BeMVO
Belgian Medicines
Verification Organisation

Falsified Medicines Directive

End User Implementation

7/09/2018

End users on boarding – Connect user

Standard process – Manual implementation by the end User

- User is created in BMVS by BeMVO
- An email is sent to the User with
  - PKI URL for certificate download
  - Client ID
  - User ID
  - TAN
- User receives Password via separate channel (post)
- User connects to PKI and get access with Login & Password
- User enters TAN to download certificate
- Passphrase appears on the screen, which the user has to write down
- User installs certificate with Passphrase (for webservices and in browser for GUI)
- User connects to the system and has to change password at first connection
- User can now start using the system

Standard process is possible but implying manual interventions

End users – automate implementation

Agree on common procedure for alternative approach

Suggestion:

- SWS provides to BeMVO a set of users he plans to implement in the coming period
- BeMVO uploads the set of selected users in the BMVS
- BeMVO extracts a file and provide the file to the SWS containing
  - User identification
  - Client ID
  - User ID
  - TAN
  - Password (initial)
- Information is completed with the PKI-URL for download the Certificate (the same for all users), as well as the other end points for system connection
- For security reasons, this information is provided in separate, protected files (with date of update)
- At installation, the SWS store user specific information in encrypted files on user's system for later use

End users on boarding – alternative option (2)

Suggestion (continued):

- Run webservice “G615 download certificate” with connection to PKI URL

```
<G615Request>
 <Header>
    <Auth>
      <ClientLoginId>G4321-14-01RT</ClientLoginId>
      <UserId>John002</UserId>
      <Password>838hdjLk#</Password>

<Body>
    <Tan>12649334</Tan>
```

- Response:

```
<G615Response>
<Body>
    <Cert name="John002"
passphrase="HJ7HK8BKAD0QLIN">TUlJSzBBSUJBekNDQ29vR0NTcUdTSWIzRFFFSEFhQ0NDbnNFZ2...</Cert>
```

- The base64 encoded certificate data needs to be written to a p12 file (with the Certificate name)
- Store information (passphrase, Certificate name) in an encrypted file for later use (with date of update)
- Implement the User, Password, Certificate with the electronic available data elements

End users on boarding – alternative option (3)

Suggestion (continued):

Set up User password and integrate the user's acceptance of the terms and conditions in the automated implementation process

- After implementation of the User, Password (initial), Certificate:
  - Request a new password from the user (or propose a new password to the user)
  - Run webservice G445 – Change password to update the password of the user (using the initial password)
- Store the new information (password) in the encrypted file for later use

- The system is ready to go!

Password updates

Password to be renewed every 90 days

- User can renew through the GUI

or

- Suggestion: Trigger automated update - 3 options
  - Store date last renewal by user on the user's system and trigger update eg 4 weeks before expiry
  - Wait for the notification by the BMVS (in a webservice) that the password will expire in 7 days, then trigger the renewal
    <ns1:Notifications ns1:notificationCode="NMVS_NOTIFY_AU_02"
  - Wait until the password expire, and trigger the update when the user can no longer access BMVS

[Be aware of the case where the seveveral, different end points were implemented for the user – the new password will have to be implemented on all end points]

Suggestion:

- When the renewal needs to be triggered
  → display screen to user showing current password and request to enter new password while also showing the password policy
  [as an alternative, the user's system can also propose a new password, generated according password policy, that the user can accept]
- Store password with date of change in the encrypted file
- Start webservice "G445 Change password" to renew password