Description of X-Road services provided by Pääsuke (Oraakliliides)

1. Introduction

This API is for third-party applications that keep information about users' rights in Pääsuke.

The motivation for an application to keep mandates in self-service is the possibility to focus on the functionality of the application and leave taking care of the mandates to Pääsuke.

The following OpenAPI definition accompanies the document:

- https://app.swaggerhub.com/apis/aasaru/paasuke-x-road-services-to-query-mandates/

In the future, this document is also going to cover the following additional services:

- https://app.swaggerhub.com/apis/aasaru/paasuke-x-road-services-to-query-role-definitions
- https://app.swaggerhub.com/apis/aasaru/paasuke-x-road-services-to-query-documents/

1.1 Versions

Version	Date	Description and changes
0.1.0		
0.2.0	05.05.2023	First public draft with the services that are offered by parties who keep mandates in Pääsuke and need to pull that info
0.3.0	06.07.2023	The query that returns mandates no longer return details about the representee and delegate, only mandates.
0.4.0	07.07.2023	"roleStartsWith" query parameter replaced with "ns", "roleIn" query parameter renamed to "role"

1.2 Terminology

- **representee** - a person (private or legal) who has given a mandate to a delegate to be represented by that delegate (or its sub-delegates)
- **delegate** - a person (private or legal), a representee has given the mandate to represent itself.
- **role** - a group of privileges to be used in an e-service that can be granted to delegate by the representee.
- **role namespace** - The first part of the role code until the first colon (colon is excluded) is called the role namespace.
- **mandate** - a role that is given to a delegate by some representee

1.3 X-Road headers

Throughout this document, the X-Road-specific headers (headers beginning with X-Road-...) are removed from the examples of HTTP requests.

If you want to test the queries then you always need to add the following x-road headers and the accept parameter:

```
curl \
-H "accept: application/json" \
-H "X-Road-Client: ee-dev/GOV/70001234/generic-consumer"\
-H "X-Road-UserId: EE39912310123" \
-H "X-Road-Id: EMTA_08544bbd2f41473800309d16bd81c64c0f54193d84b53f8ad22aacdf5e" \
...
```

1.3.1 Note about setting the header param X-Road-UserId

The X-Road-UserId parameter has to be present always if a real person is making a request. It is used for logging purposes and no access checks are performed based on the value.
If the request is made behind some background process, only then this value can be missing.

2. Set up roles

2.1 Motivation

After a self-service portal (or some other system) decides to integrate with Pääsuke and load mandates from there the first thing to do is to create RoleDefinitions. This section presents a sample use case and comes up with RoleDefinitions satisfying that use case.

2.2 Description of example use-case

Let's imagine the following scenario. There is a government agency called "Agency Q" that has:

- a self-service application
  - where representees of private companies occasionally need to log in to view information and submit reports
  - also, representees of other government bodies might need to log in to view information and submit reports
  - a private individual can log into the self-service portal and represent oneself as the individual or represent some company
- the agency offers machine-to-machine services (over X-road) for private companies
  - there is a need that one company (like software as a service provider) could call the services on behalf of another company
  - for that, the private company must first give a mandate to the software as a service provider
  - it is not possible to call the machine-to-machine service as an individual as the X-road services only return company data

This agency wants to use the Pääsuke to take care of handling the mandates. Agency Q adds information to their self-service portal that granting mandates must take place in Pääsuke (eesti.ee portal).

The requirements for self-service access are the following:

1. Regarding private companies, all the members of the management board (juhatuse liikmed) and people set as procurators (prokuristid) must be able to log in to the self-service
2. Regarding government bodies (registry code starts with 7) the representee set in Business Registry (asutuse esindusõiguslik isik) must be able to log in
3. If some physical person has been given the role "Enter" and/or role "Enter and submit" then this person is allowed to access the self-service system
4. If some person has been given the role "Mandates manager" then this person is not allowed to access the self-service system (the person must grant oneself the "Edit" role or "Edit and submit" role first)

The requirements for Pääsuke (for creating and storing mandates) are the following:

1. If the management board member or procurator has the right to represent the company alone then this person can assign roles (create mandates) on behalf of the company
2. For (local) government bodies the person with the right to represent the agency (asutuse esindusõiguslik isik) can assign roles (create mandates) on behalf of that agency
3. These mandates can be created (by persons listed above) with the following role codes
   a. role "Edit" has code "AGENCY-Q:Edit"
   b. role "Edit and submit" has code "AGENCY-Q:Edit.submit"
   c. role Mandates.manager has code "AGENCY-Q:Mandates.manager"
   d. role Machine-to-machine access has code "AGENCY-Q:Machine-to-machine-services"
4. The roles "Edit" and "Edit and submit" can be given to individuals and to legal persons and these roles can be sub-delegated
5. The Mandates.manager role can only be given to individuals and this role cannot be sub-delegated
6. If the "Edit" role and/or "Edit and submit" role is given to a company then the company cannot log in to the self-service system but the management board member (or procurist) of that company must further sub-delegate that role to a natural person (like an employee)
7. The role "AGENCY-Q:Machine-to-machine-services" can only be given to a company (to the software as a service provider) and not to an individual. This role cannot be sub-delegated.
8. When creating mandates and adding sub-delegates these operations need to be digitally signed in Pääsuke
9. If the company wants to withdraw any of the mandates then the withdrawal must also be digitally signed
10. If the physical person has received a mandate from some company and wants to waive then for that there is no need to digitally sign (the person has to just click a button in Pääsuke UI)

2.3. Sample role configuration

Based on that information the following role configurations are created and stored in Pääsuke.

	RoleDefinition parameter	**code: AGENCY-Q:Edit.Submit**	**code: AGENCY-Q:Mandates.manager**	**code: AGENCY-Q:Machine-to-machine-services**
1a	title.en	Agency Q: Enter and submit	Agency Q: Mandates manager	Agency Q: Make x-tee requests in behalf of the enterpreneur
1b	title.et	Agentuur Q: Sisestaja-esitaja	Agentuur Q: Volituste haldur	Agentuur Q: X-tee päringute tegemine ettevõtja nimel

2a	description.en	Can enter reports and submit the name of the entrepreneur. This role can be assigned to both individuals and to legal persons (like a bookkeeping company that takes care of submitting reports). If a company is assigned this role then the company must first further sub-delegate this role to some physical person (like an employee of the bookkeeping company). If this role is given to a legal person then it can be only given with the right to sub-delegate it.	Can manage mandates in the name of the entrepreneur or private person. In order to access the self-service the owner must have role "Agency Q: Enter" or "Agency Q: Enter and submit". The mandates manager can assign these roles to oneself if needed. This role cannot be assigned to legal persons.	Allows software as a service provider to query x-road services in the name of the entrepreneur. This role can only be assigned to legal persons.
2b	description.et	Saab ettevõtja nimel sisestada ja esitada raporteid. Rolli võib määrata peale füüsiliste isikute ka juriidilistele isikutele (näit raamatupidamisfirma, kes ettevõtja eest raporteid esitab), kes seejärel peavad selle rolli eesti.ee-s edasi volitama mõnele füüsilisele isikule (raamatupidamisfirma töötajale). Juriidilisele isikule saab rolli anda ainult koos edasivolitamise õigusega.	Võib füüsilise isiku või ettevõtja nimel lisada ja eemaldada volitusi, aga iseteenindusse sisenemiseks peab omama kas 1) rolli "Agentuur Q: Sisestaja" või 2) rolli "Agentuur Q: Sisestaja-esitaja" (mille antud volituste halduri rolli omanik saab endale vajadusel ise määrata eesti.ee portaalis). Seda rolli ei saa määrata juriidilistele isikutele.	Võimaldab tarkvara teenusepakkujal teha ettevõtja nimel X-Tee päringuid. Seda rolli saab määrata vaid juriidilistele isikutele.
3	representeeType	NATURAL_PERSON, LEGAL_PERSON	NATURAL_PERSON LEGAL_PERSON	LEGAL_PERSON
4	delegateType	NATURAL_PERSON, LEGAL_PERSON	NATURAL_PERSON	LEGAL_PERSON
5	addableBy	BR_REPRIGHT:JUHL_SOLEREP, BR_REPRIGHT:PROK_SOLEREP, AGENCY-Q:Mandates.manager NAT_REPRIGHT:SOLEREP	BR_REPRIGHT:JUHL_SOLEREP, BR_REPRIGHT:PROK_SOLEREP, AGENCY-Q:Mandates.manager, NAT_REPRIGHT:SOLEREP	BR_REPRIGHT: JUHL_SOLEREP, BR_REPRIGHT: PROK_SOLEREP, AGENCY-Q: Mandates.manager
6	addingMustBeSigned	TRUE	TRUE	TRUE
7	canSubDelegate	TRUE	FALSE	FALSE
8	subDelegateType	NATURAL_PERSON	-	-
9	subDelegableBy	BR_REPRIGHT:JUHL_SOLEREP, BR_REPRIGHT:PROK_SOLEREP, NAT_REPRIGHT:SOLEREP	-	-
10	waivableBy	BR_REPRIGHT:JUHL_SOLEREP, BR_REPRIGHT:PROK_SOLEREP, AGENCY-Q:Mandates.manager NAT_REPRIGHT:SOLEREP	BR_REPRIGHT:JUHL_SOLEREP, BR_REPRIGHT:PROK_SOLEREP, AGENCY-Q:Mandates.manager NAT_REPRIGHT:SOLEREP	BR_REPRIGHT: JUHL_SOLEREP, BR_REPRIGHT: PROK_SOLEREP, AGENCY-Q: Mandates.manager
11	waivingMustBeSigned	FALSE	FALSE	FALSE
12	withdrawableBy	BR_REPRIGHT:JUHL_SOLEREP, BR_REPRIGHT:PROK_SOLEREP, AGENCY-Q:Mandates.manager NAT_REPRIGHT:SOLEREP	BR_REPRIGHT:JUHL_SOLEREP, BR_REPRIGHT:PROK_SOLEREP, AGENCY-Q:Mandates.manager NAT_REPRIGHT:SOLEREP	BR_REPRIGHT: JUHL_SOLEREP, BR_REPRIGHT: PROK_SOLEREP, AGENCY-Q: Mandates.manager
13	withdrawalMustBeSigned	TRUE	TRUE	TRUE

There is an additional role "AGENCY-Q:Edit" that has an equal configuration to the role "AGENCY-Q:Edit.Submit" except the title and descriptions are different:

	RoleDefinition parameter	**code: AGENCY-Q:Edit**
1a	title.en	Agency X: Data entry clerk
1b	title.et	Agentuur Q: Sisestaja
2a	description.en	Can enter reports in the name of the entrepreneur. This role can be assigned to both individuals and to legal persons (like a bookkeeping company that takes care of submitting reports). If a company is assigned this role then the company must first further sub-delegate this role to some physical person (like an employee of the bookkeeping company). If this role is given to legal person then it can be only given with the right to sub-delegate it.
2b	description.et	Saab ettevõtja nimel sisestada raporteid. Rolli võib määrata peale füüsiliste isikute ka juriidilistele isikutele (näit raamatupidamisfirma, kes ettevõtja eest raporteid esitab), kes seejärel peavad selle rolli eesti.ee-s edasi volitama mõnele füüsilisele isikule (raamatupidamisfirma töötajale). Juriidilisele isikule saab rolli anda ainult koos edasivolitamise õigusega.
	<rest of the parameters>	<rest of the parameter values equal to the configuration of role AGENCY-Q:Edit.submit"

Explanation:

- dash (-) in the table means that the value is not specified (NULL)
- BR_REPRIGHT:JUHL_SOLEREP - this means a person described as a management board member (juhatuse liige) who has sole representation right (ainuesindusõigus)
- BR_REPRIGHT:PROK_SOLEREP - this means a person described as a procurer (prokurist) who has sole representation right (ainuesindusõigus)
- NAT_REPRIGHT:SOLEREP - this means a physical person itself who has the right to represent oneself (teovõime ei ole piiratud)

2.4 What the role configuration doesn't include

It is important to note that the role definitions presented in the previous paragraph do not have any properties of what are the privileges (individual rights) that the role consists of. This information is not stored in Pääsuke and must be kept on the self-service side.

2.5 How to verify the currently valid role configuration

Pääsuke has an X-road service to query the currently valid role configuration. This is one of the ways to detect what configuration is currently in effect.

2.6 Granting mandates in eesti.ee portal (in Pääsuke UI)

Once the roles are defined in Pääsuke the users can start logging in to eesti.ee (into Pääsuke section) and start granting these mandates. This process is not described in this document in further detail. Pääsuke prototype https://paasuke.github.io/proto is a recommended tool for anyone to investigate how Pääsuke UI is going go work.

3. Use-case to query user's mandates

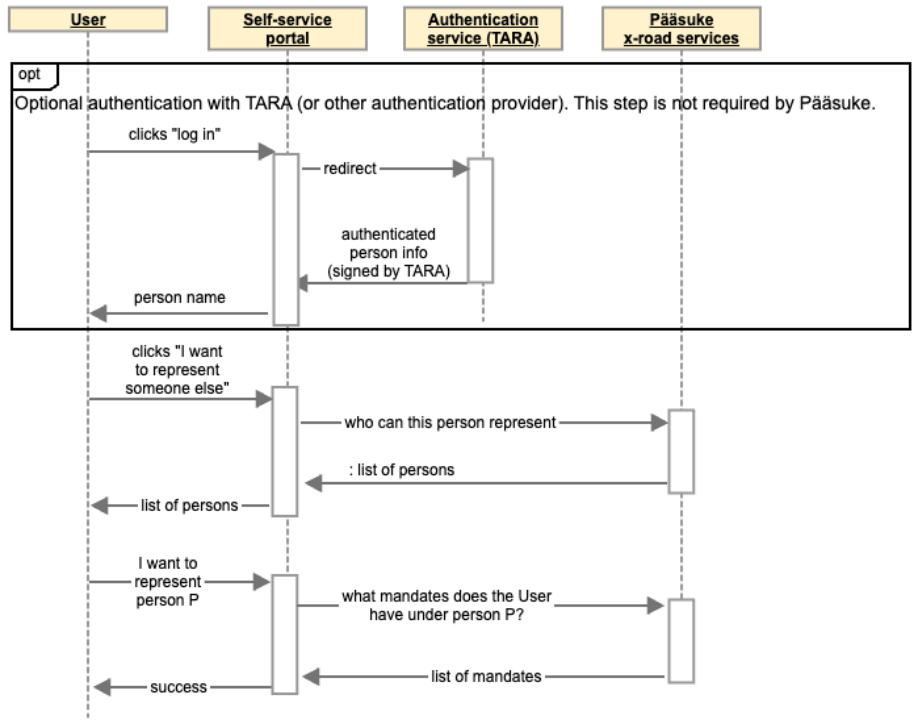
3.1 Intro to querying mandates by the self-service

Once the self-service starts to pull mandates info from Pääsuke over x-road the following steps are going to take place:

1. User authenticates with TARA
2. Self-service pulls the list of companies that the user can represent and additionally displays an option for the person to represent oneself as an individual
3. Once the person chooses the company to represent then the self-service pulls the list of mandates that the person has.

These 3 steps are illustrated by the following sequence diagram:

Oraakliliidese sequence diagramm



3.2 Query getDelegateRepresentees - "Who can this person represent"

Let's imagine that Tara returned the following parameters about the authenticated person:

```
"sub": "EE30303039816",
 "profile_attributes": {
   "date_of_birth": "1903-03-03",
   "family_name": "TUULINE",
   "given_name": "TÕNU"
 }
```

Let's look now look closer at step 2 - self-service pulls the list of companies that the user can represent and additionally displays an option for the person to represent oneself as an individual.

For this step, the self-service must pull the list of companies the user can represent.

3.2.1 getDelegateRepresenteesUsing query parameter "role"

```
curl -X 'GET' \
  'https://security-server/r1/ee-dev/GOV/70006317/volitused/oraakel/v1/delegates/EE30303039816/representees
?ns=AGENCY-Q
&role=AGENCY-Q%3AEdit
&role=AGENCY-Q%3AEdit.Submit'
```

Note that the query contains the following parts:

- the id-code of the person together with a 2-letter country code (EE30303039816)
- the value that was returned by Tara can be used directly (even if the value returned is not Estonian national identity number but belongs to some other EU country)

- the "ns" parameter that is compulsory specifies the namespace
- the "role" query parameter contains two roles: AGENCY-Q:Edit&role=AGENCY-Q:Edit.Submit (the colon will be URL encoded)
    - this means that we are interested in only persons who have given roles with the listed codes to the representee

3.2.2 Note for systems that have many roles

Systems that have a lot of roles should group such roles into separate namespaces. If Agency Q would have many roles for self-service then it would make sense to create a separate namespace for roles that give access to the self-service.

In this case, the roles that allow self-service access would be named something like AGENCY-Q-SELF-SERVICE:Edit and AGENCY-Q-SELF-SERVICE:Edit.Submit and so on.

And then it would be possible to make the previous query on a namespace level like this:

```
curl -X 'GET' \
  'https://security-server/r1/ee-dev/GOV/70006317/volitused/oraakel/v1/delegates/EE30303039816/representees
   ?ns=AGENCY-Q-SELF-SERVICE'
```

Other roles (in our case "AGENCY-Q:Mandates.manager" and "AGENCY-Q:Machine-to-machine-services") would stay in a different namespace because these don't give the right to log in to the self-service.

3.2.3 Note about parameters "ns" and "role"

The "ns" and "role" conditions are joined with AND. So if you would have the following parameters

```
?ns=AGENCY-Q
&role=AGENCY-Q-SELF-SERVICE:Edit
&role=AGENCY-Q-SELF-SERVICE:Edit.Submit
```

Then the query would return no results. You will have to include all the namespaces in "ns" (you can specify several ns values if needed).

3.2.4 Displaying the option "Who would you like to represent" to the user

In our example scenario, the self-service allows the user to represent himself as well. However, this option for the person to represent himself is not returned by Pääsuke.

This is why the self-service must add this option to the list and display it to the user:

Who would you like to represent?

- Tõnu Tuuline (EE30303039816)
- Jüri Juurikas (EE38302250123)
- Raamatupidajad OÜ (EE12345678)

3.2.5 Note about expired mandates and mandates becoming active in the future

The API-s to pull mandate information always only returns mandates that are active at the time of the request.
Expired mandates or the mandates becoming active in the future are not returned.

3.3 Query getRepresenteeDelegateMandates - "What mandates does the user have under a representee"

Let's imagine that the user chose that the person who had logged in (EE30303039816) wanted to represent Raamatupidajad OÜ (EE12345678) in the session.

Now the self-service portal needs to find out what mandates the user has under that representee.

```
curl -X 'GET' \
  'https://security-server/r1/ee-dev/GOV/70006317/volitused/oraakel/representees/EE12345678/delegates
/EE30303039816/mandates
   ?ns=AGENCY-Q
   &role=AGENCY-Q%3AEdit
   &role=AGENCY-Q%3AEdit.Submit'
```

Example result:

```
[
  {
    "role": "AGENCY-Q:Edit"
  },
  {
    "role": "AGENCY-Q:Edit.Submit"
  }
]
```

This response indicates that the person has both roles. If the user has no valid roles (or they have expired or they will become active in the future then the system returns an empty list.

4. Use-case to query company mandates

Agency Q in our example also offers x-road services. There are situations where some company is not capable of making x-road queries themselves but they are using some software as a service provider that makes queries on their behalf.

If such an x-road query arrives where some company is making a query on behalf of some customer company the Agency Q needs to check if the customer company has given a mandate.

Let's say the software as a service provider has registry code EE18765432 and they are making an x-road query where they are representing legal person EE12345678.

In order to query if EE12345678 has given the required mandate to EE18765432 the system needs to make the same query as described in Chapter 3.3 but with different input parameters

For this:

```
curl -X 'GET' \
  'https://security-server/r1/ee-dev/GOV/70006317/volitused/oraakel/representees/EE12345678/delegates/EE18765432
/mandates
   ?ns=AGENCY-Q
   &role=AGENCY-Q%3AMachine-to-machine-services'
```

Here the EE12345678 is the representee (the person who must have given a mandate) and the company making the request is the delegate (EE18765432).

If the mandate has been given then it is returned:

```
[
  {
    "role": "AGENCY-Q:Machine-to-machine-services"
  }
]
```