cetic
Your Connection to ICT Research

EVIDENCE
EUROPEAN INFORMATICS DATA EXCHANGE FRAMEWORK FOR COURTS AND EVIDENCE

A Goal-Oriented Requirements Analysis for the Collection, Use and Exchange of Electronic Evidence across EU Countries

Jean Christophe Deprez, Christophe Ponsard and Nikolaos Matskanis

iRENIC Workshop – RE'16
Beijing, September 12, 2016

PLUS HAUT
ET PLUS PROCHE
LE FONDS EUROPÉEN DE DÉVELOPPEMENT RÉGIONAL
ET LA WALLONIE INVESTISSENT DANS VOTRE AVENIR

FEDER
UNION EUROPEENNE

Wallonie

Centre d'Excellence en **Technologies** de l'**Information** et de la **Communication**
www.cetic.be

Motivation

- All legal proceedings rely on the production of evidence in order to be instituted.
- Courts are going digital, like everything else in our world

  “Electronic Evidence (EE) is no different from traditional evidence in that is necessary for the party introducing it into legal proceedings, to be able to demonstrate that it is no more and no less than it was, when it came into their possession. In other words, no changes, deletions, additions or other alterations have taken place.” -- Council of Europe
- Challenge: evidence exchange vs integrity preservation
- Our goal:
  - Present overall rationale behind different scenarios relating to the collection/use/exchange of EE across EU (EVIDENCE project)
  - Discuss - at a high level - possible directions for a software architecture on exchanging investigation data.
- Approach: goal-oriented requirements engineering
  - Give feedback about the approach

Outline

- Motivation
- Domain Description
- Methodology: GRL
- High Level Goals
- Refinement of Efficient and Trusted Exchange of Evidence
- Discussion
- Conclusions

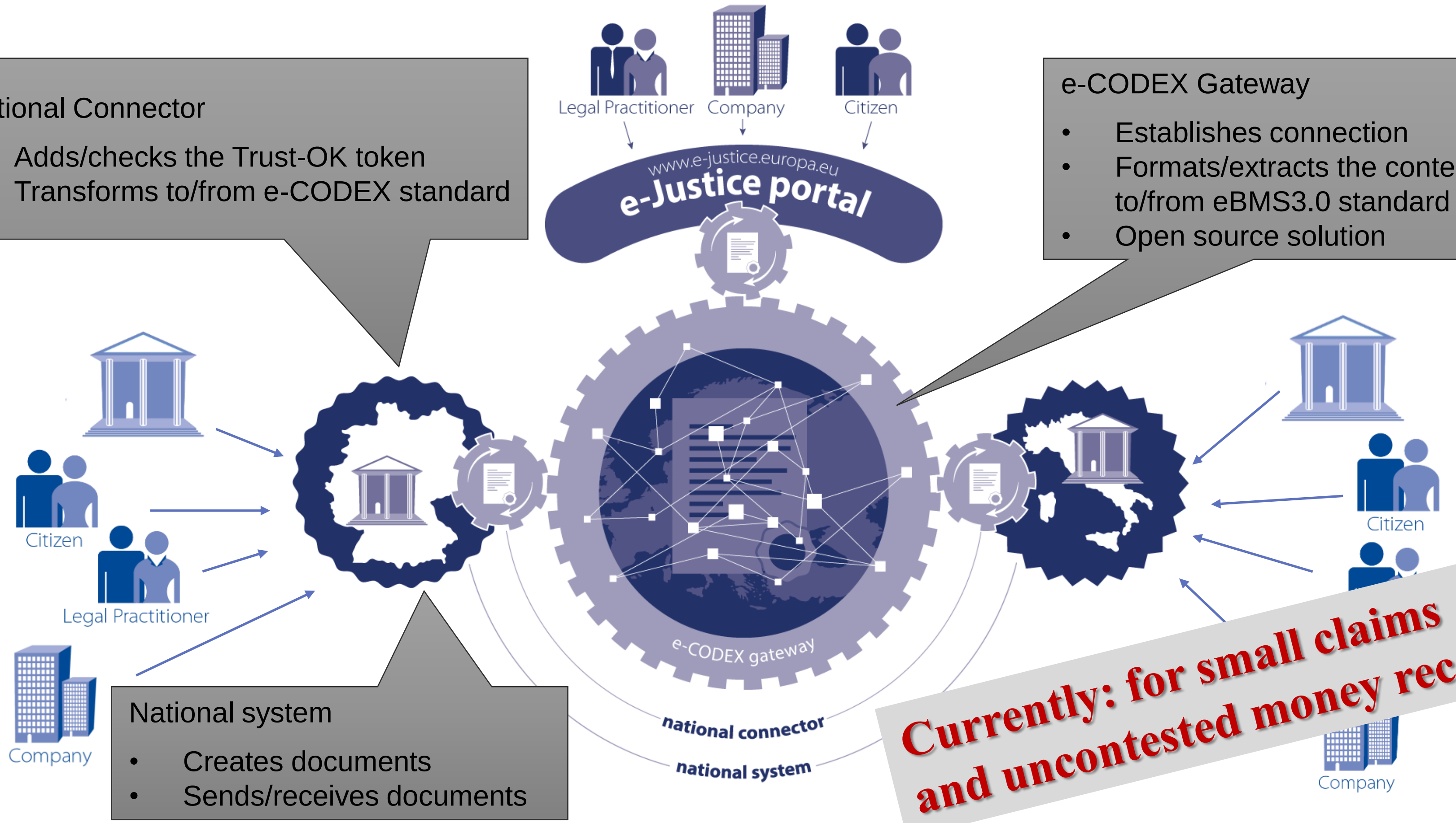
As-Is: Partial Solution (e-CODEX)

National Connector

- Adds/checks the Trust-OK token
- Transforms to/from e-CODEX standard

e-CODEX Gateway

- Establishes connection
- Formats/extracts the content to/from eBMS3.0 standard
- Open source solution



National system

- Creates documents
- Sends/receives documents

Currently: for small claims and uncontested money recovery

As-Is: Currently Used Exchanged Systems

- TESTA-NG
    - secure (encrypted) network provided by the **European Commission**.
    - Each TESTA-NG node is provided with a standard rack system to exchange with other nodes on the network.
- VPN+TESTA-NG: between **Eurojust and Member State Bureaus**
    - Message exchanging (e-mail type of services)
    - secure file transferring (SFTP),
    - video streaming services and other data services
- **INTERPOL**'s i-24/7 and I-link systems
    - based on VPN tunnels over leased lines
    - communication links between law enforcement agencies (LEA) in all member countries.
- The SIENA system at **EUROPOL** (+ also Eurojust)
    - a secure Information exchange network
    - deployed over a leased line
    - + Large File Exchange system (SFTP type) for large files

How to Define/Capture Domain Knowledge about EE

- CybOX (Cyber Observable eXpression):
  - Open Source language for representing cyber objects

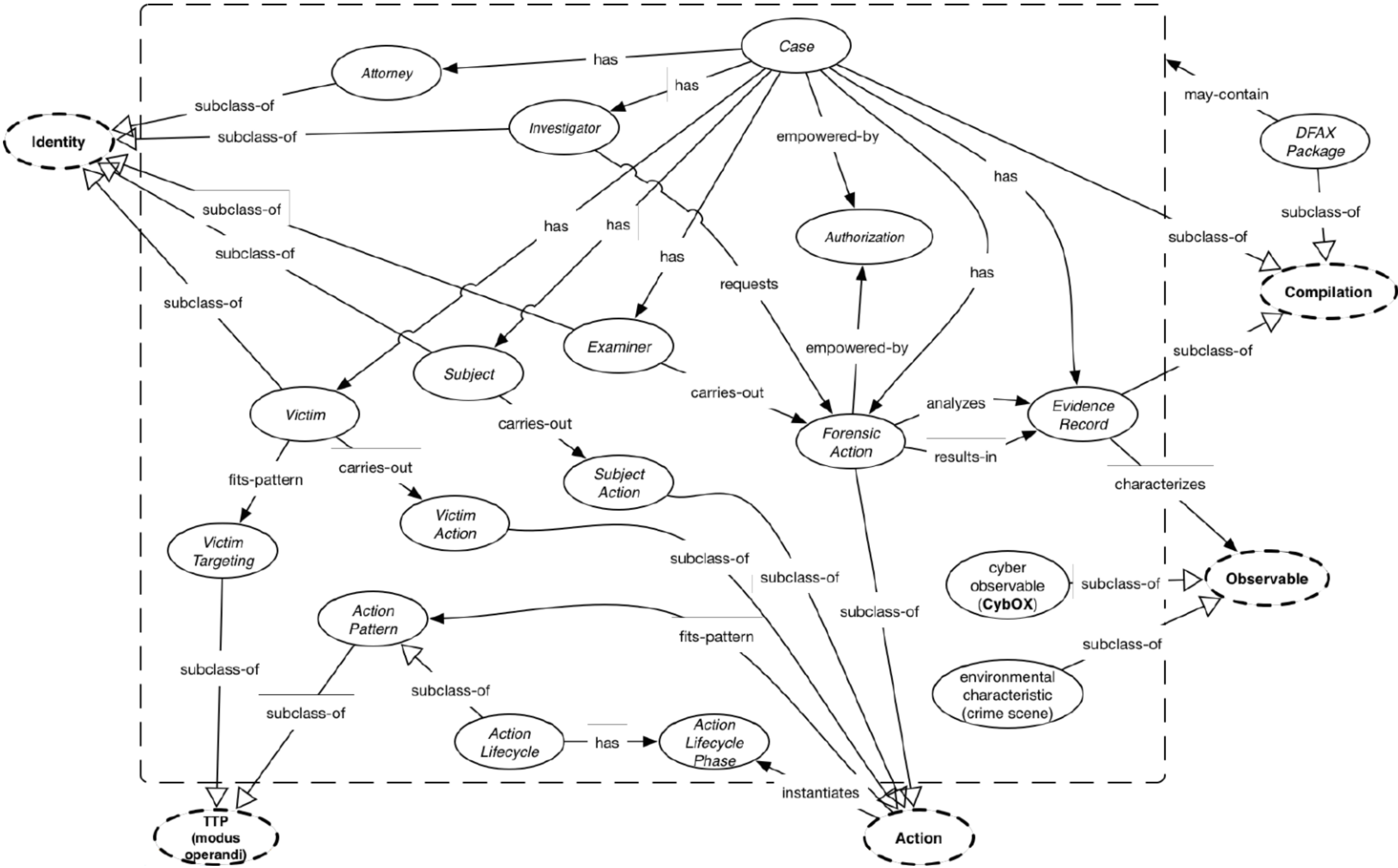
  + relationships

- DFAX (Digital Forensic Analysis eXpression)
  - Based on CybOX: observable part

  + Unified Cyber Ontology (UCO)
  - Extensible using XML schemas

- ORD2i: specialised ontology for Digital Forensic Cases
  - accurately represents a digital incident
  - and the associated digital investigation

Representation Model: DFAX



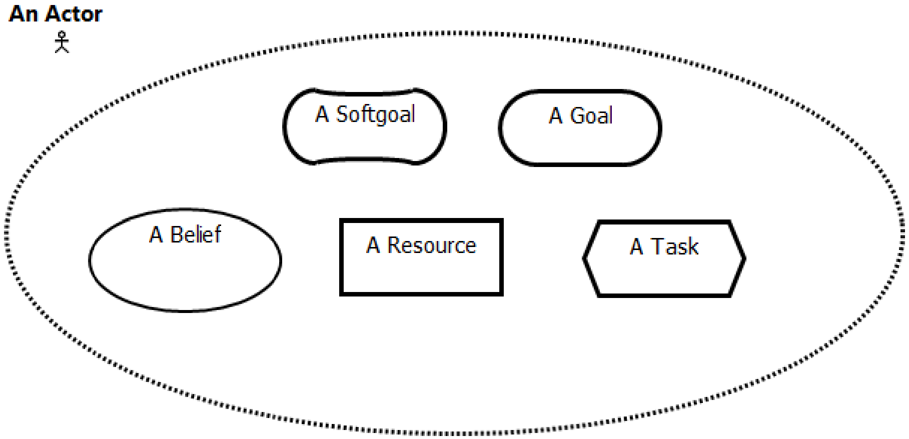
Goal-Oriented Requirements Engineering (GORE) Approach

- Why ?
  - Make goals explicit from high level goals down to operational systems
  - Assess how they interact, how current situation fulfils them

- How ?
  - Different GORE flavour available: KAOS, i*, GRL,…
  - No specific requirement on the meta-model
  - But need for open source tool and open exchange format

  ➔ GRL + jUCMNav selected
  (also based on simultaneous experience in another project)
  - See discussion about feedback on experience

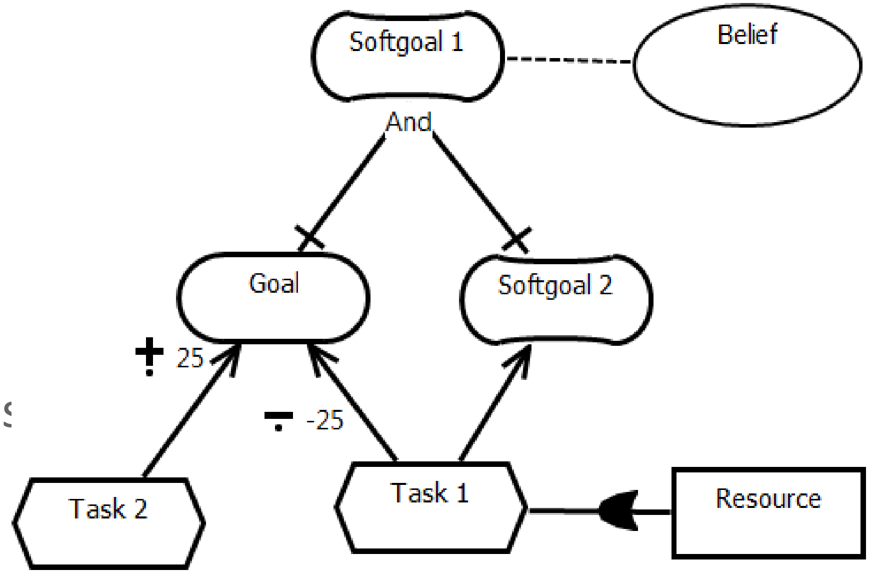
Goal-Oriented Requirements Language (GRL) – Key Concepts



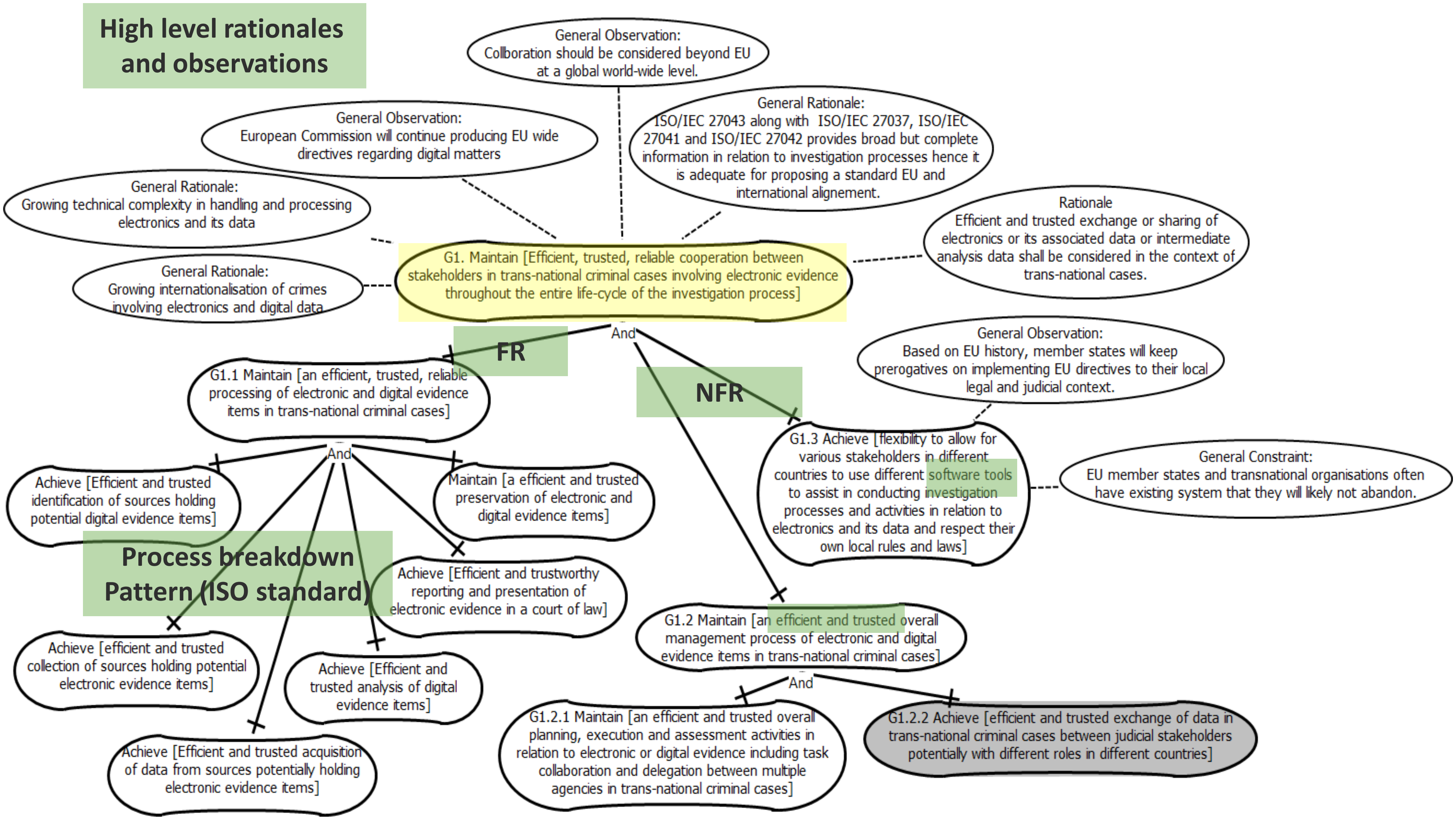
- **Goal**: a property to achieve when performing a given activity and accurately measurable (KPI)
- **Soft-Goal**: goal whose satisfaction is difficult to evaluate quantitatively E.g. non-functional properties like security or adaptability
- **Belief**: expresses a belief from stakeholders related to the goals to achieve when performing the given activity.
- **Task**: represents a concrete task to perform in order to achieve identified goals
- **Resource**: represents a resource needed by a task or needed to achieve a given goal.
- **Actor**: an actual type of stakeholders or more often a role held by certain stakeholders responsible for the elements within its perimeter

Goal-Oriented Requirements Language (GRL) – Key Relationships

- **Opinion**: --------
  association of a Belief element
  to another type of element
- **Decomposition**: ——┼
  expresses how a given goal, soft-goal,
  resource or task can be decomposed
  into a more concrete set of such concepts
  3 types: AND, OR, XOR
- **Contribution**: ⟶
  describes how Soft-goals, Tasks, or Links
  contribute to others (+ or -)
- **Dependency**:
  expressed a dependency from a depender to a dependee
  (actually between actor and through other elements)



Top-Level Goals



High level rationales and observations

General Observation: Collboration should be considered beyond EU at a global world-wide level.

General Observation: European Commission will continue producing EU wide directives regarding digital matters

General Rationale: ISO/IEC 27043 along with ISO/IEC 27037, ISO/IEC 27041 and ISO/IEC 27042 provides broad but complete information in relation to investigation processes hence it is adequate for proposing a standard EU and international alignement.

General Rationale: Growing technical complexity in handling and processing electronics and its data

Rationale Efficient and trusted exchange or sharing of electronics or its associated data or intermediate analysis data shall be considered in the context of trans-national cases.

General Rationale: Growing internationalisation of crimes involving electronics and digital data

G1. Maintain [Efficient, trusted, reliable cooperation between stakeholders in trans-national criminal cases involving electronic evidence throughout the entire life-cycle of the investigation process]

And

FR

NFR

General Observation: Based on EU history, member states will keep prerogatives on implementing EU directives to their local legal and judicial context.

G1.1 Maintain [an efficient, trusted, reliable processing of electronic and digital evidence items in trans-national criminal cases]

And

G1.3 Achieve [flexibility to allow for various stakeholders in different countries to use different software tools to assist in conducting investigation processes and activities in relation to electronics and its data and respect their own local rules and laws]

General Constraint: EU member states and transnational organisations often have existing system that they will likely not abandon.

Achieve [Efficient and trusted identification of sources holding potential digital evidence items]

Maintain [a efficient and trusted preservation of electronic and digital evidence items]

Process breakdown Pattern (ISO standard)

Achieve [Efficient and trustworthy reporting and presentation of electronic evidence in a court of law]

G1.2 Maintain [an efficient and trusted overall management process of electronic and digital evidence items in trans-national criminal cases]

Achieve [efficient and trusted collection of sources holding potential electronic evidence items]

Achieve [Efficient and trusted analysis of digital evidence items]

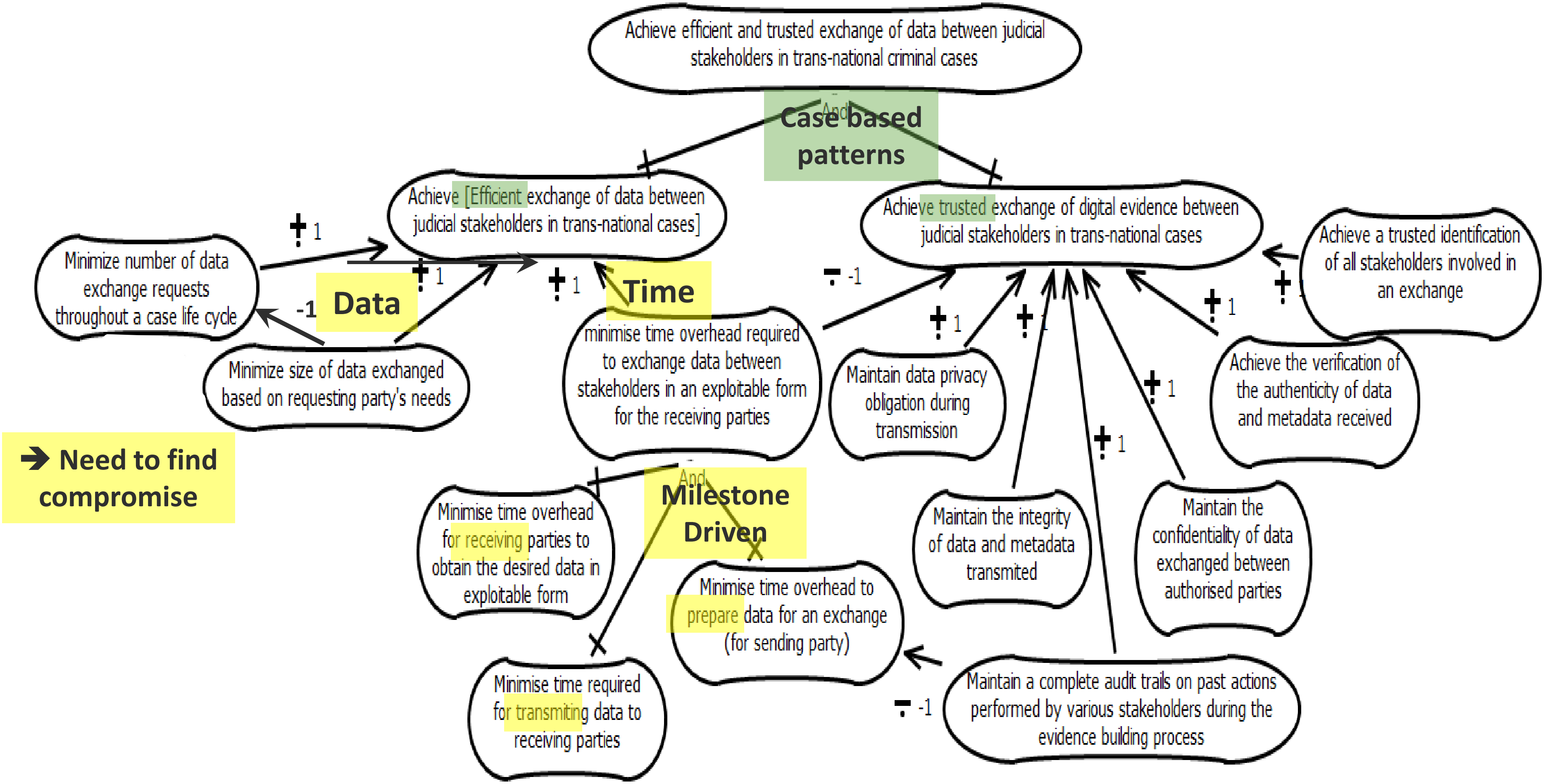
And

G1.2.1 Maintain [an efficient and trusted overall planning, execution and assessment activities in relation to electronic or digital evidence including task collaboration and delegation between multiple agencies in trans-national criminal cases]

G1.2.2 Achieve [efficient and trusted exchange of data in trans-national criminal cases between judicial stakeholders potentially with different roles in different countries]

Achieve [Efficient and trusted acquisition of data from sources potentially holding electronic evidence items]

Efficient and Trusted Exchange of Digital Evidence



Achieve efficient and trusted exchange of data between judicial stakeholders in trans-national criminal cases

Case based patterns

Achieve [Efficient exchange of data between judicial stakeholders in trans-national cases]

Achieve trusted exchange of digital evidence between judicial stakeholders in trans-national cases

Minimize number of data exchange requests throughout a case life cycle

Minimize size of data exchanged based on requesting party's needs

Data

Time

minimise time overhead required to exchange data between stakeholders in an exploitable form for the receiving parties

Milestone Driven

Minimise time overhead for receiving parties to obtain the desired data in exploitable form

Minimise time required for transmiting data to receiving parties

Minimise time overhead to prepare data for an exchange (for sending party)

Maintain data privacy obligation during transmission

Maintain the integrity of data and metadata transmited

Maintain a complete audit trails on past actions performed by various stakeholders during the evidence building process

Maintain the confidentiality of data exchanged between authorised parties

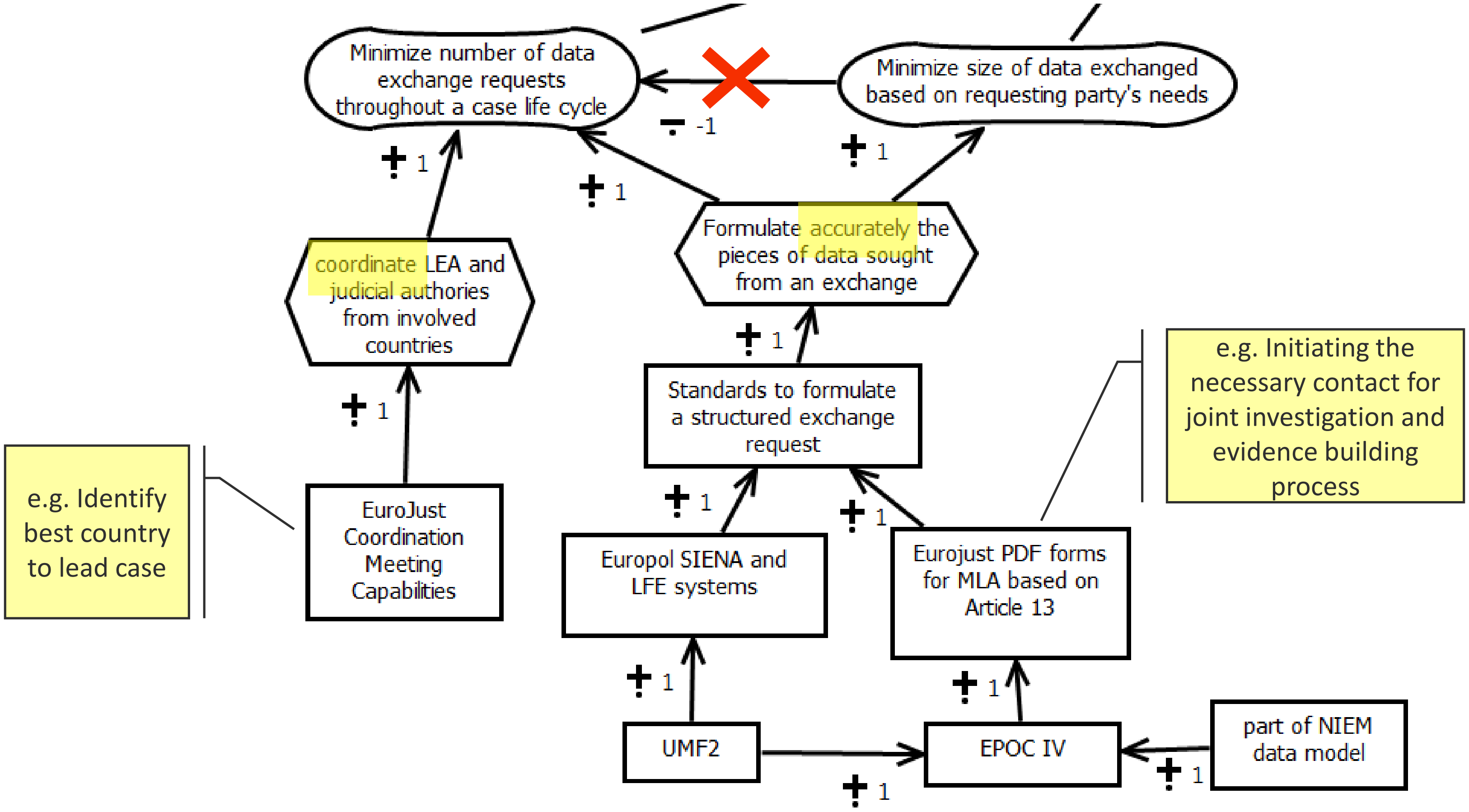
Achieve the verification of the authenticity of data and metadata received

Achieve a trusted identification of all stakeholders involved in an exchange

➔ Need to find compromise

Operationalising Efficiency – Data dimension

- Removal of potential conflicts
- Note: more concrete goals discovered in formulated explanations



Minimize number of data exchange requests throughout a case life cycle

Minimize size of data exchanged based on requesting party's needs

coordinate LEA and judicial authories from involved countries

Formulate accurately the pieces of data sought from an exchange

Standards to formulate a structured exchange request

EuroJust Coordination Meeting Capabilities

Europol SIENA and LFE systems

Eurojust PDF forms for MLA based on Article 13

UMF2

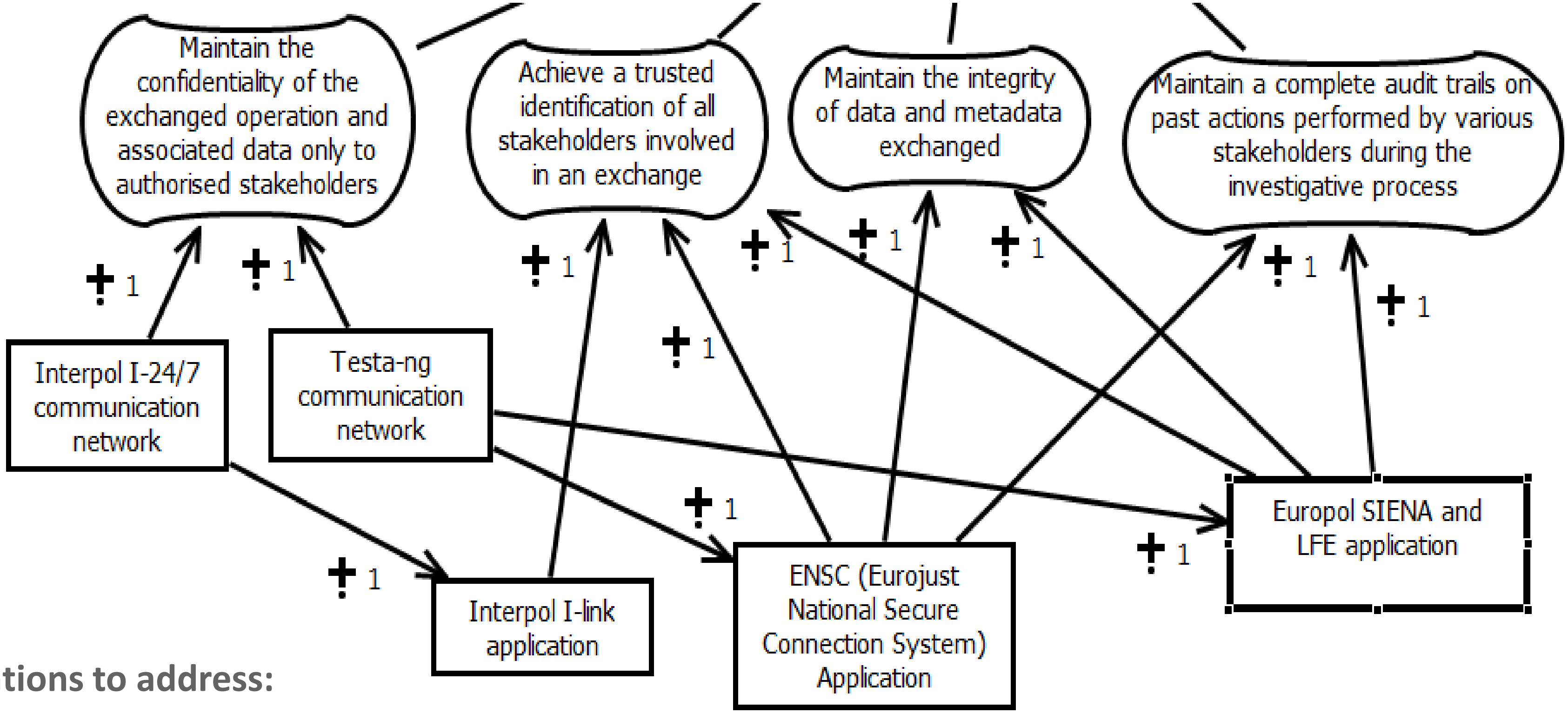
EPOC IV

part of NIEM data model

e.g. Identify best country to lead case

e.g. Initiating the necessary contact for joint investigation and evidence building process

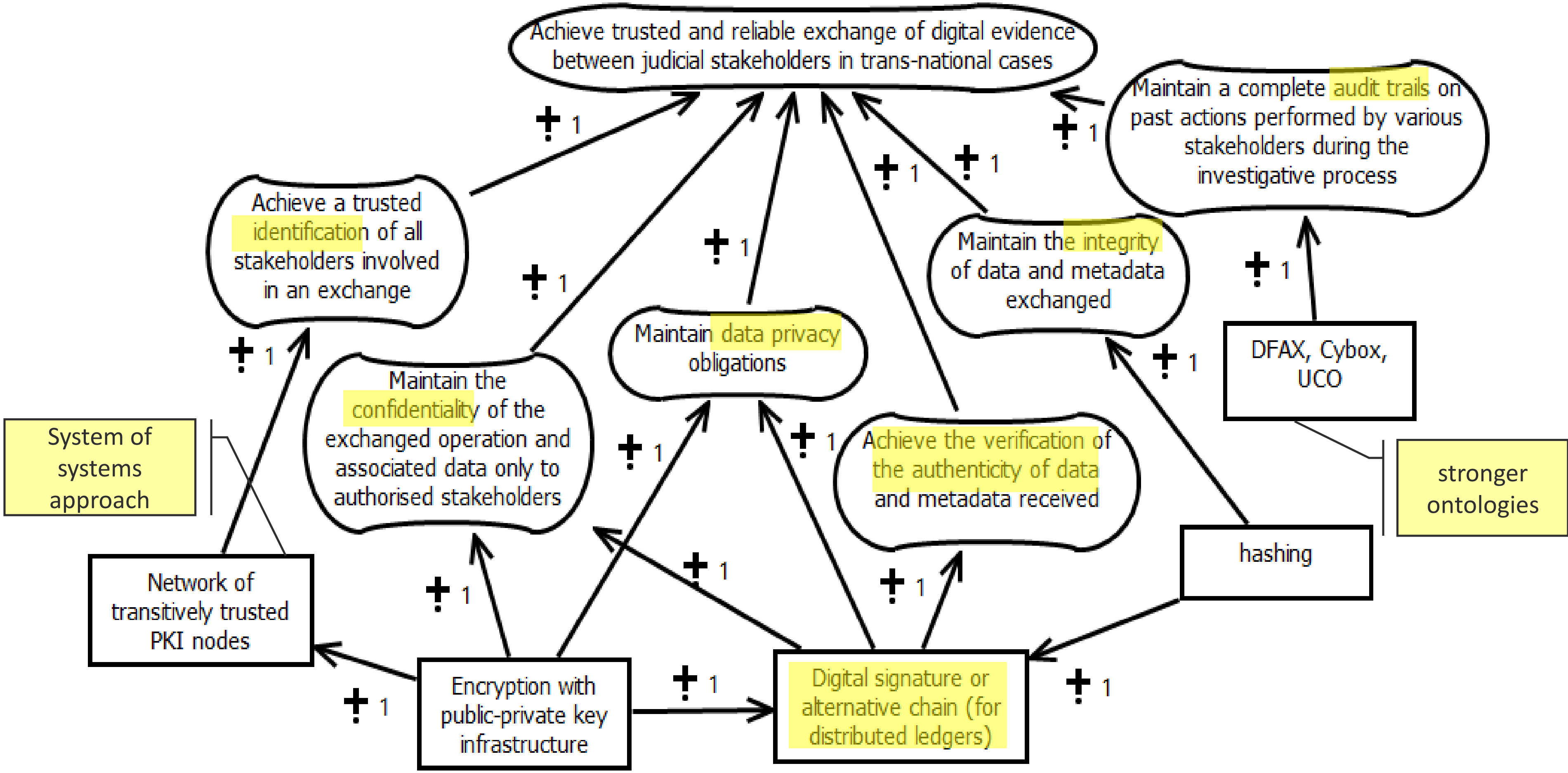
Assessing Level of Trust Satisfaction in Current System


Maintain the confidentiality of the exchanged operation and associated data only to authorised stakeholders
Achieve a trusted identification of all stakeholders involved in an exchange
Maintain the integrity of data and metadata exchanged
Maintain a complete audit trails on past actions performed by various stakeholders during the investigative process
Interpol I-24/7 communication network
Testa-ng communication network
Europol SIENA and LFE application
ENSC (Eurojust National Secure Connection System) Application
Interpol I-link application
+ 1

Limitations to address:

- **Stakeholder-specific systems** (i-Link used by LEA, Eurojust => judicial authorities)
  ➔ less easy to communicate across stakeholders
  Exception = Siena achieving some sharing: Europol agents + Europol contact point in EU member states + Eurojust authorities ➔ to be broadened
- **Lack of data structuration**: manual filtering ➔ need to rely on semantic structure
- **Achieving and verifying provenance integrity across systems (heterogeneous stakeholders)**

Improving Trust in Future System



Achieve trusted and reliable exchange of digital evidence between judicial stakeholders in trans-national cases

Achieve a trusted identification of all stakeholders involved in an exchange

Maintain the confidentiality of the exchanged operation and associated data only to authorised stakeholders

Maintain data privacy obligations

Achieve the verification of the authenticity of data and metadata received

Maintain the integrity of data and metadata exchanged

Maintain a complete audit trails on past actions performed by various stakeholders during the investigative process

DFAX, Cybox, UCO

hashing

Network of transitively trusted PKI nodes

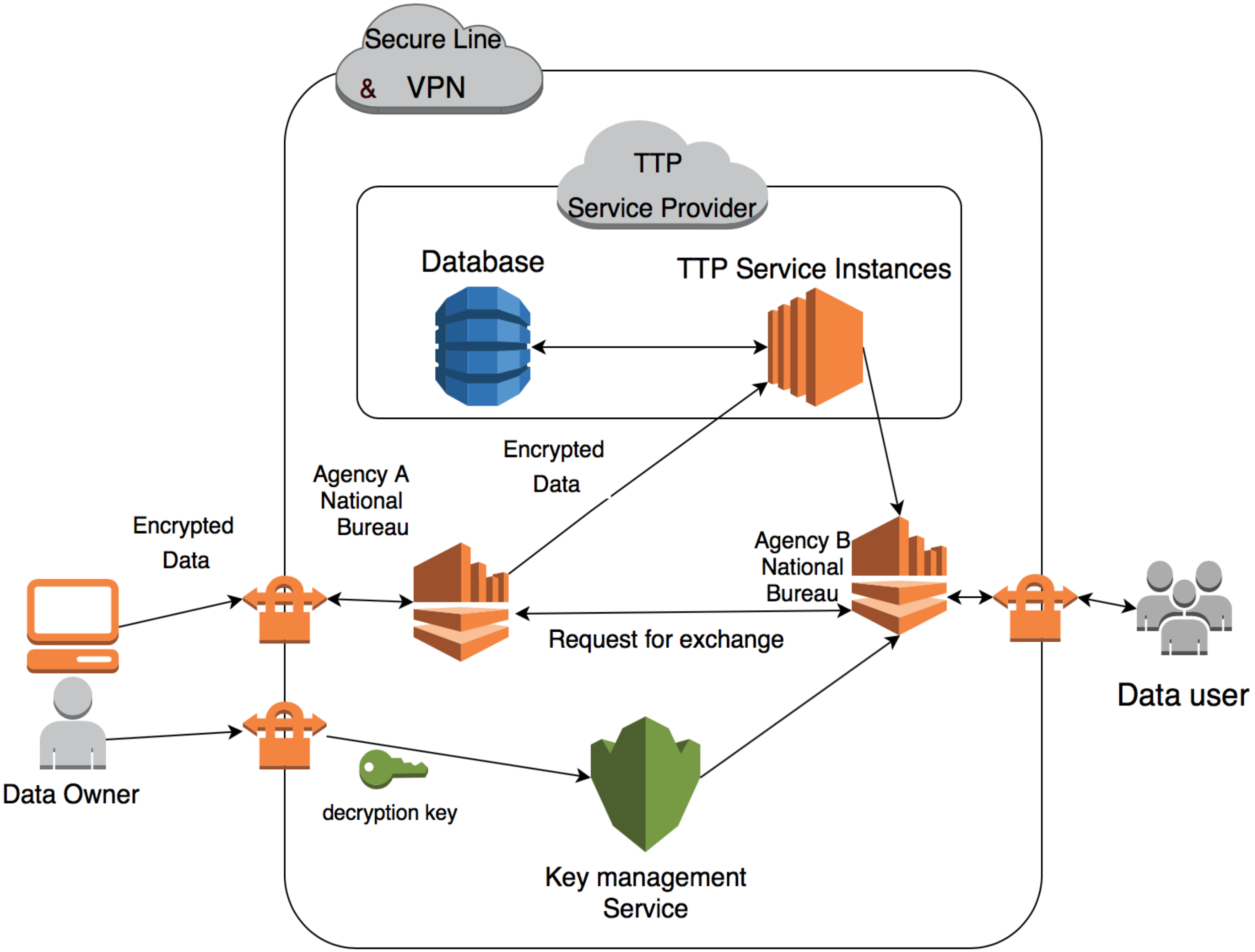
Encryption with public-private key infrastructure

Digital signature or alternative chain (for distributed ledgers)

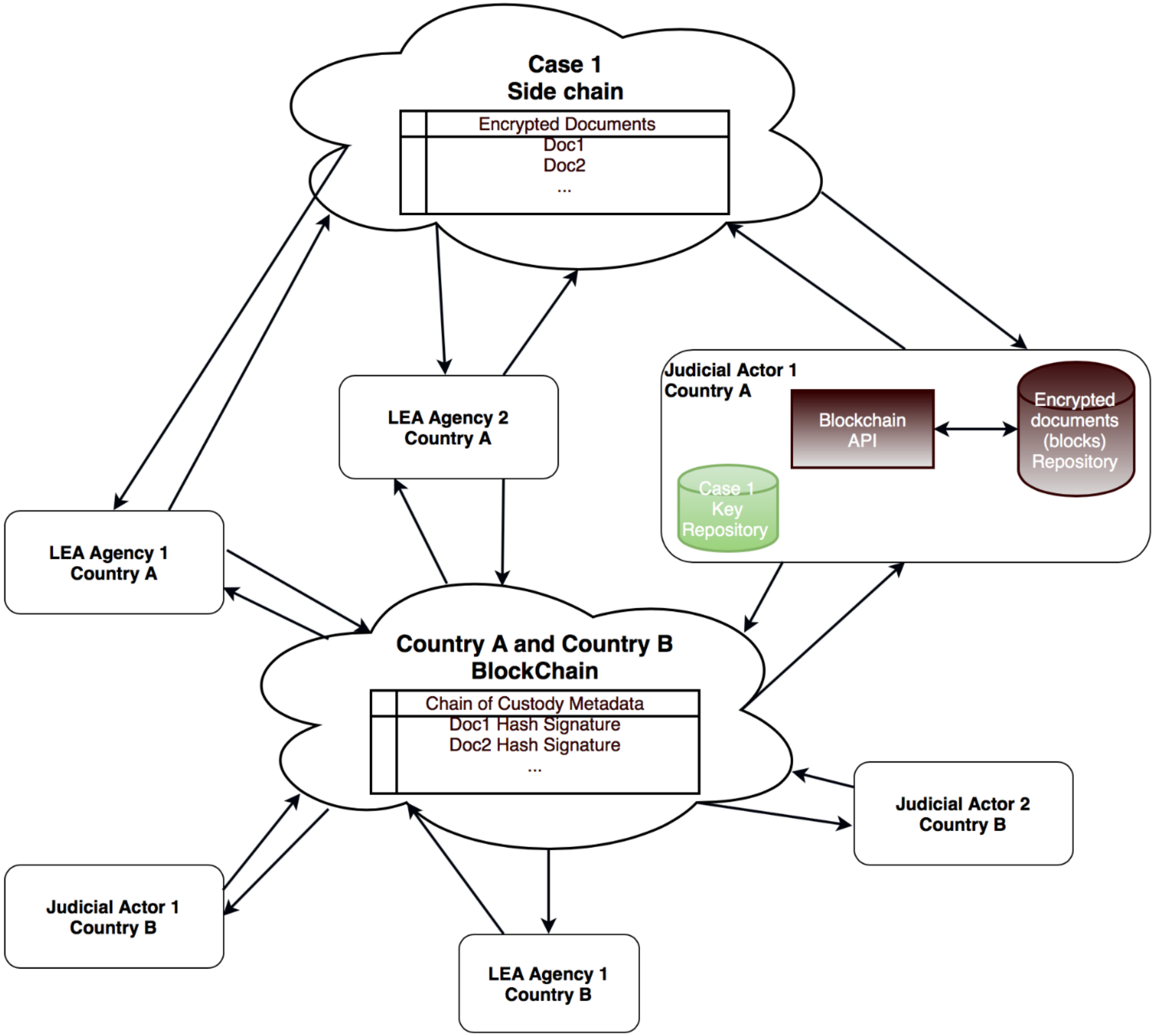
System of systems approach

stronger ontologies

Suggested Systems Integration - Centralised Alternative Trusted Third Party based Exchange



Suggested approach: Distributed Repository Alternative "Alternativechain/Blockchain"



- As used by bitcoin but for another purpose than monetary transaction (such as developed by MultiChain or Etherium)
- Provides a distributed trusted data storing approach
- Side chains for each Case
- Data content and sharing in the side chain is according to the terms that participating parties agree to.

Discussion

- Systematic structuration
  - relying on patterns: milestone, case-based
  - mostly "AND" (only some lower level design alternatives considered)
- (potential) conflict detection/resolution technique used
  - based on reasoning on contributions links at different levels
- Assessment of level of satisfaction of current system
  - Using contribution links, checking stakeholder "clustering"
  - "Gap" analysis
- Contribution weight not used (only +1, -1)
  - Too early/high level of reasoning
  - Could be further refined when more precise KPI are defined
- Some language limitation (non-blocking)
  - Belief may only be linked to other element using the Opinion link, beliefs cannot be linked with each other
- Some tool limitations
  - jUCMNav does not exactly match the GRL as defined in the standard
    e.g. relationship creation are more permissive
    using them can make sense on the problem but can generate semantic issues

Conclusions & Perspectives

- Detailed goal-oriented requirements analysis of the exchange of electronic evidence across EU Member states
- Systematic refinement process focusing on the importance of achieving both efficiency and trust in the exchange of data
- Production of fine-grained requirements
  - for assessing current system (mainly exchange part)
  - for evolving into better system (= project recommendations)

➔ GORE approach very valuable

- On-going work:
  - Proposal of reference architecture, including semantic structuring
  - Proof of concept implementation and demonstration

Questions ?