



Nymi Band 3.0 Physical Access Using CSN - Guide

March 20, 2023

Version 1.0

Table of Contents

Revision History	2
Acronyms	2
Physical Access with the Nymi Band	4
Background	4
Nymi Band PACs Technology	4
CSN Integration Guide	5
CSN Format	5
Determining the CSN	5
Compatible Readers	7
Output Format	8
Conclusion	11

Revision History

Date	Version	Revision History
March 20, 2023	1.0	Initial Release.

Acronyms

Acronym	Meaning
CSN	Card serial number, same as UID
NES	Nymi Enterprise Server

NFC	Near-field communication
UID	Unique identifier
PACs	Physical access control system

Physical Access with the Nymi Band

Background

The Nymi Band™ 3.0 is a wrist-worn biometrically authenticated device used for logical and physical access applications. A typical deployment for a physical access control system (PACs) is shown in Figure 1. Here the Nymi Band operates as a credential provider in the same way a traditional smartcard, key fob, or corporate badge would be used in an enterprise physical access deployment. By using on-board biometrics, the Nymi Band provides higher identity assurance over a traditional credential, such as a key fob, and offers the convenience of door access at the tap of the wrist.

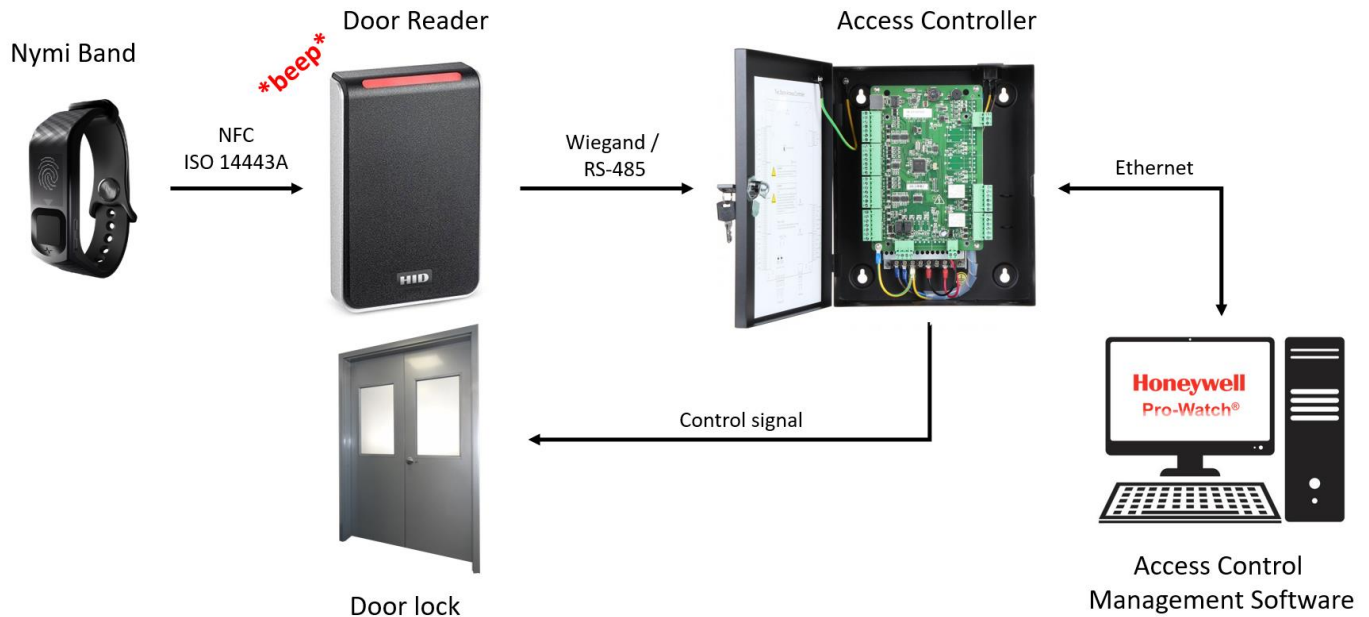


Figure 1 – Physical access system typical deployment.

Nymi Band PACs Technology

The Nymi Band provides multiple options for integrating with physical access systems, that all operate over the contactless ISO14443-A Near-Field Communication (NFC) interface at 13.56 MHz. The technology supported by the band are as follows:



1. [HID Seos](#) – The Nymi Band behaves like a HID Seos card, supporting all Seos-compatible formats including Open, Standard, CORP1000, and Elite keys. ***Note if the deployment uses HID readers, but not HID Seos technology specifically (for example prox, or iClass), the Nymi Band can still potentially be integrated with the system as most current HID readers support Seos technology out of the box. Please contact Nymi for additional details.**
2. [Legic Advant](#) – The Legic Advant card-in-card technology is hosted in the Nymi Band for integrating with Legic-compatible systems.
3. Static Card Serial Number (CSN / UID) – An ISO14443-level static identifier that is not configurable, secured, or encrypted.

This document will discuss the details of the third approach, the CSN, and how a customer can deploy a physical access solution using this credential. For details on the HID Seos or Legic technology in the Nymi Band, please contact the Nymi sales team or visit the support site for additional documentation (<https://support.nymi.com/hc/en-us>).

CSN Integration Guide

CSN Format

Each Nymi Band is configured with a static **7-byte Card Serial Number** (or UID) exposed at the NFC layer (ISO14443) during manufacturing. This **7-byte value never changes** during the lifetime of the product and can be used as a biometrically secured identifier for physical access applications.

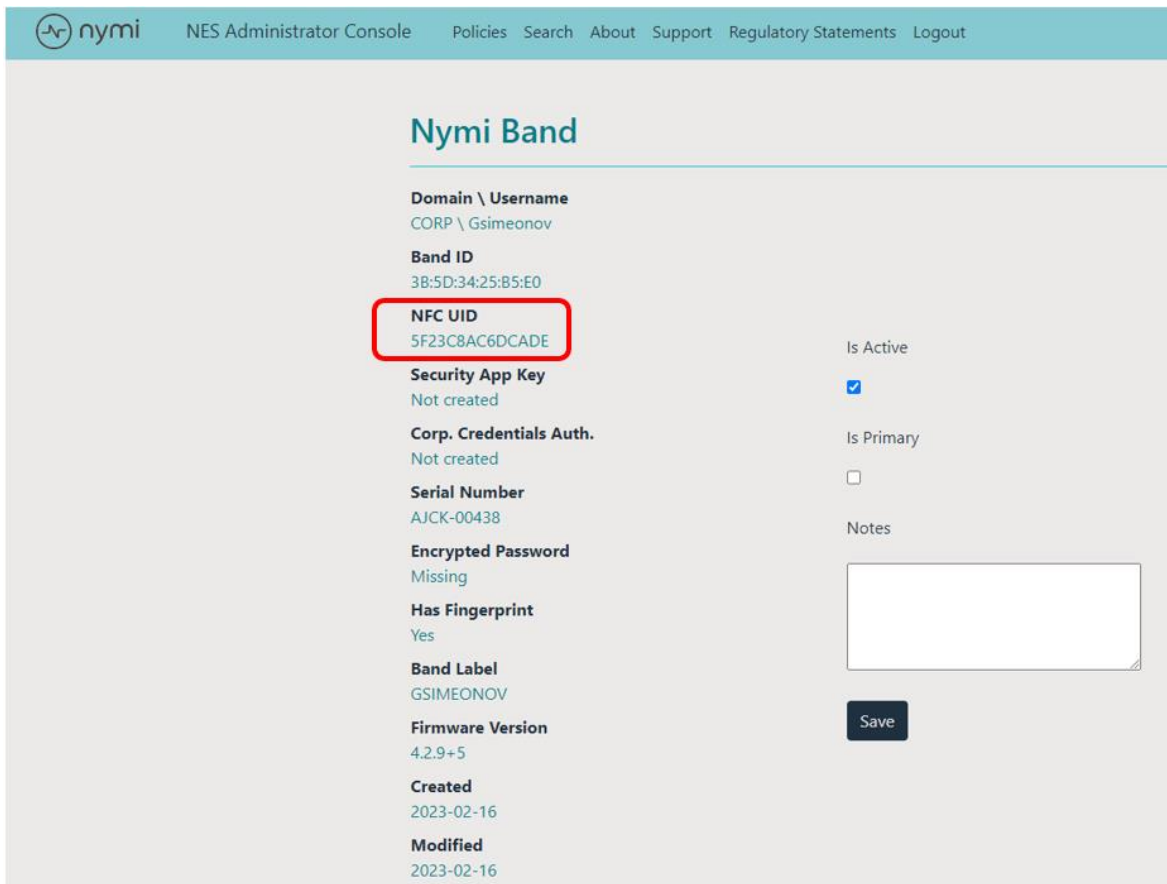
Note:

- The CSN **is not** encrypted when read, so it can in theory be cloned and replayed by using another smart card or NFC transceiver. However, Nymi Bands are typically leveraged for door access within buildings that are additionally secured with perimeter locks to protect from public access. Nymi Bands are traditionally deployed within these secured environments and thus offer valuable security and convenience to employees.
- The CSN **is not** compatible with MIFARE/DESFire CSN/UID schemes, which incorporate an unencrypted ID at the MIFARE protocol level. MIFARE/DESFire protocols are not currently supported by the Nymi Band.

Determining the CSN

The 7-byte CSN of each Nymi Band can be accessed in several ways.

1. **Purchase order serial number list** – When a purchase order is made for Nymi Bands, Nymi provides a list of band serial numbers along with some parameters of interest. These parameters include the factory-set CSN (NFC UUIDs) of each individual band. This list can then be used to connect the user assigned to the Nymi Band to their access permissions within the PACs system.
2. **NES Administrator Console** – When a Nymi Band is assigned to a user and enrolled within a deployment using our standard Nymi Enterprise Server (NES) and Nymi Band Application (NBA), the CSN of the specific band (and user) can be accessed using the administration console, as shown in **Figure 2**.
3. **Mobile App** – If a user has enrolled and authenticated their Nymi Band, the NFC radio will be active. Using a mobile phone NFC utility, such as [NFC Reader](#) on the Google Play Store, the NFC ID (CSN) can be read by tapping the band on the mobile phone NFC reader located on the back of the phone. **Figure 3** shows an example of a NFC UID scanned by a mobile phone app, showing the same value as the corresponding band in the NES Administrator Console from Figure 2. ***Note that Nymi has only verified that this approach works on Android devices, and not iOS.**



The screenshot shows the 'Nymi Band' configuration page in the NES Administrator Console. The page displays various fields for a specific band, including Domain \ Username, Band ID, NFC UID, Security App Key, Corp. Credentials Auth., Serial Number, Encrypted Password, Has Fingerprint, Band Label, Firmware Version, Created, and Modified. The NFC UID field is highlighted with a red box, showing the value 5F23C8AC6DCADE. The page also includes checkboxes for 'Is Active' and 'Is Primary', a 'Notes' field, and a 'Save' button.

Domain \ Username	CORP \ Gsimeonov
Band ID	3B:5D:34:25:B5:E0
NFC UID	5F23C8AC6DCADE
Security App Key	Not created
Corp. Credentials Auth.	Not created
Serial Number	AJCK-00438
Encrypted Password	Missing
Has Fingerprint	Yes
Band Label	GSIMEONOV
Firmware Version	4.2.9+5
Created	2023-02-16
Modified	2023-02-16

Figure 2 – Determine CSN using the NES Administrator Console.



Figure 3 – Scanning the CSN using a mobile phone app (NFC Reader app).

Compatible Readers

The access control reader must be selected or verified to support reading the CSN value of the Nymi Band. This compatibility will vary between reader manufacturers and models. In general, the reader datasheet should indicate the following:

1. Supports ISO14443A cards.
2. Supports ISO14443 CSN, or generic CSN formats.
3. Supports 13.56 MHz frequency range.

Supporting ISO14443 implies that the reader will support the 13.56 MHz NFC standard. Note that readers may be individually configured in field or by the manufacturer, depending on the customer's deployment requirements. If that is the case, certain features, including support for reading CSN may be disabled. The best way to verify this is to contact the reader manufacturer, the system integrator for the physical access system at the site, or by doing on-site testing as described in the following section.

SPECIFICATIONS

HID Signo Reader Model	20	20K	40	40K
2.4 GHz (Bluetooth) Credential Compatibility	Mobile Credentials powered by Seos* (HID Mobile Access)			
13.56 MHz (NFC) Credential Compatibility	Seos, iCLASS SE*, iCLASS SR*, iCLASS*, MIFARE Classic, MIFARE DESFire EV1/EV2, FeliCa™ & Contactless e-Purse Application Specification (CEPAS), Mobile Credentials powered by Seos (HID Mobile Access)			
125 kHz Credential Compatibility	HID Proximity*, Indala* Proximity, AWID Proximity, and EM Proximity			
Typical Read Range¹	Seos*, MIFARE Classic, MIFARE DESFire EV1/EV2 & ISO14443A Single Technology Cards - 1.6 to 4 in (4 to 10 cm) HID / AWID Proximity*, Indala Proximity*, EM Proximity & 125 kHz Single Technology Cards - 2.4 to 4 in (6 to 10 cm) <small>Suited to mount and cover single card</small>			

Figure 4 – An [HID Signo 40](#) reader datasheet, indicating support for ISO14443A cards.

Output Format

When the CSN is read by a compatible reader, some work must be done to determine what output format is read by the access controller. This will vary for every customer installation, depending on the following parameters:

- How the reader encodes the CSN and converts it to a value over the Wiegand / RS-485 interface. The CSN is 7 bytes (56-bits), however readers may trim that value into a smaller data size (for example 32-bits, or 26-bits) or pad it into a larger data size and transfer over the Wiegand interface. This must be determined through experimentation.
- The reader may also change the byte order, where the CSN value could be read in reverse.
- The access controller is typically configured to expect a certain format, for example a standard 26-bit Wiegand format (H10301). Depending on the access controller configuration, it might also trim or pad the CSN bit stream, which must be verified through testing.

In general, it is **recommended that the customer** has the capability to test a Nymi Band with their reader and physical access control system to determine the **output format** from the Nymi Band → Reader → Access Controller → Access Control Management Software (see Figure 1).

An example of this process is provided here.

A Nymi Band with the 7-byte CSN **0x5F7F5040219ED4** is enrolled with a user.

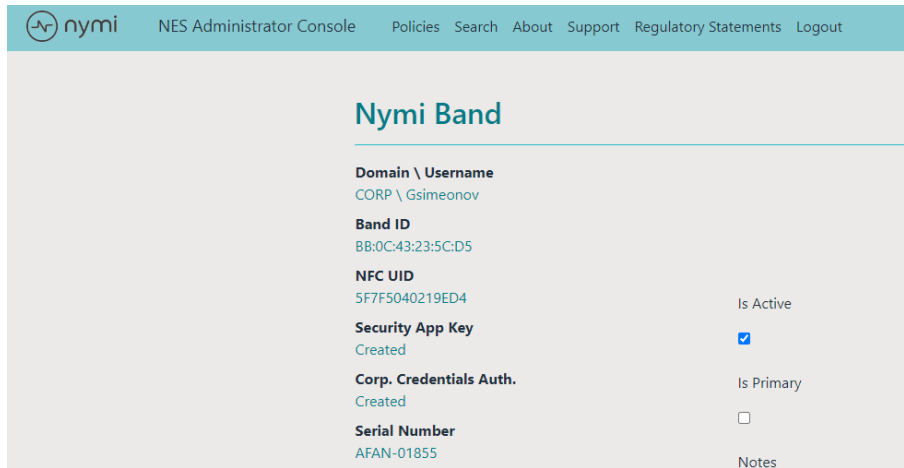


Figure 5 – Example user with CSN 0x5F7F5040219ED4.

The user is then instructed to tap their band on the door reader. In this case, an HID Signo 40 reader has been used in the demo PACs system.



Figure 6 – User tapping band on Signo 40 reader.

The access control management software is put into an enrollment, or event logging mode, where the value of the output of the Signo 40 reader is displayed in the software when the user taps the reader.

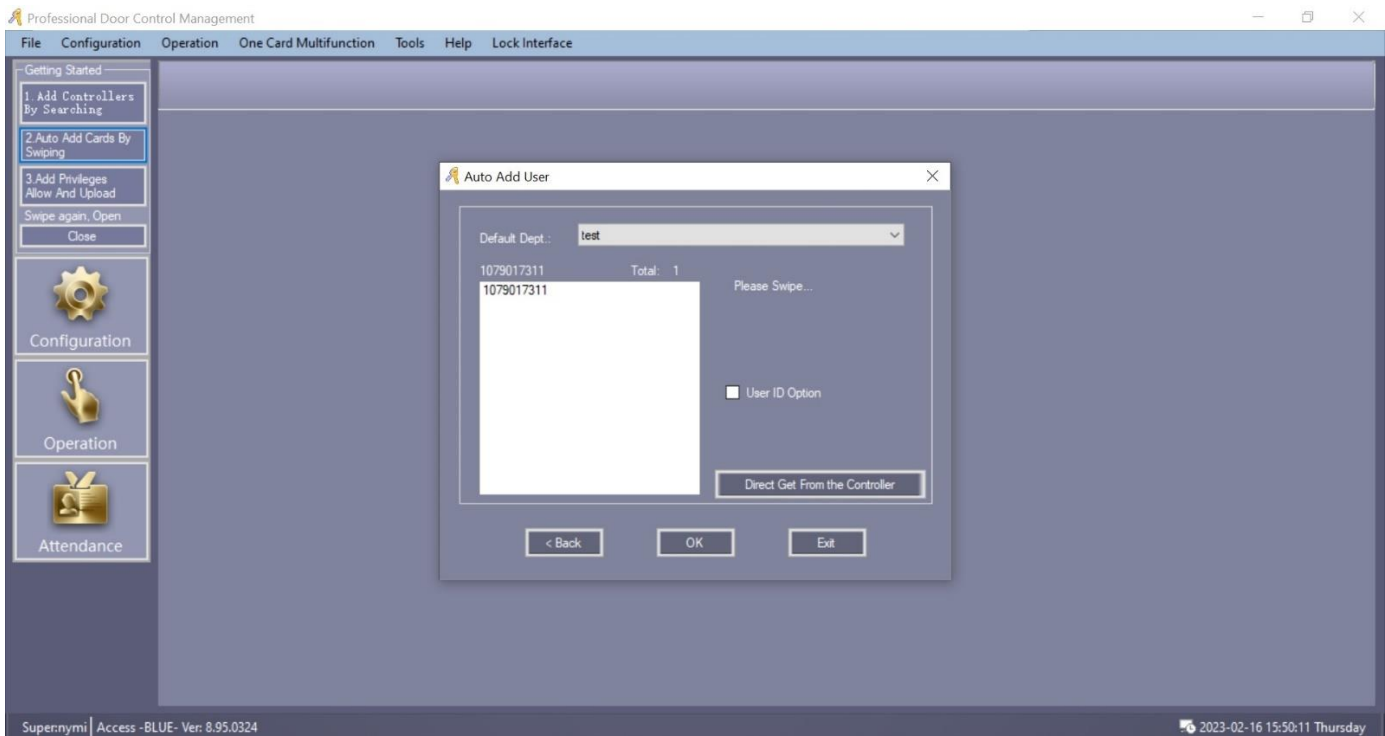


Figure 7 – Access control management software reading the CSN.

In this example, the access control software read the decimal value **1079017311**. Converting this value to hexadecimal results in **0x40507F5F**. In this case, it is determined that the reader is trimming the CSN down to a 4-byte (32-bit) value. Comparing this value to the original 7-byte CSN, it is evident that the reader is reversing the order of the CSN and transmitting the bottom 4 bytes. This is summarized in the table below.

CSN value (hex)	CSN value reversed (hex)	CSN reversed – last 4 bytes	Reversed last 4 bytes converted to decimal
0x5F7F5040219ED4	0xD49E21 40507F5F	0x40507F5F	1079017311

Table 1 – Output format of CSN read by access control system

Now that the output format of the entire communication chain has been determined, it can be used as a template for mapping CSN values from every band to an expected value read by the access control system. This process can be used to assign each user’s Nymi Band to a specific access control credential.

Conclusion

The Card Serial Number (NFC UID) is a 7-byte static credential provided by the Nymi Band that can be read over any standard ISO14443 compatible door reader. The CSN never changes during the lifecycle of the band and is set during the manufacturing process of the device. This document has discussed how the CSN of a Nymi Band can be determined, how to determine the compatibility of a door reader, and how to determine the output format of the CSN value as interpreted by the physical access controller and management software. Nymi provides services and support to help their customers with this process and trusts that this document can serve as a guide for using the Nymi Band CSN for physical access applications.



Copyright ©2023
Nymi Inc. All rights reserved.

Nymi Inc. (Nymi) believes the information in this document is accurate as of its publication date. The information is subject to change without notice.

The information in this document is provided as-is and Nymi makes no representations or warranties of any kind. This document does not provide you with any legal rights to any intellectual property in any Nymi product. You may copy and use this document for your referential purposes.

This software or hardware is developed for general use in a variety of industries and Nymi assumes no liability as a result of their use or application. Nymi, Nymi Band, and other trademarks are the property of Nymi Inc. Other trademarks may be the property of their respective owners.

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