Software Design (20VT-2DV608)

Requirements Engineering

Requirements Modelling and Management with Tools

Department of Computer Science and Media Technology

Linnaeus University

Course Outline

- Why Software Engineering - Design (Mauro Caporuscio)
  - w4
- Requirement Engineering (Francis Palma)
  - w5.1 (Jan 29th): Understanding and Elicitation of Software Requirements
  - w5.2 (Jan 31st): Requirements Validation and Management
  - w6.1 (Feb 5th): Modeling with UML
  - **w6.2 (Feb 7th): Requirements Modelling and Management with Tools**
  - W7: ASSIGNMENT RE
- Performance Engineering (Diego Perez)
  - w8.1 to w10
- Design and Refactoring (Mauro Caporuscio)
  - w11.1 to w13

The STS Tool

- http://www.sts-tool.eu
  - http://www.sts-tool.eu/downloads/

- Download and install using your email.
  - Requirement: Java JDK 7 to 11

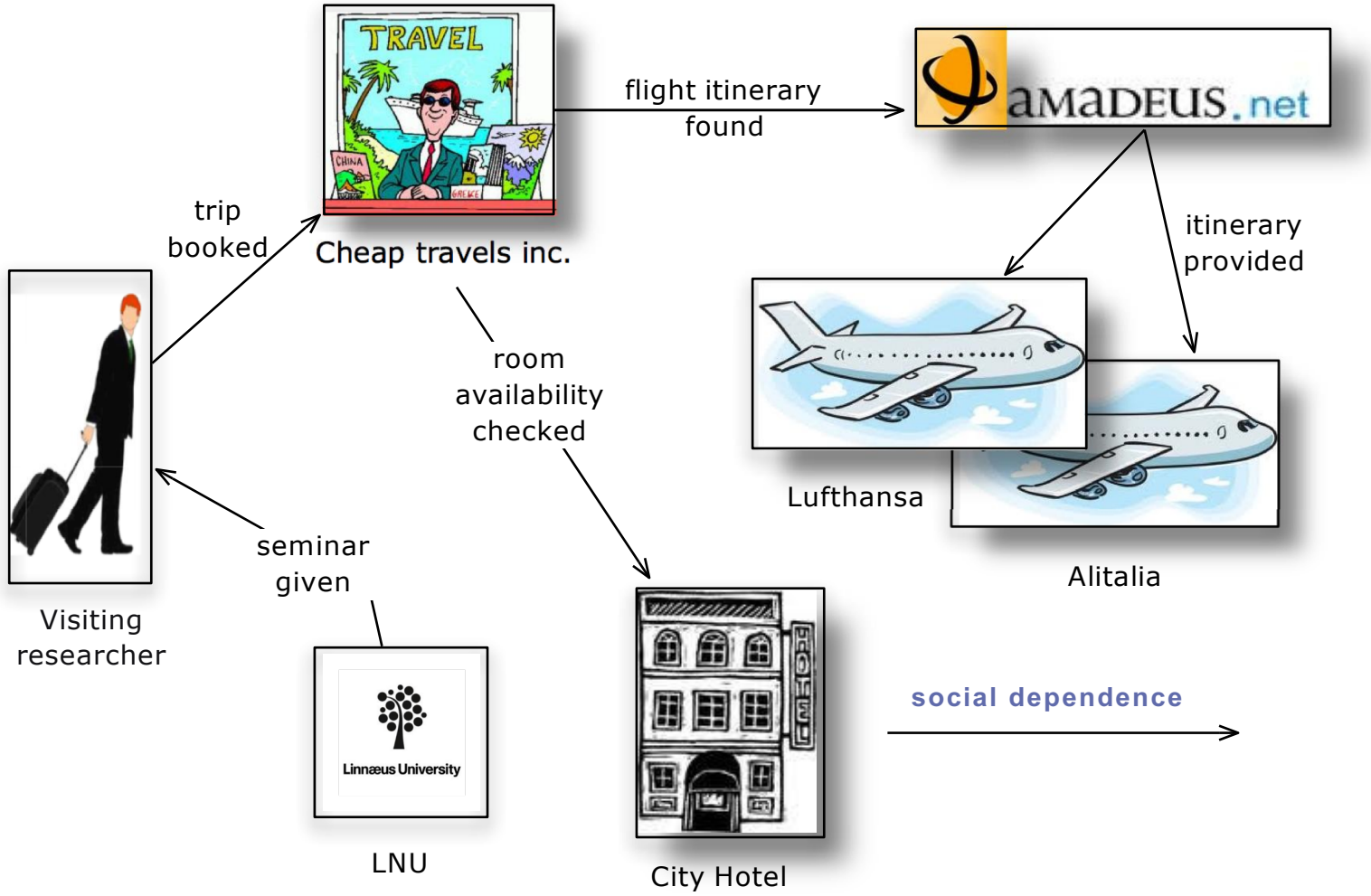
- http://www.sts-tool.eu/manuals/

Socio-Technical Systems (STS)

- Socio-technical systems are an interplay of social (human and organizations) and technical subsystems, which interact with one another to reach their objectives, making a system – *a network of social relationships*.

- Examples include:
  - Smart homes, e-Commerce sites, eHealth systems, e-Marketing systems, etc.

An Example of STS



Socio-Technical Security Modeling Language (STS-ml)

- Actor- and goal-oriented requirements modeling language.
- Participants or actors (each subsystem) in a socio-technical system are autonomous, and the system is defined in terms of the interactions among participants.

- Models are built using diagrams
  - Graphical concepts and relations are used to create the models
  - **Multiple views**, each focusing on a specific perspective

- STS-ml allows stakeholders to express constraints (security needs) over interactions.

- **In STS systems, many security issues arise from the interaction among participants, and on how the exchanged information is manipulated.**

Modelling Views in STS

- The **STS method** allows security requirements engineers to model different perspectives for a setting/context. These different perspectives are ***views*** over the same model.

- The STS method can model the following ***operational*** views:
  - **Social view:** represents actor intentionality and sociality. Actors can be either social or technical in nature. Example: A web service that acts on behalf of a travel agency is technical; a customer interacting with such web service is social.
  - **Information view:** represents the information in the considered organization/setting together with the documents that represent such information, as well as the relationships among these informational entities or documents.
  - **Authorization view:** represents the authorizations granted by some actors *to other actors* concerning the exchange and manipulation of information for particular purposes.

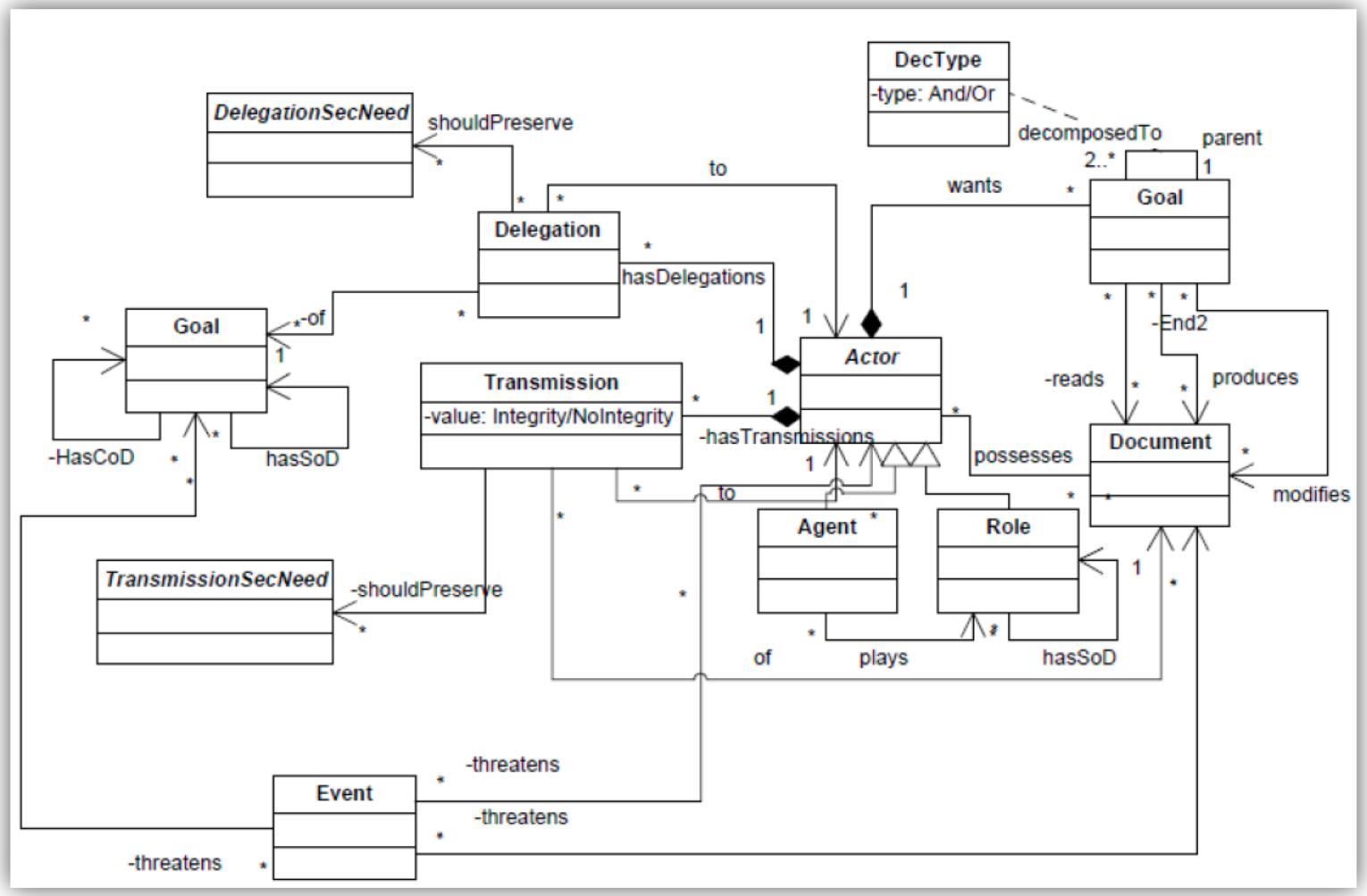
Social View

- Social interaction enables actors to achieve goals that they are not capable to achieve individually.
- The social view supports two types of social relationship, namely goal delegation and document transmission.
  - **Goal delegation:** captures the expectations that one actor has from others in terms of the goals that he can delegate.
    - Example: The visiting researcher depends on *Cheap Travel Inc.* to book the hotel and flight tickets.
  - **Document transmission:** enables to represent the information flow – how documents are transferred from one actor to another.
    - Example: The visiting researcher wants *Cheap Travel Inc.* to use his personal data strictly to book the hotel and flight tickets, but not for any other purposes.

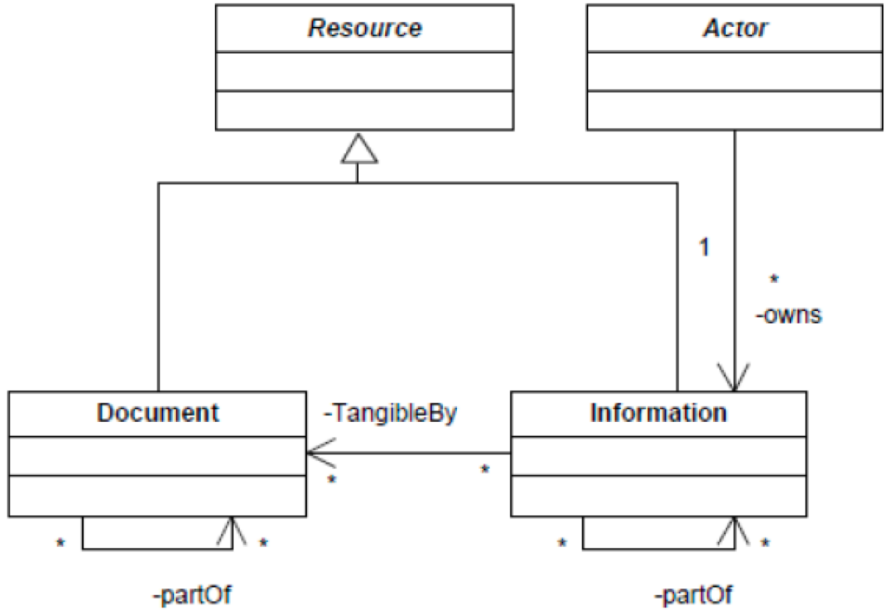
- **A key concept in the social view is that of security need.**

- In STS-ml, security is related to actors' interactions, thus, *security need* refers to the expectation concerning security that actors impose on the interactions they participate in.

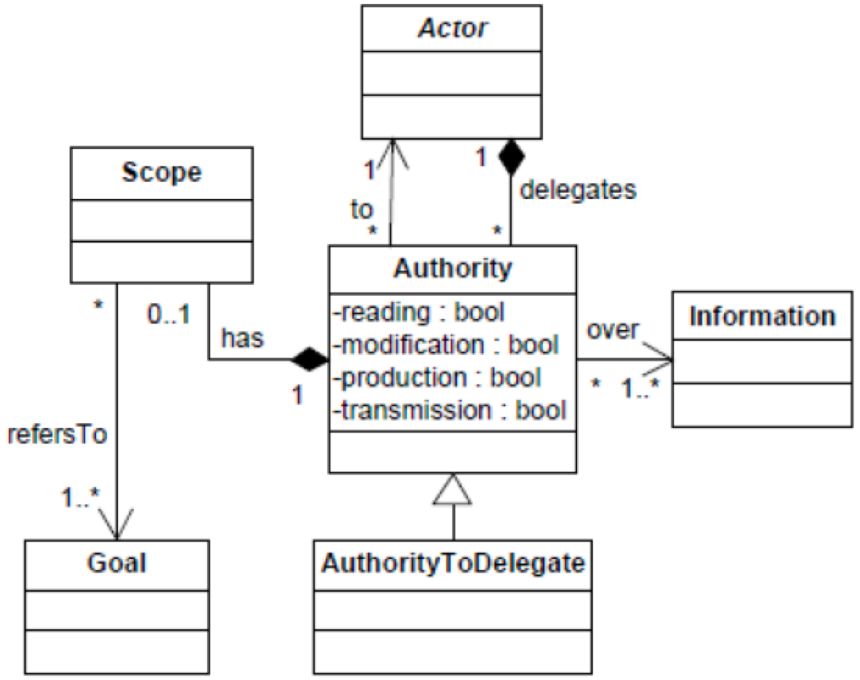
Social View Metamodel



Information and Authorization View Metamodel

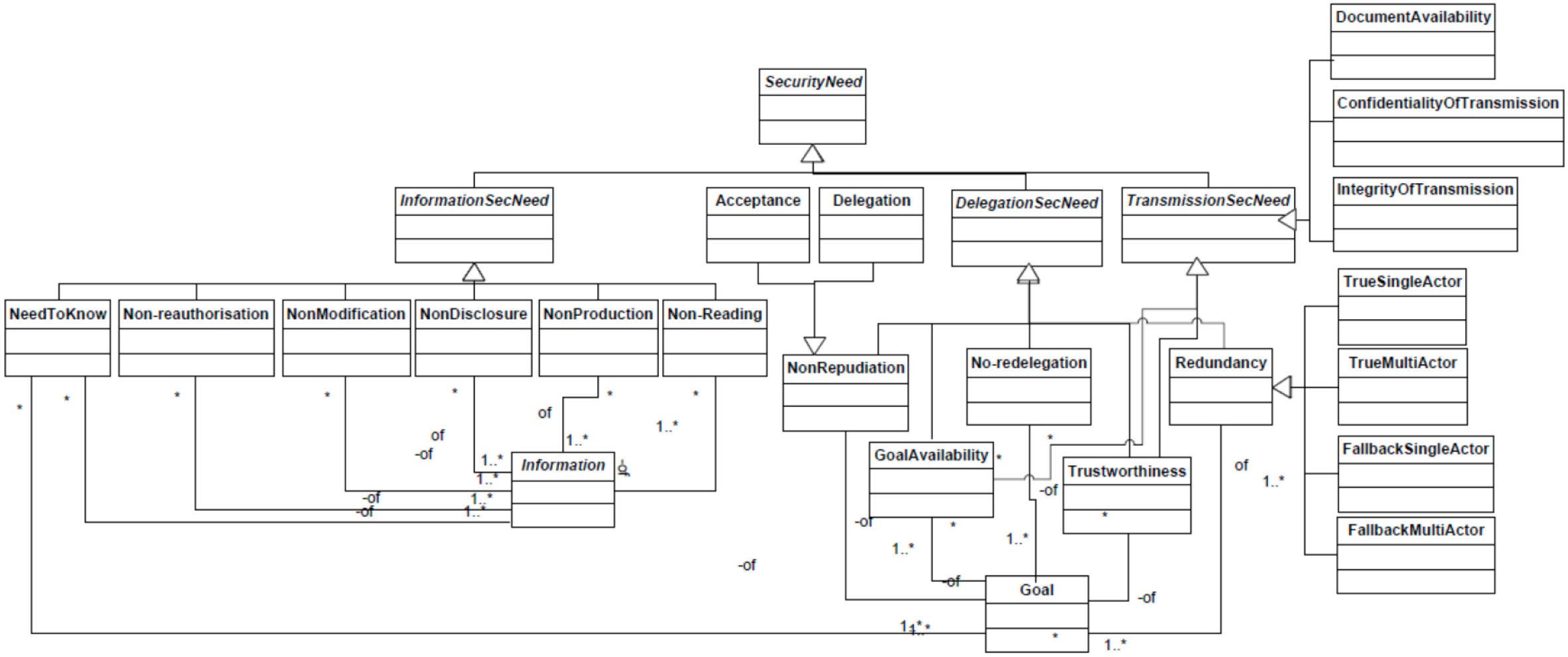


Information View Metamodel



Authorization View Metamodel

Security Needs in STS



Security Needs

- More than 25 security needs in STS-ml.

- 11 security needs related to related to **Delegated Goals**.
  - **Non-repudiation (NonRep):** the delegator actor wants the delegatee actor not to be able to challenge the validity of the goal delegation.
  - **Redundancy:** the delegatee has to adopt redundant strategies for the achievement of the delegated goal.
  - **No-redelegation (No-del):** this requirement is expressed over goal delegations where delegatee takes full responsibility for achieving the delegated goal, without relying on any other actor.
  - **Trustworthiness:** this security need specifies a requirement to potential actors playing the delegatee role.
  - **Availability:** the delegator wants the delegatee to guarantee a minimum availability level concerning the provision of the delegated goal.
  - **Authentication:** For the delegator, this requirement about authenticity indicates the delegatee's request that the delegator shall be authenticated.

Security Needs

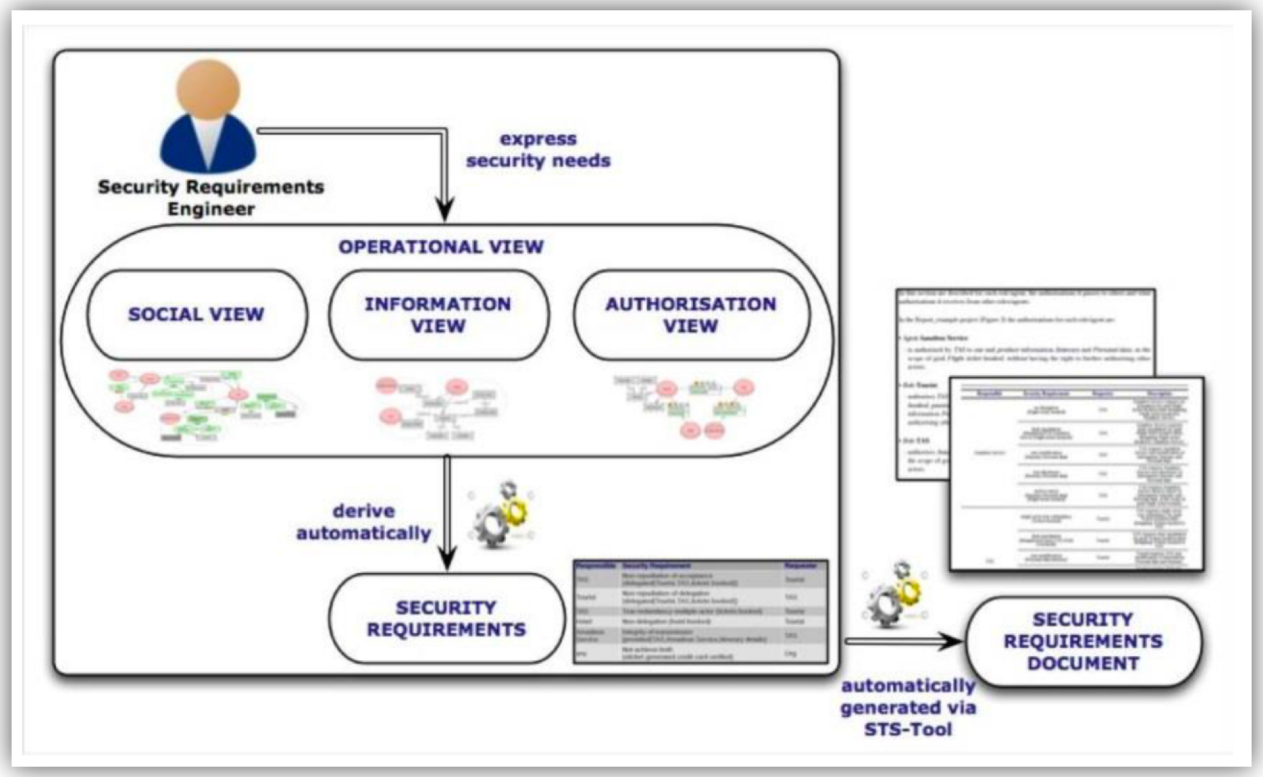
- 4 security needs related to **Documents**.

  - **Integrity of transmission:** requires the sender to guarantee the integrity of the given document while providing it.
  - **Document Availability:** requires the sender to guarantee an availability level of x% for the transmission of the specified document.
  - **Confidentiality of transmission:** requires the transmitted to guarantee the confidentiality of transmission of the given document while providing it.
  - **Authentication:** this requirement about authenticity could be specified either by the sender or by the receiver to the other party during a document transmission.

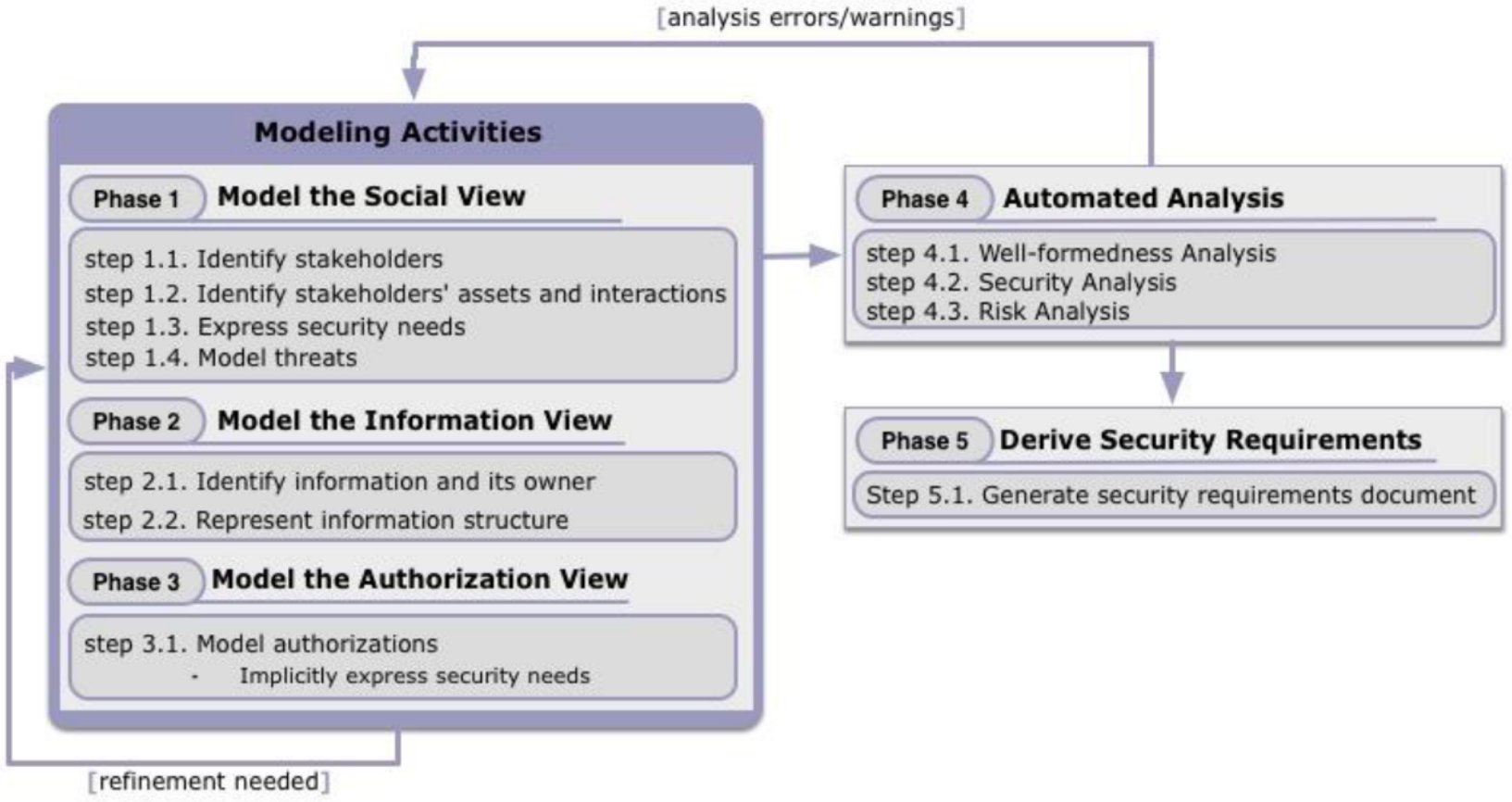
Security Needs

- 6 security needs related to **Information**.
  - **Non-reading:** prohibiting the read operation expresses a non-reading security requirement, which requires the information is not read in an unauthorized way.
  - **Non-modification:** prohibiting the right to modify information expresses a security need about the non-modification of such information.
  - **Non-production:** requires the information is not produced in a new document in an unauthorized way.
  - **Non-disclosure:** requires that no document representing the specified information is transmitted to other actors by the authorizee.
  - **Need-to-know:** when restricted to a goal scope, the authorization reflects a need-to-know security need.
  - **Non-reauthorization:** requires that the authorization is not transferrable.
- 4 security needs related to **Authorization** relationship.
  - Allowed/prohibited operations, Information, Scope of authorization, and Transferability of the permissions

High-level View of STS

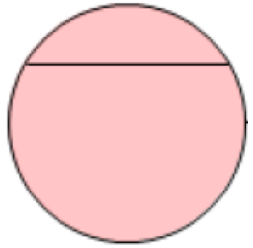


Detailed View of the STS Modelling Tool

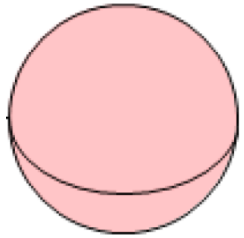


Concepts: Agent, Role, and Goal

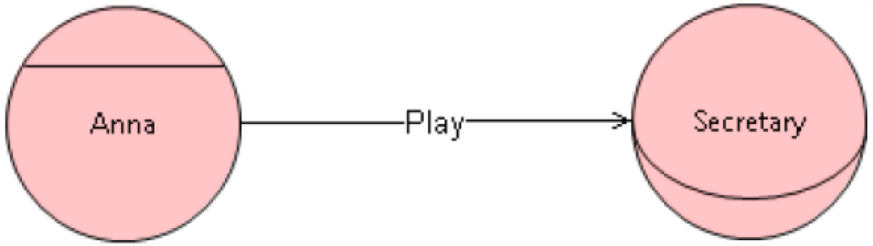
- An actual participant – *agent* – plays a *role*.



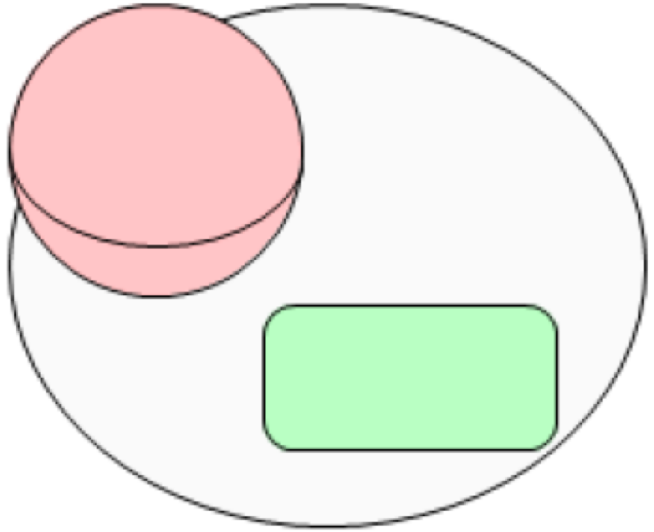
agent



role



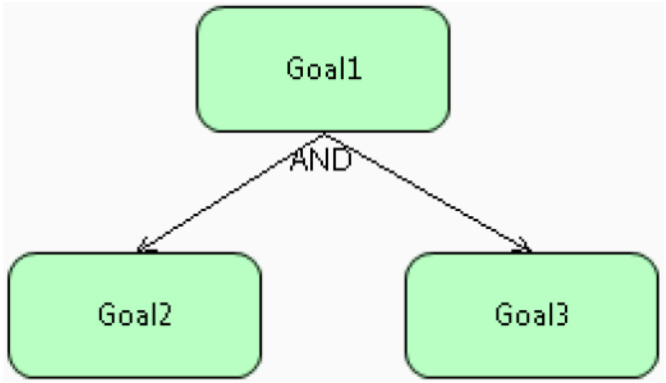
- A goal represents a desired state of affairs (e.g., a course is registered, a flight is booked).

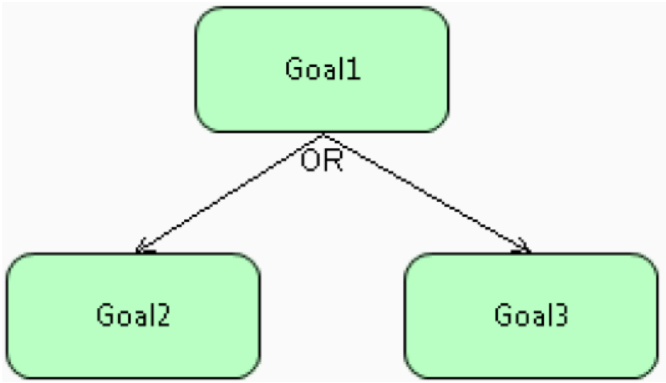


Concepts: Goal Decomposition

- STS analyze goals from the actor perspective and refine them, creating a goal model.

- Goals are analyzed and refined in STS-ml via AND/OR decompositions -- refine goals into sub-goals.



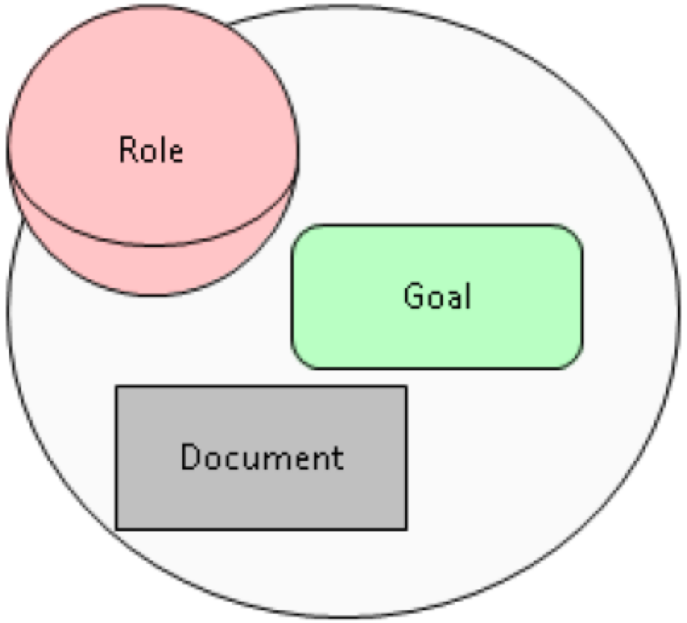


Concepts: Document and Information

- A document represents an exchangeable entity (e.g., reference letter), which may contain some information (e.g., personal data, salary).

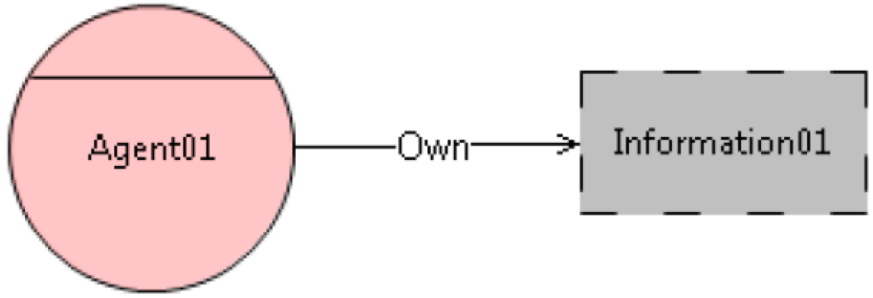
Concepts: Scope and Possession

- The scope of a role (agent) defines the strategic construction of the role (agent):
  - The goals the role/agent wants to achieve;
  - The documents the role/agent possesses.



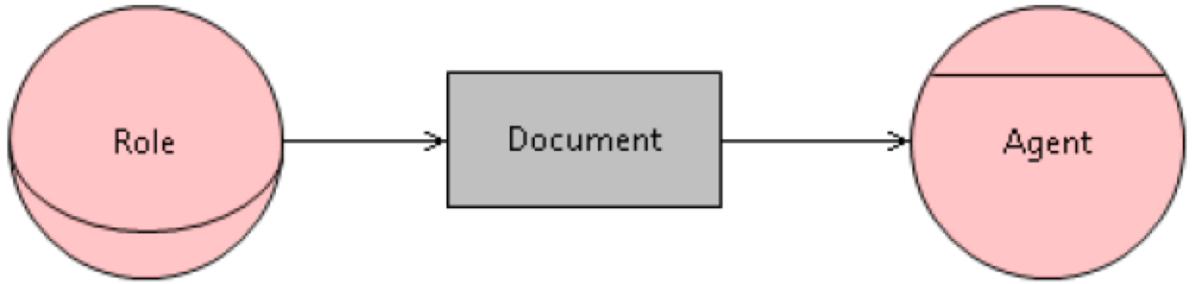
Concepts: Own

- A role/agent is the legitimate owner of some information and can freely dispose of it, as well as decide to transfer rights about it to others (e.g., a student is the owner of her personal data).



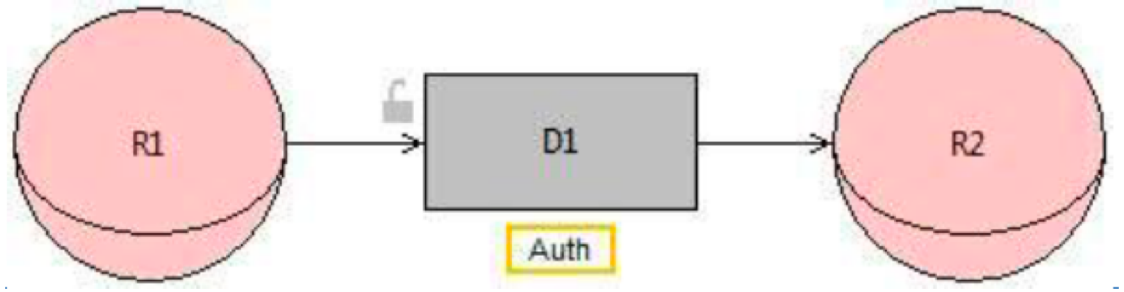
Concepts: Document Transmission

- A role/agent transmits a document that she possesses to another role/agent. For example, a student transmits his report to the professor or the hotel transmit the final invoice of the hotel reservation to the guest.



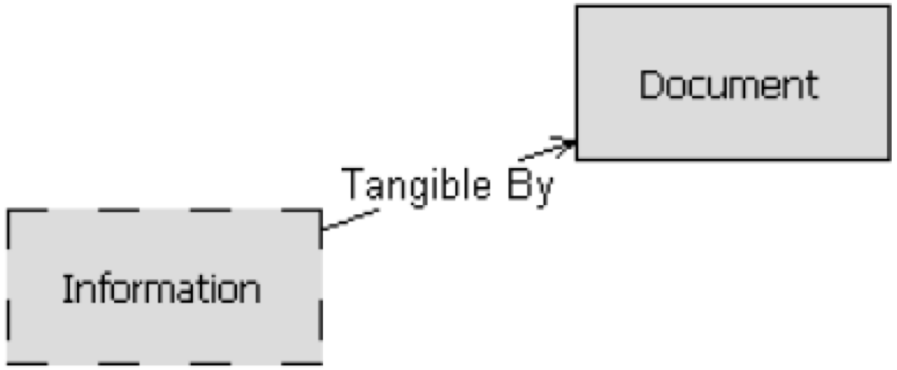
Concepts: Document Authentication

- Sender/Receiver requires authentication of the receiver/sender for getting/transmitting the document.



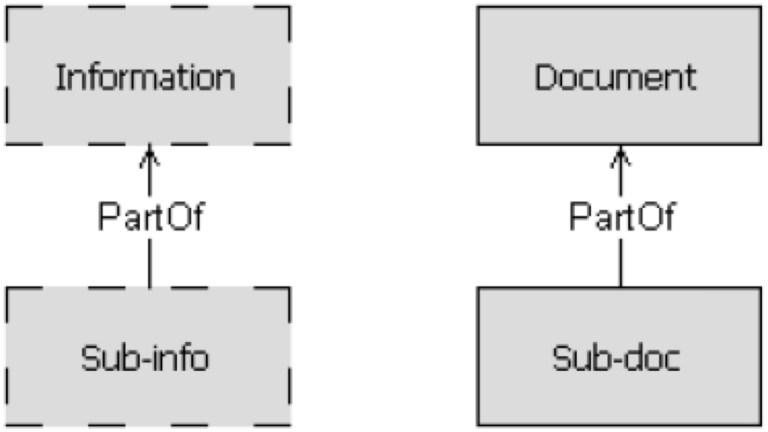
Concepts: Tangible Information

- An information entity is made tangible by a document (e.g., the student's personal data is made tangible by a reference letter)



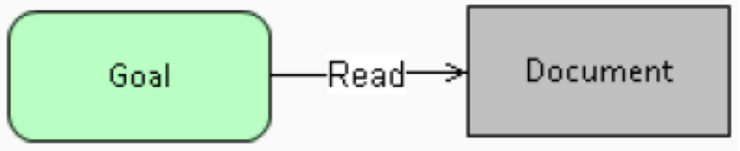
Concepts: ‘PartOf’ Relation

- An information entity (a document) is part of another information entity (another document).
- The part of relationship applies between homogeneous concepts.
  - For example, the ‘date of birth’ information is part of the ‘personal data’ information. Also, the ‘letter header’ is part of the ‘recommendation letter’.



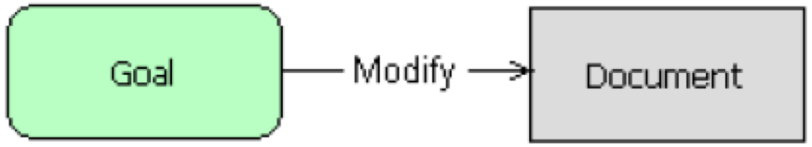
Concepts: Goal-Document Relationships

- A document is read in order to achieve a goal. For example, document “letter template” is read to achieve goal “old letter copied”.



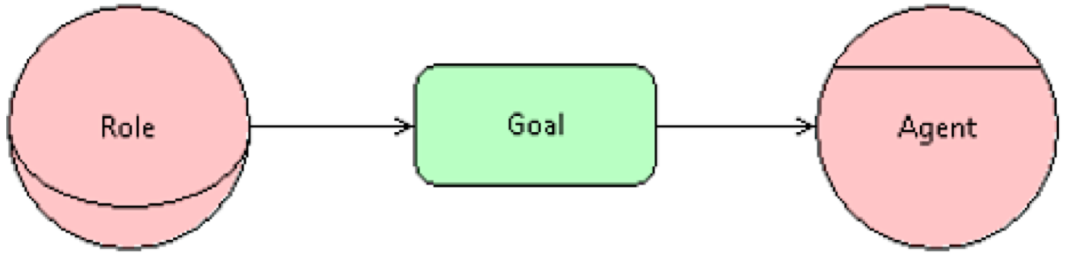
- A document is produced while achieving a goal. For instance, document “reference letter” is produced while achieving goal “recommendation letter written”.

- The content of a document is modified while achieving a goal. For instance, document “health record” is modified while achieving goal “update patient’s health record”.



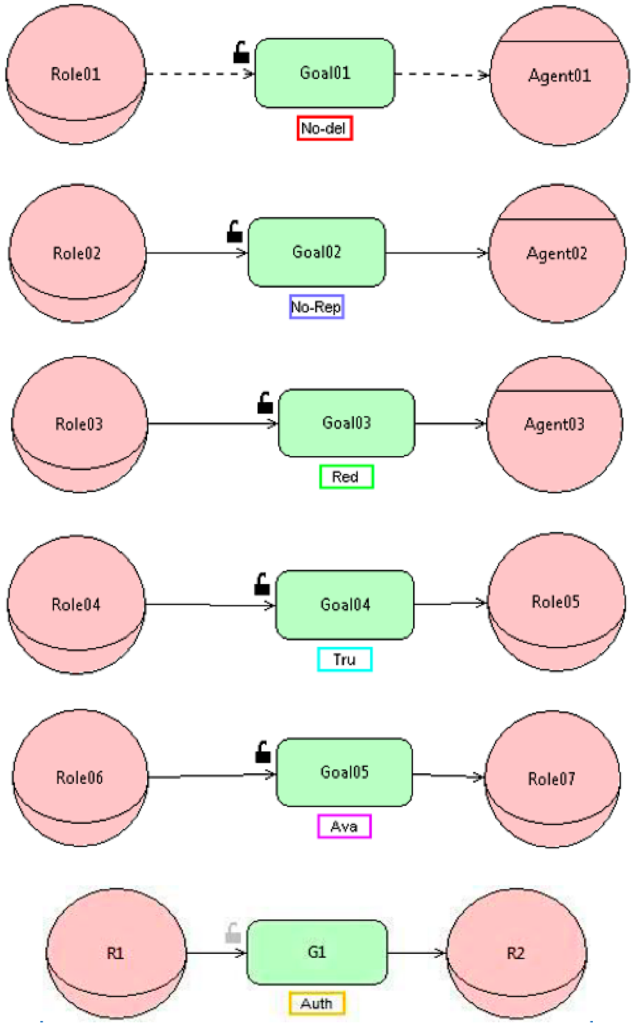
Concepts: Goal Delegation

- A goal delegation implies that a role or agent (delegator) delegates the fulfillment of a goal (delegatum) to another role or agent (delegatee).



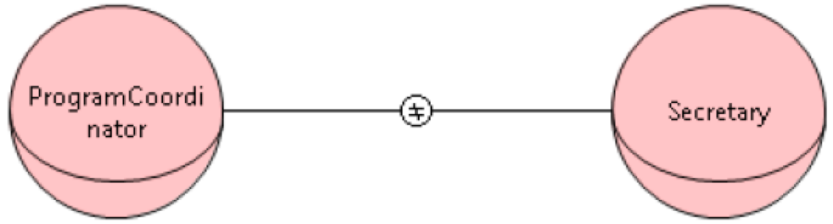
Concepts: Goal Delegation

- The STS-ml supports some variants of delegation:
  - **No-delegation:** the delegatee cannot further delegate the goal.
  - **Non-repudiation:** the delegatee cannot deny/challenge that the delegation has taken place.
  - **Redundancy:** the delegatee shall adopt measures to provide redundant fulfillment of a goal.
  - **Trustworthiness:** the delegatee shall provide a proof of trustworthiness, e.g., issued by a certification authority.
  - **Availability:** the delegatee shall ensure a minimum level of availability for the delegated goal.
  - **Authentication:** the delegator/delegatee shall authenticate for delegating/getting the goal.

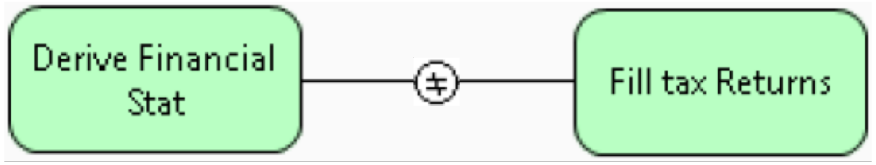


Concepts: Separation of Duties (SoD)

- Between roles: defines incompatible roles – when specified between the two roles, it does not allow the same agent to play both the roles.

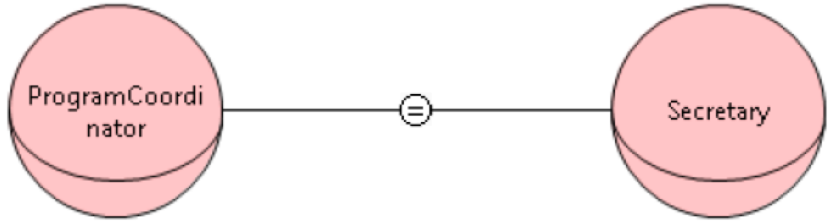


- Between goals: defines incompatible goals -- when SoD is specified between two goals an actor is not allowed to or should not achieve both.

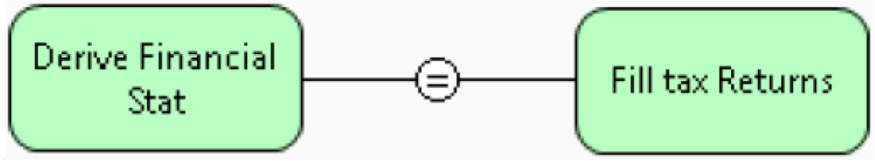


Concepts: Combination of Duties (CoD)

- Between roles: defines compatible roles – when specified between the two roles, it allows the same agent to play both the roles.

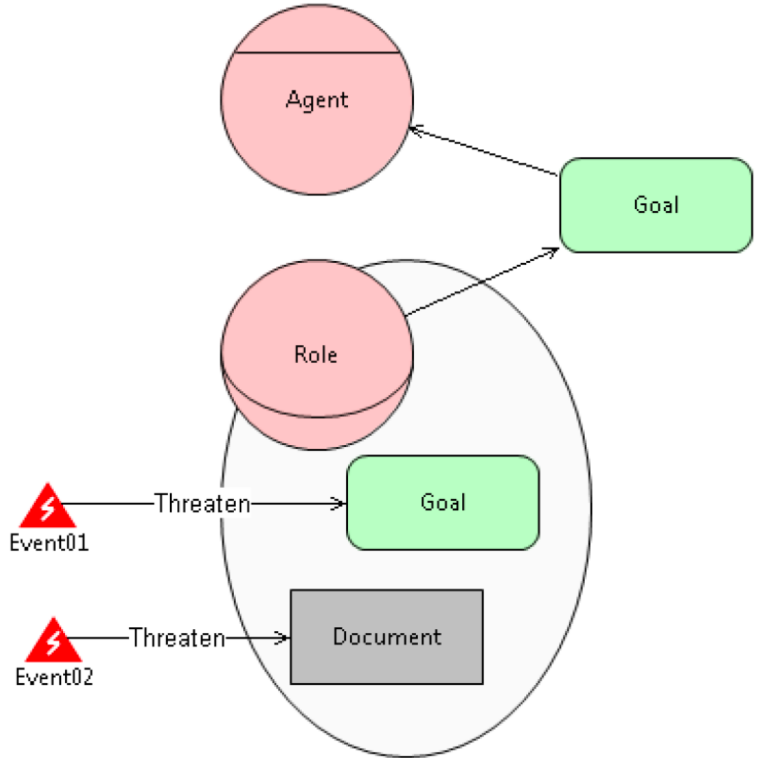


- Between goals: defines compatible goals -- when CoD is specified between two goals, an actor is allowed to or should achieve the both.



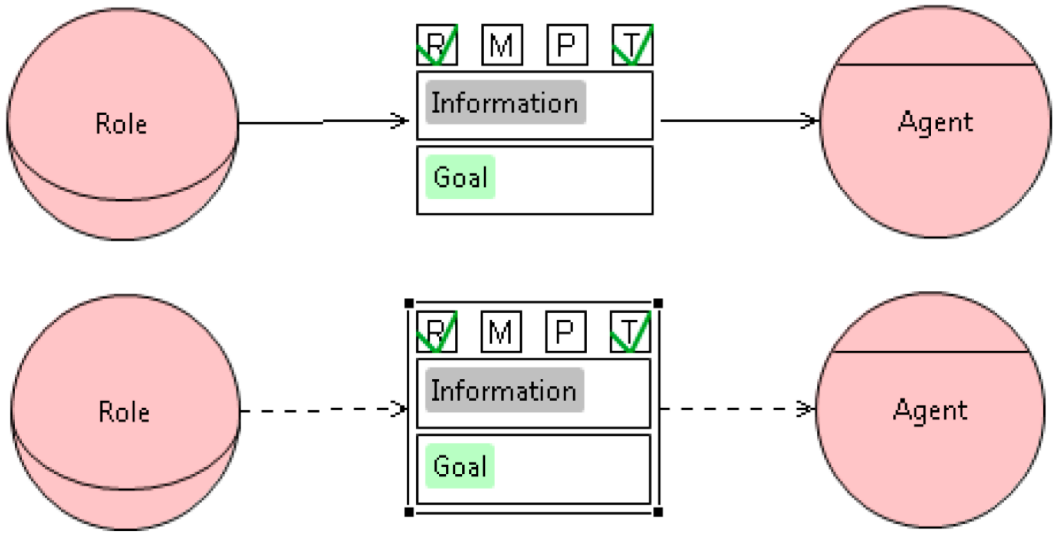
Concepts: Events

- An event threatens actors (agents and roles), goals, goal delegations, and documents.



Concepts: Authorization

- A role or agent authorizes another role or agent for certain operations to be performed on one or more information items, within the scope of a given goal.
- Operations are: Read (R), Modify (M), Produce (P), and Transmit (T).



Linnéuniversitetet

A Case Study using the STS Tool

The Scenario

- Consider a scenario where an international student needs an official document from the program coordinator; and such document has to be presented to the local immigration office to extend his study permit. The following roles are involved:
  - **Student:** Needs an official document to prove he is enrolled in the study program in LNU and his incomes are enough to afford the stay. He asks the program coordinator to issue the document. For this reason, he has to transmit his personal and financial information. His personal data is stored in the LNU information system.
  - **Program Coordinator:** Issues the official document for the student. She might transfer responsibility for parts of this activity to his secretary.
  - **Secretary:** Retrieves student information (personal data and financial data) from the LNU information system and drafts the document.
  - **Data Manager:** Manages the data about students stored in the LNU information system in accordance with confidentiality restrictions.

RE Assignment

- **RE1.1 Requirements Elicitation, Analysis, Validation, and Modelling:**
  - Identify stakeholders.
  - Elicit and label the functional and non-functional requirements, a minimum of **three** for each type.
  - Perform a systematic 'checklist-based' requirements analysis.
  - Classify the identified requirements using the 'faceted approach', and systematically assess their risks.
  - Perform a 'systematic validation' of the requirements.
  - Propose at least <u>one</u> test case (criteria) for each of the requirements.
  - Define and develop a final 'requirements document'.
    - ✓ ***Deliverable 1:*** *Create and deliver a final* ***pdf*** *document as 'requirements document'.*
  - Pick <u>one</u> of the requirements and model using UML by identifying classes, attributes, operations, and relationships.
  - On your UML diagram, define at least three OCL constraints verifying different properties.
    - ✓ ***Deliverable 2:*** *Export the Eclipse OCL project in* ***.zip*** *and upload.*
- **RE1.2 Identification and Modelling of Security Requirements:**
  - Express the security needs for the problem context using the 'social view', 'information view', and 'authorization view' of your security needs after identifying the roles, goals, and interactions.
  - Perform the security and risk analysis and derive the security requirements document for the problem context.
    - ✓ ***Deliverable 3:*** *Create and deliver a final* ***pdf*** *document by exporting (i) the social, information, and authorization views and (ii) the derived security requirements after performing security and risk analysis.*

RE Assignment: Writing and Evaluation Guideline

- Recommended tools: for **RE1.1** Eclipse Modelling Tool and OCL, for **RE1.2** STS-tool
- Font: Times New Roman
- Font Size: 12pt
- Text Alignment: “Justified”
- Font color: Always black
- Line Spacing: At 1.5 lines
- Page limit: No page limit
- Page size: Letter/A4
- Format: pdf for report and zip for OCL project (from Latex, Doc, STS)
- Evaluation: Content quality 90%, presentation quality 10%

Questions?