Nymi With Evidian User Requirements Specifications

Connected Worker Platform

1.3

2021-06-01

Contents

Introduction

This document is the User Requirements Specification (URS) for a solution in which user authentication for login and electronic signatures is based on biometrics instead of usernames and passwords.

The solution combines Evidian Enterprise Access Management (EAM) and `Connected Worker Platform`(CWP) for providing biometric authentication with configured application, such as a Manufacturing Execution System (MES).

Nymi provides a biometric wearable (Nymi Band) as the authentication device.

Overview

This document is intended to document solution requirements for a fictitious environment. The environment details described in this document are for an example exercise and are not indicative of the full environmental support that is offered by the Nymi solution. Environment details that are used in this example are provided below.

- Windows 10 OS on terminal computers
- Virtualized environment (thin clients) used in production for configured applications
- Windows 2016 OS for the server
- Manufacturing environment is Class A/B
- Cleaning requirement for manufacturing environment is isopropyl alcohol wipes (70%)

Nymi provides a biometric wearable (Nymi Band) as the authentication device. The overall goal of the system is to implement a biometric authentication solution to allow users of the system the ability to:

- Login and logout from windows, MES solutions and other applications
- Sign off using e-signatures on electronic records as outlined by process requirements

Implementation of a biometric authentication solution offers improved data integrity, reduced risk of compromised credentials and an improvement in user experience across the organization, particularly in secure pharmaceutical manufacturing.

The system must maintain compliance with 21 CFR Part 11 and follow standards as outlined in GMP environments.

Responsibilities

This section is drafted on typical responsibilities for stakeholders involved in the GAMP5 validation process. It is expected this section is tailored based on the company's project teams and roles.

In general, all stakeholders are required to review and approve this document.

Additional responsibilities are as follows:

System Owner:	• Editing and approving this URS. • Ensuring this URS adheres to established internal and external guidelines for GAMP5 User Requirement Specification document generation. • Owning Supplier Evaluation efforts with Supplier
IT Team:	• Providing input and guidance in the creation of this URS as related to Information Technology and corporate business Solutions.
Automation team:	• Providing input and guidance in the creation of this URS as related to automation Solutions.
QA:	• Ensuring this URS adheres to established internal and external guidelines. • Assist with Supplier Evaluation

Quality Requirements

A service agreement and quality agreement will be developed and agreed to by both parties involved. The vendor must be willing to participate in an audit of their development and quality practices against industry standard and organizational criteria.

There are no requirements that have been identified as critical to quality for the solution. Quality critical requirements, such as critical process parameters (CPP) and critical quality attributes (CQA) are unique to a specific manufacturing environment. The impact and risk related to the implementation of Connected Worker Platform is low.

As a supplier, the pharmaceutical manufacturing company needs to leverage supplier activities to the maximum possible extent, and also ensure fitness for intended use, which is why Nymi, as outlined in the GAMP guidance, fully supports customers with GAMP Software Validation packages and supports supplier assessments.

Solution Overview

The objective of the solution is to provide standard functionality for the following activities:

- Enroll and unenroll a wearable biometric device with a user.
- Authenticate users to facilitate log in to and log out from the Windows 10 OS
- Administer the configuration of the Solution, modify configuration settings, and maintain users and devices

This project introduces a solution that can be utilized during the manufacturing of products, to reduce reliance on a username and password for authentication/sign off on production activities.

Operational Requirements

This section has been drafted based on a fictitious customer environment, and evaluation of the solution within this environment. This document does not cover all environment requirements (ie. Windows 7, Windows Server 2012 R2). This section / infrastructure should be updated based on the production systems.

The following section identifies requirements for the Solution.

Functional Requirements

Functional Requirements that enable a system to perform the business process being automated. Items covered are safety, security including access control, audit trails, use of electronic signatures, output and unambiguous error messages.

Table 1: Functional requirements

Number	Requirement	Importance
URS-027	The Solution provides an administrator with the ability to view and print reports that provide information about additions and modifications of users and device associations.	Mandatory
URS-028	The Solution provides the ability to report on an authentication action, the user that performed the action, the date of the action and the time of the action, historically and in real time.	Mandatory
URS-018	The Solution provides an automatic user logoff from the Windows session if the operator removes the wearable authentication device/ the device is deauthenticated.	Mandatory
URS-023	The Solution only provides access to authorized users.	Mandatory
URS-039	The Solution provides a mechanism to associate Nymi Bands to a single user.	Mandatory

Data requirements

Data handling requirements should be considered to understand the impact to patient safety, product quality and data integrity. Items covered include electronic records, definition of data, required fields, data migration, data input and subsequent editing, backup and recovery, archive requirements, data security and integrity.

Table 2: Data requirements

Number	Requirement	Importance
URS-010	The Solution stores biometric information in an encrypted format.	Mandatory
URS-011	The Solution supports the backup and restore of any internal database that is used in the Solution.	Mandatory
URS-012	Biometric information for authentication is not stored centrally.	Mandatory
URS-013	All passwords which are stored by the Solution are encrypted.	Mandatory

Technical Requirements

Technical requirements outline any changes in system operation, disaster recovery, performance requirements, actions required in case of failure, access speed, hardware, portability, efficiency and configurability requirements.

Table 3: Technical requirements

Number	Requirement	Importance
URS-029	The Solution shall be configured so that there is no single point of failure.	Mandatory
URS-030	An alternative method of authentication for the user shall be available for the operator if the wearable biometric is unavailable.	Mandatory
URS-009	The wearable biometric authentication device shall have means for charging.	Mandatory

Number	Requirement	Importance
URS-007	The wearable biometric authentication device function shall function for the duration of an Operator shift (8-10hrs) on a single charge.	Mandatory
URS-020	The Solution supports NFC taps to signal intent when the Authentication Module is configured to use NFC-only (RFID).	Mandatory

Interface requirements (User interface)

Table 4:

Number	Requirement	Importance
URS-001	The Solution shall operate on standard IT infrastructure. (Windows Server 2016).	Mandatory
URS-002	The Solution supports a deployment of server components in a virtualized environment.	Mandatory
URS-003	The Solution integrates with single and multi-domain configurations in a single or multi-forest environment, with one-way or two-way trust.	Mandatory
URS-004	The Solution provides secure communication with endpoints that require credential verification.	Mandatory
URS-014	The solution provides the capability to log into Windows and Enterprise Single Sign-On to on-boarded applications (including MES applications).	Mandatory

Number	Requirement	Importance
URS-015	The Solution provides a configurable login to the MES Applications with a pop-up windows for authentication.	Mandatory
URS-019	The Solution provides a self-service administrative interface to associate and disassociate a user with a biometric device.	Mandatory
URS-021	The Solution supports remote desktop services such as RDP to access and authenticate a remote MES Solution.	Mandatory
URS-022	The Solution supports the use of thin clients to remotely access configuration applications and provide e-signatures over RDP and Citrix sessions.	Mandatory
URS-024	The Solution provides an administrator with the ability to view and modify Policies for the wearable authentication device.	Mandatory
URS-025	Operators shall be able to visually check battery charge on the wearable device.	Mandatory
URS-026	Operators shall be able to visually check the authentication status of the wearable biometric device. (authenticated or de-authenticated)	Mandatory

Environment Requirements

Environment requirements outline that in which the system is to work including physical layout, physical conditions, physical security, power requirements and any special physical or logical requirements.

Table 5: Hardware and infrastructure requirements

Number	Requirement	Importance
URS-005	The wearable biometric authentication device does not introduce any unacceptable risks to the health and safety risk of the person who wears the device.	Mandatory
URS-006	The wearable biometric device functions under personal protective equipment (PPE) suitable for Class A/B, Class C and Class D environments.	Mandatory
URS-008	The wearable biometric authentication device function shall be suitable for cleaning with isopropyl alcohol (IPA) 70% wipes	Mandatory
URS-016	The Solution provides an automatic user logoff from the Windows session if s/he walks away from a logged in Windows session. Log off will trigger when the wearable biometric device is outside of the BLE range.	Mandatory
URS-017	The solution shall recognize the wearable biometric on the NFC reader if 3 cm of plexiglass is between the NFC reader and the band.	Mandatory

Constraints

Table 6: Constraints

Number	Requirement	Importance
URS-031	The Supplier provides maintenance and support for the Solution.	Mandatory
URS-034	The Supplier meets the requirements for the Supplier Evaluation Process.	Mandatory
URS-035	A Service Level Agreement shall be implemented with the Supplier.	Mandatory

Lifecycle Requirements

Table 7: General supplier requirements

Number	Requirement	Importance
URS-031	The Supplier provides maintenance and support for the Solution.	Mandatory
URS-032	The Supplier provides administrator and user training documents.	Mandatory
URS-033	The Supplier is able to license and support the software.	Mandatory
URS-036	The Supplier has a mechanism in place to provide notification of software changes, including software upgrades, hotfixes, and patches.	Mandatory
URS-037	The Supplier shall provide specifications for the function and design of the Solution to satisfy applicable requirements in the URS.	Mandatory
URS-038	The Supplier shall provide documentation in the form of system manuals and software administration manuals in electronic format, at a minimum, where applicable.	Mandatory

Glossary

Definitions/acronyms used throughout this document are defined below.

Table 8: Glossary

Acronym	Definition
AD	Active Directory. Directory service for domain networks.
AD LDS	Active Directory Lightweight Directory Services. Directory service for domain networks.
IAM	Identity Access Management
SSO	Single Sign-On
MES	Manufacturing Execution System
CWP	Connected Worker Platform
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.

Approvals

This document is approved for use as a sample URS.

Out of Scope

For the intent of this sample URS the solution covers Connected Worker Platform (CWP) for providing biometric authentication with configured application, such as a Manufacturing Execution System (MES).

The sample requirements outlined in this document are related to NEE requirements. The sample does not cover requirements covered by an MES and a thorough URS that should cover the entire system, including processes, procedures and policies. Each customer environment is unique, and a full set of requirements should be produced when implementing CWP with an MES.

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