

## CzechIdM - Task #2234

### Authorization policies - use selected permissions only from transitive evaluator

04/29/2020 01:11 PM - Radek Tomiška

<b>Status:</b>	Closed	<b>Start date:</b>	04/29/2020
<b>Priority:</b>	Normal	<b>Due date:</b>	
<b>Assignee:</b>	Radek Tomiška	<b>% Done:</b>	100%
<b>Category:</b>	Authentication / Authorization	<b>Estimated time:</b>	0.00 hour
<b>Target version:</b>	10.3.0		
<b>Description</b>			
When transitive evaluator is configured, then all owner permissions are granted transitively. This is not required in some UC.			
Example: - i want to read and edit subordinate (identity), but i don't want to edit all its contracts.			
Add permissions support to transitive policies (AbstractTransitiveEvaluator) - configured permissions will be used for owner permissions intersection => only selected permissions will be granted by owner.			
<b>Related issues:</b>			
Related to CzechIdM - Task #2229: Identity projection - support edit more con...		<b>Closed</b>	<b>04/23/2020</b>
Related to CzechIdM - Task #1784: LRT: support multiple properties		<b>Closed</b>	<b>08/07/2019</b>
Related to CzechIdM - Task #2239: Authorization policies - prevent to configu...		<b>New</b>	<b>05/06/2020</b>

### History

#### #1 - 04/29/2020 01:11 PM - Radek Tomiška

- Related to Task #2229: Identity projection - support edit more contracts in projection added

#### #2 - 05/04/2020 11:47 AM - Radek Tomiška

- Related to Task #1784: LRT: support multiple properties added

#### #3 - 05/04/2020 12:47 PM - Radek Tomiška

- Status changed from In Progress to Needs feedback
- Assignee changed from Radek Tomiška to Vít Švanda
- % Done changed from 0 to 90

It's implemented - only selected permissions can be used from owner permissions transitively.  
I've added new abstract transitive evaluator property (include-permissions), but is needed to override and implement this new feature by each evaluator (getPredicate method has to be changed and new configuration form attribute has to be used) - new behavior is implemented in IdentityContractByIdentityEvaluator only for now.

Commit:

<https://github.com/bcvsolutions/CzechIdMng/commit/c12ba746ded7759df8719b1f380fd6a6c6825b41>

Doc:

<https://wiki.czechidm.com/devel/documentation/security/dev/authorization#abstracttransitiveevaluator>  
[https://wiki.czechidm.com/devel/documentation/security/dev/authorization#manager\\_and\\_subordinates](https://wiki.czechidm.com/devel/documentation/security/dev/authorization#manager_and_subordinates)

Could you provide me a feedback, please?

#### #4 - 05/06/2020 11:16 AM - Vít Švanda

- Status changed from Needs feedback to Resolved
- Assignee changed from Vít Švanda to Radek Tomiška
- % Done changed from 90 to 100

I did review and tested it. Works nice. Thanks for this feature.

I had one obstacle. By my mistake I configured permissions in combination IdentityContractByIdentityEvaluator and IdentityByContractEvaluator. This caused over looping. I know, this combination is totally wrong, but some validation could be created in future for this.

**#5 - 05/06/2020 12:07 PM - Radek Tomiška**

I think so, created [#2239](#) - hard validation in product will be better then doc.

**#6 - 05/06/2020 12:08 PM - Radek Tomiška**

- *Related to Task #2239: Authorization policies - prevent to configure IdentityContractByIdentityEvaluator and IdentityByContractEvaluator simultaneously added*

**#7 - 05/15/2020 01:36 PM - Radek Tomiška**

- *Status changed from Resolved to Closed*