Fostering European Justice collaboration using strong authentication and light authorisation schemes.

Jean-Christophe Pazzaglia
September, 23rd 2005

Eurécom (http://www.eurecom.fr/)
eJustice (http://www.ejustice.eu.com/)
Summary

In this presentation, we will demonstrate the advantages of the eJustice solution to foster the collaboration using strong authentication (biometric on card and PKI) and a light authorization scheme (distributed and fine grained attribute based authorization).

Our framework enable to keep the confidentiality of biometric, to use standard PKI primitives (authentication and signature) and to offer a versatile and traceable authorization scheme using advanced certification techniques.
eJustice Overview

Reengineering Justice Community working methods in Europe

- Seamless environment which:
  - uses ID smartcards to authenticate individuals
  - links this authentication process with the electronic signature of individuals
  - links a person's electronic signature with their rights to access digital data
  - links a workflow representation of a legal process with the simultaneous legal rights of the individual

- Consortium roles
  - Biometry and smartcard: Thales, Viisage
  - Law Modelisation: Saarbrucken University, IWI, MPI
  - Right Management and PKI: SAP, Eurecom, Infocamere, ...
  - Integration and prototype: Unisys, SAP, Metadat, BKA, ...

---
eJustice fact sheet
Project Reference: 001567
Duration: 24 months from 2004-03
Contract Type: Integrated Project
Project Cost: 6.67 million euro
Project Funding: 4.00 million euro
Consortium members: Thales, SAP, Unisys, Viisage, Saarbrucken University, MPI, BKA, Eurecom, DFKI ...
Web: http://www.ejustice.eu.com/

---
eJustice is an Integrated Project supported by the EC’s 6th Framework Programme. Its objective is to harness proportionate technology to improve the efficiency of legal procedures, too often cumbersome and paper-based, leading to confusion, delay, and miscarriage of justice.

It offers innovative solutions by integrating ICT and biometrics for controlling and tracking authorized access to a legal process which is automated as workflow systems, and represented in visual format. This cross-cutting approach addresses the needs and interactions of legal services at national level, as pioneered by the Austrian Government.

eJustice also provides solutions for cross-border procedures such as the European Arrest Warrant and European Judicial Assistance, with the support of the European Judicial Network and Eurojust, helping provide and create better justice across the EU, strengthening its wider role and impact internationally.

More information under http://www.ejustice.eu.com/
Phase I: From Law Text to Law Representation

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 despite 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.

[to be published, available upon request]

The need for interviews became apparent after the start of the project. The « practice » is not in the law text, it differs from court to court. The simultaneous recording of the law text and of the practice is a significant achievement of the project.
Phase II: Supporting procedures understanding and refinement (lexecute)

Lexecute - automated judicial assistance

"Lexecute is a tool to make the access to legal information easier both for lay people and legal professionals."

Lexecute is a prototype, thus its content may be erroneous or incomplete. We disclaim any liability.

Lexecute shows legal procedures from a new perspective. A process is not shown as a huge wall of text, as an example to illustrate our idea of an intuitively usable, practical knowledge representation system.

http://rechtsinformatik.jura.uni-sb.de/ejustice/lexecute/
Phase III: Enabling cross-border workflow implementation

- Technical as well as organisational security requirements must be satisfied:
  - Separation of duties
  - Digital signature
  - Secure Communication channels
  - etc.

The last stage consists to enable the assisted execution of procedures taking into account technical and organizational security requirements.
Rights Management and Workflow security (1/2)

- Workflow security design principles: WAB
  - ‘within’
    - Explicit capture at design stage of activity input/output, responsible entities and authentication means
  - ‘around’
    - Protects workflow interactions with external entities by rights/roles-based user authentication through the use of a distributed, PKI-based Attribute Certificate framework
  - ‘beyond’
    - Permits full traceability of the workflow activities w.r.t. the actors through non-repudiable, secure logs;

- Security services
  - enforce Strong Authentication and Authorization scheme using a dedicated, possibly biometric[19], device;
  - enable ‘secure’ 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].

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:

- ‘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.

- ‘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.

- ‘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.

From Stefano Crosta, Jean-Christophe Pazzaglia, Hendrik Schöttle "Modelling and Securing European Justice Workflows" ISSE'2005 – September 2005
[to be published, available upon request]
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[1] 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.

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

[to be published, available on request will be integrated to D6.6.2 (eJustice)]
Authentication Challenges

- Mitigate risk of Identity theft
- Comply with Regulation
- Be ethically acceptable
- Provide a cost effective solution
- Compatible with PKI
- Cross-border compatibility
Authentication Challenges: eJustice proposals

- Use *standard* contact smart cards
  - Standard encryption/signature capabilities
- Biometric solution for the verification of the cardholder
  - On-chip Biometric Match (no central database)
  - Multimodal features (fingerprint and face)
  - Use low cost sensors (webcam/fingerprint reader)
- Private and confidential information never disclosed
  - Private key storage/generation
  - Biometric values
- Versatile framework
  - Selective security measure (PIN, one biometric or two biometric checks) to comply with different legislation

Smart Card with On-chip Biometric Match

A smart card with on-chip biometric match is a smart card which takes as an input the biometric values measured by system sensors and provides as an output the result of the match with the on-chip biometric template of the card owner.

Since both the user biometric templates and the matching algorithm are on the card, user biometric data is never disclosed[2].

We emphasize that biometric information is an intrinsically public feature of individuals[9] and then cannot be considered as a secret by itself, although it is confidential. Authentication through biometry is based on the fact that the physical information *is* the person, and not on the knowledge of this data.

The security of a biometric system relies partly on the ability of the system to determine authenticity of shown physical features to avoid attacks such as fake fingerprints or face pictures; it can be necessary, depending on the application, to implement some trust measure of the equipment performing the biometric scan, and to have it assess the retrieved data. We also remind that physical human features cannot be revoked and it is thus a critical choice the way to use biometry.
WP4 (Thales-Viisage) demonstrated that combining two biometries (face and FP) improves by a factor of 30 the error rate achieved with one single biometry (with FAR fixed at 1/10000).
Improving 2D face recognition algorithm

Problem
- Higher likelihood of verification (i.e. higher matching score), if pose angles of images to compare are similar.

Bypassing 2D limitation
- Mapping of 2D texture information on a 3D model

3D model
- Texture image projected onto shape
- Rendering in under different conditions

3D shape model
- Generalized (average shape model)

2D texture image

Problem
- Higher likelihood of verification (i.e. higher matching score), if pose angles of images to compare are similar.
eJustice Authentication

- eJustice card in line with EU resolution on EU citizen passport 2004/0039(CNS)

Article 1, paragraph 2

“The passport shall include a highly secure storage medium with sufficient capacity and the capability of safeguarding the integrity, authenticity and confidentiality of the data stored. It shall contain a facial image. The Member States may also include fingerprints in interoperable formats. No central database of European Union passports and travel documents containing all EU passport holders’ biometric and other data shall be set up.”

- eJustice match on card biometric solution well accepted by privacy-conscious groups (activity in France, UK, …)
- Protect confidentiality of biometric artifacts (contrary to ICAO)
- Face/FP individual error rate improved by 2, combined error rate by 30.
  => to optimise matching time & FRR for FAR=1/10,000,
- Compatible with PKI
  - NB: European PKI interoperability is another challenge
  - D5.3 - Cryptography and PKI Survey – (6MS: Austria, Belgium, France, Germany, Italy, UK)

P6_TA(2004)0073
EU citizens' passports *
Amendment 5
Article 1, paragraph 2

The passport shall include a highly secure storage medium with sufficient capacity and the capability of safeguarding the integrity, authenticity and confidentiality of the data stored. It shall contain a facial image. The Member States may also include fingerprints in interoperable formats. No central database of European Union passports and travel documents containing all EU passport holders' biometric and other data shall be set up.
Cross border Collaboration Scenario

An investigator Maigret based in one country requires to consult some facts/evidences collected regarding a different case in another country (Italy under the supervision of Montalbano) and, eventually, to request a certified copy of relevant documents.

- Issues to solve
  - Identify the external investigator and mission
  - Give a temporary and restricted access to the system
  - Avoid that Maigret divulgate confidential information outside of the scope of the warrant
  - Do not allow Maigret to give away its access rights
  - Force Maigret to follow local workflow (laws)
  - Untamperable Traceability of the information to certify: how, who, where and why it was searched/delivered

EUROPA - Justice and Home Affairs - Freedom Security and Justice - Judicial cooperation in civil matters European Commission"European Union (EU) leaders recognise the need to tackle the problems that sometimes make the judicial and administrative systems of EU Member States complex and incompatible with each other. To enable individuals and companies to exercise their rights in a Member State other than their own, EU leaders laid out three priorities for action: better access to justice, mutual recognition of judicial decisions and increased convergence in the field of procedural law."[
http://europa.eu.int/comm/justice_home/fsj/civil/wai/fsj_civil_intro_en.htm ]

Scenario story:

Mr Jules Maigret and Salvano Montalbano are respectively Inspecteur appointed by the French Justice Ministry (Hotel Bourvallais) and Comissario appointed by the Italian Ministry (Palazzo Piacentini). A case concerning goods imitation occurs in the Ventimiglia town (XXMiglia), Comissario Montalbano is designated to investigate on this affair by the italian Ministry. Since some goods which are likely to come from the Italian Riviera were discovered in France, the Inspecteur Maigret requests the right to investigate in Ventimiglia to its counterpart Salvano Montalbano.

The only purpose of this scenario is to provide a straightforward illustration of our RM usage: it does not pretend to be legally correct. It is not inspired by the Rogatory Letter or European Arrest Warrant scenarios developed by other eJustice WPs.
PKI + ACL + RBAC based solution

- X509 identity certificate (stored on cards and controlled by biometrics) only solve authentication issues
- Standard RBAC usually involves static role
- Security Realm are requested to associate accounts and roles
  - Complex Realm should be reproduced for each subsystems
  - Interoperability may be problematic
- Data specific restriction is difficult
- Untamperable Traceability is problematic

Security Realm

A database of users, groups, and access control lists. Used to specify which users have access to the resources of a specific service (for example, to the Web Page Service). [Borland]
Attribute Certificate Solution

- Maigret exhibits case related credentials
- Montalbano generates on-purpose credentials
  - Rights subset can be delegated
  - Short period lifespan
  - Specific role
  - Specific resources
- Montalbano can grant more/less rights on demand very easily
Mr Jules Maigret and Salvano Montalbano are respectively Inspecteur appointed by the French Justice Ministry (Hotel Bourvallais) and Commissario appointed by the Italian Ministry (Palazzo Piacentini). A case concerning goods imitation occurs in the Ventimiglia town (XXMiglia), Commissario Montalbano is designated to investigate on this affair by the Italian Ministry. Since some goods which are likely to come from the Italian Riviera were discovered in France, the Inspecteur Maigret requests the right to investigate in Ventimiglia to its counterpart Salvano Montalbano.

The only purpose of this scenario is to provide a straightforward illustration of our RM usage: it does not pretend to be legally correct. It is not inspired by the Rogatory Letter or European Arrest Warrant scenarios developed by other eJustice WPs.
Eurecom Attribute Certificates

- Associate generic credentials to users (not only identity based)
- Suitable for Distributed Infrastructure
- Off/On-line deployment
- Role Based Access Control, Fine grain authorization scheme, ...
- Support for delegation schemes (person to person, person to software,...)
- Enhanced traceability (chain of command, multi-layer traceability, ...)

- Attribute Certificate in XML
- Polymorphism for attributes and signature (dsig)
- Flexible attribute structure
  - Name, Value, <<your wish>>
  - <<your wish>>: Controllable delegation, Resource, Embedded Policy, Programmable Delegation, PII...

Prototype library used for demonstrator development (Java/XML based)

D6.7.1 Prototype Library implementing Roles Management Framework API
EuréCA User guide version 0.9b Eurecom Updated: 20050413
Comparison

System A
Security Realm
Identity -> Roles
Roles -> ACL

System B
Security Realm
Identity -> Roles
Roles -> ACL

Security Realm
Credentials -> ACL

System A
Security Realm
Credentials -> ACL

System B
Security Realm
Credentials -> ACL

Credentials
Maigret
X509
Inspecteur

Credentials
Ventimiglia
Case

Jean-Christophe Pazzaglia
@eurecom.fr
September 23rd 2005
eJustice – Eurécom©
Summary

- Fostering Justice collaboration
  - Mutual understanding
  - Mutual trust
  - Agile framework
  - Local procedure enforcement
  - Traceability
  - Legislation compliance (European and local)

- eJustice approach
  - Task oriented approach (workflow)
  - Security as prime actor
    - WAB workflows
    - Strong authentication (biometric)
    - Portable and delegable authorization (EuréCA)

- Divide, Demonstrate and Conquer approach
  - 3 demonstrators
    - Law practitioners (Germany)
    - Government (Austria)
    - European bodies (EJN, European)
Future work

- Extend our scope
  - From justice to government procedures handling
  - Collaborative and distributed workflows (multiple engine on different administrative domains)
  - Address security and privacy issue from a wider organizational control perspective

- eJustice follow-up is under negotiation
  FP6Call5 (R4eGov (2006-2009?)) – DG INFSO Unit eGovernment
References

Stefano Crosta, Jean-Christophe Pazzaglia, Hendrik Schöttle: “Modelling and Securing European Justice Workflows”, ISSE2005


M. Rits, B. De Boe, and A. Schaad, “XacT: A Bridge between Resource Management and Access Control in Multi-layered Applications” presented at ACM Software Engineering Notes of Software Engineering for Secure Systems (ICSE05), St. Louis, Missouri, USA, 2005

“Biometry and IT : The Achievements of eJustice”, RTD Info Magazine, July 2005