Introduction to Pääsuke and configuring roles

Version 0.2 (11 December 2023)

In this document, we describe the aspects that are common for both sides:

1) pulling mandates from external systems and displaying them in the central system and

2) storing mandates centrally and offering API to other systems for pulling them

1. Versions

Version	Date	Description and changes
0.1	11.12.2023	Document split from "Description of X-Road services offered to Pääsuke"
0.2	11.12.2003	delegateCanEqualToRepresentee renamed into delegateMustEqualToRepresenteeOnAdd

2. What is a role

The role is a group of privileges to be used in a self-service that can be granted to delegate by the representee. Role always belongs to a namespace.

Roles usually have descriptive code that indicates the profession that needs that role ("Andmeesitaja") or what the owner can do (like "TOLLIDEKL_ESITAMINE").

Roles in Pääsuke always start with the namespace code followed by a colon (for example: "STAT_ESTAT:Andmeesitaja", "EMTA: TOLLIDEKL_ESITAMINE").

Let's say some institution, for example, AgencyABC, wants to declare a role "Job ad editor".
This institution must first request a namespace from Pääsuke and usually, namespace reflects the name of the institution - that is "AGENCY_ABC" in our case.

Since the role code in Pääsuke must begin with namespace, the new role will be "AGENCY_ABC:Job.Ad.Editor")

Is solely the responsibility of that agency to:

- Decide what can be done by a person who has a mandate for that role
- Declare the code, title, and description of that role

Properties of a role:

- the role belongs to a namespace
  - the namespaces are assigned to agencies by Pääsuke. So an agency must agree with RIA before it can start to use a namespace.
- the role has a code (unique identifier, not shown out to end user) that is unique in that namespace
  - in Pääsuke the role codes always are prefixed with the namespace so all the roles are unique in Pääsuke
- the role must have a title in Estonian
  - it is recommended to always provide the translation of the role title in English and in Russian
- the role can have a description
  - if there is a description it must have an Estonian translation and may have translations in English, and Russian

2.1 Role code

When some object has a property "role" it refers to role code.

Role codes can contain any UTF-8 symbols (including colons and spaces although spaces are not recommended)

NB! The roles are everywhere prefixed with their namespace that is separated by a colon. When separating the namespace from a role it must be kept in mind that the role code can contain several colons.

The role code must be unique using a case-insensitive comparison.

2.2 RoleDefinition parameters

Note: all boolean parameters default to false.

Property	Man-da-tory	Type	Precondition (s)	Description
code	yes	string		*Unique identifier of the role. The prefix until the first colon is called the role namespace. Max length 4000 characters.*
title	yes	Translation (see chapter 3.7)		*Role title in different languages.*
delegateType	yes	enum [LEGAL_PERSON, NATURAL_PERSON]		*Type of persons this role can be assigned to. Setting delegateType only to LEGAL_PERSON is meant to be used for machine-to-machine roles. For example EMTA has a role "Käibedeklaratsiooni (KMD) andmete saatmine masin-masin liidese vahendusel (code XT_MM_KMD)".* See Chapter 2.2.3 for more info.
representeeIdentifierIn	no	list of strings (up to 10 identifiers are allowed)		New mandates with this role code can only be created for representees in this list. This parameter only has an effect if it is not null and not empty.
representeeType	yes	enum [NATURAL_PERSON, LEGAL_PERSON]		*Type of representees who can add a mandate with this role*
GOVERNMENT_PERSON	no	list of strings		*New mandates with this role code can only be created for representees in this list. This parameter only has an effect if it is not null and not empty*
addableBy	no	list of strings		*In order to add a mandate with this role, the user representing the representee must have a valid mandate with a role in this list. If the value is empty or null, this role cannot be assigned from Pääsuke.* **Note about natural persons** *If the role is configured so that representeeType has the value NATURAL_PERSON in it, then add "NAT_REPRIGHT: SOLEREP" to this list - this value indicates that a natural person (as a representee) is allowed to add a mandate with this role if the natural person adding the mandate has the right to represent oneself (kui volituse andja teovõime ei ole piiratud).* **Assigning a role through Admin Portal (MISP2)** Pääsuke allows adding roles through its MISP2 based admin portal (this is a different portal than eesti.ee). If a role must be addable from the admin portal then addableBy list must include the value "ADMIN_PORTAL:ADMIN_USER". Before 0.9.0 this was named assignableBy If the role is addable also depends on parameter 'addableOnlyIfRepresenteeHasRoleIn' (if it is specified)
addableOnlyIfRepresenteeHasRoleIn	no	list of strings	addableBy has at least one item	*Defining this list is used in rare cases where in order to assign the role, the representee also must have at least one mandate with a role in this list. For example to add some PRIA role the user representing the representee must have a role in the addableBy list and the representee must have the role "PRIA:PRIA.customer"* Before 0.9.0 this was named assignableOnlyIfRepresenteeHasRoleIn
addingMustBeSigned	no	boolean	addableBy has at least one item	*If this is set as true then the user adding a mandate with this role needs to digitally sign it.*
canSubDelegate	no	boolean		*If this is set as true then a mandate with this role can be added with the right to further sub-delegate it.* If this parameter is changed from true to false (which is not recommended) for a role then existing mandates and sub-delegates are left intact but it wouldn't be possible to add new sub-delegates. The delegates who have previously received this mandate with the right to sub-delegate should be notified that they cannot execute this right anymore (this notifying has to be carried out outside Pääsuke as there is no automatic process in place for this).
delegateMustEqualToRepresenteeOnAdd	no	boolean	addableBy contains at least one role that starts with "PAASUKE_ADMIN:".	*If this is set to true then in the Pääsuke Admin Portal it is possible to create mandates with this role where the value of the representee equals the value of the delegate. This functionality is used for the eesti.ee RR partner services. These types of roles where representee=delegate can only be added and deleted from the Admin portal (so in eesti.ee they are displayed as read-only).*
description	no	Translation (see chapter 3.7)		*Role description in different languages. If the description is provided it must have at least the description translation in Estonian.*
hidden	no	boolean		*Mandates with hidden roles are not shown in Pääsuke UI. A hidden role is a method to add extra information about the person. For example, we could create a role AA with property addableBy=BB, hidden=false. Now we can create hidden role BB and we can add a mandate with the role BB to persons who are allowed to add role AA. False by default. If hidden is set to true then all of the role properties are ignored.* See Chapter 2.2.3 for more info about hidden roles. If hidden is set to true then all of the following properties are ignored.
validityPeriodFromNotInFuture	no	boolean		*If true then Pääsuke UI restricts setting validityPeriod.from into the future when adding a new mandate. If adding a sub-delegate is allowed then this check is also applied when adding a sub-delegate.*
validityPeriodThroughMustBeUndefine	no	boolean		*If true then Pääsuke UI forces setting validityPeriod.through to infinity. If adding a sub-delegate is allowed then this check is also applied when adding a sub-delegate.*
subDelegateType	no	enum [LEGAL_PERSON, NATURAL_PERSON]	canSubDelegate=true	*Type of persons this role can be sub-delegated to. This should have a value if canSubDelegate is set to true and normally (except in rare corner cases) the value will be NATURAL_PERSON.*
subDelegableBy	no	list of strings	canSubDelegate=true	*In order to add a sub-delegate for a mandate with this role the user representing the delegate must have a valid mandate with a role in this list. This should have a value if canSubDelegate is set to true.*

subDelegatingMustBeSigned	no	boolean	canSubDelegate=true	*If this is set as true then the user is adding a sub-delegate for a mandate with this role then the user needs to digitally sign it.*
waivableBy	no	list of strings		*Waiving means deleting a mandate from the delegate side (volitusest loobumine).* *The user representing the delegate must have a valid mandate with a role in the list to waive this mandate from the delegate side. If this is set to null or to an empty list then this mandate cannot be waived.* **Some examples** Adding "BR_REPRIGHT:SOLEREP" to this list indicates that if a legal person is a delegate (or sub-delegate) then any person who has a sole representation right for this delegate is allowed to waive a mandate with this role. Adding "NAT_REPRIGHT:SOLEREP" to this list indicates that if a natural person is a delegate (or sub-delegate) then that person is allowed to waive a mandate with this role.
waivingMustBeSigned	no	boolean	waivableBy has at least one value	*If this is set true then the delegate has to digitally sign when the delegate (volituse saaja) wants to waive the mandate (volitusest loobumine).*
withdrawableBy	no	list of strings		*Withdrawing means deleting a mandate from the representee side (volituse tagasivõtmine).* *The user representing the representee must have a mandate with a role in the list to withdraw this mandate from the representee side.*
withdrawalMustBeSigned	no	boolean	withdrawableBy or addableBy has a value	*If this is set true then the representee (or the person representing the representee) has to digitally sign when he wants to withdraw the mandate (volituse tagasivõtmine).*

3. Configuring who can perform some action

3.1 Natural persons representing themselves

If some aciton can be performed by a natural person representing oneself then this is expressed using "NATURAL_PERSONS:SELFREP".

For example is natural person is allowed to waive a mandate that has been given to him, then the configuration must have:

```
waivableBy: [
  "NATURAL_PERSONS:SELFREP"
]
```