A New Approach to International Judicial Cooperation through Secure ICT platforms

Mauro Cislaghi[1], George Eleftherakis[2],
Domenico Pellegrini[3], and Konstantinos Rousis[2]

[1] Project Automation S.p.A.,
42 Viale Elvezia, 20052 Monza, Italy
mauro.cislaghi@p-a.it
http://www.p-a.it
[2] South-East European Research Centre (SEERC),
17 Mitropoleos Str., 54624 Thessaloniki, Greece
{geleftherakis,konrousis}@seerc.org
http://www.seerc.org
[3] Italian Ministry of Justice-DG SIA,
Rome, Italy
domenico.pellegrini@giustizia.it
http://www.giustizia.it/

Abstract. Cooperation between judicial systems is a key element for sustainable development and one of the key priorities for EU. Due to cross-border crimes rise, the EU is working on the development of judicial cooperation between Member States. Increase of illegal immigration, trafficking of drugs, weapons and human beings, and the advent of terrorism, made necessary a stronger judicial collaboration between States. Judicial cooperation includes mutual recognition of judicial decisions, cooperation in investigation phase, and approximation of penal legislation of involved states. During the investigations an exchange of information on criminal offences and administrative infringements takes place between judges and investigators belonging to different countries, actually based mostly on paper support. The paper presents an overview of judicial cooperation in cross-border investigations, describing how ICT infrastructures and computer supported cooperative work (CSCW), coped with security technologies, can support judicial cooperation of magistrates' activities during cross-border investigations on criminal matters in a process still paper based.

1 Introduction

Justice is a key success factor in Sustainable Development, in particular in areas whose development is lagging back the average development of the European Union and criminal organisation may found a favourable ground to develop. Criminal activities are following the development of the Internet era, becoming every day 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 about require the issue of several international judicial cooperation requests inside and outside the EU, following the evidence flows and involving different judicial organisation and departments. It is a complex process, still paper based even inside the same judicial organisation.

The European Commission is actually pushing the implementation of e-Justice as a part of the Lisbon Strategy1 and e-Government and supporting the enhancement cross border judicial cooperation both in EU Member states and pre-accession countries. The creation 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), electronically connecting the criminal registers of the EU Member States, the EPOC III project with Eurojust as partner and the PROSECO2 project (Support to prosecutors' network in South Eastern Europe, funded by CARDS program) are between the many relevant ongoing activities. DG-INFSO is supporting perspective initiatives in ICT for criminal justice, such as the JWeB3 [6][9](IST program) and JUMAS4 (ICT program) projects. Relevant statistics about the trial phase have been collected by the Council of Europe through CEPEJ.

Many relevant projects in complementary field, such as the mutual recognition of electronic signatures5 and electronic identity and legal document interoperability, are in progress with a strong support by the European Commission.

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

Judicial cooperation actually benefit of limited ICT support; recent practices showed that ICT technologies can support investigating magistrates and all judicial actors, providing them in a **Secure Judicial Cooperation Workspace** (SCJW) integrated e-services, such as 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 give an overview on the user point of view on these issues through the achievements of the SecurE-Justice [11] and JWeB projects, where cross-border judicial cooperation is supported by different ICT platforms called Judicial Collaboration Platforms (JCP) [6], based on Web-based groupware tools supporting collaboration and knowledge sharing among geographically distributed workforces, within and between judicial organizations, having the Italian and Montenegrin Ministries of Justice as partners.

[1] i2010 initiative, www.europa.eu.int/information_society/eeurope/i2010/index_en.htm

[2] EuropeAid/125802/C/ACT/Multi, http://ec.europa.eu/europeaid/cgi/frame12.pl , 2007

[3] JWeB project, http://www.jweb-net.com/

[4] JUMAS project, http://www.jumasproject.eu

[5] 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

[6] SICP project, http://www.albertomaritati.org/site_upload/files/sigi_schema.pdf

[7] SIDIP project, https://www.giustiziacampania.it/file/1053/File/mozzillosidipsalerno.ppt

2 Cross-border judicial cooperation during criminal investigations

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

1. In the requesting country, the magistrate starts preliminary checks to understand if her/his requests to another country are likely to produce the expected results. Liaison magistrate support and preliminary contacts with magistrates in the other country are typical actions.
2. The "requesting" magistrate prepares and sends the judicial cooperation request (often referred to as "letter of rogatory") containing the list of specific requests to the other country. Often the flow in the requesting country is named "active rogatory", while the flow in the requested country is named "passive rogatory". In the EU member states there is a well defined frame for judicial cooperation8In case no agreement between countries exists, the Ministries of Justice are connected through the Ministries of Foreign Affairs and the embassies.
3. The judicial cooperation request coming from the other country is evaluated, usually by a court of appeal, that in case of positive evaluation, appoints the prosecutors' office in charge of the requested activities. This prosecutors' office appoints a magistrate. The requesting magistrate, directly or via the office delegated to international judicial cooperation, receives back these information and judicial cooperation starts.
4. Judicial cooperation requests are fulfilled: **requests for documents, for evidences, interrogations (also via videoconference where possible), specific actions (interceptions, sequestration, an arrest, etc.), joint investigations, etc.** At fulfilment, the judicial cooperation ends.

These activities may imply complex actions in the requested country, involving people (magistrates, police, etc.) in different departments. The liaison magistrate can support requesting magistrates, helping them to understand how to address the judicial counterpart and, once judicial cooperation has been granted, in understanding and overcoming possible obstacles. Where no judicial cooperation agreement exists, all information must flow through the Ministry of Foreign affairs and the Embassies.

While agreements for mutual judicial assistance are now in force in the EU member states, just a few instruments in the judicial systems are available to track the "rogatories", in particular the "passive" ones, and the magistrate action often suffers from this lack.

Each national judicial system is independent from the others, both in legal and infrastructural terms. Judicial cooperation, on the ICT point of view, implies cooperation between two different infrastructures, the "requesting" one ("active") and the "requested" ("passive"), and activities such as judicial cooperation setup, joint

[8] Judicial Cooperation, http://ec.europa.eu/justice_home/fsj/criminal/fsj_criminal_intro_en.htm

activities of the workgroups, secure exchange of not repudiable information between the two countries. These activities can be effectively supported by a secure collaborative workspace, as described in the next section.

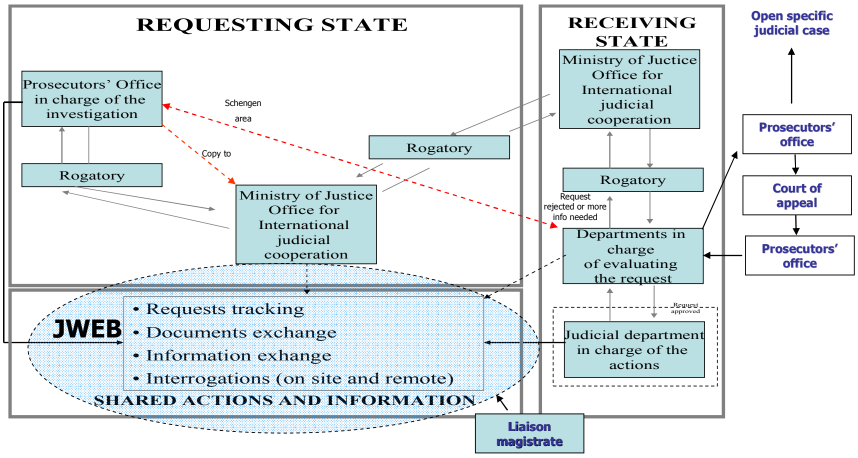
REQUESTING STATE
RECEIVING STATE
Open specific judicial case
Prosecutors' Office in charge of the investigation
Schengen area
Copy to
Rogatory
Rogatory
Ministry of Justice Office for International judicial cooperation
Ministry of Juctice Office for International judicial cooperation
Rogatory
Request rejected or more info needed
Departments in charge of evaluating the request
Prosecutors' office
Court of appeal
Prosecutors' office
Request approved
Judicial department in charge of the actions
JWEB
• Requests tracking
• Documents exchange
• Information exhange
• Interrogations (on site and remote)
SHARED ACTIONS AND INFORMATION
Liaison magistrate

Fig. 1. The cross-border judicial cooperation: a general workflow.

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 straightforward user interface, easy data retrieval, seamless integration with procedures and systems already in place.

All that implemented providing top-level security standards. Accordingly, the main issues for judicial collaboration are:

- A "Judicial Case Workspace" is a secure private virtual workspace accessed by law enforcement and judicial authorities, that need to collaborate in order to achieve common objectives and tasks on a specific judicial case.
- JCP delivers 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 investigation folder.

- Each country will have its own infrastructure. Shared ICT systems will lead to the need of a supervising agency, similar to EUROJUST.

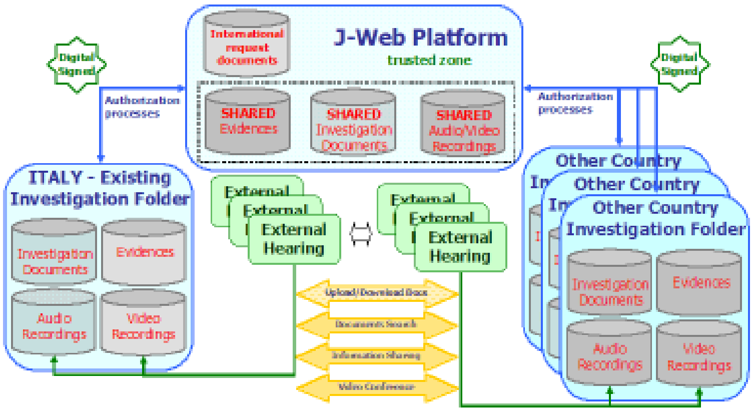

Fig. 2. Logical Overview of the workspace for judicial cooperation.

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 connections. It connects the investigating team, the liaison magistrates and in perspective the embassies. Different JCPs in different countries may cooperate during judicial cooperation. The platform, organised on three layers (presentation, business, persistence), supports availability and data security and provides the following core 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, to which all entitled judicial participants in dispersed locations can access and interact 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. On the physical point of view, the workspace is supported by the JCP.

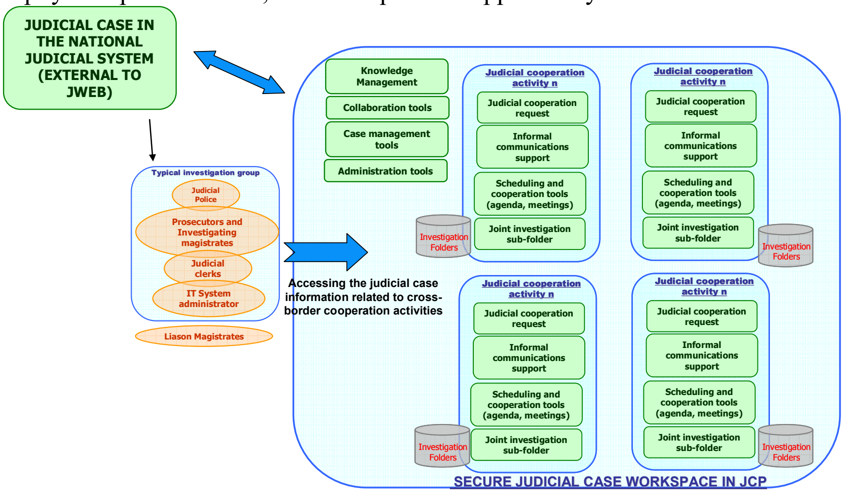
JUDICIAL CASE IN THE NATIONAL JUDICIAL SYSTEM (EXTERNAL TO JWEB)
Typical investigation group
Judicial Police
Prosecutors and Investigating magistrates
Judicial clerks
IT System administrator
Liason Magistrates
Accessing the judicial case information related to cross-border cooperation activities
Knowledge Management
Collaboration tools
Case management tools
Administration tools
Judicial cooperation activity n
Judicial cooperation request
Informal communications support
Scheduling and cooperation tools (agenda, meetings)
Joint investigation sub-folder
Investigation Folders
SECURE JUDICIAL CASE WORKSPACE IN JCP

Fig. 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 have been inserted into the target investigation folder, external to the JCP. In this 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 on the user point of view:

- **JCA judicial information**. The documentation produced during the judicial cooperation will be stored in a configurable tree folder structure. Typical contents are:
  - "**JCA judicial cooperation request**". It contains information related to the judicial cooperation request, including further documents exchanged during the set-up activities.
  - "**JCA decisions**". It contains the outcomes of the formal process of judicial cooperation and any internal decision relevant to the specific JCA (for example letter of appointment of the magistrate(s), judicial acts authorising interceptions or domicile violation, etc.)
  - "**JCA investigation evidences**". It contains the documents to be sent/ received:
    - *Audio/video recordings*, from audio/video conferences and phone interceptions
    - *Images*. It contains pictures and photos.
    - *Objects and documents*. It contains text documents and scanned documents.
    - *Supporting documentation*, not necessarily to be inserted in the investigation folder.

3.2 The 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 channel, and implemented through a secure collaboration gateway, as shown in figure 4.

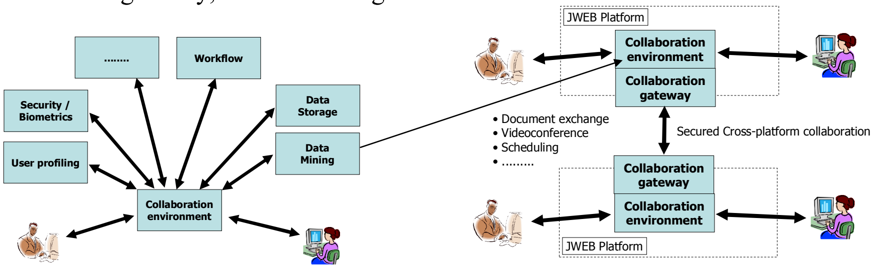

Fig. 4. JCP and different JCPs implementing the Judicial Cooperation Activities.

The concept is shown in figure 5, where two JCP platforms are connected via a set of secure Web Services. Two different level of security are implemented: the JCP is intrinsically secure and communication between JCPs are made secure, so creating 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.

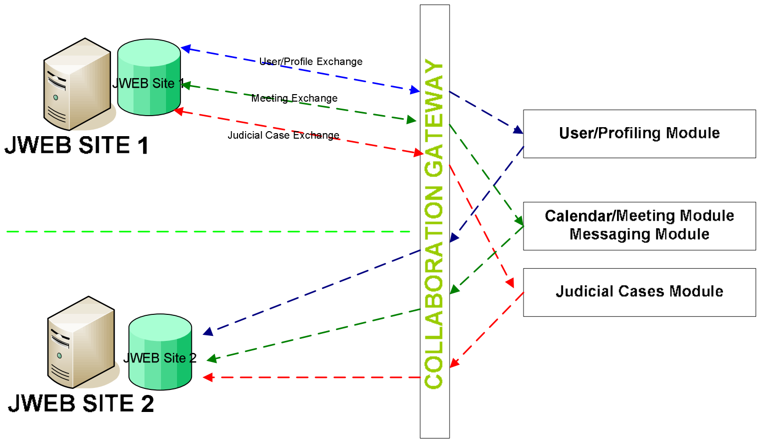

Fig. 5. The collaboration gateway architecture.

JCP access is protected by user authentication by means of his/her X.509v3[9] 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[10]), 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, is composed by the following components:

- Security Access Systems (Crypto-router). Crypto-routers prevent unauthorized intrusions, offers protection against external attacks and offer tunnelling capabilities and data encryption, providing both Network and Resources Authentication.
- S-VPN clients (Secure Virtual Private Network Client), through which the users 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 are 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.

[9] International Telecommunication Union http://www.itu.int/ITU-T/asn1/database/itu-t/x/x509/

[10] IPSEC working group at IETF http://www.ietf.org/html.charters/ipsecme-charter.html

Providing Network authentication is a key element for connecting JCP to the judicial systems without affecting the security of judicial network. External connections to the judicial systems are all managed by the JCP, connected to the judicial network via trusted links. JCP will potentially constitute the “last mile” connecting judicial actors inside the national judicial network with other actors and systems outside it.

4 Potential impact of ICT support to judicial cooperation

Judicial cooperation requests issued every year may vary from hundredths in smaller EU Member States to thousands in the more populated ones, both in terms of active and passive rogatories. Notwithstanding the relatively small number of criminal cases (a few percent or less) where judicial cooperation is requested compared with the overall number of criminal cases (an average in the EU of about 4800 criminal offences and 900 convicted persons each 100.000 inhabitants[11]), they are indispensable in most of the major investigations about organised crime, terrorist groups, illegal trafficking, relevant episodes of corruption and fraud, where relevant resources of the judicial organisations are spent and top investigating magistrates are engaged and where the support of the liaison magistrate or of Eurojust may be fundamental.

Electronic case management is demonstrating that a dramatic reduction of required time in many daily operations can be achieved through ICT support: a recent paper about UYAP[12] system in Turkey showed how the time required by simple operations such, as accessing to criminal records or transferring documents, decreased from an average of two weeks to few minutes. Similar data are available in most of EU countries.

Videoconference in courtrooms[13] is used in Italy and other countries since 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 early 2009. Usage of videoconference in compliance of 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, comparables with the ones achieved with case management systems. They are still difficult to be precisely quantified against the actual figures, due to limited existing statistics about. These e-services will make the link of the single investigation team with offices in charge of

[11] The European Sourcebook project, “European Sourcebook of Crime and Criminal Justice Statistics – 2006”, http://www.europeansourcebook.org/

[12] Ali Riza Cam “EU principles in modernisation of Justice and the Turkish IT project UYAP” , European Journal of ePractice · www.epracticejournal.eu Nº 3 · May 2008 · ISSN: 1988-625X

[13] Aki Hietanen “Videoconferencing in crossborder court proceedings” *www.ejustice2008.si/en/wp-content/uploads/2008/06/**videoconferencing**_in_crossborder_court_proceedings.ppt*

international cooperation, liaison magistrate and Ministry of foreigner affairs more effective, reducing the existing inefficiencies due mainly to complex procedures not supported by straightforward communication channels, shortening investigation times and contributing to the general reduction of time duration 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 Member State and in perspective connecting together different Member States. All in full respect of the requirements of security, non repudiation, confidentiality and strong authentication and 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 one in the smaller States, may be sufficient to manage the yearly issued or received requests and that the communication environment is the Web. Possible vulnerabilities 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 a 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 full deployment.

Judicial secure collaboration environment will be the basis for the future judicial 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 and on judicial ICT infrastructure 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 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, so giving further contributions to the Ministries of

Justice about the activities required for the full electronic management of activities in a delicate area such as the one of the international judicial cooperation.

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, 2005
5. European Commission. Security for judicial cooperation. In: 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
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, 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.