Technical and Legal Perspectives

in Data Sharing Agreements Definition

Speaker: Gabriele Lenzini
University of Luxembourg

Agenda

* Data Sharing, what and why?
* DSA and DSA Lifecycle
* Proposal for a three step DSA definition phase
* The DSA authoring tool
* What's next?

Data sharing: a lot of variables!

* Which kind of data shall I share? Data Classification
* With whom? Actors
* For which use? Purpose
* Which kind of operations? Policies
* Under which conditions? Context
* …

Business Data Sharing Rules

* Only specific corporate users can access business highly confidential data [subject and object constraints]

* Highly confidential data access and usage is allowed only from corporate buildings [geographical constraint]

Health Services Data Sharing Rules

* All accesses and attempts to access medical data must be recorded [logging]

* Medical data cannot be accessed from, nor transferred to, countries outside EEA plus the countries approved by European commission [International transfer of data]

* The patient can revoke the access to his/her medical data to specific doctors (or people) [End user preference]

From paper contracts to Data Sharing Agreements

* Traditionally, legal bindings to regulate how data is shared
  * complex, non standardised
  * natural languages -> machine-processable languages

* DSA intends to be
  - A human-readable contract
  - A machine-processable electronic document, whose data sharing rules can automatically analised and transformed into enforceable policies

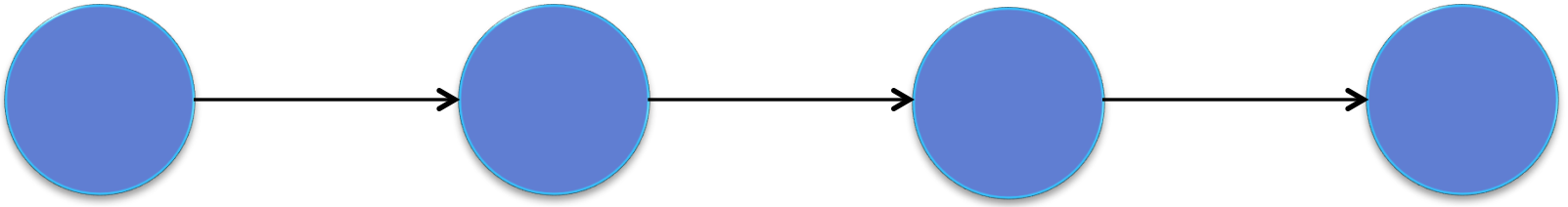
Fields in a DSA

* Interdisciplinary collaboration plays a central role:
  * Legals
  * Service providers, companies, PAs (Education, health, e-government..)
  * End users

title
parties
roles & responsibilities
validity
vocabulary
data classification
purpose
data sharing rules
economics, governing law

DSA lifecycle

* Stages of a DSA lifecycle



Template definition

Authoring

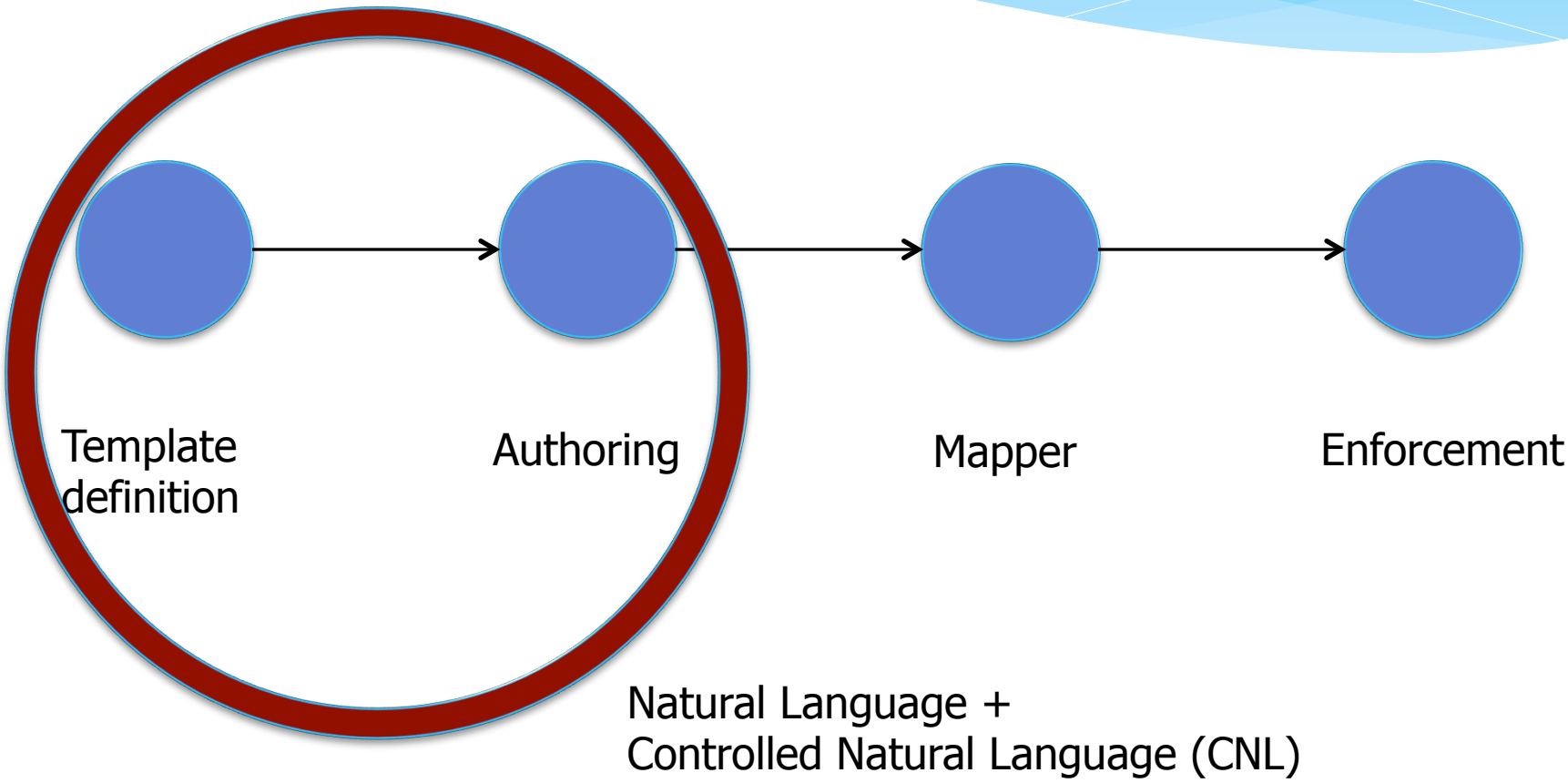
Mapper

Enforcement

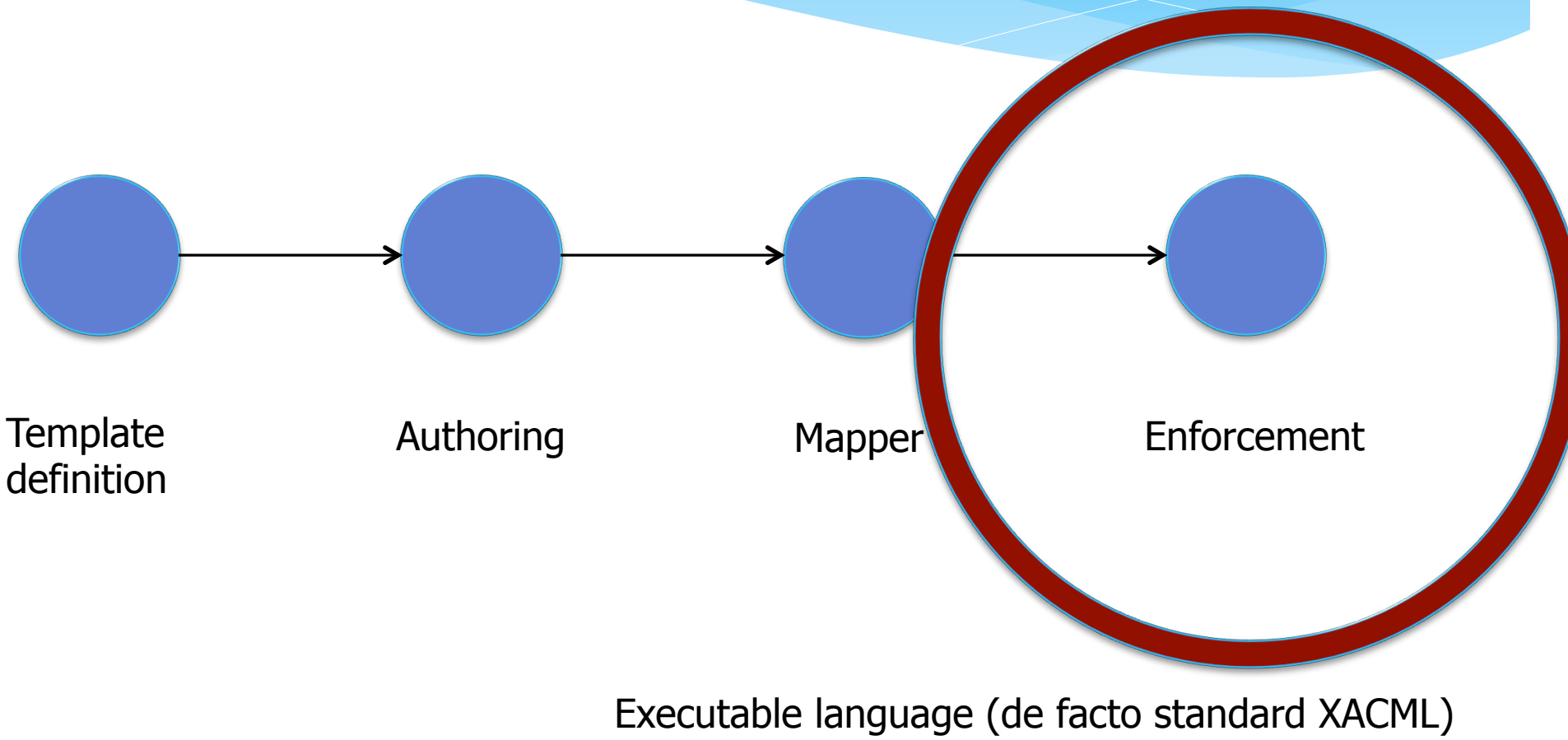
Three step DSA definition process

* Template
  * Roles of parties (Controller, Processor, Subject)
  * High level data classification (personal vs non personal)
  * Purpose of data sharing
  * Relevant legal rules
* Organization level
  * Parties and data instantiated
  * Validity
  * Organization-specific data sharing rules
* End user
  * End user data sharing preferences
* Three actors participate:
  * Law Expert: defines the DSA template (1st step)
  * Policy Expert: adds business policies instancing a DSA template (2nd step)
  * End User: completes the DSA with user preferences (3rd step - optional)

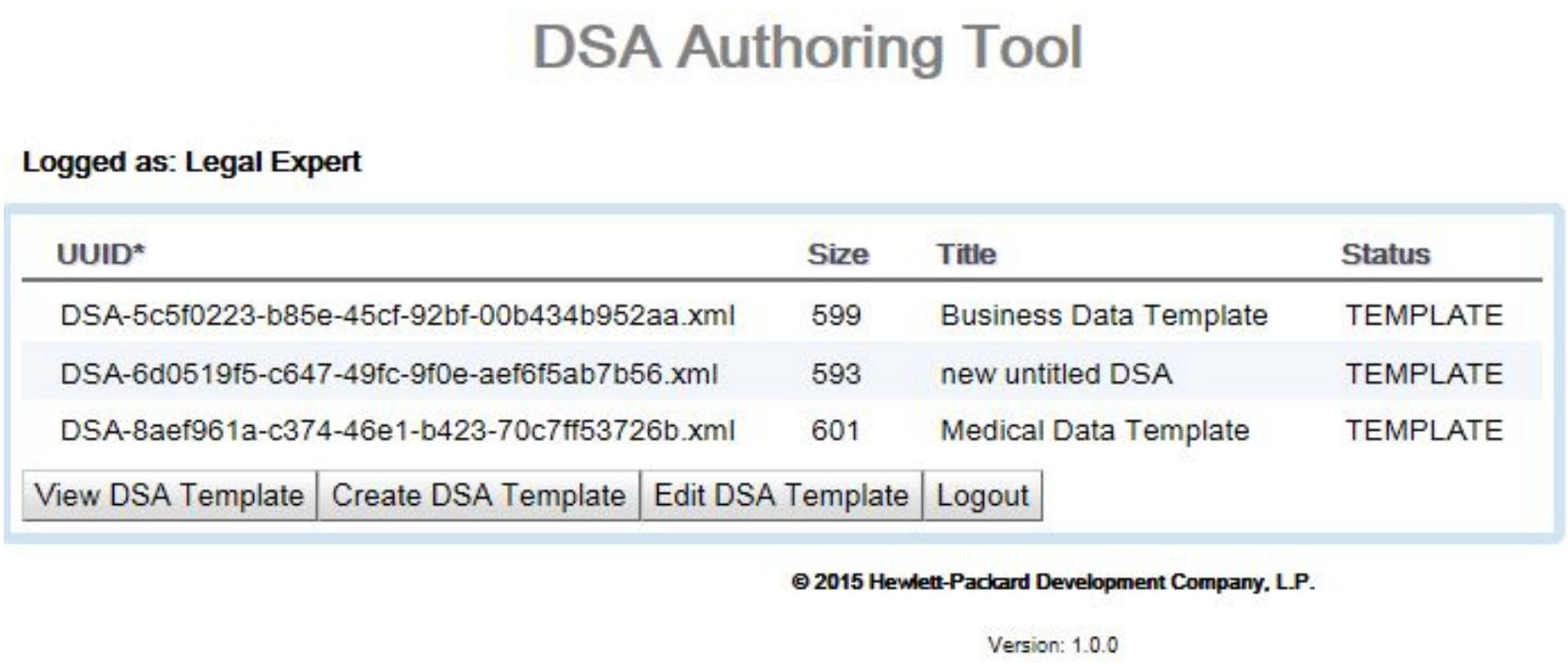
DSA languages



DSA languages



DSA authoring tool web interface



DSA Authoring Tool

Logged as: Legal Expert

Save DSA Template | Back

UUID*: DSA-6d0519f5-c647-49fc-9f0e-aef6f5ab7b56.xml **Data Classification**

⊞ Non Personal Data

⊞ Personal Data

Vocabulary URI*: http://127.0.0.1:8080/vocabularies/healthcare_vocabulary.owl#

Title* new untitled DSA

Purpose

- Marketing
- Healtcare Services
- Research

Parties*	**Role***	**Responsibilities**
Party 1	Data Controller	
Party 2	Data Processor	

▶ Change

Validity*

start date: 2015 May 11 ▶ Change

end date: 2016 May 10 ▶ Change

Kind of data

- Non personal data
  - Business data
    - Highly Confidential (e.g., strategic business plans, etc.)
    - Confidential (e.g., price lists, etc.)
    - Public (e.g., a list of products)
    - Administrative data (e.g., customers invoices, etc.)
- Personal data
  - Common personal data
    - Identification details (e.g., name and surname)
    - Contact details (e.g., address, phone number)
    - …..
  - Special categories
    - Sensitive data (e.g., medical data)
    - Judicial data (e.g., data relating to offences or criminal convictions)

Purpose of use

1. Administrative and Accounting (e.g., for booking, for payment)
2. Healthcare services (e.g., for diagnoses)
3. Scientific Research
4. Statistical (e.g., public costs control, epidemiological)
5. Marketing (e.g., for commercial proposal of services/needs)
6. Fulfil law obligations (e.g., to access or share data in case of legitimate requests of public authorities)

Authorizations

Parties Policies

Authorisations

IF a Subject hasRole Doctor AND a Data hasType Radiological THEN that Subject CAN Append that Data

IF a Subject hasRole DelegateOfPatient AND a Data hasCategory Medical THEN that Subject CAN Read that Data

IF a Subject hasRole Patient AND a Data hasCategory Medical THEN that Subject CAN Download that Data

Add

Parties Policies

Authorisations

IF a Subject hasRole Doctor AND a Data hasType Radiological THEN that Subject CAN Append that Data

IF a Subject hasRole DelegateOfPatient AND a Data hasCategory Medical THEN that Subject CAN Read that Data

IF a Subject hasRole

Add

Select one of the following choices

- available choices ...
  - REFERENCE
  - a Role
    - DelegateOfPatient
    - Doctor
    - HealthProfessional
    - LegalExpert

Conclusions

* From legal paper contracts to electronic Data Sharing Agreements
* The authoring tool allows from a three step definition phase, with involvement of law experts, policy experts, and end users
* Open issues:
  * Conflicts detection and resolution
  * Usability issues (end users)
  * What about dynamic changes in the DSA?
    * Expiration
    * Revocation

Thank you!

* Claudio Caimi, Carmela Gambardella, Mirko Manea
  Hewlett Packard Italiana, Milan Italy
* Marinella Petrocchi, CNR, Pisa, Italy
* Debora Stella, Bird & Bird Milan, Italy

* Questions? marinella.petrocchi@iit.cnr.it