# Modelling and Securing European Justice Workflows

Stefano Crosta[1], Jean-Christophe Pazzaglia[1], Hendrik Schöttle[2]

[1]Institut Eurecom

2229 Route des Crêtes
BP 193 - 06904 Sophia Antipolis - France
Tel: (+33) 493 00 26 78 - Fax: (+33) 493 00 26 27
{ Stefano.Crosta | Jean-Christophe.Pazzaglia}@eurecom.fr

[2]Institute of Law and Informatics

Saarland University
66123 Saarbrücken, Germany
Tel +49 681 302-3105 - Fax +49 681 302-4469
h.schoettle@mx.uni-saarland.de

## Abstract

Law and Justice are domains which can extremely benefit from proper representation of judicial workflows capable of capturing the specificities of their processes. Workflows would provide the bases for automated systems capable of verified process handling. A suitable model would support both a clear understanding of the procedure, and the correct design of an automated workflow execution engine. In this paper we outline justice peculiarities and present enhanced workflows capable of describing them. We propose to enrich those workflows with security annotations describing critical aspects of the processes; and describe the design mechanisms to support such security requirements into a real application. The use of xml based Attribute Certificates is proposed as a solution to provide secure distributed management of user capabilities and certified data, thus completing the solution of enhanced workflows for judicial processing empowered with security requirements.

# Introduction

The main objective of eJustice project[1] is to investigate the workflow paradigm to model the judicial domain and specifically procedures, and to identify the specific need of the domain in term of security and rights management by analyzing the organization and structures of judicial bodies across Europe.

In the framework of the project we also aim at enriching workflow models with security annotations in order to provide and enforce security in an automated process.

---

[1] This work has been performed in the context of the EU FP6 project eJustice IST-2002-001567[1], however this paper represents the view of the authors only.

The security analysis over a workflow is consolidated into three design rules that guarantee security enforcement over the automated process: *within* workflow through atomic operations; *around* workflow through authenticated rights based access; *beyond* workflow through non-repudiable and secure logs.

Workflow analysis is based on the paradigms of Business Process Modelling (BPM) which we extend to provide security annotations and functionalities. To achieve these objectives we combine an original distributed attribute certificates framework with extended signature formats.

This document is organized as follow: after showing the specificities of the eJustice domain in term of modelling and Right managements, we will show how workflow model security can be enhanced following a number of principles, procedures and techniques and how our flexible certificate architecture can embed the mandatory information to support advanced authorization scheme.

# 1. Insights in Justice Modelling

Our efforts focused on representing judicial processes and model judicial workflows are not intended to representing laws, but the whole flow of activities based on prescriptions or internal directives. This possibility might be restricted by the fact that the concrete sequence of a judicial process often depends on interpretations of laws and ad hoc decisions (e.g. by prescriptions or internal instructions). The latter may be taken for granted regarding (more or less strictly formalised) application procedures, e.g. the payment order procedure. It has also to be noted that, and despites the increasing ratification of European directives, each European country has its own legal system, which an expert from another country might not fully appraise without prior thoughtfully study of this legal system.

eJustice demonstrates the feasibility of workflow modelling in the judicial domain by representing processes of the following scenarios: the Judicial Assistance in Criminal Matters, the European Arrest Warrant, the Rechtsinformationssystem (RIS) and the European Payment Order Procedure and by analysing the organisations of different judicial authorities, member of our users group, around Europe (France, Austria, Belgium and Germany)[5][10].

The explicit representation of judicial processes as a workflow model can bring huge benefits to involved actors and citizens alike. This holds in particular for models of trans-European workflows which can be used to efficiently inform citizens about legal proceedings in other European countries. This constitutes an issue of growing importance as Europe becomes increasingly integrated[4].

# 2. Case-centric hierarchical framework

Judicial procedures deal with sensitive information. The right to access information (e.g. court files or evidences…) and to take initiatives (e.g. investigation…) derived from a complex structure rooted in our democratic system and legislative infrastructure that is eJustice objective to comply with.

As a first result we highlighted that European and national laws do not contain sufficient security requirements; only role based definitions are given, and partially: therefore the feasibility of providing security lies in the identification of different threats and user roles that are not defined by law and may be organization specific.

Roles - representing a group of users - can be defined and represented at the level of business function within the modelled business process. However, the cornerstone of the judicial

process is the 'judicial case'. The business process represents the case management including the flow of business functions under the responsibility of different roles and users that may be part of different bodies or authorities. Apart from supervision and auditing, representation of roles within the judicial context should therefore be strongly linked with the judicial case they are working on. RBAC supporting the notion of dynamic team [20] appears to address nicely these issues.

A judiciary system is composed of several branches and bodies or authorities. The Investigation offices, the Prosecutors offices and the Courts are three independent branches. A branch (e.g. the Courts) may have several bodies or Authorities depending on hierarchy (regional court, district court, appeal court, Supreme Court) and from the matter (civilian, criminal, commerce, military, labour) Specific authorities may cover several branches (e.g. a Supreme Judicial Council, responsible for general administration and human resources).

Each authority may have one or more services composed from one or more people; the notion of compartment is to be introduced: a compartment is specific for the right management aspect in the judicial world: a compartment is «the community of users (human & technical) belonging to one or more services of a judicial authority in charge of the case». Each authority in charge of a case may have one or more compartments. The administration of access rights (users, roles) should be done at compartment level.

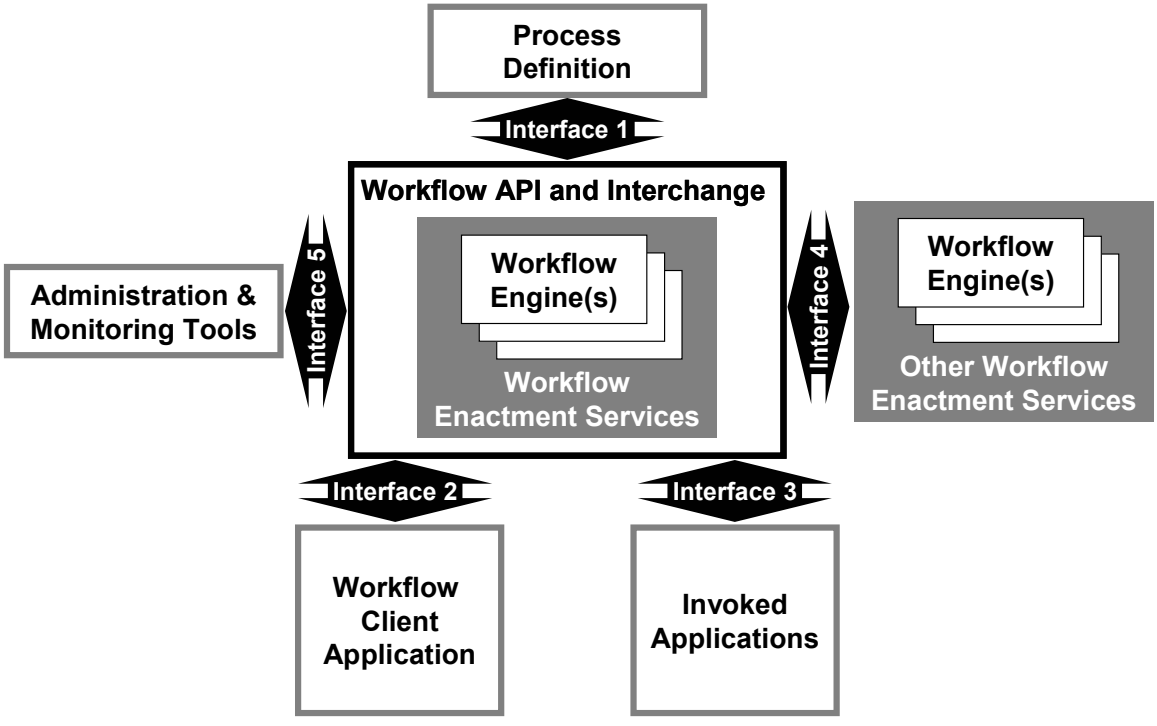


**Figure 1 – Workflow Reference Model [22]**

# 3. Securing the Workflow End-to-end

Workflow modelling techniques have been adopted to describe judicial processes within eJustice. A workflow management system enable to take as input a formal description of business processes and to maintain the state of processes executions, thereby delegating activities amongst people and applications. A specific process instance would be then spawned

and managed by a workflow engine for each judicial procedure. Figure 1 presents an overview of the different software components involved during the lifecycle of a workflow.

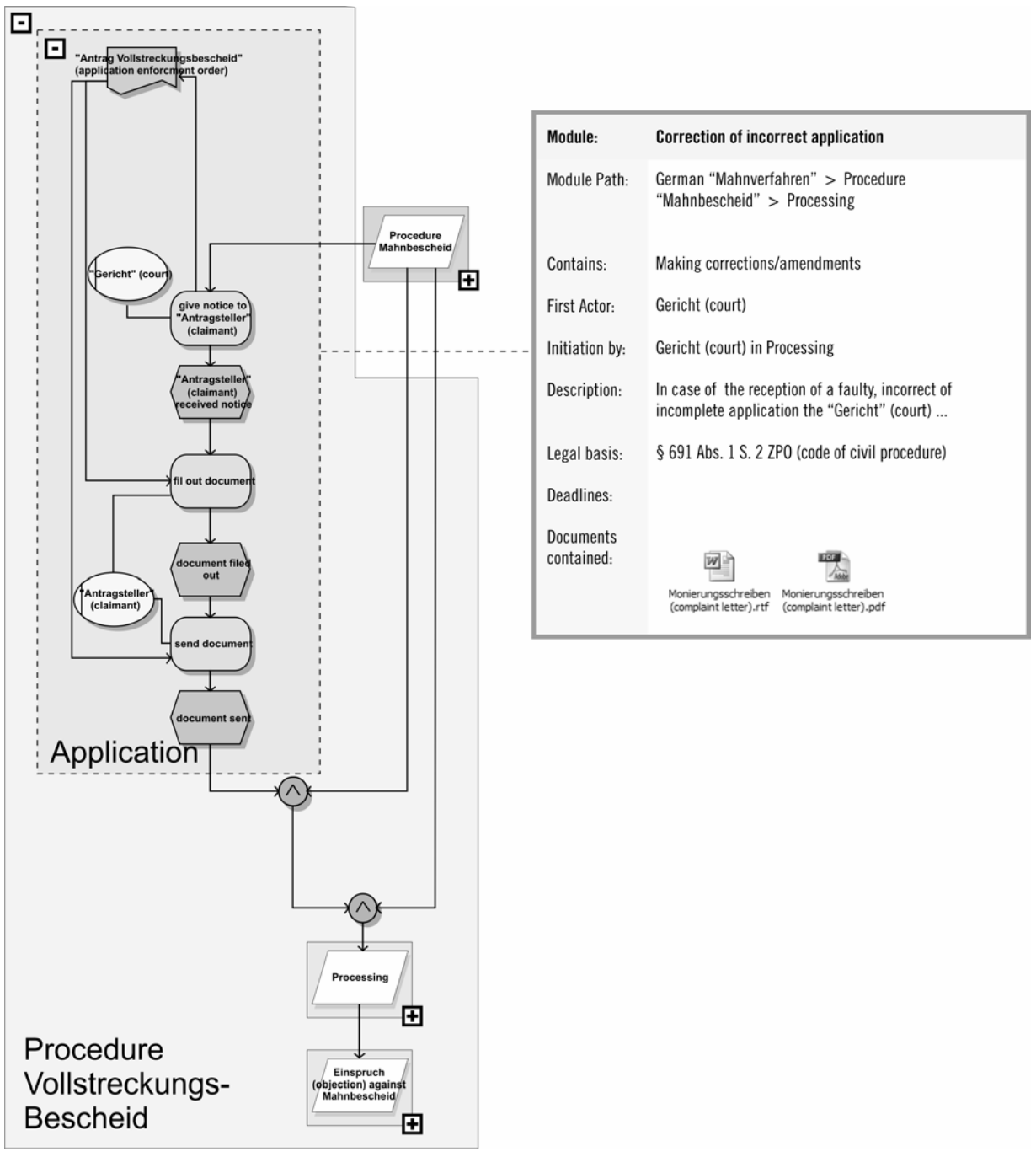


**Figure 2 – Workflow model for order for payment procedure**

Figure 2 shows an excerpt of a workflow model representing the German "Mahnbescheidsverfahren" (order for payment procedure). Speaking in judicial dimensions, it is a rather structured process. The absence of any vague terms or judgemental elements made it suitable for automation – a chance that meanwhile most of the German federal states made use of. Anyhow, this workflow was complex enough to test and enhance existing workflow

modelling techniques. To improve the visibility of this process, several issues had to be dealt with, such as a modularization, additional information displayed in an extra info-box. Modular/collapsing views allow focusing on particular elements of the workflow – isolating independent elements of the process being part of the modelling work. For every model we define the elements which characterise it, as shown in the figure for the example.

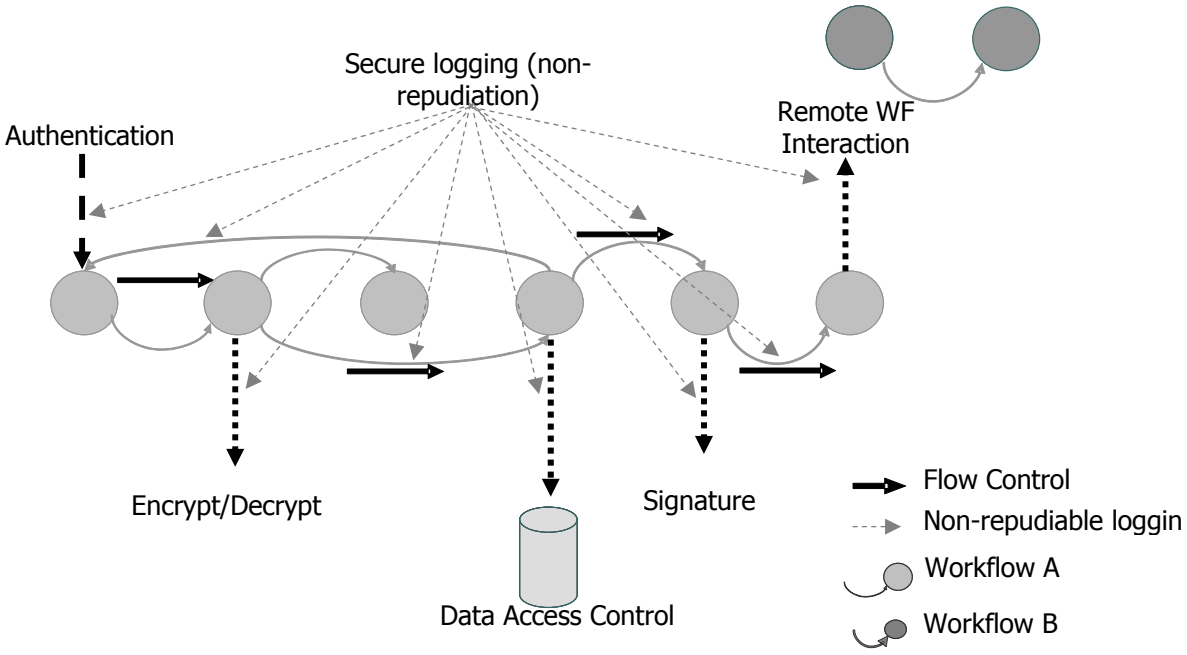


**Figure 3 – Security design principles within workflow**

This workflow model is the starting input to a Workflow Platform capable of capturing the judicial annotations. The following step is to translate verbal requirements into security annotations which are unambiguous. Once the model security requirements are clearly expressed, it can be implemented into a secure workflow which respects our security design rules to guarantee satisfaction of security principles.

The objectives of our right management platform (EJRMS) is to provide a common framework to enforce security constraints captured during the process definition within a centralized workflow engine but also to enable interactions with external applications (interface 2,3 in figure 1) and interoperability with remote workflows (interface 4). Complementary, the platform should be able to provide support for certain aspects of the monitoring and logging which may be challenging in terms of Data Integrity, Confidentiality or Non-repudiation (interface 5). In other words, EJRMS provides the support for the security principles, which are better described hereafter, while satisfying the common workflow reference model.

A large subset of the business process is captured using a set of activities combined with the relations between them known as control flow. Figure 3 illustrates our approach to provide and enforce security of the workflow execution.

We recall here the three principles that we defined to provide secure design: *'within'* workflow security, *'around'* workflow security, *'beyond'* workflow security. Let's examine them:

## 3.1. '*within*' workflow security

'*within'* workflow security covers aspects related to execution of each single task.

It provides access control and non-repudiation for task executions, and validation of task parameters and result.

While the execution of the task itself is out of the control of the workflow engine, task input/output parameters are. We consider the task execution as an **atomic operation**. Intrinsic security of such operation is outside the scope of the workflow engine – and thus, of this paper. Relations of this operation within the workflow must instead be controlled.

The *'within'* workflow security design principle consists in that: each activity must explicitly declare input and output w.r.t. the responsible entities, and clearly state acceptance rules for authenticating the users and the data.

When using a secured framework such as EJRMS, I/O of the atomic operation are monitored and logged. The actor allowed to perform an operation is requested to authenticate himself; upon validation, he receives in exchange the capability to access the task. The workflow log user authentication and task execution (see principle 3), providing non-repudiation for a given action $A_i$ with I/O set $IO_i$ at time $T_i$.

It is important to notice how a correct model of the judicial procedure is a mandatory step to permit inferring correct rules for tasks transitions and execution.

## 3.2. '*around*' workflow security

*'around'* workflow security protects workflow interactions with external entities by rights/roles-based user authentication through the use of a distributed, PKI based Attribute Certificate framework, in combination with principle 1.

To satisfy this design rule, explicit definition of inter-workflow relations and actors' interactions must be stated in terms of secure properties (credentials). This implies taking into account Trust Management aspects of workflow entities. The use of a PKI or a similar system makes the assumption that a-priori trust is defined; our proposed attribute certificate framework (see Section 4) allows for dynamic trust establishment within certain responsibility limits.

Using properties/capabilities/roles instead of personal identifiers also permits a more flexible management of workflow actors, limiting the risk of overpowering users to make up for the system limits.

## 3.3. '*beyond*' workflow security

*'beyond'* workflow security permits full traceability of the workflow activities w.r.t. the actors through non-repudiable, secure logs, exploiting principles 1. and 2.

They are complemented by ***inter-workflow security*** for distributed workflows.

This first part of 'beyond' design principle does not refer to any specific security annotation in the workflow, and must be peculiar of the enhanced workflow engine itself.

Storing logs of workflow activity raises an additional requirement: privacy and access control of such logs. Workflow model must specify super-users allowed to dig into this logs; this annotation also specifies the context (reasons) and limits of log analysis. Some privacy properties can be applied, for instance in a particular situation a procedure could be cancelled for procedural fault, without need to disclose the identity of the actor which produced such a fault, or without disclosing which data have been manipulated.

## 3.4. Applying 'wab' principles

Such principles are mapped to different categories of services (security annotations) which rely on EJRMS to:

- enforce Strong Authentication and Authorization scheme using a dedicated, possibly biometric[19], device;
- enable activities such as Signature, Encryption, Data Access Control and Remote Interaction which typically take place within activities[7];
- allow the construction of secure, privacy aware, audit trails as defined in[3].

Access control may depend on the context of the request: for example a lawyer should have the right to consult a document according that he is acting on behalf of the defence during a specific case. He may disclose it to his client[2] or to a legal expert if, and only if, this specific communication is protected by a non-disclosure agreement. On the other hand, he may not have the right to use/access this evidence on another trial or to disclose it to the media; prosecutors might or might not have the right to know which documents a defense lawyer has accessed, while judges rights might have different limitations. These are part of the requirements which the workflow model must state in order to permit automated validation of workflow flow.

Documents produced/stored within the system may also potentially be used as legal evidence or used during trials. Consequently, the system should insured the integrity and confidentiality of documents and be able to generate qualified signatures [9]. Other security annotations provide the means to specify which qualities a document must satisfy; principle 1 would guarantees that every step is correctly executed, principle 2 that the right entity is performing a task, and principle 3 guarantees non-repudiation of actions and verifiable correctness of the workflow flow at any moment.

In order to protect citizen rights in term of privacy and protection of data [7] but also to insure transparency, our framework enables fine-grained access control and full traceability. This implies being able to trace not only the identity of the user, but also to identify the chain of command (ministry, court, case) and potentially the context (terrorism threat) exhibited to enter a workflow or to access some information. Moreover, access to these auditing trails is protected as described in principle 3, using bespoke cryptographic techniques respecting privacy considerations to avoid malicious eavesdropping and to guarantee the judiciary independence.

Cross European scenarios raise this level of complexity, since authorization rules are defined by multiple organizations involving different structures and security policies for independent domains without supranational authority. Consequently, legal actors should be able to acquire temporary privileges from external authorities while not being appointed by the host country.

Finally, investigations and trials have to respect very precise rules/constraints (delay, notification, etc), which can moreover be different depending on the context; these rules should not be respected the system must not only forbid further interactions in the canonical path but may also explicitly mark certain evidences as invalid. These rules will be captured and reified within the eJustice platform (using the mentioned workflow annotations).

---

[2] In France, the *Perben II* law introduced a, controversy, new delict called *information divulgation* (§ 434-7-2)

Expressing mutual trust and delegation of rights in an inter-domain environment following the principles and techniques indicated in this paper provides a solution to these concerns taking into account the mandatory distributed architecture of justice systems.

# 4. Adaptive Attribute Certificates for Secure Distributed Workflows

Certificates provide a valid distributed alternative for access control and identity management over centralized Access Control Lists. No standard solution (including X.509v3 Attribute Certificate[14], SPKI[14], Akenti[11], SAML assertions[16]) was found to completely satisfy our requirements with respect to flexibility, traceability and advanced delegation. Therefore we decided to use and extend Eurecom Attribute Certificates [14] to provide a satisfactory AC framework to eJustice. Eurecom Attribute Certificates have been originally designed during ICare[12] and Witness[13] projects to provide a fully distributed Privilege Management Infrastructure which would exploit XML strengths, most specifically extensibility and readability for the programmer. Especially the latter aspects have been enhanced during eJustice, providing a new xml schema and a working library for AC management.

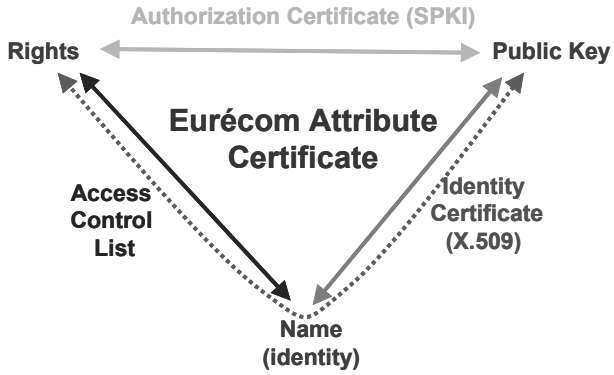


**Figure 4 – Eurécom Attribute Certificate**

Figure 4 compares the bindings that are authenticated with SPKI, X.509, ACLs and with attribute certificates. The Eurécom attribute certificate model (EuréCA) provides a flexible data structure for the management of distributed credentials that places identity and attributes on the same level. All attributes are defined in a uniform and extensible manner, with "identity" being just one like any other attribute. The flexible nature of attributes makes possible to embed information to assess platform trust, restrict rights to resources, embed roles, etc.

A certificate associates attributes to a principal (the holder) by a data structure signed by the certificate issuer; Certificate holder and issuer can either be a public key, like in SPKI, or a reference to another certificate (for example X.509v3 or EuréCA certificates).

Attribute structures traditionally associate a *name* with a *value*. As an open framework, the EuréCA model promotes the use of polymorphic attribute values: specific xml schemas can be developed to capture application level semantic (role hierarchy, resource access, time, trust…) both in term of structure and behaviour: the structural aspect can be used to further refine the value of an attribute, while behavioural aspect enables to add, for example, complex delegation

rules; the library exposes a plug-in based architecture, which permits to easily develop new attribute types along with their validators. The figure 5 shows the schema provided by default, custom attributes should subclass `AbstractAttributeType`.

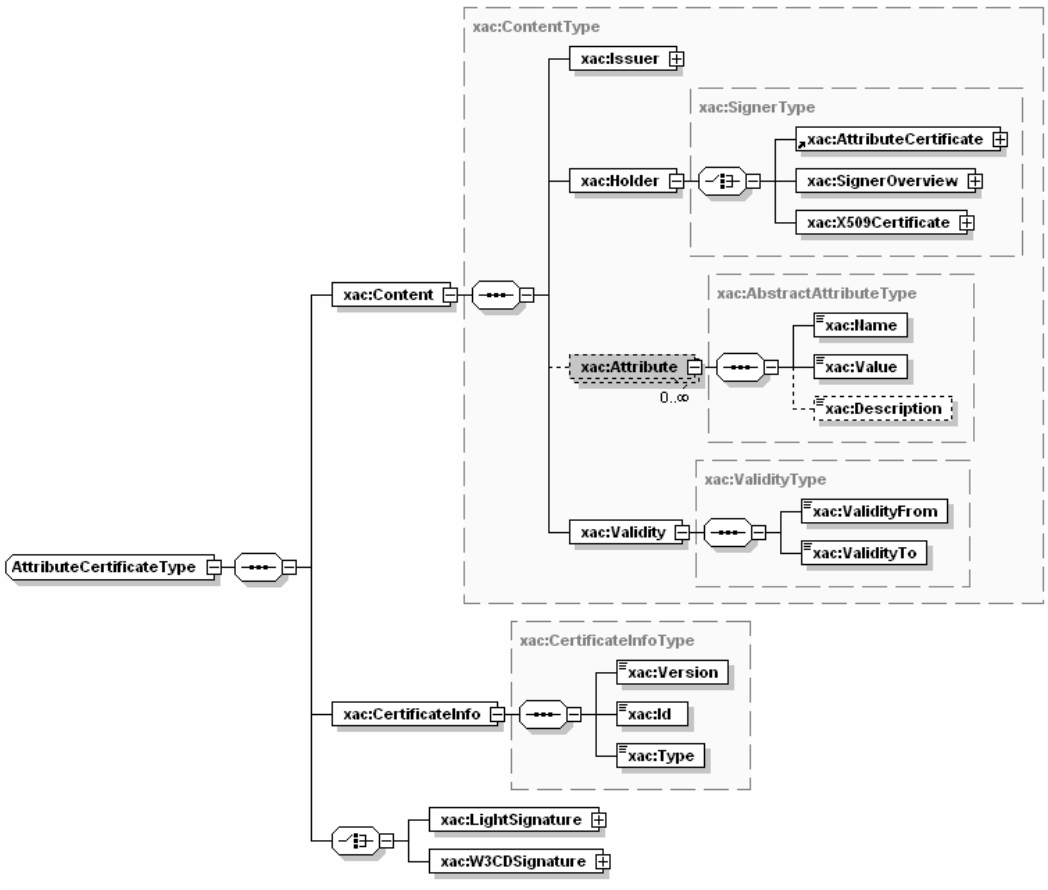


**Figure 5 - EuréCA XML Schema**

Any entity is entitled to act as a certification authority, thus makes this framework flexible and particularly suitable to distributed organizations aiming to trace the chain of command.

The delegating certificate (issuer) being embedded into the delegated signed certificate structure creates a tamper-proof trust chain which permits distributed validation; inter-domain delegation and trust-building is supported by chains nesting. This at the sole, although perceptible, expense of an increased size of certificates and chains.

Embedding qualified X.509 certificates and using secure signature creation devices (SSCD) enables the Holder to sign documents and to issue EuréCA certificates conform to the European directive on digital signatures [9].

# Perspectives and conclusion

We have presented a comprehensive approach which models Justice procedures into workflows while providing the design principles and the technical means to enforce security requirements. While justice workflow modelling is now mature, in this paper we present only the principles and a prototypical solution to provide enhanced security to judicial workflows

and support its enforcement; it is our intention to provide a more structured and formal definition of the design pattern described and the underlying security model.

An interoperable solution should support the latest results in distributed authentication and authorization. Web Services Security (WSS) suite (XACML, SAML, etc) associated with workflow orchestration and complementing EuréCa is likely to provide a good candidate as a basis for the architecture.

Moreover, the infrastructure should interact with legacy system (Schengen Information System [21][6]) and support a large number of heterogeneous trustworthy third party systems (time server, escrow, translation services …); these aspects are being taken into account in eJustice project.

Finally, this paper focuses on flow aspects of BPM; an interesting aspect currently under study is document-centric modelling.

# Index

Justice, Workflow, Security, Certificate, PKI, BPM

# References

[1] eJustice Project IST-2002-001567 http://www.ejustice.eu.com/

[2] eJustice D5.4 Using Biometric Smart Cards for Authentication and Signature

[3] eJustice D6.1 Workflow Security Requirements

[4] eJustice D7.3 Requirements and feasibility analysis

[5] eJustice D8.3.x WP6-8 Case study scenario

[6] Electronic Signatures and Infrastructures (ESI); Policy requirements for time-stamping authorities, ETSI TS 102 023 V1.2.1 (2003-01).

[7] European Directives 2002/58/EC on Privacy and Electronic communications (supersedes European Directive 1995/46/EC)

[8] European Electronic Signature Standardization Initiative (EESSI), iD2 Technologies, Sweden. http://www.ict.etsi.fr/eessi/Documents/Final-Report.pdf

[9] European Directive 1999/93/EC, on a Community framework for electronic signatures, December 13, 1999.

[10] Geschäftsverteilungsplan of the Oberlandesgericht Cologne, http://www.olg-koeln.nrw.de/home/wir/gvp/2005/gvp_s_05.pdf

[11] Akenti : Distributed Access Control http://www-itg.lbl.gov/Akenti/

[12] ICare project: http://www.cert-i-care.org/

[13] WiTness project: http://www.wireless-trust.org/

[14] Laurent Bussard, Joris Claessens, Stefano Crosta, Yves Roudier, Alf Zugenmaier *Can we take this offline?*, in Proceedings of the 4th Conference on Security and Network Architectures (SAR'05)

[15] RFC 2527 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework: ftp://ftp.isi.edu/in-notes/rfc2527.txt

[16] SAML: http://xml.coverpages.org/saml.html

[17] Kang, M. H., Park, J. S. and Froscher, J. N., *Access Control Mechanisms for Inter-organizational Workflow*, in Proceedings of the Sixth ACM Symposium on Access Control Models and

Technologies, pp. 66-74, 2001.

[18] RFC 2693 – SPKI Certificate Theory: ftp://ftp.isi.edu/in-notes/rfc2693.txt

[19] Strong Authentication: An Essential Component of Identity and Access Management, White Paper, RSA, August 2004.

[20] Team-and-role-based organizational context and access control for cooperative hypermedia environments, Weigang Wang,Proceedings of the tenth ACM Conference on Hypertext and hypermedia, 1999.

[21] The Schengen acquis and its integration into the Union http://europa.eu.int/scadplus/leg/en/lvb/l33020.htm

[22] The Workflow Management Coalition, http://www.wfmc.org/