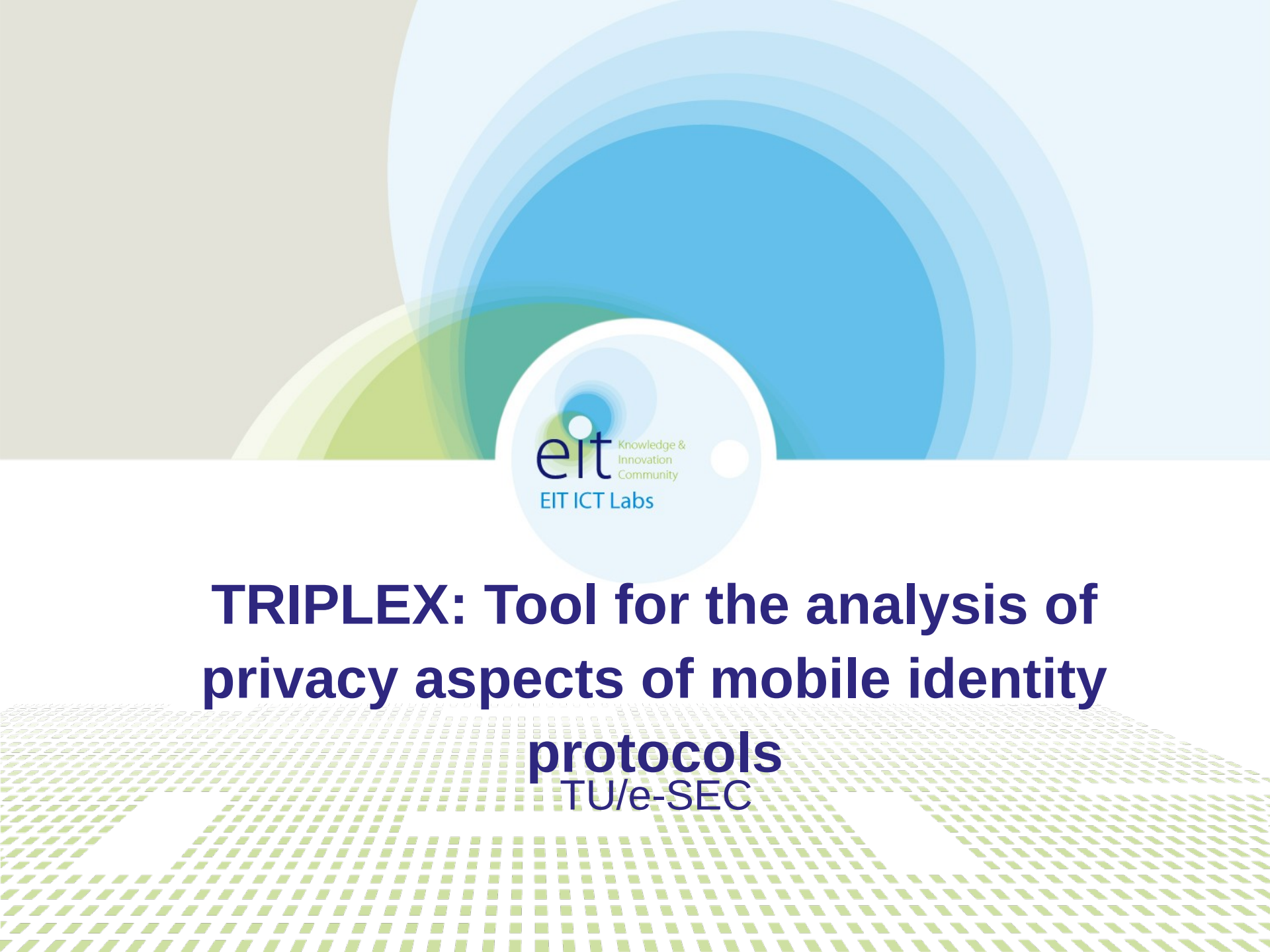


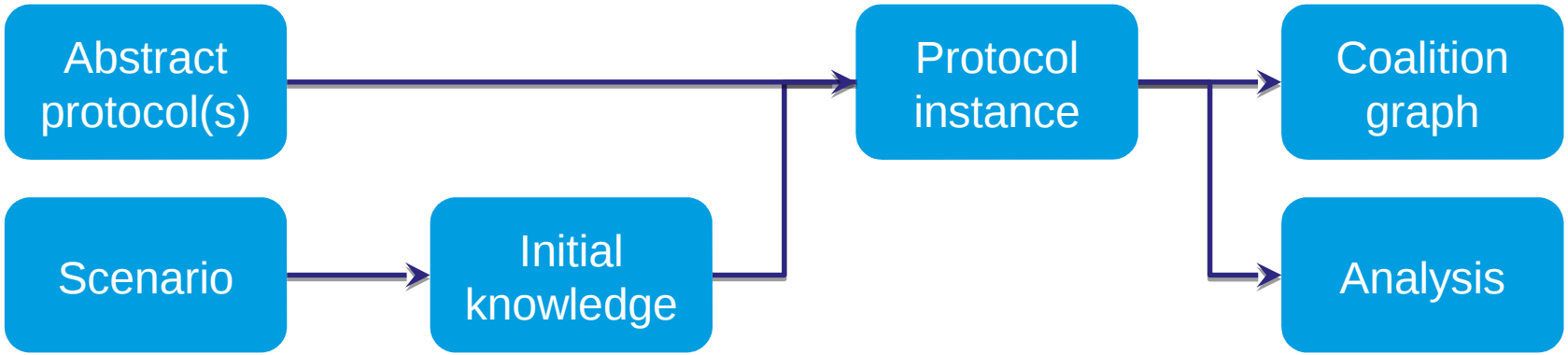
TRIPLEX: Tool for the analysis of privacy aspects of mobile identity protocols

TU/e-SEC

Goal / How to

- Tool for the analysis of privacy aspects of mobile identity protocol
  - analyse the communication between parties
  - validate privacy properties of identification systems and protocols

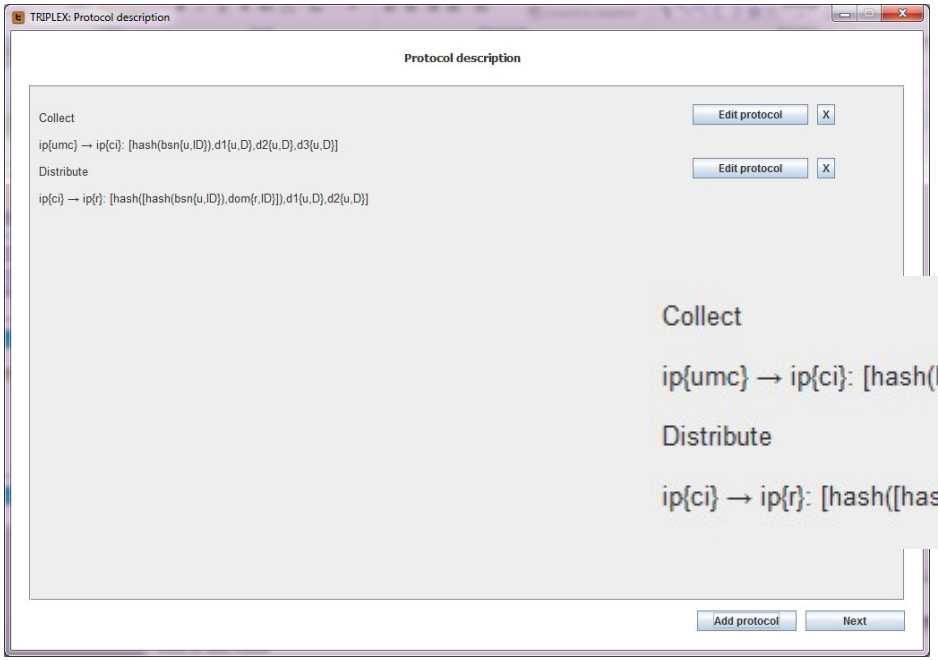
- We developed a framework (TRIPLEX) which allows
  - modelling identification protocols
  - stating/analysing privacy properties
  - capturing the knowledge of a single agent or a coalition of agents after the execution of one or more given protocols



Case study: Parelsnoer initiative

- Roles
  - Hospital
  - Central Infrastructure
  - Researcher
  - Patient
- Protocol Collect
  - Hospital sends to central infrastructure: h(bsn), d1, d2, d3
- Protocol Distribute
  - Central infrastructure sends to researcher: h(h(bsn), researcherID), d1, d2
- Test:
  - 2 protocol sessions for each protocol
  - 2 hospitals: umc1, umc2
  - 1 central infrastructure: ci
  - 1 researcher: r
  - 1 patient: u

TRIPLEX

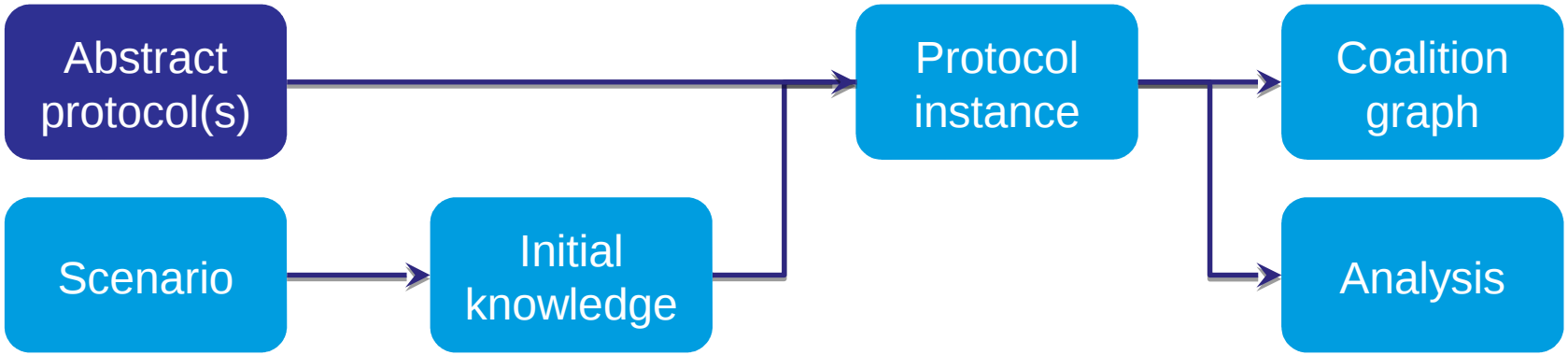


Collect

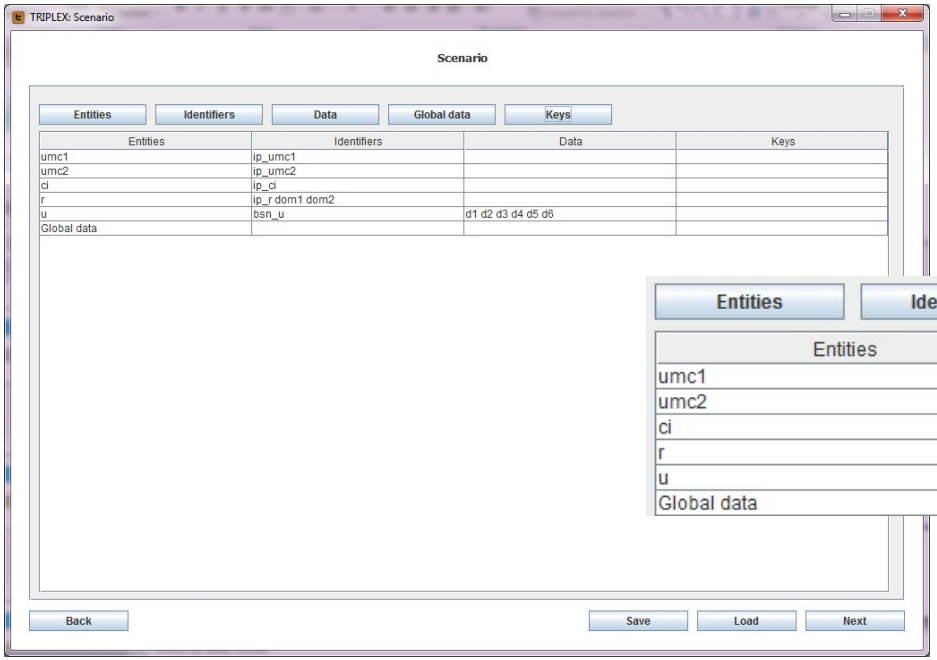
ip{umc} → ip{ci}: [hash(bsn{u,ID}),d1{u,D},d2{u,D},d3{u,D}]

Distribute

ip{ci} → ip{r}: [hash([hash(bsn{u,ID}),dom{r,ID}]),d1{u,D},d2{u,D}]

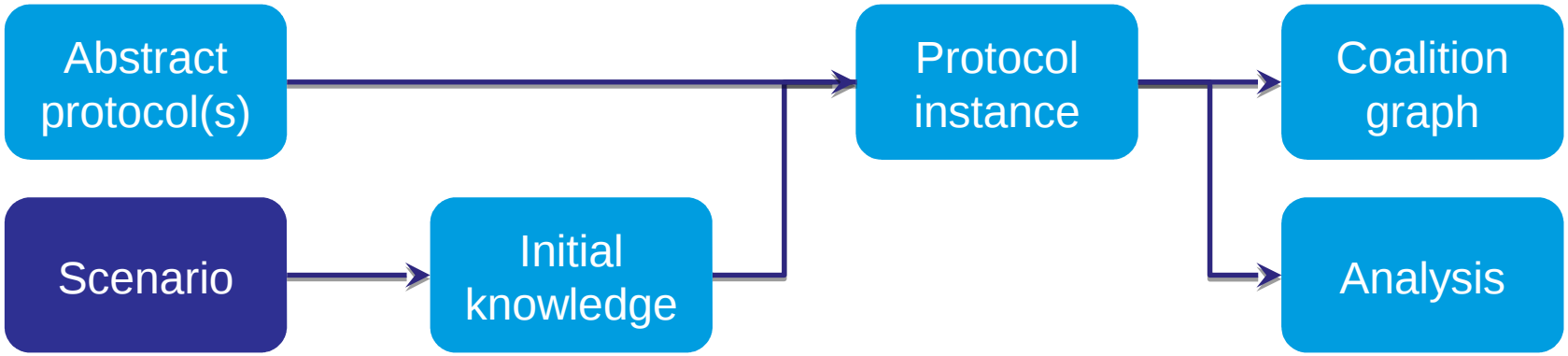


TRIPLEX

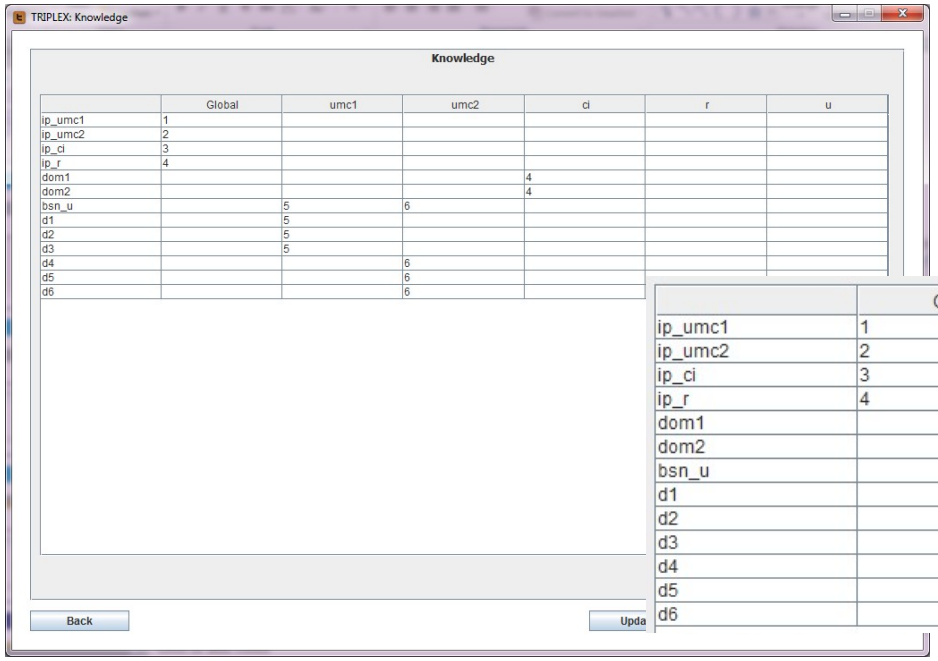


Entities	Identifiers	Data	Global data	Keys

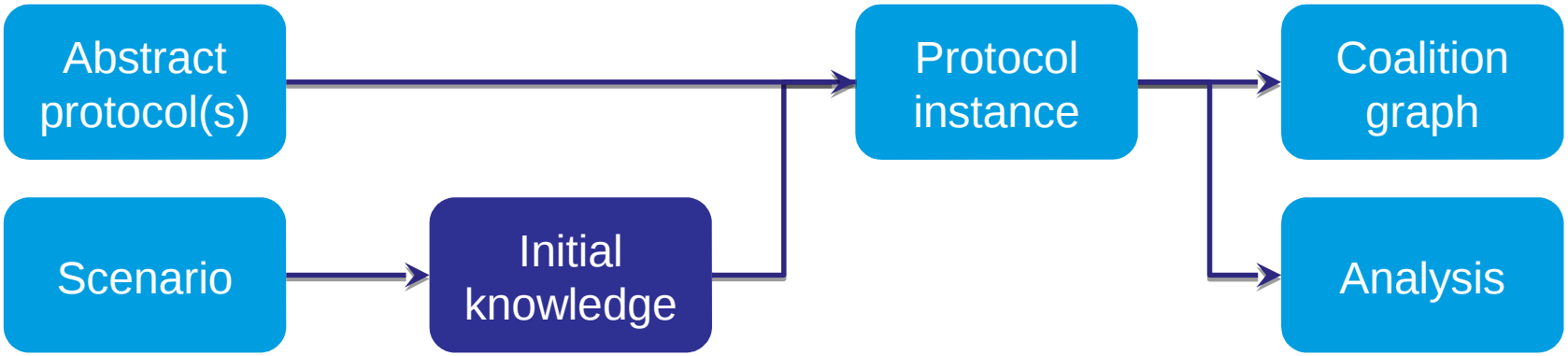
Entities	Identifiers	Data
umc1	ip_umc1	
umc2	ip_umc2	
ci	ip_ci	
r	ip_r dom1 dom2	
u	bsn_u	d1 d2 d3 d4 d5 d6
Global data		



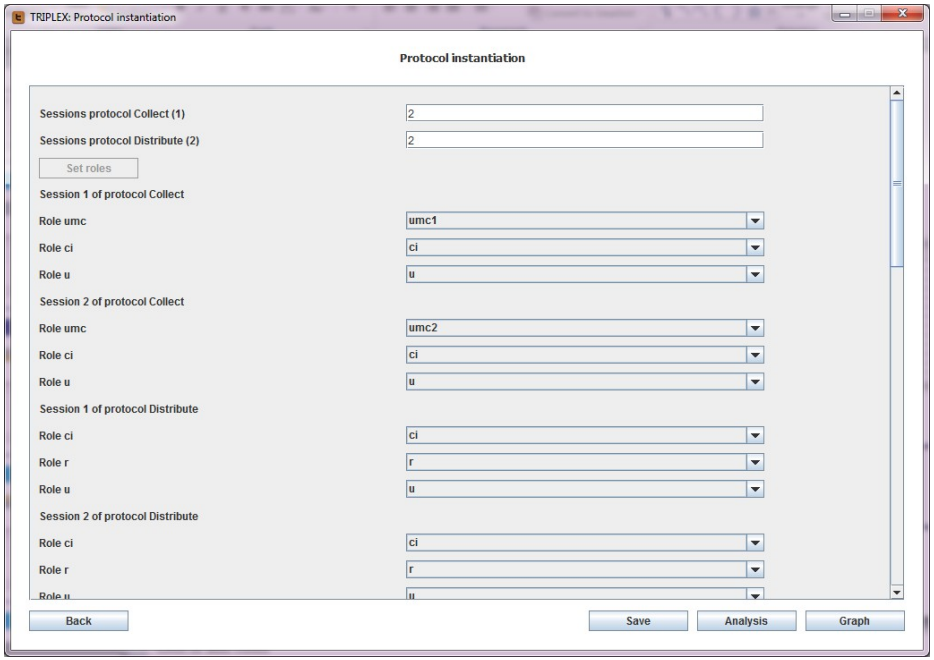
TRIPLEX

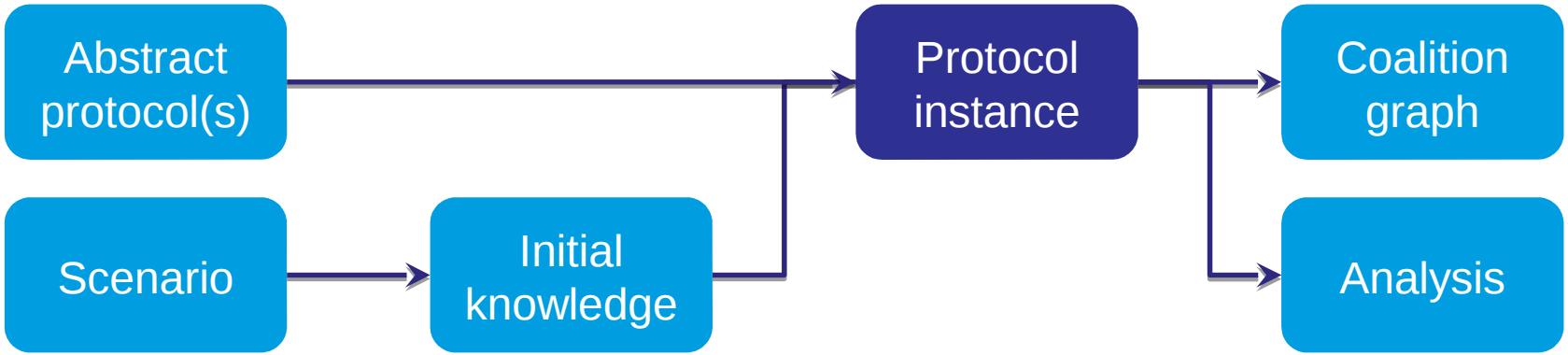


	Global	umc1	umc2	ci	r	u
ip_umc1	1					
ip_umc2	2					
ip_ci	3					
ip_r	4					
dom1				4		
dom2				4		
bsn_u		5	6			
d1		5				
d2		5				
d3		5				
d4			6			
d5			6			
d6			6			

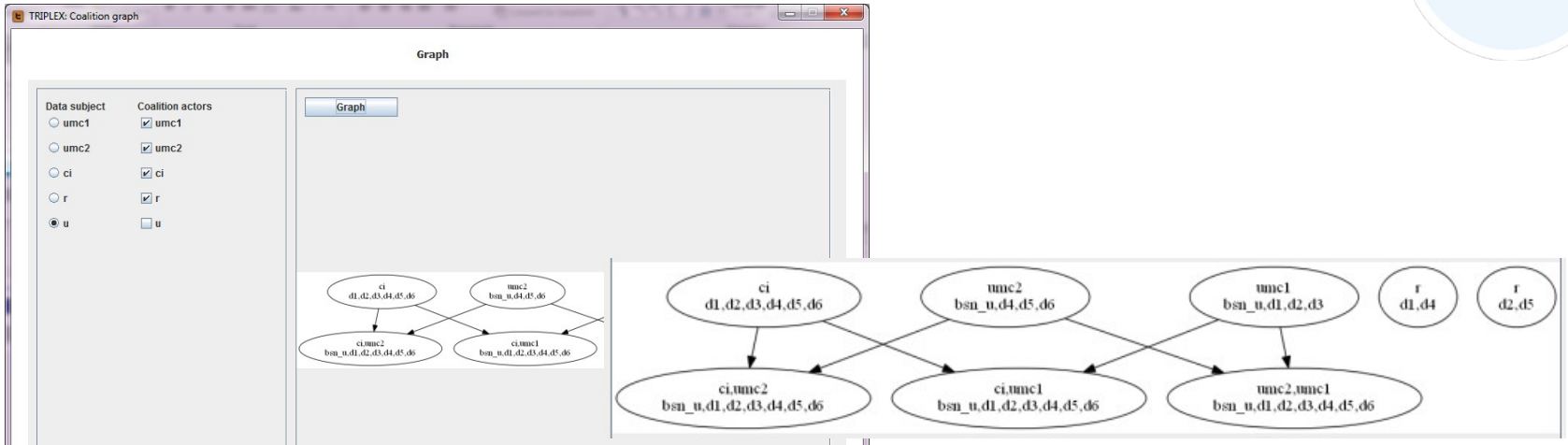


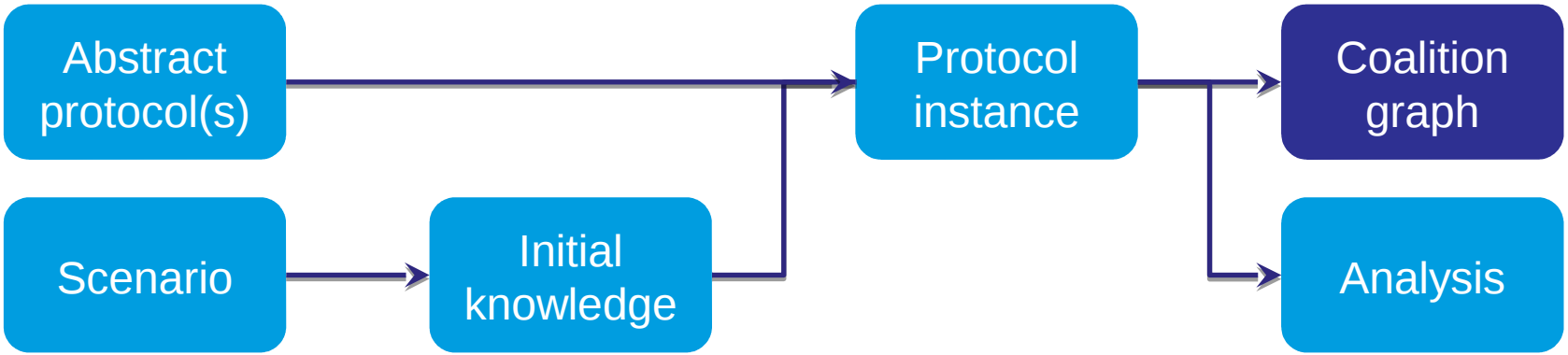
TRIPLEX


TRIPLEX: Protocol instantiation
Protocol instantiation
Sessions protocol Collect (1)
2
Sessions protocol Distribute (2)
2
Set roles
Session 1 of protocol Collect
Role umc
umc1
Role ci
ci
Role u
u
Session 2 of protocol Collect
Role umc
umc2
Role ci
ci
Role u
u
Session 1 of protocol Distribute
Role ci
ci
Role r
r
Role u
u
Session 2 of protocol Distribute
Role ci
ci
Role r
r
Back
Save
Analysis
Graph

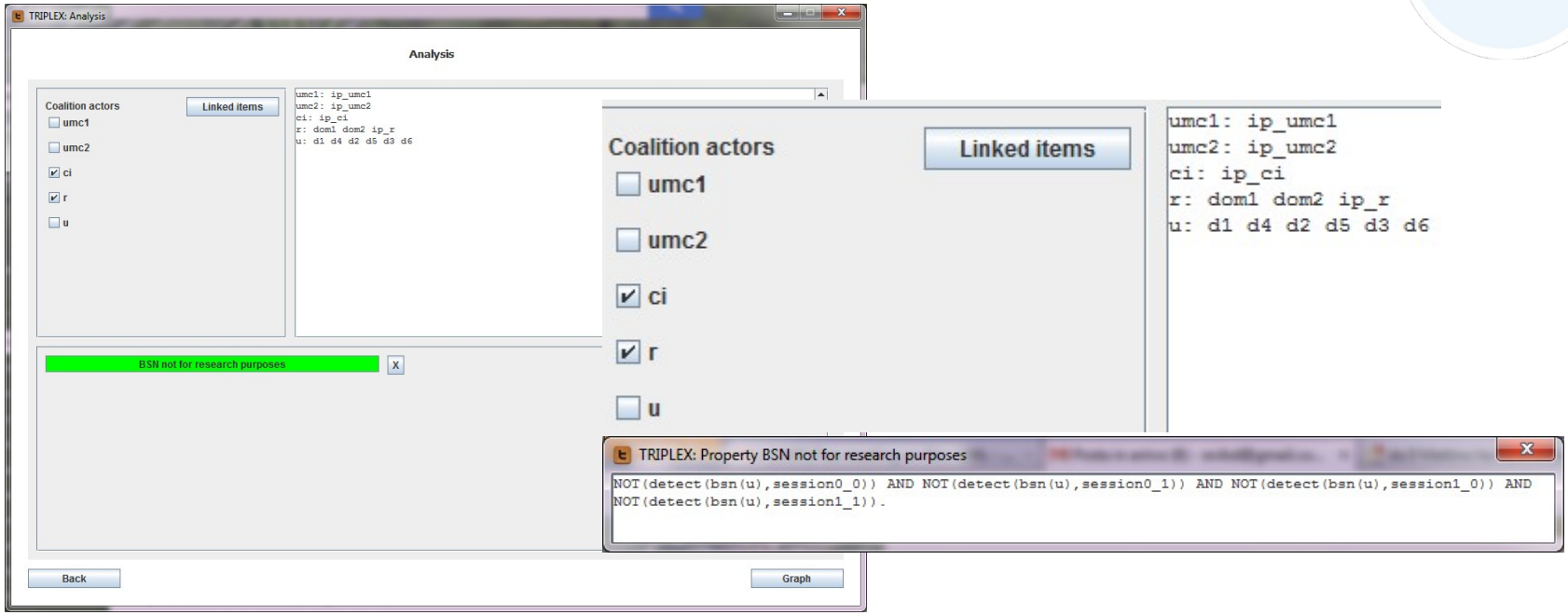

Abstract protocol(s)
Scenario
Initial knowledge
Protocol instance
Coalition graph
Analysis

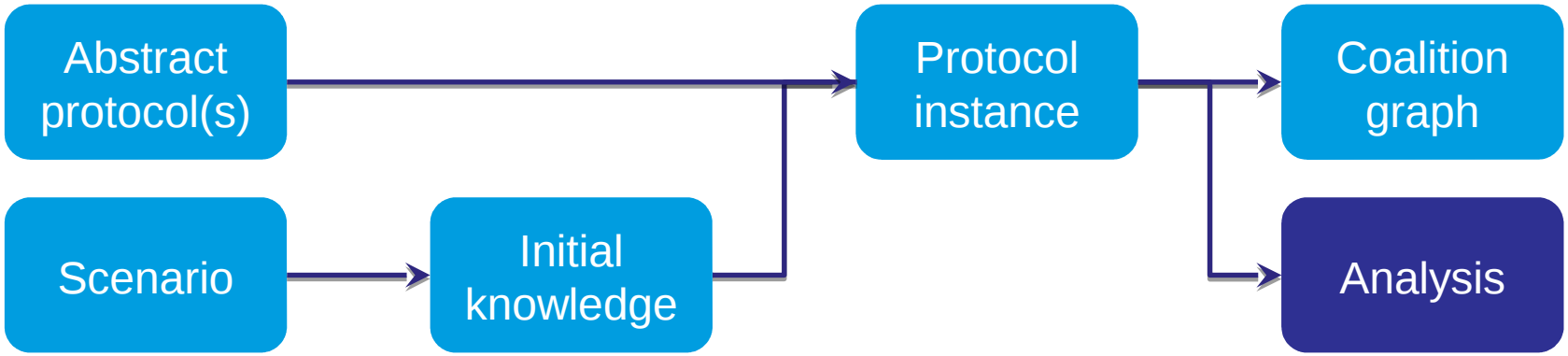
TRIPLEX


TRIPLEX: Coalition graph
Graph
Data subject
Coalition actors
umc1
umc2
ci
r
u
Graph
Back
Analysis
ci
d1,d2,d3,d4,d5,d6
umc2
bsn_u,d4,d5,d6
umc1
bsn_u,d1,d2,d3
r
d1,d4
r
d2,d5
ci,umc2
bsn_u,d1,d2,d3,d4,d5,d6
ci,umc1
bsn_u,d1,d2,d3,d4,d5,d6
umc2,umc1
bsn_u,d1,d2,d3,d4,d5,d6


Abstract protocol(s)
Scenario
Initial knowledge
Protocol instance
Coalition graph
Analysis

TRIPLEX


TRIPLEX: Analysis
Analysis
Coalition actors
Linked items
umc1
umc2
ci
r
u
umc1: ip_umc1
umc2: ip_umc2
ci: ip_ci
r: dom1 dom2 ip_r
u: d1 d4 d2 d5 d3 d6
BSN not for research purposes
X
Back
Graph
TRIPLEX: Property BSN not for research purposes
NOT(detect(bsn(u),session0_0)) AND NOT(detect(bsn(u),session0_1)) AND NOT(detect(bsn(u),session1_0)) AND NOT(detect(bsn(u),session1_1)).


Abstract protocol(s)
Scenario
Initial knowledge
Protocol instance
Coalition graph
Analysis