Registration and On-Boarding

Created by Charles Young on Nov 10, 2016

This section provides a high-level description of the generic registration process supported by the NBS. It explains the general approach. The details of the registration process will vary from market to market. However, the approach is expected to be similar across most or all markets.

This document uses the term 'connected organisation' to represent any organisation that includes wholesalers and persons authorised or entitled to supply medicinal products to the public. It uses the term 'system management organisation' to represent any organisation that is responsible for implementation, deployment or operational management of pharmacy or wholesaler systems. Note that a single legal entity (e.g., a company owning a large chain of pharmacies) may act in both roles.

The following diagram illustrates the registration and on-boarding process supported by the Solidsoft Reply National Blueprint System. This is described and explained in the following sections.

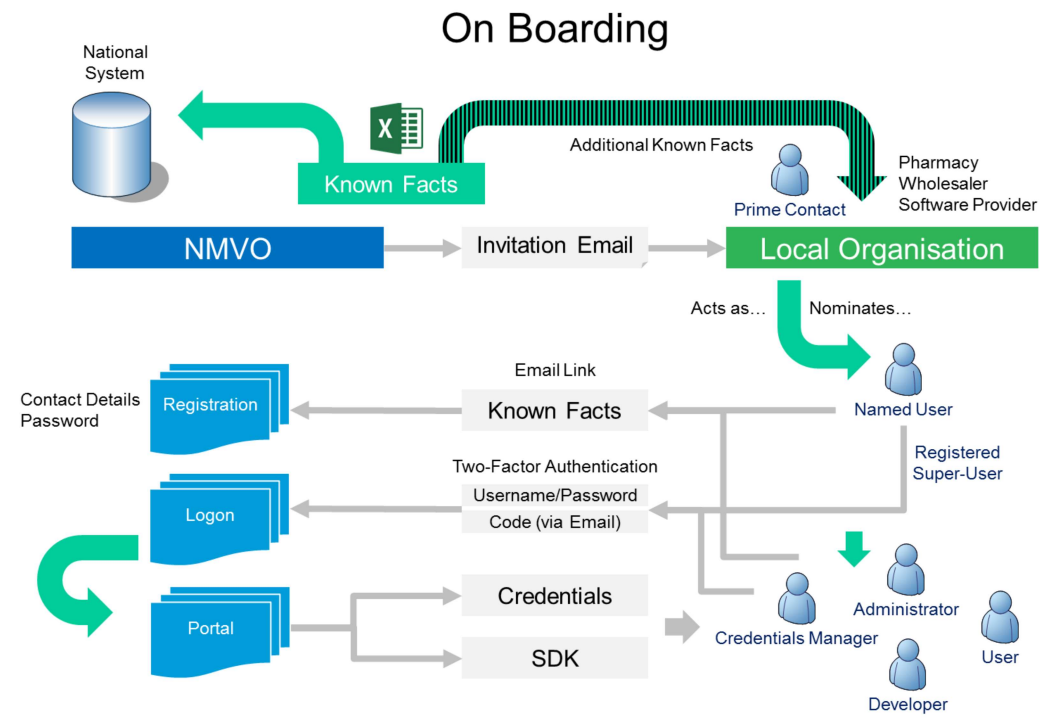

Figure 5: Registration and On-Boarding Process

Registration of Organisations

The EMVS must take all reasonable steps to ensure that access to its systems is secure and that the systems are accessed only by authorised systems and users. It must also maintain audit trails of usage. This includes the ability to identify and record the connected organisations and locations which access the national system and the individual users who carry out specific operations. This may include users at system management organisations that are authorised to access certain resources on behalf of connected organisations.

Systems that connect to the NBS must provide credentials which the NBS can authenticate in order to authorise the system to invoke the programmatic API. However, systems may be built and maintained by third-party software or service providers, rather than by connected organisations. The NBS must support the needs of both software vendors and connected organisations.

To facilitate this, the NBS supports a registration process. The process depends on the use of 'known facts'. A known fact is some unique piece of information known to both the NMVO and the connected organisation or system management organisation. The NBS does not mandate any specific known facts, but makes provision for markets to maintain records of one or more known facts for each system management or connected organisation. The system does not restrict the meaning of 'organisation' in this context. For example, different sets of known facts may be recorded for the same company to reflect geographic locations or organisational units. Markets are free to represent and model the entities for which facts are known in accordance with their specific needs.

Examples of known facts might include a national registration number issued to a connected organisation, or some identifier provided by the NMVO to a software vendor. Connected organisations within a given market will already be in possession of suitable known facts, but markets may wish to issue known facts to support the EMVS. It is strongly recommended that at least one known fact for each organisation should not be generally known or discoverable outside of the organisation. The mechanism used to generate and distribute known facts to individual connected organisations is not within the scope of the National System. NMVOs are free to implement whatever approach they wish.

The NBS does not define how the registration process is initiated. One option might be for an organisation to initiate the registration process by requesting an invitation through an on-line interface. Alternatively, the NMVO may initiate registration based on its knowledge of organisations in the local market. The only requirement made by the NBS is to identify a named person at the connected or system management organisation, together with general details of the organisation and location (e.g., name, postal address). The named person will be configured initially to act as a super-user. Their details will be captured within the national system.

For each registration, the national system will generate an invitation code and send it via email to the primary contact at the organisation. The NMVO may support alternative delivery approaches (e.g., registered mail) if it wishes. The email will contain a link to a portal site. The link contains has an expiration date, after which attempted access to the portal using the link will be denied.

The registration process centres on the identification of a named person at each organisation. Each organisation will have a single named person who acts as the person with overall responsibility for the connection of that organisation to the National Blueprint System. This could be primary contact or someone else nominated by the organisation to whom the email can be forwarded.

When the named person clicks on the link, they are taken to a registration site where they enter various details including the invitation code and a set of known facts. This information is passed over a secure connection to the national system which verifies the known facts against the invitation code. If these verification tests are passed, the national system allows the named person to set up their portal credentials, consisting of a user name and password. They must also provide their contact details including an email alias. The National System automatically assigns the 'super-user' role to the named person. The super user has full privileges which cannot be revoked.

Logon with Multi-Factor Authentication

Having registered the organisation, the super user can now log onto the system using the user name and password they assigned during the registration process. They do this within a logon screen provided by the portal. If the user name and password are valid, the super user is challenged to enter an additional code. This is a one-time (single use) code with a short expiry time (less than five minutes) generated by the National Blueprint System and returned to the user through an out-of-band channel. By default, the National Blueprint System supports email using the email alias provided by the named user. Other channels (e.g., SMS) may be supported, subject to negotiation with individual markets. If the user enters the code correctly before it expires, they are authorised to access the portal. If the code expires, the super user must perform a new logon.

The same multi-factor authentication approach is mandated for all portal users, including additional users created by the super user or designated administrator. For additional users, they will be challenged to change their initial password, set by an administrator, on first logon. All users can reset their passwords. Passwords can be configured to expire after a set period (e.g., three months), forcing the user to register a new password the next time they log on.

Users and Roles

The super-user bears overall responsibility for ensuring authorised access to various resources. To facilitate this, the super user can create additional users. However, before they can perform any further actions on the portal, they must first indicate the roles they wish to assign to themselves (see below). This is for auditing purposes. The super user can change their own role selection at any time.

In addition to the super user, the following roles for local users are supported by the NBS portal.

- **Administrator –** A user with the right to create, change or remove other users, reset passwords, assign roles, etc.
- **Credentials Manager –** A user with the right to obtain and download a set of client credentials that will be used to configure the pharmacy system so that it can be authenticated and authorised to access the National System API.
- **Developer –** A user with privileges to download this SDK, together with tools, example code, etc.
- **Validation User –** A user with privileges to perform pack validation using the emergency browser-based user interface provided as part of the NBS. This user interface can be used by pharmacies and wholesalers to verify the authenticity of the unique pack identifier and decommission it in case of failure of their own software.

Super-users must select themselves into the administrator role to create additional users in these roles. Each user account has a designated user name and an initial password which must be changed on first log-on. The super user assigns one or more roles to each account.

The super user can transfer their role to a new named person. Only one named person can be a super user for a given system management or connected organisation at any one time. The NMVO also retains the ability and authority to re-assign the super-user role to a different named person.

A credentials manager can download the client credentials. These consist of a client identifier and a client secret. All downloads are made over a secure connection and are audited. The credentials comply with the OAuth 2.0 framework. It is the responsibility of the Credentials Manager to ensure that credentials are managed and provisioned securely within a given instance of a pharmacy system. This may be for development and test purposes, or for a production instance of the pharmacy system at a specified location. Individual NMVOs may implement additional processes beyond the National System to validate the security and management of client credentials on pharmacy systems.

A developer can download SDK material and access any additional developer-centric functionality (e.g., forums) that may be provided via the portal. Developers must be covered by a non-disclosure agreement, signed by the organisation they represent, to access these resources.

The roles described above are used solely to manage authentication of portal users. Individual users of pharmacy and wholesaler systems are not authenticated by the NBS. These users are authenticated locally by the pharmacy or wholesaler system using whatever mechanism that system implements for this purpose. Systems pass an opaque requestor identifier to the national system with each request. These identifiers are recorded within the audit trail. They may be used for forensic purposes to trace activities back to individual users authenticated by a given pharmacy or wholesaler system. The NBS does not hold any information to map requestor identifiers to named users. Mapping can only be done by consulting data stored by a given instance of a pharmacy or wholesaler system.

No labels