**COUNCIL OF
THE EUROPEAN UNION**

Brussels, 10 November 2005

**13558/1/05
REV 1**

LIMITE

DOCUMENT PARTIALLY
ACCESSIBLE TO THE PUBLIC

**CRIMORG 112
ENFOPOL 134
ENFOCUSTOM 59**

NOTE

From :	Presidency
To :	Multidisciplinary Group on Organised Crime/Article 36 Committee
No. prev. doc. :	10669/05 CRIMORG 62 CATS 38 ENFOPOL 82 ENFOCUSTOM 31
	13558/05 CRIMORG 112 ENFOPOL 134 ENFOCUSTOM 59
Subject :	Report by the Friends of the Presidency on the technical modalities to implement the principle of availability

1. The JHA Council in April 2005 agreed that "a first report on the technical modalities to implement the principle of availability on the six types of information [in the Presidency's Note] be presented to the Council by the end of 2005". The Article 36 Committee agreed subsequently that the Multidisciplinary Group on Organised crime (MDG) should oversee the production of this report.

2. To achieve this aim as efficiently as possible the Presidency established a Friends of the Presidency group made up of relevant experts from Member States along with the Commission, and representatives of Europol and Eurojust. The Friends of the Presidency group has now produced its report, which is attached to this note.

3. At the meeting of the MDG on organised crime on 8 November 2005 the report was in general welcomed by delegations. A substantial number of issues were raised by delegations with regard to possible ways to implement the principle of availability.

Many of the questions raised pertain to essential policy decisions concerning the overall approach the Council should take towards the principle of availability. These merit a substantial discussion. To this end, the Presidency intends to table a discussion paper for closer examination at the Article 36 Committee in December. The Presidency would also note that the report of the Friends of the Presidency would be translated into a greater number of EU languages by December so as to facilitate a broader discussion of its content at that meeting as well.

4. As delegations in the Multi-Disciplinary Group on organised crime have in general welcomed the report, the Presidency proposes that, pending the debate on the fundamental questions raised at the MDG meeting, the JHA Council on 1 and 2 December is invited to take note of the report, thus acknowledging the importance of the work accomplished by the Friends of Presidency.

The fact that the Council would take note of the report obviously does not imply that all delegations fully agree with its content. That the Council took note of the report would also in no way prejudice the discussion to be held at the December Article 36 Committee on the fundamental questions referred to above. It would simply allow at a procedural level for the fulfilment of the task set by the JHA Council in April 2005 (for "a first report on the technical modalities to implement the principle of availability on the six types of information [in the Presidency's Note] be presented to the Council by the end of 2005").

5. The Article 36 Committee is invited to agree on the procedural approach outlined above and to note that a fuller discussion that occur at the Article 36 Committee on 8 December 2005 concerning the principle of availability.

_____

Report of the Friends of the Presidency group on the technical modalities to implement the Principle of Availability

1. Introduction

1.1 The Hague Programme on strengthening freedom, security and justice in the European Union (EU) states that with effect from 1 January 2008 the exchange of law-enforcement information should be governed by the principle of availability, which means that throughout the Union a law enforcement officer in one Member State who needs information in order to perform his duties should be able to obtain this information from another Member State, and that the law enforcement agency in the other Member State which holds this information will make it available for the stated purpose, taking into account the requirements of any ongoing investigations in that State.

1.2 At the JHA Council on 14 April 2005 it was agreed that a first report on the technical modalities available for implementing the principle of availability would be presented to the Council by the end of 2005. It was decided that the report should focus on six areas of information– DNA; fingerprints; ballistics; vehicle registrations; telephone numbers; and minimum data for the identification of persons [contained in civil registers].

1.3 Under the oversight of the Multidisciplinary Group on organised crime a Friends of the Presidency group was established made up of relevant experts from Member States, the Commission, Eurojust, Europol and Interpol to take this work forward. This report is the findings of that group.

1.4 The report represents the views of the experts participating in the Group acting in their independent professional capacity and it is recognised that the views expressed may not represent the positions of the Member States or institutions from which the experts derive. The findings seek to inform debate in the Council structure and do not in any way bind Member States.

2. Context

2.1 The report has been prepared against a backdrop of a series of initiatives, forthcoming or under way, that are seeking to implement the principle of availability. The Commission and Council Action Plan to implement the Hague Programme includes references to inter alia a Framework Decision on simplifying the exchange of information between the law enforcement authorities of the EU as well as Commission legislative proposals on the establishment of the principle of availability and on adequate safeguards and effective legal remedies for the transfer of personal data for the purpose of police and judicial co-operation in criminal matters.

2.2 In addition, Germany, Austria, France, Belgium, Luxembourg, the Netherlands and Spain signed the Prüm Treaty on 27 May 2005. The Treaty seeks to strengthen cross-border co-operation in particular to combat terrorism, cross-border crime and illegal immigration. The Treaty includes provisions for the exchange of DNA, fingerprints and vehicle registrations. Albeit not an EU-instrument, the Treaty will contribute to the options for implementing the principle of availability.

3. Information Exchange

3.1 The ability to exchange accurate information quickly and efficiently is essential to effective international co-operation in combating crime. Exchange mechanisms must look beyond the confines of Europe as crime is a global phenomenon. This report has therefore included reference to Interpol and the services which can be offered in this respect taking into account that EU Member States are also Interpol member countries.

3.2 Much international data exchange continues (depending on the type of data to be exchanged) to take place within the EU via the classic "police-to-police" approach of indirect access to information upon request or through using mutual legal assistance (MLA) channels. Various channels of communication for such indirect exchanges exist, including via the national Interpol, Europol or SIRENE national units or bureaux, or via the bilateral liaison officers network. The Framework Decision on simplifying the exchange of information between the law enforcement authorities of the EU will, once adopted, improve the efficiency of such exchanges by requiring certain information to be made available spontaneously or on request to law enforcement authorities in other Member States with a minimum of formality and will specify timeframes and short deadlines for urgent cases. In addition work could be undertaken to minimise the potential for overlap and duplication of effort at the national level (in particular between Interpol, Europol and Sirene national units/bureaux). The efficiency of these entities could be improved by ensuring that the national units for each of these possible channels are housed in the same agency, in the same location and under the same management and Government Ministry (or in the same virtual surroundings). Where internationally agreed service standards exist, these should be followed and may provide a mechanism for improving response times. In undertaking such reforms it will be important to consider the different competencies and responsibilities of police and judicial authorities in the Member States and to bear in mind data protection concerns.

3.3 However, in commissioning the report the JHA Council identified a number of other possible modalities for implementing the principle of availability. These are:

(a)   direct access to the databases of another Member State;
(b)   indirect access to information of another Member State through a central index on a hit-no-hit basis;
(c)   the creation or extended use of central European and international databases; and
(d)   enhanced access to police data rendered public by Member States' law enforcement authorities.

3.4 A detailed explanation of what is understood by each of the modalities is attached at Annex A. However, it should be emphasised that, in terms of creating new databases, the Hague Programme states that "new centralised European databases should only be created on the basis of studies that have shown their added value". It should further be emphasised that technical modalities for implementing the principle of availability will rely heavily on information technology. There is a need to ensure that the solutions devised consider present or future demands on interoperability and integration, and, given business development in the field of law enforcement is rapid and not always foreseen, enable and do not constrain future expansion and modification. This reinforces the need, as stated in 3.1(k) of the Hague Programme for a coherent approach to the development of information technology to support the collection, storage, processing, analysis and exchange of information. Some good practice guidelines are included in the report at Annex B.

3.5 The following sections of the report consider in detail how information exchange for each of the data areas could be improved and value added to law enforcement, either by enhancing the efficiency of the existing mechanisms or by adopting alternative modalities. There are generic advantages and disadvantages to the different modalities, but the applicable approach will also depend and must be proportional to the law enforcement need and the sensitivity of the data. The effectiveness of existing practices and the need for reform will be vital in informing the potential added value to be derived from structural reform, and close consideration is therefore warranted of information exchange in each of the data areas. The report thus considers each of the data areas separately. However the objective is the same – to establish business processes which can facilitate the quick, efficient and cost-effective means for exchanging data. These processes must be accountable and incorporate good practices in the sharing of data, such as appropriate safeguards to ensure the accuracy of data and the security of data (both during transmission and its subsequent retention), management procedures to log and record data exchanges, and limitations imposed on the use of exchanged information.

DELETED FROM THIS POINT TO PAGE 42 INCLUDED

ANNEX A

Definitions of the Modalities

i. Indirect access to information upon request.

Member state A must ask a contact point in member state B to advise, on their behalf, as to whether they hold or have access to specified information (on a database if appropriate). Member state B's contact point conducts a search on the database or causes a search to be conducted and is able to give a response. This may be transmitted through mutual legal assistance or a simplified procedure.

ii. Direct access to databases of another member state.

This requires the creation of a search engine / search request network.

Member state A, using a computer terminal in his/her own state, either enters and sends a search to a database which is held in member state B or sends a single search request to a central searching facility in order to search the databases of several Member states. The result is automatically returned without further human input. The result may be:

> a. "hit/no hit". A bilateral follow up will be required for any hit OR
> b. the return of data from certain data fields (fields to be determined by Member state B). A bilateral follow-up is required for any further information) OR
> c. the return of a complete set of data and no bilateral follow up will be required.

The range of choice available in terms of "a", "b" or "c" will depend on the I.T. arrangements and data sharing agreements and the law governing the database and privacy rights in country B.

Direct access to the databases of another member state may be restricted to a national contact point or may be permitted for appropriate competent law enforcement authorities.

Where direct access is on a hit / no hit basis, or where only a selected range of data is automatically supplied, follow-up will be via mutual legal assistance or a simplified procedure.

iii. Access to information of another member state through a central index on a "hit/no hit" basis.

This requires the creation and maintenance of a central index populated with a limited range of data from member states. This index would require Member states to possess their own databases to feed the central index.

Member State A, using a computer terminal in his/her own state, enters and sends a search to the central index. The central index will query the data held on the index. The central index will then respond automatically stating:

> a. no match or
> b. that a possible match exists in Member State X.

Possible matches will be pursued through mutual legal assistance or a simplified procedure.

iv. The creation and extended use of central European and international databases.

This option requires the creation of central European and international databases.

This option also anticipates the existence of such databases and considers extending their use.

Access to these databases may be "direct" or "indirect".

If <u>direct</u>, member state A, using a computer terminal in his/her own state, enters and sends a search to the central European or international database. The result is automatically returned without further human input. The direct access to such databases may be restricted to a national contact point (such as the Interpol National Central Bureau) or may be permitted for appropriate competent law enforcement authorities.

If <u>indirect</u>, member state A must ask a contact point at the central / international entity holding the database who could search the database on their behalf.

<u>The applicable approach will depend on the availability and access regime to the database.</u>

A response will be provided. This may be:

     a. "hit/no hit". A bilateral follow up will be required for any hit OR
     b. the return of data from certain data fields (fields to be determined by the data owner). A
     bilateral follow-up is required for any further information) OR
     c. the return of a complete set of data and no bilateral follow up will be required.

Again, the availability-of "a", "b" or "c" will depend on the I.T. arrangements and data sharing agreements and the law governing the database and privacy rights.

<u>Where direct access is on a hit / no hit basis, or where only a selected range of data is automatically supplied, follow-up will be via</u> mutual legal assistance or a simplified procedure.

v. Enhanced access to police data rendered public by member state's law enforcement authorities.

The precondition is that law enforcement information has been made public and is available for consultation without further reference to any law enforcement agency in the state where the data is held or by whom it is owned. It may be presumed that the internet would be used for such consultation.

ANNEX B

Friends of the Presidency Group on the technical modalities to implement the principle of availability

Definition of a policy for a coherent approach on the development of information technology to support the collection, storage, processing, analysis and exchange of information

Following a recommendation of the Article 36 Committee at its meeting on 7-8 November 2002, an ad hoc expert group was set up to make an inventory and an evaluation of the existing and planned information systems in the fields of law enforcement and judicial co-operation with a view to identify possible overlaps and/or gaps.

Part of the background to the setting-up of the group was that it was felt that there was a lack of overview on information technology systems and their development. A report of the ad hoc group was presented at the meeting of the Article 36 Committee on 3 October 2003 (8857/03, JAI 118). The report provides an overview of existing communication networks and databases.

The ad hoc expert group came to the conclusion that overlaps and gaps may exist as regards user population, data stored or exchanged through the system, and purpose/objective of the system. For the long term future of law enforcement systems, the Article 36 Committee expressed its support for the so called middle ground solution: "To investigate and implement the harmonisation of data formats and their respective access rule between the various systems while allowing current systems to evolve to provide interoperability".

In May 2004, An Garda Siochana, organised an AGIS seminar in Dublin on Police IT Co-operation in an Enlarged EU. Conclusions and key findings of the seminar include:

o "The effectiveness of strategies to combat global terrorism and organized crime rely heavily on information technology. Currently no forum exists for law enforcement Heads of Information Technology [development] to meet, to share experiences and discuss best practice. Informal communication between Police Heads of Information Technology in the European Union is dependent on personal contacts. Improved co-operation through such a forum can only result in more effective law enforcement. Utilizing the knowledge and expertise of a broad expertise would undoubtedly improve the quality and cost effectiveness of IT systems."

o "The idea of a central catalogue of both law enforcement systems and law enforcement IT experts was seen…as a relatively simple idea that could be of enormous value and consequently an idea that should be progressed promptly. In particular a catalogue of contacts was seen as facilitating ease of communication and a catalogue of systems and technologies would among other things, short circuit the research process. Ownership and funding of this particular finding will be necessary to ensure that it is not just set up, but updated very regularly to ensure its usefulness."

o "Effective sharing of technical information by law enforcement agencies is hampered by the absence of common or converging technical standards for Law Enforcement information systems across the EU. While best practice in Information Technology exists in many individual EU countries, significant benefits can be achieved through a process enabling the transmission of and sharing of such practices. Valuable sources of technical expertise are going to waste if there is no forum to share expertise and best

practice on a regular basis. Best practice has identified that IT needs to be acknowledged and resourced as a primary enabler in the fight against terrorism and organized crime both nationally and internationally."

Since the study of the ad hoc group on the third pillar information systems and the initiative of An Garda Siochana, work at EU-level on developing IT systems for law enforcement purposes has continued. Experience shows that the development has been quite a challenge and work currently under way has encountered many difficulties causing unnecessary costs and delays, e.g. SIS II and Europol Information System (EIS). For instance, the development of EIS led to significant, unnecessary costs both for Europol and the Member States. At the national level nothing or very little of the results of the EIS implementation preparations can be reused for the implementation of the new Europol IS and the new system offers less functionality than its predecessor would have done. Current problems (delays) in SIS II and FADO can be explained partly by the arrangements for interaction between roleplayers and by the sequence of work. The management of security issues and accreditation of the systems differ between all three of them, apparently for organisational reasons. Furthermore, and most important, all systems implemented up to now, including ongoing projects for SIS II, FADO and Europol IS, have been developed for specific purposes without any considerations on present or future demands on interoperability and integration. Since business development in the field of international law enforcement information exchange is very fast and not always foreseeable, solutions must be made easy to expand and to modify.

Recommendations

- **Short term:**
    o Representatives of the law enforcement business- and IT-development departments or the equivalent in the Member States should meet within an existing forum (is such a forum exists), or where this is not possible a new forum should be established, to ensure the application of recommended guidelines and to work towards an overall improvement and coherence of EU IT-development to support law enforcement co-operation.
    o The ad hoc study on the third pillar information systems is updated and developed in accordance with the recommended guidelines in order to provide the necessary basis for an improved IT-development to support law enforcement co-operation.

- **Long term:** For the long-term development of law enforcement IT systems at EU-level a set of common guidelines to steer the work towards a coherent approach is proposed. Such guidelines would provide the basic elements for the definition of a policy for a coherent approach on the development of information technology to support the collection, storage, processing, analysis and exchange of information as called for by the Action Plan to implement the Hague Programme.

    o *Guideline 1: Assessment of the added value, the needs, the usefulness and the requirements of the law enforcement community on information technology*

        This guideline reflects the Hague Programme itself as it sets out the requirement for an assessment of the added value before new databases are established at EU-level. An assessment of the added value must include the perspective of law enforcement work and working methods. What are the needs and requirements of the law enforcement co-operation (including for instance intelligence requirements as

included in a European Criminal Intelligence Model)? How will the IT-solutions be used and how useful will it be for enhancing the capacity of law enforcement co-operation?

The application of this guideline will lead to a methodologically sound sequence of work. The IT-development will be based on and driven by the needs and requirements of law enforcement co-operation and an assessment of the usefulness of developments will help to set priorities for the work on IT to support the implementation of the principle of availability. In other words, IT-developments or technical improvements of existing systems will be made only after the law enforcement needs, requirements, and usefulness have been assessed, documented an decided upon.

o *Guideline 2: IT systems to support agreed law enforcement workflows, intelligence models and intelligence requirements*

This guideline means that the use of IT shall support the workflows of the international law enforcement co-operation. These flows must therefore be described, known and accessible. They should be an integral part when systems are developed and procurement is taking place.

The application of this guideline will provide well described processes and work flows. It will be easier to understand and change the workflows and the handling information and information flows will be more efficient. Furthermore, there will be a better management and documentation of the IT-development and the needs of international law enforcement co-operation will guide the IT development.

o *Guideline 3: A coherent, service oriented (SOA) EU-architecture for law enforcement IT*

Principles for IT-architecture provide a basis for decision-making on IT-development and play a key role in achieving required results and functions for law enforcement co-operation. More coherence in the IT-architecture provides for instance lesser costs in the long run, improved technical standards, increased opportunities for interoperability, and improved functionality throughout the portfolio of IT functions. Experiences from large organisations show that testing an IT-development project against a set of principles of a coherent IT-architecture helps in achieving this. Broadly agreed best practices of a coherent IT-architecture include at least:

a) the use of system quality attributes such as scalability and modifiability;
b) using the financial benefits of eliminating repetition, incompatibility and unnecessary redundancy;
c) incorporating standards that provide open systems, seamless integration, and that establish an overarching perspective for the organisation;
d) promoting the integration of services, programs, data and networks throughout the organisation;
e) providing assistance for a stable development by identifying techniques that work together in order to satisfy the needs and requirements of the end users in the law enforcement services;
f) securing possibilities for co-operation within and outside the law enforcement services;

g) enabling the implementation of changes with a minimum of disruptions in the law enforcement work;

h) ensuring activities and solutions that stop external penetration (security);

i) promoting electronic alliances between external and internal partners.

Consequently, the application of this guideline will assist in assessing whether an IT-development project is on the right track and if it fits in to the portfolio of IT functions. Furthermore, it contributes to new developments, management and reutilisation. The co-existence of and co-operation between systems will be facilitated and it reduces the costs in the long run by making easier rational and strategic decisions to invest in IT-development.

o *Guideline 4: Do not re-invent the wheel*

This guideline means that the priority for IT-development and technical improvement is re-utilisation. It helps to avoid parallel systems and to further develop existing systems, their integration and usefulness. It requires the existence of a system map, providing an overview of the existing systems, functions and components, i.e. a development of the ad-hoc study on the third pillar information systems.

The application of this guideline will lead to increased use of already made investments and a lesser need for new investments. Reutilised components will be independent of the technical platform and the implementation of commercial components will be simplified. Furthermore, the quality of reutilised components will increase the more they are used. The time necessary for IT-development will also decrease the more components are at hand.

o *Guideline 5: Assessment of the legal requirements and security standards for law enforcement information technology*

This guideline means that correct information shall be available to authorised users in a traceable way when there is a need. Furthermore, it means that adequate data protection regimes are developed for different types of information in the implementation of the principle of availability. It also means that the right levels of security standards are ensured for EU IT-systems.

The application of this guideline will ensure an adequate level of data protection and security standards.

o *Guideline 6: Interoperability and co-ordination between IT-systems at EU-level to support the requirements of law enforcement co-operation*

This guideline means that the IT-systems and their components shall comply with defined standards and principles that support interoperability and co-ordination between systems and exchange of information. It requires a system map (the systems and their components are known) as well as a chart of law enforcement information flows. The guideline also means that the existing systems and their components will form an integral part of the process to develop new systems.

The application of this guideline will lead to better and increased use of existing IT systems. It will contribute to a development where the IT-systems can support work processes in more stages. The need for double storage and double registration will decrease. The proposed update and development of the ad hoc study of the third pillar information systems forms an integral part of this guideline.

o *Guideline 7: Standard technical solutions for EU law enforcement IT*

This guideline means that the IT-development shall be based on industrial standards and by the market accepted de-facto standards and best practices, including a well defined standard for communication between access points (contact points being also technical "integration points"). It requires that used standards are included in a system map with information on where the standard can be found (procured). Again, the proposed update and development of the ad hoc study on third pillar information systems would be an integral part in fulfilling this guideline.

The application of this guideline will provide coherence in the development and management of the IT-systems. By applying standards, the law enforcement co-operation can be supported by several suppliers and not only one supplier. The guideline will make IT-development and management easier since a well defined standard for communication between access points in the Member States will be used. In the long run it will decrease the cost for adaptation in the Member States.

o *Guideline 8: A limited number of technical solutions for EU law enforcement IT*

This guideline means that the number of redundant technologies, products and versions shall be limited in order to simplify the IT-development and management. It requires a system map including technologies, products and services. However, the guideline shall not hinder opportunities for modernisation or renewal of information technology.

The application of this guideline will simplify the IT-development and management. It will contribute to integration and co-ordination between the IT-systems.

o *Guideline 9: MS law enforcement authorities responsible for implementation (business and IT) to be involved from the very initial stage of the process to develop EU law enforcement IT*

This guideline means that the fully functional end result is put at the forefront of IT-development to support law enforcement co-operation. It requires that those responsible for the national implementation are involved at an early stage of the process and that a dedicated forum is set up for this purpose.

The application of this guideline will ensure the reciprocity or interaction between the EU-level and national level that must guide the IT-development in order to improve it and to prevent problems before they occur. It will also ensure a better prepared and smoother implementation process in the Member States.

o *Guideline 10: Clear division of responsibility for each part of the process to develop EU law enforcement IT*

This guideline connects to guideline nine and seeks to clarify the roles of those actors involved in IT-development in order to better gear and steer the process. This includes the need for the established forum to have an agreed mandate. The procurement process and technical specifications are examples on issues that would benefit from an increased clarity in this respect.

The application of this guideline will, as is the case with guideline nine, ensure the reciprocity or interaction between the EU-level and national level in implementing IT-developments.

Through the entire development (or procurement) process the application of these guidelines or principles must be ensured by the use of well-known, business oriented methodologies for system development, including project management, governance and documentation.