Security Requirements Document

Taslab

STS-Tool team

Nov 10, 2014

This document has been generated by STS-Tool
http://www.sts-tool.eu

Table of Contents:

Introduction

This document describes the security requirements for the Taslab project. It provides a detailed description of the socio-technical security requirements models from different views (*Social*, *Information*, *Authorization*) and then presents the list of *security requirements* derived from them.

The *Social view* represents stakeholders as intentional and social entities, representing their goals and important information in terms of documents, together with their interactions with other actors to achieve these goals and to exchange information. Stakeholders express constraints over their interactions in terms of *security needs.* The *Information view* represents the informational content of stakeholders' documents, showing how information and documents are interconnected, as well as how they are composed respectively. The *Authorization view* represents which stakeholders own what information, and captures the flow of permissions or prohibitions from one stakeholder to another. The modelling of authorizations expresses other *security needs* related to the way information is to be manipulated.

The document ends with the list of *security requirements* for the system to be expressed in terms of *social commitments*, namely promises with contractual validity stakeholders make to one another. The security requirements are derived automatically once the modelling is done and the designer has expressed the security needs. Whenever a security need is expressed over an interaction from one stakeholder to the other, a commitment on the opposite direction is expected from the second stakeholder to satisfy the security need.

Social View

The social view shows the involved stakeholders, which are represented as *roles* and *agents*. Agents refer to actual participants (stakeholders) known when modelling the Taslab project, whereas roles are a generalisation (abstraction) of agents. To capture the connection between roles and agents, the *play* relation is used to express the fact that certain agents play certain roles.

Stakeholders have goals to achieve and they make use of different information to achieve these goals. They interact with one another mainly by *delegating goals* and *exchanging information*. Information is represented by means of documents, which actors manipulate to achieve their goals.

Social View Diagram

Figure 1 presents the graphical representation of the social view (a larger picture is shown in appendix A).

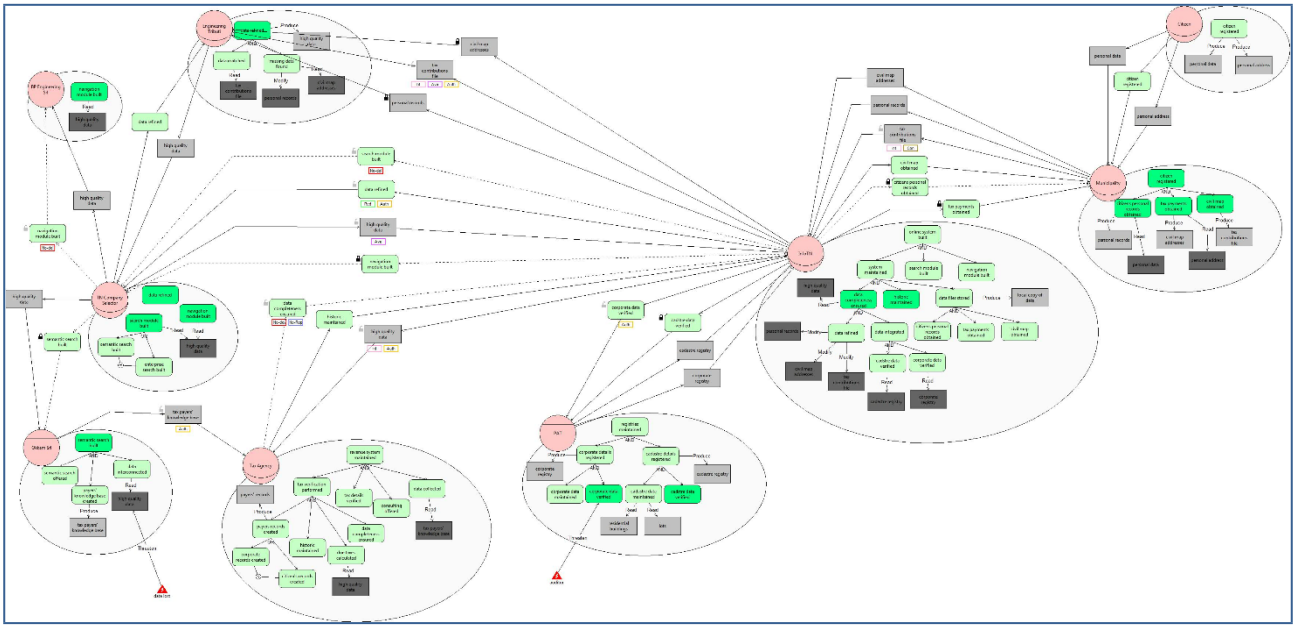

Figure 1 - Social View for the Taslab project

Stakeholders

This section describes the stakeholders identified in the Taslab project. Stakeholders are represented as roles or agents.

In particular, identified roles are: *Tax Agency*, *Engineering Tributi*, *InfoTN*, *TN Company Selector*, *Citizen* and *Municipality* (Figure 1), while identified agents are: *PAT*, *Okkam Srl* and *BP Engineering Srl* (Figure 1). Table 1 and Table 2 summarise the stakeholders.

Role	Description	Mission	Purpose
Tax Agency			
Engineering Tributi			
InfoTN			
TN Company Selector			
Citizen			
Municipality			

Table 1 - Roles in the Taslab project.

Agent	Description	Abilities	Important Features	Certifications Accreditations	Type Of Organisation
PAT					
Okkam Srl					
BP Engineering Srl					

Table 2 - Agents in the Taslab project

In the Taslab project there are no plays relationships taking place for the given agents/roles.

Stakeholders' documents

Stakeholders have documents they possess or exchange with others to achieve their goals. Documents are represented within the rationale of the role/agent (Figure 1).

In the Taslab project (Figure 1) we have:

- **Tax Agency** has document *payers' records*. Moreover it has document *tax payers' knowledge base* provided by *Okkam Srl* and document *high quality data* provided by *InfoTN*.
- **Engineering Tributi** has document *high quality data*. Moreover it has document *civil map addresses* provided by *InfoTN*, document *tax contributions file* provided by *InfoTN* and document *personal records* provided by *InfoTN*.
- **InfoTN** has document *local copy of data*. Moreover it has document *civil map addresses* provided by *Municipality*, document *tax contributions file* provided by *Municipality*, document *corporate registry* provided by *PAT*, document *cadastre registry* provided by *PAT*, document *personal*

records provided by *Municipality* and document *high quality data* provided by *TN Company Selector*.

- **TN Company Selector** has document *high quality data* provided by *Engineering Tributi*.
- **Citizen** has documents *personal data* and *personal address*.
- **Municipality** has documents *personal records*, *civil map addresses* and *tax contributions file*. Moreover it has document *personal address* provided by *Citizen* and document *personal data* provided by *Citizen*.
- **PAT** has documents *corporate registry*, *cadastre registry*, *residential buildings* and *lots*.
- **Okkam Srl** has document *tax payers' knowledge base*. Moreover it has document *high quality data* provided by *TN Company Selector*.
- **BP Engineering Srl** has document *high quality data* provided by *TN Company Selector*.

Table 3 summarises stakeholders' *documents* for the Taslab project.

Agent/Role	Document	Description
Tax Agency	payers' records	
	high quality data	
	tax payers' knowledge base	
Engineering Tributi	high quality data	
	personal records	
	civil map addresses	
	tax contributions file	
InfoTN	high quality data	
	local copy of data	
	personal records	
	civil map addresses	
	tax contributions file	
	corporate registry	
	cadastre registry	
TN Company Selector	high quality data	
Citizen	personal data	
	personal address	
Municipality	personal records	
	personal data	
	civil map addresses	
	personal address	
	tax contributions file	
PAT	corporate registry	
	cadastre registry	
	residential buildings	

	lots
Okkam Srl	high quality data
	tax payers' knowledge base
BP Engineering Srl	high quality data

Table 3 - Stakeholders' documents in the Taslab project

Stakeholders' documents and goals

Stakeholders' documents are linked to their goals: they read (make) documents to achieve their goals, they modify documents while achieving their goals, and they may produce documents from achieving their goals.

In the Taslab project (Figure 1) stakeholders' documents and goals are related as follows:

- **Tax Agency** *produces* document *payers' records* to achieve goal *payers records created*, *reads* document *tax payers' knowledge base* to achieve goal *data collected* and *reads* document *high quality data* to achieve goal *due taxes calculated*.
- **Engineering Tributi** *reads* document *tax contributions file* to achieve goal *data matched*, *produces* document *high quality data* to achieve goal *data refined* and *reads* document *civil map addresses* and *modifies* document *personal records* to achieve goal *missing data found*.
- **InfoTN** *reads* document *cadastre registry* to achieve goal *cadstre data verified*, *reads* document *corporate registry* to achieve goal *corporate data verified*, *produces* document *local copy of data* to achieve goal *data files stored*, *reads* document *high quality data* to achieve goal *data completeness ensured* and *modifies* document *personal records*, *modifies* document *civil map addresses* and *modifies* document *tax contributions file* to achieve goal *data refined*.
- **TN Company Selector** *reads* document *high quality data* to achieve goal *search module built* and *reads* document *high quality data* to achieve goal *navigation module built*.
- **Citizen** *produces* document *personal data* and *produces* document *personal address* to achieve goal *citizen registered*.
- **Municipality** *reads* document *personal address* and *produces* document *civil map addresses* to achieve goal *tax payments obtained*, *produces* document *tax contributions file* to achieve goal *civil map obtained* and *reads* document *personal data* and *produces* document *personal records* to achieve goal *citizens personal records obtained*.
- **PAT** *produces* document *corporate registry* to achieve goal *corporate details registered*, *reads* document *residential buildings* and *reads* document *lots* to achieve goal *cadastre data maintained* and *produces* document *cadastre registry* to achieve goal *cadastre details registered*.
- **Okkam Srl** *produces* document *tax payers' knowledge base* to achieve goal *payers' knowledge base created* and *reads* document *high quality data* to achieve goal *data interconnected*.
- **BP Engineering Srl** *reads* document *high quality data* to achieve goal *navigation module built*.

Table 4 summarises goal-document relations for all stakeholders in the Taslab project.

Agent/Role	Goal	Document	Relation

Tax Agency	payers records created	payers' records	Produce
	data collected	tax payers' knowledge base	read
	due taxes calculated	high quality data	read
Engineering Tributi	data matched	tax contributions file	read
	data refined	high quality data	Produce
	missing data found	civil map addresses	read
		personal records	Modify
InfoTN	cadstre data verified	cadastre registry	read
	corporate data verified	corporate registry	read
	data files stored	local copy of data	Produce
	data completeness ensured	high quality data	read
	data refined	personal records	Modify
		civil map addresses	Modify
		tax contributions file	Modify
TN Company Selector	search module built	high quality data	read
	navigation module built	high quality data	read
Citizen	citizen registered	personal data	Produce
		personal address	Produce
Municipality	tax payments obtained	personal address	read
		civil map addresses	Produce
	civil map obtained	tax contributions file	Produce
	citizens personal records obtained	personal data	read
		personal records	Produce
PAT	corporate details registered	corporate registry	Produce
	cadastre data maintained	residential buildings	read
		lots	read
	cadastre details registered	cadastre registry	Produce
Okkam Srl	payers' knowledge base created	tax payers' knowledge base	Produce
	data interconnected	high quality data	read
BP Engineering Srl	navigation module built	high quality data	read

Table 4 - Relation of stakeholders' documents to their goals

Goal Refinement

Stakeholders have goals to achieve. Goals are represented within the rationale (round compartment attached to the role/agent, see Figure 1) of the role/agent representing the stakeholder. They achieve

their goals by further refining them into finer-grained goals (subgoals) by means of AND/OR-decompositions. AND-decompositions structurally refine a goal into multiple subgoals (all AND subgoals need to be achieved for the goal to be achieved), while OR-decompositions represent alternative ways for achieving a goal (at least one of the subgoals in the OR-decomposition needs to be achieved for the goal to be achieved).

In the Taslab project (Figure 1) we have:

- **Tax Agency** has to achieve goal *revenue system maintained*. To achieve *revenue system maintained*, Tax Agency should achieve goal *tax verification performed*, goal *data collected*, goal *tax details verified* and goal *consulting offered* To achieve *tax verification performed*, Tax Agency should achieve goal *payers records created*, goal *historic maintained*, goal *due taxes calculated* and goal *data completeness ensured* To achieve *payers records created*, Tax Agency should achieve either goal *corporate records created* or goal *citizen's records created*
- **Engineering Tributi** has to achieve goal *data refined*. To achieve *data refined*, Engineering Tributi should achieve goal *data matched* and goal *missing data found*
- **InfoTN** has to achieve goal *online system built*. To achieve *online system built*, InfoTN should achieve goal *system maintained*, goal *search module built* and goal *navigation module built* To achieve *system maintained*, InfoTN should achieve goal *data completeness ensured*, goal *data files stored* and goal *historic maintained* To achieve *data files stored*, InfoTN should achieve goal *citizens personal records obtained*, goal *tax payments obtained* and goal *civil map obtained* To achieve *data completeness ensured*, InfoTN should achieve goal *data refined* and goal *data integrated* To achieve *data integrated*, InfoTN should achieve goal *cadstre data verified* and goal *corporate data verified*
- **TN Company Selector** has to achieve goal *data refined*, goal *search module built* and goal *navigation module built*. To achieve *search module built*, TN Company Selector should achieve either goal *semantic search built* or goal *enterprise search built*
- **Citizen** has to achieve goal *citizen registered*.
- **Municipality** has to achieve goal *citizen registered*. To achieve *citizen registered*, Municipality should achieve goal *citizens personal records obtained*, goal *tax payments obtained* and goal *civil map obtained*
- **PAT** has to achieve goal *registries maintained*. To achieve *registries maintained*, PAT should achieve goal *corporate details registered* and goal *cadastre details registered* To achieve *corporate details registered*, PAT should achieve goal *corporate data maintained* and goal *corporate data verified* To achieve *cadastre details registered*, PAT should achieve goal *cadastre data maintained* and goal *cadstre data verified*
- **Okkam Srl** has to achieve goal *semantic search built*. To achieve *semantic search built*, Okkam Srl should achieve goal *semantic search offered*, goal *payers' knowledge base created* and goal *data interconnected*
- **BP Engineering Srl** has to achieve goal *navigation module built*.

Table 5 summarises the goals of each agent/role in the Taslab project and how they are decomposed, when applicable.

Agent/Role	Goal	Dec. Type	Subgoals

Tax Agency	revenue system maintained	AND	tax verification performed
			data collected
			tax details verified
			consulting offered
Engineering Tributi	data refined	AND	data matched
			missing data found
InfoTN	online system built	AND	system maintained
			search module built
			navigation module built
TN Company Selector	data refined	-	
	search module built	OR	semantic search built
			enterprise search built
	navigation module built	-	
Citizen	citizen registered	-	
Municipality	citizen registered	AND	citizens personal records obtained
			tax payments obtained
			civil map obtained
PAT	registries maintained	AND	corporate details registered
			cadastre details registered
Okkam Srl	semantic search built	AND	semantic search offered
			payers' knowledge base created
			data interconnected
BP Engineering Srl	navigation module built	-	

Table 5 - Goal Decompositions

Goal Contributions

Goals can contribute one to another. A contribution identifies the impact the fulfilment of one goal has on the fulfilment of another goal. This impact can be either positive or negative, and is represented with "++" and "--" respectively. Positive contribution means that the achievement of a goal also achieves the other goal. Negative contribution means that the achievement of a goal inhibits the achievement of another goal.

In the Taslab project there are no contribution relations taking place for the given agents/roles.

Stakeholders Interactions

This section describes stakeholders' interactions, providing insights on whom they interact with to fulfil their desired objectives, as well as which are the stakeholders that rely on them to fulfil their respective goals. This kind of interaction is carried out by means of *goal delegations*.

To achieve their goals stakeholders might need specific information. If they do not possess this information, they may ask other stakeholders to provide them documents. *Document transmission* is used to capture this interaction.

Goal Delegations

Stakeholders interact with others to achieve some of their goals by means of goal delegations. Goal delegations are graphically represented as a relation that starts from a delegator actor to a delegatee actor (following the direction of the arrow), having a rounded corner rectangle representing the goal being delegated. Security needs are graphically specified as labels that appear below the delegated goal (Figure 1).

The following description enlists all the delegations from one role/agent to the others. When applicable, security needs expressed over the delegations are enumerated.

In the Taslab project (Figure 1), we have the following goal delegations:

- **Tax Agency** delegates goal *historic maintained* to **InfoTN**.
- **Tax Agency** delegates goal *data completeness ensured* to **InfoTN**.

  The following security needs apply to this delegation:

  No-Delegation and Non Repudiation: acceptance.
- **InfoTN** delegates goal *data refined* to **TN Company Selector**.

  The following security needs apply to this delegation:

  Redundancy: true-multi-actor and Authentication: delegatee.
- **InfoTN** delegates goal *citizens personal records obtained* to **Municipality**.

  The following security needs apply to this delegation:

  No-Delegation and Non Repudiation: delegation-acceptance.
- **InfoTN** delegates goal *tax payments obtained* to **Municipality**.

  The following security needs apply to this delegation:

  Non Repudiation: acceptance and Availability: 95.
- **InfoTN** delegates goal *civil map obtained* to **Municipality**.
- **InfoTN** delegates goal *cadstre data verified* to **PAT**.

  The following security needs apply to this delegation:

  Authentication: delegatee.
- **InfoTN** delegates goal *corporate data verified* to **PAT**.

  The following security needs apply to this delegation:

Authentication: delegator.

- **InfoTN** delegates goal *search module built* to **TN Company Selector**.

  The following security needs apply to this delegation:

  No-Delegation.

- **InfoTN** delegates goal *navigation module built* to **TN Company Selector**.

  The following security needs apply to this delegation:

  Redundancy: true-multi-actor and No-Delegation.

- **TN Company Selector** delegates goal *data refined* to **Engineering Tributi**.
- **TN Company Selector** delegates goal *semantic search built* to **Okkam Srl**.

  The following security needs apply to this delegation:

  No-Delegation.

- **TN Company Selector** delegates goal *navigation module built* to **BP Engineering Srl**.

  The following security needs apply to this delegation:

  No-Delegation.

- **Citizen** delegates goal *citizen registered* to **Municipality**.

Table 6 summarises *goal delegations*, together with the eventual *security needs* when applicable, and eventual description respectively.

Delegator	Goal	Delegatee	Security Needs	Delegation Description
Tax Agency	historic maintained	InfoTN		
	data completeness ensured	InfoTN	**No-Delegation** **Non Repudiation**: *acceptance*	
InfoTN	data refined	TN Company Selector	**Redundancy**: *true-multi-actor* **Authentication**: *delegatee*	
	citizens personal records obtained	Municipality	**No-Delegation** **Non Repudiation**: *delegation-acceptance*	
	tax payments obtained	Municipality	**Non Repudiation**: *acceptance* **Availability**: *95*	
	civil map obtained	Municipality		
	cadstre data verified	PAT	**Authentication**: *delegatee*	
	corporate data verified	PAT	**Authentication**: *delegator*	
	search module built	TN Company Selector	**No-Delegation**	
	navigation module	TN Company	**Redundancy**: *true-multi-actor*	

	built	Selector	**No-Delegation**
TN Company Selector	data refined	Engineering Tributi	
	semantic search built	Okkam Srl	**No-Delegation**
	navigation module built	BP Engineering Srl	**No-Delegation**
Citizen	citizen registered	Municipality	

Table 6 - Goal Delegations and Security Needs

Document Transmission

Stakeholders exchange information by means of documents with other stakeholders. The following description enlists all the transmission from one role/agent representing the stakeholder, to other roles/agents. *Document transmission* is represented as an arrow from the transmitter to the receiver, with a rectangle representing the document. The security needs expressed over the transmission are described, if applicable. Security needs are specified with the help of labels that appear below the document being transmitted.

In the Taslab project (Figure 1), we have the following *document transmissions*:

- **Engineering Tributi** transmit document *high quality data* to **TN Company Selector**.
- **InfoTN** transmit document *high quality data* to **Tax Agency**.

  The following security needs apply to this transmission:

  Integrity: sender and Authentication: receiver.
- **InfoTN** transmit document *personal records* to **Engineering Tributi**.

  The following security needs apply to this transmission:

  Integrity: sender.
- **InfoTN** transmit document *civil map addresses* to **Engineering Tributi**.

  The following security needs apply to this transmission:

  Integrity: sender.
- **InfoTN** transmit document *tax contributions file* to **Engineering Tributi**.

  The following security needs apply to this transmission:

  Integrity: sender, Availability: 90 and Authentication: receiver.
- **TN Company Selector** transmit document *high quality data* to **InfoTN**.

  The following security needs apply to this transmission:

  Availability: 98.
- **TN Company Selector** transmit document *high quality data* to **Okkam Srl**.
- **TN Company Selector** transmit document *high quality data* to **BP Engineering Srl**.
- **Citizen** transmit document *personal data* to **Municipality**.

- **Citizen** transmit document *personal address* to **Municipality**.
- **Municipality** transmit document *personal records* to **InfoTN**.
- **Municipality** transmit document *civil map addresses* to **InfoTN**.
- **Municipality** transmit document *tax contributions file* to **InfoTN**.

  The following security needs apply to this transmission:

  Integrity: receiver and Confidentiality: receiver.
- **PAT** transmit document *corporate registry* to **InfoTN**.
- **PAT** transmit document *cadastre registry* to **InfoTN**.
- **Okkam Srl** transmit document *tax payers' knowledge base* to **Tax Agency**.

  The following security needs apply to this transmission:

  Authentication: receiver.

Table 7 summarises the *document transmissions* for the Taslab project.

Transmitter	Document	Recivier	Security Needs	Transmission Descr.
Engineering Tributi	high quality data	TN Company Selector		
InfoTN	high quality data	Tax Agency	**Integrity**: *sender* **Authentication**: *receiver*	
	personal records	Engineering Tributi	**Integrity**: *sender*	
	civil map addresses	Engineering Tributi	**Integrity**: *sender*	
	tax contributions file	Engineering Tributi	**Integrity**: *sender* **Availability**: *90* **Authentication**: *receiver*	
TN Company Selector	high quality data	InfoTN	**Availability**: *98*	
	high quality data	Okkam Srl		
	high quality data	BP Engineering Srl		
Citizen	personal data	Municipality		
	personal address	Municipality		
Municipality	personal records	InfoTN		
	civil map addresses	InfoTN		
	tax contributions file	InfoTN	**Integrity**: *receiver* **Confidentiality**: *receiver*	
PAT	corporate registry	InfoTN		
	cadastre registry	InfoTN		
Okkam Srl	tax payers' knowledge base	Tax Agency	**Authentication**: *receiver*	

Table 7 - Document Transmissions and Security Needs

Organisational Constraints

Apart from the security needs actors specify over their interactions, there are others, which are dictated either by the organisation, business rules and regulations, or law. In this section we enlist these constraints, together with the security requirements derived from them. Currently, the language supports these organisational constraints: *Separation of Duties (SoD)* and *Binding of Duties (BoD)*. Graphically we represent these constraints using a similar notation to that used in workflows, as a circle with the *unequal* sign within and as a circle with the *equals* sign within, respectively. The relations are symmetric, and as such they do not have any arrows pointed to the concepts they relate (being these roles or goals).

In the Taslab project (Figure 1) the following organisational constraints have been specified:

- **corporate records created** is incompatible with **citizen's records created**, given that *SoD* constraint is specified between these goals.
- **citizen's records created** is incompatible with **corporate records created**, given that *SoD* constraint is specified between these goals.
- **enterprise search built** should be combined with **semantic search built**, given that *BoD* constraint is specified between these goals.
- **semantic search built** should be combined with **enterprise search built**, given that *BoD* constraint is specified between these goals.

Table 8 summarises the organisational constraints for the Taslab project.

Organisational Constraint	Role/Goal	Role/Goal	Description
SoD (Goal - Goal)	corporate records created	citizen's records created	
	citizen's records created	corporate records created	
BoD (Goal - Goal)	enterprise search built	semantic search built	
	semantic search built	enterprise search built	

Table 8 - Organisational Constraints

Events

Table 9 represents all the events modeled in the project Taslab together with the set of elements each event threatens. Additionally, for each reported event a textual description is provided.

Event name	Threatened elements	Description
auditor sick	GoalReference: corporate data verified	
data lost	DocumentReference: high quality data	

Table 9 - Events

Information View

The information view gives a structured representation of the information and documents in the Taslab project. It shows what is the informational content of the documents represented in the social view. Information is represented by one or more documents (*tangible by*), and the same document can make tangible multiple information entities. Moreover, the information view considers composite documents (information) capturing these by means of *part of* relations.

Information View Diagram

Figure 2 presents the graphical representation of the information view (a larger picture is shown in appendix A).

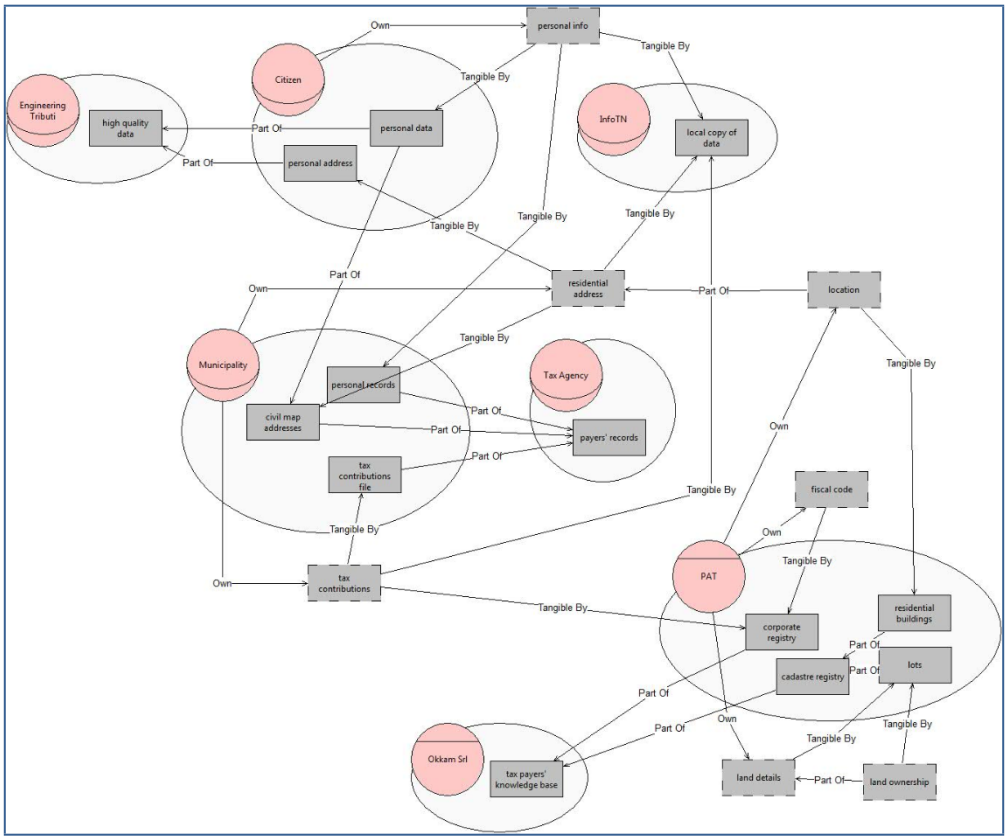

Figure 2 - Information View for the Taslab project

Modelling Ownership

The information view represents also who are the *owners* of the information that is being manipulated through the documents that represent them in the social view.

The owners for the different information in the Taslab project are summarised in Table 10.

Agent/Role	Information	Description
Citizen	personal info	
Municipality	residential address	
	tax contributions	
PAT	fiscal code	
	land details	
	location	

Table 10 - Information owners

Representation of Information

Information is represented (*made tangible by*) by documents, which stakeholders have and exchange.

The documents stakeholders in the Taslab project (Figure 2) have and exchange with one another contain the information as summarised in Table 11:

Information	Document	Description
residential address	personal address	
	local copy of data	
	civil map addresses	
land details	lots	
fiscal code	corporate registry	
location	residential buildings	
personal info	personal data	
	local copy of data	
	personal records	
tax contributions	local copy of data	
	tax contributions file	
	corporate registry	

Table 11 - Representation of Information through Documents

Structure of Information and Documents

Documents (information) are composed of other documents (information). Composition of documents (information) is captured through *part of* relations. This gives us an idea of how information and/or documents in the Taslab project are structured.

Table 12 and Table 13 summarises the information and documents in the Taslab project (Figure 2), showing how they are composed and describing the composition.

Information	Composition	Description
residential address	location	
land details	land ownership	

Table 12 - Information composition

Document	Composition	Description
cadastre registry	residential buildings	
	lots	
tax payers' knowledge base	cadastre registry	
	corporate registry	
high quality data	personal address	
	personal data	
civil map addresses	personal data	
payers' records	civil map addresses	
	personal records	
	tax contributions file	

Table 13 - Documents composition

Authorization View

The authorization view shows the permissions or prohibitions flow from a stakeholder to another, that is, the authorizations stakeholders grant or deny to others about information, specifying the operations the others can and must perform over the information. Apart from granting authority on performing operations, a higher authority can be granted, that of further authorising other actors (i.e. authorization transferability)

Authorizations start from the information owner. Therefore, in the authorization view, ownership is preserved and inherited from the information view.

Authorization View Diagram

Figure 3 presents the graphical representation of the Authorization view (a larger picture is rappresented in appendix A).

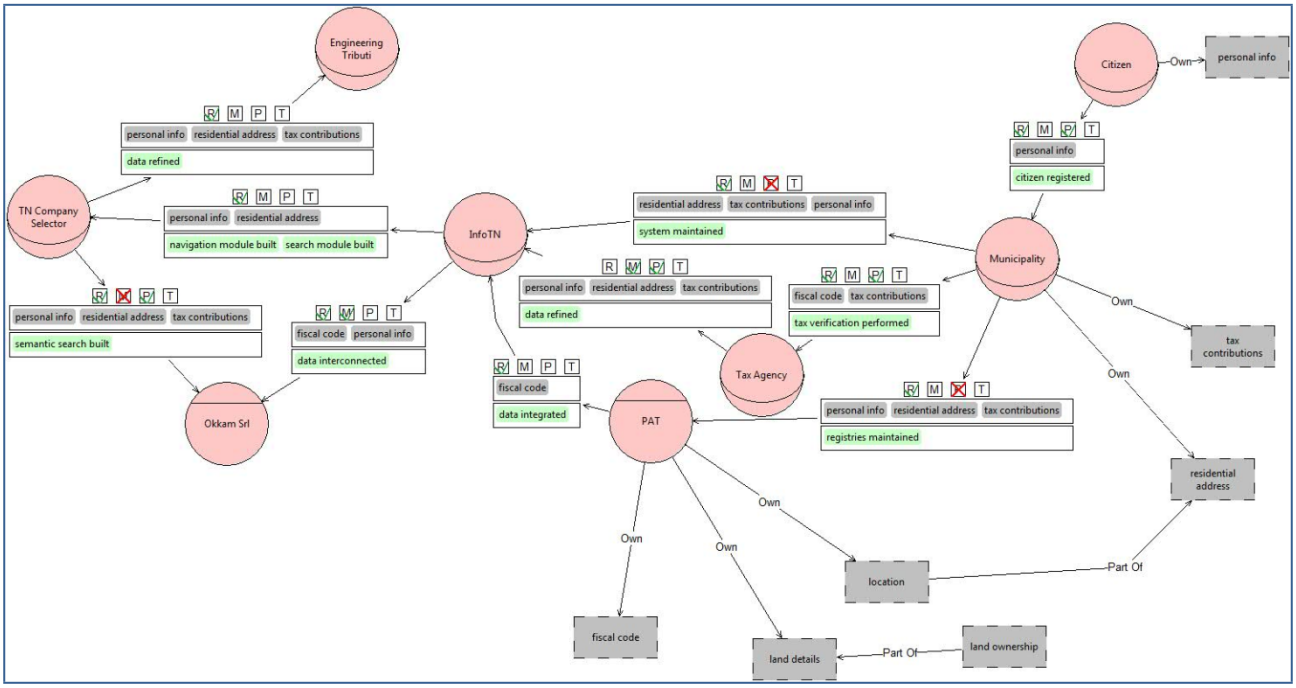

Figure 3 - Authorization View for the Taslab project

Authorization Flow

In this section are described for each role/agent, the authorizations it passes to others and what authorizations it receives from other roles/agents.In the Taslab project (Figure 3) the authorizations for each role/agent are:

- *Role* **Tax Agency**:
  - **Tax Agency** authorises *InfoTN* to *modify* and *produce* information *personal info*, *residential address* and *tax contributions*, in the scope of goal *data refined*, *passing* the right to further authorising other actors.
  - **Tax Agency** is authorised by *Tax Agency* to *read* and *produce* information *fiscal code* and *tax contributions*, in the scope of goal *tax verification performed*, *having* the right to further authorising other actors.
- *Role* **Engineering Tributi**:
  - **Engineering Tributi** is authorised by *Engineering Tributi* to *read* information *personal info*, *residential address* and *tax contributions*, in the scope of goal *data refined*, *having* the right to further authorising other actors.
- *Role* **InfoTN**:
  - **InfoTN** authorises *Okkam Srl* to *read* and *modify* information *fiscal code* and *personal info*, in the scope of goal *data interconnected*, *passing* the right to further authorising other actors, and authorises *TN Company Selector* to *read* information *personal info* and *residential address*, in the scope of goals *navigation module built* and *search module built*, *passing* the right to further authorising other actors.
  - **InfoTN** is authorised by *InfoTN* to *modify* and *produce* information *personal info*, *residential address* and *tax contributions*, in the scope of goal *data refined*, *having* the right to further authorising other actors, and is authorised by *InfoTN* to *read* and prohibited to *produce* information *residential address*, *tax contributions* and *personal info*, in the scope of goal *system maintained*, *having* the right to further authorising other actors, and is authorised by *InfoTN* to *read* information *fiscal code*, in the scope of goal *data integrated*, *having* the right to further authorising other actors.
- *Role* **TN Company Selector**:
  - **TN Company Selector** authorises *Okkam Srl* to *read* and *produce* and prohibits to *modify* information *personal info*, *residential address* and *tax contributions*, in the scope of goal *semantic search built*, *passing* the right to further authorising other actors, and authorises *Engineering Tributi* to *read* information *personal info*, *residential address* and *tax contributions*, in the scope of goal *data refined*, *passing* the right to further authorising other actorss.
  - **TN Company Selector** is authorised by *TN Company Selector* to *read* information *personal info* and *residential address*, in the scope of goal *navigation module built* and *search module built*, *having* the right to further authorising other actors.
- *Role* **Citizen**:

- **Citizen** authorises *Municipality* to *read* and *produce* information *personal info*, in the scope of goal *citizen registered*, *passing* the right to further authorising other actors.

- *Role* **Municipality**:
  - **Municipality** authorises *PAT* to *read* and prohibits to *produce* information *personal info*, *residential address* and *tax contributions*, in the scope of goal *registries maintained*, *passing* the right to further authorising other actors, and authorises *Tax Agency* to *read* and *produce* information *fiscal code* and *tax contributions*, in the scope of goal *tax verification performed*, *passing* the right to further authorising other actors, and authorises *InfoTN* to *read* and prohibits to *produce* information *residential address*, *tax contributions* and *personal info*, in the scope of goal *system maintained*, *passing* the right to further authorising other actors.
  - **Municipality** is authorised by *Municipality* to *read* and *produce* information *personal info*, in the scope of goal *citizen registered*, *having* the right to further authorising other actors.
- *Agent* **PAT**:
  - **PAT** authorises *InfoTN* to *read* information *fiscal code*, in the scope of goal *data integrated*, *passing* the right to further authorising other actors.
  - **PAT** is authorised by *PAT* to *read* and prohibited to *produce* information *personal info*, *residential address* and *tax contributions*, in the scope of goal *registries maintained*, *having* the right to further authorising other actors.
- *Agent* **Okkam Srl**:
  - **Okkam Srl** is authorised by *Okkam Srl* to *read* and *modify* information *fiscal code* and *personal info*, in the scope of goal *data interconnected*, *having* the right to further authorising other actors, and is authorised by *Okkam Srl* to *read* and *produce* and prohibited to *modify* information *personal info*, *residential address* and *tax contributions*, in the scope of goal *semantic search built*, *having* the right to further authorising other actors.

Security Requirements

This section provides the list of security requirements derived for the Taslab project.

The list of security requirements shows the roles/agents that are *responsible* to satisfy them, so that stakeholders know what they have to bring about in order to satisfy the corresponding security needs. Security requirements also include the authorizations granted by stakeholders to other stakeholders.

Security needs are expressed mainly over goal delegations, document provisions and authorizations. Therefore, the list of security requirements is derived from every type of security need. Moreover, the organisational constraints specify further *needs* over roles and goal, leading to the generation of other security requirements.

Finally, the *requester* actors are represented to capture the actors requiring certain security needs to be brought about.

The security requirements for the Taslab project (Table 14) are:

- **Tax Agency** requires *InfoTN no-delegation* on goal *data completeness ensured* and *non-repudiation-of-acceptance* of the delegation of goal *data completeness ensured*, when delegating *data completeness ensured* to *InfoTN*.
- **InfoTN** requires *TN Company Selector multi-actor-true-redundancy* (true_rm) and *delegatee-authentcation* , when delegating *data refined* to *TN Company Selector*; while it requires *Municipality no-delegation* on goal *citizens personal records obtained* and *non-repudiation-of-acceptance* of the delegation of goal *citizens personal records obtained*, when delegating *citizens personal records obtained* to *Municipality*; while it is required by *Municipality non-repudiation-of-delegation* of the delegation of goal *citizens personal records obtained*when delegating *citizens personal records obtained* to *Municipality*; while it requires *Municipality non-repudiation-of-acceptance* of the delegation of goal *tax payments obtained* and an *availability* level of 95%, when delegating *tax payments obtained* to *Municipality*; while it requires *PAT delegatee-authentcation* , when delegating *cadstre data verified* to *PAT*; while it is required by *PAT delegator-authentcation* when delegating *corporate data verified* to *PAT*; while it requires *TN Company Selector no-delegation* on goal *search module built*, when delegating *search module built* to *TN Company Selector*; while it requires *TN Company Selector multi-actor-true-redundancy* (true_rm) and *no-delegation* on goal *navigation module built*, when delegating *navigation module built* to *TN Company Selector*.
- **InfoTN** requires *Tax Agency* a *receiver-authentcation* , when transmitting *high quality data* to *Tax Agency*; while it is required by *Tax Agency* a *sender-integrity* when transmitting *high quality data* to *Tax Agency*is required by *Engineering Tributi* a *sender-integrity* when transmitting *personal records* to *Engineering Tributi*is required by *Engineering Tributi* a *sender-integrity* when transmitting *civil map addresses* to *Engineering Tributi*requires *Engineering Tributi* an *availability* level of 90% and a *receiver-authentcation* , when transmitting *tax contributions file* to *Engineering Tributi*; while it is required by *Engineering Tributi* a *sender-integrity* when transmitting *tax contributions file* to *Engineering Tributi*.
- **TN Company Selector** requires *Okkam Srl no-delegation* on goal *semantic search built*, when delegating *semantic search built* to *Okkam Srl*; while it requires *BP Engineering Srl no-delegation* on goal *navigation module built*, when delegating *navigation module built* to *BP Engineering Srl*.

- **TN Company Selector** requires *InfoTN* an *availability* level of 98%, when transmitting *high quality data* to *InfoTN*.
- **TN Company Selector** requires *Okkam Srl* the *non-modification* of information *personal info*, *residential address* and *tax contributions*, and *need-to-know* of these pieces of informations for the goal *semantic search built*, when authorising *Okkam Srl* to *read* and *produce personal info*, *residential address* and *tax contributions* in the scope of goal *semantic search built*.
- **Municipality** requires *InfoTN* a *receiver-integrity* and a *receiver-confidentiality* , when transmitting *tax contributions file* to *InfoTN*.
- **Municipality** requires *PAT* the *non-production* of information *personal info*, *residential address* and *tax contributions*, and *need-to-know* of these pieces of informations for the goal *registries maintained*, when authorising *PAT* to *read personal info*, *residential address* and *tax contributions* in the scope of goal *registries maintained*; while it requires *InfoTN* the *non-production* of information *residential address*, *tax contributions* and *personal info*, and *need-to-know* of these pieces of informations for the goal *system maintained*, when authorising *InfoTN* to *read residential address*, *tax contributions* and *personal info* in the scope of goal *system maintained*.
- **Okkam Srl** requires *Tax Agency* a *receiver-authentcation* , when transmitting *tax payers' knowledge base* to *Tax Agency*.
- *Any agent* achieving *corporate records created* is required not to achieve *citizen's records created*, and any agent achieving *citizen's records created* is required not to achieve *corporate records created*, when specifying a SoD constraint between these goals.
- *Any agent* achieving *semantic search built* is required to achieve *enterprise search built*, and any agent achieving *enterprise search built* is required not to achieve *semantic search built*, when specifying a CoD constraint between these goals.

Responsible	Security Requirement	Requester	Description
Tax Agency	receiver-authentication (transmitted(Tax Agency,InfoTN,high quality data))	InfoTN	InfoTN require Tax Agency to authenticate in order to receive document high quality data.
	receiver-authentication (transmitted(Tax Agency,Okkam Srl,tax payers' knowledge base))	Okkam Srl	Okkam Srl require Tax Agency to authenticate in order to receive document tax payers' knowledge base.
	need-to-know (fiscal code,tax contributions) (tax verification performed)	Municipality	Municipality requires Tax Agency need-to-know of Information fiscal code and tax contributions, in the scope of goal tax verification performed.
Engineering Tributi	availability (tax contributions file,90%)	InfoTN	InfoTN require Engineering Tributi to assure an availability level of 90% for document tax contributions file.
	receiver-authentication	InfoTN	InfoTN require Engineering

	(transmitted(Engineering Tributi,InfoTN,tax contributions file))		Tributi to authenticate in order to receive document tax contributions file.
	need-to-know (personal info,residential address,tax contributions) (data refined)	TN Company Selector	TN Company Selector requires Engineering Tributi need-to-know of Information personal info, residential address and tax contributions, in the scope of goal data refined.
InfoTN	no-delegation (data completeness ensured)	Tax Agency	InfoTN requires no-delegation for goal data completeness ensured,when delegating data completeness ensured to InfoTN.
	non-repudiation-of-acceptance (delegated(Tax Agency,InfoTN,data completeness ensured))	Tax Agency	Tax Agency require non-repudiation-of-acceptance for goal data completeness ensured,when delegating data completeness ensured to InfoTN.
	non-repudiation-of-delegation (delegated(InfoTN,Municipality,citizens personal records obtained))	Municipality	Municipality require non-repudiation-of-delegation for goal citizens personal records obtained,when delegated citizens personal records obtained by InfoTN.
	availability (high quality data,98%)	TN Company Selector	TN Company Selector require InfoTN to assure an availability level of 98% for document high quality data.
	recivier-confidentiality (transmitted(Municipality,InfoTN,tax contributions file))	Municipality	InfoTN shall ensure the confidentiality of transmission of the document tax contributions file being transmitted.
	receiver-integrity (transmitted(Municipality,InfoTN,tax contributions file))	Municipality	InfoTN shall ensure the integrity of transmission of the document tax contributions file being transmitted.
	sender-integrity (transmitted(Tax Agency,InfoTN,high quality data))	Tax Agency	InfoTN shall ensure the integrity of transmission of the document high quality data while being transmitted.
	sender-integrity (transmitted(Engineering Tributi,InfoTN,personal records))	Engineering Tributi	InfoTN shall ensure the integrity of transmission of the document personal records while being transmitted.
	sender-integrity (transmitted(Engineering Tributi,InfoTN,civil map addresses))	Engineering Tributi	InfoTN shall ensure the integrity of transmission of the document civil map addresses while being transmitted.
	sender-integrity	Engineering Tributi	InfoTN shall ensure the integrity of transmission of

	(transmitted(Engineering Tributi,InfoTN,tax contributions file))		the document tax contributions file while being transmitted.
	need-to-know (personal info,residential address,tax contributions) (data refined)	Tax Agency	Tax Agency requires InfoTN need-to-know of Information personal info, residential address and tax contributions, in the scope of goal data refined.
	non-production (residential address,tax contributions,personal info)	Municipality	Municipality requires InfoTN non-production of Information residential address, tax contributions and personal info.
	need-to-know (residential address,tax contributions,personal info) (system maintained)	Municipality	Municipality requires InfoTN need-to-know of Information residential address, tax contributions and personal info, in the scope of goal system maintained.
	need-to-know (fiscal code) (data integrated)	PAT	PAT requires InfoTN need-to-know of Information fiscal code, in the scope of goal data integrated.
TN Company Selector	multi-actor-true-redundancy (data refined)	InfoTN	TN Company Selector requires multi-actor-true-redundancy for goal data refined,when delegating data refined to TN Company Selector.
	delegatee-authentication (delegated(InfoTN,TN Company Selector,data refined))	InfoTN	InfoTN require TN Company Selector to authenticate in order to achieve goal data refined.
	no-delegation (search module built)	InfoTN	TN Company Selector requires no-delegation for goal search module built,when delegating search module built to TN Company Selector.
	multi-actor-true-redundancy (navigation module built)	InfoTN	TN Company Selector requires multi-actor-true-redundancy for goal navigation module built,when delegating navigation module built to TN Company Selector.
	no-delegation (navigation module built)	InfoTN	TN Company Selector requires no-delegation for goal navigation module built,when delegating navigation module built to TN Company Selector.
	need-to-know (personal info,residential address) (navigation module	InfoTN	InfoTN requires TN Company Selector need-to-know of Information personal info and residential address, in the

	built,search module built)		scope of goal navigation module built and search module built.
Municipality	no-delegation (citizens personal records obtained)	InfoTN	Municipality requires no-delegation for goal citizens personal records obtained,when delegating citizens personal records obtained to Municipality.
	non-repudiation-of-acceptance (delegated(InfoTN,Municipality,citizens personal records obtained))	InfoTN	InfoTN require non-repudiation-of-acceptance for goal citizens personal records obtained,when delegating citizens personal records obtained to Municipality.
	non-repudiation-of-acceptance (delegated(InfoTN,Municipality,tax payments obtained))	InfoTN	InfoTN require non-repudiation-of-acceptance for goal tax payments obtained,when delegating tax payments obtained to Municipality.
	availability (tax payments obtained,95%)	InfoTN	InfoTN require Municipality to assure an availability level of 95% for goal tax payments obtained.
	need-to-know (personal info) (citizen registered)	Citizen	Citizen requires Municipality need-to-know of Information personal info, in the scope of goal citizen registered.
PAT	delegatee-authentication (delegated(InfoTN,PAT,cadstre data verified))	InfoTN	InfoTN require PAT to authenticate in order to achieve goal cadstre data verified.
	non-production (personal info,residential address,tax contributions)	Municipality	Municipality requires PAT non-production of Information personal info, residential address and tax contributions.
	need-to-know (personal info,residential address,tax contributions) (registries maintained)	Municipality	Municipality requires PAT need-to-know of Information personal info, residential address and tax contributions, in the scope of goal registries maintained.
Okkam Srl	no-delegation (semantic search built)	TN Company Selector	Okkam Srl requires no-delegation for goal semantic search built,when delegating semantic search built to Okkam Srl.
	need-to-know (fiscal code,personal info) (data interconnected)	InfoTN	InfoTN requires Okkam Srl need-to-know of Information fiscal code and personal info, in the scope of goal data interconnected.
	non-modification (personal info,residential	TN Company Selector	TN Company Selector requires Okkam Srl non-

	address,tax contributions)		modification of Information personal info, residential address and tax contributions.
	need-to-know (personal info,residential address,tax contributions) (semantic search built)	TN Company Selector	TN Company Selector requires Okkam Srl need-to-know of Information personal info, residential address and tax contributions, in the scope of goal semantic search built.
BP Engineering Srl	no-delegation (navigation module built)	TN Company Selector	BP Engineering Srl requires no-delegation for goal navigation module built,when delegating navigation module built to BP Engineering Srl.
"Any agents"	not-achieve-both (corporate records created,corporate records created)	-	Any agent that achieves corporate records created or corporate records created, is required not to achieve the other goal too.
	achieve-in-combination (semantic search built,semantic search built)	-	Any agent that achieves one of semantic search built or semantic search built, is required to achieve the other goal too.

Table 14 - Security Requirements for the Taslab Project

Table 15 summarises the authorizations actors in the Taslab project grant to one another.

Authorisor	Information	Goal	Allowed Operations	Denyed Operations	Authorisee	Description
Tax Agency	personal info residential address tax contributions	data refined	M, P		InfoTN	Transferable authority
InfoTN	fiscal code personal info	data interconnected	R, M		Okkam Srl	Transferable authority
	personal info residential address	navigation module built search module built	R		TN Company Selector	Transferable authority
TN Company Selector	personal info residential address tax	semantic search built	R, P	M	Okkam Srl	Transferable authority

	contributions					
	personal info residential address tax contributions	data refined	R		Engineering Tributi	Transferable authority
Citizen	personal info	citizen registered	R, P		Municipality	Transferable authority
Municipality	personal info residential address tax contributions	registries maintained	R	P	PAT	Transferable authority
	fiscal code tax contributions	tax verification performed	R, P		Tax Agency	Transferable authority
	residential address tax contributions personal info	system maintained	R	P	InfoTN	Transferable authority
PAT	fiscal code	data integrated	R		InfoTN	Transferable authority

Table 15 - Authorizations in the Taslab project

Well-formedness Analysis

The purpose of well-formedness analysis is to verify whether the diagram for the project Taslab is consistent and valid. A diagram is considered to be consistent if its constituent elements (concepts and relationships) are drawn and interconnected following the semantics of the modelling language (STS-ml in our case). Thus, well-formedness analysis performs post checks to verify compliance with STS-ml semantics for all checks that cannot be performed live over the models.

More details about the performed checks and their purpose can be found in Appendix B.

The Well-formedness Analysis analysis for Taslab project didn't find any errors.

Security Analysis

The purpose of security analysis is to verify whether the diagram for the project Taslab allows the satisfaction of the specified security needs or not. As a result, for all security needs expressed by stakeholders, it checks in the model whether there is any possibility for the security need to be violated. This analysis takes into account the semantics of STS-ml, defining the behaviour of the different elements represented in the models. The elements' behaviour is defined by propagation rules that consider what concepts and what relationships the specification of a given security need affects. Datalog is used to define the semantics of STS-ml to express facts (things always hold) and rules.

You can find more details about the performed checks in Appendix C.

The Security Analysis analysis for the Taslab has identified the problems summarised in Table 16.

Type	Category	Text	Description
ERROR	No_Delegation Violation check	"TN Company Selector" makes an unauthorised redelegation of goal "semantic search built"	"InfoTN" has expressed a no_delegation security need over the delegation of the goal "search module built" to "TN Company Selector", and yet "TN Company Selector" is re-delegating goal "semantic search built" to "Okkam Srl"
ERROR	No_Delegation Violation check	"InfoTN" makes an unauthorised redelegation of goal "data refined"	"Tax Agency" has expressed a no_delegation security need over the delegation of the goal "data completeness ensured" to "InfoTN", and yet "InfoTN" is re-delegating goal "data refined" to "TN Company Selector"
ERROR	No_Delegation Violation check	"TN Company Selector" makes an unauthorised redelegation of goal "navigation module built"	"InfoTN" has expressed a no_delegation security need over the delegation of the goal "navigation module built" to "TN Company Selector", and yet "TN Company Selector" is re-delegating goal "navigation module built" to "BP Engineering Srl"
ERROR	Redundancy Violation check	InfoTN is violating the multi actor redundancy requirement expressed by TN Company Selector on navigation module built	InfoTN is violating the multi actor redundancy requirement specified by TN Company Selector on the fulfilment of navigation module built
ERROR	Redundancy Violation check	InfoTN is violating the multi actor redundancy requirement expressed by TN Company Selector on data refined	InfoTN is violating the multi actor redundancy requirement specified by TN Company Selector on the fulfilment of data refined
ERROR	Authorization Conflict check	There is a conflict of authorizations related to the production of	There is a conflict of authorizations on production of information

		information tax contributions for actor InfoTN	tax contributions for InfoTN, since there are two incoming authorizations to InfoTN, one from Tax Agency allowing InfoTN and the other one from Municipality requiring non-production of information tax contributions.
ERROR	Authorization Conflict check	There is a conflict of authorizations related to the production of information residential address for actor InfoTN	There is a conflict of authorizations on production of information residential address for InfoTN, since there are two incoming authorizations to InfoTN, one from Tax Agency allowing InfoTN and the other one from Municipality requiring non-production of information residential address.
ERROR	Authorization Conflict check	There is a conflict of authorizations related to the modification of information personal info for actor Okkam Srl	There is a conflict of authorizations on modification of information personal info for Okkam Srl, since there are two incoming authorizations to Okkam Srl, one from InfoTN allowing Okkam Srl and the other one from TN Company Selector requiring non-modification of information personal info.
ERROR	Authorization Conflict check	There is a conflict of authorizations related to the production of information location for actor InfoTN	There is a conflict of authorizations on production of information location for InfoTN, since there are two incoming authorizations to InfoTN, one from Tax Agency allowing InfoTN and the other one from Municipality requiring non-production of information location.
ERROR	Authorization Conflict check	There is a conflict of authorizations related to the production of information personal info for actor InfoTN	There is a conflict of authorizations on production of information personal info for InfoTN, since there are two incoming authorizations to InfoTN, one from Tax Agency allowing InfoTN and the other one from Municipality requiring non-production of information personal info.
ERROR	Non_Modification Violation	"Engineering Tributi" makes an unauthorised modification of information "personal info"	There is no authorization relationship towards "Engineering Tributi" for information "personal info", but "Engineering Tributi" can modify "personal info"

				since there is a modify relationship from its goal "missing data found" towards document "personal records" representing "personal info"
	ERROR	Non_Production Violation	"Citizen" makes an unauthorised production of information "location"	There is no authorization relationship towards "Citizen" for information "location", but "Citizen" can produce "location" since there is a produce relationship from its goal "citizen registered" towards document "" representing "location"
	ERROR	Non_Production Violation	"Citizen" makes an unauthorised production of information "residential address"	There is no authorization relationship towards "Citizen" for information "residential address", but "Citizen" can produce "residential address" since there is a produce relationship from its goal "citizen registered" towards document "personal address" representing "residential address"
	ERROR	Non_Production Violation	"PAT" makes an unauthorised production of information "tax contributions"	"Municipality" has required "PAT" non_production of information "tax contributions", but "PAT" can produce "tax contributions" since there is a produce relationship from its goal "corporate details registered" towards document "corporate registry" representing "tax contributions"
	ERROR	Non_Disclosure Violation	"Municipality" makes an unauthorised distribution of information "personal info"	There is no authorization relationship towards "Municipality", but "Municipality" is distributing "personal info" to "InfoTN" by providing document "personal records" to "InfoTN"
	ERROR	Non_Disclosure Violation	"Citizen" makes an unauthorised distribution of information "residential address"	There is no authorization relationship towards "Citizen", but "Citizen" is distributing "residential address" to "Municipality" by providing document "personal address" to "Municipality"
	ERROR	Non_Disclosure Violation	"InfoTN" makes an unauthorised distribution of information "residential address"	There is no authorization relationship towards "InfoTN", but "InfoTN" is distributing "residential address" to "Engineering Tributi" by providing

				document "civil map addresses" to "Engineering Tributi"
	ERROR	Non_Disclosure Violation	"InfoTN" makes an unauthorised distribution of information "location"	There is no authorization relationship towards "InfoTN", but "InfoTN" is distributing "location" to "Engineering Tributi" by providing document "civil map addresses" to "Engineering Tributi"
	ERROR	Non_Disclosure Violation	"InfoTN" makes an unauthorised distribution of information "tax contributions"	There is no authorization relationship towards "InfoTN", but "InfoTN" is distributing "tax contributions" to "Engineering Tributi" by providing document "tax contributions file" to "Engineering Tributi"
	ERROR	Non_Disclosure Violation	"InfoTN" makes an unauthorised distribution of information "personal info"	There is no authorization relationship towards "InfoTN", but "InfoTN" is distributing "personal info" to "Engineering Tributi" by providing document "personal records" to "Engineering Tributi"
	ERROR	Non_Disclosure Violation	"Citizen" makes an unauthorised distribution of information "location"	There is no authorization relationship towards "Citizen", but "Citizen" is distributing "location" to "Municipality" by providing document "personal address" to "Municipality"
	ERROR	Non_Disclosure Violation	"PAT" makes an unauthorised distribution of information "tax contributions"	There is no authorization relationship towards "PAT", but "PAT" is distributing "tax contributions" to "InfoTN" by providing document "corporate registry" to "InfoTN"
	ERROR	Non-reauthorization Violation: read	"TN Company Selector" violates its authority passing permission to read, in an unauthorised way	"TN Company Selector" has no authority to read information "tax contributions", but still authorises "Engineering Tributi" to read "tax contributions"
	ERROR	Non-reauthorization Violation: read	"Municipality" violates its authority passing permission to read, in an unauthorised way	"Municipality" has no authority to read information "fiscal code", but still authorises "Tax Agency" to read "fiscal code"
	ERROR	Non-reauthorization Violation: read	"TN Company Selector" violates its authority passing permission to read, in an unauthorised way	"TN Company Selector" has no authority to read information "tax contributions", but still authorises "Okkam Srl" to read "tax contributions"

ERROR	Non-reauthorization Violation: modify	"Tax Agency" violates its authority passing permission to modify, in an unauthorised way	"Tax Agency" has no authority to modify information "residential address", but still authorises "InfoTN" to modify "residential address"
ERROR	Non-reauthorization Violation: modify	"Tax Agency" violates its authority passing permission to modify, in an unauthorised way	"Tax Agency" has no authority to modify information "tax contributions", but still authorises "InfoTN" to modify "tax contributions"
ERROR	Non-reauthorization Violation: modify	"Tax Agency" violates its authority passing permission to modify, in an unauthorised way	"Tax Agency" has no authority to modify information "location", but still authorises "InfoTN" to modify "location"
ERROR	Non-reauthorization Violation: modify	"Tax Agency" violates its authority passing permission to modify, in an unauthorised way	"Tax Agency" has no authority to modify information "personal info", but still authorises "InfoTN" to modify "personal info"
ERROR	Non-reauthorization Violation: modify	"InfoTN" violates its authority passing permission to modify, in an unauthorised way	"InfoTN" has no authority to modify information "fiscal code", but still authorises "Okkam Srl" to modify "fiscal code"
ERROR	Non-reauthorization Violation: produce	"TN Company Selector" violates its authority passing permission to produce, in an unauthorised way	"TN Company Selector" has no authority to produce information "residential address", but still authorises "Okkam Srl" to produce "residential address"
ERROR	Non-reauthorization Violation: produce	"TN Company Selector" violates its authority passing permission to produce, in an unauthorised way	"TN Company Selector" has no authority to produce information "tax contributions", but still authorises "Okkam Srl" to produce "tax contributions"
ERROR	Non-reauthorization Violation: produce	"TN Company Selector" violates its authority passing permission to produce, in an unauthorised way	"TN Company Selector" has no authority to produce information "location", but still authorises "Okkam Srl" to produce "location"
ERROR	Non-reauthorization Violation: produce	"Tax Agency" violates its authority passing permission to produce, in an unauthorised way	"Tax Agency" has no authority to produce information "residential address", but still authorises "InfoTN" to produce "residential address"
ERROR	Non-reauthorization Violation: produce	"TN Company Selector" violates its authority passing permission to produce, in an unauthorised way	"TN Company Selector" has no authority to produce information "personal info", but still authorises "Okkam Srl" to produce "personal info"
ERROR	Non-reauthorization Violation: produce	"Tax Agency" violates its authority passing permission to produce, in	"Tax Agency" has no authority to produce information "personal info",

		an unauthorised way	but still authorises "InfoTN" to produce "personal info"
ERROR	Non-reauthorization Violation: produce	"Tax Agency" violates its authority passing permission to produce, in an unauthorised way	"Tax Agency" has no authority to produce information "location", but still authorises "InfoTN" to produce "location"
ERROR	Non-reauthorization Violation: produce	"Municipality" violates its authority passing permission to produce, in an unauthorised way	"Municipality" has no authority to produce information "fiscal code", but still authorises "Tax Agency" to produce "fiscal code"
ERROR	Sod Goal Violation	There is a separation of duty violation with respect to the goals "corporate records created" and "citizen's records created"	Goal "corporate records created" and goal "citizen's records created" should not be achieved by the same actor, since a separation of duty is expressed between these two goals, but "Tax Agency" wants to achieve them both
ERROR	Bod Goal Violation	There is a binding of duty violation with respect to the goals "semantic search built" and "enterprise search built"	Goal "semantic search built" and goal "enterprise search built" should be achieved by the same actor, since a binding of duty is expressed between these goals, but there is no actor to achieve them both, "Okkam Srl" wants to achieve semantic search built but not "enterprise search built"
ERROR	Bod Goal Violation	Possible violation of binding of duties between goals, there is no agent playing the roles	Goal "semantic search built" and goal "enterprise search built" should be achieved by the same actor, since a binding of duty is expressed between these goals, but there is no actor to achieve them both

Table 16 - Security Analysis Analysis Results

Appendix A

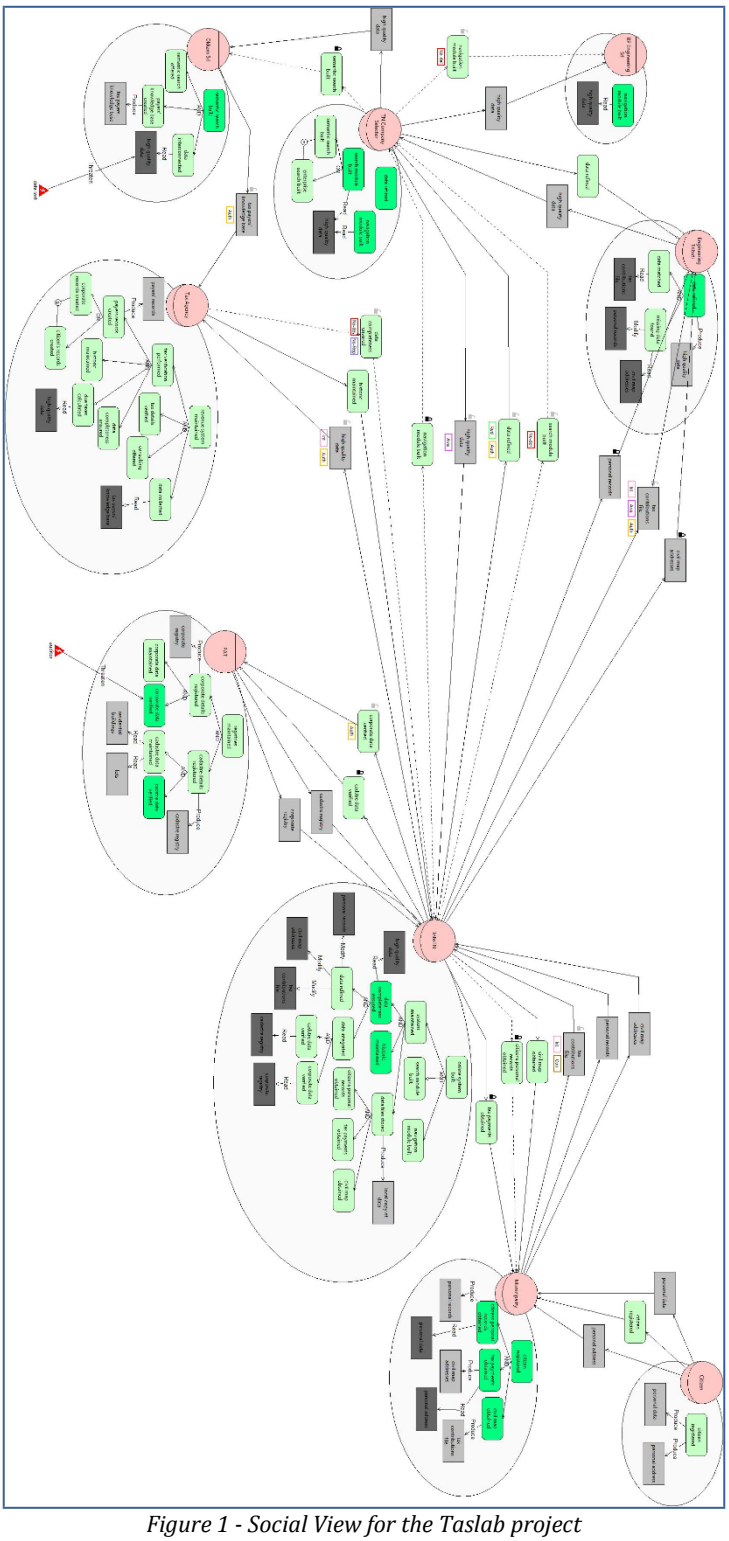

Figure 1 - Social View for the Taslab project

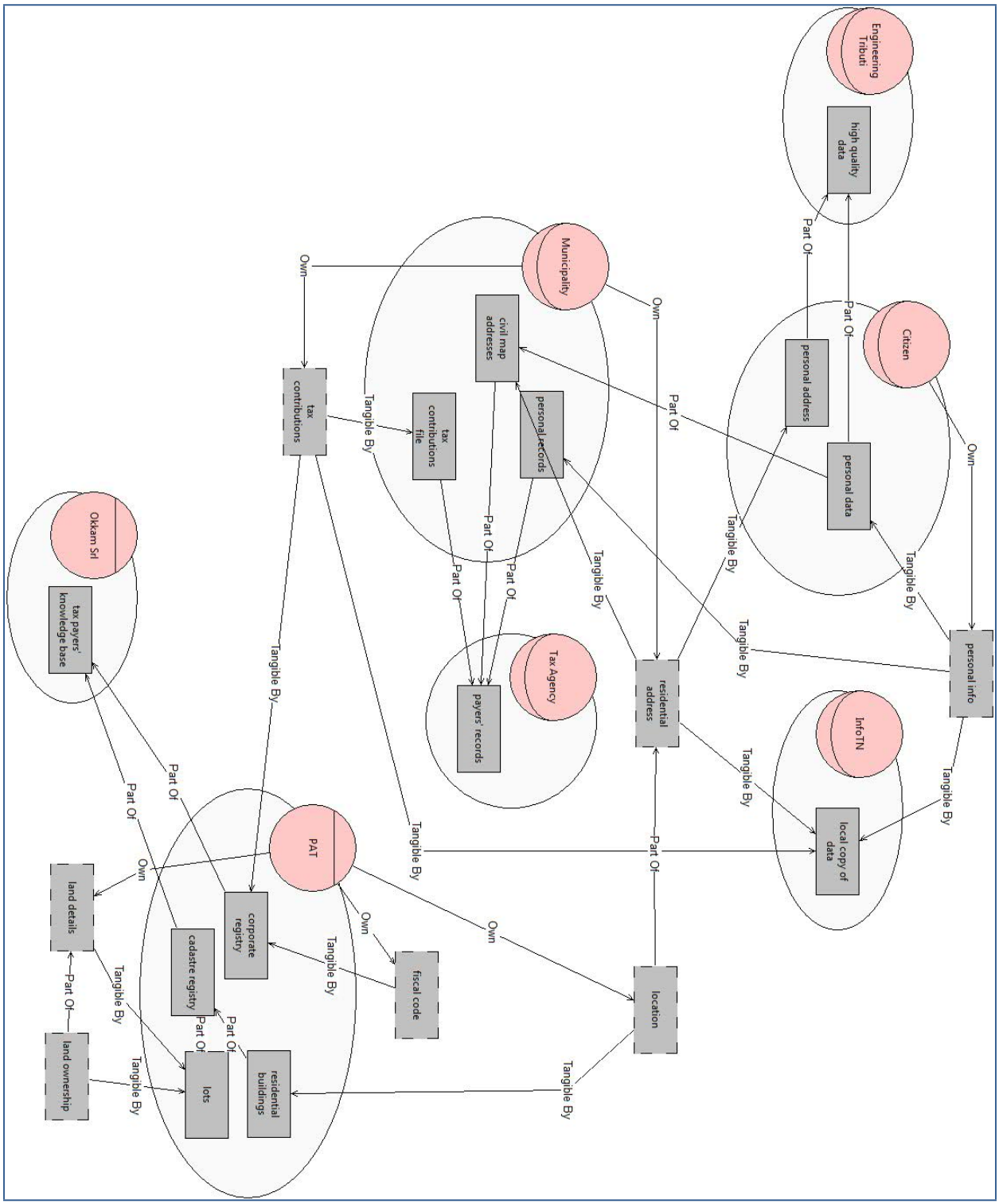

Figure 2 - Information View for the Taslab project

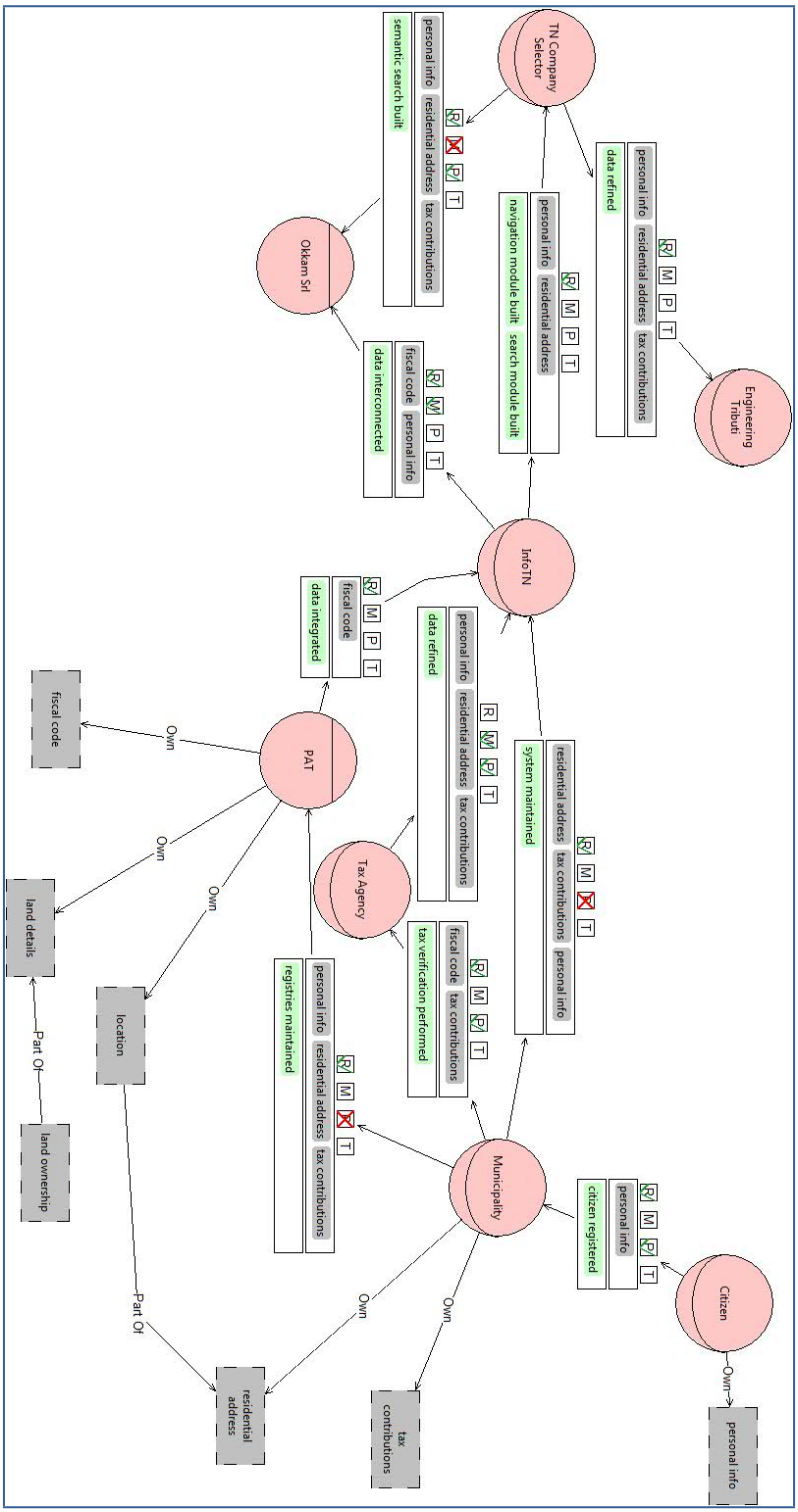

Figure 3 - Authorization View for the Taslab project

Appendix B

Details of Well-formedness analysis:

- **Empty Diagram**

This check verifies whether the given diagram is empty or not. If that is the case, then no other well-formedness checks are performed. If the diagram is not empty, the well-formedness analysis returns: “No errors found” and continues performing the rest of the well-formedness checks.

- **Goal Single Decomposition**

This check verifies the consistency of goal decompositions. Following the semantics of STS-ml a given goal is decomposed in two or more subgoals. As a result, the decomposition should specify at least two subgoals. Therefore, goal single decomposition verifies whether there are cases of decompositions to a single subgoal.

- **Delegation Child Cycle**

This check verifies the consistency of goal delegations, so that no cycles or loops are identified as a result of the delegatee decomposing the delegatum (delegated goal) and re-delegating back one of the subgoals. Delegation child cycle verifies exactly this and gives a warning in case of inconsistency.

- **Delegated Goal Part Of a Decomposition**

This check verifies that all goals (in the delegatee’s scope) that have been delegated are not child (subgoals) in the decomposition.

- **Inconsistent Contribution Cycle**

This check verifies whether there are loops of positive or negative contribution relationships, and whether this loop contains contradictory relationships. If such a loop is identified, the well-formedness analysis returns a warning.

- **Negative Contributions Between AND Subgoals**

This check verifies that there are no negative contribution relationships between and-subgoals of a given goal (within an actor’s scope). It returns a warning if such a case is identified.

- **Documents PartOf Cycle**

This check verifies whether there is a loop or cycle of Part Of relationships starting from and ending to a given document. If a case like this is verified, a warning is returned enumerating the documents that form the cycle.

- **Informations PartOf Cycle**

This check verifies whether there is a loop or cycle of Part Of relationships starting from and ending to a given document. If a case like this is verified, a warning is returned enumerating the documents that form the cycle.

- **Information No Ownership**

This check verifies that all information have an owner. If there are cases of information without any ownership relationships from any actor in the diagram, the well-formedness analysis returns a warning.

- **Authorizations Validity**

This check verifies that all authorization relationship between two given actors are valid. An authorization relationship specifies authorizations or permissions an actor grants to another on some information, to perform some allowed operations. The authorizations could be limited to a goal scope and they can be re-delegated or not. However, the first two attributes should be specified for an authorization relationship to be valid. If there are no information specified, the well-formedness analysis returns an error. The same applies to the cases, in which no allowed operations are specified.

- **Duplicate Authorizations**

This check verifies that there are no duplicate authorization relationships, that could be merged. There are several cases that are addressed by this check: (i) we encounter two identical authorization, i.e., between the same roles, in the same direction, for the same set of information, allowed operations and goals, and having the same value of transferability; (ii) identify authorization relationships between the same roles, in the same direction, in which one grants permissions that are subset of the other authorization's relationship.

Appendix C

Details of security analysis:

- **No_Delegation Violation check**

This violation is verified whenever a delegatee actor further delegates a goal, over the delegation of which a no-delegation security need is specified from the delegator actor. No-delegation is specified over a goal delegation by the delegator, who requires the delegatee not to further delegate the delegated goal. Therefore, to check for any violations of no-delegation, the analysis searches for redelegations of the delegatum (delegated goal) or any of its subgoals.

- **Redundancy Violation check**

This check verifies if redundancy is satisfied by controlling that single actor redundancy or multi actor redundancy are not violated. At design time we cannot make the distinction between fallback and true redundancy, so they cannot be verified at this stage.Therefore, both fallback redundancy single and true redundancy single are mapped to single actor redundancy. Similarly for multi actor redundancy. The analysis verifies a redundancy violation if one of the following occurs: (1) actor does not decompose the delegated goal in any or-subgoals, for which both types of redundancy are violated (2) actor decomposes the goal into or-subgoals and delegates one to another actor when single actor redundancy has been specified, for which this type of redundancy is violated (3) actor decomposes the goal into or-subgoals, but does not delegate any of the subgoals to another actor when multi actor redundancy has been specified, for which this type of redundancy is violated.

- **Authorization Conflict check**

This task identifies a conflict of authorization whenever at least two authorization relationships for the same information are drawn towards the same actor from two illegible actors (being the owner of information or another authorised actor) such that: (1) one limits the authorization to a goal scope (requiring a need-to-know security need) and the other does not (authorising the actor without any limitations) (2) for the same goals or intersecting goal scopes, different permissions are granted in terms of operations or authority to transfer authoristaion. That is, one passes the actor the authority to perform operations (use, modify, produce, distribute) on a given information, and the other does not (requiring non-usage, non-modification, non-production, non-disclosure); one passes the actor the authority to further transfer authorizations and the other requires no further authorizations take place.

- **Non_Reading Violation**

This violation is detected whenever an actor discloses information without having the right to distribute it. Non-disclosure expresses the need of not disclosing or further distributing the given information to other actors, apart from the authoriser. Thus, authority to distribute the information is not passed. The way actors exchange information is through document provision. In order to disclose some information, an actor would have to provide to others the document(s) containing that information. Hence, to verify if there are any unauthorized disclosures of information, the analysis checks for provisions of documents representing the given information from any unauthorized actors towards other actors.

- **Non_Modification Violation**

This violation is detected whenever an actor modifies information without having the right to modify it. Non-modification expresses the need that information should not be changed (modified), i.e. authority to modify the information is not granted. To verify if there could be any violations of non-modification, the analysis looks if the authorisee (or an actor that is not authorised by authorised party) modifies the given information. For this, it searches for modify relationships from any goal of this actor to any document representing the given information.

- **Non_Production Violation**

This violation is detected whenever an actor produces information without having the right to produce it. Non-production expresses the need that information should not be produced in any form, i.e. authority to produce the information is not granted. To verify if there could be any violations of non-production, the analysis checks whether if the authorisee (or an actor that is not authorised by authorised party) produces the given information. For this, it searches for produce relationships from any goal of this actor to any document representing the given information.

- **Non_Disclosure Violation**

This violation is detected whenever an actor discloses information without having the right to distribute it. Non-disclosure expresses the need of not disclosing or further distributing the given information to other actors, apart from the authoriser. Thus, authority to distribute the information is not passed. The way actors exchange information is through document provision. In order to disclose some information, an actor would have to provide to others the document(s) containing that information. Hence, to verify if there are any unauthorized disclosures of information, the analysis checks for provisions of documents representing the given information from any unauthorized actors towards other actors.

- **NTK Violation**

This violation is detected whenever an actor uses, modifies or produces information for other purposes (goal achievement) than the ones for which it is authorized. Need-to-know requires that the information is used, modified, or produced in the scope of the goals specified in the authorization. This security need concerns confidential information, which should not be utilised for any other purposes other than the intended ones. To verify if there could be any violations of need-to-know, security analysis checks if the authorisee (or an actor that is not authorised by any authorised party) uses, modifies or produces the given information while achieving some goal different from the one it is authorised for. In a nutshell, it searches for need, modify, or produce relationships starting from goals different from the specified ones towards documents representing the given information.

- **Explicit non-reauthorization**

Verifies whether a given actor transfer rights to others even when it does not have the authority to further delegate rights.

- **Non-reauthorization Violation: read**

Verifies whether a given actors transfer to other actors the right to use a given information, without having itself the right to do so.

- **Non-reauthorization Violation: modify**

Verifies whether a given actors transfer to other actors the right to modify a given information, without having itself the right to do so.

- **Non-reauthorization Violation: produce**

Verifies whether a given actors transfer to other actors the right to modify a given information, without having itself the right to do so.

- **Non-reauthorization Violation: transmit**

Verifies whether a given actors transfer to other actors the right to distribute a given information, without having itself the right to do so.

- **Sod Goal Violation**

This violation is detected whenever a single actor may perform both goals, between which an SoD constraint is expressed. Goal-based SoD requires that there is no actor performing both goals among which SoD is specified. To perform this verification, the analysis checks that the final performer of the given goals is not the same actor.

- **Bod Goal Violation**

This violation is detected whenever a single actor may perform both goals, between which an SoD constraint is expressed. Goal-based SoD requires that there is no actor performing both goals among which SoD is specified. To perform this verification, the analysis checks that the final performer of the given goals is not the same actor.

- **Agent Play Sod**

This check verifies the consistency of the Separation of Duty (SoD) constraint between roles. This constraint requires that two roles are not played by the same agent, therefore the check verifies whether there is one agent playing both roles. If that is the case an error is identified, otherwise the check finds no errors.

- **Agent Not Play Bod**

This check verifies the consistency of the Binding of Duty (BoD) constraint between roles. This constraint requires that two roles are played by the same agent, therefore the check verifies whether there is one agent playing both roles. If that is the case the check finds no errors, otherwise an error is identified.

- **Organizational Constraint Consistency**

This check verifies that no conflicting organisational constraints (SoD or BoD) between goals are specified.