Aligning Service-Oriented Architectures with Security Requirements

Mattia Salnitri Fabiano Dalpiaz Paolo Giorgini

Software Evolution

- It affects all software systems
- From a software engineering perspective what may evolve are:
  - Software architectures:
    - due to technical changes (e.g.: a component is dismissed);
    - due to technical prerequisites (e.g.: new version of the O.S.).
  - Software requirements:
    - The needs of the Stakeholders may change;
    - Laws and norms may change.

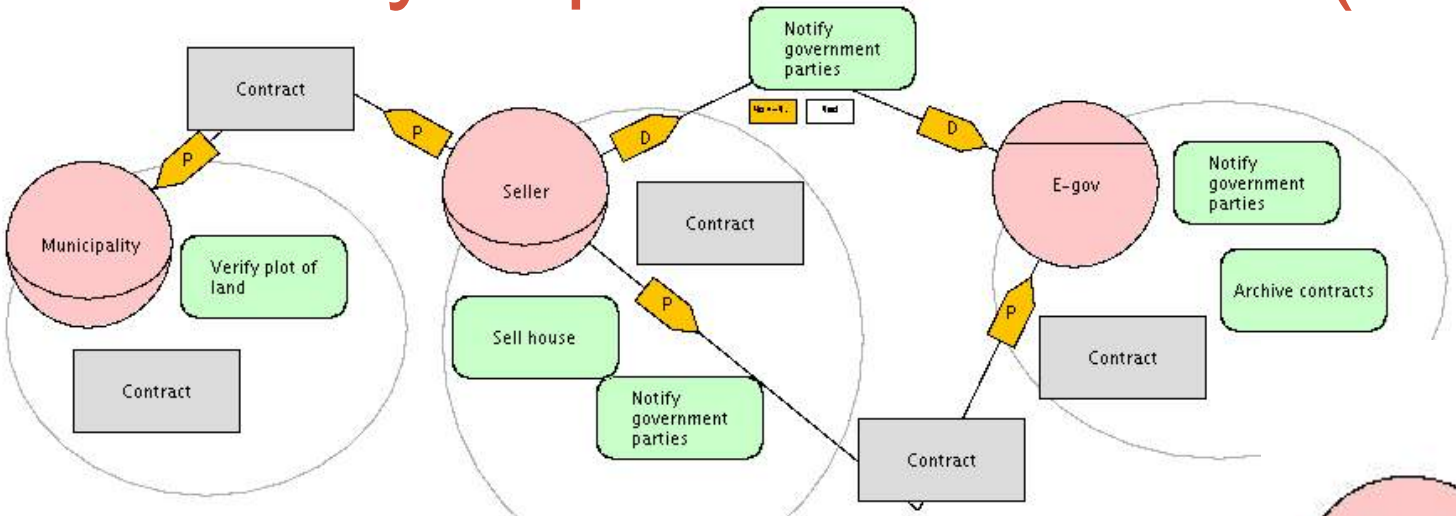
Requirement-Architecture Alignment

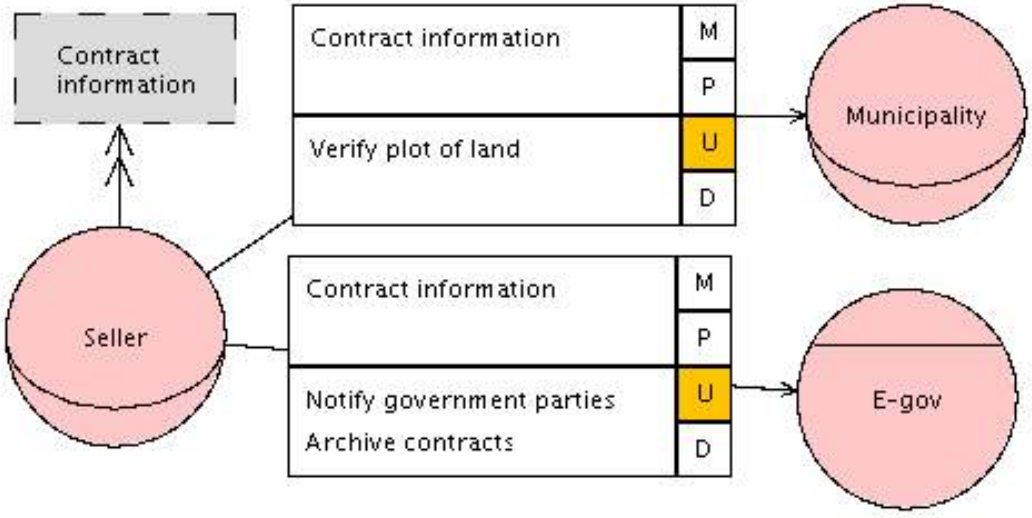
- Evolution may lead architecture and requirements to diverge.
- If they are not aligned, it means the requirements are not fulfilled
  - The system does not do what it is expected to do!
- Keeping an architecture aligned with requirements is a key process in the era of (software) evolution

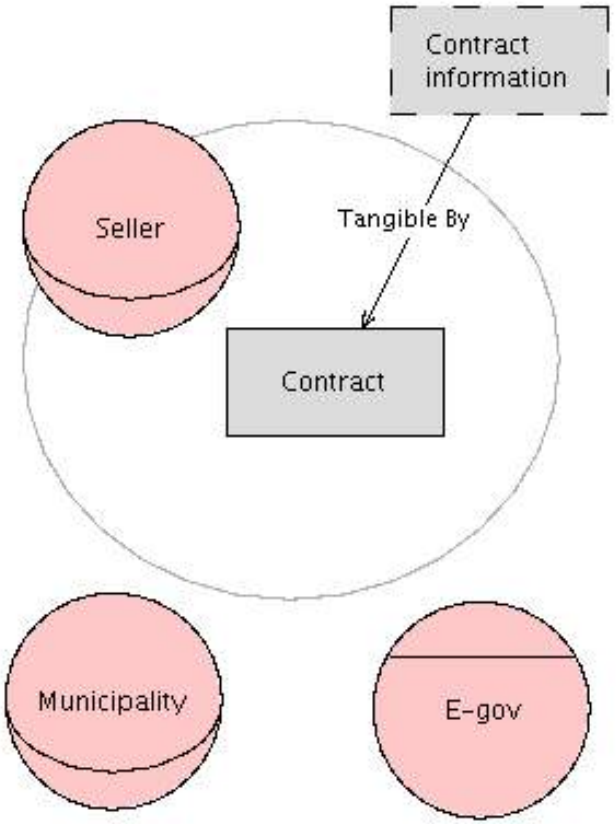
Security requirements…

- We focus on security requirements
  - If violated they have severe consequences
    - Law compliance
    - Loss of money
  - Examples
    - Integrity : Ensuring that information is not accessed by unauthorized persons [1]
    - Confidentiality : Ensuring that information is not altered by unauthorized persons in a way that is not detectable by authorized users [1]
- We model security requirements with commitments
  - Using STS-ml approach [2]

Security requirements models (STS-ml)







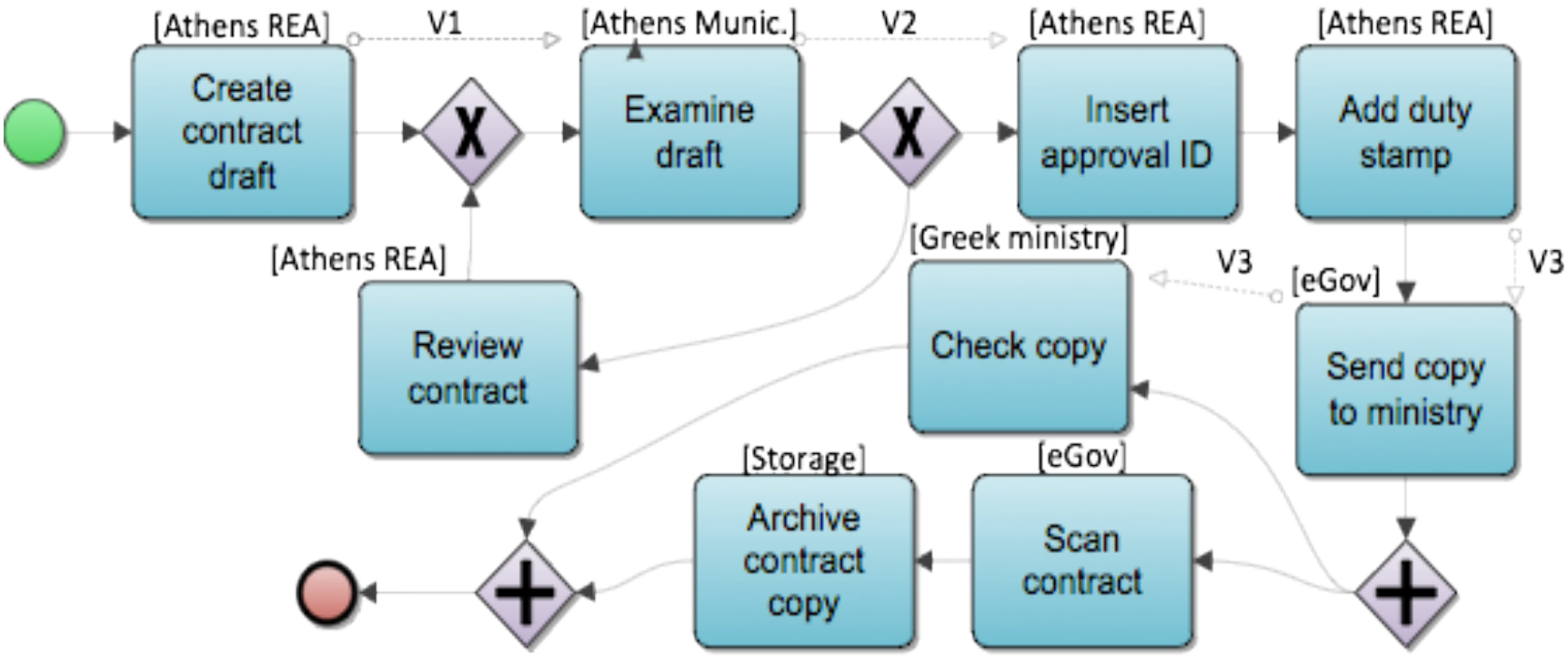
Security requirements specification (SRS)

Security requirements:
C(eGov application, Seller, D=delegation(Seller, eGov application, Government notified), non-rep(D))
C(e-Gov application, Seller, T, non-disc(Municipal approval $\wedge$ Sale information))
C(Municipality, Seller, T, non-discl(Sale information))
…
Knowledge base:
part-of(Land details, Sale information)
part-of(Price, Sale information)
…
tangible-by(Sale information, Official contract)
tangible-by(Sale information, Contract draft)
…
owns(Seller, Sale information)

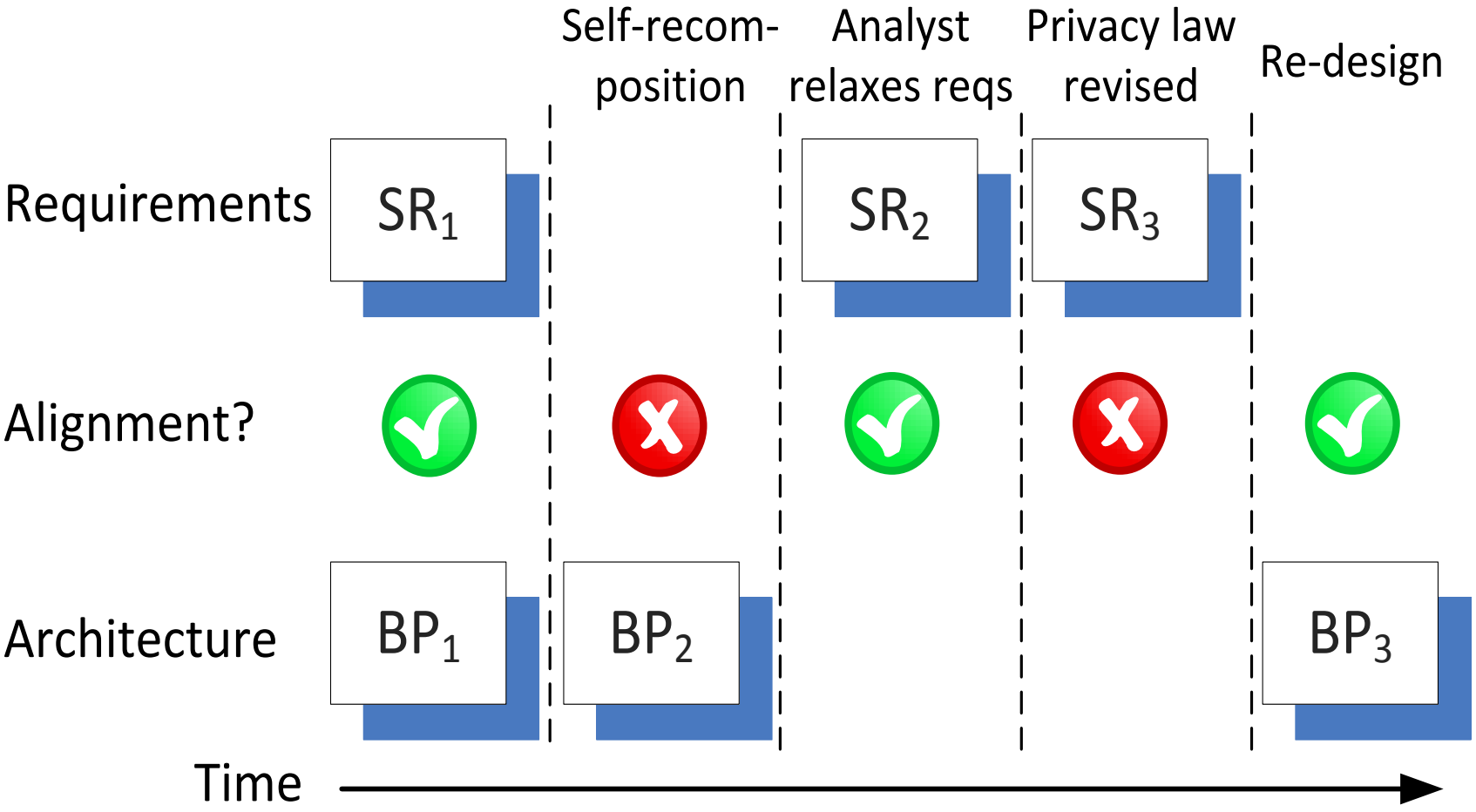
…and Service Oriented Architectures

- Service Oriented Architectures
  - Services provide functionalities to third parties
  - Evolution is intrinsic in services
- Service compositions
  - Used to describe the architecture of a set of interrelated services
  - Modelled as business process models(BPMN)

Service composition (eGov scenario)



Requirement-Architecture Alignment



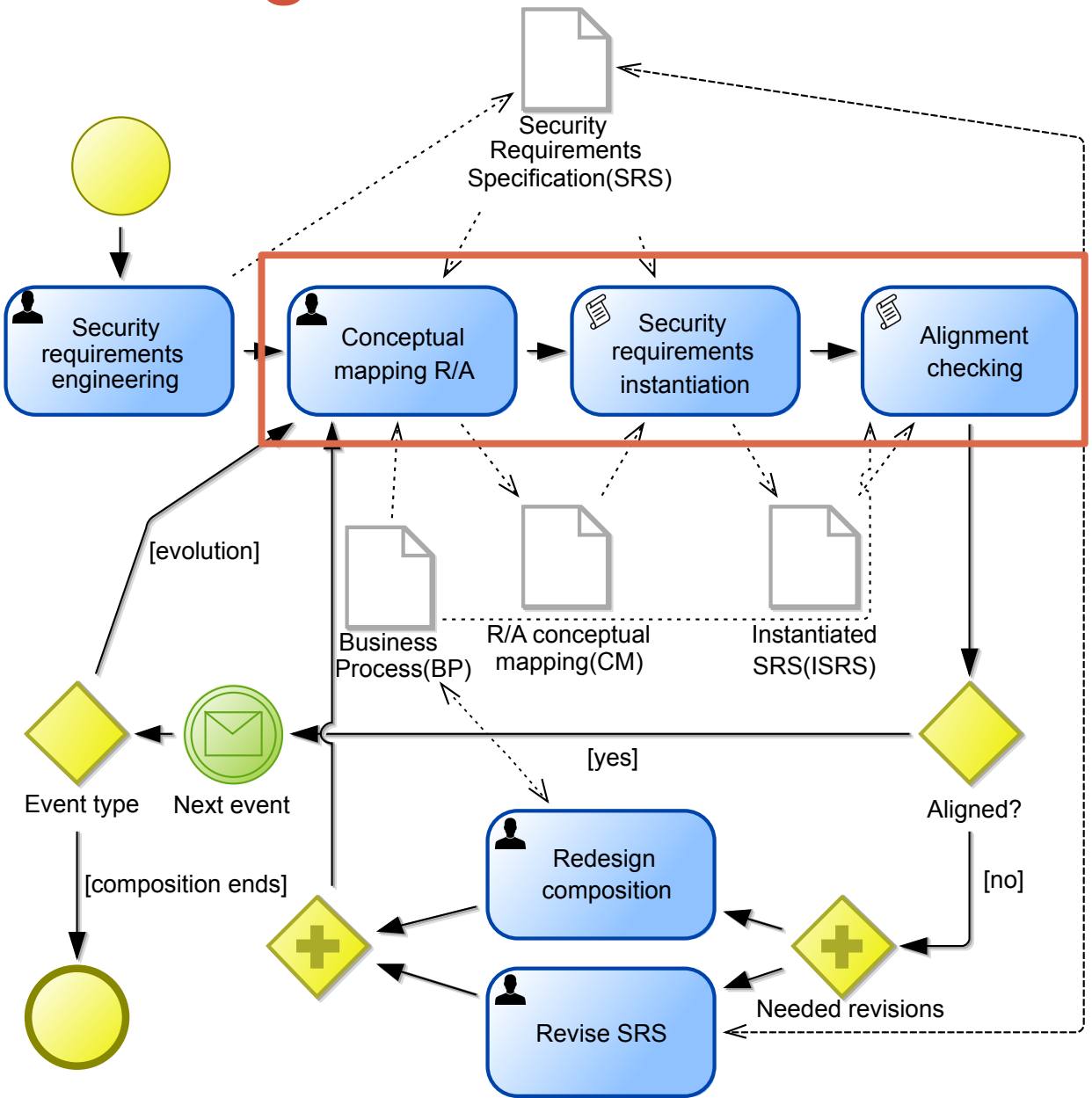
Objectives

- Define a methodological approach which permits the analyst to check the compliance (alignment) between security requirements and service composition
  - Define the conceptual mapping between security requirements elements and service composition elements
  - Automated algorithms to check compliance

Conceptual mapping

BPMN Element	Relation	STS-ml Element
Participant	is-a	Actor
Activity	relates-to	Goal
Variable (Data object)	represents	Information

Methodological framework



Example: Non-disclosure

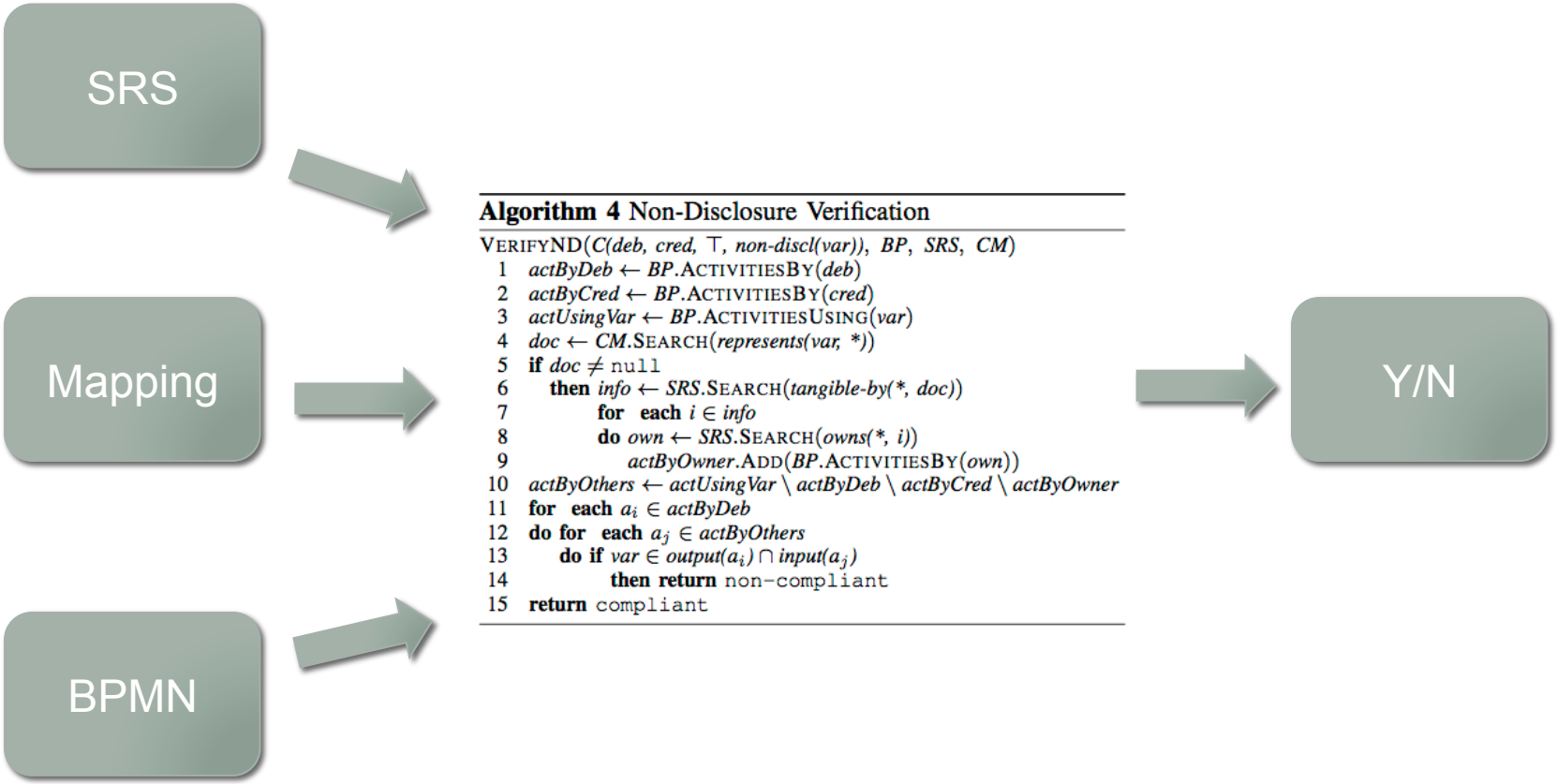
- Suppose to check the security requirement:
  - C1:C(eGov application, Seller, T, non-disc(Sale information))
- With the business process described above

Example: Non-disclosure

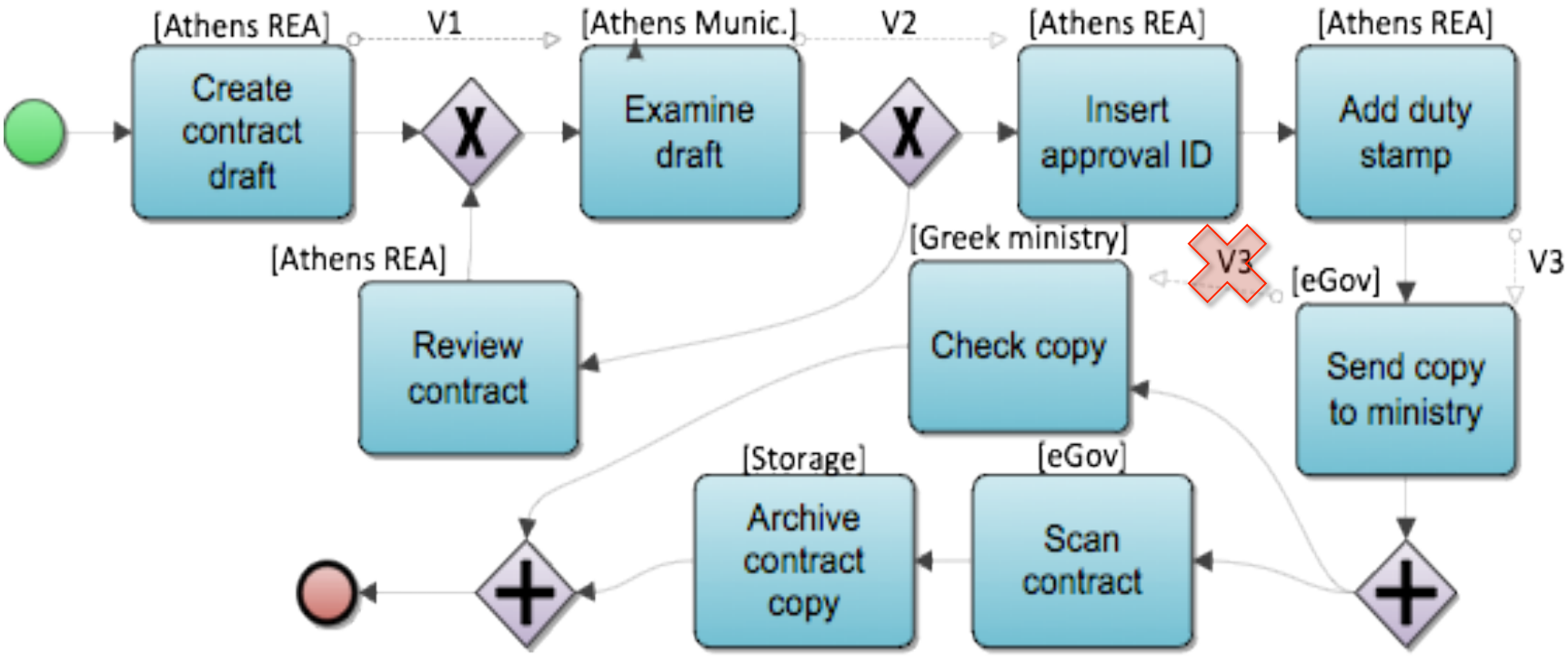
BPMN element	relation	STS-ml element
eGov	IS-A	eGov application
Storage	IS-A	eGov application
Athens REA	IS-A	Seller
V1	Represents	Sale information
V3	Represents	Sale information

- C1 is instantiated in
  - C1.1:C(eGov, Athens REA, T, non-discl(V1))
  - C1.2:C(eGov, Athens REA, T, non-discl(V3))
  - C1.3:C(Storage, Athens REA, T, non-discl(V1))
  - C1.4:C(Storage, Athens REA, T, non-discl(V3))

Example: Non-disclosure



Example: Non-disclosure



C1.2:C(eGov, Athens REA, T, non-discl(V3)) ✖

Conclusions & future works

- We have proposed:
  - a methodological approach to check alignment between security requirements and service compositions in an evolutionary system
- Future works
  - Implementation (Aniketos)
  - Extension of supported Security requirements

THANK YOU

Questions?

References

1. http://www.albion.com/security/intro-4.html
2. F. Dalpiaz, E. Paja and P. Giorgini, "Security requirements engineering via commitments" in Proc of STAST'11, 2001