

## A new approach to International Judicial Cooperation through secure ICT platforms

Cooperation between judicial systems is a key factor for sustainable development, one of the EU's major priorities. eGovernment plans and e-Justice initiatives supported by the European Commission and national governments create a very favourable background for the adoption of ICT standards in the area of cross-border judicial cooperation, both in Member States and in pre-Accession countries.

Intensification of illegal immigration, trafficking of drugs, weapons and human beings and the advent of terrorism have made necessary a stronger judicial collaboration between European countries. This cooperation includes mutual recognition of judicial decisions, collaboration in investigation phases and approximation of national penal legislations. During investigations, an exchange of information on criminal offences and administrative infringements takes place between judges and investigators belonging to different countries. This exchange is still mainly based on paper support.

This essay presents an overview of judicial cooperation in cross-border investigations and describes how computer supported cooperative work (CSCW), coped with security technologies, can improve magistrates' activities during cross-border investigations on criminal matters.



**Mauro Cislaghi**  
Project  
Automation  
S.p.A.

**Dominico Pellegrini**  
Ministero della Giustizia



**Elisa Negroni**  
Gov3 Limited

### Keywords

Judicial cooperation, investigations, e-Justice, e-services, security, magistrates, SCJW, JCP, Jweb, crime, workgroups, criminal records, CSCW

“ Electronic case management is demonstrating a dramatic reduction of required time in many daily operations through ICT support. ”

## 1 Introduction. An overview of the background in the European Union

Justice is a crucial variable of sustainable development, particularly in areas where development is lagging back the average growth of the European Union and where criminal organisations may find a favourable ground to flourish. Criminal activities are getting familiar with the Internet, becoming every day more and more borderless and global. For example, money coming from corruption may be transferred in different countries just with a few “clicks” on a personal computer. Investigations imply the delivery of several international judicial cooperation requests inside and outside the EU, following evidence flows and involving different organisation and departments. It is a complex process, still based on paper format even inside the same judicial organisation.

The European Commission is currently fostering e-Justice as part of the Lisbon Strategy<sup>1</sup> and eGovernment and supporting the enhancement of cross border judicial cooperation in both EU Member States and pre-accession countries. The establishment of Eurojust in 2002 and the strong support given by the [Directorate-General for Justice, Freedom and Security](#) and by the Council of Europe through several funding schemes are key factors in this process. The Network of Criminal Registers (NJR project, supported by DG JLS), which connects electronically the criminal registers of the EU Member States; the EPOC III project, with Eurojust as partner, and the PROSECO<sup>2</sup> project (Support to prosecutors’ network in South Eastern Europe, funded by CARDS program) are some of the many relevant ongoing activities. DG-INFSO is financing initiatives in ICT for criminal justice, such as the JWeB<sup>3</sup> [6][9](IST program) and JUMAS<sup>4</sup> (ICT program) projects. Relevant statistics about the trial phase have been collected by the Council of Europe through CEPEJ.

Many relevant projects in complementary fields, such as the mutual recognition of electronic signatures<sup>5</sup> and electronic identity and legal document interoperability, are running with strong support of the European Commission.

National e-Justice plans are in progress as well. In Italy the SICP project<sup>6</sup> re-organises the Italian ICT judicial system on district basis, connecting together judicial registers and deploying ICT systems for trial management (SIDIP project<sup>7</sup>, under deployment in South Italy in areas with high density of organised crime).

Judicial cooperation actually benefits from limited ICT support. Recent practices showed that ICT technologies can support investigating magistrates and all judicial actors providing them with **Secure Judicial Cooperation Workspace** (SCJW) integrated e-services, like information and document sharing, workflow sharing, videoconference, shared agendas, and granting at the same time the fundamental pre-requisites of non repudiation, confidentiality, data security and integrity. The paper gives an overview on these issues from the user point of view, through the analysis of the SecurE-Justice [11] and JWeB projects achievements. In the latter, cross-border judicial cooperation is supported by different ICT platforms called Judicial Collaboration Platforms (JCP) [6], based on groupware online tools which support collaboration and knowledge sharing among geographically distributed workforces, within and among judicial organizations. The Italian and the Montenegrin Ministries of Justice participate as partners.

## 2 Cross-border judicial cooperation during criminal investigations

The investigation phase includes all activities from the crime notification to the trial, including cross-border judicial cooperation. This may vary from simple to complex judicial actions; but it has complex procedures and requirements (e.g. information security and non repudiation). Each investigation may include multiple cross-border judicial cooperation requests, as the following general flow shows (figure 1):

---

<sup>1</sup> i2010 initiative, [www.europa.eu.int/information\\_society/eeurope/i2010/index\\_en.htm](http://www.europa.eu.int/information_society/eeurope/i2010/index_en.htm)

<sup>2</sup> EuropeAid/125802/C/ACT/Multi, <http://ec.europa.eu/europeaid/cgi/frame12.pl>, 2007

<sup>3</sup> JWeB project, <http://www.jweb-net.com/>

<sup>4</sup> JUMAS project, <http://www.milanoricerche.it/jumas/new/home.html>

<sup>5</sup> Recognition of electronic signature <http://ec.europa.eu/idabc/en/document/6485> and [http://ec.europa.eu/information\\_society/eeurope/i2010/esignature/index\\_en.htm](http://ec.europa.eu/information_society/eeurope/i2010/esignature/index_en.htm)

<sup>6</sup> SICP project, [http://www.albertomaritati.org/site\\_upload/files/sigi\\_schema.pdf](http://www.albertomaritati.org/site_upload/files/sigi_schema.pdf)

<sup>7</sup> SIDIP project, <https://www.giustiziacampania.it/file/1053/File/mozzillosidipsalerno.ppt>

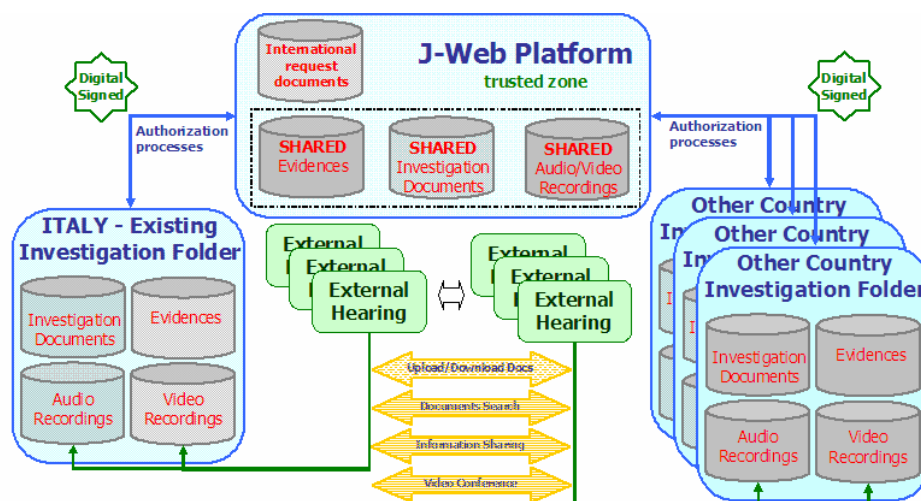


### 3 The cross-border Judicial Cooperation via secure ICT platforms

#### 3.1 The services provided by a Judicial Collaboration Platform (JCP)

A workspace for judicial cooperation (figure 2) involves legal, organisational and technical issues, and requires a wide consensus in judicial organisations. It has to allow a straightforward user interface, easy data retrieval, and a seamless integration with procedures and systems already in place. All this, provided according to top-level security standards. In more detail, the main issues for judicial collaboration are:

- A Judicial Case is a secure private virtual workspace accessed by law enforcement and judicial authorities who need to collaborate in order to achieve common objectives and tasks.
- JCP services are on-line services, supplying various collaborative functionalities to the judicial authorities in a secure communication environment.
- User profile is a set of access rights assigned to a user. The access to a judicial case and to JCP services are based on predefined, as well as customised, role-based user profiles.
- Mutual assistance during investigations creates a shared part of the investigation folder.
- Each country will have its own infrastructure.



*Figure 2. Logical Overview of the workspace for judicial cooperation.*

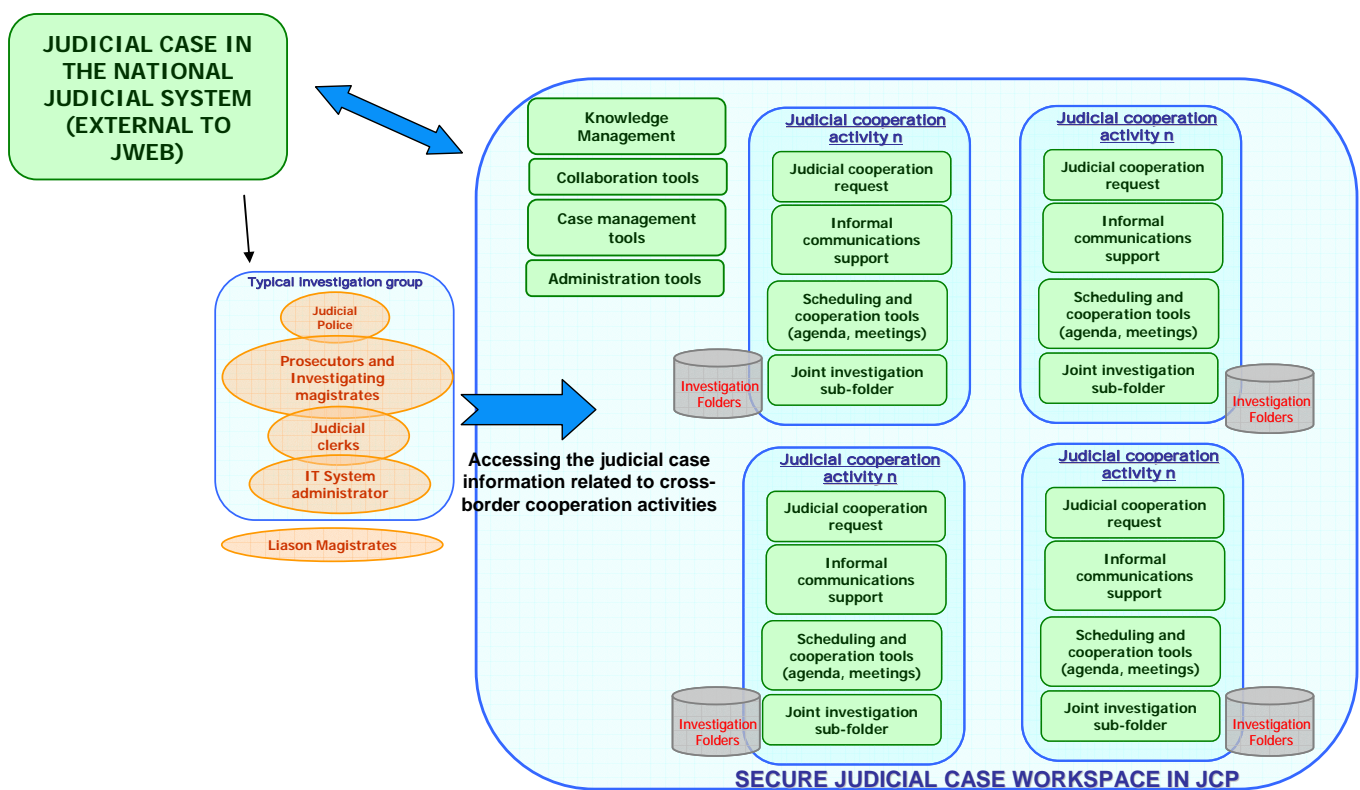
The core system supporting judicial cooperation (figure 3) is the secure JCP [6]. It is part of a national ICT judicial infrastructure, connected to the national judicial network via secure and trusted interfaces. It connects the investigating team, the liaison magistrates and, in perspective, the embassies. Different JCPs in different countries may work together during judicial cooperation. The platform, organised on three layers (presentation, business, persistence), supports availability and data security supplying the following main services:

- **Profiling:** user details, user preferences, users roles.
- **Services supplied via Web:**
  - **Collaboration:** collaborative tools so that users can participate and discuss on the judicial cooperation cases.
  - **Workflow Management:** execution of judicial cooperation workflows, including the ones required to set-up judicial cooperation.

- **Audio/Video Management:** real time audio/video streaming of a multimedia file, videoconference support, with the possibility to create direct links with already equipped prisons and prosecutors offices and between the workgroups.
- **Knowledge Management:** documents uploading, indexing, search, exchange.
- **Security and non repudiation:** Biometric authentication, digital certificates, time stamping, digital signature, secure communication, cryptography, role based access control.

### 3.2 The Secure Judicial Cooperation Workspace and Judicial Cooperation Activities

The **Secure Judicial Cooperation Workspace (SCJW)** is a secure inter-connected environment related to a specific judicial case, in which all entitled judicial participants in dispersed locations can access and interact with each other just as inside a single entity. The environment is supported by secure [electronic communications](#) and [groupware](#) tools, which enable participants to overcome space and time differentials. From the physical point of view, the workspace is supported by the JCP.



*Figure 3. Secure Collaborative Judicial Workspace and Judicial Cooperation Activities.*

The SCJW allows the actors to use shared communication and scheduling instruments (agenda, shared data, videoconference, digital signature, document exchange) in a secured environment.

A **Judicial Cooperation Activity (JCA)** is the implementation of a specific judicial cooperation request. It is a self-consisting activity, opened inside the SCJW and supported by specific judicial workflows and by the collaboration tools. It fulfils the judicial actions in a single letter of rogatory.

Each SCJW, "owned" by the investigating magistrate in charge of the judicial case, is related to a single judicial case and may contain multiple JCAs, also running in parallel. Each JCA ends when rejected or when all requests contained in the letter of rogatory have been fulfilled and the information collected has been inserted into the target investigation folder, external to the JCP. At that moment the JCA may be archived. The SCJW ends when the investigation phase is concluded.

Each JCA has dedicated temporary repository for the ongoing activities. The permanent archive is outside the JCP, in the judicial ICT national system, where the investigation folders are stored. This is due to security, confidentiality and non repudiation constraints and to the limited lifetime of a JCA. The repository associated to the single JCA contains, from the users perspective:

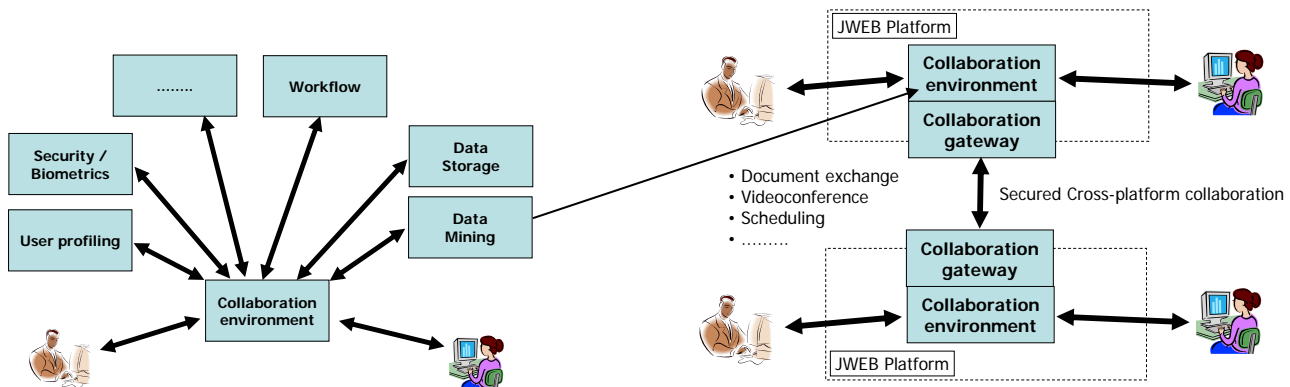
– **JCA judicial information**

The documentation produced during the judicial cooperation will be stored in a configurable tree folder structure. Typical contents are:

- 1) “**JCA judicial cooperation request**”. It contains information related to the judicial cooperation request, including further documents exchanged during the set-up activities.
- 2) “**JCA decisions**”. It contains the outcomes of the formal process of judicial cooperation and any internal decision relevant to the specific JCA (for example letters of appointments of the magistrate(s), judicial acts authorising interceptions or domicile violation, etc.)
- 3) “**JCA investigation evidences**”. It contains the documents to be sent/ received:
  - a. *Audio/video recordings*, from audio/video conferences and phone interceptions
  - b. *Images*. It contains pictures and photos.
  - c. *Objects and documents*. It contains text documents and scanned documents.
  - d. *Supporting documentation*, not necessarily to be inserted in the investigation folder.

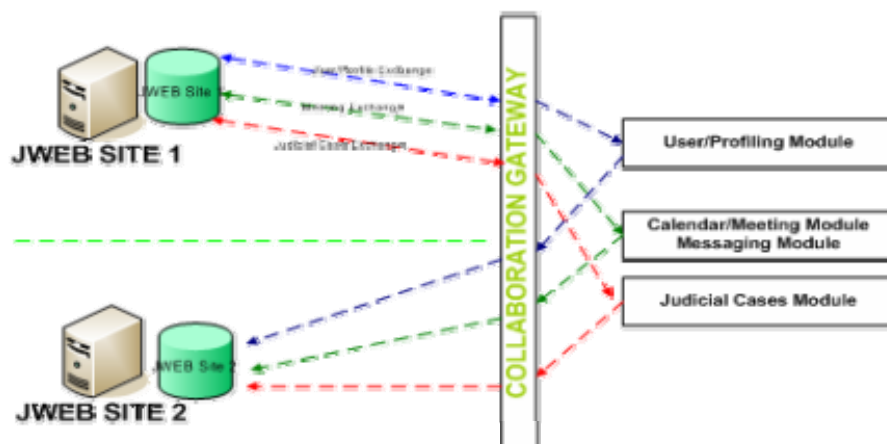
### 3.3 Connecting and accessing JCPs in a secure way

SCJW is implemented in a single JCP, while the single JCA is distributed on two JCP connected via secure communication channels, and implemented through a secure collaboration gateway, as showed in figure 4.



*Figure 4. The JCP and different JCPs implementing the Judicial Cooperation Activities.*

The concept is showed in figure 5, where two JCP platforms are connected via a set of secure Web Services.



*Figure 5. The collaboration gateway architecture*

Two different level of security are implemented: the JCP is intrinsically secure and communication between JCPs are made secure, so as to create a trusted virtual space inside the JCP and between JCPs. Security is managed through the Security Module, designed to properly manage Connectivity Domains, to assure access rights to different entities, protecting information and segmenting IP network in secured domains. Any communication is hidden to third parties, protecting privacy, preventing unauthorised usage and assuring data integrity.

JCP access is protected by user authentication by means of his/her X.509v3<sup>9</sup> digital certificate issued by the Certification Authority, stored in his smart card and protected by biometry. Communication with the JCP and between JCPs are via the implementation of Internet Protocol Security (IPSec<sup>10</sup>), through secure channels, called VPN (Virtual Private Network) tunnels, which guarantee the confidentiality of any communication. Data flows may have different levels of encryption.

Only authenticated and pre-registered users and systems can access the JCP; no access is allowed without the credentials given by the PKI (Public Key Infrastructure).

The JCP includes an Access and Network Security System, integrated by the following components:

- Security Access Systems (Crypto-router). Crypto-routers prevent unauthorized intrusions, offers protection against external attacks and tunnelling capabilities and data encryption, providing both Network and Resources Authentication.
- S-VPN clients (Secure Virtual Private Network Client), through which the user can entry in the JCP VPN and so can be authenticated by the Security Access System.
- Access control of judicial actors to JCP functions via biometric authentication (fingerprint) Role-Based Access Control [10] (RBAC). In RBAC, access permissions re associated with roles, and users are made members of appropriate roles. This model simplifies access administration, management, and audit procedures. Examples of roles are “magistrate”, “judicial clerk”, “liaison magistrate”, “videoconference technician”, “ICT administrator”, each of them with specific access permission.

### 3.4 Documents, information exchange and interoperability in JCP

The JCP is intended mainly as a trustworthy web-based platform supporting a shared workspace (including capabilities for audio/video recordings via videoconference) and a secure exchange of documents and information. It has to support the nearly 300 most common documents and audio/video files formats, giving the possibility to use standard commercial and open source readers and players available on different

<sup>9</sup> International Telecommunication Union <http://www.itu.int/ITU-T/asn1/database/itu-t/x/x509/>

<sup>10</sup> IPSEC working group at IETF <http://www.ietf.org/html.charters/ipsecme-charter.html>

operating systems, with support for digital signatures. Documents are both working and legal archives directly connected to the JCA (judicial cooperation request, decisions by the counterpart, the requested evidences, usually scanned documents, textual or audio-video), exchanged between a restricted number of actors, as it usually happens during investigations. Many of them are scanned paper documents.

Key features in JCP are interoperability, the confidentiality of investigation documents and information in the JCAs and non-repudiation of documents, which sets new challenges and constraints regarding format and information retrieval. The search is restricted to authorised operators on the JCAs where they are entitled to have access. This is limited according to the role of the person seeking for information. Metadata and XML files generated by search engines may contain confidential information. This point is still open, and the usefulness of a fully semantic search engine in JCP is under discussion.

Relevant initiatives related to JCP interoperability are the European Metalex<sup>11</sup>, the OJP Information Technology Initiatives<sup>12</sup> by the United States Department of Justice and the related National Information Exchange Model (NIEM), based on the Global Justice XML Data Model (GJXDM), and the Judicial Reference Architecture (JRA), based on OASIS SOA (Service Oriented Architecture) Reference model. Widespread adoption of XML and secure SOA architectures are crucial elements in deploying systems for judicial cooperation. Adoption of SOA is pushed by eGovernment initiatives. JCP collaboration environment benefits from the experiences of several eGovernment projects, including Terregov<sup>13</sup> project, and secure SOA and SOAP messaging constitute the technical basis of communication between systems.

## 4 Potential impact of ICT support to judicial cooperation

Judicial cooperation requests issued every year may vary from hundreds in small EU Member States to thousands in the more populated ones, both in terms of active and passive rogatories. Notwithstanding the relatively low number of criminal cases (a little percentage or less) where judicial cooperation is requested, out of the overall number of criminal cases (an average in the EU of about 4,800 criminal offences and 900 convicted persons each 100,000 inhabitants<sup>14</sup>), they are indispensable in most of the major investigations about organised crime, terrorist groups, illegal trafficking, relevant episodes of corruption and fraud, where significant resources of the judicial organisations are spent, with top investigating magistrates engaged, and where the support of the liaison magistrate of Eurojust may be fundamental.

Electronic case management is demonstrating a dramatic reduction of required time in many daily operations through ICT support: a recent paper about UYAP<sup>15</sup> system in Turkey showed how the time required by simple operations such as accession to criminal records or transfer of documents decreased from an average of two weeks to few minutes. Similar data are available in most of EU countries.

Videoconference in courtrooms<sup>16</sup> has been used in Italy and other countries for the last 10 years and a first manual on e-Justice videoconferencing in cross-border judicial activities is likely to be published by the Council of Europe in early 2009. Usage of videoconference in compliance with the “principle of fair trial”, for example for remote interrogations of witnesses, persons under protection and persons in prison, will allow a considerable savings of time also in judicial cooperation activities.

JCP e-services such as secure document transfer, videoconference, information sharing and traceability of judicial cooperation activities, in particular in passive rogatories, will progressively allow considerable savings, similar to the ones achieved with case management systems. These savings are still difficult to be precisely quantified against the actual figures, due to limited existing statistics. These e-services will make the link of the single investigation team with offices in charge of international cooperation, liaison magistrate and the

---

<sup>11</sup> <http://www.metalex.eu/>

<sup>12</sup> <http://it.ojp.gov/index.jsp>

<sup>13</sup> [http://www.terregov.eupm.net/my\\_spip/index.php](http://www.terregov.eupm.net/my_spip/index.php)

<sup>14</sup> The European Sourcebook project, “European Sourcebook of Crime and Criminal Justice Statistics – 2006”, <http://www.europeansourcebook.org/>

<sup>15</sup> Ali Riza Cam “EU principles in modernisation of Justice and the Turkish IT project UYAP”, European Journal of ePractice · [www.epracticejournal.eu](http://www.epracticejournal.eu) N° 3 · May 2008 · ISSN: 1988-625X

<sup>16</sup> Aki Hietanen “Videoconferencing in crossborder court proceedings” [www.ejustice2008.si/en/wp-content/uploads/2008/06/videoconferencing\\_in\\_crossborder\\_court\\_proceedings.ppt](http://www.ejustice2008.si/en/wp-content/uploads/2008/06/videoconferencing_in_crossborder_court_proceedings.ppt)

Ministry of Foreigner Affairs more effective. They will reduce the existing inefficiencies, mainly due to complex procedures not supported by straightforward communication channels, and shorten the duration of investigations and of criminal cases, one of the main objectives of e-Justice.

## 5 Conclusions

The SecurE-Justice and JWeB pilot actions demonstrate how international judicial cooperation may be supported by ICT platforms through the integration of state of the art ICT technologies, connecting and providing e-services first to organisations inside the same country and in perspective connecting together different Member States. All this in total respect with the requirements of security, non repudiation, confidentiality and strong authentication, as well as in full compliance with national judicial procedures and practices.

The economical effort required for infrastructure is quite sustainable, considering that in most EU Member States a very limited number of JCPs, even only one in the small states, may be sufficient to manage the yearly issued or received requests and that the communication environment is the web. Possible failures external to JCPs (such as denial of service attack to telecom operators and web providers) may always be mitigated using disaster recovery strategies.

The progressive adoption of mutual recognition of digital signature and the adoption of an EU-wide recognised standard format for legal document exchange, actually in progress and strongly pushed also by other fields such as e-commerce and e-procurement, will create the basis in the near future for the full exploitation of the JCP as a part of the European Judicial Space.

eGovernment plans and e-Justice initiatives supported by the European Commission and by the national governments create a very favourable background to the adoption of ICT support and standards in the area of cross-border judicial cooperation, both in the Member States and in the pre-Accession countries. CARDS and IPA funds represent today a relevant financial support to regional development in Western Balkans, including Justice as one of the key factors. This creates a strong EU support to JCP deployment, while projects such as JWeB and SICP demonstrated that electronic case management is now ready for a complete deployment.

A judicial secure collaboration environment will be the basis for future trans-national cooperation, and systems such as the JCP may lead to a considerable enhancement of cross-border judicial cooperation. While technologies are mature and ready to be used, their impact on the judicial organisations in cross-border cooperation is still under analysis. It is one of the main non technological challenges for deployment of solutions such as the one under development in the JWeB project. The analysis conducted so far in the JWeB project gives a reasonable confidence that required organisational changes will become fully evident through the pilot usage of the developed ICT solutions, hence contributing further to the Ministries of Justice work enhancement by allowing the full electronic management of activities in a delicate area such as the one of the international judicial cooperation.

Uptake of the pilot experience can be done progressively in the different judicial systems: starting at national level first, by integrating vertically, in a common workspace, the activities of each judicial workgroup (investigating magistrates, their assistants, the judicial clerks, the liaison magistrates, the embassies and the liaison magistrates), then extending horizontally the single JCP to cooperation between JCPs in different countries. This approach will help to solve a relevant number of problems posed by legacy systems in force and allow to build up the interconnection layer between different countries, taking into account the upcoming standards for cross-border information exchange, such as the ones of Metalex<sup>17</sup> initiative on an Open XML interchange format for legal and legislative resources and ESTRELLA<sup>18</sup> European Project. The JWeB experience is demonstrating that JCP can contribute to sort out one of the main problems related to security of judicial networks: how to provide services to investigation teams and systems located “outside the national judicial network” without affecting security. This is the case of the ICT platform developed in the EPOC III project led by EUROJUST. Trusted connections included in JCP will allow to close “the last mile” between

---

<sup>17</sup> <http://www.metalex.eu/>

<sup>18</sup> <http://www.estrellaproject.org/>

judicial actors without lowering the level of security of the network and connecting transparently the legacy judicial systems.

## References

- [1] CARDS project: Support to the Prosecutors Network, EuropeAid/125802/C/ACT/Multi in <http://ec.europa.eu/europeaid/cgi/frame12.pl>, 2007
- [2] G. Armone et.al. Diritto penale europeo e ordinamento italiano : le decisioni quadro dell'Unione europea : dal mandato d'arresto alla lotta al terrorismo In: Giuffrè editions, 2006. ISBN 88-14-12428-0.
- [3] EUROJUST at: <http://eurojust.europa.eu>
- [4] European Commission , ICT in the courtroom, the evidence is clear at: [http://ec.europa.eu/information\\_society/activities/policy\\_link/documents/factsheets/jus\\_ecourt.pdf](http://ec.europa.eu/information_society/activities/policy_link/documents/factsheets/jus_ecourt.pdf), 2005
- [5] European Commission. Security for judicial cooperation. In: [http://ec.europa.eu/information\\_society/activities/policy\\_link/documents/factsheets/just\\_secure\\_justice.pdf](http://ec.europa.eu/information_society/activities/policy_link/documents/factsheets/just_secure_justice.pdf), 2006
- [6] M. Cislaghi, F. Cunsolo, R. Mazzilli, R. Muscillo, D. Pellegrini, V. Vuksanovic. Communication environment for judicial cooperation between Europe and Western Balkans In: Expanding the knowledge economy, eChallenges 2007 conference proceedings, The Hague, The Netherlands, October 2007. ISBN 978-1-58603-801-4, 757-764.
- [7] Italian Committee for IT in Public Administrations (CNIPA), Linee guida per la sicurezza ICT delle pubbliche amministrazioni. In Quaderni CNIPA 2006, <http://www.cnipa.gov.it/site/files/Quaderno20.pdf>.
- [8] Italian Committee for IT in Public Administrations (CNIPA), CNIPA Linee guida per l'utilizzo della Firma Digitale, in CNIPA May 2004 [http://www.cnipa.gov.it/site/files/LineeGuidaFD\\_200405181.pdf](http://www.cnipa.gov.it/site/files/LineeGuidaFD_200405181.pdf)
- [9] JWeB project consortium and website at: [http://www.jweb-net.com/index.php?option=com\\_content&task=category&sectionid=4&id=33&Itemid=63](http://www.jweb-net.com/index.php?option=com_content&task=category&sectionid=4&id=33&Itemid=63), 2007-2008
- [10] Ferraiolo D F, Sandhu R, Gavrila S, Kuhn D R, Chandramouli. A proposed standard for rolebased access control. Technical report, National Institute of Standards & Technology, 2000.
- [11] SecurE-justice project website <http://83.103.118.7/project.asp>, 2007.

## Authors

**Mauro Cislaghi**

International Project Manager  
Project Automation S.p.A., Italy  
<http://www.epractice.eu/people/cislaghi>

**Domenico Pellegrini**

Ministero della Giustizia - DGSIA AreaPenale  
<http://www.epractice.eu/people/1817>

**Elisa Negroni**

Project Manager  
Gov3 Limited, UK  
[j-web.project@gov3innovation.eu](mailto:j-web.project@gov3innovation.eu)  
<http://www.epractice.eu/people/Elisa>



The European Journal of ePractice is a digital publication on eTransformation by ePractice.eu, a portal created by the European Commission to promote the sharing of good practices in eGovernment, eHealth and inclusion.

Edited by P.A.U. Education, S.L.  
Web: [www.epracticejournal.eu](http://www.epracticejournal.eu)  
Email: [editorial@eppractice.eu](mailto:editorial@eppractice.eu)



The texts published in this journal, unless otherwise indicated, are subject to a Creative Commons Attribution-NonCommercial-NoDerivs 2.5 licence. They may be copied, distributed and broadcast provided that the author and the e-journal that publishes them, European Journal of ePractice, are cited. Commercial use and derivative works are not permitted. The full licence can be consulted on <http://creativecommons.org/licenses/by-nc-nd/2.5/>