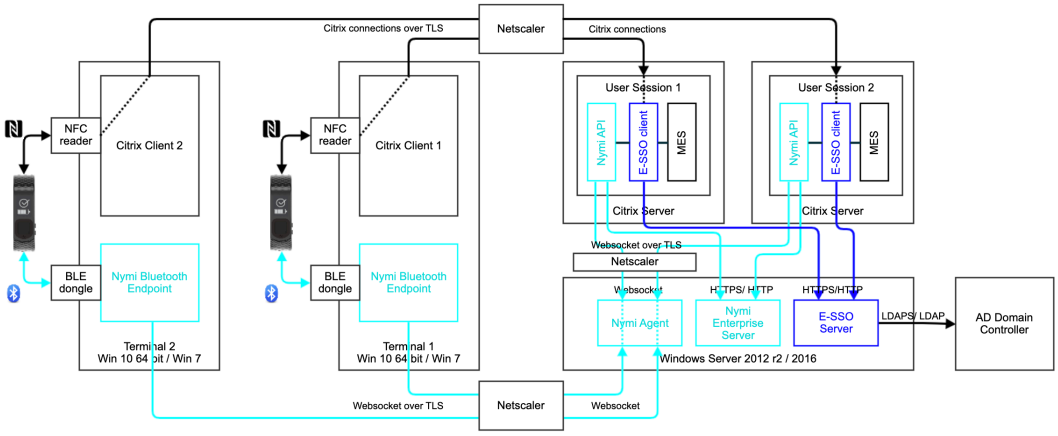
URS #	FS #	Functional Specification	CS #	Configuration Specification
URS-019 URS-024	FS-APP-002	The NES Administrator Console is a web-based application that allows administrators to manage NES policies and users. The EAM Console is provided to manage users and their Nymi Bands.	CS-APP-002	The `NES Administrator Console` is a secure web interface into NES that an NES Administrator accesses from any computer on the network, to manage policies, Nymi Band users and certificates. The EAM Console is a desktop application provided to manage users and Nymi Band assignment.
URS-013	FS-NB-016	`Nymi Enterprise Edition` solution ensures that the Nymi Band user is valid in Active Directory. Usernames and passwords are not stored by NES.	CS-NB-016	NES can be configured to check a user's AD user status with every action that they perform with the Nymi Band. If the user is inactive in AD, the user cannot log into the terminal, MES application or perform an e-signature with their Nymi Band. As error is reported and logged.
URS-014 URS-023	FS-MES-001	The Active Directory user status is queried for every user authentication provided by a Nymi Band to Windows and MES login.	CS-MES-001	The Evidian ESSO server checks Active Directory every time user authentication is provided, and requests the ciphered user password from Active Directory.
URS-004 URS-015	FS-MES-006	Integrate the Nymi API into an MES to support the use of a Nymi Band for login.	CS-MES-006	MES applications make use of the intent notification and assert_identity request to implement this functionality.
URS-016 URS-018	FS-MES-008	The System shall provide automatic user logoff from a Windows session if s/he walks away from a logged in Windows session or the Nymi Band deauthenticates.	CS-MES-008	Log off occurs when the authenticated Nymi Band is no longer within BLE range of the Windows system. This includes when the Nymi Band becomes deauthenticated.

Remote application support via Citrix and RDP

Allows users to access multi-user applications running on a remote RDP-based and Citrix-based environment solution and have multiple user sessions running on it by using an authenticated Nymi Band .

Nymi Enterprise Edition Deployment in Citrix Environment

The following figure provides an overview of the `Nymi Enterprise Edition` components that are installed in a Citrix environment.



`Figure 1: Nymi Enterprise Edition components in a Citrix environment`

This figure shows the following configuration:

- The `Nymi Bluetooth Endpoint` is installed on each Citrix client. The `Nymi Bluetooth Endpoint` service on each Citrix client communicates with the `Nymi Agent` service, which is installed on a separate host, on websocket port 9120.
- The `Nymi Agent` is installed in an central location that is accessible to all user terminals, for example on the NES server.
- An *nbe.toml* file is installed on the Citrix client, and is configured with the location of the `Nymi Agent`.
- An NEA runs on the Citrix server and includes the *nymi_api* for communicating with Nymi Bands.

Nymi Enterprise Edition Deployment in RDP Environment

`Nymi Enterprise Edition` support deployments in RDP Environments.

The following figure provides an overview of the `Nymi Enterprise Edition` components that are installed in an RDP environment.

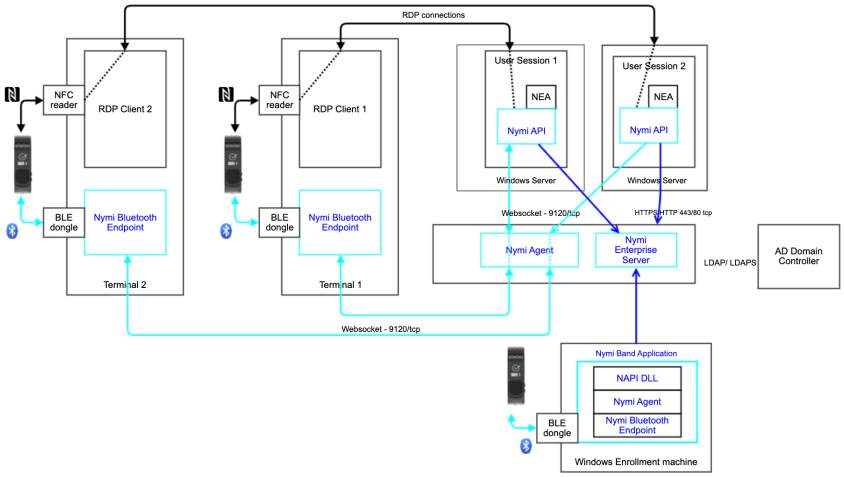


Figure 2: Nymi Enterprise Edition components in a RDP environment

This figure shows the following configuration:

- The `Nymi Bluetooth Endpoint` is installed on each RDP client. The `Nymi Bluetooth Endpoint` service on each RDP client communicates with the `Nymi Agent` service, which is installed on a separate host, on websocket port 9120.
- The `Nymi Agent` is installed in an central location that is accessible to all user terminals, for example on the NES server.
- An *nbe.toml* file is installed on the RDP client, and is configured with the location of the `Nymi Agent`.
- An NEA runs on the RDP server and includes the *nymi_api* for communicating with Nymi Bands.

Citrix and RDP specifications

The following table summarizes the configuration specifications and related user specifications for remote application support requirements.

Table 2: Configuration specifications for remote application support

URS #	FS #	Functional Specification	CS #	Design / Configuration Specification
URS-020 URS-021 URS-022	FS-RDP-005	Administrators can install NEAs on Windows 10 thin clients running Citrix (compatibility requirement).	CS-RDP-005	NEAs installed on the thin client require the *nymi_api.dll* file. The *nymi_api.dll* must be compatible with Windows 7 32-bit and 64-bit, and Windows 10 64-bit.

Hardware Design

Nymi Band 3.0

The Nymi Band wearable is a biometric device used by companies to increase security and improve workflows.

Nymi Band Physical Features

The following figures show the front and back of the Nymi Band.

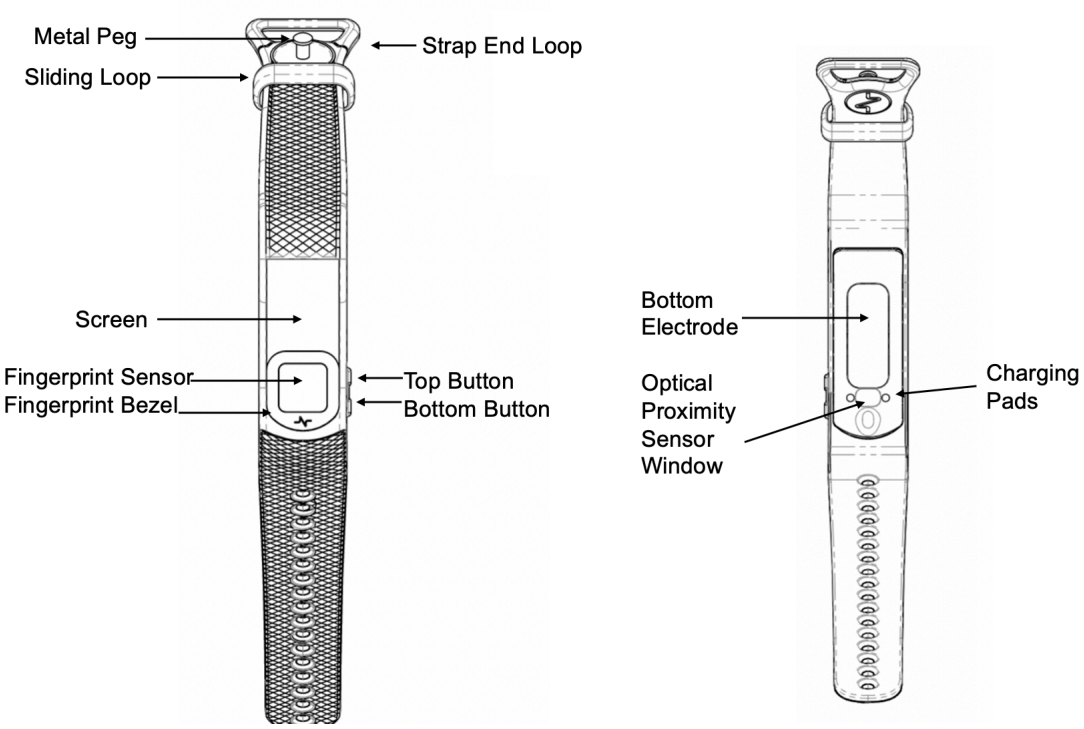


Figure 3: Nymi Band front and back

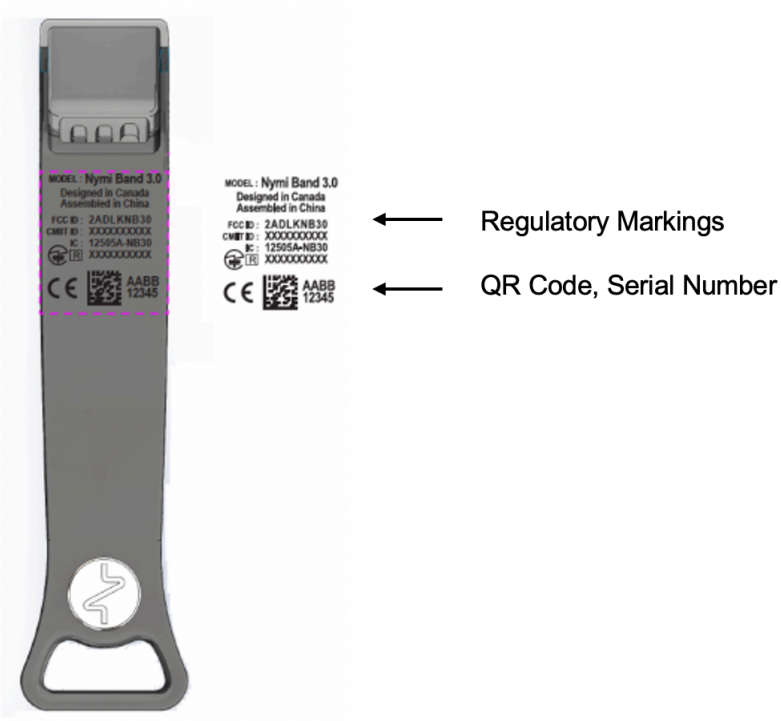


Figure 4: Nymi Band Strap

The Nymi Band is made up of the following main components:

- Screen—Visual interface on the face of the Nymi Band.
- Fingerprint sensor—Fingerprint detection pad on the face of the Nymi Band.
- Fingerprint bezel— Electrode that is used to capture the electrocardiogram (ECG) signal during authentication.
- Top and Bottom buttons—Turns on the Nymi Band and allows users to navigate through screens. The buttons are also used to access administrative functions while the Nymi Band is charging.
- Charging pads—Makes contact with the pins of the charger.
- Optical Proximity Sensor Window—Sensor that detects if the Nymi Band is on the wrist of the user.
- Bottom electrode—Electrode that is used to capture the ECG signal during authentication. Also used to capacitively sense that the Nymi Band is on the user's wrist.
- Metal Peg - Peg that is used to secure the Nymi Band strap while it is on the wrist of the user.
- Sliding Loop - Loop used to keep any excess Nymi Band strap in place while it is on the wrist of the user.
- Strap End Loop - The loop integrated into the strap that helps the user get a good fit on their wrist. The wearer uses the strap loop in the same way that they would use a watch buckle.

The Nymi Band strap contains regulatory markings, a QR code, and the Nymi Band serial number. When scanned, the QR code displays the serial number.

Note: The Nymi Band is shipped with a protective film on the optical sensor and bottom electrode. Remove the protective film before use.

Nymi Band Functionality

Configuration specifications outlining setting, parameters, tools or methods that are used to set required options, any dependencies or impacts on other systems, infrastructure items such as operating systems and layered software, and any security settings.

Table 3: Configuration specifications for the computer system

URS #	FS #	Functional Specification	CS #	Configuration Specification
URS-010 URS-012	FS-NB-012	The biometric information that is stored on the Nymi Band consists of a fingerprint template, which is securely stored locally on the micro-controller unit (MCU). The biometric information is permanently deleted when the Nymi Band is security wiped. No biometric information is stored in the server and the fingerprint template never leaves the Nymi Band.	CS-NB-012	The Nymi Band uses an FPC 1321 fingerprint sensor FPC 2050 drive IC. The FPC 1321 is a capacitive fingerprint sensor that uses arrays of tiny capacitor circuits to capture the fingerprint. It has a scratch-resistant coating and is made by Fingerprints Cards AB (1). Physical communication lines (USB, serial) are disabled on the MCU. If the MCU were physically removed from the Nymi Band, physical communication lines remain disabled ensuring no access to MCU memory by design.
URS-009	FS-BAT-005	Nymi Band contains a rechargeable battery and Nymi performs standard benchmark battery life tests that can be used to provide estimations to customers and compare battery life between different firmware releases.	CS-NB-013	The Nymi Band features a rechargeable 48 mAh lithium polymer battery that is charged by using a Nymi-provided charging cradle. The battery life is continually monitored and benchmarked in every subsequent release to meet the requirement.
URS-007	FS-BAT-001	The Nymi Band supports a 3-day battery life, assuming 10-hour shifts, 900 taps total (300 per shift) with one shift per day.	CS-BAT-001	The Nymi Band supports a 3-day battery life, assuming 10-hour shifts, 900 taps total (300 per shift) with one shift per day.
URS-026	FS-PHY-007	The Nymi Band has a display which provides information to the user.	CS-PHY-007	Display information such as battery life, band label, and authentication status (authenticated/ deauthenticated).

Inputs and Outputs

Input and output format may include digital and/or analog signals. External equipment should consider accuracy, isolation, range of current and voltage, type and numbers of interface cards and timing.

Table 4: Configuration specifications for inputs and outputs

URS #	FS #	Functional Specification	CS #	Configuration Specification
URS-030	FS-NB-015	`Nymi Enterprise Edition` allows authentication to the Nymi Band by biometrics or an external authenticator, such as Active Directory.	CS-NB-015	NES Administrator can configure the default policy to allow an External Authenticator for authentication.

Environment

The operating environments for hardware shall be defined to include use, temperature, humidity, external interface, physical security, shielding against radio frequency, electro-magnetic or US interfaces, hardening against physical hazards such as dust or vibration.

Table 5: Configuration specifications for the environment

URS #	FS #	Functional Specification	CS #	Configuration Specification
URS-005	FS-ENV-001	The Nymi Band maintains biocompatibility and chemical resistance.	CS-SAF-001	n/a

URS-005	FS-ENV-002	• The Nymi Band is certified by:
		  • FCC (United States)
		  • CE (Europe)
		  • IC (Canada)
		• The Nymi Band is made of hypoallergenic material.
			CS-SAF-002	n/a

URS #	FS #	Functional Specification	CS #	Configuration Specification
URS-008	FS-ENV-003	The Nymi Band can be sanitized with an alcohol wipe or spray.	CS-SAF-003	The external surface of the Nymi Band shall be cleanable daily by soap and brush cleaning, 70% isopropanol wipe or 70% isopropanol submersion without any negative impact on reliability or functionality over a 3-year span. The external surface of the Nymi Band shall be durable to daily cleaning by soap and brush, 70% isopropanol wipe or 70% isopropanol submersion without any objectionable degradation in surface finish over a 3-year span.
URS-006 URS-017	FS-NB-019	The Nymi Band NFC antennae supports a read-range that allows detection by an NFC reader through protective clothing and plexiglass coverings.	CS-NB-01	This functionality is qualified as part of the QA and user acceptance testing process for the `Nymi Enterprise Edition` solution.
URS-025	FS-BAT-006	Users can accurately tell whether their Nymi Band's battery is Low, Medium, or High from the battery indicator on the screen.	CS-BAT-006	The Nymi Band hardware utilizes a fuel gauge chip which tracks the state of charge of the battery to a roughly 1% accuracy. This state of charge is read in firmware and mapped out to a battery charge indicator on the band’s screen, which shows 4 levels of charge (3 bars, plus empty battery).

Glossary

Definitions/acronyms used throughout this document are defined below.

Table 6: Glossary

Acronym	Definition
AD	Active Directory. Directory service for domain networks.
ADLDS	Active Directory Lightweight Directory Services. Directory service for domain networks.
IAM	Identity Access Management
SSO	Single Sign-On
MES	Manufacturing Execution System
NEE	Nymi Enterprise Edition
EAM	Enterprise Access Management
ESSO	Enterprise Single Sign on
RFID	Radio-frequency identification
Solution	All components that enable biometric authentication, including Nymi Enterprise Edition components , Evidian components and the MES.
Class A	Class A clean rooms are for high-risk operations (eg. filling zone, stopper bowls, open ampoules and vials and, making aseptic connections). Class A environments are sterile environments
Class B	Class B Clean rooms provide the background environment for grade A zone items needing aseptic preparation and filling.
Class D	Environments for less critical tasks in the manufacturing process.
21 CFR Part 11	Part of Title 21 of the Code of Federal Regulations that establishes the United States Food and Drug Administration regulations on electronic records and electronic signatures.

Published in Canada.
Nymi Inc.
Toronto, Ontario
www.nymi.com