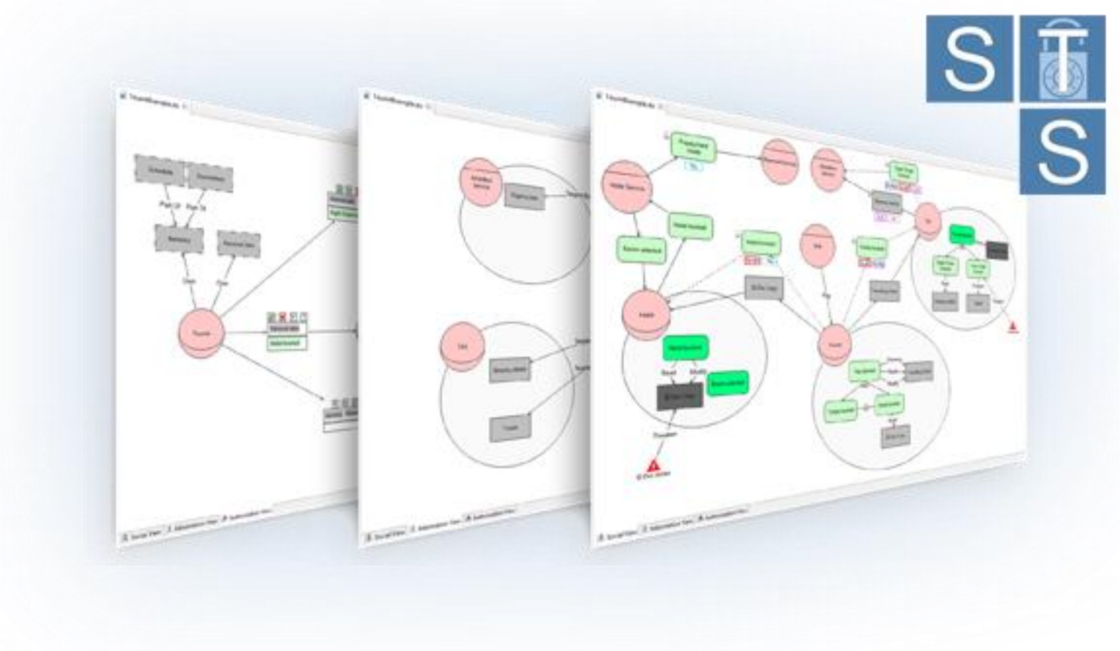
Socio-Technical Security Modeling Tool

Elda Paja

November 2014

Outline

- Installing STS-Tool
- Running example
- Tool initialization
  - Creating a diagram
- Using the tool



Installing the tool

- Go to http://www.sts-tool.eu/Downloads.php

- Download STS-Tool
  - Get the version suitable for you machine and operating system

- Installation
  - Extract the archive to a folder
  - Execute the STS-Tool binaries

Running example: eGov Lot Searching

- Department of Urban Planning (DoUP) wants to build an application which integrates the existing back-office system with the available commercial services to facilitate the interaction of involved parties when searching for a lot

  - Lot owner wants to sell the lot
    - He/she defines the lot location
    - Assigns a Real Estate Agency (REA) to create the lot record with all the lot details

  - REA has the responsibility to publish the lot record together with additional legal information arising from the current Legal Framework

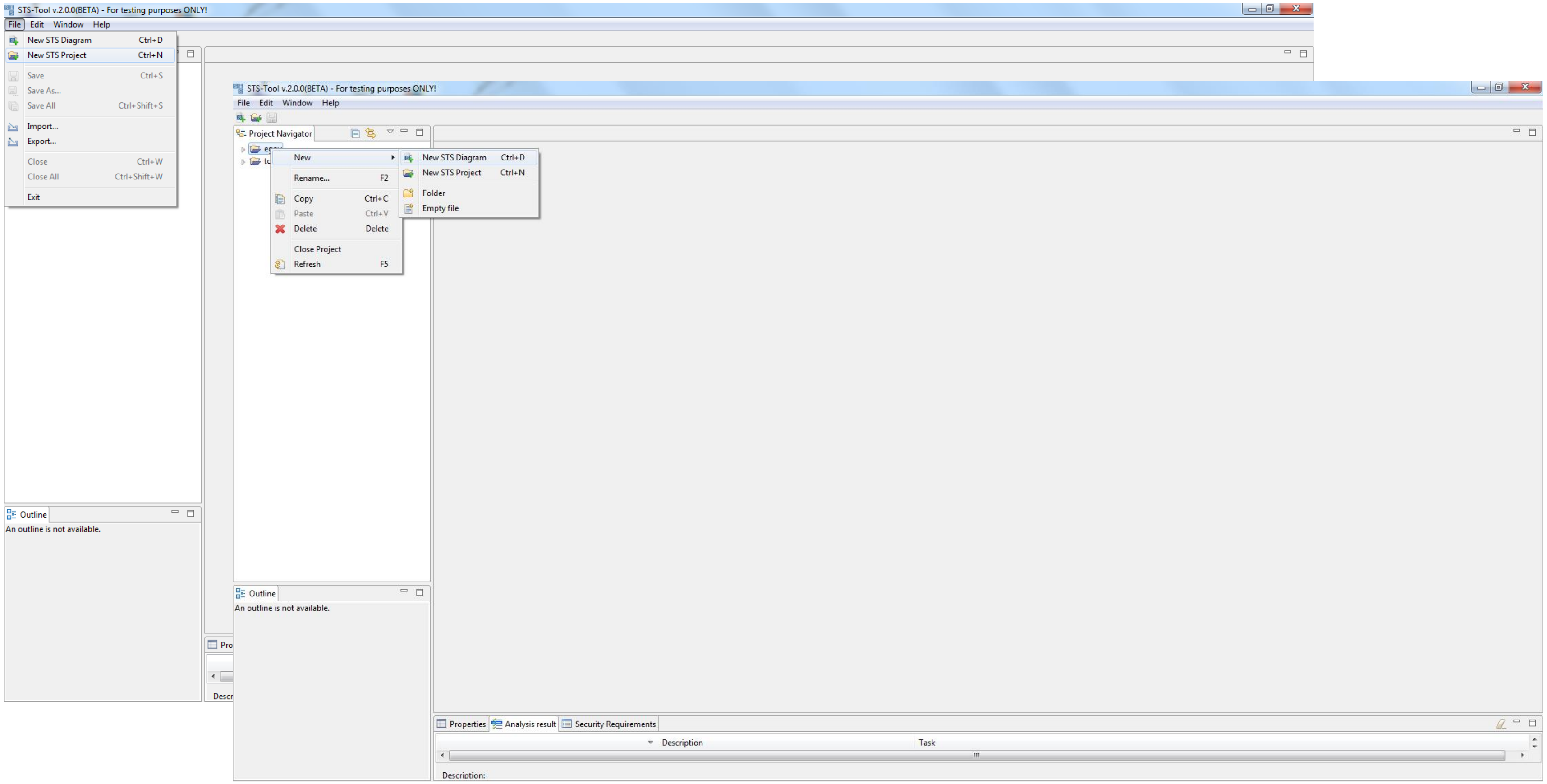
  - Ministry of Law publishes the accompanying law on building terms for the lot

Running example: eGov Lot Searching

- Interested Party is searching for a lot and
  - Accesses the DoUP application to invoke services offered by the various REAs
  - Defines a trustworthiness level to allow only trusted REAs to contact him/her
  - Sets a criteria to search and select a Solicitor and a civil engineer (CE) to asses the conditions of the lot
  - Assigns solicitor and CE to act on his/her behalf so that the lot info is available for evaluation
  - Populates the lot selection for the chosen CE and Solicitor
- Aggregated REA defines the list of trusted sources to be used to search candidate lots
  - Collect candidate lots from trusted sources
  - Rank them to visualize to the user
- The Chambers provide the list of creditable professionals (CE, Solicitors)

Hands on the tool

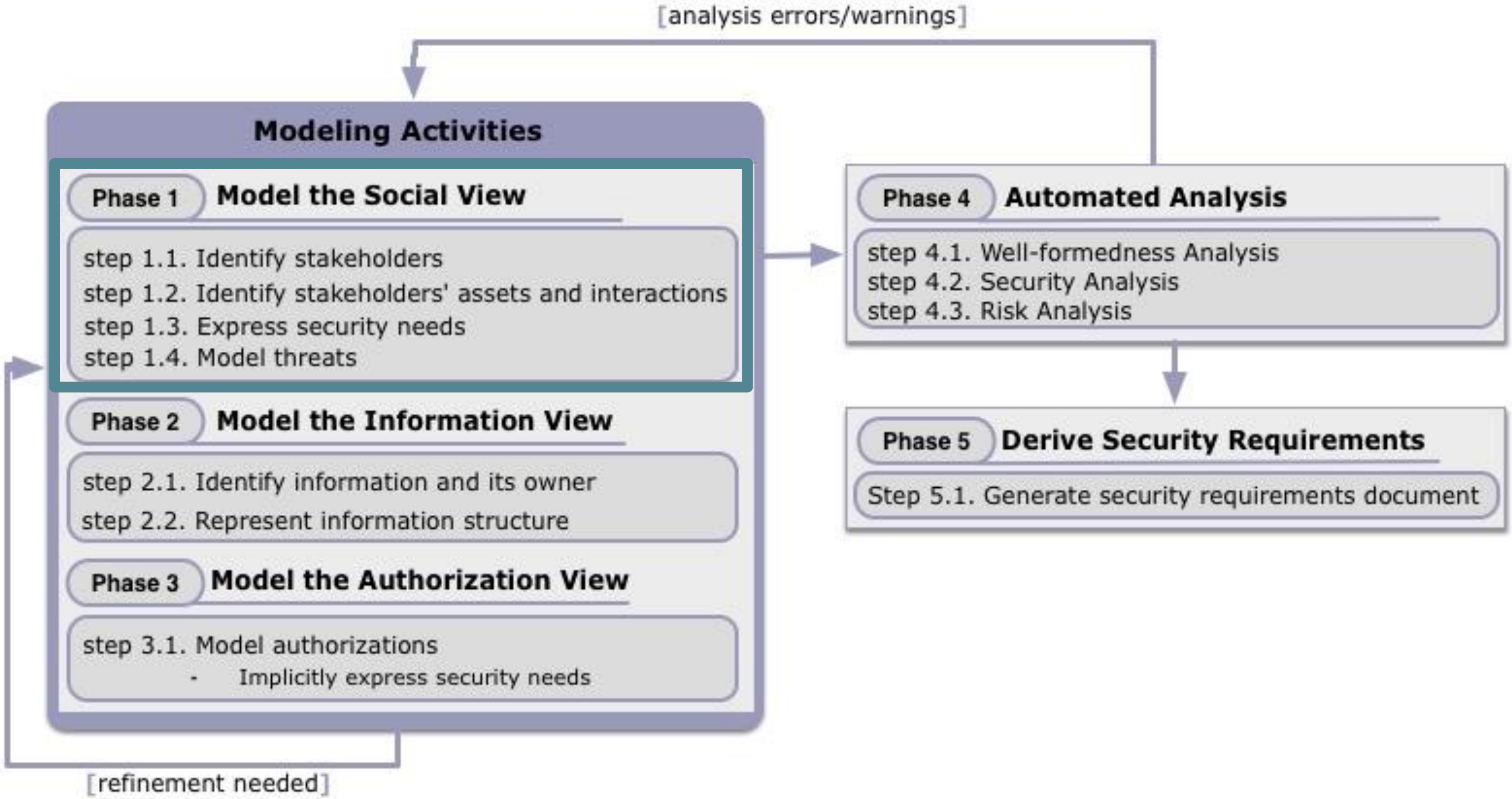
- Create a new diagram
  - File ⟶ New STS Project⟶ New STS Diagram



An outline is not available.

An outline is not available.

Phase 1: Model the Social View



[analysis errors/warnings]

Modeling Activities

Phase 1 Model the Social View

step 1.1. Identify stakeholders
step 1.2. Identify stakeholders' assets and interactions
step 1.3. Express security needs
step 1.4. Model threats

Phase 2 Model the Information View

step 2.1. Identify information and its owner
step 2.2. Represent information structure

Phase 3 Model the Authorization View

step 3.1. Model authorizations
- Implicitly express security needs

Phase 4 Automated Analysis

step 4.1. Well-formedness Analysis
step 4.2. Security Analysis
step 4.3. Risk Analysis

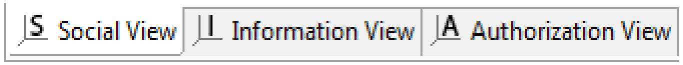
Phase 5 Derive Security Requirements

Step 5.1. Generate security requirements document

[refinement needed]

1.1 Identify Stakeholders

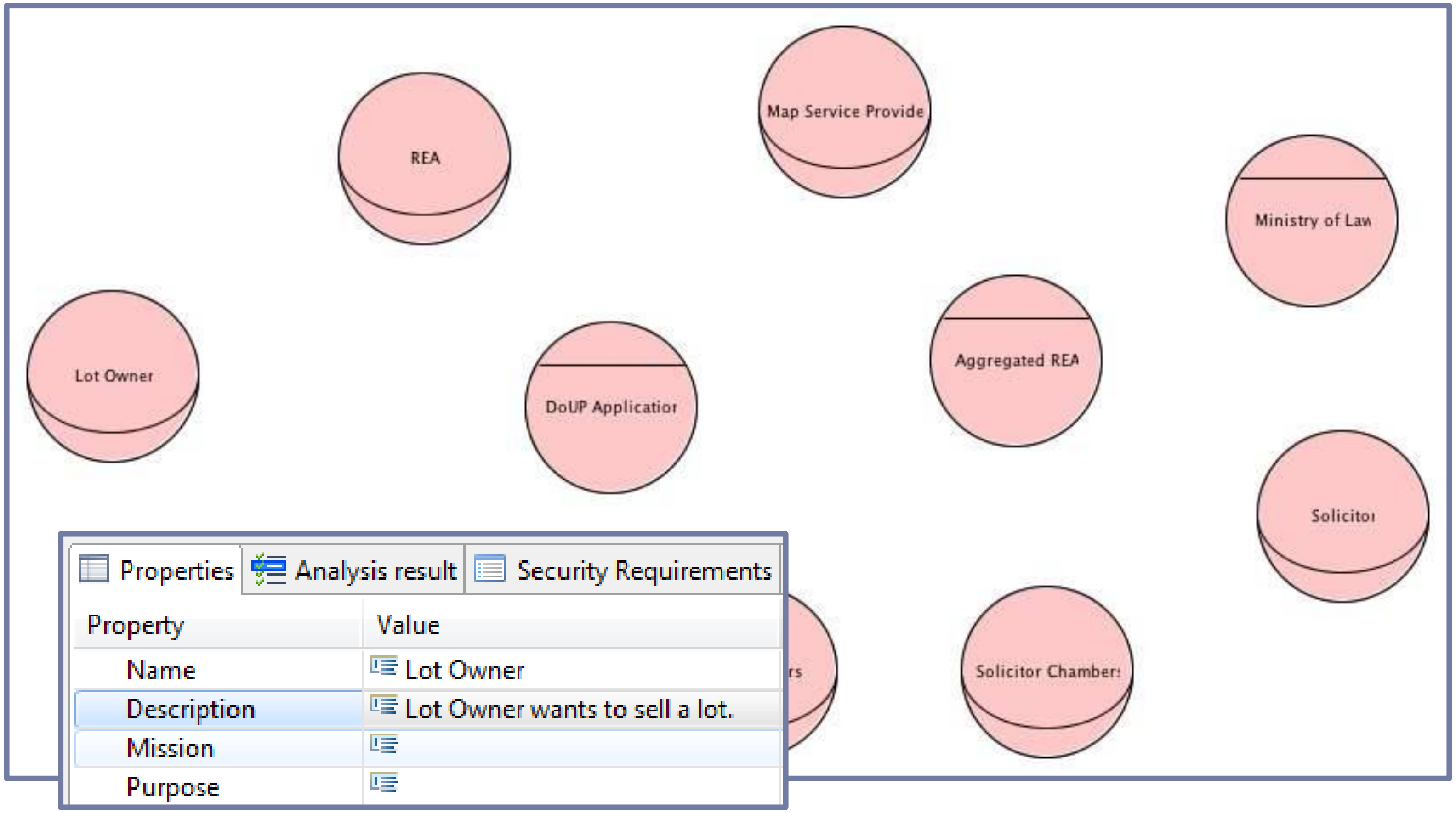
- Make sure you are on the Social View



- Draw identified roles and agents
  - Use properties to better describe the roles and agents

1.1 Identify Stakeholders

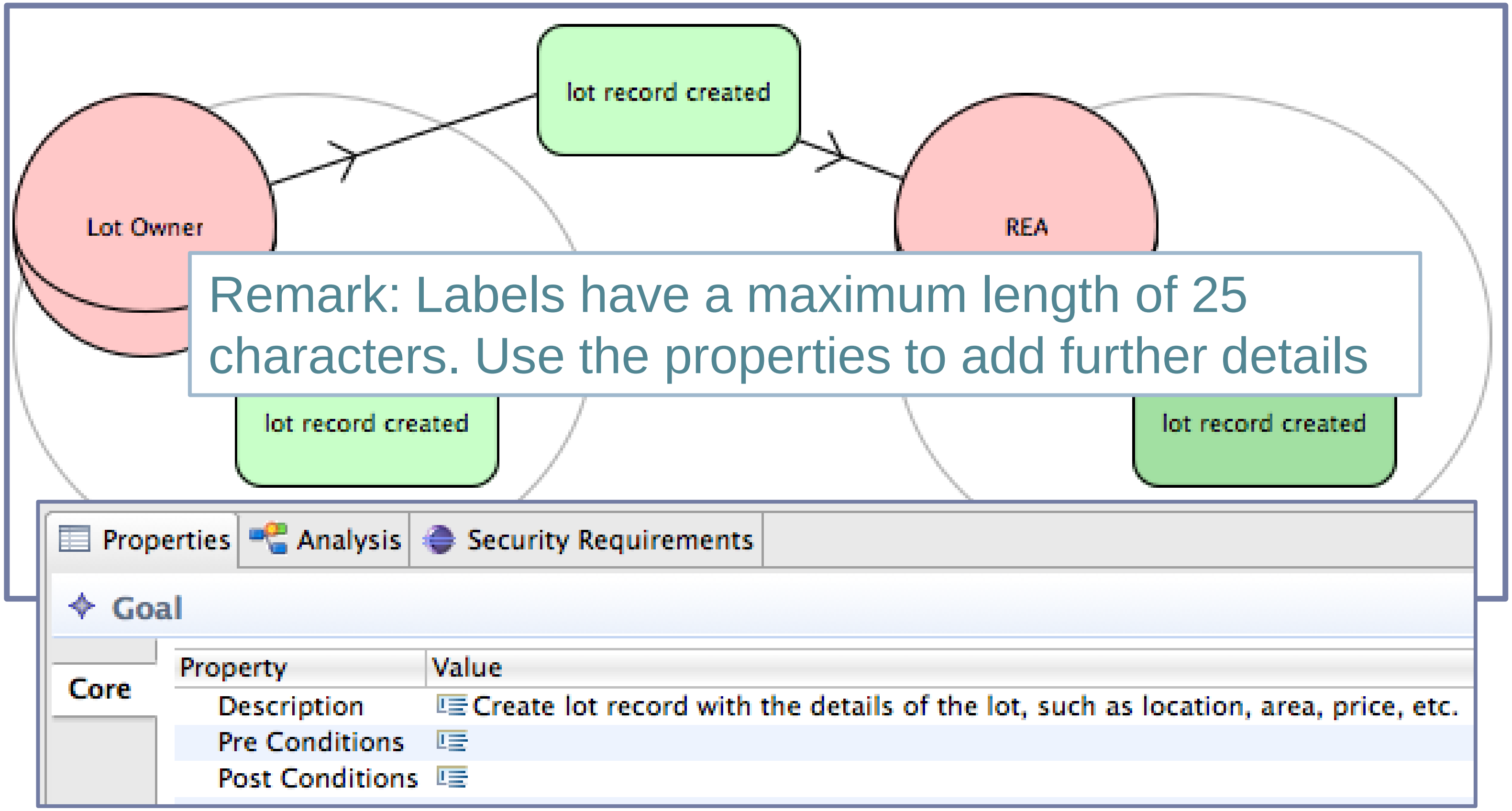
- Draw identified roles and agents
  - Use properties to better describe the roles and agents



Property	Value
Name	Lot Owner
Description	Lot Owner wants to sell a lot.
Mission	
Purpose	

1.2. Assets and Interactions

- To have the lot record published Lot Owner delegates goal lot record created to REA

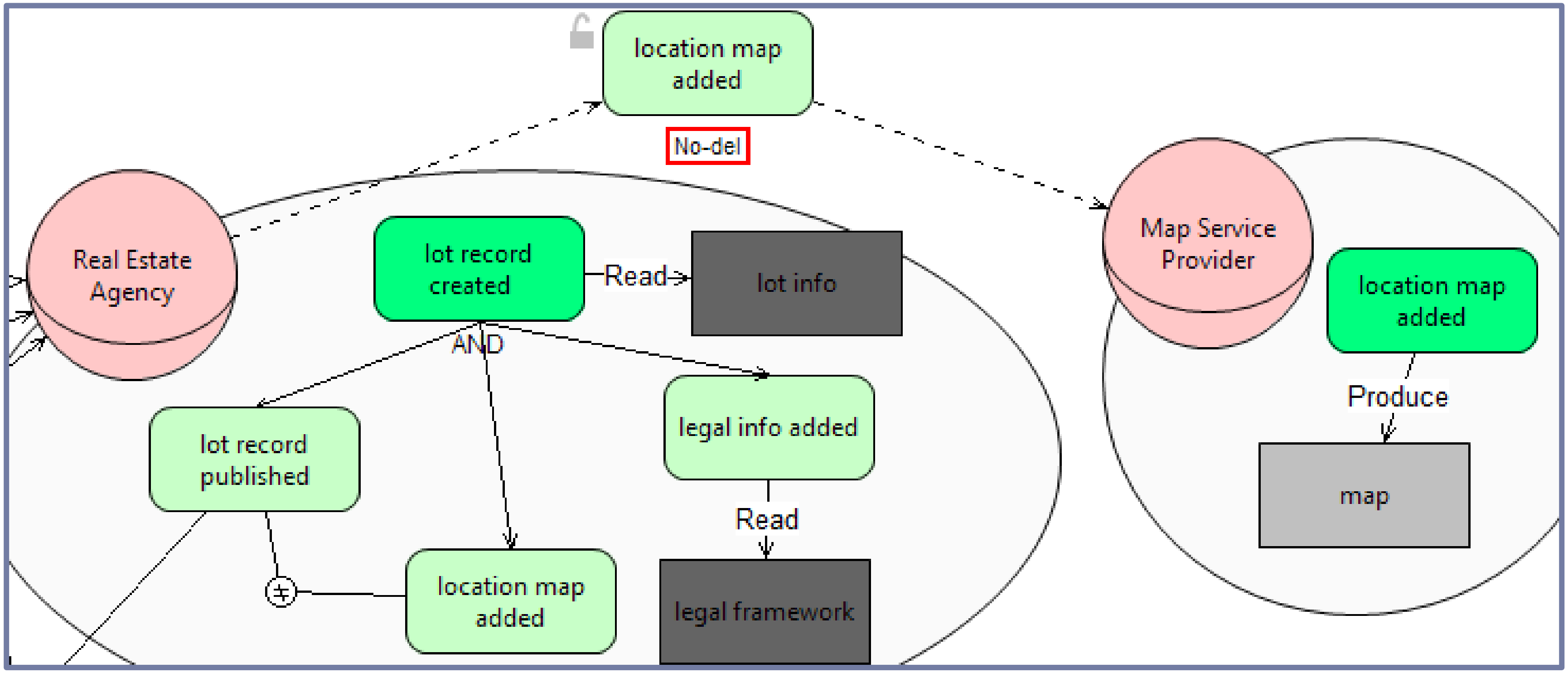


Remark: Labels have a maximum length of 25 characters. Use the properties to add further details

Property	Value
Description	Create lot record with the details of the lot, such as location, area, price, etc.
Pre Conditions	
Post Conditions	

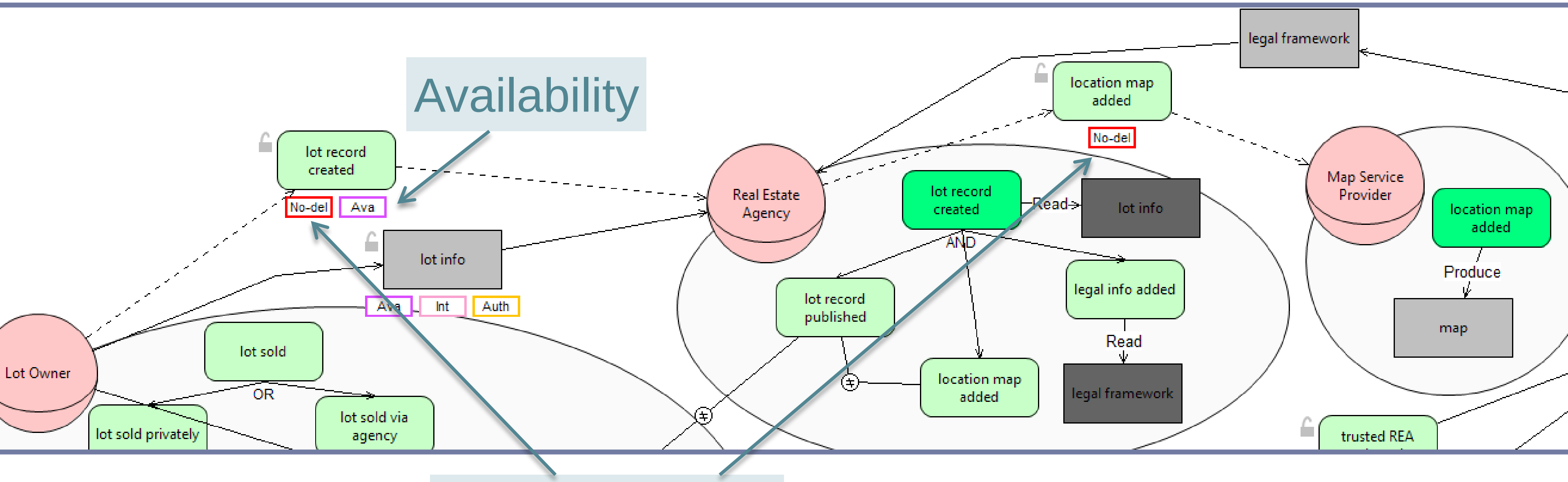
1.2. Assets and Interactions

- How can the delegatee achieve the delegated goal?
  - More details about REA
  - Goal AND/OR decompositions, Documents, Doc-Goal Relations, Re-Delegations



1.3 Express security needs

- Analyze goal delegations
  - Non-repudiation, Redundancy, No-redelegation, Trustworthiness, Availability, Authentication

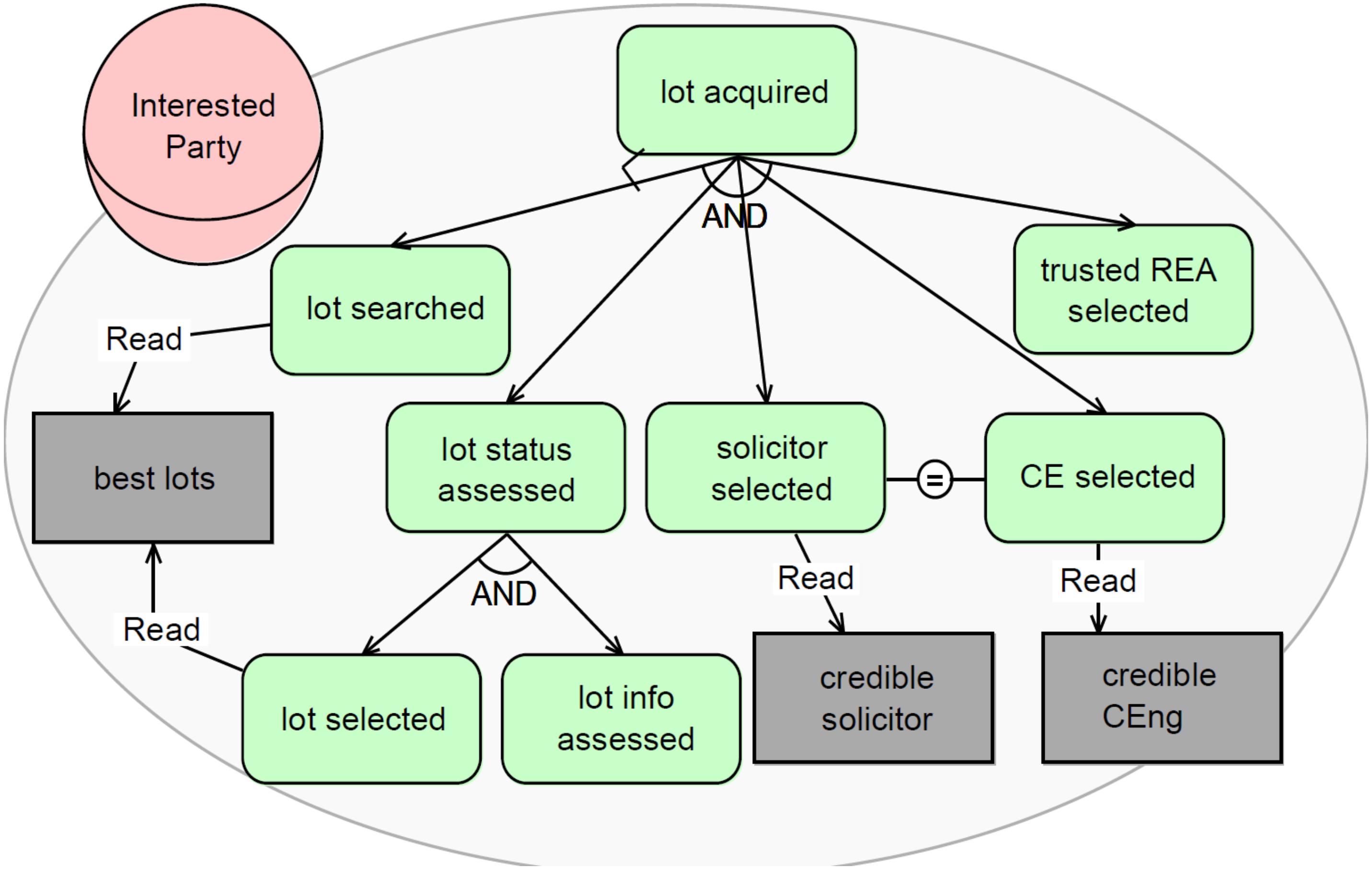


Availability

No-redelegation

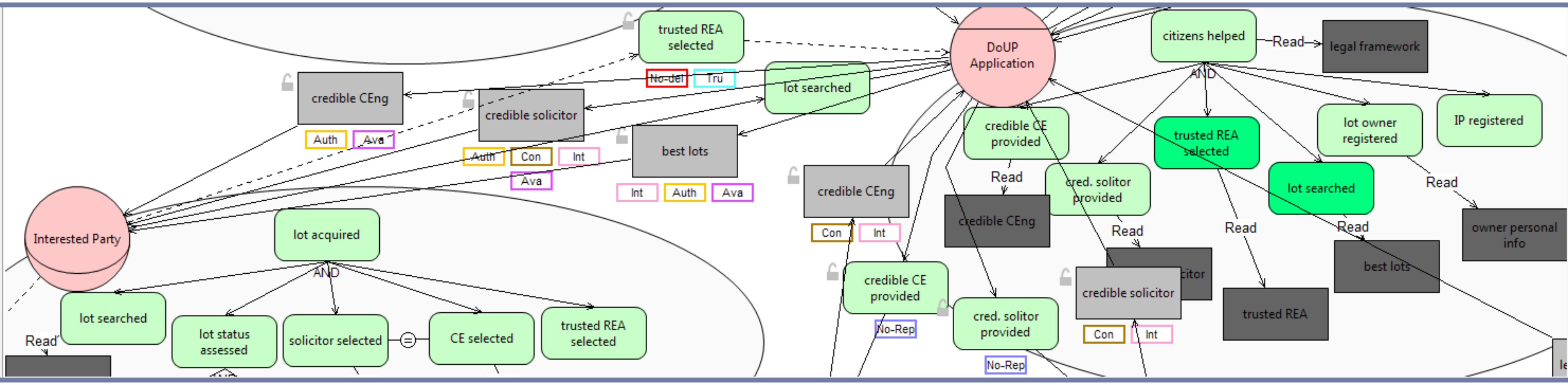
1.2. (Iteration) Assets and Interactions

- What about other parties?



1.2. (Iteration) Assets and Interactions

- Identify goal delegations and document provisions Interested Party relies upon



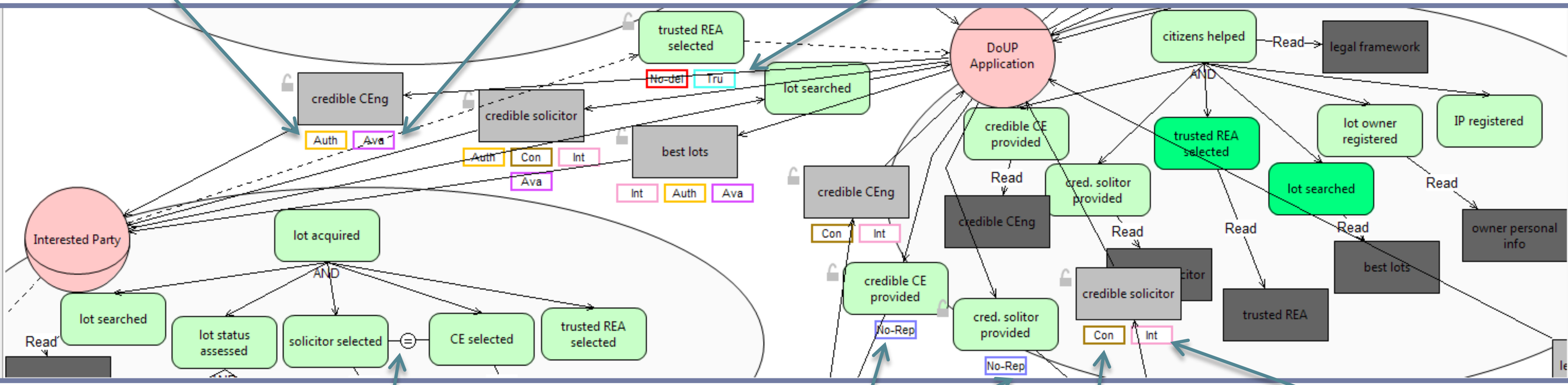
1.3. (Iteration) Expressing security needs

- Analyze goal delegations and document provisions
  - Availability, authentication
  - Non-repudiation, Trustworthiness, Separation of Duty, Binding of Duty
  - Integrity and confidentiality of transmission

Authentication

Availability

Trustworthiness



BoD

Non-repudidation

Integrity of

Confidentiality of transmission

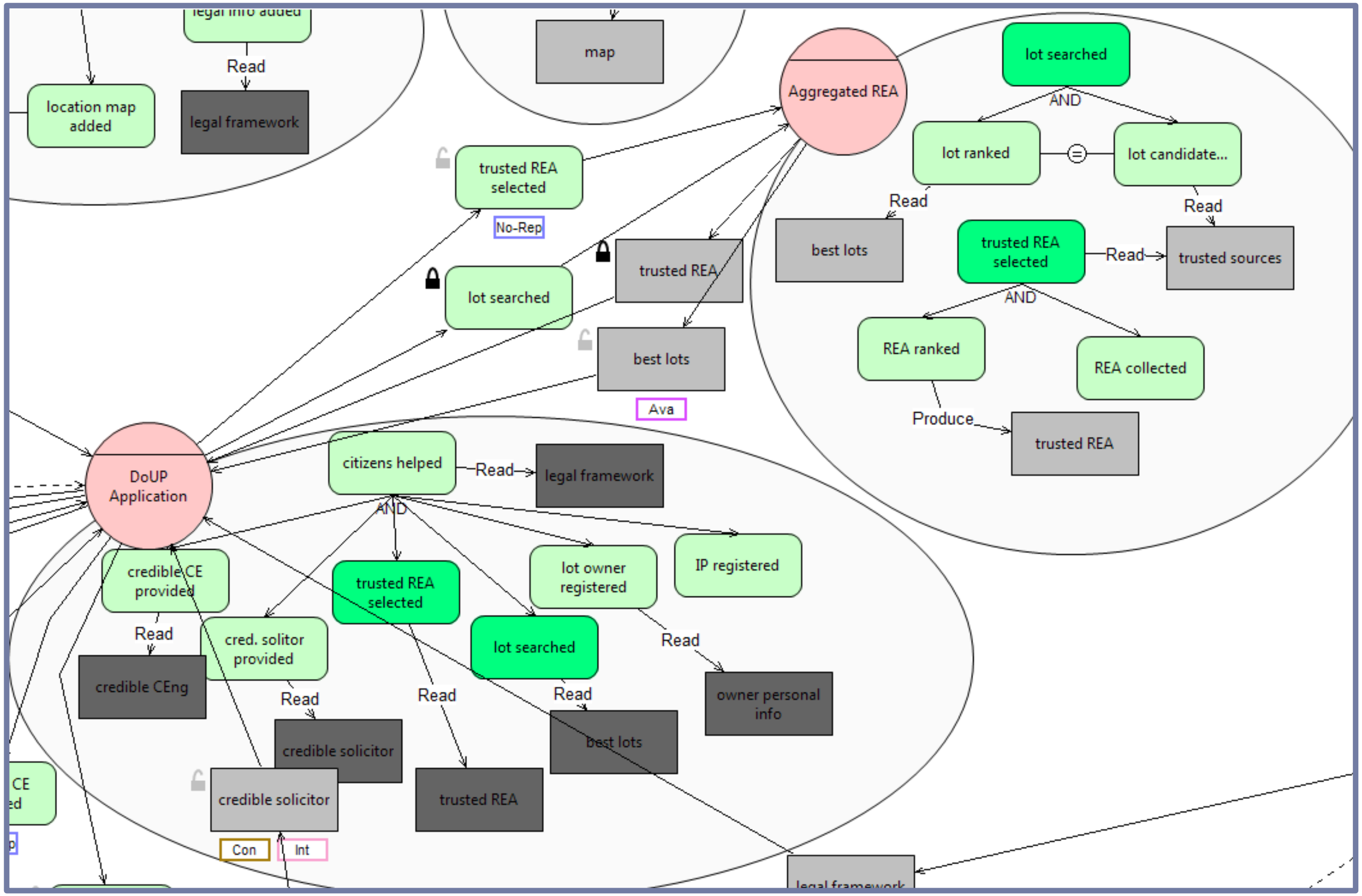
Iterative modeling process

- Steps 1.2. and 1.3. are iterative
- Continue till all actor models are built and all security needs are captured
  - Which are the remaining actors?
  - How can they achieve their goals (+ delegated goals)
    - What documents do they manipulate?
    - What actors they rely upon?
      - Goal delegations
      - Document provisions

1.2. and 1.3. Iteration

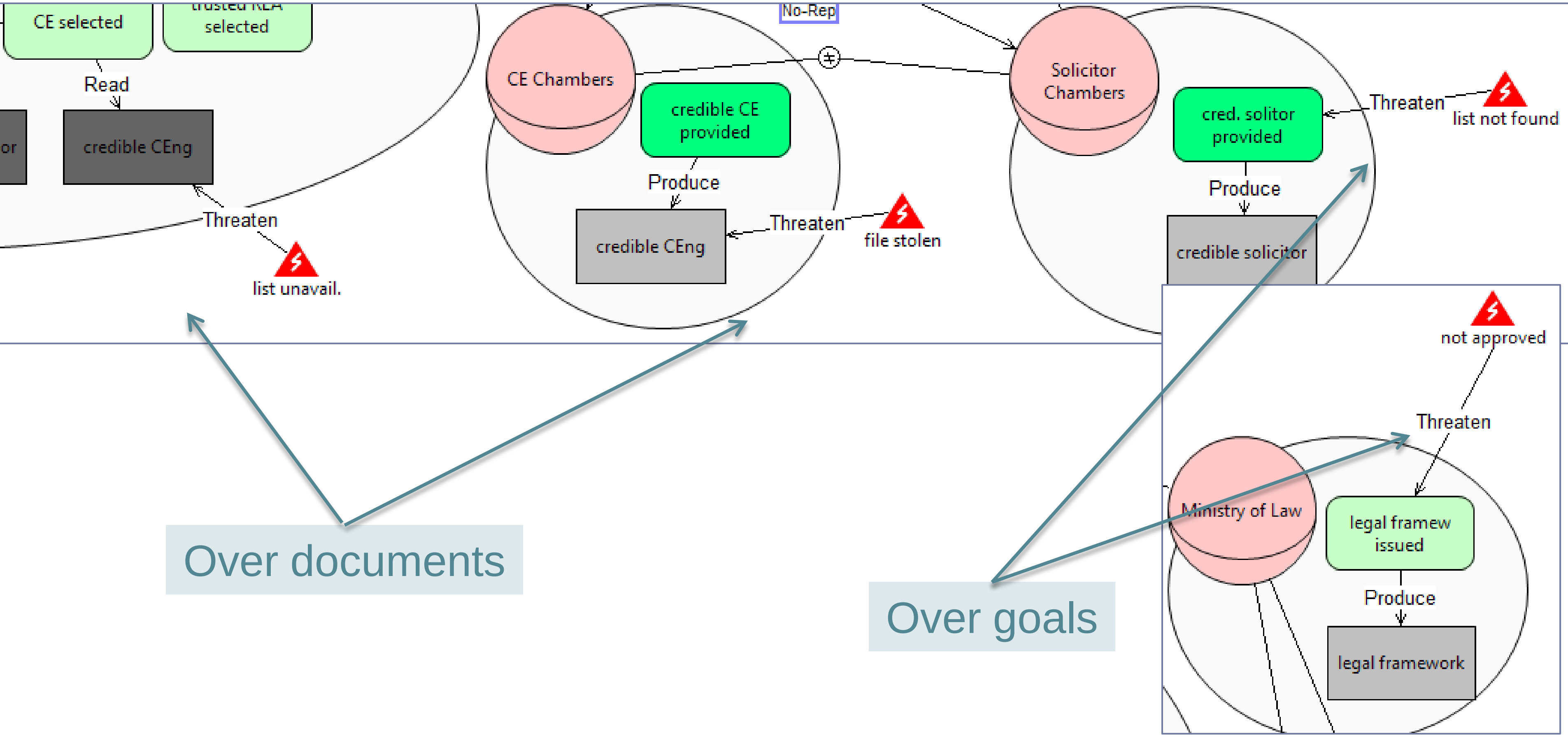
- DoUP application
- Aggregated REA
- Ministry of Law
- The Chambers
  - Solicitors’ Chambers, CE Chambers
- Solicitor

1.2. and 1.3. Iteration



1.4. Model threatening events

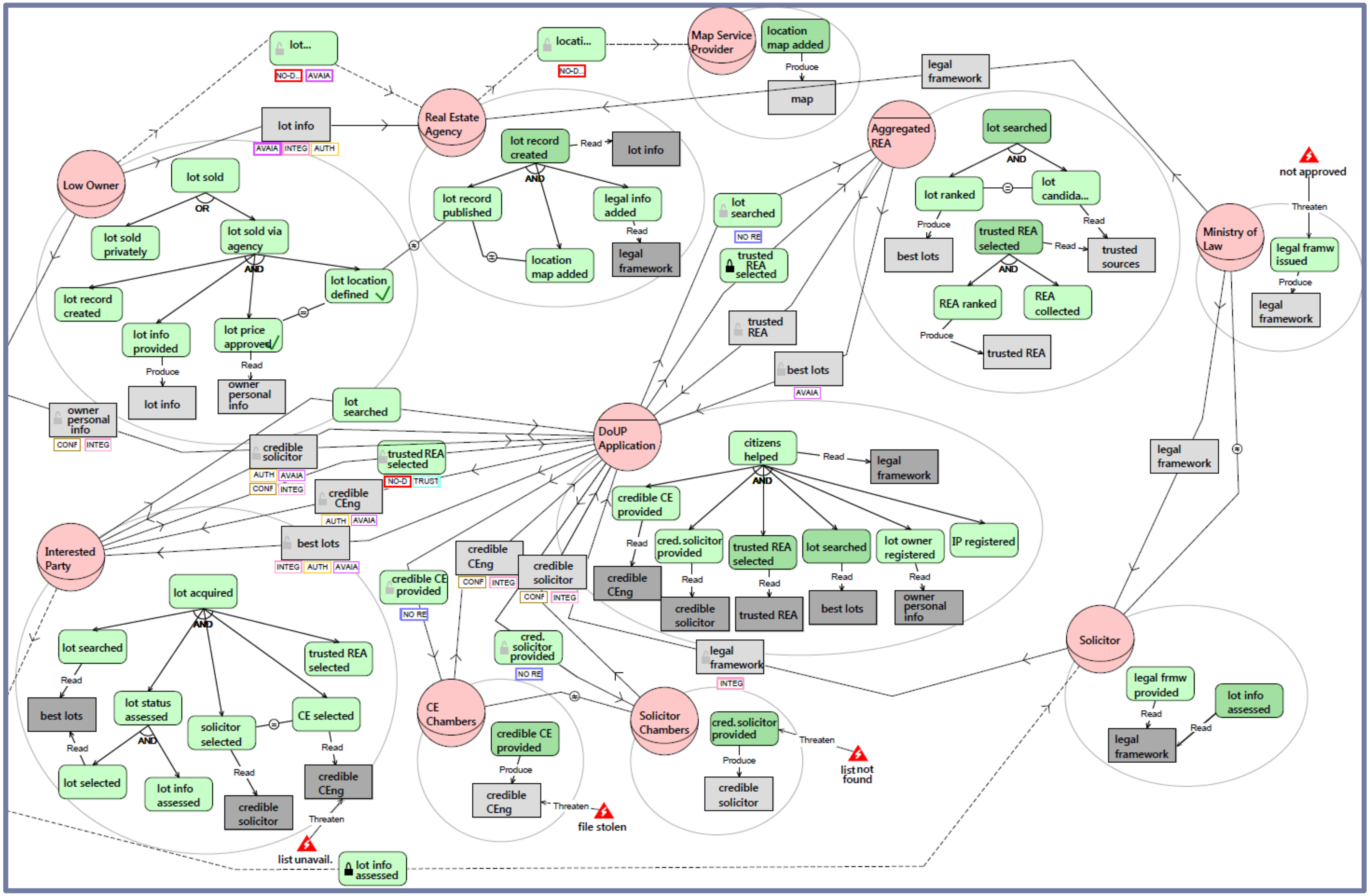
- Which actor’s goals and documents are threatened?



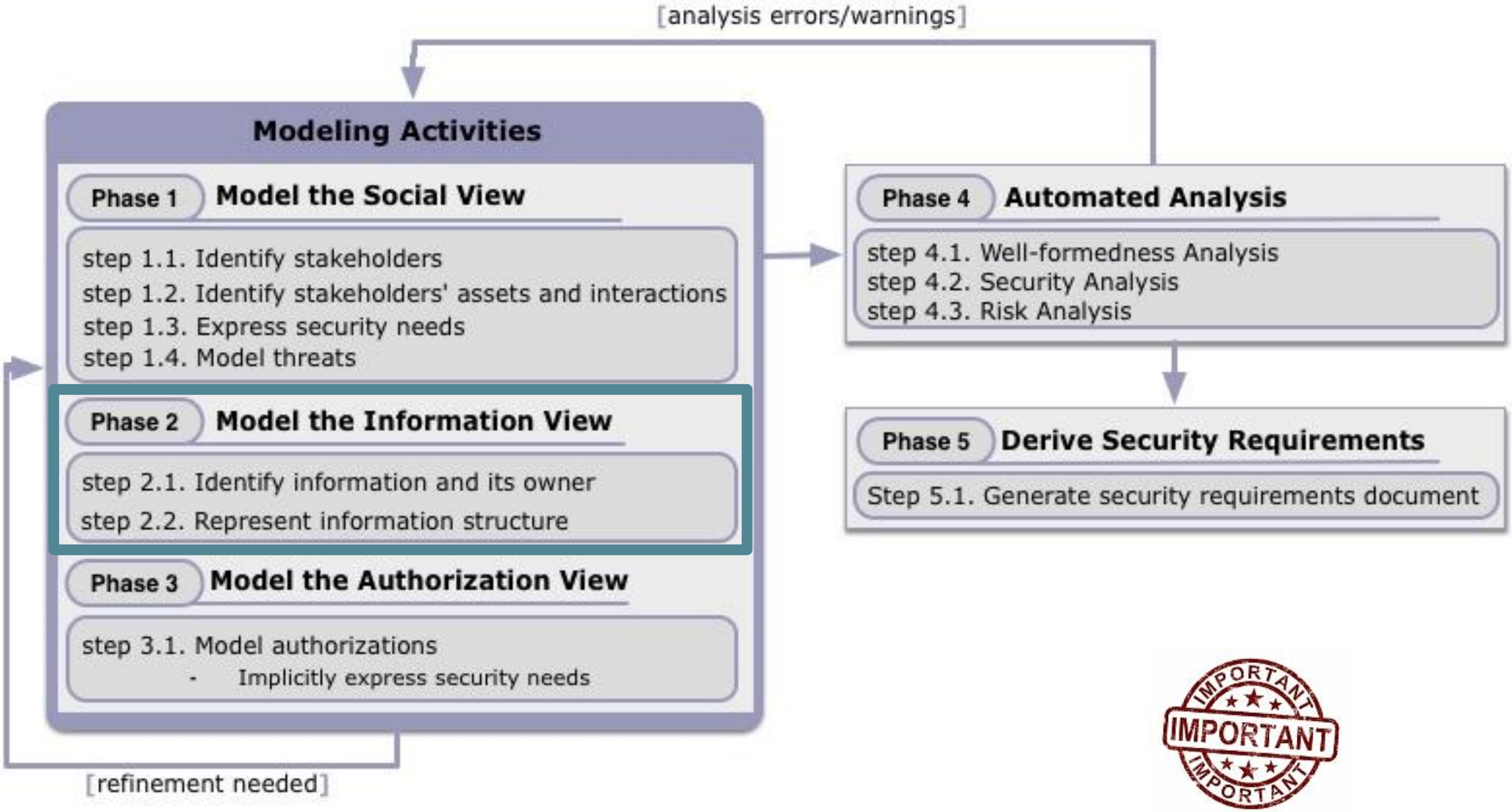
Over documents

Over goals

The Social View



Phase 2: Model the Information View



[analysis errors/warnings]

Modeling Activities

Phase 1 **Model the Social View**

step 1.1. Identify stakeholders
step 1.2. Identify stakeholders' assets and interactions
step 1.3. Express security needs
step 1.4. Model threats

Phase 2 **Model the Information View**

step 2.1. Identify information and its owner
step 2.2. Represent information structure

Phase 3 **Model the Authorization View**

step 3.1. Model authorizations
- Implicitly express security needs

[refinement needed]

Phase 4 **Automated Analysis**

step 4.1. Well-formedness Analysis
step 4.2. Security Analysis
step 4.3. Risk Analysis

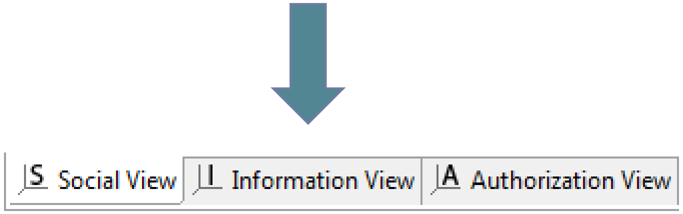
Phase 5 **Derive Security Requirements**

Step 5.1. Generate security requirements document

IMPORTANT ★★★ IMPORTANT ★★★ IMPORTANT

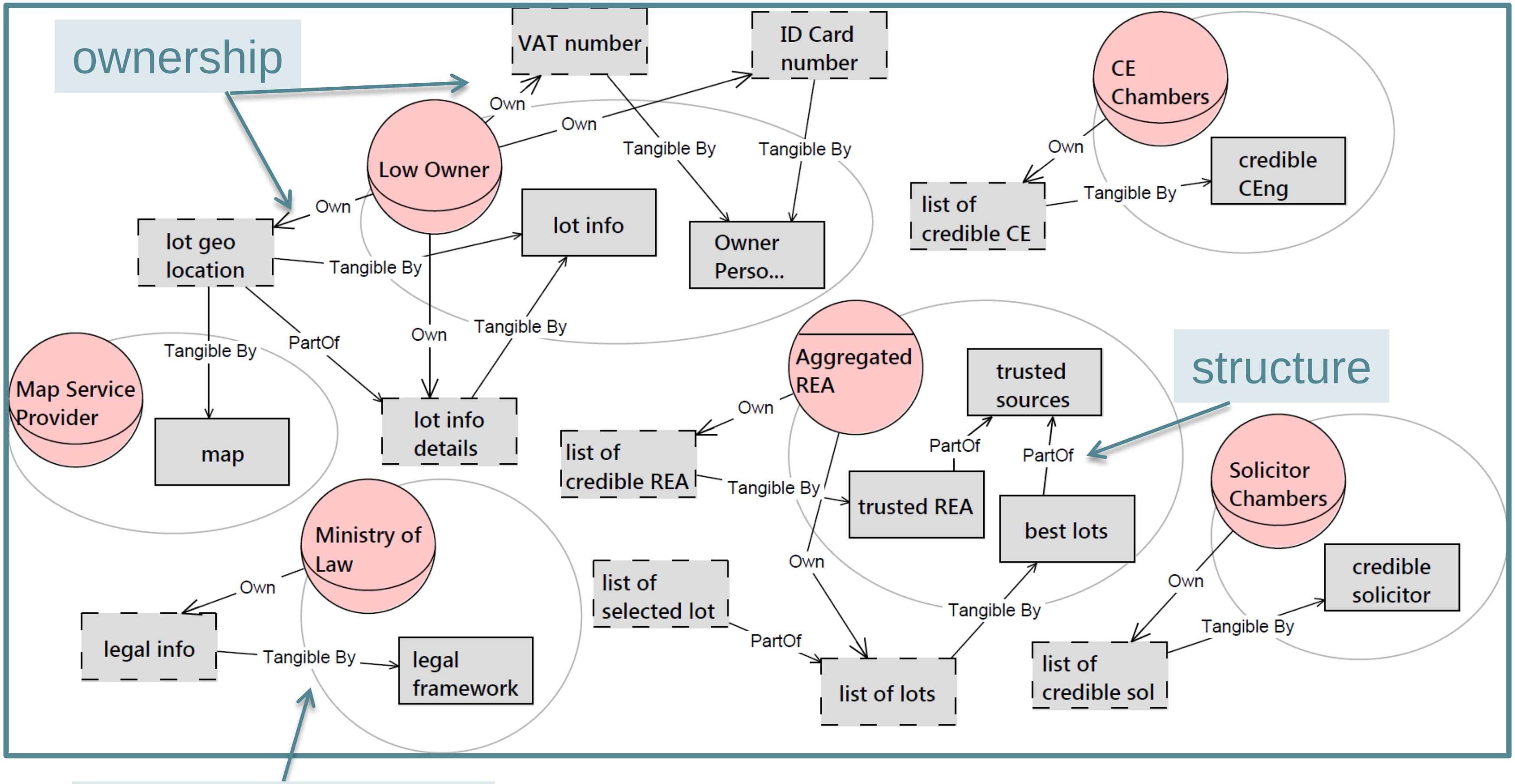
2.1. Identify information and owners

- Switch to the Information View



  - Identify information
  - Relate documents with information

2.1. and 2.2. Identify info, owners and info structure

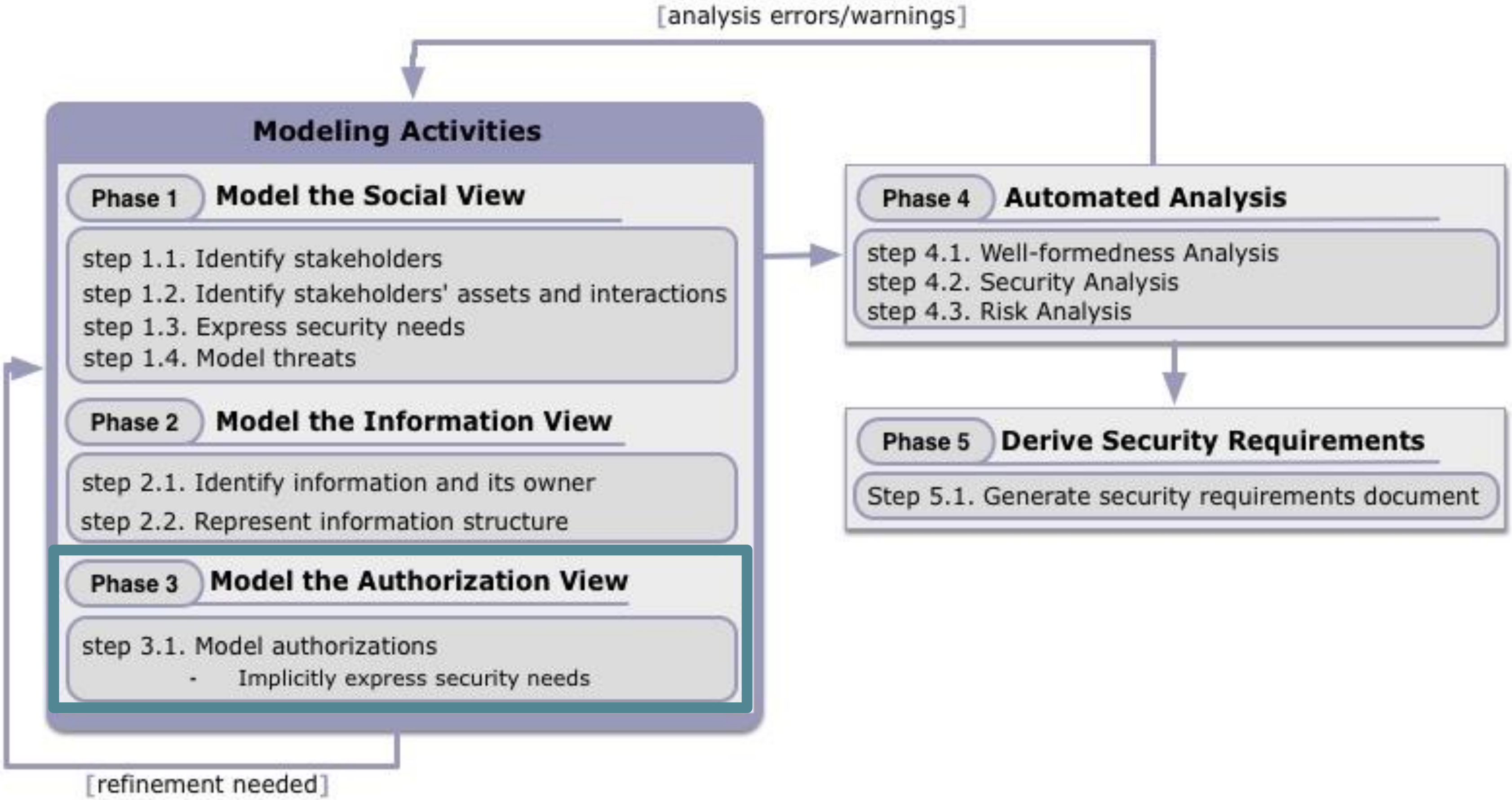


ownership

structure

info representation

Phase 3: Model the Authorization View



[analysis errors/warnings]

Modeling Activities

Phase 1 Model the Social View

step 1.1. Identify stakeholders
step 1.2. Identify stakeholders' assets and interactions
step 1.3. Express security needs
step 1.4. Model threats

Phase 2 Model the Information View

step 2.1. Identify information and its owner
step 2.2. Represent information structure

Phase 3 Model the Authorization View

step 3.1. Model authorizations
- Implicitly express security needs

Phase 4 Automated Analysis

step 4.1. Well-formedness Analysis
step 4.2. Security Analysis
step 4.3. Risk Analysis

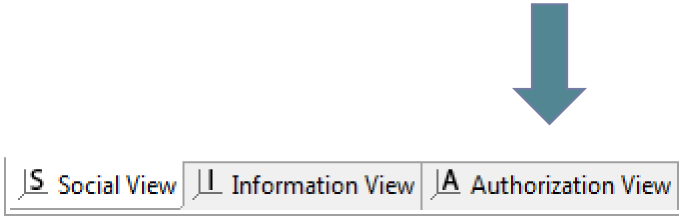
Phase 5 Derive Security Requirements

Step 5.1. Generate security requirements document

[refinement needed]

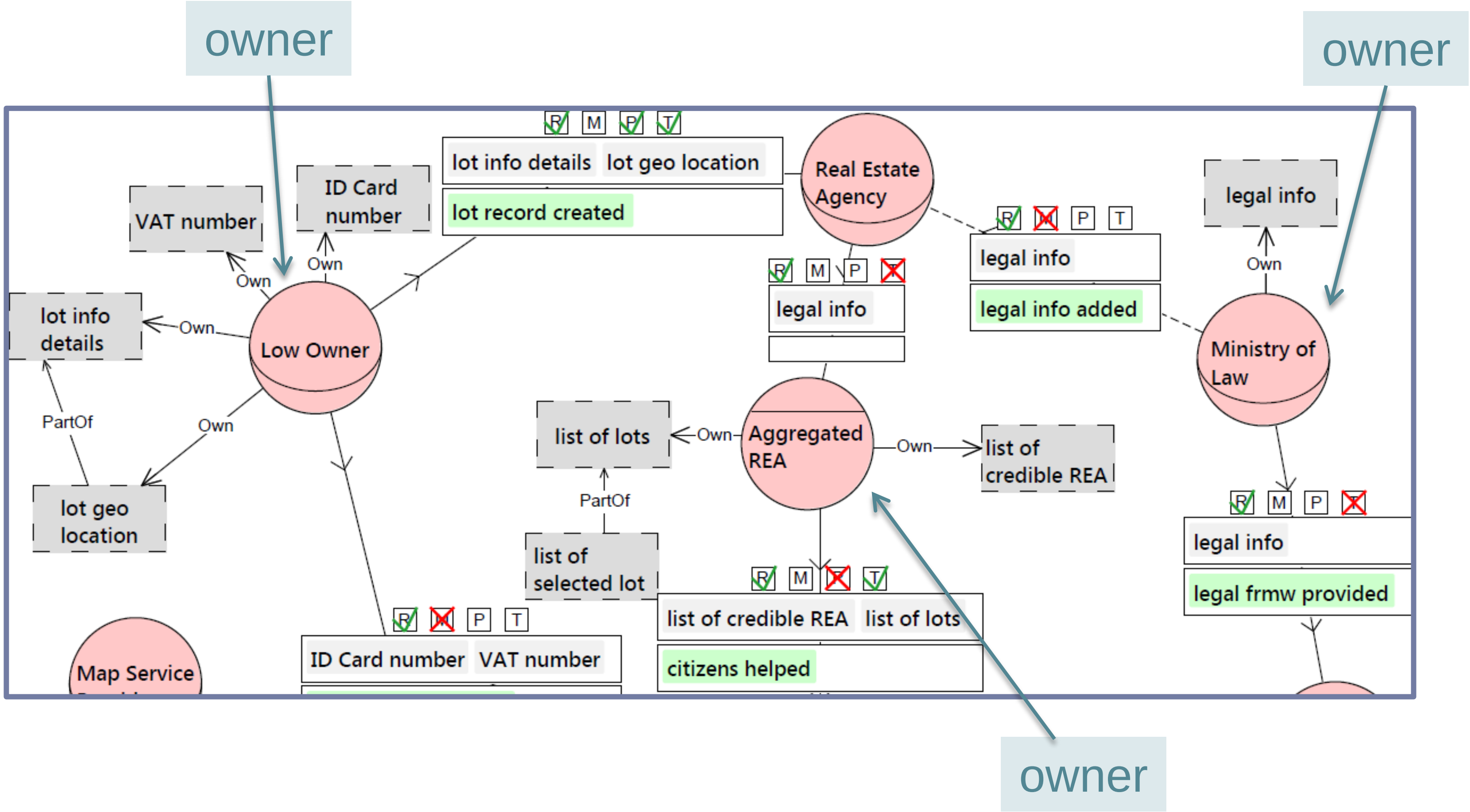
3.1. Model authorizations

- Switch to the Authorization View



  - Starting from information owners
  - Is authority to transfer authorizations granted?

3.1. Model authorizations



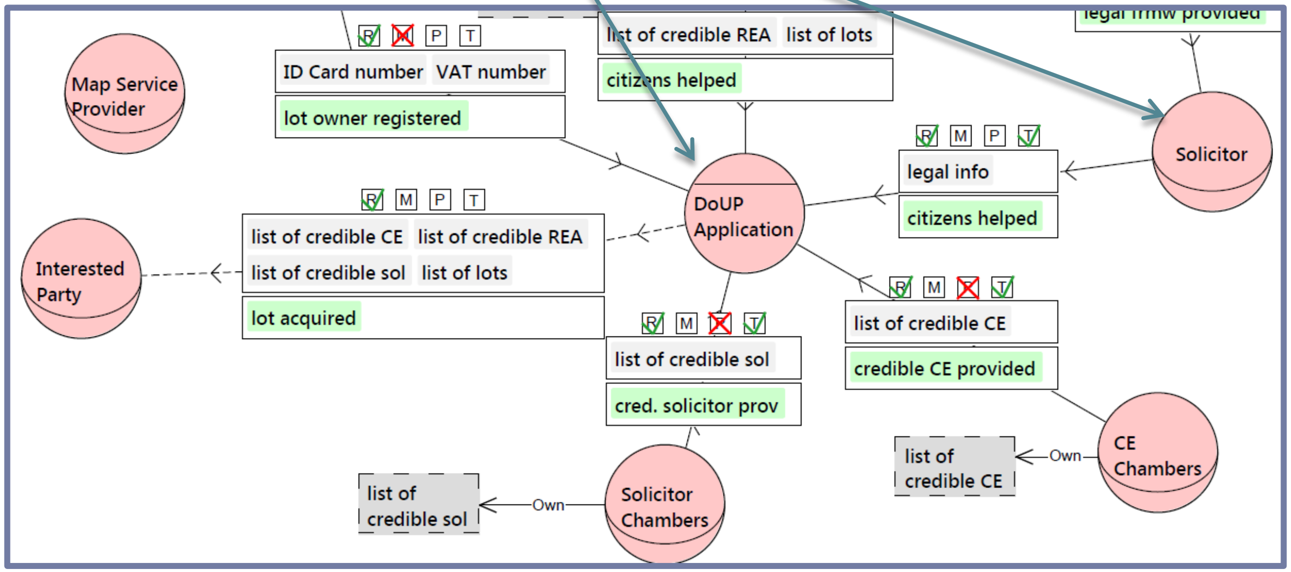
owner

owner

owner

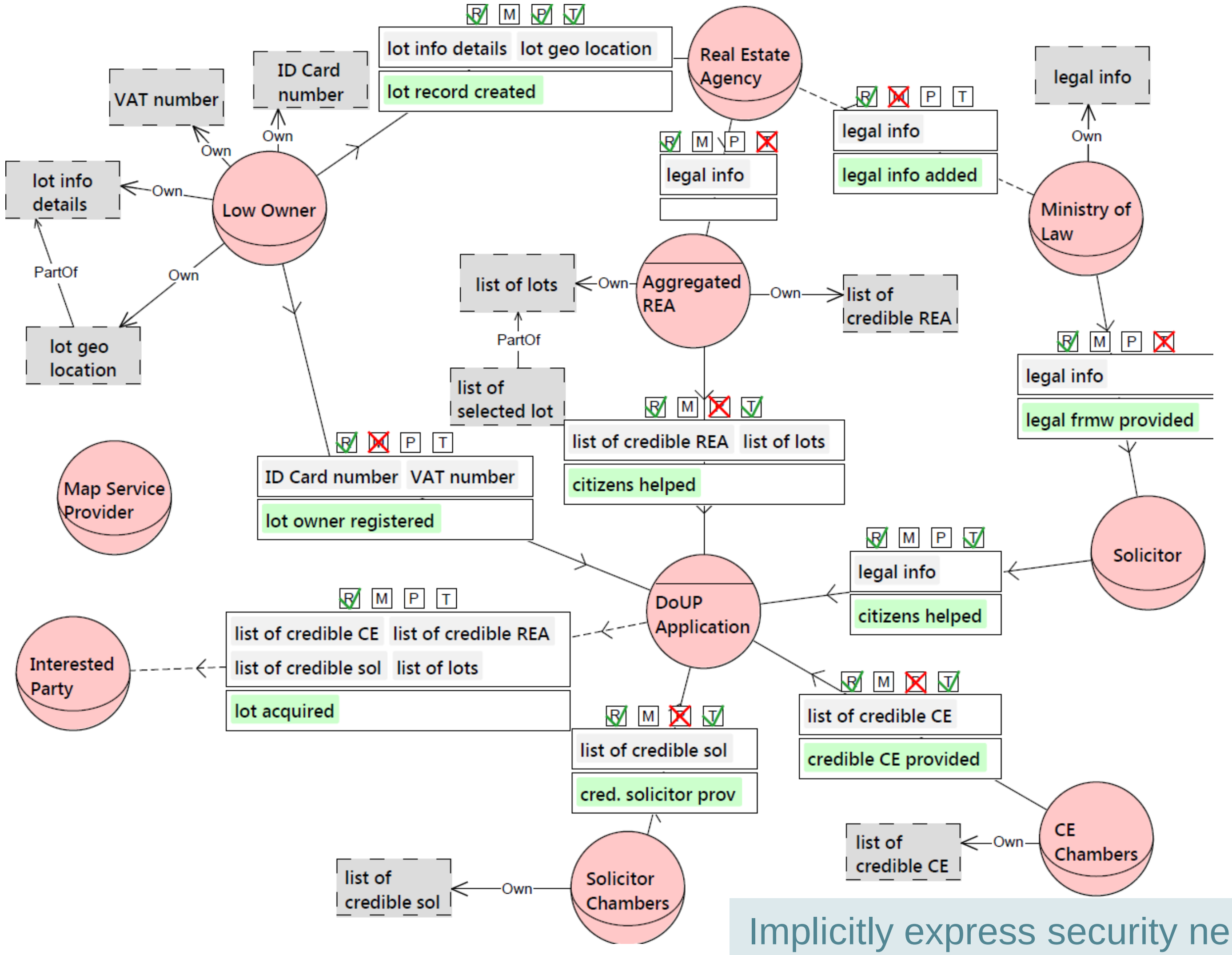
3.1. Model authorizations

Authorized party



Implicitly express security needs

Authorization view

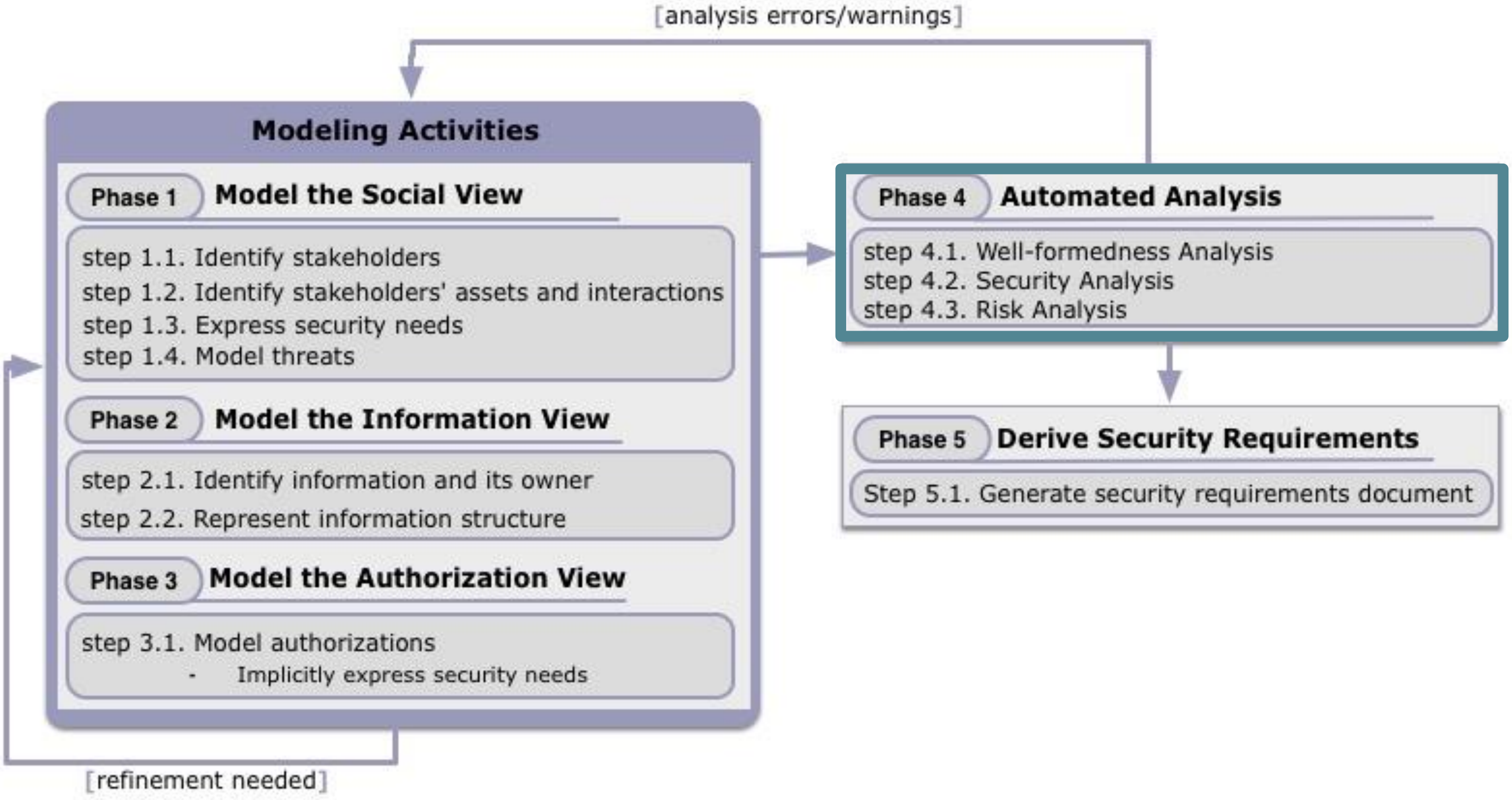


Implicitly express security needs

… and now?

- Iterative modeling
  - The views can be refined
  - Changes in one view have effects on the other views
- Termination criteria
  - Did I capture all important interconnections?
  - Did I express all the security needs?
- Use properties to better describe the model

Phase 4: Automated Analysis



[analysis errors/warnings]

Modeling Activities

Phase 1 **Model the Social View**

step 1.1. Identify stakeholders
step 1.2. Identify stakeholders' assets and interactions
step 1.3. Express security needs
step 1.4. Model threats

Phase 2 **Model the Information View**

step 2.1. Identify information and its owner
step 2.2. Represent information structure

Phase 3 **Model the Authorization View**

step 3.1. Model authorizations
- Implicitly express security needs

Phase 4 **Automated Analysis**

step 4.1. Well-formedness Analysis
step 4.2. Security Analysis
step 4.3. Risk Analysis

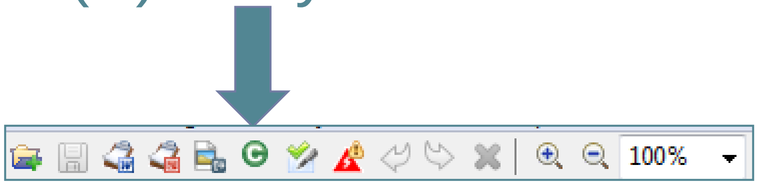
Phase 5 **Derive Security Requirements**

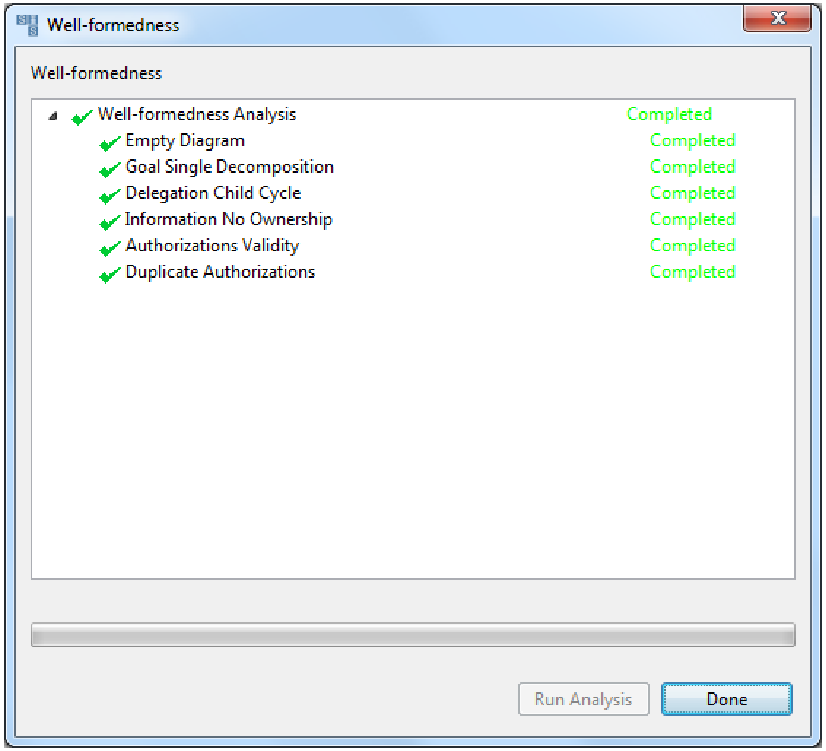
Step 5.1. Generate security requirements document

[refinement needed]

4.1. Well-formedness Analysis

- Go to the well-formedness (C) analysis tab



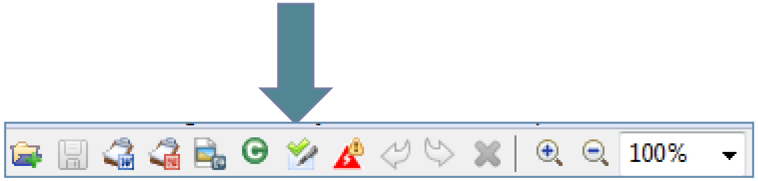


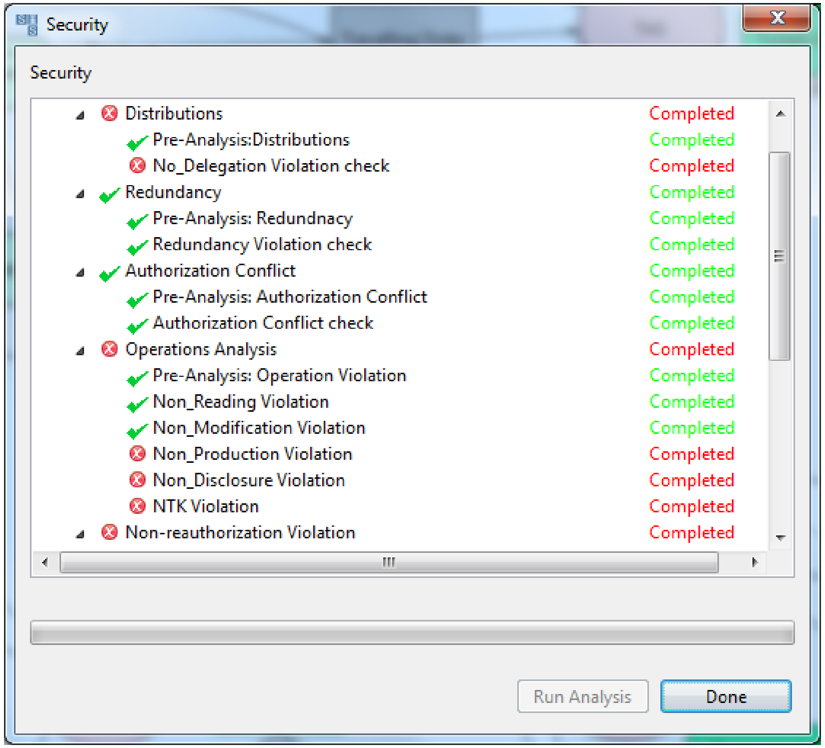
Well-formedness

```
◢ ✓ Well-formedness Analysis                 Completed
    ✓ Empty Diagram                            Completed
    ✓ Goal Single Decomposition                Completed
    ✓ Delegation Child Cycle                   Completed
    ✓ Information No Ownership                 Completed
    ✓ Authorizations Validity                  Completed
    ✓ Duplicate Authorizations                 Completed
```

4.2. Security Analysis

- Go to the Security Analysis tab

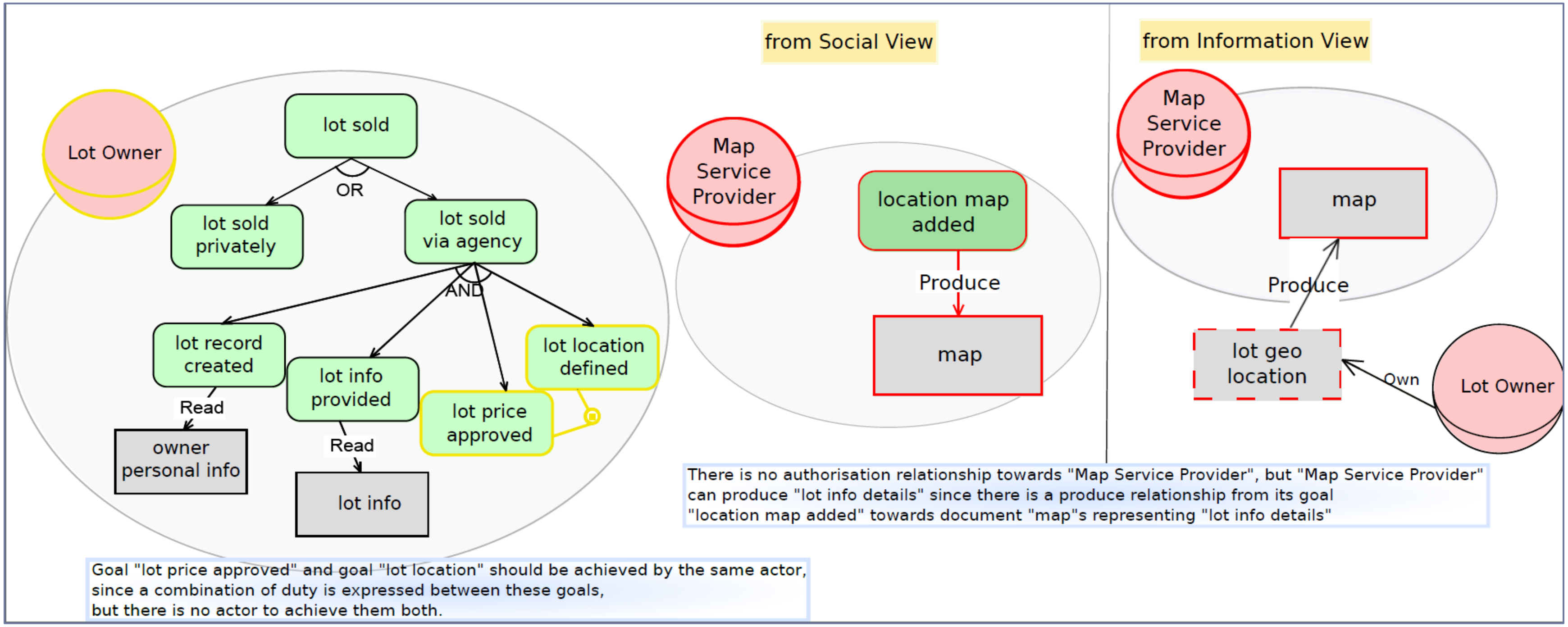



Security

Security

✗ Distributions	Completed
✓ Pre-Analysis:Distributions	Completed
✗ No_Delegation Violation check	Completed
✓ Redundancy	Completed
✓ Pre-Analysis: Redundnacy	Completed
✓ Redundancy Violation check	Completed
✓ Authorization Conflict	Completed
✓ Pre-Analysis: Authorization Conflict	Completed
✓ Authorization Conflict check	Completed
✗ Operations Analysis	Completed
✓ Pre-Analysis: Operation Violation	Completed
✓ Non_Reading Violation	Completed
✓ Non_Modification Violation	Completed
✗ Non_Production Violation	Completed
✗ Non_Disclosure Violation	Completed
✗ NTK Violation	Completed
✗ Non-reauthorization Violation	Completed

4.2. Security Analysis

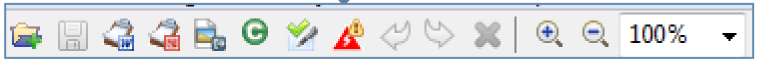


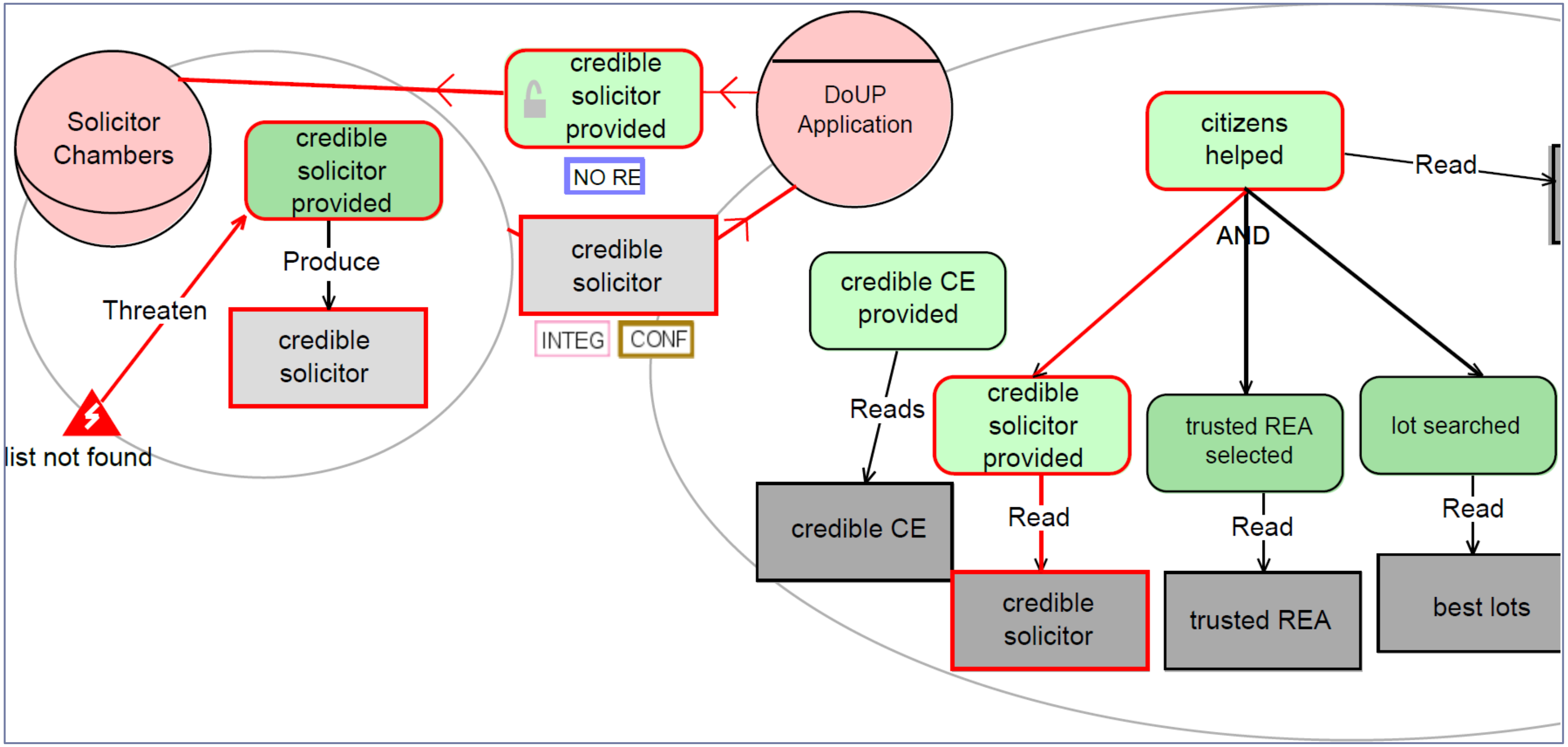
There is no authorisation relationship towards "Map Service Provider", but "Map Service Provider" can produce "lot info details" since there is a produce relationship from its goal "location map added" towards document "map"s representing "lot info details"

Goal "lot price approved" and goal "lot location" should be achieved by the same actor, since a combination of duty is expressed between these goals, but there is no actor to achieve them both.

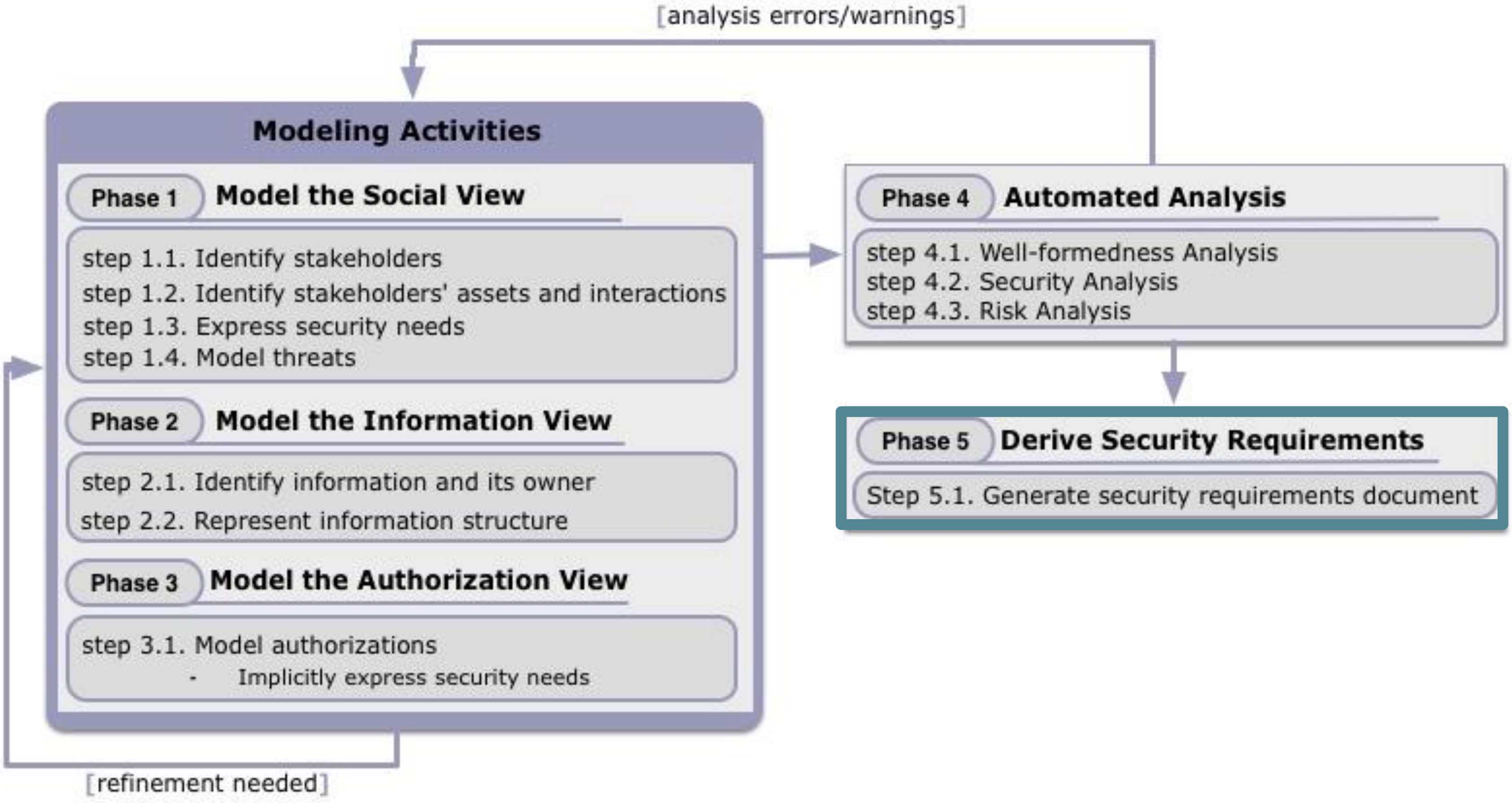
4.3. Risk Analysis

- Go to the Risk Analysis tab
  - Threat propagation





Phase 5: Derive Security Requirements



[analysis errors/warnings]

Modeling Activities

Phase 1 Model the Social View

step 1.1. Identify stakeholders
step 1.2. Identify stakeholders' assets and interactions
step 1.3. Express security needs
step 1.4. Model threats

Phase 2 Model the Information View

step 2.1. Identify information and its owner
step 2.2. Represent information structure

Phase 3 Model the Authorization View

step 3.1. Model authorizations
- Implicitly express security needs

[refinement needed]

Phase 4 Automated Analysis

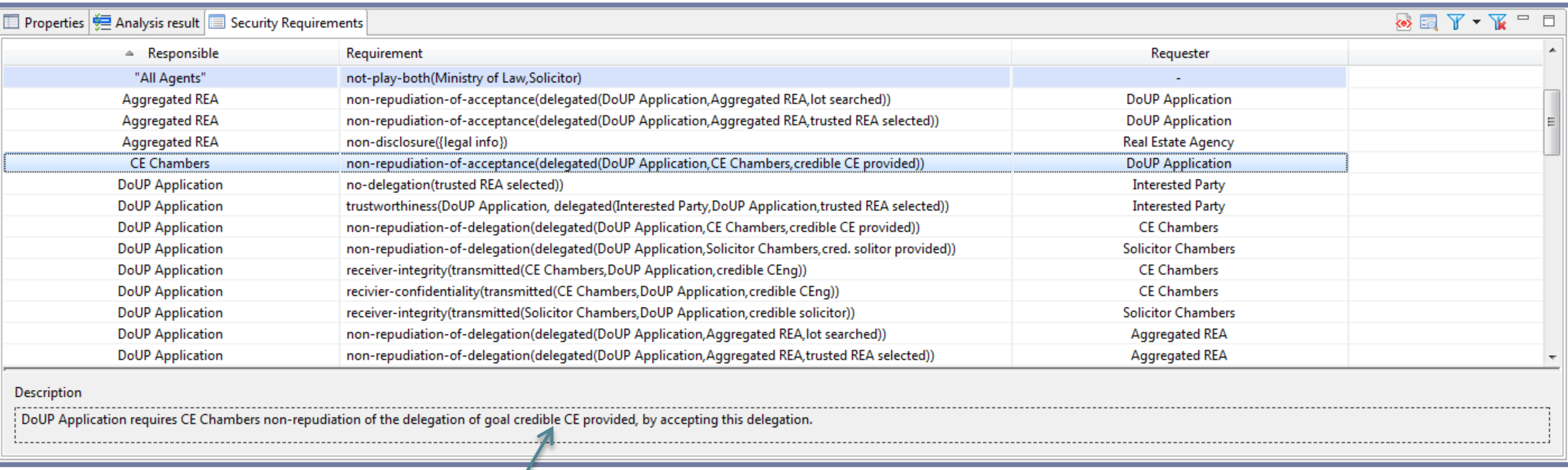
step 4.1. Well-formedness Analysis
step 4.2. Security Analysis
step 4.3. Risk Analysis

Phase 5 Derive Security Requirements

Step 5.1. Generate security requirements document

5.1. Derive security requirements document

- Derived security requirements for eGov scenario



Responsible	Requirement	Requester
"All Agents"	not-play-both(Ministry of Law,Solicitor)	-
Aggregated REA	non-repudiation-of-acceptance(delegated(DoUP Application,Aggregated REA,lot searched))	DoUP Application
Aggregated REA	non-repudiation-of-acceptance(delegated(DoUP Application,Aggregated REA,trusted REA selected))	DoUP Application
Aggregated REA	non-disclosure({legal info})	Real Estate Agency
CE Chambers	non-repudiation-of-acceptance(delegated(DoUP Application,CE Chambers,credible CE provided))	DoUP Application
DoUP Application	no-delegation(trusted REA selected))	Interested Party
DoUP Application	trustworthiness(DoUP Application, delegated(Interested Party,DoUP Application,trusted REA selected))	Interested Party
DoUP Application	non-repudiation-of-delegation(delegated(DoUP Application,CE Chambers,credible CE provided))	CE Chambers
DoUP Application	non-repudiation-of-delegation(delegated(DoUP Application,Solicitor Chambers,cred. solitor provided))	Solicitor Chambers
DoUP Application	receiver-integrity(transmitted(CE Chambers,DoUP Application,credible CEng))	CE Chambers
DoUP Application	recivier-confidentiality(transmitted(CE Chambers,DoUP Application,credible CEng))	CE Chambers
DoUP Application	receiver-integrity(transmitted(Solicitor Chambers,DoUP Application,credible solicitor))	Solicitor Chambers
DoUP Application	non-repudiation-of-delegation(delegated(DoUP Application,Aggregated REA,lot searched))	Aggregated REA
DoUP Application	non-repudiation-of-delegation(delegated(DoUP Application,Aggregated REA,trusted REA selected))	Aggregated REA

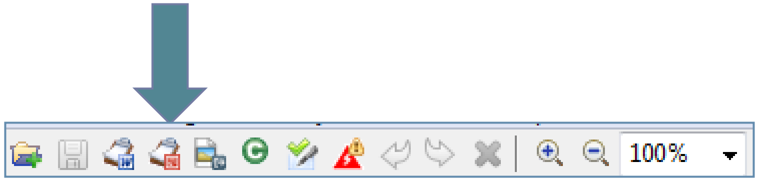
Description

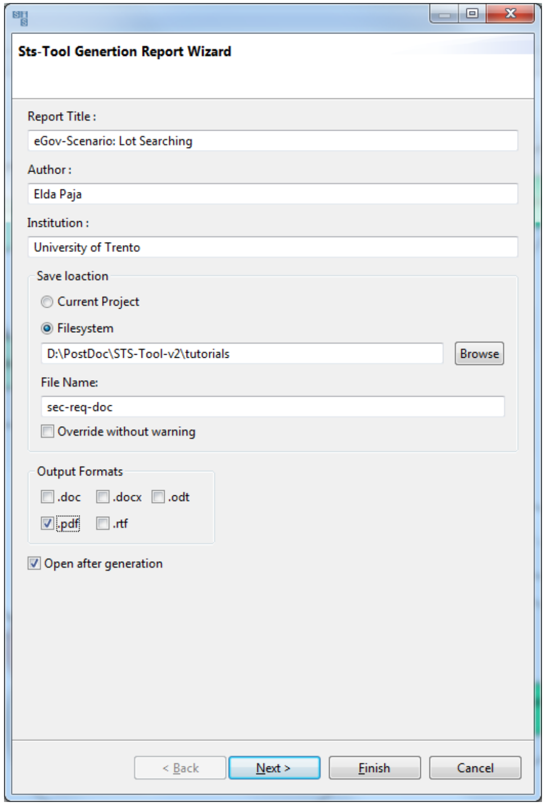
DoUP Application requires CE Chambers non-repudiation of the delegation of goal credible CE provided, by accepting this delegation.

textual description

5.1. Derive security requirements document

- Go to the Generate Requirements Document tab




Sts-Tool Genertion Report Wizard

Report Title : eGov-Scenario: Lot Searching

Author : Elda Paja

Institution : University of Trento

Save loaction

○ Current Project

● Filesystem

D:\PostDoc\STS-Tool-v2\tutorials

File Name: sec-req-doc

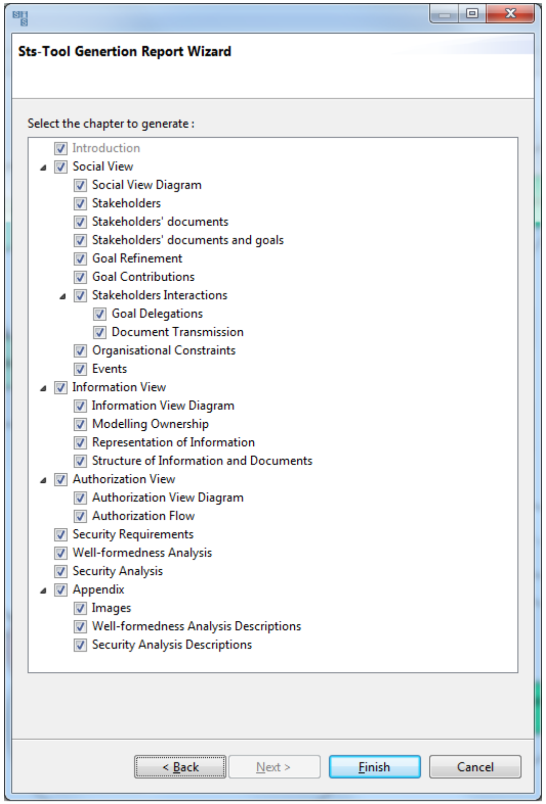
□ Override without warning

Output Formats

□ .doc □ .docx □ .odt

☑ .pdf □ .rtf

☑ Open after generation


Sts-Tool Genertion Report Wizard

Select the chapter to generate :

- ☑ Introduction
- ☑ Social View
  - ☑ Social View Diagram
  - ☑ Stakeholders
  - ☑ Stakeholders' documents
  - ☑ Stakeholders' documents and goals
  - ☑ Goal Refinement
  - ☑ Goal Contributions
  - ☑ Stakeholders Interactions
    - ☑ Goal Delegations
    - ☑ Document Transmission
  - ☑ Organisational Constraints
  - ☑ Events
- ☑ Information View
  - ☑ Information View Diagram
  - ☑ Modelling Ownership
  - ☑ Representation of Information
  - ☑ Structure of Information and Documents
- ☑ Authorization View
  - ☑ Authorization View Diagram
  - ☑ Authorization Flow
- ☑ Security Requirements
- ☑ Well-formedness Analysis
- ☑ Security Analysis
- ☑ Appendix
  - ☑ Images
  - ☑ Well-formedness Analysis Descriptions
  - ☑ Security Analysis Descriptions

5.1. Derive security requirements document

eGov Scenario: Lot Searching

Elda Paja

Nov 7, 2014

The End

paja@disi.unitn.it

- Thank you!

November 2014