The KYC flow from within the Eesti.ee system

30th December 2021
NB! Confidential, not to be distributed without the author's consent.

1. - Overview

The goal of this document is to describe a version where the KYC flow would be a part of the Eesti.ee system rather than a separate microservice. The definitions, terms and ideas used in this document are created to provide a generalistic bird's-eye view of how the KYC process could work if it was part of the larger system rather than a separate microservice or a standalone system. The whole document is written in English as it makes it easier to describe the IT-related terms.

2. Table of contents

3. - Definitions

Obliged Entity

Obliged (for example a bank) or any other entity who has to, due to KYC regulations, have reasonable interest for the KYC data

Data Register

Governmental or other database, where data about persons is being handled or stored (for example. Äriregister, Rahvastikuregister)

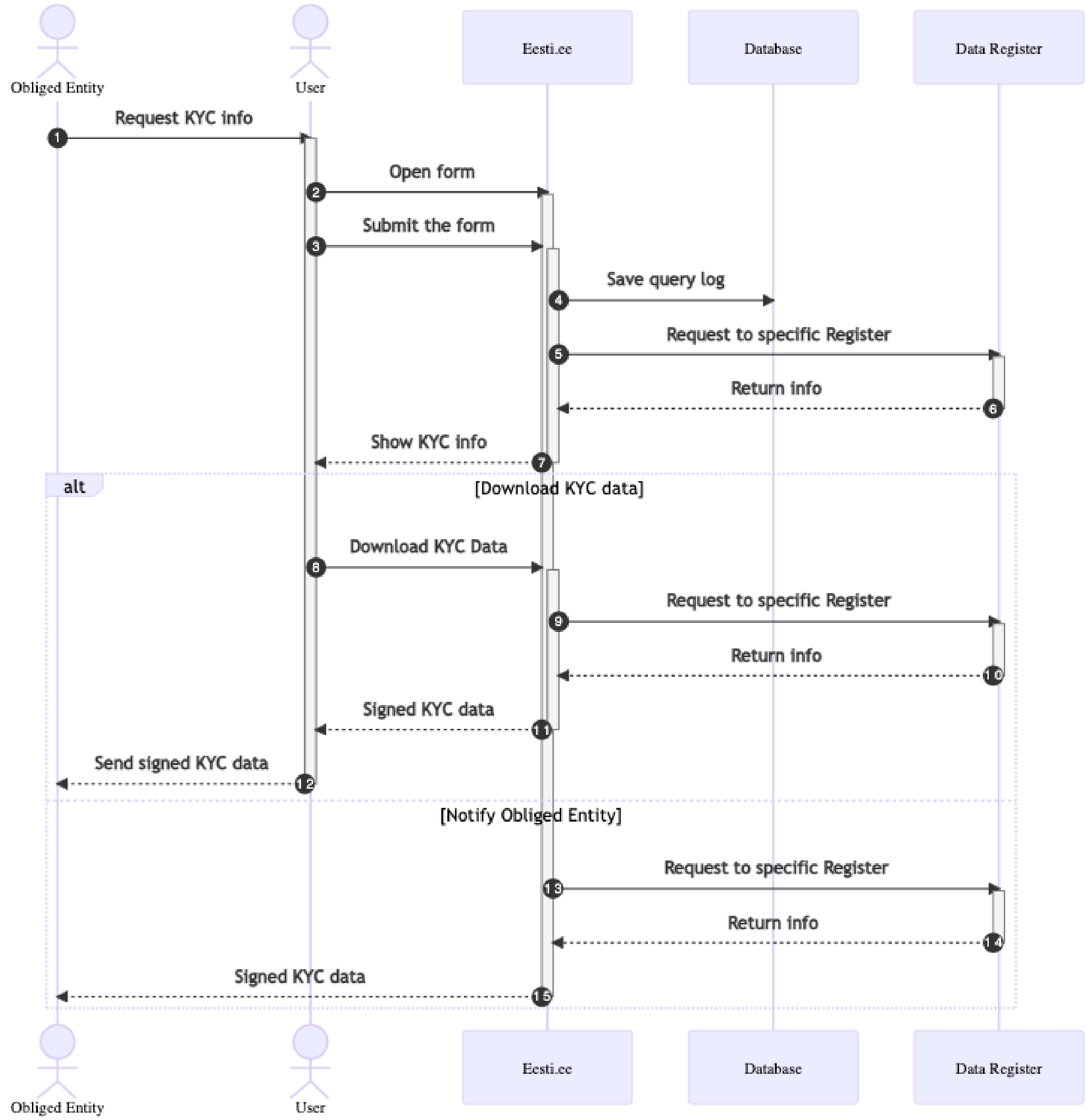
KYC Profile

Profile is a dataset which defines the data from one or multiple data registers. Profile itself does not contain any personal data

Query Log

Saved information regarding who, for whom and when requested data from data-register

4. - Graphical overview



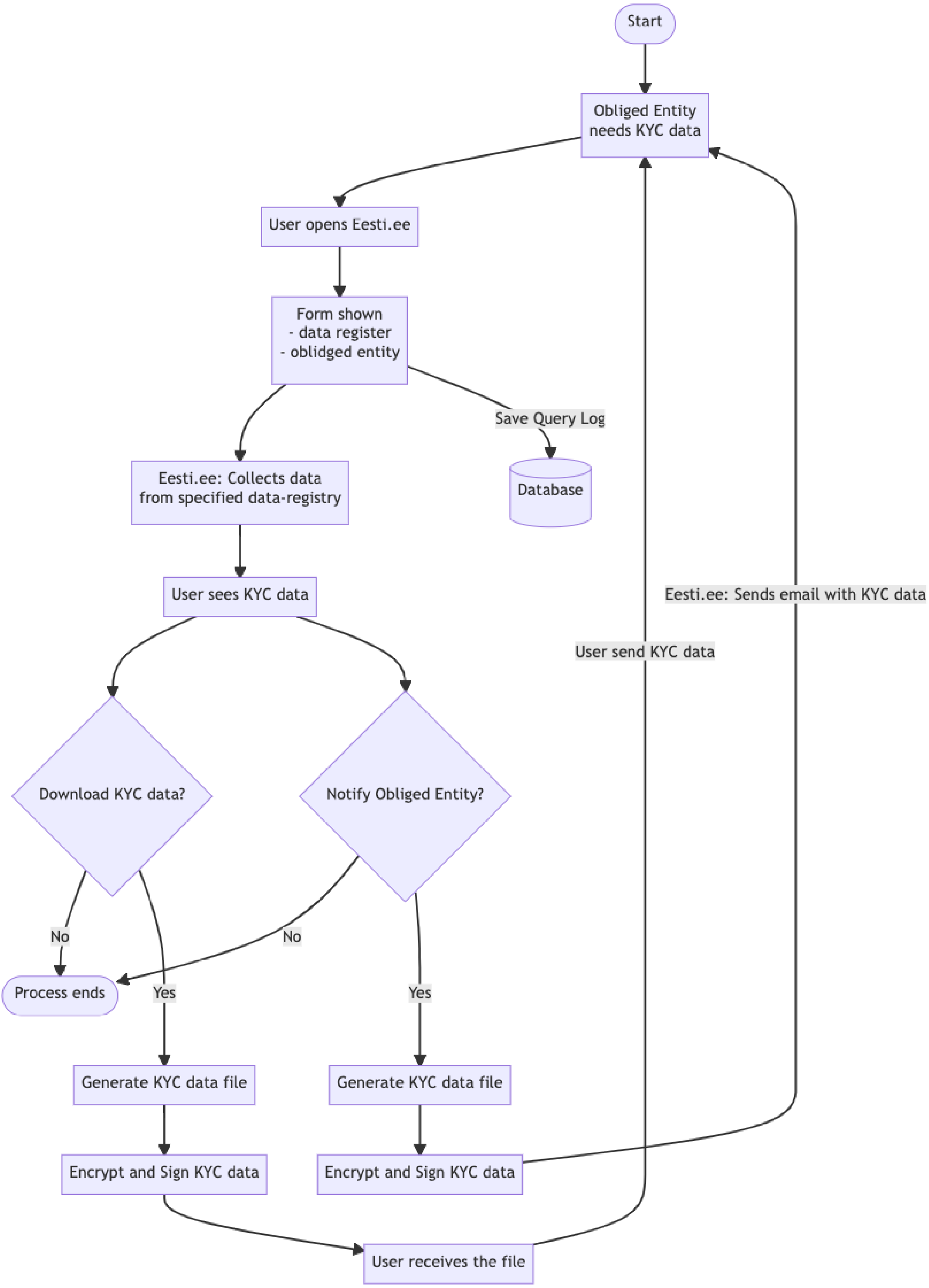
1. Obliged Entity requests the User to provide the needed KYC information
2. User logs in into the Eesti.ee and starts the process by visiting the page/clicking on a button
3. User selects the desired data source and the obliged entity that requested this information
4. Query log is saved to DB
5. Eesti.ee knows how to communicate to different protocols for different data-registers and makes a request for PII (Personally Identifiable Information)
6. PII is returned from the data-register
7. Eesti.ee displays the requested information to the User along with a link to download it

8. User initiates the download action
9. Eesti.ee makes a request to the chosen data register again as the information might have changed since the data was presented to the user.
10. Data from data-register returned
11. Eesti.ee formats the data, generates file in machine-readable format, encrypts and sign it with a digital signature
12. User provides the signed KYC data to Obliged Entity
13. In an alternative approach, the User would be able to enter the target email in the data request submission form (will be used in step 15) and when the form is submitted, Eesti.ee makes a call to data-register
14. Eesti.ee then receives the KYC data from the register as in the other flow.
15. Using the predefined email address, Eesti.ee sends the email along with the signed KYC data to Obliged Entity

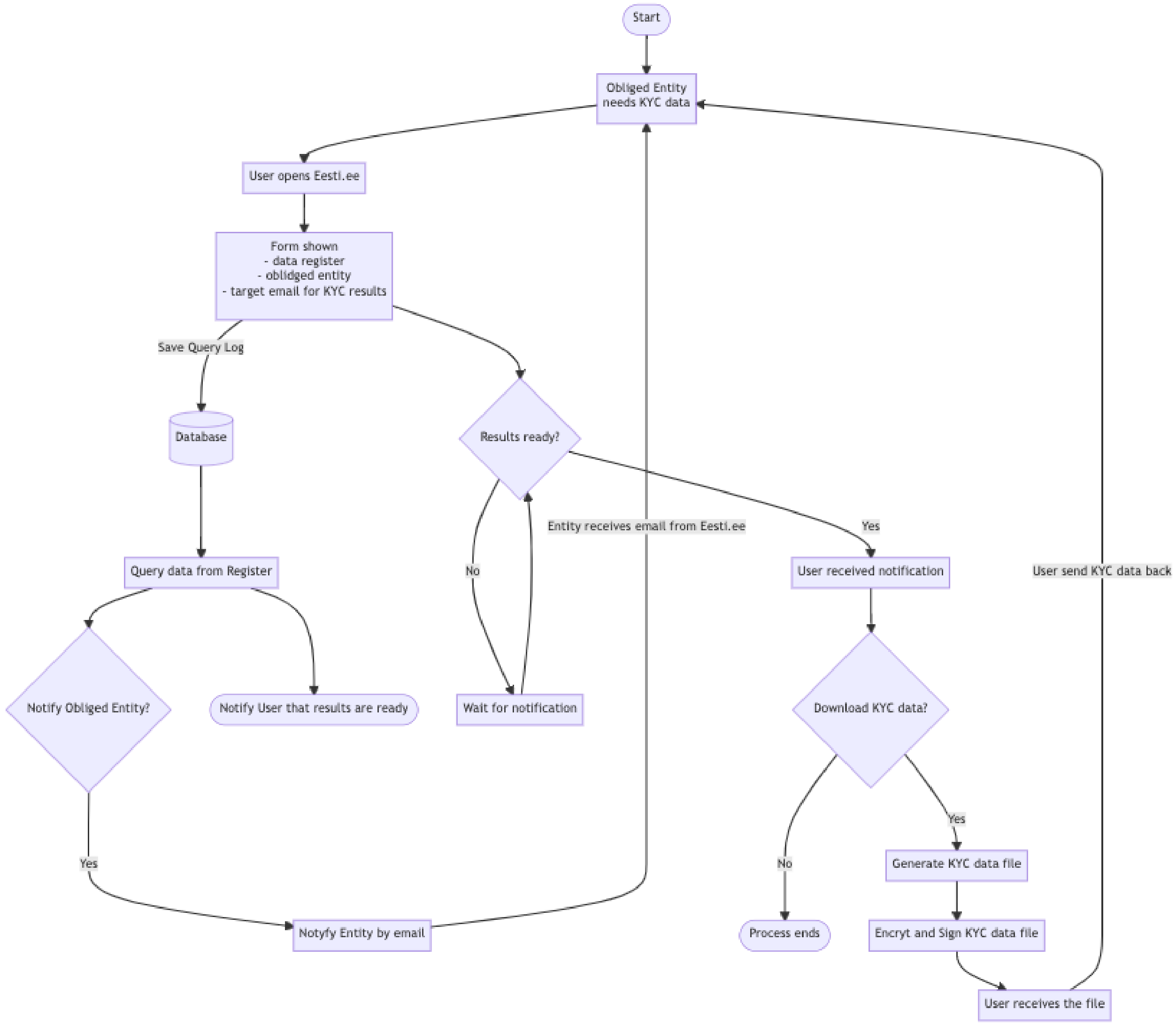
In total, there could be 3 potential paths:

1. The most likely path - The user downloads the data in a machine-readable format that is signed digitally by the Eesti.ee system to ensure data integrity.
2. The user has a chance to share the digitally signed data to an email address that is sent out via the Eesti.ee portal.
3. The user can select an obliged entity who will receive this data. Based on that the information required for that obliged entity type is pre-filled by the system. This way, the end user doesn't need to know the correct data type that would need to be requested from the data register but rather they just need to select the obliged entity. As a result, the user would just need to click the *Share data* or something similar to share the generated data and it would be shared in a pre-agreed format with the Obliged Entity without the user ever needing to download and reupload it. Not only would this be more convenient, it would also be more secure as the data is sent directly across systems rather than being downloaded in-between..

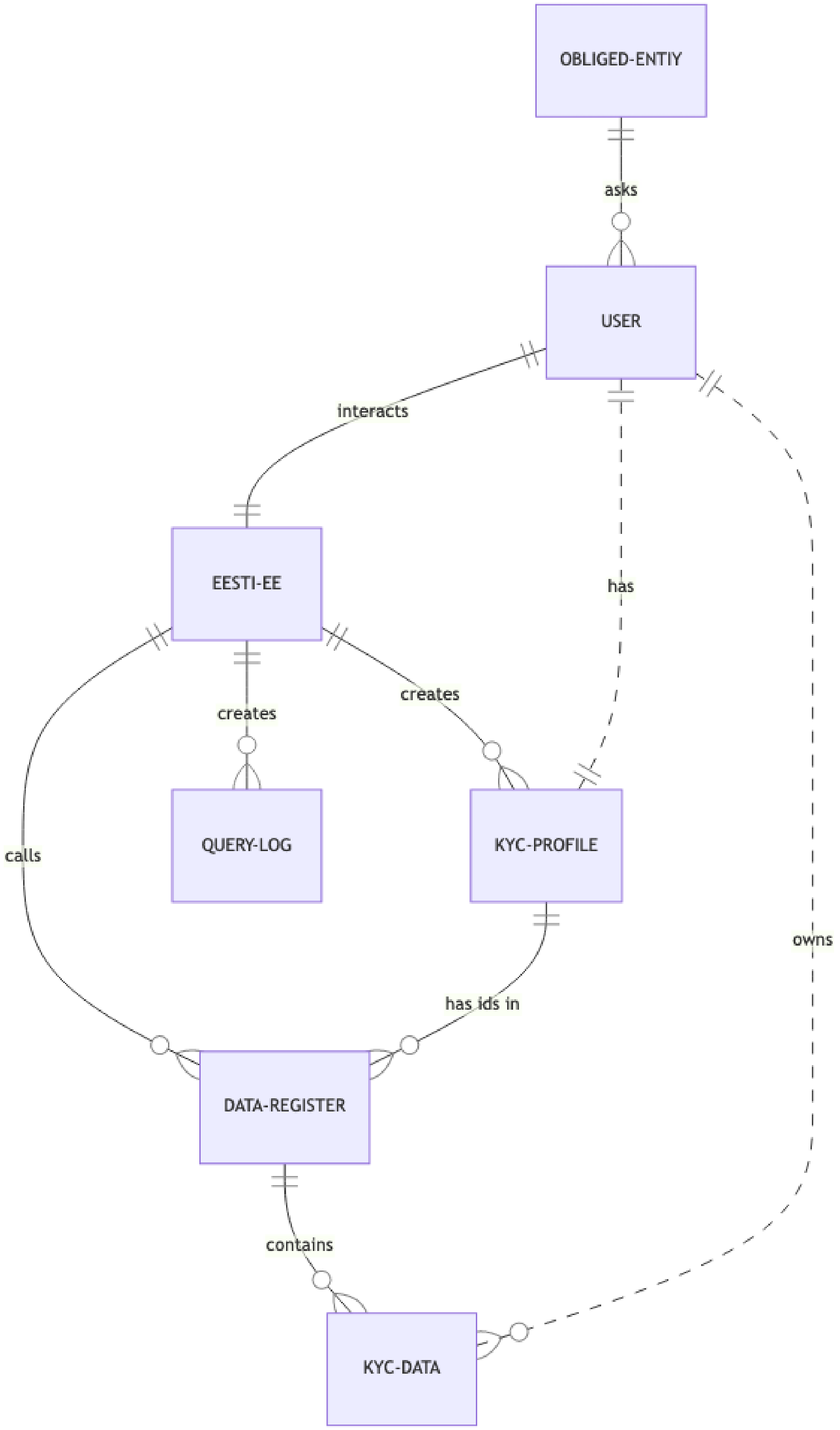
5. Synchronous user flow



6. Asynchronous user flow



7. Domain Model


OBLIGED-ENTIY
asks
USER
interacts
has
owns
EESTI-EE
creates
creates
calls
QUERY-LOG
KYC-PROFILE
has ids in
DATA-REGISTER
contains
KYC-DATA