nymi™ | SOLUTION BRIEF

Connected Workers in the Passwordless Smart Factory

A wearable smart authentication solution that delivers all-access convergence and e-signatures in GxP-validated environments

The pharmaceutical and biopharmaceutical sectors encounter distinct obstacles when it comes to integrating digital transformation strategies into their manufacturing operations. Rigorous regulatory standards designed to safeguard vital medications also challenge innovation. Nevertheless, fostering new technologies and improving processes are crucial for advancing patient care. To optimize pharmaceutical production, digital transformation initiatives often focus on enhancing operational efficiency, ensuring data integrity, and promoting worker satisfaction. A shared pain point that impacts each of these areas is authentication.

The Password Pain Point in Manufacturing

In drug manufacturing, quality and compliance regulations necessitate extensive documentation. While digitalization efforts like ERP, MES, EBR, LIMS, and other industrial platforms have automated many shop floor processes, operators still shoulder the burden of repetitive authentications within these systems.

For example, electronic signatures (e-signatures) that require username and password entries can exceed 100 instances in an operator's shift. Furthermore, the pervasive password problem at large has prompted stricter IT policies that require frequent password changes and increased character complexity. As a result, operators are uniquely at risk for password fatigue, productivity slowdowns, and security vulnerabilities. In addition, the immediate challenges from password authentication can have greater downstream consequences.

How Password Authentication Challenges Affect the Enterprise

- Password fatigue and workarounds
  → *Quality and compliance issue*

- Productivity slowdowns
  → *Increases time and cost*

- Cybersecurity attacks
  → *Threaten IT and OT networks*

The Adoption of Biometric Authentication

Biometric authentication has emerged as a promising solution that tackles the unique password pain point in the pharmaceutical industry. Successful biometric authentication in this context requires GxP-validation, strong security measures, and user-friendly functionality that specifically serves the needs of active workers. These criteria aim to enhance efficiency in authentication processes, ensure data integrity, and ease the overall operator experience by removing manual password entries.

While various solutions exist today, such as biometric mouses, iris scanners, and facial recognition readers, beware of critical limitations that can hinder effectiveness in manufacturing environments.

Critical Considerations for Deskless Workers Using Biometric Authentication Solutions

Is it designed for use on communal devices?

Traditional biometric authentication methods are best designed for single-user devices like personal computers. Here the user needs to enroll their biometrics once and they can be securely stored on the device. In manufacturing settings with shared devices, users must either enroll their biometrics on multiple devices, which is cumbersome and makes data deletion challenging, or biometric data can be stored centrally. While the latter is common, centralized storage of biometric data compromises data security and user privacy.

How does centralized PII storage affect the enterprise and its end-users?

Centralized storage of personally identifiable information (PII), as related to communal device designs, exposes it to cybersecurity threats and removes user ownership. The biometric data becomes the property of the enterprise and becomes vulnerable to cybersecurity attacks, which occur at an increasing rate. In critical environments, offline functionality becomes another crucial consideration. Centralized approaches can work with data replication, but this further spreads sensitive data, akin to the importance of not duplicating private keys in public key systems.

Can it work with PPE?

The use of Personal Protective Equipment (PPE) is standard practice in many manufacturing areas and strictly required in sterile environments. Cleanroom compatibility adds a layer of complexity in evaluating a biometric authentication solution. While different solutions can be deployed in different areas, this increases the IT sprawl for managing and scaling technologies in the long-run.

Smart Authentication: A Future of Connected Workers

Nymi revolutionized authentication in the pharmaceutical industry with an innovative operator-centric approach. Unlike traditional methods focused on system authentication, the Nymi connected worker solution enables continuous authentication at the person-level, facilitating uninterrupted workflows across applications, systems, and networks.

By leveraging industry-leading security protocols, Privacy by Design principles, and emphasizing the user experience, the Nymi connected worker solution digitally empowers operators to authenticate a single time to their wearable device, the Nymi Band^{TM}, and seamlessly continue their work in passwordless, contactless, and handsfree workflows.

The "connected worker" is a transformative authentication solution that combines biometrics, presence, and persistent identity to deliver across intersecting priorities desired in regulated manufacturing industries: time savings, enhanced productivity, better data integrity, and strong security that is easy to use – even in GxP-validated environments.

The Nymi Connected Worker Solution

Wearable Device + Platform

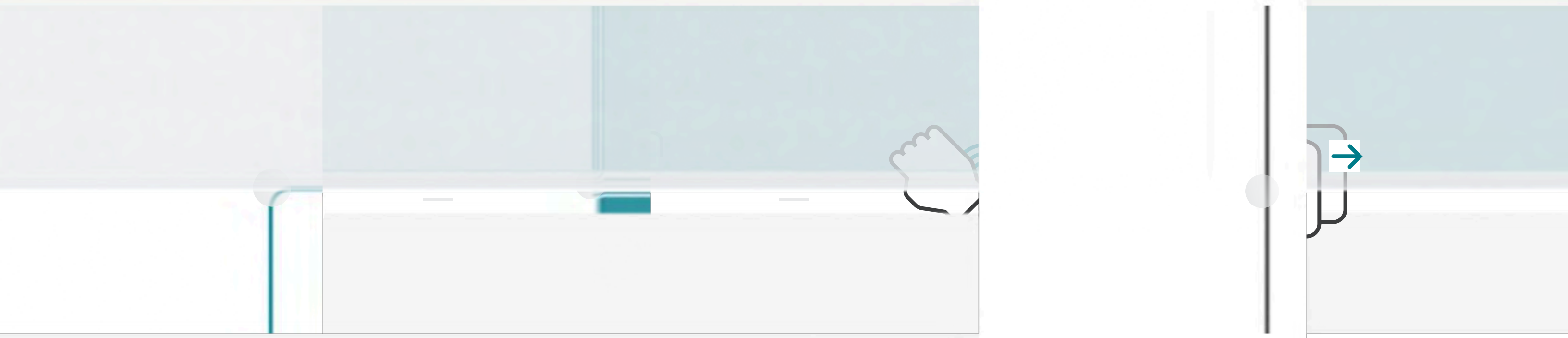
Nymi connects people to multiple applications, systems, and networks in a single authentication to their Nymi Band™. A Nymi connected worker is digitally empowered with passwordless, contactless, and handsfree authentication-based workflows, such as for app sign-in, e-signatures, physical access, and more.

Nymi Band™

The Nymi Band is a workplace wearable that is enrolled by an individual and afterwards biometrically authenticated via fingerprint for continuous use.

The Nymi Band applies a Zero Trust framework to identity by combining biometric authentication, continuous Always-On Authentication™, and Multi-Factor Authentication (MFA) in an easy-to-use wearable device.

In addition to strong identity assurance, the band is equipped with presence, activity, and other physiological systems, making it a next-generation smart authentication device that utilizes a powerful combination of functions beyond identity alone.



De-
ntication

Nymi Connected Worker Platform

The Nymi Connected Worker Platform is deployed on-premise and connects to the enterprise Active Directory. It manages the biometric security and privacy of Nymi Band users and connects people to a growing ecosystem of applications and devices through technology integrations and standards.

Core Use Cases in the Pharmaceutical and Biopharmaceutical Industry

All-Access Convergence
Logical systems

- Passwordless Login
- Nymi Lock Control™

Physical access systems
IT/OT networks

Electronic Signatures

Additional Use Cases (Bespoke Examples from Customers)

- Occupancy management
- Geofencing
- Visitor and contract management
- Access management with LMS
- Social distancing and contact tracing

Nymi-Ready Integrations

SOFTWARE

MANUFACTURING/QC LABS

ERP

- SAP (via bioLock or Evidian)

MES/EBR

- POMSnet Aquila
- Körber PAS-X
- Emerson DeltaV MES (Formerly Syncade)
- Rockwell FactoryTalk®PharmaSuite®
- Siemens OpCenter EXPH
- Siemens OpCenter EX MDD
- Tulip
- EIS OpsTrakker
- Lonza MODA-ES

HMI/SCADA

- Siemens WinCC
- Siemens PM Logon
- GE iFix
- Rockwell PanelView
- Rockwell FactoryTalk® View SE

DCS

- Emerson DeltaV
- Siemens SIMATIC PCS 7

VLMS

- Kneat
- ValGenesis
- handshake Smart Document System

Historians

- Aspentech
- ABB 800xA

Remote Desktop Services

- Rockwell Automation ThinManager
- Citrix

Document Management System

- CIMCON Software eInfoTree Excel

Corporate IT

- Windows 10
- iGEL
- Transparent ScreenLock RFID

HARDWARE

CLEANROOM GRADE MONITORS, TABLETS, AND TERMINALS

systec & solutions

CAITRON® INDUSTRIAL SOLUTIONS

tangent

KINETIC-iD Innovate | Design | Deliver

Getac

BLUE LINE IT for Demanding Environments

GENERAL ENDPOINT DEVICES

Microsoft Surface

iPad

IGEL

NFC READERS

HID

rf IDEAS

ELATEC RFID Systems

Nymi-Ready Integrations

SOFTWARE

R&D LABS

LIMS

- LabWare
- LabVantage

ELN

- PerkinElmer

SSO

- Evidian Authentication Manager
- Microsoft Azure AD
- Okta
- Ping Identity
- Duo
- ForgeRock
- OneLogin
- SurePassID

CDS

- Waters Empower

STANDARDS

PHYSICAL ACCESS SYSTEMS (PACS)

HID LEGIC

OPEN STANDARDS

fido CERTIFIED FIDO2

Looking to a Digitally Empowered Future for Deskless Workers

As innovation continues to digitalize the workplace, operators now have the opportunity to interact with their shop floor systems through a digitally empowered, secure, and smart authentication process.

Nymi is dedicated to forging enduring partnerships and has built a solution designed to adapt, scale, and grow alongside their customer's digital transformation journeys. This commitment ensures that organizations can navigate an unknown future and gain ongoing returns by investing in their connected workforce.

About Nymi

Nymi connects people to their digital world in a single authentication to their Nymi Band. We are delivering connected workers to regulated industries with our innovative solution that enables tap-to-access with a compliant wearable wristband. With Nymi, organizations can simultaneously upgrade their security and employee experience to unlock the true value of digital transformation, one that includes the connected workforce.

For more information, contact:
nymi.com
info@nymi.com

FCC Caution

This device complies with part 15 of the FCC Rules. Operation is subject to the following two conditions:
(1) This device may not cause harmful interference, and
(2) this device must accept any interference received, including interference that may cause undesired operation.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

-Reorient or relocate the receiving antenna.
-Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/TV technician for help.

The device has been evaluated to meet general RF exposure requirement. The device can be used in portable exposure condition without restriction.

IC Warning

This device complies with Innovation, Science and Economic Development Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:
(1) This device may not cause interference, and
(2) This device must accept any interference, including interference that may cause undesired operation of the device.
Cet appareil est conforme aux normes RSS exemptées de licence d'Innovation, Sciences et Développement économique Canada. L'exploitation est soumise aux deux conditions suivantes:
(1) Cet appareil ne peut pas causer d'interférences, et
(2) Cet appareil doit accepter toute interférence, y compris celles qui pourraient entraîner un fonctionnement accidentel de l'appareil.

Any Changes or modifications not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.
Tout changement ou modification non expressément approuvé par la partie responsable de la réglementation de l'OCDE peut faire perdre à l'utilisateur le droit d'utiliser l'appareil.

Note: This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates uses and can radiate radio frequency energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no
guarantee that interference will not occur in a particular installation. If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:
-Reorient or relocate the receiving antenna.
-Increase the separation between the equipment and receiver.
-Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
-Consult the dealer or an experienced radio/TV technician for help.

Remarque: cet appareil a été testé pour répondre aux limites des appareils numériques de classe B conformément à la partie 15 des règles de la Federal Communications Commission des États - Unis. Ces limites sont conçues pour fournir une protection raisonnable contre les interférences nuisibles dans les installations résidentielles. L'appareil génère de l'énergie RF utilisée et rayonne, ce qui peut causer des interférences nocives pour les communications radio s'il n'est pas installé et utilisé conformément aux instructions. Cependant, aucun
Garantie contre les interférences dans une installation spécifique. Si l'appareil cause des interférences nuisibles à la réception de la radio ou de la télévision, qui peuvent être déterminées en éteignant et en allumant l'appareil, l'utilisateur est encouragé à tenter de corriger les interférences par une ou plusieurs des mesures suivantes:
- redirection ou repositionnement de l'antenne de réception.
- augmenter l'espacement entre l'appareil et le récepteur.
- Connecter l'appareil à une prise sur un circuit différent de celui auquel le récepteur est connecté.
- consultez votre revendeur ou un technicien radio / tv expérimenté pour obtenir de l'aide.

RF warning for Portable device:
The device has been evaluated to meet general RF exposure requirement. The device can be used in portable exposure condition without restriction.

Avertissement RF pour les appareils portables:
L'appareil a été évalué pour répondre aux exigences générales d'exposition aux radiofréquences. Équipement Peut être utilisé sans restriction dans des conditions d'exposition portables.