User and organization attributes - CustomerID

Description

Ubisecure CustomerID supports storing basic user information to predefined repository objects. Also custom information can be stored to the main user authentication data repository by creating a mapping between the Ubisecure CustomerID internal field name and the repository attribute name. (See `eidm2.properties data.attribute.mapping`)

Ubisecure CustomerID internal user information fields are:

```
firstname, surname, email, mobile, login, locale, password, customerid, companyid, acceptTerms
```

Mapping of basic internal fields to repository attributes goes as follows:

```
firstname = givenName
surname = sn
email = mail
mobile = mobile
login = uid (configurable with general.login.attribute)
locale = By default not mapped. Can be mapped using data.attribute.mapping.
password = UbiloginAuthMethod-object
```

Mapping of extra fields to repository:

```
ssn = description (configurable with data.attribute.mapping)
customerid = Virtual organization structure (depending on configuration)
companyid = Virtual organization structure (depending on configuration)
```

Custom attributes

Mapping of custom fields to repository attributes is configured with `data.attribute.mapping` –properties.

Ubisecure CustomerID supports custom attributes for users and organizations. For users custom attributes will be stored in the database. They may be additionally stored also in the main user authentication data repository. For organizations custom attributes will only be stored in the database.

Storing user custom attributes in the main user authentication data repository is defined using the `data.attribute.mapping.<attribute name>` property as defined below in *Data Storing Properties* chapter. All user custom attributes will be automatically stored to the database as strings. Defining if the user attributes should be encrypted is done using the `data.attribute.encrypt` property as defined below in *Data Storing Properties* chapter.

All organization custom attributes will be automatically stored to the database as strings.

Ubisecure CustomerID does not provide default language text keys for custom attributes because we don't know the names of the custom attributes beforehand. Therefore always when new custom attributes are defined also the language files need to be updated. At least the following new language keys may be required for each new user custom attribute:

```
admin.approval.user.<custom user attribute name>.tooltip
admin.roleinvitation.user.<custom user attribute name>.tooltip
registerWizard.<custom user attribute name>
registration.<registration name>.input.user.<custom user attribute name>.tooltip
tooltip.user.attribute.modification.<custom user attribute name>
user.<custom user attribute name>
```

The display text for each new organization attribute must also be added to the messages_XX.properties file. At least the following new language keys may be required for each new organization custom attribute:

customerid/custom/messages_XX.properties

```
registerWizard.organization.<custom organization attribute name> = <custom organization attribute text shown before field during registration>
organization.<custom organization attribute name> = <custom organization attribute text shown before field>
```

An example of localization for the custom attribute "sic".

customerid/custom/messages_en.properties

```
# shown during registration
registerWizard.organization.sic = SIC Code
# shown on organization details page
organization.sic = Industry Classification Code
```

Organization custom attributes that have not been set for organizations will not be returned in API responses.

Reserved attribute names

There are some reserved names that cannot be used for custom attribute names. They are:
acceptterms, cn, companyid, create, customerid, disable, email, enable, firstname, friendlyname, hetu, locale, login, mandates.remove, mobile, organizationclass, organizationid, organizationtype, otp, otp.activated, otp.state, parentorganizationid, password, pwd, pwd.activated, registration, repouser, responseidformat, roleid, roles.remove, sms, sms.activated, ssn, status, surname, technicalname, uid, userid, username and virtual.

Built-in validations

Password

- Maximum lenght for password value is 64 characters.

Custom attributes

- Maximum length for a custom attribute value is 255 characters.
- Only lower case alphanumeric characters are allowed when naming custom attributes.

Configurations

These configurations are available in the eidm2.properties file.

data.attribute.encrypt

This is a comma separated list of custom attributes that should be encrypted to all data storage facilities, i.e. internal database, Ubisecure Directory and Active Directory. This cannot be enabled for certain attributes, such as cn, mobile or email.

Attributes that are encrypted cannot be used for Directory User Mapping. Attributes that are encrypted can only be found in searches by the exact value (not for example by just a prefix).

Default is <none set>.
Example:

```
data.attribute.encrypt = ssn
```

data.attribute.mapping.<fieldname>

These properties define the mapping between user interface field names and repository attribute names. Some fields have fixed attributes where they are stored to (see previous chapter) and these properties define the attributes where other fields are stored to.
Default is data.attribute.mapping.ssn = description
Example:

```
data.attribute.mapping.ssn = description
```

NOTE: There is no need to define mapping for built-in attributes firstname, surname, email, mobile and login.

data.attribute.country

This property lists attributes that store country values. The values are stored as two-character codes, but all user interfaces for the attribute modification show a country selector user interface element. See *Customization - CustomerID page* on how to configure the country selector options.
Default is <not set>.
Example:

```
data.attribute.country = country
```