Security Requirements Document

egov

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 egov 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 egov 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).

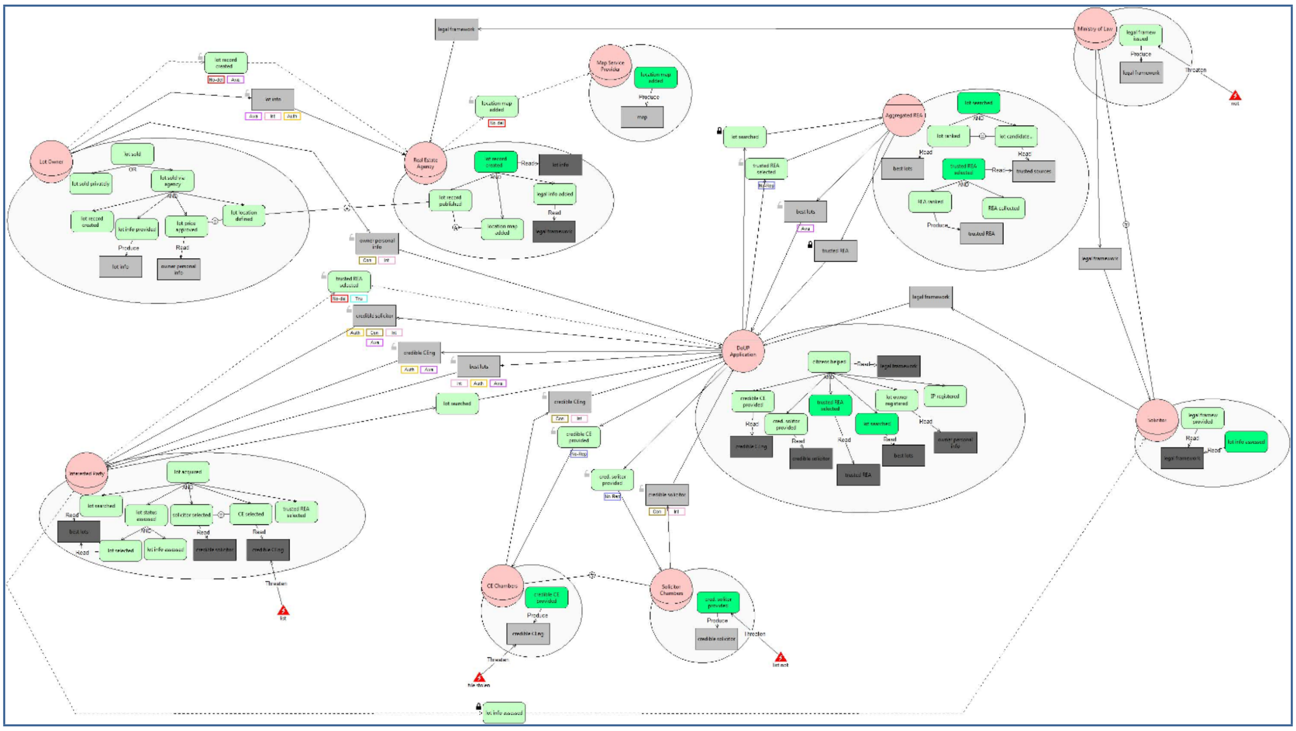

Figure 1 - Social View for the egov project

Stakeholders

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

In particular, identified roles are: *Lot Owner*, *Real Estate Agency*, *Map Service Provider*, *Interested Party*, *CE Chambers*, *Solicitor Chambers*, *Ministry of Law* and *Solicitor* (Figure 1), while identified agents are: *DoUP Application* and *Aggregated REA* (Figure 1). Table 1 and Table 2 summarise the stakeholders.

Role	Description	Mission	Purpose
Lot Owner			
Real Estate Agency			
Map Service Provider			
Interested Party			
CE Chambers			
Solicitor Chambers			
Ministry of Law			
Solicitor			

Table 1 - Roles in the egov project.

Agent	Description	Abilities	Important Features	Certifications Accreditations	Type Of Organisation
DoUP Application					
Aggregated REA					

Table 2 - Agents in the egov project

In the egov 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 egov project (Figure 1) we have:

- **Lot Owner** has documents *lot info* and *owner personal info*.
- **Real Estate Agency** has document *lot info* provided by *Lot Owner* and document *legal framework* provided by *Ministry of Law*.
- **Map Service Provider** has document *map*.
- **Interested Party** has document *credible solicitor* provided by *DoUP Application*, document *credible CEng* provided by *DoUP Application* and document *best lots* provided by *DoUP Application*.

- **DoUP Application** has document *trusted REA* provided by *Aggregated REA*, document *credible solicitor* provided by *Solicitor Chambers*, document *credible CEng* provided by *CE Chambers*, document *owner personal info* provided by *Lot Owner*, document *best lots* provided by *Aggregated REA* and document *legal framework* provided by *Solicitor*.
- **CE Chambers** has document *credible CEng*.
- **Solicitor Chambers** has document *credible solicitor*.
- **Aggregated REA** has documents *trusted sources*, *best lots* and *trusted REA*.
- **Ministry of Law** has document *legal framework*.
- **Solicitor** has document *legal framework* provided by *Ministry of Law*.

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

Agent/Role	Document	Description
Lot Owner	lot info	
	owner personal info	
Real Estate Agency	lot info	
	legal framework	
Map Service Provider	map	
Interested Party	credible CEng	
	credible solicitor	
	best lots	
DoUP Application	credible CEng	
	credible solicitor	
	trusted REA	
	best lots	
	owner personal info	
	legal framework	
CE Chambers	credible CEng	
Solicitor Chambers	credible solicitor	
Aggregated REA	trusted sources	
	best lots	
	trusted REA	
Ministry of Law	legal framework	
Solicitor	legal framework	

Table 3 - Stakeholders' documents in the egov 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 egov project (Figure 1) stakeholders' documents and goals are related as follows:

- **Lot Owner** *produces* document *lot info* to achieve goal *lot info provided* and *reads* document *owner personal info* to achieve goal *lot price approved*.
- **Real Estate Agency** *reads* document *lot info* to achieve goal *lot record created* and *reads* document *legal framework* to achieve goal *legal info added*.
- **Map Service Provider** *produces* document *map* to achieve goal *location map added*.
- **Interested Party** *reads* document *best lots* to achieve goal *lot searched*, *reads* document *credible CEng* to achieve goal *CE selected*, *reads* document *best lots* to achieve goal *lot selected* and *reads* document *credible solicitor* to achieve goal *solicitor selected*.
- **DoUP Application** *reads* document *credible CEng* to achieve goal *credible CE provided*, *reads* document *legal framework* to achieve goal *citizens helped*, *reads* document *best lots* to achieve goal *lot searched*, *reads* document *credible solicitor* to achieve goal *cred. solitor provided*, *reads* document *trusted REA* to achieve goal *trusted REA selected* and *reads* document *owner personal info* to achieve goal *lot owner registered*.
- **CE Chambers** *produces* document *credible CEng* to achieve goal *credible CE provided*.
- **Solicitor Chambers** *produces* document *credible solicitor* to achieve goal *cred. solitor provided*.
- **Aggregated REA** *produces* document *trusted REA* to achieve goal *REA ranked*, *reads* document *trusted sources* to achieve goal *trusted REA selected*, *reads* document *best lots* to achieve goal *lot ranked* and *reads* document *trusted sources* to achieve goal *lot candidate...*.
- **Ministry of Law** *produces* document *legal framework* to achieve goal *legal framew issued*.
- **Solicitor** *reads* document *legal framework* to achieve goal *lot info assessed* and *reads* document *legal framework* to achieve goal *legal framew provided*.

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

Agent/Role	Goal	Document	Relation
Lot Owner	lot info provided	lot info	Produce
	lot price approved	owner personal info	read
Real Estate Agency	lot record created	lot info	read
	legal info added	legal framework	read
Map Service Provider	location map added	map	Produce
Interested Party	lot searched	best lots	read
	CE selected	credible CEng	read
	lot selected	best lots	read
	solicitor selected	credible solicitor	read

DoUP Application	credible CE provided	credible CEng	read
	citizens helped	legal framework	read
	lot searched	best lots	read
	cred. solitor provided	credible solicitor	read
	trusted REA selected	trusted REA	read
	lot owner registered	owner personal info	read
CE Chambers	credible CE provided	credible CEng	Produce
Solicitor Chambers	cred. solitor provided	credible solicitor	Produce
Aggregated REA	REA ranked	trusted REA	Produce
	trusted REA selected	trusted sources	read
	lot ranked	best lots	read
	lot candidate...	trusted sources	read
Ministry of Law	legal framew issued	legal framework	Produce
Solicitor	lot info assessed	legal framework	read
	legal framew provided	legal framework	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 egov project (Figure 1) we have:

- **Lot Owner** has to achieve goal *lot sold*. To achieve *lot sold*, Lot Owner should achieve either goal *lot sold privately* or goal *lot sold via agency* To achieve *lot sold via agency*, Lot Owner should achieve goal *lot record created* , goal *lot info provided*, goal *lot price approved* and goal *lot location defined*
- **Real Estate Agency** has to achieve goal *lot record created* . To achieve *lot record created* , Real Estate Agency should achieve goal *lot record published*, goal *location map added* and goal *legal info added*
- **Map Service Provider** has to achieve goal *location map added*.
- **Interested Party** has to achieve goal *lot acquired*. To achieve *lot acquired*, Interested Party should achieve goal *lot searched*, goal *lot status assessed*, goal *solicitor selected*, goal *CE selected* and goal *trusted REA selected* To achieve *lot status assessed*, Interested Party should achieve goal *lot selected* and goal *lot info assessed*

- **DoUP Application** has to achieve goal *citizens helped*. To achieve *citizens helped*, DoUP Application should achieve goal *credible CE provided*, goal *cred. solitor provided*, goal *trusted REA selected*, goal *lot searched*, goal *lot owner registered* and goal *IP registered*
- **CE Chambers** has to achieve goal *credible CE provided*.
- **Solicitor Chambers** has to achieve goal *cred. solitor provided*.
- **Aggregated REA** has to achieve goal *lot searched* and goal *trusted REA selected*. To achieve *lot searched*, Aggregated REA should achieve goal *lot ranked* and goal *lot candidate...* To achieve *trusted REA selected*, Aggregated REA should achieve goal *REA ranked* and goal *REA collected*
- **Ministry of Law** has to achieve goal *legal framew issued*.
- **Solicitor** has to achieve goal *legal framew provided* and goal *lot info assessed*.

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

Agent/Role	Goal	Dec. Type	Subgoals
Lot Owner	lot sold	OR	lot sold privately
			lot sold via agency
Real Estate Agency	lot record created	AND	lot record published
			location map added
			legal info added
Map Service Provider	location map added	-	
Interested Party	lot acquired	AND	lot searched
			lot status assessed
			solicitor selected
			CE selected
			trusted REA selected
DoUP Application	citizens helped	AND	credible CE provided
			cred. solitor provided
			trusted REA selected
			lot searched
			lot owner registered
			IP registered
CE Chambers	credible CE provided	-	
Solicitor Chambers	cred. solitor provided	-	
Aggregated REA	lot searched	AND	lot ranked
			lot candidate...
	trusted REA selected	AND	REA ranked
			REA collected
Ministry of Law	legal framew issued	-	
Solicitor	legal framew provided	-	

	lot info assessed	-

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

- **Lot Owner** delegates goal *lot record created* to **Real Estate Agency**.

  The following security needs apply to this delegation:

  No-Delegation and Availability: 90.

- **Real Estate Agency** delegates goal *location map added* to **Map Service Provider**.

  The following security needs apply to this delegation:

  No-Delegation.

- **Interested Party** delegates goal *lot searched* to **DoUP Application**.
- **Interested Party** delegates goal *trusted REA selected* to **DoUP Application**.

  The following security needs apply to this delegation:

  No-Delegation and Trustworthiness.

- **Interested Party** delegates goal *lot info assessed* to **Solicitor**.

  The following security needs apply to this delegation:

  No-Delegation.

- **DoUP Application** delegates goal *credible CE provided* to **CE Chambers**.

  The following security needs apply to this delegation:

  Non Repudiation: delegation-acceptance.

- **DoUP Application** delegates goal *cred. solitor provided* to **Solicitor Chambers**.

  The following security needs apply to this delegation:

  Non Repudiation: delegation-acceptance.

- **DoUP Application** delegates goal *lot searched* to **Aggregated REA**.

  The following security needs apply to this delegation:

  Non Repudiation: delegation-acceptance.

- **DoUP Application** delegates goal *trusted REA selected* to **Aggregated REA**.

  The following security needs apply to this delegation:

  Non Repudiation: delegation-acceptance.

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

Delegator	Goal	Delegatee	Security Needs	Delegation Description
Lot Owner	lot record created	Real Estate Agency	**No-Delegation** **Availability**: *90*	
Real Estate Agency	location map added	Map Service Provider	**No-Delegation**	
Interested Party	lot searched	DoUP Application		
	trusted REA selected	DoUP Application	**No-Delegation** **Trustworthiness**	
	lot info assessed	Solicitor	**No-Delegation**	
DoUP Application	credible CE provided	CE Chambers	**Non Repudiation**: *delegation-acceptance*	
	cred. solitor provided	Solicitor Chambers	**Non Repudiation**: *delegation-acceptance*	
	lot searched	Aggregated REA	**Non Repudiation**: *delegation-acceptance*	
	trusted REA selected	Aggregated REA	**Non Repudiation**: *delegation-acceptance*	

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

- **Lot Owner** transmit document *lot info* to **Real Estate Agency**.

  The following security needs apply to this transmission:

  Availability: 90, Integrity: receiver and Authentication: receiver.

- **Lot Owner** transmit document *owner personal info* to **DoUP Application**.

  The following security needs apply to this transmission:

  Confidentiality: receiver and Integrity: receiver.

- **DoUP Application** transmit document *credible CEng* to **Interested Party**.

  The following security needs apply to this transmission:

  Authentication: receiver and Availability: 90.

- **DoUP Application** transmit document *credible solicitor* to **Interested Party**.

  The following security needs apply to this transmission:

  Authentication: sender, Confidentiality: receiver, Integrity: sender and Availability: 87.

- **DoUP Application** transmit document *best lots* to **Interested Party**.

  The following security needs apply to this transmission:

  Integrity: sender, Authentication: receiver and Availability: 90.

- **CE Chambers** transmit document *credible CEng* to **DoUP Application**.

  The following security needs apply to this transmission:

  Confidentiality: receiver and Integrity: receiver.

- **Solicitor Chambers** transmit document *credible solicitor* to **DoUP Application**.

  The following security needs apply to this transmission:

  Confidentiality: sender and Integrity: receiver.

- **Aggregated REA** transmit document *trusted REA* to **DoUP Application**.

  The following security needs apply to this transmission:

  Availability: 95.

- **Aggregated REA** transmit document *best lots* to **DoUP Application**.

  The following security needs apply to this transmission:

Availability: 95.

- **Ministry of Law** transmit document *legal framework* to **Real Estate Agency**.
- **Ministry of Law** transmit document *legal framework* to **Solicitor**.
- **Solicitor** transmit document *legal framework* to **DoUP Application**.

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

Transmitter	Document	Recivier	Security Needs	Transmission Descr.
Lot Owner	lot info	Real Estate Agency	**Availability**: *90* **Integrity**: *receiver* **Authentication**: *receiver*	
	owner personal info	DoUP Application	**Confidentiality**: *receiver* **Integrity**: *receiver*	
DoUP Application	credible CEng	Interested Party	**Authentication**: *receiver* **Availability**: *90*	
	credible solicitor	Interested Party	**Authentication**: *sender* **Confidentiality**: *receiver* **Integrity**: *sender* **Availability**: *87*	
	best lots	Interested Party	**Integrity**: *sender* **Authentication**: *receiver* **Availability**: *90*	
CE Chambers	credible CEng	DoUP Application	**Confidentiality**: *receiver* **Integrity**: *receiver*	
Solicitor Chambers	credible solicitor	DoUP Application	**Confidentiality**: *sender* **Integrity**: *receiver*	
Aggregated REA	trusted REA	DoUP Application	**Availability**: *95*	
	best lots	DoUP Application	**Availability**: *95*	
Ministry of Law	legal framework	Real Estate Agency		
	legal framework	Solicitor		
Solicitor	legal framework	DoUP Application		

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

- **Solicitor Chambers** is incompatible with **CE Chambers**, since *SoD* constraints are specified between these roles.
- **CE Chambers** is incompatible with **Solicitor Chambers**, since *SoD* constraints are specified between these roles.
- **Ministry of Law** is incompatible with **Solicitor**, since *SoD* constraints are specified between these roles.
- **Solicitor** is incompatible with **Ministry of Law**, since *SoD* constraints are specified between these roles.
- **lot record published** is incompatible with **location map added** and **lot location defined**, given that *SoD* constraint is specified between these goals.
- **location map added** is incompatible with **lot record published**, given that *SoD* constraint is specified between these goals.
- **lot location defined** is incompatible with **lot record published**, given that *SoD* constraint is specified between these goals.
- **lot price approved** should be combined with **lot location defined**, given that *BoD* constraint is specified between these goals.
- **CE selected** should be combined with **solicitor selected**, given that *BoD* constraint is specified between these goals.
- **lot ranked** should be combined with **lot candidate...**, given that *BoD* constraint is specified between these goals.
- **lot location defined** should be combined with **lot price approved**, given that *BoD* constraint is specified between these goals.
- **lot candidate...** should be combined with **lot ranked**, given that *BoD* constraint is specified between these goals.
- **solicitor selected** should be combined with **CE selected**, given that *BoD* constraint is specified between these goals.

Table 8 summarises the organisational constraints for the egov project.

Organisational Constraint	Role/Goal	Role/Goal	Description
SoD (Role - Role)	Solicitor Chambers	CE Chambers	
	CE Chambers	Solicitor Chambers	
	Ministry of Law	Solicitor	
	Solicitor	Ministry of Law	
SoD (Goal - Goal)	lot record published	location map added	

		lot location defined
	location map added	lot record published
	lot location defined	lot record published
BoD (Goal - Goal)	lot price approved	lot location defined
	CE selected	solicitor selected
	lot ranked	lot candidate...
	lot location defined	lot price approved
	lot candidate...	lot ranked
	solicitor selected	CE selected

Table 8 - Organisational Constraints

Events

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

Event name	Threatened elements	Description
list not found	GoalReference: cred. solitor provided	
list unavail.	DocumentReference: credible CEng	
not approved	Goal: legal framew issued	
file stolen	Document: credible CEng	

Table 9 - Events

Information View

The information view gives a structured representation of the information and documents in the egov 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).

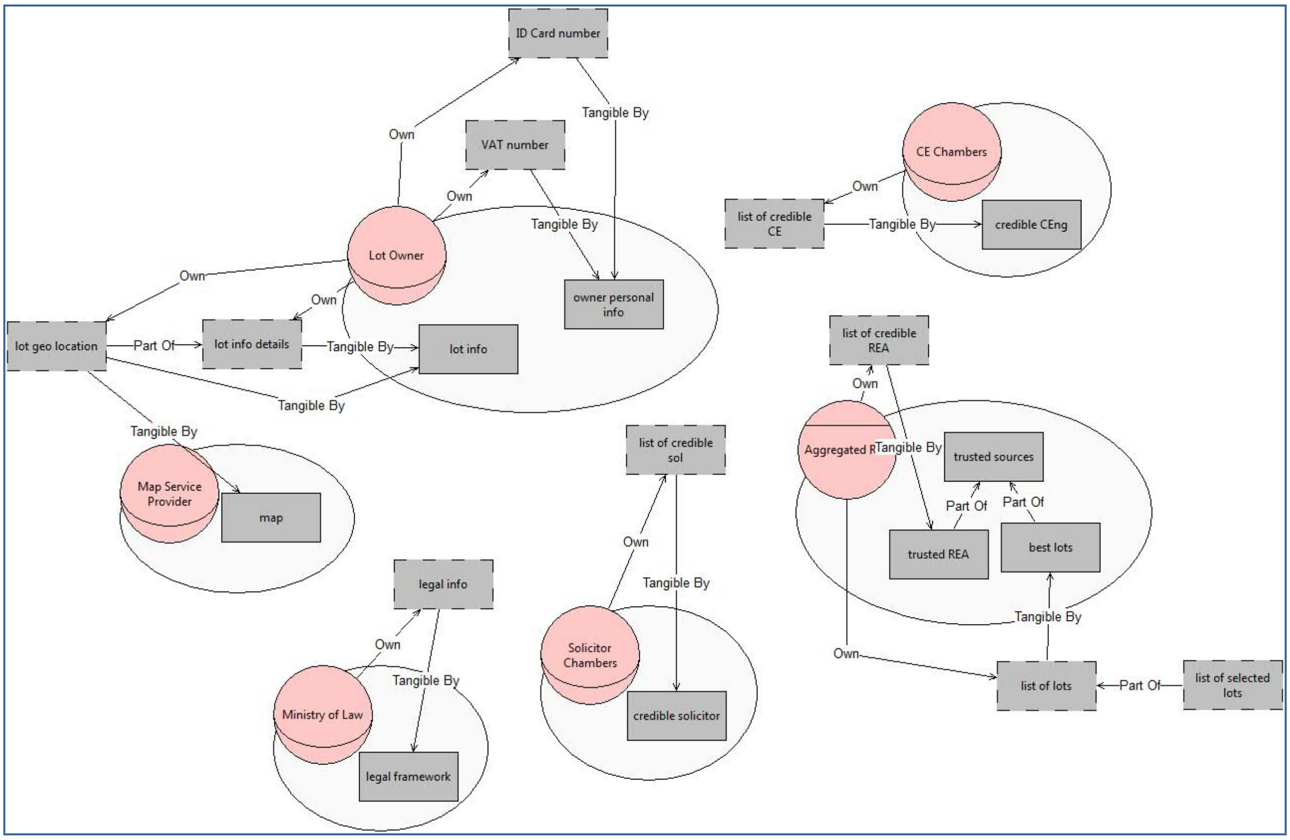

Figure 2 - Information View for the egov project

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 egov project are summarised in Table 10.

Agent/Role	Information	Description
Lot Owner	lot geo location	
	lot info details	
	VAT number	
	ID Card number	
CE Chambers	list of credible CE	
Solicitor Chambers	list of credible sol	
Aggregated REA	list of credible REA	
	list of lots	
Ministry of Law	legal info	

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

Information	Document	Description
list of credible CE	credible CEng	
list of credible sol	credible solicitor	
legal info	legal framework	
lot info details	lot info	
lot geo location	lot info	
	map	
list of credible REA	trusted REA	
ID Card number	owner personal info	
list of lots	best lots	
VAT number	owner personal info	

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 egov project are structured.

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

Information	Composition	Description
lot info details	lot geo location	
list of lots	list of selected lots	

Table 12 - Information composition

Document	Composition	Description
trusted sources	trusted REA	
	best lots	

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).

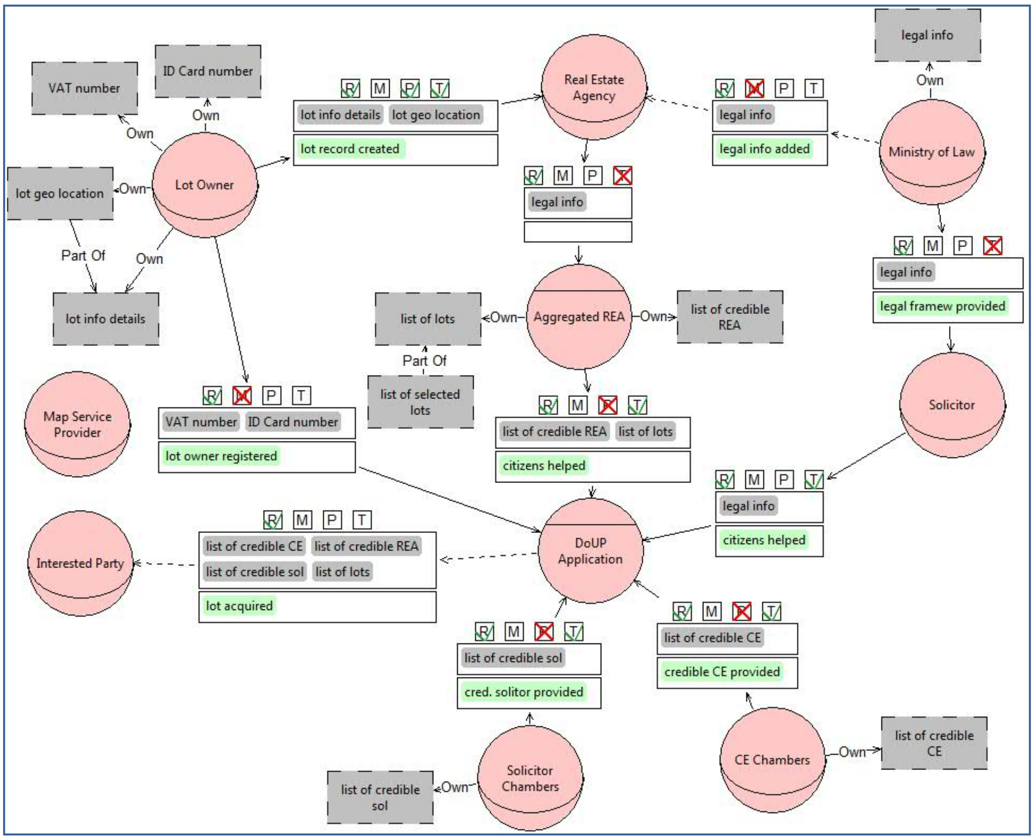

Figure 3 - Authorization View for the egov project

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 egov project (Figure 3) the authorizations for each role/agent are:

- *Role* **Lot Owner**:
    - **Lot Owner** authorises *Real Estate Agency* to *read*, *produce* and *transmit* information *lot info details* and *lot geo location*, in the scope of goal *lot record created* , *passing* the right to further authorising other actors, and authorises *DoUP Application* to *read* and prohibits to *modify* information *VAT number* and *ID Card number*, in the scope of goal *lot owner registered*, *passing* the right to further authorising other actors.
- *Role* **Real Estate Agency**:
    - **Real Estate Agency** authorises *Aggregated REA* to *read* and prohibits to *transmit* information *legal info*, *passing* the right to further authorising other actors.
    - **Real Estate Agency** is authorised by *Real Estate Agency* to *read*, *produce* and *transmit* information *lot info details* and *lot geo location*, in the scope of goal *lot record created* , *having* the right to further authorising other actors, and is authorised by *Real Estate Agency* to *read* and prohibited to *modify* information *legal info*, in the scope of goal *legal info added*, *having* the right to further authorising other actors.
- *Role* **Interested Party**:
    - **Interested Party** is authorised by *Interested Party* to *read* information *list of credible CE*, *list of credible REA*, *list of credible sol* and *list of lots*, in the scope of goal *lot acquired*, *having* the right to further authorising other actors.
- *Agent* **DoUP Application**:
    - **DoUP Application** authorises *Interested Party* to *read* information *list of credible CE*, *list of credible REA*, *list of credible sol* and *list of lots*, in the scope of goal *lot acquired*, *passing* the right to further authorising other actors.
    - **DoUP Application** is authorised by *DoUP Application* to *read* and *transmit* and prohibited to *produce* information *list of credible REA* and *list of lots*, in the scope of goal *citizens helped*, *having* the right to further authorising other actors, and is authorised by *DoUP Application* to *read* and *transmit* information *legal info*, in the scope of goal *citizens helped*, *having* the right to further authorising other actors, and is authorised by *DoUP Application* to *read* and prohibited to *modify* information *VAT number* and *ID Card number*, in the scope of goal *lot owner registered*, *having* the right to further authorising other actors, and is authorised by *DoUP Application* to *read* and *transmit* and prohibited to *produce* information *list of credible sol*, in the scope of goal *cred. solitor provided*, *having* the right to further authorising other actors, and is authorised by *DoUP Application* to *read* and *transmit* and prohibited to *produce* information *list of credible CE*, in the scope of goal *credible CE provided*, *having* the right to further authorising other actors.
- *Role* **CE Chambers**:

  - **CE Chambers** authorises *DoUP Application* to *read* and *transmit* and prohibits to *produce* information *list of credible CE*, in the scope of goal *credible CE provided*, *passing* the right to further authorising other actors.

- *Role* **Solicitor Chambers**:
  - **Solicitor Chambers** authorises *DoUP Application* to *read* and *transmit* and prohibits to *produce* information *list of credible sol*, in the scope of goal *cred. solitor provided*, *passing* the right to further authorising other actors.

- *Agent* **Aggregated REA**:
  - **Aggregated REA** authorises *DoUP Application* to *read* and *transmit* and prohibits to *produce* information *list of credible REA* and *list of lots*, in the scope of goal *citizens helped*, *passing* the right to further authorising other actors.
  - **Aggregated REA** is authorised by *Aggregated REA* to *read* and prohibited to *transmit* information *legal info*, *having* the right to further authorising other actors.

- *Role* **Ministry of Law**:
  - **Ministry of Law** authorises *Real Estate Agency* to *read* and prohibits to *modify* information *legal info*, in the scope of goal *legal info added*, *passing* the right to further authorising other actors, and authorises *Solicitor* to *read* and prohibits to *transmit* information *legal info*, in the scope of goal *legal framew provided*, *passing* the right to further authorising other actors.

- *Role* **Solicitor**:
  - **Solicitor** authorises *DoUP Application* to *read* and *transmit* information *legal info*, in the scope of goal *citizens helped*, *passing* the right to further authorising other actors.
  - **Solicitor** is authorised by *Solicitor* to *read* and prohibited to *transmit* information *legal info*, in the scope of goal *legal framew provided*, *having* the right to further authorising other actors.

Security Requirements

This section provides the list of security requirements derived for the egov 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 egov project (Table 14) are:

- **Lot Owner** requires *Real Estate Agency no-delegation* on goal *lot record created* and an *availability* level of 90%, when delegating *lot record created* to *Real Estate Agency*.
- **Lot Owner** requires *Real Estate Agency* an *availability* level of 90%, a *receiver-authentcation* and a *receiver-integrity* , when transmitting *lot info* to *Real Estate Agency*requires *DoUP Application* a *receiver-integrity* and a *receiver-confidentiality* , when transmitting *owner personal info* to *DoUP Application*.
- **Lot Owner** requires *DoUP Application* the *non-modification* of information *VAT number* and *ID Card number*, and *need-to-know* of these pieces of informations for the goal *lot owner registered*, when authorising *DoUP Application* to *read VAT number* and *ID Card number* in the scope of goal *lot owner registered*.
- **Real Estate Agency** requires *Map Service Provider no-delegation* on goal *location map added*, when delegating *location map added* to *Map Service Provider*.
- **Real Estate Agency** requires *Aggregated REA* the *non-disclosure* of information *legal info*, , when authorising *Aggregated REA* to *read legal info*.
- **Interested Party** requires *DoUP Application no-delegation* on goal *trusted REA selected* and *trustworthiness*, when delegating *trusted REA selected* to *DoUP Application*; while it requires *Solicitor no-delegation* on goal *lot info assessed*, when delegating *lot info assessed* to *Solicitor*.
- **DoUP Application** requires *CE Chambers non-repudiation-of-acceptance* of the delegation of goal *credible CE provided*, when delegating *credible CE provided* to *CE Chambers*; while it is required by *CE Chambers non-repudiation-of-delegation* of the delegation of goal *credible CE provided*when delegating *credible CE provided* to *CE Chambers*; while it requires *Solicitor Chambers non-repudiation-of-acceptance* of the delegation of goal *cred. solitor provided*, when delegating *cred. solitor provided* to *Solicitor Chambers*; while it is required by *Solicitor Chambers non-repudiation-of-delegation* of the delegation of goal *cred. solitor provided*when delegating *cred. solitor provided* to *Solicitor Chambers*; while it requires *Aggregated REA non-repudiation-of-acceptance* of the delegation of goal *lot searched*, when delegating *lot searched* to *Aggregated REA*; while it is required by *Aggregated REA non-repudiation-of-delegation* of the delegation of goal *lot searched*when delegating *lot searched* to *Aggregated REA*; while it requires *Aggregated REA non-repudiation-of-acceptance* of the delegation of goal *trusted REA selected*, when delegating *trusted*

REA selected to *Aggregated REA*; while it is required by *Aggregated REA non-repudiation-of-delegation* of the delegation of goal *trusted REA selected*when delegating *trusted REA selected* to *Aggregated REA*.

- **DoUP Application** requires *Interested Party* an *availability* level of 90% and a *receiver-authentcation* , when transmitting *credible CEng* to *Interested Party*requires *Interested Party* an *availability* level of 87% and a *receiver-confidentiality* , when transmitting *credible solicitor* to *Interested Party*; while it is required by *Interested Party* a *sender-authentcation* and a *sender-integrity* when transmitting *credible solicitor* to *Interested Party*requires *Interested Party* an *availability* level of 90% and a *receiver-authentcation* , when transmitting *best lots* to *Interested Party*; while it is required by *Interested Party* a *sender-integrity* when transmitting *best lots* to *Interested Party*.
- **CE Chambers** requires *DoUP Application* a *receiver-integrity* and a *receiver-confidentiality* , when transmitting *credible CEng* to *DoUP Application*.
- **CE Chambers** requires *DoUP Application* the *non-production* of information *list of credible CE*, and *need-to-know* of these pieces of information for the goal *credible CE provided*, when authorising *DoUP Application* to *read* and *distribute list of credible CE* in the scope of goal *credible CE provided*.
- **Solicitor Chambers** requires *DoUP Application* a *receiver-integrity* , when transmitting *credible solicitor* to *DoUP Application*; while it is required by *DoUP Application* a *sender-confidentiality* when transmitting *credible solicitor* to *DoUP Application*.
- **Solicitor Chambers** requires *DoUP Application* the *non-production* of information *list of credible sol*, and *need-to-know* of these pieces of information for the goal *cred. solitor provided*, when authorising *DoUP Application* to *read* and *distribute list of credible sol* in the scope of goal *cred. solitor provided*.
- **Aggregated REA** requires *DoUP Application* an *availability* level of 95%, when transmitting *trusted REA* to *DoUP Application*requires *DoUP Application* an *availability* level of 95%, when transmitting *best lots* to *DoUP Application*.
- **Aggregated REA** requires *DoUP Application* the *non-production* of information *list of credible REA* and *list of lots*, and *need-to-know* of these pieces of informations for the goal *citizens helped*, when authorising *DoUP Application* to *read* and *distribute list of credible REA* and *list of lots* in the scope of goal *citizens helped*.
- **Ministry of Law** requires *Real Estate Agency* the *non-modification* of information *legal info*, and *need-to-know* of these pieces of information for the goal *legal info added*, when authorising *Real Estate Agency* to *read legal info* in the scope of goal *legal info added*not-reauthorised is required since the authorization is non-transferable; while it requires *Solicitor* the *non-disclosure* of information *legal info*, and *need-to-know* of these pieces of information for the goal *legal framew provided*, when authorising *Solicitor* to *read legal info* in the scope of goal *legal framew provided*.
- *Any agent* playing *CE Chambers* is required not to play *Solicitor Chambers*, and any agent playing *Solicitor Chambers* is required not to play *CE Chambers*, given that an SoD constraint is specified between *CE Chambers* and *Solicitor Chambers*.
- *Any agent* playing *Ministry of Law* is required not to play *Solicitor*, and any agent playing *Solicitor* is required not to play *Ministry of Law*, given that an SoD constraint is specified between *Ministry of Law* and *Solicitor*.

- *Any agent* achieving *lot location defined* is required not to achieve *lot record published*, and any agent achieving *lot record published* is required not to achieve *lot location defined*, when specifying a SoD constraint between these goals.
- *Any agent* achieving *lot record published* is required not to achieve *location map added*, and any agent achieving *location map added* is required not to achieve *lot record published*, when specifying a SoD constraint between these goals.
- *Any agent* achieving *lot price approved* is required to achieve *lot location defined*, and any agent achieving *lot location defined* is required not to achieve *lot price approved*, when specifying a CoD constraint between these goals.
- *Any agent* achieving *solicitor selected* is required to achieve *CE selected*, and any agent achieving *CE selected* is required not to achieve *solicitor selected*, when specifying a CoD constraint between these goals.
- *Any agent* achieving *lot ranked* is required to achieve *lot candidate...*, and any agent achieving *lot candidate...* is required not to achieve *lot ranked*, when specifying a CoD constraint between these goals.

Responsible	Security Requirement	Requester	Description
Real Estate Agency	no-delegation (lot record created)	Lot Owner	Real Estate Agency requires no-delegation for goal lot record created ,when delegating lot record created to Real Estate Agency.
	availability (lot record created ,90%)	Lot Owner	Lot Owner require Real Estate Agency to assure an availability level of 90% for goal lot record created .
	availability (lot info,90%)	Lot Owner	Lot Owner require Real Estate Agency to assure an availability level of 90% for document lot info.
	receiver-authentication (transmitted(Real Estate Agency,Lot Owner,lot info))	Lot Owner	Lot Owner require Real Estate Agency to authenticate in order to receive document lot info.
	receiver-integrity (transmitted(Lot Owner,Real Estate Agency,lot info))	Lot Owner	Real Estate Agency shall ensure the integrity of transmission of the document lot info being transmitted.
	need-to-know (lot info details,lot geo location) (lot record created)	Lot Owner	Lot Owner requires Real Estate Agency need-to-know of Information lot info details and lot geo location, in the scope of goal lot record created .
	non-modification (legal info)	Ministry of Law	Ministry of Law requires Real Estate Agency non-modification of Information

			legal info.
	need-to-know (legal info) (legal info added)	Ministry of Law	Ministry of Law requires Real Estate Agency need-to-know of Information legal info, in the scope of goal legal info added.
	not-reauthorized ({legal info},{legal info added},{R})	Ministry of Law	Ministry of Law wants Real Estate Agency not to redistribute permissions on information {legal info} to other actors.
Map Service Provider	no-delegation (location map added)	Real Estate Agency	Map Service Provider requires no-delegation for goal location map added,when delegating location map added to Map Service Provider.
Interested Party	trustworthiness (DoUP Application, delegated(Interested Party,DoUP Application,trusted REA selected))	Interested Party	DoUP Application shall provide proof of trustworthiness for Interested Party to delegate him goal trusted REA selected.
	availability (credible CEng,90%)	DoUP Application	DoUP Application require Interested Party to assure an availability level of 90% for document credible CEng.
	receiver-authentication (transmitted(Interested Party,DoUP Application,credible CEng))	DoUP Application	DoUP Application require Interested Party to authenticate in order to receive document credible CEng.
	availability (credible solicitor,87%)	DoUP Application	DoUP Application require Interested Party to assure an availability level of 87% for document credible solicitor.
	recivier-confidentiality (transmitted(DoUP Application,Interested Party,credible solicitor))	DoUP Application	Interested Party shall ensure the confidentiality of transmission of the document credible solicitor being transmitted.
	availability (best lots,90%)	DoUP Application	DoUP Application require Interested Party to assure an availability level of 90% for document best lots.
	receiver-authentication (transmitted(Interested Party,DoUP Application,best lots))	DoUP Application	DoUP Application require Interested Party to authenticate in order to receive document best lots.
	need-to-know (list of credible CE,list of credible REA,list of credible sol,list of lots) (lot acquired)	DoUP Application	DoUP Application requires Interested Party need-to-know of Information list of credible CE, list of credible REA, list of credible sol and list of lots, in the scope of goal lot acquired.

	not-reauthorized ({list of credible CE,list of credible REA,list of credible sol,list of lots},{lot acquired},{R})	DoUP Application	DoUP Application wants Interested Party not to redistribute permissions on information {list of credible CE,list of credible REA,list of credible sol,list of lots} to other actors.
DoUP Application	no-delegation (trusted REA selected)	Interested Party	DoUP Application requires no-delegation for goal trusted REA selected,when delegating trusted REA selected to DoUP Application.
	non-repudiation-of-delegation (delegated(DoUP Application,CE Chambers,credible CE provided))	CE Chambers	CE Chambers require non-repudiation-of-delegation for goal credible CE provided,when delegated credible CE provided by DoUP Application.
	non-repudiation-of-delegation (delegated(DoUP Application,Solicitor Chambers,cred. solitor provided))	Solicitor Chambers	Solicitor Chambers require non-repudiation-of-delegation for goal cred. solitor provided,when delegated cred. solitor provided by DoUP Application.
	non-repudiation-of-delegation (delegated(DoUP Application,Aggregated REA,lot searched))	Aggregated REA	Aggregated REA require non-repudiation-of-delegation for goal lot searched,when delegated lot searched by DoUP Application.
	non-repudiation-of-delegation (delegated(DoUP Application,Aggregated REA,trusted REA selected))	Aggregated REA	Aggregated REA require non-repudiation-of-delegation for goal trusted REA selected,when delegated trusted REA selected by DoUP Application.
	recivier-confidentiality (transmitted(CE Chambers,DoUP Application,credible CEng))	CE Chambers	DoUP Application shall ensure the confidentiality of transmission of the document credible CEng being transmitted.
	receiver-integrity (transmitted(CE Chambers,DoUP Application,credible CEng))	CE Chambers	DoUP Application shall ensure the integrity of transmission of the document credible CEng being transmitted.
	receiver-integrity (transmitted(Solicitor Chambers,DoUP Application,credible solicitor))	Solicitor Chambers	DoUP Application shall ensure the integrity of transmission of the document credible solicitor being transmitted.
	availability (trusted REA,95%)	Aggregated REA	Aggregated REA require DoUP Application to assure an availability level of 95% for document trusted REA.

availability (best lots,95%)	Aggregated REA	Aggregated REA require DoUP Application to assure an availability level of 95% for document best lots.
recivier-confidentiality (transmitted(Lot Owner,DoUP Application,owner personal info))	Lot Owner	DoUP Application shall ensure the confidentiality of transmission of the document owner personal info being transmitted.
receiver-integrity (transmitted(Lot Owner,DoUP Application,owner personal info))	Lot Owner	DoUP Application shall ensure the integrity of transmission of the document owner personal info being transmitted.
sender-integrity (transmitted(Interested Party,DoUP Application,credible solicitor))	Interested Party	DoUP Application shall ensure the integrity of transmission of the document credible solicitor while being transmitted.
sender-authentication (transmitted(DoUP Application,Interested Party,credible solicitor))	Interested Party	Interested Party requires DoUP Application to be authenticated in order to transmit the document credible solicitor.
sender-integrity (transmitted(Interested Party,DoUP Application,best lots))	Interested Party	DoUP Application shall ensure the integrity of transmission of the document best lots while being transmitted.
non-production (list of credible REA,list of lots)	Aggregated REA	Aggregated REA requires DoUP Application non-production of Information list of credible REA and list of lots.
need-to-know (list of credible REA,list of lots) (citizens helped)	Aggregated REA	Aggregated REA requires DoUP Application need-to-know of Information list of credible REA and list of lots, in the scope of goal citizens helped.
need-to-know (legal info) (citizens helped)	Solicitor	Solicitor requires DoUP Application need-to-know of Information legal info, in the scope of goal citizens helped.
non-modification (VAT number,ID Card number)	Lot Owner	Lot Owner requires DoUP Application non-modification of Information VAT number and ID Card number.
need-to-know (VAT number,ID Card number) (lot owner registered)	Lot Owner	Lot Owner requires DoUP Application need-to-know of Information VAT number and ID Card number, in the scope of goal lot owner registered.
non-production	Solicitor Chambers	Solicitor Chambers requires

	(list of credible sol)		DoUP Application non-production of Information list of credible sol.
	need-to-know (list of credible sol) (cred. solitor provided)	Solicitor Chambers	Solicitor Chambers requires DoUP Application need-to-know of Information list of credible sol, in the scope of goal cred. solitor provided.
	non-production (list of credible CE)	CE Chambers	CE Chambers requires DoUP Application non-production of Information list of credible CE.
	need-to-know (list of credible CE) (credible CE provided)	CE Chambers	CE Chambers requires DoUP Application need-to-know of Information list of credible CE, in the scope of goal credible CE provided.
CE Chambers	non-repudiation-of-acceptance (delegated(DoUP Application,CE Chambers,credible CE provided))	DoUP Application	DoUP Application require non-repudiation-of-acceptance for goal credible CE provided,when delegating credible CE provided to CE Chambers.
Solicitor Chambers	non-repudiation-of-acceptance (delegated(DoUP Application,Solicitor Chambers,cred. solitor provided))	DoUP Application	DoUP Application require non-repudiation-of-acceptance for goal cred. solitor provided,when delegating cred. solitor provided to Solicitor Chambers.
	sender-confidentiality (transmitted(Solicitor Chambers,DoUP Application,credible solicitor))	DoUP Application	Solicitor Chambers shall ensure the confidentiality of transmission of the document credible solicitor while being transmitted.
Aggregated REA	non-repudiation-of-acceptance (delegated(DoUP Application,Aggregated REA,lot searched))	DoUP Application	DoUP Application require non-repudiation-of-acceptance for goal lot searched,when delegating lot searched to Aggregated REA.
	non-repudiation-of-acceptance (delegated(DoUP Application,Aggregated REA,trusted REA selected))	DoUP Application	DoUP Application require non-repudiation-of-acceptance for goal trusted REA selected,when delegating trusted REA selected to Aggregated REA.
	non-disclosure (legal info)	Real Estate Agency	Real Estate Agency requires Aggregated REA non-disclosure of Information legal info.
Solicitor	no-delegation (lot info assessed)	Interested Party	Solicitor requires no-delegation for goal lot info assessed,when delegating lot info assessed to Solicitor.
	non-disclosure (legal info)	Ministry of Law	Ministry of Law requires Solicitor non-disclosure of

			Information legal info.
	need-to-know (legal info) (legal framew provided)	Ministry of Law	Ministry of Law requires Solicitor need-to-know of Information legal info, in the scope of goal legal framew provided.
"Any agents"	achieve-in-combination (lot price approved,lot price approved)	-	Any agent that achieves one of lot price approved or lot price approved, is required to achieve the other goal too.
	not-achieve-both (lot location defined,lot location defined)	-	Any agent that achieves lot location defined or lot location defined, is required not to achieve the other goal too.
	not-achieve-both (lot record published,lot record published)	-	Any agent that achieves lot record published or lot record published, is required not to achieve the other goal too.
	achieve-in-combination (solicitor selected,solicitor selected)	-	Any agent that achieves one of solicitor selected or solicitor selected, is required to achieve the other goal too.
	not-play-both (CE Chambers,Solicitor Chambers)	-	Any agent that play CE Chambers or CE Chambers, is required not to play (adopt) the other role too.
	achieve-in-combination (lot ranked,lot ranked)	-	Any agent that achieves one of lot ranked or lot ranked, is required to achieve the other goal too.
	not-play-both (Ministry of Law,Solicitor)	-	Any agent that play Ministry of Law or Ministry of Law, is required not to play (adopt) the other role too.

Table 14 - Security Requirements for the egov Project

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

Authorisor	Information	Goal	Allowed Operations	Denyed Operations	Authorisee	Description
Lot Owner	lot info details lot geo	lot record created	R, P, T		Real Estate Agency	Transferable authority

	location					
	VAT number ID Card number	lot owner registered	R	M	DoUP Application	Transferable authority
Real Estate Agency	legal info		R	T	Aggregated REA	Transferable authority
DoUP Application	list of credible CE list of credible REA list of credible sol list of lots	lot acquired	R		Interested Party	Non-transferable authority
CE Chambers	list of credible CE	credible CE provided	R, T	P	DoUP Application	Transferable authority
Solicitor Chambers	list of credible sol	cred. solitor provided	R, T	P	DoUP Application	Transferable authority
Aggregated REA	list of credible REA list of lots	citizens helped	R, T	P	DoUP Application	Transferable authority
Ministry of Law	legal info	legal info added	R	M	Real Estate Agency	Non-transferable authority
	legal info	legal framew provided	R	T	Solicitor	Transferable authority
Solicitor	legal info	citizens helped	R, T		DoUP Application	Transferable authority

Table 15 - Authorizations in the egov project

Well-formedness Analysis

The purpose of well-formedness analysis is to verify whether the diagram for the project egov 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 egov project didn't find any errors.

Security Analysis

The purpose of security analysis is to verify whether the diagram for the project egov 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 egov has identified the problems summarised in Table 16.

Type	Category	Text	Description
ERROR	No_Delegation Violation check	"Real Estate Agency" makes an unauthorised redelegation of goal "location map added"	"Lot Owner" has expressed a no_delegation security need over the delegation of the goal "lot record created " to "Real Estate Agency", and yet "Real Estate Agency" is re-delegating goal "location map added" to "Map Service Provider"
ERROR	No_Delegation Violation check	"DoUP Application" makes an unauthorised redelegation of goal "trusted REA selected"	"Interested Party" has expressed a no_delegation security need over the delegation of the goal "trusted REA selected" to "DoUP Application", and yet "DoUP Application" is re-delegating goal "trusted REA selected" to "Aggregated REA"
ERROR	Non_Production Violation	"Map Service Provider" makes an unauthorised production of information "lot geo location"	There is no authorization relationship towards "Map Service Provider" for information "lot geo location", but "Map Service Provider" can produce "lot geo location" since there is a produce relationship from its goal "location map added" towards document "map" representing "lot geo location"
ERROR	Non_Production Violation	"Map Service Provider" makes an unauthorised production of information "lot info details"	There is no authorization relationship towards "Map Service Provider" for information "lot info details", but "Map Service Provider" can produce "lot info details" since there is a produce relationship from its goal "location map added" towards document "" representing "lot info details"

ERROR	Non_Disclosure Violation	"Solicitor" makes an unauthorised distribution of information "legal info"	"Ministry of Law" has required "Solicitor" non_disclosure of information "legal info", but "Solicitor" is distributing "legal info" to "DoUP Application" by providing document "legal framework"
ERROR	NTK Violation	"Solicitor" violates its authority performing operations in another goal scope	"Ministry of Law" has required "Solicitor" need_to_know over information "legal info", requiring "Solicitor" not to perform any operations over "legal info" other than for "legal framew provided", but "Solicitor" can perform operations over "legal info" for "lot info assessed", which is different from "legal info" and is not a subgoal of "legal info"
ERROR	Explicit non-reauthorization	"Real Estate Agency" violates its authority passing permissions without having the authority to transfer rights	"Real Estate Agency" has no authority to transfer authority to other actors, but it still authorises "legal info"
ERROR	Non-reauthorization Violation: transmit	"Solicitor" violates its authority passing permission to distribute, in an unauthorised way	"Solicitor" has no authority to distribute information "legal info", but still authorises "DoUP Application" to distribute "legal info"
ERROR	Sod Goal Violation	There is a separation of duty violation with respect to the goals "lot record published" and "location map added"	Goal "lot record published" and goal "location map added" should not be achieved by the same actor, since a separation of duty is expressed between these two goals, but "Real Estate Agency" wants to achieve them both
ERROR	Bod Goal Violation	Possible violation of binding of duties between goals, there is no agent playing the roles	Goal "solicitor selected" and goal "CE selected" 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
ERROR	Bod Goal Violation	There is a binding of duty violation with respect to the goals "lot ranked" and "lot candidate..."	Goal "lot ranked" and goal "lot candidate..." 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, "Aggregated REA" wants to achieve lot ranked but not "lot candidate..."

ERROR	Bod Goal Violation	Possible violation of binding of duties between goals, there is no agent playing the roles	Goal "lot price approved" and goal "lot location defined" 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

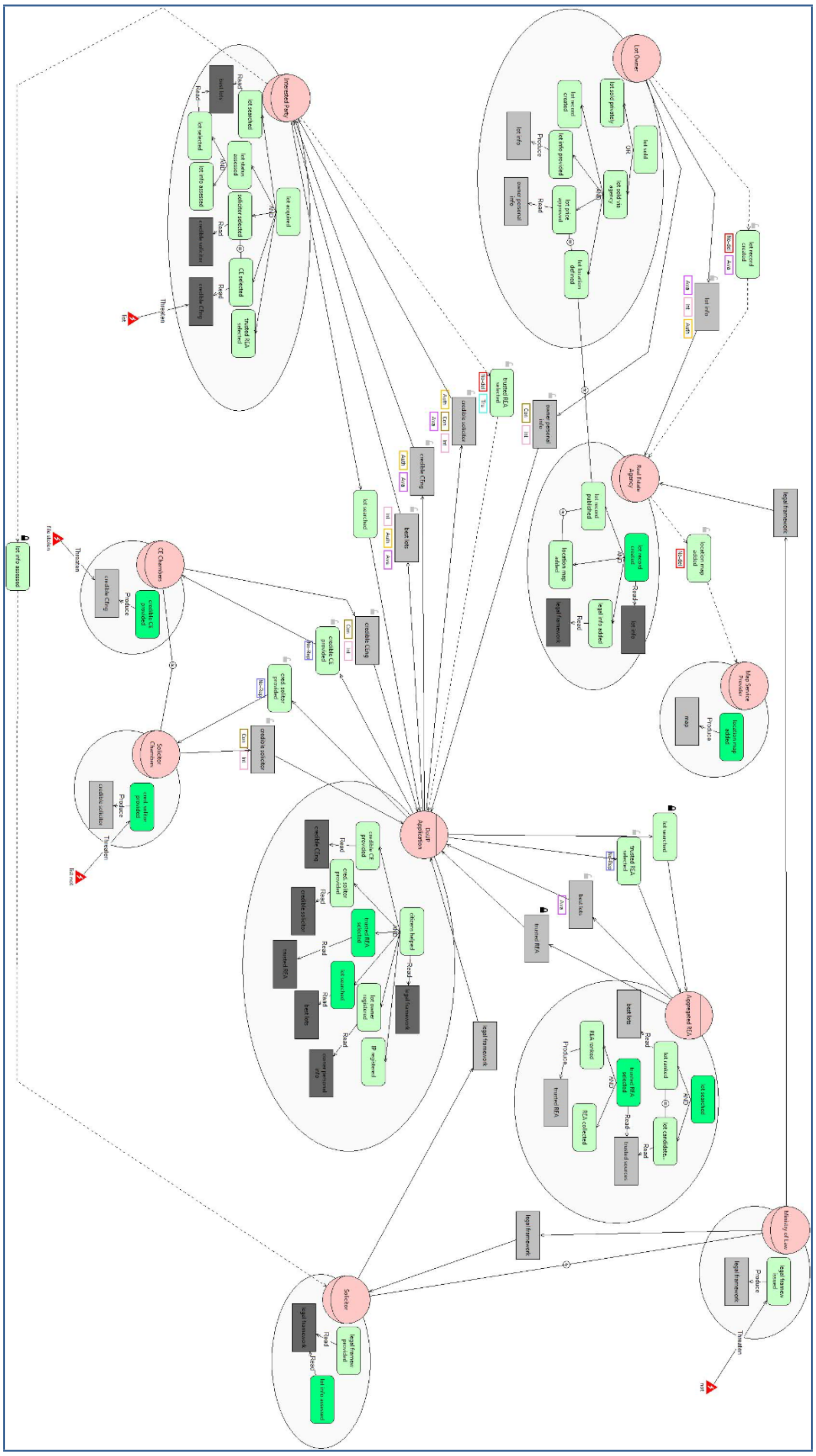

Figure 1 - Social View for the egov project

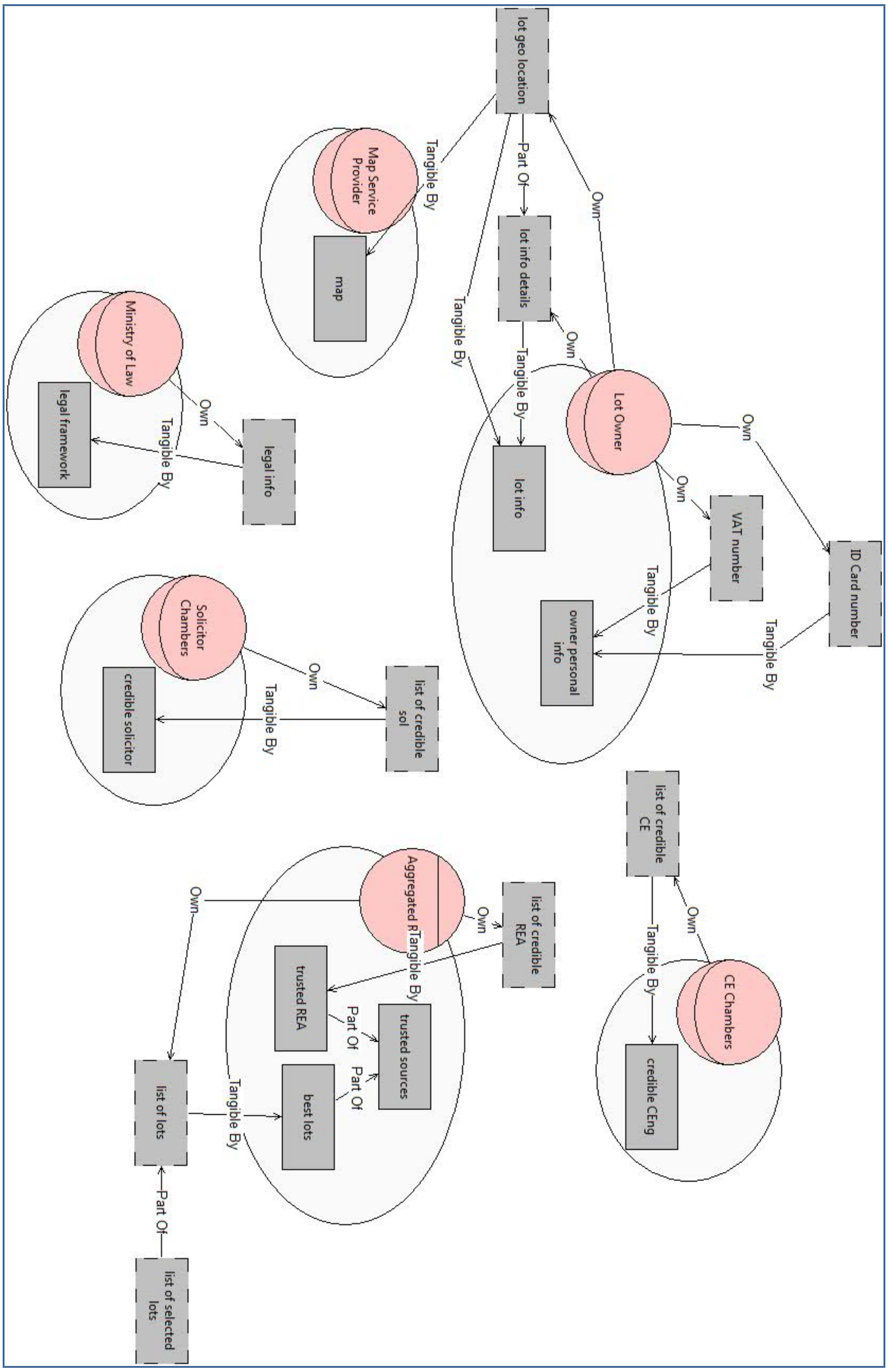

Figure 2 - Information View for the egov project

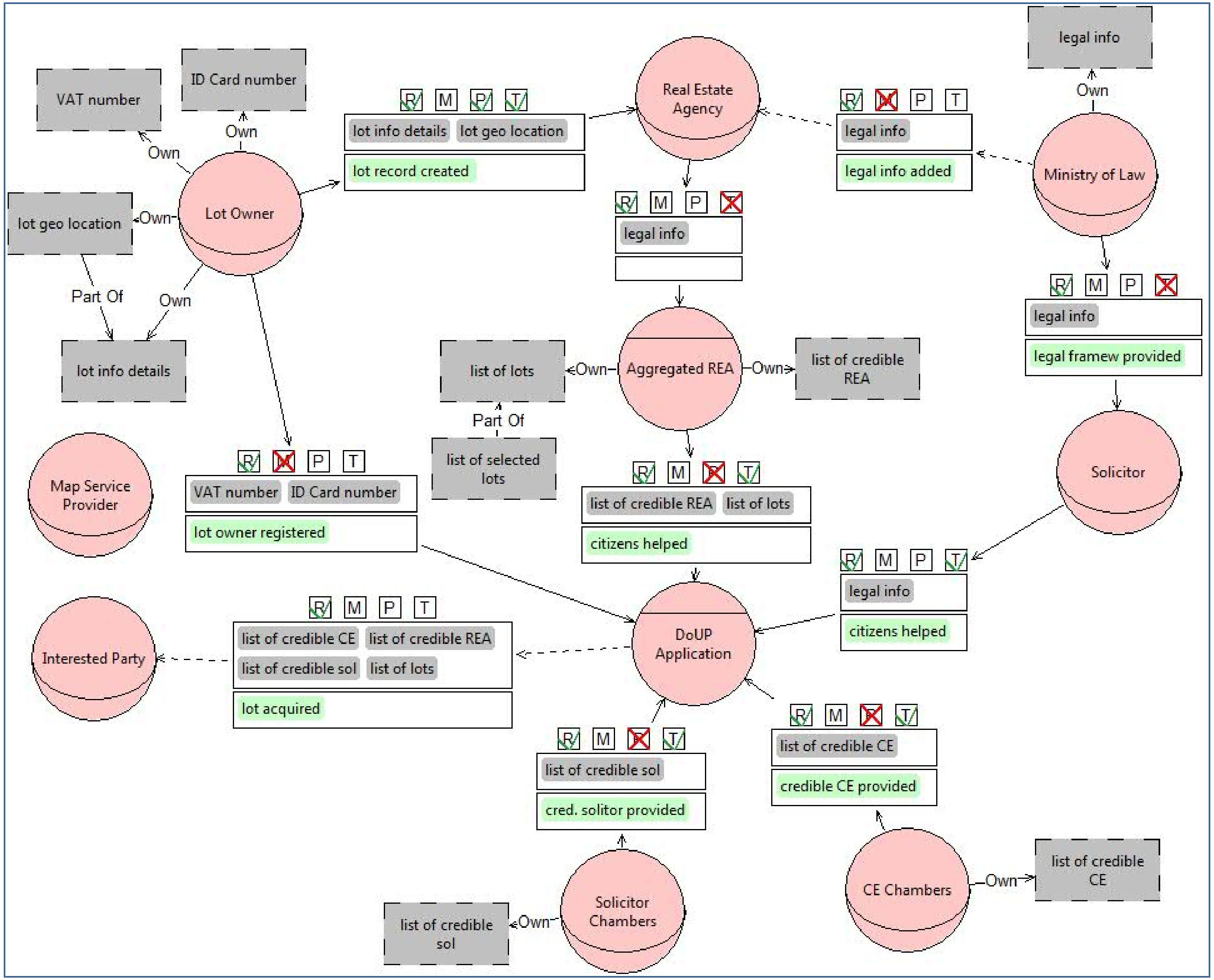

Figure 3 - Authorization View for the egov project

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.