Aniketos Socio-technical Security Modeling Language

Elda Paja (University of Trento)

AOSE Lecture

28 November 2011 – Trento

STS modeling language (STS-ml)

- Extends Tropos and Secure Tropos exploiting high level abstractions to analyze security
  - Tailored for Service-oriented settings (especially cross-organizational)

- Features
  - Focuses on Security Requirements Engineering
    - Detect and analyze security issues early in the SW development process
  - Derive security specifications for services under development

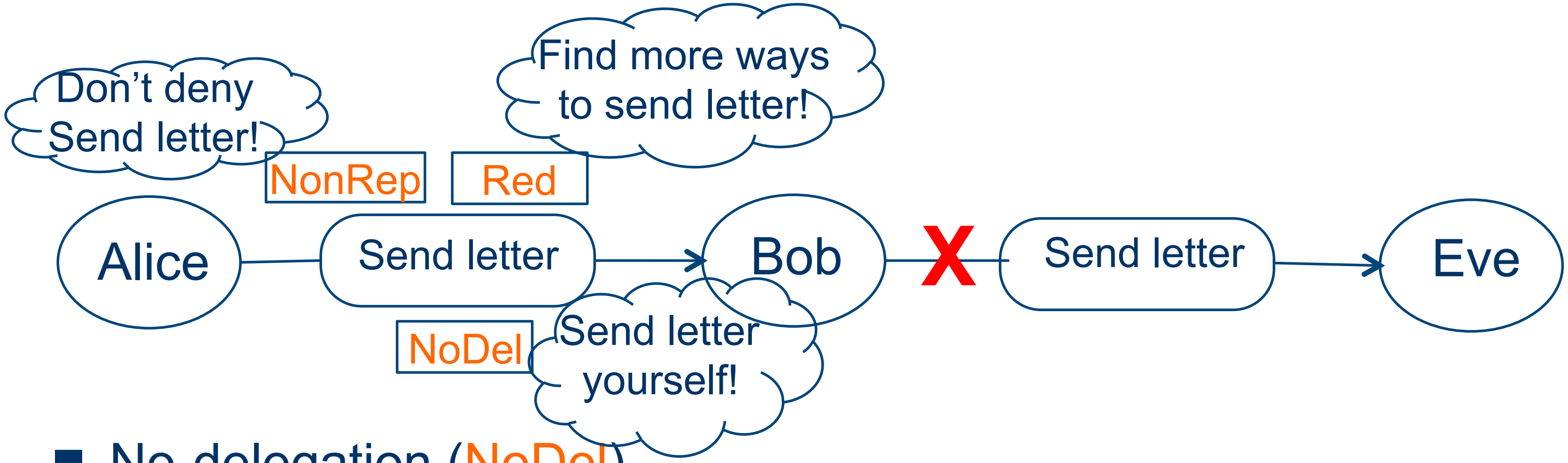
STS-ml

- Goal–oriented modelling language

- Models are built diagrammatically
  - Graphical Concepts and Relations are used to create models

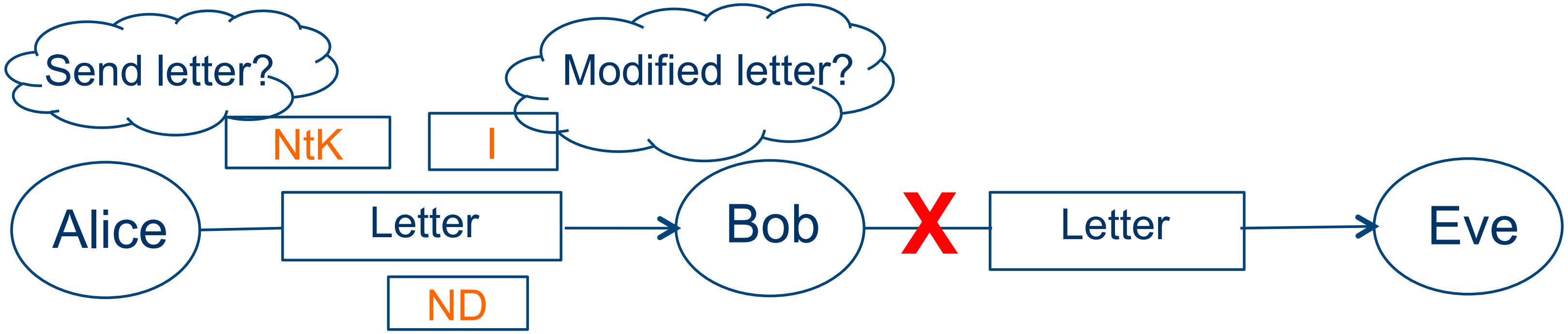
- What is the expected outcome?
  - An organizational structure that supports a set of **security needs**
  - Security requirements that enable secure and trustworthy interaction

Security Needs: which kind?



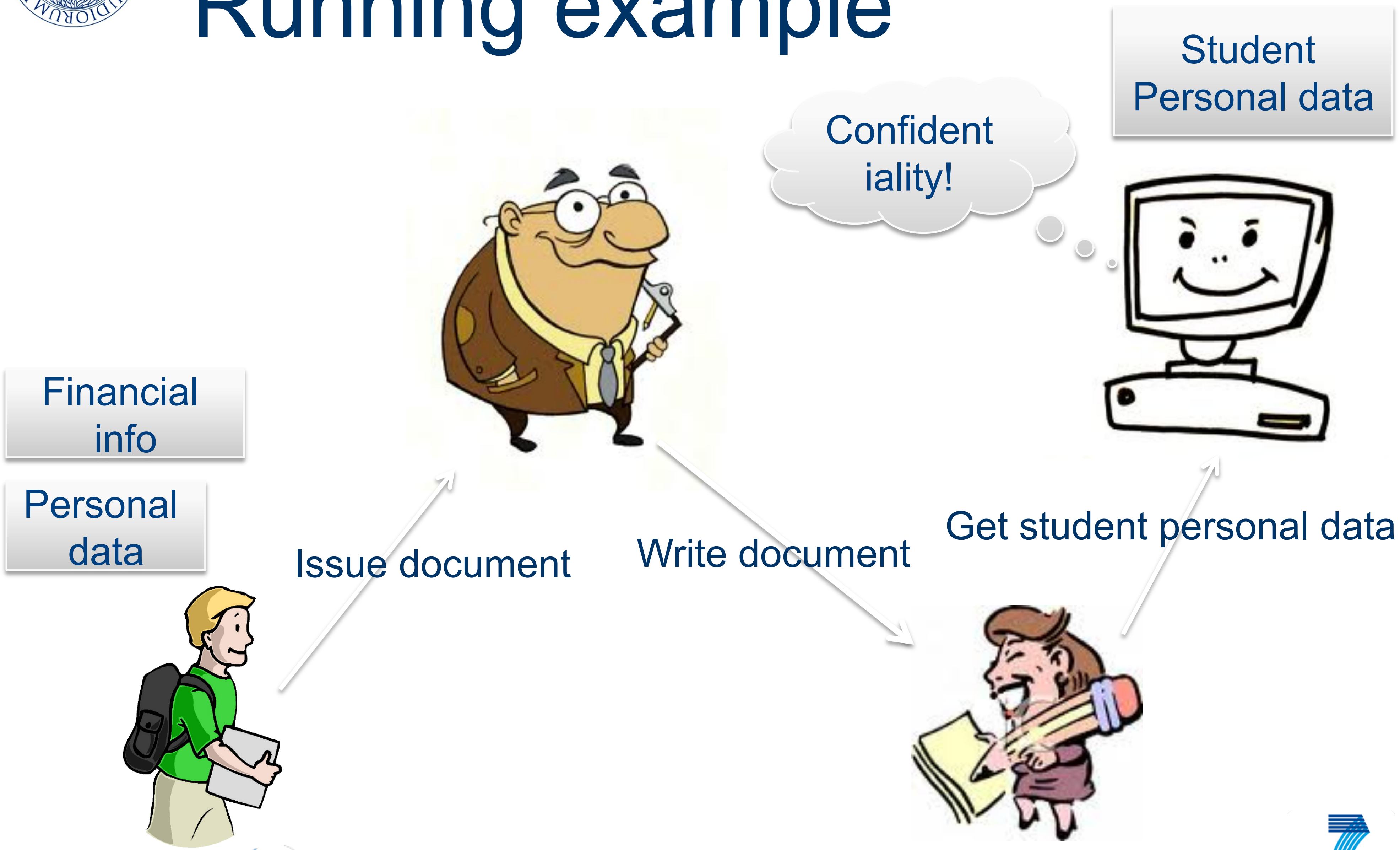
- No-delegation (NoDel)
  - Further delegation of the fulfilment of a goal is not allowed
- Non-repudiation (NonRep)
  - When delegated the fulfilment of a goal, the actor cannot deny this transfer of responsibility
- Redundancy (Red)
  - *Redundancy refers to the various ways of achieving a goal.*
  - *Especially for critical goals, there should be redundant ways for their achievement.*

Security Needs: which kind?



- Need-to-Know (NtK): confidential information should be disclosed only for its intended purpose
- Non-Disclosure (ND): confidential data should not be further disclosed
- Integrity (I): sensitive data has not been modified in an unauthorized and undetected manner

Running example



Financial info

Personal data

Issue document

Write document

Get student personal data

Confident
iality!

Student Personal data

Supported Security needs

- Non-repudiation
  - *Programme coordinator wants to ensure non-repudiation for goal "Write document" to the secretary*
- Redundancy
  - *Secretary wants the IS manager to adopt redundant strategies to obtain the student's income statement.*
- No-delegation
  - *Secretary wants the IS Manager not to delegate goal "Get student personal data".*

Supported Security needs

- Non-disclosure
  - *IS Manager might expresses it over resources personal data and financial status granted to the secretary.*
- Need to know
  - *Student expresses a need-to-know security need to the IS Manager: personal data and financial status should be produced or distributed in the scope of goal "Write document for immigration office".*
- Integrity
  - *IS Manager expresses such security need passing personal data and financial status to the secretary.*

Security Needs

- How can we capture them?

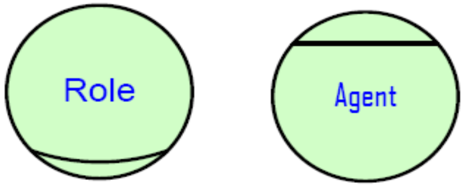
Red NoDel NonRep

- Expectations concerning security actors impose on social relationships they participate in!

NtK ND I

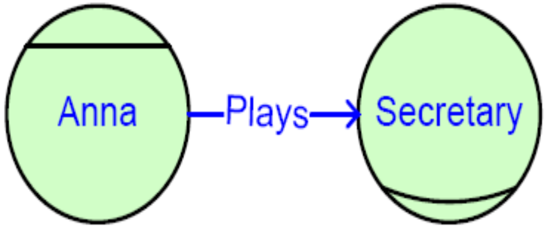
- Expectations concerning security regarding data/information usage and flow!

Actors: Agent and Role



- **Role** *is an abstract characterization of the behavior of an active entity within some context*
  - We do not know who are going to be the participants at runtime, thus we specify such applications at the role level.
  - **E.g.**: Professor, Student, …

- **Agent**
  - Play (adopt) roles at runtime, and they can change the roles they play
  - **E.g.**: Bob, Alice, Prof. Rossi
  - Some agents are known since requirements time
  - **E.g.**: Prefecture of Trento

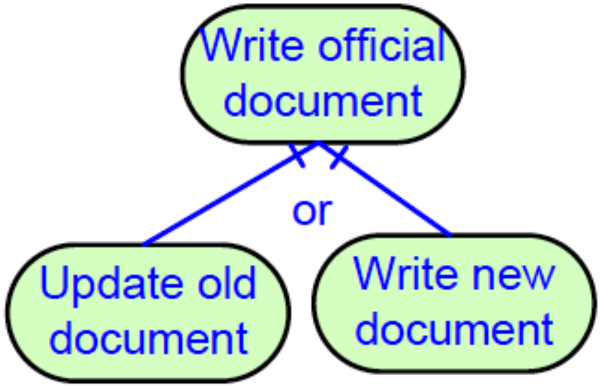


Goals

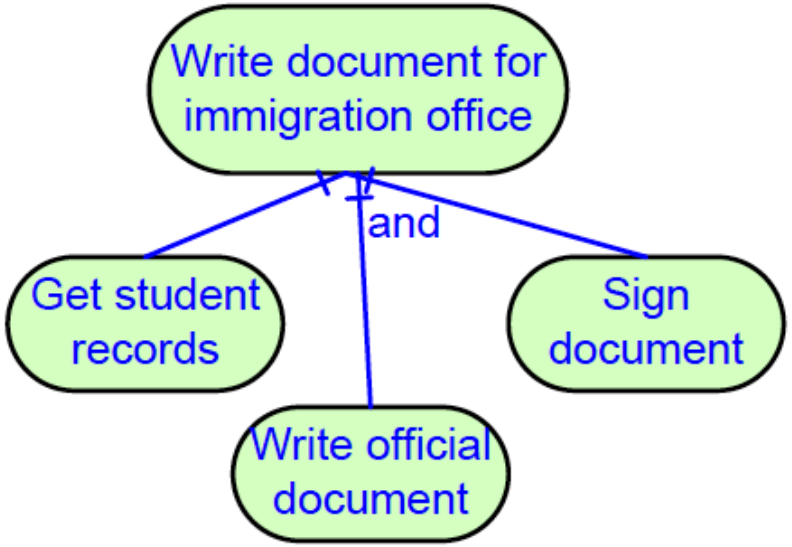
- **Goal** is a state of affair which an actor intends to achieve
  - **E.g.**: write new document, get student records
  - Used to capture motivations and responsibilities of actors

- **Goal decompositions**: refinements

Or decomposition

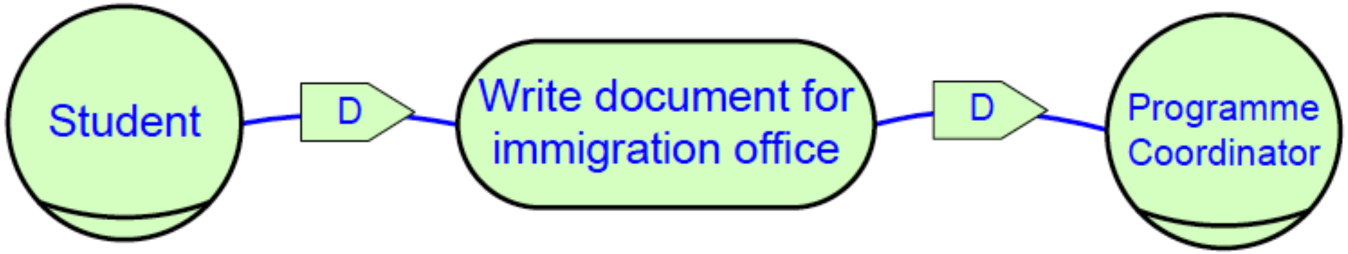


And decomposition

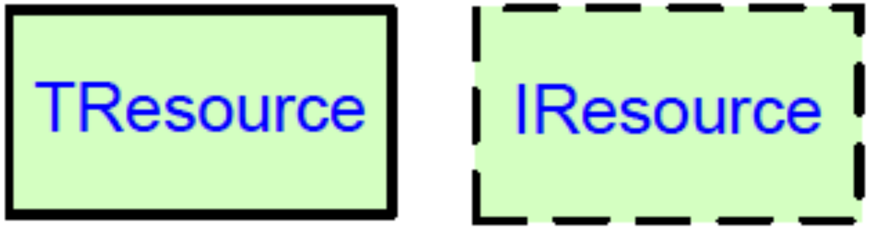


Goal Delegation

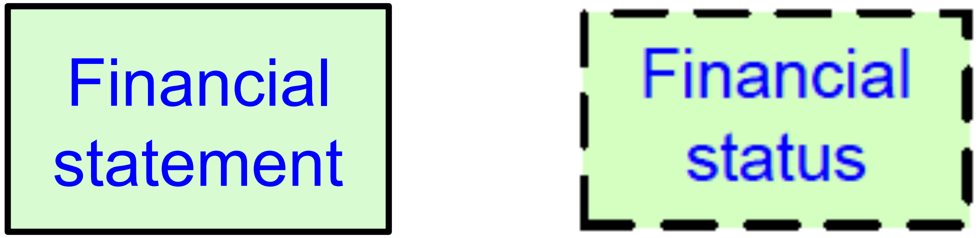
- A Delegator actor delegates the fulfilment of a goal (delegatum) to a different actor (delegatee)
  - Student is not capable of writing the document on his own, he depends on the programme coordinator to achieve his goal



Resources

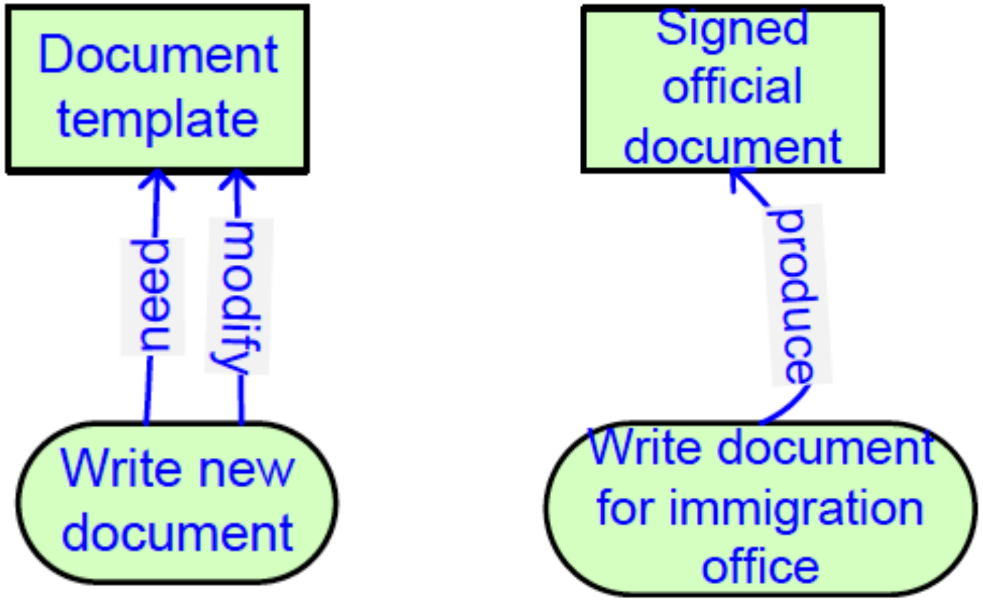


- A **Resource** represents a physical or information artifact
- Resource types
  - **Tangible (TResource)**: concrete entities, including electronic ones
    - E.g. e-mail, ID document, financial statement
  - **Intangible (IResource)**: informational content, ideas
    - E.g. birthday, financial status



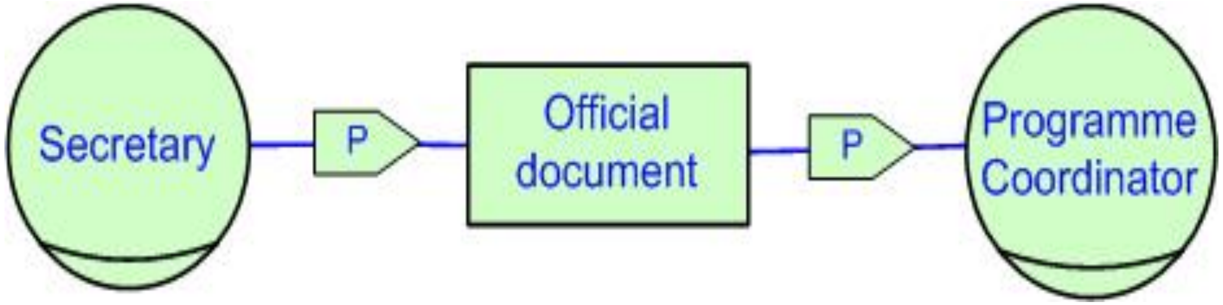
Goal and Resource relations

- An actor needs one or more resources to fulfil a goal
- An actor produces resources while fulfilling a goal
- An actor modifies a resource while fulfilling a goal



Resource provision

- Captures exchange of tangible resources between actors
  - Intangible resources **cannot** be transferred unless made concrete by a tangible means!
  - E.g. idea → paper, recommendation, document → official document

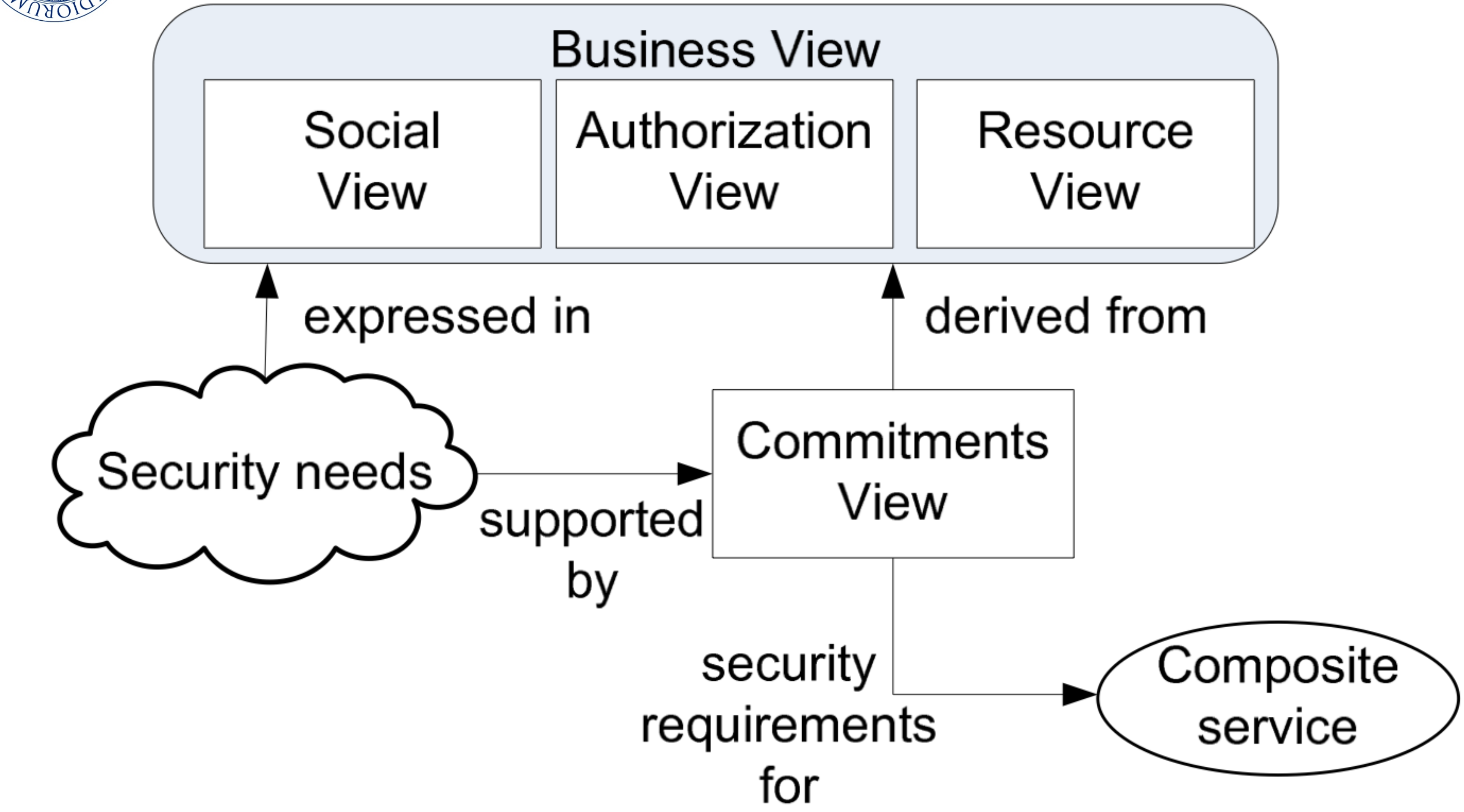


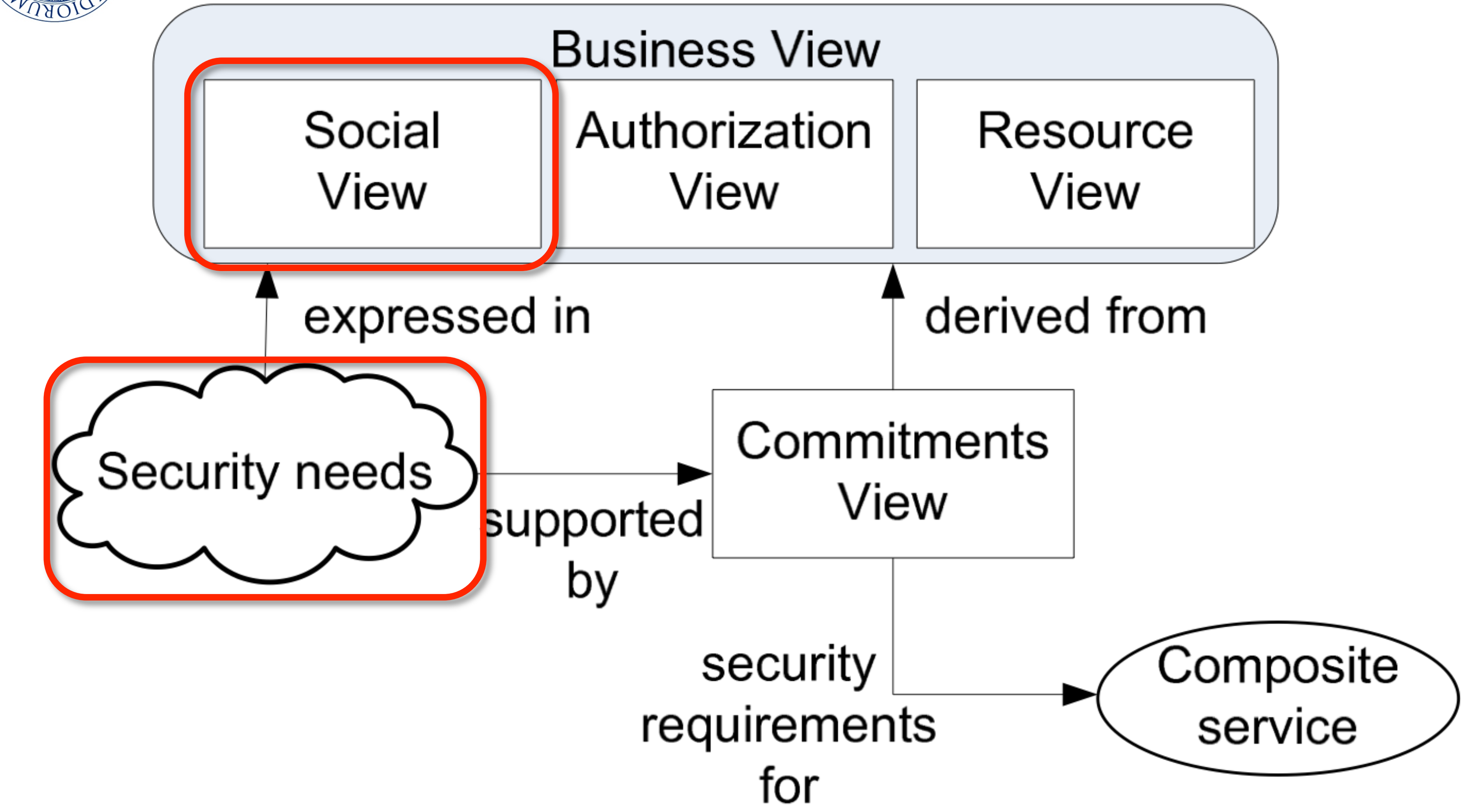
Aniketos STS modelling language

- Captures security requirements at the organisational level
  - We specify applications at the role level

- Allows to express security needs
  - Constrain interaction
  - Constrain data usage and flow

- Multi-view modelling
  - Model different *perspectives* of the socio-technical security model separately
  - Promote modularity and separation of concerns


Business View
Social View
Authorization View
Resource View
expressed in
derived from
Security needs
supported by
Commitments View
security requirements for
Composite service

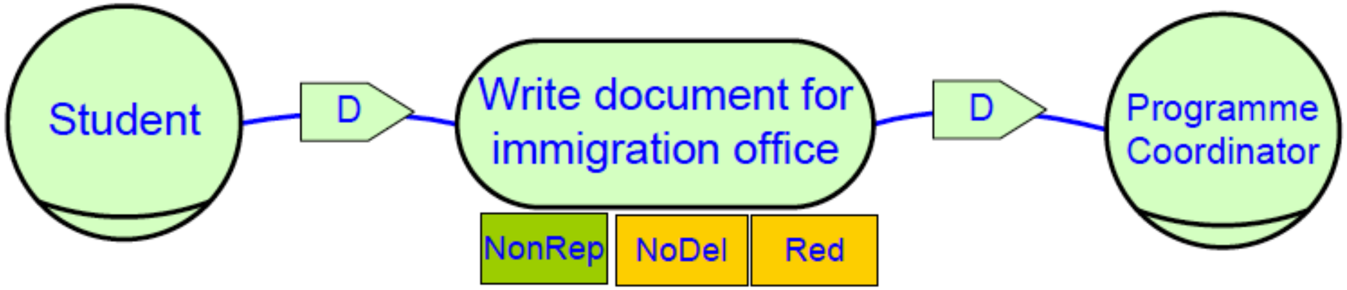

Business View
Social View
Authorization View
Resource View
expressed in
derived from
Security needs
supported by
Commitments View
security requirements for
Composite service

Social View

- Actor intentionality and sociality
  - Goal delegations
  - Resource provisions

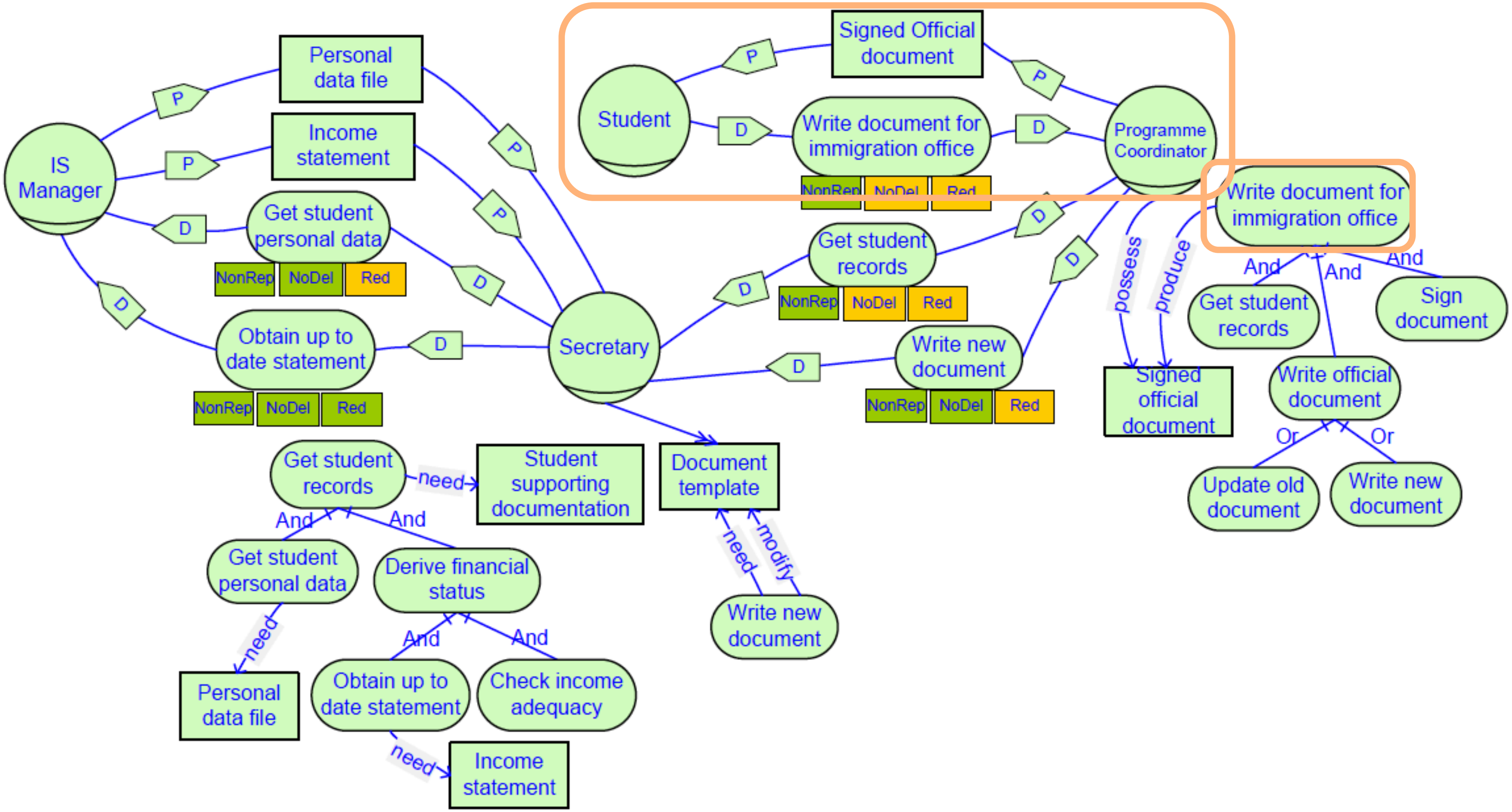
- Given that this view represents social relationships actors participate in, they can express their expectations concerning security need!

- Delegations can be annotated via security needs the delegator wants the delegatee to comply with



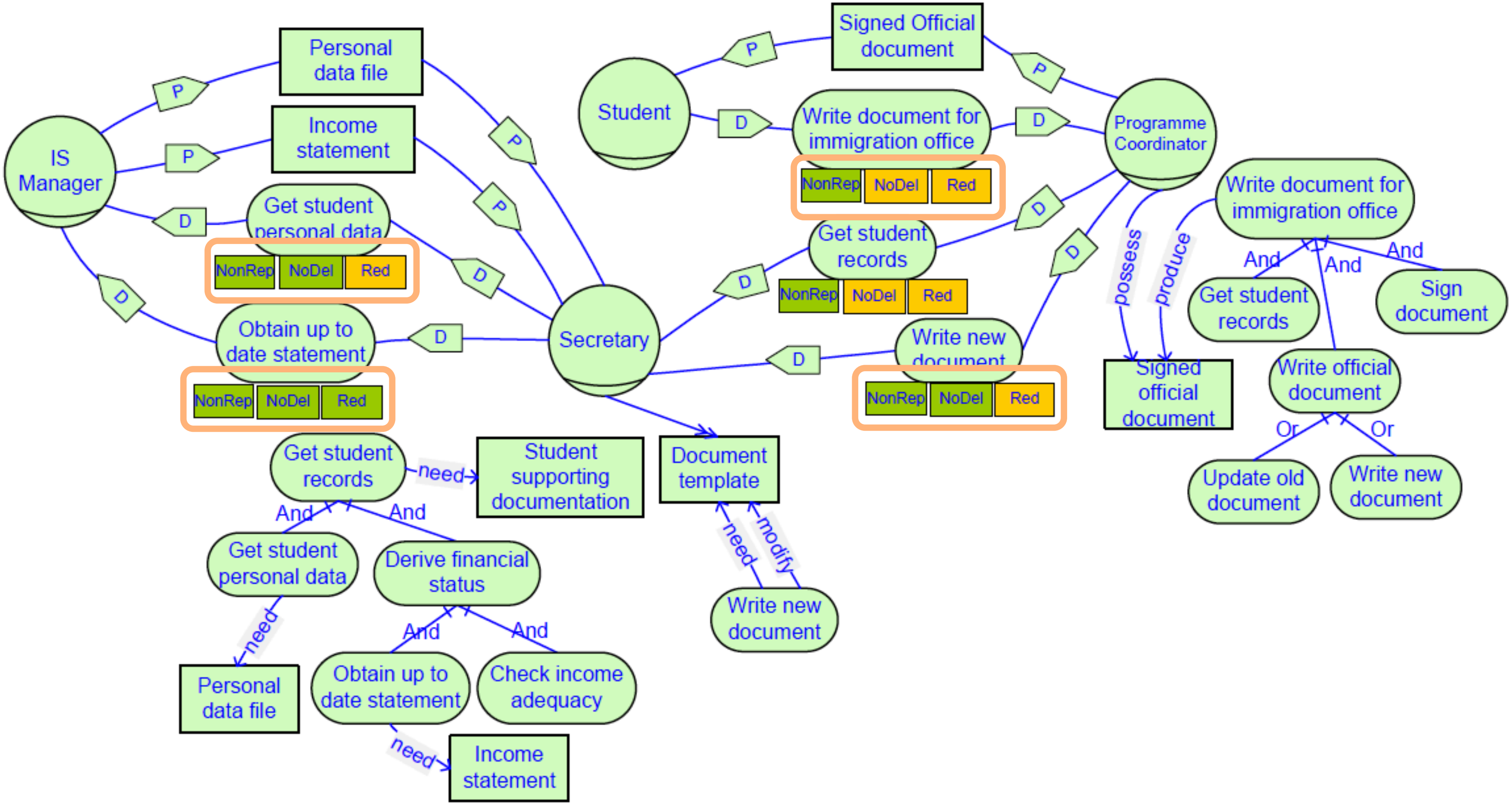
Social View

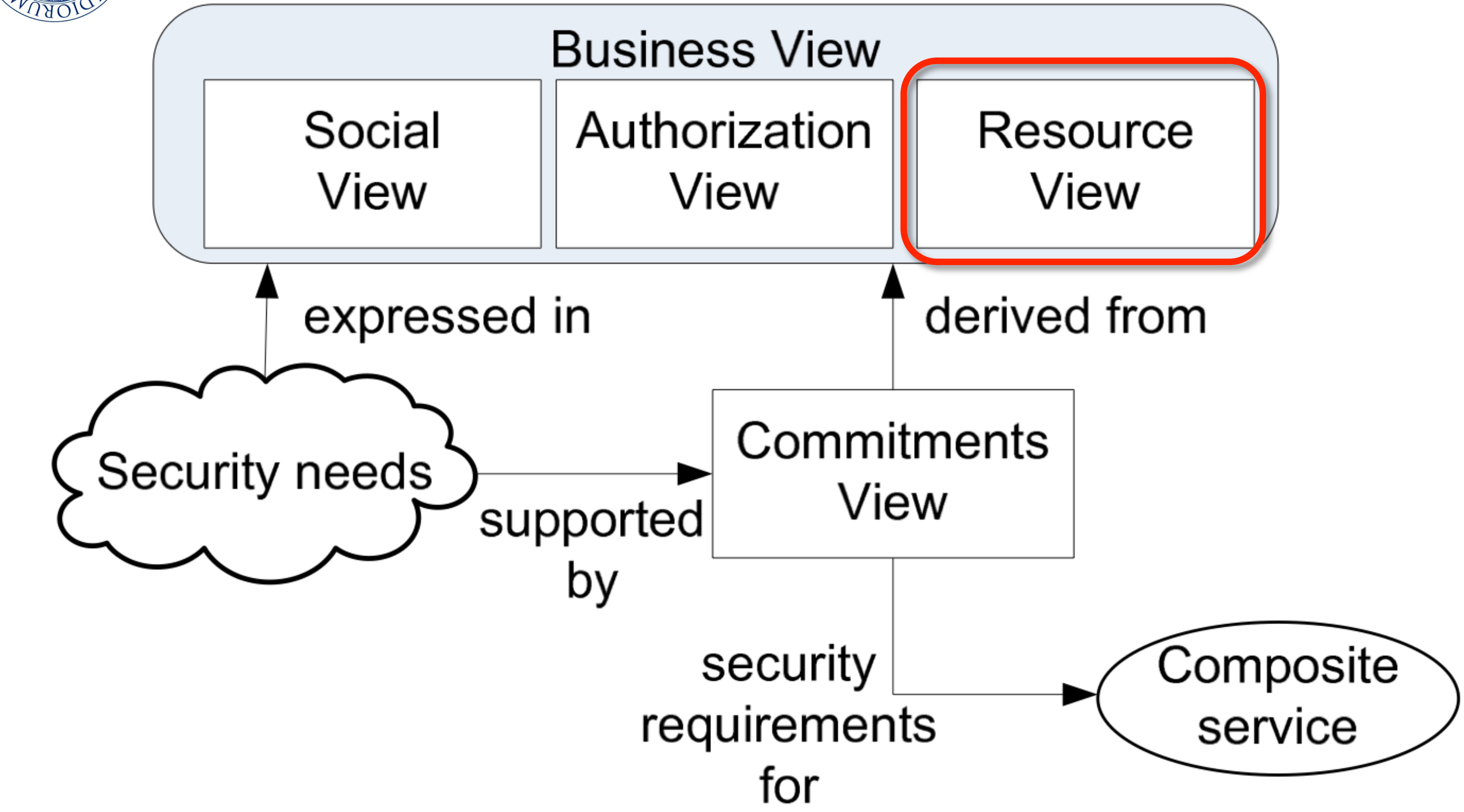
- Actor intentionality and sociality



Social View

- Actor intentionality and sociality




Business View
Social View
Authorization View
Resource View
expressed in
derived from
Security needs
supported by
Commitments View
security requirements for
Composite service

Resource view

- Characterize the resources in the considered setting
  - How they are structured

- Tangible vs Intangible
  - Made Tangible By: To understand which information (IResource) is transferred during provision of TResources
  - Composite Resources
    - Part Of: Between homogenous resources (tangible to tangible, intangible to intangible)

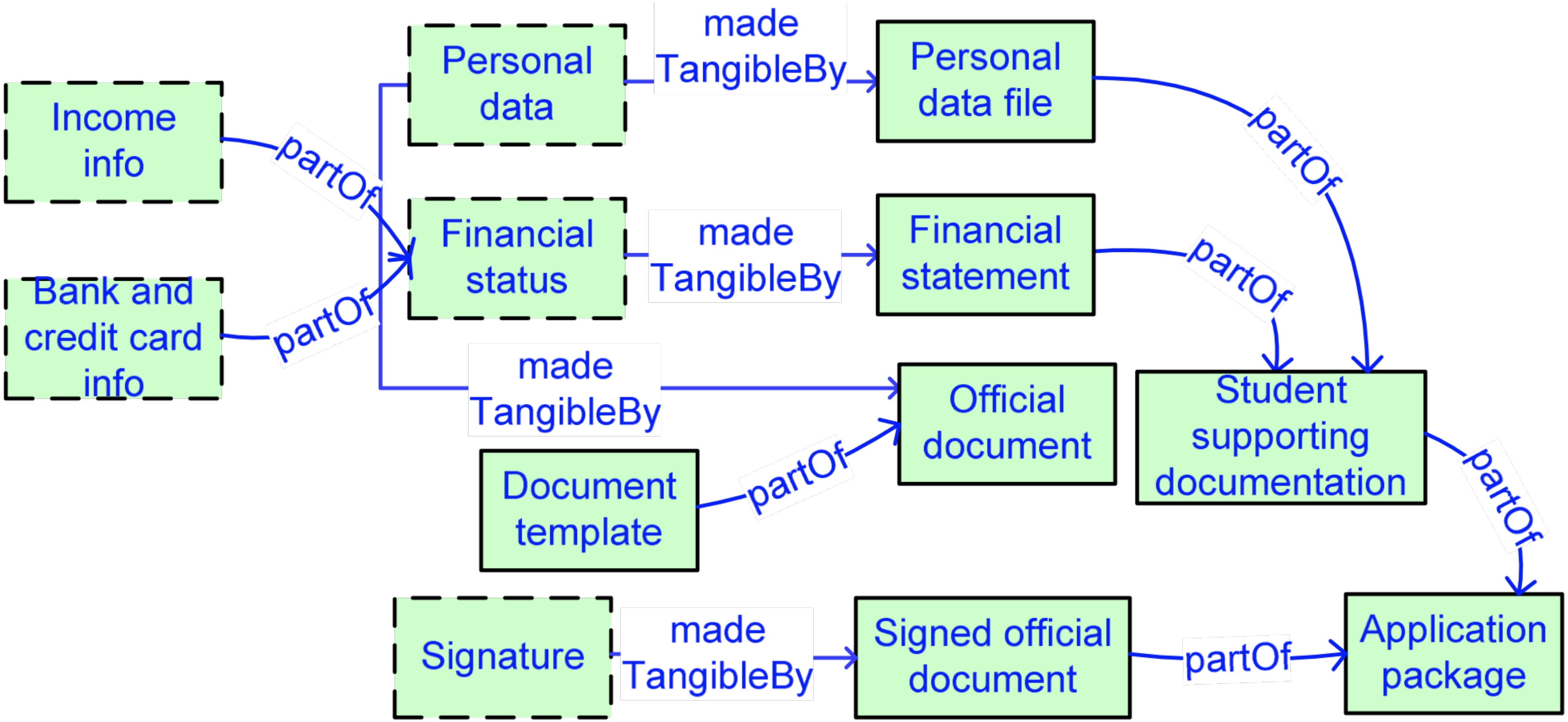
Resource view

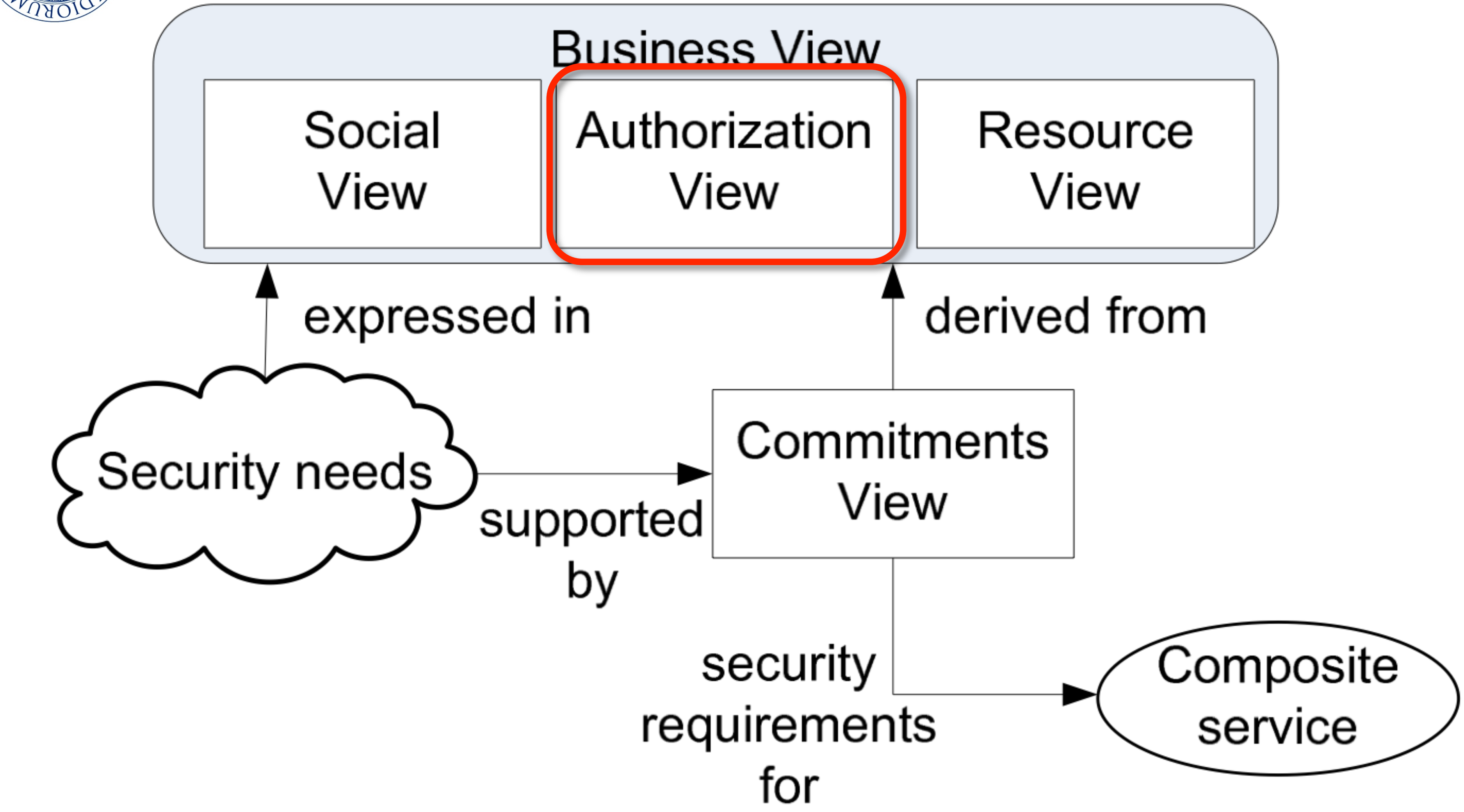
- Flexible representation of resources and relationships between them
  - An **IResource** can be made tangible by different **TResources**
    - **E.g.:** “Personal data” is made tangible by both “Personal data file” and “Official document”
  - A **TResource** can have no relevant **IResource**
    - **E.g.**: “Document template” contains no relevant information concerning the issuing of a permit of stay for an international student
  - A **TResource** might be part of multiple **TResources**
    - **E.g.: “**Income statement” might be part of a scholarship application too.

ANIKETOS

SEVENTH FRAMEWORK PROGRAMME

Resource view

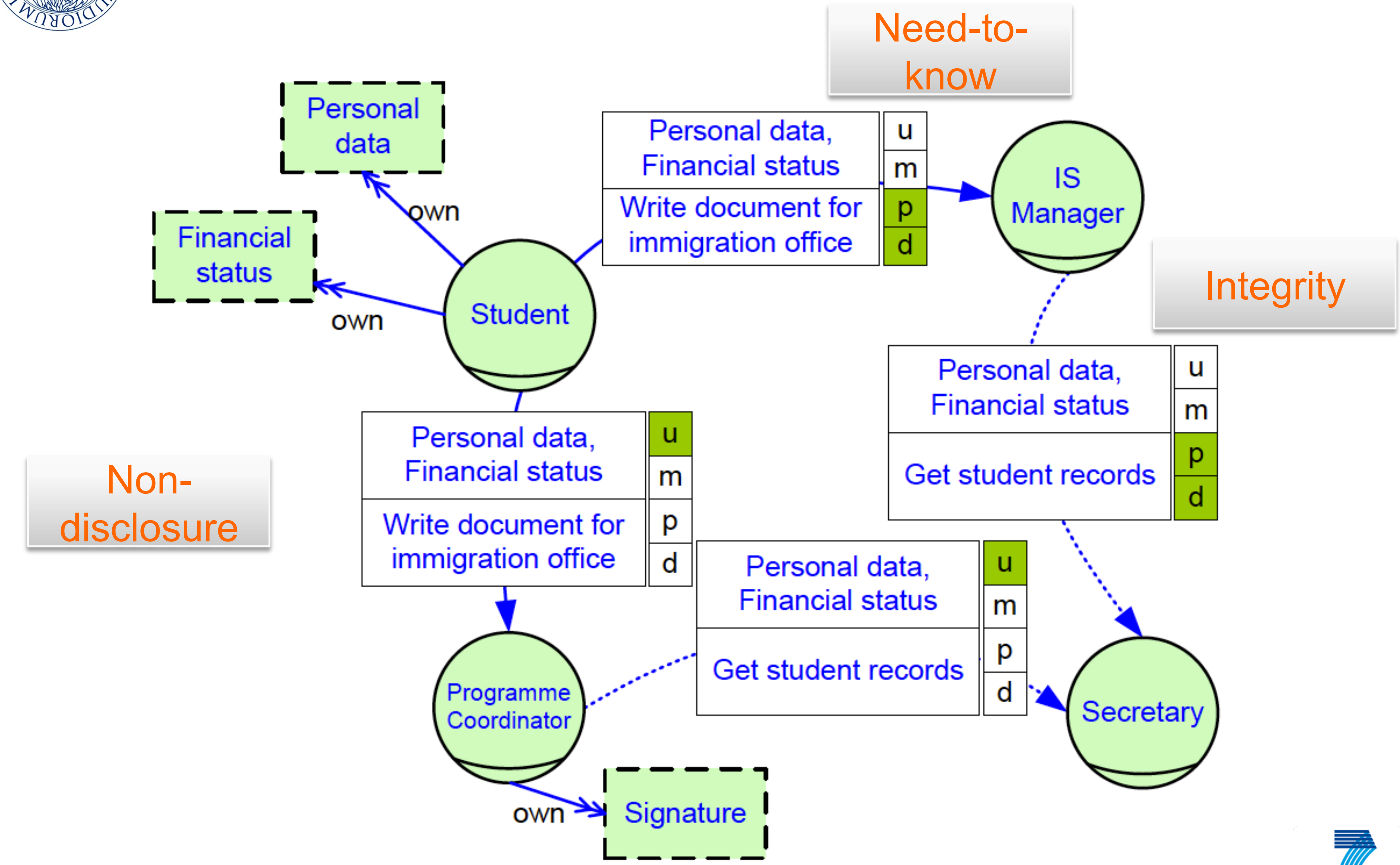


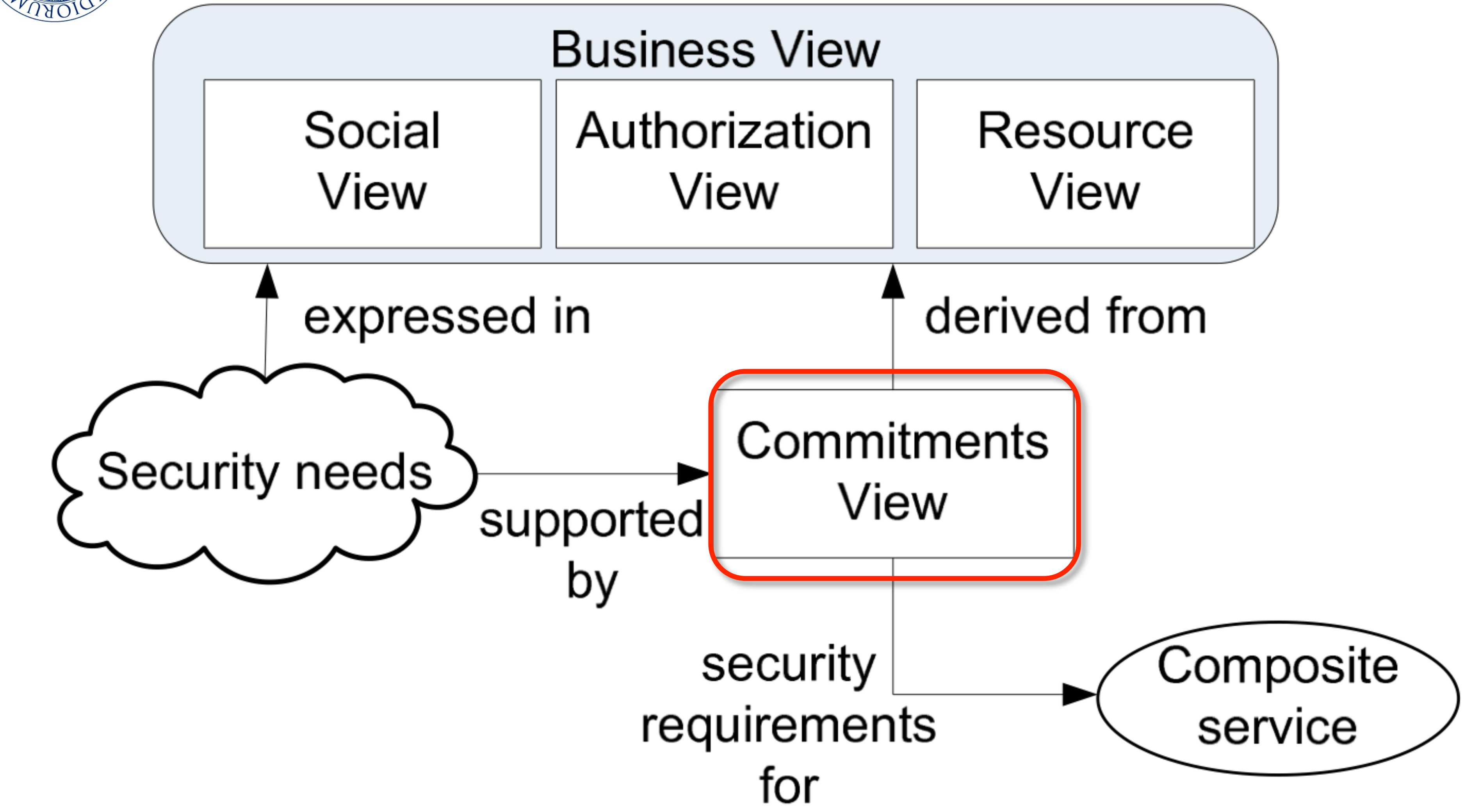

Business View
Social View
Authorization View
Resource View
expressed in
derived from
Security needs
supported by
Commitments View
security requirements for
Composite service

Authorization view

- Representation of authorizations necessary to determine if resources are exchanged and used in compliance with confidentiality restrictions.
  - Authorization
    - Transfer of rights between two actors
  - Authority can be limited by 3 orthogonal attributes:
    - Scope (of certain goals)
    - Operations
      - Usage, modification, production, distribution
    - Transferability
      - Further propagate rights to other actors

Authorization view


Need-to-know
Integrity
Non-disclosure
Personal data
Financial status
own
own
Student
Personal data, Financial status
Write document for immigration office
u
m
p
d
IS Manager
Personal data, Financial status
Get student records
u
m
p
d
Personal data, Financial status
Write document for immigration office
u
m
p
d
Personal data, Financial status
Get student records
u
m
p
d
Programme Coordinator
Secretary
own
Signature

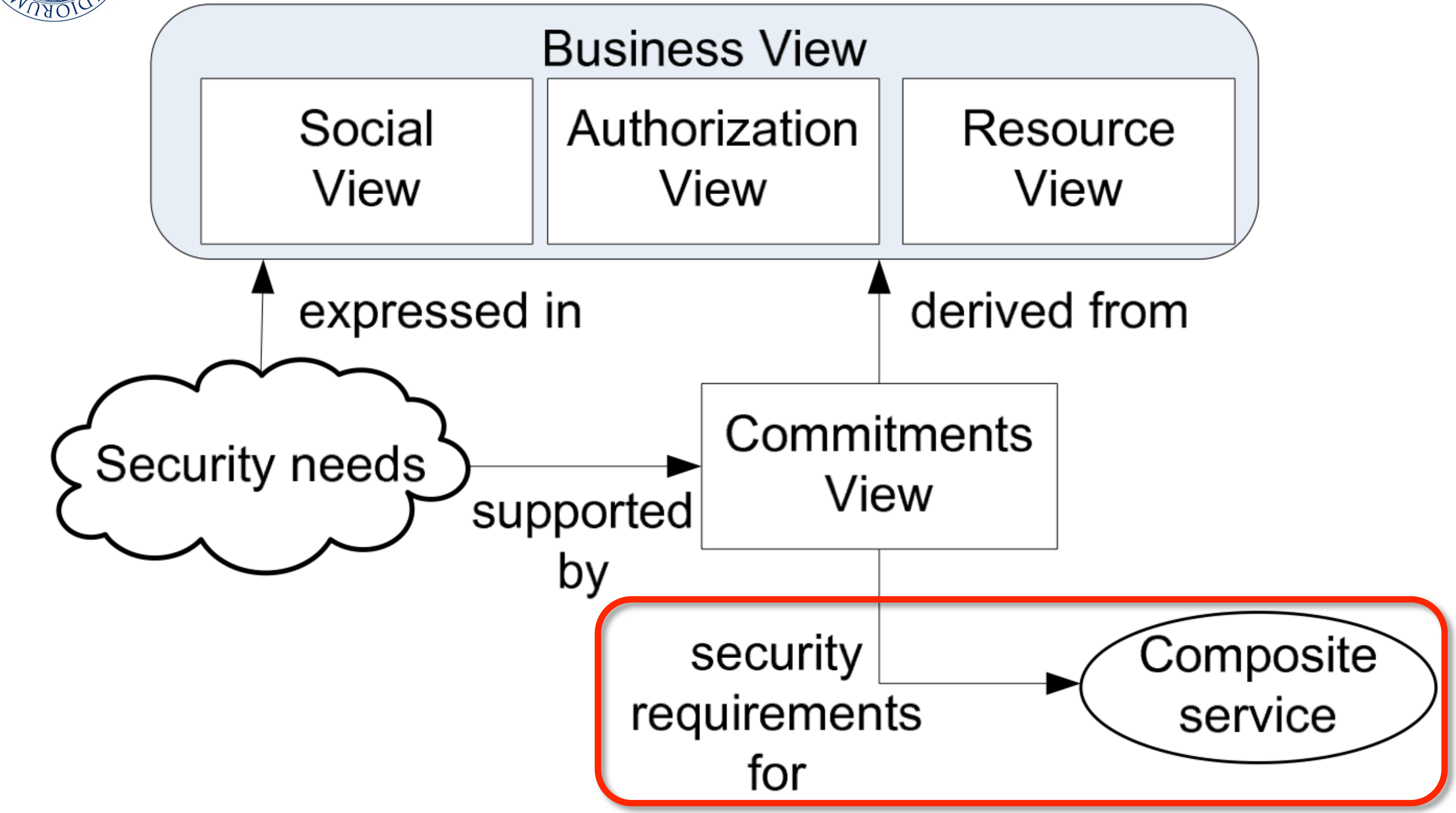

Business View
Social View
Authorization View
Resource View
expressed in
derived from
Security needs
supported by
Commitments View
security requirements for
Composite service

Ensuring Trustworthiness via Commitments

- Social Commitments are a simple yet powerful abstraction to model social interactions between actors
  - Interaction in terms of a contractual relation
- Formally
  - quaternary relation *C (debtor, creditor, antecedent, consequent)*
- Examples
  - A service interface is a set of commitments the service provider makes to prospective service consumers
  - *C (hotel, customer, prepayment done, room booked)*
- Unconditional commitments
  - *C (Assistant, Boss, T, organize trip)*

Why Social Commitments?

- Mechanism of control
  - Ensure security needs are met
- Obtain a more robust system
  - Guarantee things work in compliance with
    - organizational rules and regulations
    - software restrictions


Business View
Social View
Authorization View
Resource View
expressed in
derived from
Security needs
supported by
Commitments View
security requirements for
Composite service

Security requirements expressed via commitments

Debtor	Creditor	Security Requirement
IS Manager	Student	need-to-know(personal data ^ financial status, write document for immigration office, p ^ d)
Progr. Coord.	Student	need-to-know(personal data ^ financial status, write document for immigration office, u)
Secretary	Progr. Coord	need-to-know(personal data ^ financial status, get student records ^ write new document, u)
Secretary	IS Manager	need-to-know(personal data ^ financial status, get student records, p ^ d)

Secretary	IS Manager	non-disclosure(personal data ^ financial status)

IS Manager	Student	integrity(personal data ^ financial status)
Progr. Coord.	Student	integrity(personal data ^ financial status)
Secretary	Progr. Coord.	integrity(official document)
Secretary	IS Manager	integrity(personal data ^ financial status)

Security requirements expressed via commitments

Debtor	Creditor	Security Requirement
Progr. Coord	Student	non-repudiation(write document for immigration office)
Secretary	Progr. Coord.	non-repudiation(write document ^ get student records)
IS Manager	Secretary	non-repudiation(get student personal data ^ obtain up to date statement)
IS Manager	Secretary	redundancy(obtain up to date statement)
Secretary	Progr. Coord.	no-delegation(write document)
IS Manager	Secretary	no-delegation(get student personal data ^ obtain up to date statement)

Aniketos Socio-technical Security Modeling language

Elda Paja (University of Trento)

paja@disi.unitn.it