COUNCIL OF THE EUROPEAN UNION

Brussels, 10 November 2005

13558/1/05 REV 1

LIMITE

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.

4. DNA

4.1 <u>The Current Practices and Initiatives</u>

- DNA is an important tool to law enforcement which has transformed the fight against crime by providing invaluable information that can connect individuals to crime scenes and identify links between crimes. It has helped detect thousands of repeat criminals and equally importantly provided information that has helped to quickly eliminate innocent suspects. In addition to being of vital evidential value DNA samples have significant value at the investigatory state of an enquiry, allowing police to speed up detections and make earlier arrests. It has also helped police conclude long outstanding unsolved crimes and is increasingly being used in some Member States as an intelligence tool to establish patterns of offending well beyond the investigation of individual cases. The chances of solving criminal cases are considerably increased since DNA profiles from scenes of crime, from offenders, unidentified corpses or missing persons from any country can be compared with those of others world wide. The extension of the comparison of DNA profiles from domestic to multilateral searching of international databases is an important way to realise the potential of DNA technology and strengthen the effectiveness of the fight against organised crime and terrorism, and to consolidate the area of freedom, security and justice.

- The Council Resolution of 9 June 1997 on the exchange of DNA analysis results invited Member States to consider establishing DNA databases and to construct such databases using the same standards and in a compatible manner with a view to facilitating the exchange of DNA analysis results. The Council recognised that such a system for information exchange would need to offer sufficient safeguards for the security and protection of personal data. [i]

- The majority of Member States now have DNA Databases and consider a DNA database to be an important and efficient tool in tackling crime.[ii] All Member States which have DNA databases have the capability to compare a profile from another Member State to their own database and vice versa. This can be done on a case by case basis. However, the request for such an exchange currently needs to be made via existing communication channels such as Interpol, Europol, Article 39 of the Schengen Convention or via the bilateral liaison officers network. In some Member States the use of mutual legal assistance provisions is required. Exchange of data via Interpol's National Central Bureaux is the main transmission channel and this is done using the Interpol standardised DNA profile transmission form. Data is then transmitted electronically. This approach was specifically encouraged by the Council Resolution of 25 June 2001 on the exchange of DNA analysis results.[iii] Transmission of personal information linked to the profile may only occur with the consent of the country which "owns" the data and Mutual Legal Assistance provisions will be required for some countries.

- In order to share DNA data, Interpol has also developed a criminal intelligence DNA Database to provide the opportunity to link individuals to unsolved crimes committed in other countries and to identify crimes that have been committed by the same person in different countries. The Interpol DNA Database (with basic matching tools and using seven common DNA markers) has been in use since 2003. It currently contains 14376 DNA profiles from 32 different countries (of which 2044 are from EU states) and is being upgraded with new matching routines and nationally specified filters. Testing of this system by 12 countries is underway and an online version of the system should be available soon. Member States and other European countries have been asked to send DNA profiles from unsolved offences to the Interpol DNA database for searching.

- However, while procedures for exchanging DNA data are already in place, law enforcement authorities have noted that current procedures can be time consuming, and since many involve manual input of data these can also be subject to error. The manual processes are resource intensive and there have been occasions where investigative leads have been missed. The sharing of this information is still based on a "send and wait" system. Benefits are not being fully realised due to outmoded approaches to data sharing and a lack of rigorous business processes. For a lot of states mutual legal assistance is required, yet in some states a public prosecutor will not be involved at an early stage of an investigation, when knowledge of a match in another state may be of significant assistance.

- Initiatives are already underway which if implemented may address some of these deficiencies:

(i) The Commission is preparing a proposal for a Council Decision on automated comparison of DNA profiles. This will be forwarded to the Council before the end of 2005 in line with the Hague Action Plan and will accompany the draft Framework Decision on the exchange of information under the principle of availability. Signatories to the Prüm Treaty are committed to sharing DNA profiles via direct access to the national databases of the participating Member States through a national contact point on a hit/no hit basis. A technical mechanism by which the databases of participating countries might be joined up is currently being developed, and this is likely to provide a substantial improvement in the exchange of DNA data.

(ii) The Commission has agreed to fund an AGIS project that aims to to test the feasibility of a search engine as a possible cost effective solution for meeting 'The Hague Programme' objective of improving exchange of information by mutual access to or interoperability of national DNA databases, (Reference 13993/04 JAI 408 - "strengthening freedom, security and justice in the European Union"). This is an objective that meets Member States' privacy and other legal restrictions and which will also enhance domestic data capability for the same investment.

4.2 The Future – options for enhancing information exchange

With the current approach being a mix between **indirect access to information upon request** (mutual legal assistance), and the use of an **International Database** (Interpol), and taking into account the various initiatives under way, the Friends of the Presidency group has considered a variety of options in order to improve the exchange of DNA data:

(i) indirect access to information upon request

This is the current approach. Improvements could be achieved via an arrangement between the authority in a Member State which is the guardian of DNA profiles and its National Central Bureau of Interpol, or other national contact points for existing communication channels, to ensure that there is an effective chain for the transmission and receipt of DNA profiles. There would also have to be an effective mechanism for obtaining the result of DNA profile comparisons and transmitting these to the originator of any request. Adoption of the Interpol standardised form for the transmission of DNA would be an important step to ensure that errors associated with the manual recording of DNA data are reduced. 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 and will specify timescales.

Advantages	**Disadvantages**
• Application of common standards will reduce the numbers of errors. • Application of the Framework Decision should simplify procedures and ensure more efficient and expedient exchange. • Avoid cost of creating central applications. • Closer and individual consideration can be give to differences in legislation and ensuring the safeguarding of the rights of individuals.	• Still based on a "send and wait" system. • Not real time searching • Resource intensive and burden will rest with requested state. • Dependent on request being promptly actioned in another Member State. • Dependent on existing intelligence to target search. • Time consuming.

(ii) Direct access to the databases of another Member State

Direct access could be achieved through a search request network / search engine which would establish an international network of national DNA Registers. This would require clearly defined and universally accepted scientific standards underpinned by rigorous quality assurance; secure and cost effective data transmission and searching and safeguards for civil rights and compliance with privacy laws. This possibility is already being investigated; advice has been received about the technical feasibility of such a system, and funding is now available from the European Commission to pilot test such an arrangement.

Advantages	**Disadvantages**
• Efficient – timeliness and quality of search should be as good as for a national search • Real time searching • No human input required from the requested state • Avoid need for participating states to download its data to another database or index • Avoid large overheads of constructing a central application – has the potential to therefore start with a few members. • Can be locally driven. • Such arrangements are well established in other areas requiring the sharing of data without compromising the data owners' control/security (e.g. bank central clearing systems). • Possibility of collaboration outside of EU – in particular with the US and with Canada.	• Adaptations are required to the national systems and regulations in order to make it possible for other states to have access • Requires clearly defined and universally accepted scientific standards underpinned by rigorous quality assurance; secure and cost effective data transmission and searching safeguards for civil rights and compliance with privacy laws • Adequate safeguards necessary if sovereign control of database is not to be compromised • Solutions will need to be devised to prevent the need to re-search periodically for searches which do not generate a match • No cold hit capacity (i.e. the ability to obtain an unexpected match without prior information). • If data is not visual or numeric, translations tools will need to be incorporated into the network, or data will have to start being stored in common languages. • It is also 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.

The Prüm Treaty provides for a variation of direct access by granting direct access to a part of the national DNA databases of participating Member States through a national contact point on a hit-no-hit basis. Exchange of DNA data under this system is expected to be governed by Interpol standards, and is safeguarded by the relevant data protection measures. Rather than using Mutual Legal Assistance to check records in all 25 Member States, the Prüm approach will allow the requesting State to know (via an automated search) which of the signatory Member States actually has the data required, through granting direct access to the DNA profiles on code (hit / no hit). Once a hit has been identified, the personal information or the information belonging to the criminal case can be obtained through existing communication channels including Mutual Legal Assistance provisions where required.

(iii) Access to information of another Member State through a central index on a hit-no-hit basis

An alternative option would be to create a central index populated with a limited range of data (the profile and an identifying reference code). The central index could be searched and would be able to identify a possible match and provide a reference to obtain that profile. The actual data could then be obtained through existing communication channels

Advantages	**Disadvantages**
• Algorithms for optimal matching of DNA profiles of various standards could be established centrally. • The development work would be relatively light compared to establishing a central database. • Would be independent of local choice of implementation technology – providing they can communicate via a web service. • Sovereign control over data since only selected data will be shared	• Require existence of national DNA databases able and willing to expose their services through a web service. • Complex to establish what the standard for the central application should be. • Procedures would need to be established for downloading data from the national databases to the central index – ideally these should foresee frequent, automatic updates. • Dependent on countries populating the index • Matches, hit/no/hit, reported on limited data therefore increased follow up of individual enquiries • Difficult to distinguish what limited data would be stored on this database – if DNA profiles are stored this index might resemble a central database

(iv) The creation or extended use of central European and international databases

A central database already exists at Interpol. One option would be to develop this database further.

Advantages	**Disadvantages**
• Already in existence – useful stop gap even if not long term preferred option. • Little need for local implementation work apart from providing access to data. • Avoids need to harmonise varied information systems. • A central application provides an option for central governance and validation of searches. • Filters can be provided in central databases to restrict countries that can access each depositing state's data. • Useful repository for unidentified crime stains and the ability to offer the added value of trend analysis.	• Some countries would not be able to provide data to a central database because of civil rights legislation. • Would involve the overhead of maintaining the data both nationally and centrally. • There is a danger that data in central databases may be out of date compared with national databases. • National sovereign control of data is shared with third external party • Common language and data format required. This may require either a conversion tool during uploading or manual conversion and inputting of data.

(v) Enhanced access to police data rendered public by Member States' law enforcement authorities.

This modality is not applicable in the case of DNA data.

4.3 Recommendations

- Continued use should be made of the existing mechanisms for DNA exchange and **use of the Interpol database, where possible within national law, should be strongly encouraged**. Efforts should be made to improve the efficiency of existing channels of transmission.

- The Friends of the Presidency Group welcomes the efforts made to establish a technical solution aimed at facilitating direct access from a national contact point to certain Member States' DNA databases on a hit/no-hit basis (as set out in the Prüm Treaty). Other Member States should be kept informed of progress in this area, and should consider the practicalities of joining their own DNA databases to the system that is being developed.

- The Interpol Database and work as a result of the Prüm Treaty are seen as complementary work streams that should with others lay down the foundations on which we can build our future direction/strategy

- In light of the experiences of implementing direct access by signatories to the Prüm treaty, the long term objective should be to investigate further the possibilities of enhancing the mechanism foreseen by the Prüm Treaty, if possible increasing the number of participating countries (including non-EU states) and possibly allowing direct access to national DNA databases via a search engine / search request network. The Interpol database should be included as one of the databases linked by the search request network to reach out to the majority of its member countries who do not have and / or will not have any prospect of having their own DNA capability. The inclusion of the Interpol database in any DNA identification process, where possible, using the Interpol I-24/7 communications network for access would provide all participant countries with a cold hit capacity (i.e. the ability to obtain an unexpected match without prior information).The combined search engine linking states with DNA capability and including Interpol facility on behalf of states without their own capability would therefore provide:

  (i) global cover:
  (ii) a cold hit capacity;
  (iii) the most effective means for engaging EU and non-EU countries; and
  (iv) the most time efficient method of comparing DNA data. .

The network would require clearly defined and universally accepted scientific standards underpinned by rigorous quality assurance (QA); secure and cost effective data transmission and searching and safeguards for civil rights and compliance with privacy laws. The system should be designed to allow for continuous improvement in DNA data exchange and to allow Member States to pursue enhanced co-operation should they see fit, always ensuring that the necessary safeguards are put in place regarding data protection and criminal procedural law.

5. Fingerprints

5.1 The Current Practice and Initiatives

- Confirmation of the identity of an individual is a very important aspect of any criminal investigation process. The standard format for this is the use of "10 print" records which record the impressions of each finger. Equally, the ability to transmit and compare individual fingerprints which have been taken from crime scenes is of vital importance to investigators. Member States use a variety of Automated Fingerprint Identification Systems (AFIS) and manual systems for processing fingerprint data. Human input may be required to confirm a match on an AFIS system.

- Fingerprints are already exchanged between Member States on a regular basis upon request. The most popular route for such requests is via the Interpol National Central Bureaux, though in certain Member States mutual legal assistance provisions are required. Various channels for the transmission exist including Interpol's Virtual Private Network, the I-24/7 system, and also SISNET via means of the SIRPIT messages.[iv] A common standard (INT-I), recognised by several Member States, exists for fingerprint data which is based on the current version ANSI/NIST-ITL 1-2000. However, it is not clear the extent to which this standard is being implemented.[v]

- In addition to the transmission facility provided by the I-24/7 system, Interpol also maintains a central database. Not all fingerprints transmitted via the I-24/7 system are stored on this database, but as a result of significant efforts made in 2004[vi], aided by the increased visibility delivered by the I-24/7 system, the number of samples on the database has risen to 44606.[vii] An expanded database has resulted in an increase in the number of identifications and confirmations of identity.

- A number of bilateral arrangements also exist which provide for enhanced access between specific Member States. Denmark, Finland, Sweden and Norway for instance, utilise an electronic exchange system which permits the rapid exchange of fingerprints upon request. The system uses the "Fingerprint Image Transmission" (FIT) software.

- FIT technology allows for high quality fingerprints to be rapidly checked against other AFIS databases. Fingerprints transmitted using this software can be transferred directly into the national AFIS systems of the receiving country by an operator in the requested state. Any matches generated or results from the search can then be transmitted to the requesting party via the FIT mail system. To function effectively FIT requires: the existence of an AFIS database in the requested state; appropriate software to interface the FIT station with the AFIS system; a secure channel for electronic transmission (such as the Interpol I-24/7 system or SISNET); and the application of common approved standards (such as ANSI/NIST-ITL 1-2000). FIT has the potential to be applied to all the various European AFIS systems and meets the strictest of international standards including those applied by Interpol and the FBI. It had already been purchased by a number of other Member States and is being utilised for immigration and domestic law enforcement purposes. It is also used by the European Commission within the scope of the EURODAC system for processing asylum applications.

- However, it is clear that, while procedures for exchanging fingerprint data are already in place, the exchange of fingerprints does not take place in every case where a Member State is dealing with a criminal process involving a national of another Member State or third country. This means that potential investigative leads are being missed. Fingerprint databases are also held in Member States by non-law enforcement authorities and for other purposes, and whilst access regimes to these databases vary, the potential exists of a significant resource for law enforcement. With the introduction of biometric passports additional databases to store fingerprints and other biometric data will develop and expand this potential further.[viii] The ability to confirm the identity of an individual as well as determining whether they are criminally known is an important part of any criminal investigation process.[ix]

- In practice law enforcement authorities have noted that the current procedures for exchanging fingerprint data can be time consuming, subject to error and resource intensive. Requests for information have not always been actioned in a timely manner. The sharing of this information is still based on a "send and wait" system. Benefits are not being fully realised due to outmoded approaches to data sharing and lack of rigorous business processes.

- In an attempt to reduce the number of potential investigative leads being missed, the Salzburg Forum (Hungary, Austria, Czech Republic, Poland Slovenia and Slovakia) adopted a joint declaration in November 2004 on the functional extension of the EURODAC, the central fingerprint index currently used to record asylum applicants prints, into the domains of police co-operation and of alien policing. Under their proposal fingerprints of individuals convicted of serious crimes would be entered onto the EURODAC index. Member State law enforcement authorities, as well as Europol and Eurojust, would be able to query the database in carrying out criminal investigations. In this regard the Commission will be producing a Communication on interoperability of EU databases in October 2005, and has recently issued a discussion paper (DG JLS/D1/SW(2005)) detailing the differences between centralised and decentralised sharing of fingerprints.

- Other initiatives are also underway. The Prüm Treaty provides for direct access to the national fingerprint databases of the participating Member States through a national contact point on a hit/no hit basis. A technical mechanism by which this might take place is in the process of being worked up. Once a technical solution has been found to join up the databases of participating countries the treaty is likely to provide a substantial improvement in the exchange of fingerprint data.

5.2 <u>The Future – options for enhancing information exchange</u>

The current model for fingerprint data exchange between Member States (except for the existence of a small central database at Interpol and in a few instances where separate bilateral arrangements exist) is currently one of **indirect access to information upon request**. The Friends of the Presidency group has considered a variety of options in order to improve the exchange of fingerprint data:

i. Indirect access to information upon request.

This is the current approach. There is some scope for improving the functioning of this modality. Implementation of SIS 2 for example, which is underway, should provide improvements and more efficient processes for sharing data (although it is not planned at the moment for Member States to search on the basis of the fingerprints). A more efficient approach could also be achieved via an arrangement between the authority in a Member State which is the guardian of the fingerprint records and its National Central Bureau of Interpol, or other national contact points for existing communication channels, to ensure that there is an effective chain for the transmission and receipt of prints. There would also have to be an effective mechanism for obtaining the result of fingerprint comparisons and transmitting these to the originator of any request. Access to the national AFIS systems (for transmission and not comparison) within the Interpol National Central Bureaux or other national contact points would assist this approach, as would the application of common agreed standards. 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 and will specify timescales

The utilisation of such software as FIT would also assist in facilitating the rapid exchange of high quality fingerprint data electronically. Such technology requires Member States to possess their own AFIS systems with appropriate software to interface with FIT and to apply common agreed standards for its potential to be fully realised.

Advantages	**Disadvantages**
• Application of common standards will reduce the numbers of errors • Use of software such as FIT would improve the speed at which high quality fingerprints could be exchanged • The cost of creating central applications would be avoided. • Closer and individual consideration can be give to differences in legislation and ensuring the safeguarding of the rights of individuals.	• Still based on a "send and wait" system • Not real time searching • Resource intensive and burden will rest with requested state • Dependent on request being promptly actioned in another Member State • Dependent on existing intelligence to target search • Time consuming

ii. Direct access to the databases of another Member State

Direct access could be achieved through a search request network / search engine which would establish an international network of national AFIS databases. This would require clearly defined and universally accepted scientific standards underpinned by rigorous quality assurance; secure and cost effective data transmission and searching and safeguards for civil rights and compliance with privacy laws.

Advantages	**Disadvantages**
• Efficient – timeliness and quality of search should be as good as for a national search. • Real time searching • Avoids need for participating states to download its data onto other databases or indexes. • Avoids large overheads of constructing a central application – has the potential to therefore start with a few members • Can be locally driven. • Such arrangements are well established in other areas requiring the sharing of data without compromising the data owners' control/security (e.g. bank central clearing systems) • Possibility of collaboration outside of EU – in particular with the US and with Canada.	• Adaptations are required to the national systems and regulations in order to make it possible for other states to have access. • Requires clearly defined and universally accepted scientific standards underpinned by rigorous quality assurance; secure and cost effective data transmission and searching safeguards for civil rights and compliance with privacy laws (if sovereign control of data is not to be compromised) • Risk of sovereign control of database being compromised • Human input still required to confirm a match. • If data is not visual or numeric, translations tools will need to be incorporated into the network, or data will have to start being stored in common languages. • No cold hit capacity (i.e. the ability to obtain an unexpected match without prior information).

The Prüm Treaty will provide for direct access to the reference data in the national AFIS databases. Reference data shall only include fingerprinting data and a reference. This will make it possible to undertake hit / no hit automated searches. The hit / no hit system will protect personal data whilst making it possible to target and significantly speed up the search for information. Where a possible hit is identified a further confirmation of the hit can be undertaken by the national contact point in possession of the data. Any further personal data and information can then be exchanged via existing communication channels. The treaty is likely to provide a substantial improvement in the exchange of fingerprint data. Rather than using Mutual Legal Assistance to check records in all 25 Member States, the technical solution will allow the requesting State to know (via an automated search) which of the signatory Member States actually have the data required, before Mutual Legal Assistance is needed to exchange it.

iii. Access to information of another Member State through a central index on a hit-no-hit basis

An alternative would be to create a central index searched and fed by Member States law enforcement authorities. The index could reveal matches on a hit-no-hit basis. After a hit on the index, the querying Member State could then request the Member State where there was a hit to provide information on the basis of indirect access. Eurodac, the central asylum fingerprint index, is an example of such a system.

Advantages	**Disadvantages**
• Common standards could be established centrally • The development work would be relatively light compared to establishing a central database • Would be independent of local choice of implementation technology – providing they can communicate via a web service • Sovereign national control over data since only selected data will be shared.	• Require national AFIS databases to be able and willing to expose their services through a web service • Complex to establish the standard for the central application • Procedures will need to be established for downloading data from the national databases to the central index – ideally these should foresee frequent, automatic updates • Dependent on countries populating the index • Matches, hit/no-hit, reported on limited data therefore increased follow up of individual enquiries

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

A central fingerprint database already exists at Interpol. This database is, despite significant recent expansion, under populated. One option would be to use this database.

Advantages	**Disadvantages**
• Already in existence • Little need for local implementation work apart from providing access to data. • Avoids need to harmonise varied information systems. • A central application provides an option for central governance and validation of searches. • Filters can be provided in central databases to restrict countries that can access each depositing state's data. • Useful repository for unidentified crime stains and the ability to offer the added value of trend analysis.	• Some countries would not be able to provide data to a central database because of civil rights legislation • Would involve overhead of maintaining the data both nationally and centrally. • Danger data in central databases may be out of date compared with national databases. • National sovereign control of data is shared with a third (external) party • Common language and data format required. This may require either a conversion tool of uploading or manual conversion and inputting of data.

v. Enhanced access to police data rendered public by Member States' law enforcement authorities.

This modality is not applicable in the case of fingerprint data.

5.3 Recommendations

- Continued use should be made of the existing mechanisms for fingerprint exchange and use of the Interpol database, where possible within national law, should be strongly encouraged. Efforts should be made to improve the efficiency of the existing channels of transmission using AFIS and FITS or equivalent software rather than paper copies, and implementing service standards. The national units servicing these channels should have access to their national AFIS system to assist in transmission.

- The Friends of the Presidency group welcomes the efforts made to establish a technical solution aimed at facilitating direct access from a national contact point to certain Member States fingerprint databases on a hit/no-hit basis (as set out in the Prüm Treaty). Other EU Member States should be kept informed of progress in this area, and should consider the practicalities of joining their own fingerprint databases to the system being developed.

- In light of the experiences of implementing direct access by signatories to the Prüm treaty, the long term objective should be to consider the options for enhancing the Prüm system, increasing the number of participating countries (with consideration given to exchanging information with non-EU states) and possibly increasing the level of direct access granted so that direct access to national fingerprint databases is provided via a search engine / search request network. The Interpol AFIS data base should be included in any fingerprint identification or search process, using the Interpol I-24/7 communications network for access. The combined search engine linking states with AFIS capability and including Interpol facility on behalf of states without their own capability would provide:

  (i) global cover;
  (ii) a cold hit capacity (i.e. obtaining an unexpected match without prior info);
  (iii) the most effective means for engaging EU and non-EU countries; and
  (iv) the most time efficient method of comparing fingerprint data.

  When a match is obtained via the AFIS network, procedures would need to be established for a prompt, final, visual identification to take place. The network would require clearly defined and universally accepted scientific standards underpinned by rigorous quality assurance (QA); secure and cost effective data transmission and searching and safeguards for civil rights and compliance with privacy laws. The system should be designed to allow for continuous improvement in fingerprint data exchange.

- Consideration should also be given to widening access to other fingerprint databases and indexes held within Member States (including the EURODAC index and future databases established in Member States to store biometric information on passports). It would be desirable from a law enforcement perspective that access to these databases is available to the police in Member States through the modality used for police fingerprint databases.

6. Ballistics

6.1 The Current Position – Practice and initiatives

- The forensic analysis of firearms and fired ammunition can link a firearm to a crime, and also identify links between crime scenes. The evidential and intelligence value of ballistics data is further enhanced by the interrogation of other sources of firearms data which can identify ownership and lost and stolen firearms. Such information can assist in the investigation of firearms related crime.

- A variety of databases exist in Member States containing ballistics and firearms data. These include:

  (i) ballistics databases containing information obtained from the forensic analysis of firearms and ammunition;
  (ii) police databases of stolen and scenes of crime firearms; and
  (iii) administrative databases of licensed firearms holders and registered firearms (which, where they exist, can identify the last legal holder of the firearm recovered)

- Data is currently exchanged from these databases upon request via the existing communication channels that exist between Member States, such as the Interpol, Europol and Sirene bureaux / national units. Data may also be exchanged direct between forensic laboratories in Member States. It should further be noted that data on stolen, lost and misappropriated firearms is also stored on the Schengen Information System (SIS). The Europol Information System will also have the capacity to handle data on ballistics and contains a specific data object for ballistics.

- For the purposes of these discussions the focus of consideration is the current capacity and potential enhancements that could be made in the exchanging of ballistics data (though where solutions could be implemented to other non-forensic forms of data, this potential is noted). In particular the potential to exploit the technical possibilities of the automated ballistic identification systems possessed by a number of Member States. Whilst various systems are in use in Member States, the most extensively used is the Integrated Ballistics Identification System (IBIS). IBIS has the potential to link physical items, crime to crime or firearm to crime. IBIS can compare components of fired ammunition from outstanding crimes and from recovered weapons and suggest a list of possible matches. However to confirm a match beyond doubt still requires manual comparison of the specific cartridge cases or bullets by a firearms examiner.

- The possibilities such assets create for boosting information exchange is currently under consideration. One initiative is the EUROBIS project, which is seeking to create a coordinated system linking the various EU Member States' IBIS systems in a similar way to that which has been adopted in the USA linking Canada and certain EU countries. The amount of information stored on IBIS servers is also quite limited, especially for intelligence use. A current EU AGIS funded study is considering the possibility of establishing a Networked Firearms Intelligence Database. An interim report into this issue was published in December 2004[x].

- There are also a number of other AGIS sponsored projects looking at improving the nomenclature covering exchange of technical information across Europe.[xi] Such work will assist with the identification of firearms from class markings on fired ammunition. This work, which has not yet been completed, links in with a Swedish run project – ENFOPOL 16 + ENFOPOL 27 7932/05 – which aims to facilitate exchange and bring consistency to terminology across Europe for technical ballistics information exchange.

- Denmark, Norway and Sweden already share a common IBIS database.

6.2 The Future – options for enhancing information exchange

The current model for information exchange is one of **indirect access to information upon request**. The Friends of the Presidency group has considered a variety of options in order to improve the exchange of ballistics data:

(i) Indirect access to information upon request

This is the current modality for data exchange. Improving this modality would require an improved arrangement between the authority in a Member State which is the guardian of ballistics data, its National Central Bureau of Interpol and Sirene to ensure that there is an effective chain for transmission and receipt of data. There would also have to be an effective mechanism for obtaining the result of data comparisons and transmitting these to the originator of any request. Alternatively, to facilitate bilateral exchanges between forensic laboratories in Member States, steps should be taken to ensure that contact points within each are known.

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 and will specify timescales.

Advantages	**Disadvantages**
• Little implementation work or development costs incurred. • Preserves sovereign control of data. • Source data is only stored in one place and would therefore always be as up to date as national databases.	• Even with improved chains of transmission this process may be slow. • Resource intensive and requires human input. • No real time searching

(ii) Direct access to the databases of another Member State

Direct access could be achieved through a "s*earch request network (search engine)"*. This would establish an international network of ballistics and firearms databases. It requires clearly defined common standards to be applied and underpinned by rigorous quality assurance (QA); secure and cost effective data transmission and searching and safeguards for civil rights and compliance with privacy laws. The EUROBIS project will seek to network the IBIS databases. Similar networking of non-forensic databases could also be investigated.

Advantages	**Disadvantages**
• Avoids the need for a Member State to down-load its data elsewhere (which would otherwise compromise the exclusive sovereign control over data). • Source data is only stored in one place and would therefore always be as up to date as the national databases. • Provides for rapid response to enquiries (either supplying the requested data or a hit/no-hit response). • Development work would be relatively light compared to establishing a central database. • Independent of local choice of implementation technology as long as it can communicate through a web service.	• Would (for forensic material) be complex to establish what the standard for the central application should be unless this has already been developed for existing applications. • Requires that national databases can and will expose their services through a web service. • Would (for forensic material) still require a manual examination to confirm a match. • Requires Member States to possess there own forensic databases which could be searched automatically. • Requires clearly defined and universally accepted scientific standards, underpinned by rigorous quality assurance, secure and cost effective data transmission and searching and safeguards for civil rights and compliance with privacy laws • Need to overcome differences in national automated ballistic identification systems – not all Member States use IBIS (Germany for instance uses Condor) • Solutions will need to be devised to prevent the need to re-search periodically for searches which do not generate a match • No cold hit capacity (i.e. the ability to obtain an unexpected match without prior information). If data is not visual or numerical, translation tools will need to be

	incorporated into the network, or data will have to start being stored in common languages.

(iii) Access to information of another Member State through a central index on a hit-no-hit basis

An alternative option would be to create a central index which could be populated with a limited range of data. The central index would be able to identify a possible match and provide a reference to obtain further information. That data could then be obtained through existing communication channels.

Advantages	**Disadvantages**
• Common standards could be established centrally. • The development work would be relatively light compared to establishing a central database. • Would be independent of local choice of implementation technology – providing they can communicate via a web service.	• Require national ballistics databases to be able and willing to expose their services through a web service. • Complex to establish the standard for the central application. • Dependent on countries populating the index • Matches, hit no/hit reported on limited data therefore increased follow up or individual enquiries • Difficult to distinguish what limited data would be stored on this index

(iv) The creation or extended use of central European and international databases

A central database of stolen firearms or used firearms exists currently at Interpol but the participation of countries to the database is very low. A central database could be created to store ballistics data or administrative information. Denmark, Norway and Sweden already share an IBIS database.

Advantages	**Disadvantages**
• Little need for national implementation work apart from providing access to data. • Central application provides an option for central governance and validation of searches. • Filters can be provided to restrict the countries that can access each depositing state's data.	• National sovereign control of data is shared with a third (external) party. • Some countries would not be able to provide data to a central database because of civil rights legislation. • Information on a central database may be significantly out of date compared with national databases. • Requires an overhead of maintaining data both locally as well as centrally (unless the national databases are abandoned). • Disproportionately costly compared to need. • Common language and data format required. This may require either a conversion tool of uploading or manual conversion and inputting of data.

(v) Enhanced access to police data rendered public by Member States' law enforcement authorities.

This modality does not appear applicable for the exchange of ballistics data.

6.3 Recommendations

- In the long term the possibility of establishing a search engine / search request network to allow for the direct exchange of forensic ballistics data should be investigated. The potential and added value of this networking will need to be considered closely.

- An initial step which might assist would be to catalogue the available databases in Member States and their access regimes. This will provide a clearer indication as to how the principle of availability may be applied to ballistics.

- It is clear the ability to network will depend on the existence of automated ballistic identification systems. Such systems can make a valuable contribution and Member States who do not yet possess such systems should consider the added value that such a system would bring to law enforcement. It is recognised that in some Member States, where firearms related crime is a lesser problem, the added value from such an investment might not be persuasive.[xii] Such states should consider the feasibility of entering their data on the system of another Member State. Where new systems are introduced, Member States should seek to ensure that they are compatible with systems existing in other Member States.

- Networking of IBIS systems is currently being considered in the EUROBIS project. This should be pursued as a valuable tool in investigating specific crimes, as should efforts to establish common standards to facilitate data exchange. The actual creation of such a network would need to be on the basis of a proven cost-benefit analysis. It is recognised that not all Member States possess IBIS databases, and the technical solution to support the network must allow for functionality with non-IBIS automated ballistic identification systems.

- In the long term a more extensive sharing of intelligence linked to firearms and ballistics should also be facilitated so as to assist in the investigative phase of enquiries. Member States should be encouraged, where such databases do not exist already, to each establish a national firearms forensic intelligence database. These databases should link ballistics intelligence with other forms of intelligence to feed into an overarching system that provides real time information for investigators across Europe. This could be achieved by the use of technology to develop networks / links / interfaces between existing firearms (guns and ammunition) databases.

7. Vehicle Registrations

7.1 The Current Position – Practice and Initiatives

- Vehicle registration data is of use to law enforcement officers to:

  (i) identify registered owners and drivers – and obtain historic data about vehicles and their owners; and
  (ii) identify lost and stolen vehicles

  Such information can be vital in solving crimes including minor volume offences (such as driving and parking offences) but also major forms of crime such as identity fraud, stolen vehicle trafficking and organised immigration crime.

Identifying Registered Owners and drivers – and obtaining historic data about vehicles and their owners

- Data on vehicle registrations is currently exchanged between Member States via three principal channels. The first is the informal, reciprocal, arrangements which exist between registration authorities. These links allow for the indirect exchange of data.

- The second is ad hoc requests transmitted via existing law enforcement communication channels such as via the Interpol, Europol or Sirene bureaux.

- The third is the formal IT link that will exist in the EUCARIS Treaty. The **Eu**ropean **Car** and Driving Licence **I**nformation **S**ystem (EUCARIS) is a communications network which links electronically the national driver and vehicle databases of participating countries[xiii]. The IT interface has been constructed and is operational, but one more signatory is required to formally establish the Treaty.

- EUCARIS is a system designed for authorities responsible for the registration of motor vehicles and the issuing of driving licences. EUCARIS will make it possible to verify the identity of a vehicle in the country of origin and alerts the enquirer prior to registration in the country of import if something is wrong such as cases where the vehicle has been reported as stolen or scrapped. EUCARIS also provides for an exchange of driving licence information, which enables the validity of licences from participating countries to be checked prior to exchange. However, whilst the system can also be used by law enforcement agencies responsible for tracing stolen vehicles and fraud prevention, it does not currently provide for the exchange of personal information.[xiv] This is being considered in proposals to develop an enhanced version - EUCARIS II.

Identifying Lost and Stolen Vehicles

- In addition to the channels for exchanging data on vehicle registrations, particular capacities exist for exchanging data on lost and stolen vehicles. Data on lost and stolen vehicles is recorded on the Schengen Information System (SIS) – which is accessible to all law enforcement officers in the participating Schengen states and will also shortly be available to the registration authorities in those states – and a central database of stolen vehicles is held at Interpol. This database currently contains details of approximately 3.3 million stolen vehicles and supplies data on stolen vehicles in a total of 93 countries. The database can reach beyond

the EU's borders and can be searched by registration number and vehicle identification number (VIN) on Interpol's I-24/7 system. It can be accessed via the I-24/7 network and offers member countries the possibility to access the data on stolen motor vehicles through their national application which implies no additional cost, no additional training but access to the information from 93 countries. The so-called integrated system means that one query from a national police application could generate a query to national and Interpol databases at the same time with the reply back to the user in one transaction.

The Effectiveness of Current Arrangements and Current Problems

- These assets and processes can all assist law enforcement. The importance of effective data exchange in this field was highlighted by the Council Decision of 22 December 2004 on tackling vehicle crime with cross-border implications (2004/919/EC). The decision noted as of particular importance the co-operation between law enforcement authorities and vehicle registration authorities and the contribution that could be made by Member States acceding to EUCARIS. The Decision also requires Member States, to take the necessary steps to enhance mutual co-operation between national competent authorities and to ensure that whenever a vehicle is reported stolen, that a stolen vehicle alert is immediately entered into SIS and, where possible, the Interpol database.

- Mechanisms to exchange data on lost and stolen vehicles appear to be working effectively. However, improvements are required in terms of data exchange on vehicle registrations and driving licences to combat volume offences. There is increasing evidence from different Member States that non-resident drivers ignore Licensing, Registration, Traffic and Parking laws when travelling abroad as they do not fear punishment. Overseas vehicles operating under a 'plate of convenience' are a serious threat to the work and credibility of registration authorities and investigative leads may be being missed by the police investigating other forms of crime. This problem is recognised and EU Registration Authorities are in the process of establishing their own association for which a priority task will be to tackle the problem of cross border information exchange.

- A range of initiatives are underway or forthcoming which seek to improve the exchange of this information:

    (i) The Commission is currently investigating the possibility of an EU information exchange network, REGNET, specifically dedicated to vehicle registration applications. REGNET will support initiatives to allow authorities to carry out cross-border enforcement of financial penalties[xv]; cross-border enforcement of non-payment of road tolls[xvi]; and cross border enforcement of non-pecuniary sanctions such as driving bans, restrictions to drive and criminal penalties[xvii]. The Commission is also seeking to create a network, RESPER, to facilitate the exchange of driving licence data. RESPER will increase document security and combat document fraud. The Commission has been working to make the system available in 2006 to all Member State Licensing Authorities.

    (ii) The Prüm Treaty provides for the sharing of data on vehicle registrations via direct access to the national databases of the involved Member States through a national contact point.

7.2 The Future – options for enhancing information exchange

The model for the exchange of vehicle registration data is currently a mix of **indirect access to information upon request** and, for participating states, **direct access to information of another Member State on a hit-no-hit basis via the EUCARIS communications network**.

Data on stolen vehicles is also contained within a **central database** held at Interpol and the SIS. The mechanism for exchanging data on stolen vehicles appear to be working effectively and efficiently and the consideration of further modalities to improve the exchange of this information does not appear necessary.

The Friends of the Presidency group has considered a variety of options in order to improve the exchange of vehicle registration data:

i. Indirect access to information upon request

This modality is already the mode of information exchange between some Member States and other third countries. Indirect access has its merits and is well suited to individual matters that require clarification or are sensitive. However it has proved slow and inefficient, especially for the clearing of bulk data. Exchange is hampered by language barriers, difficulties in technical / process translation and different working hours and is also dependant on the availability of a 'presence' permanently allocated to respond to queries.

Steps could be taken to improve the efficiency of this modality. This would require an arrangement between the authority in a Member State which is the guardian of the vehicle registration and driving licence data and its National Central Bureau of Interpol to ensure that there is an effective chain for the handling of requests and the dissemination of results. Access to the national databases would assist this approach. Similar improvements could be made to cover requests made via the other existing communication channels.

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 and will specify timescales.

Advantages	**Disadvantages**
• Avoids cost and resource investment in new IT structures. • Can be established quickly (would form the basis for developing information sharing)	• Slow (despite any improvements in the end-to-end process) – not suitable for vehicle registration data which often needs to be checked rapidly, perhaps instantly (for example when a vehicle is leaving the EU). • Resource intensive (especially given volume of this data). • Resource burden rests with the requested state (who cannot control the number of requests).

ii. Direct access to the databases of another Member State

Direct access could be established through the construction of a search engine / search request network. This modality already exists albeit for a limited range of data in the IT link to support the exchange network which will be created by the EUCARIS Treaty. The Prüm Treaty also provides for direct online access to national vehicle registration data for Contracting Parties' national contact points. The Treaty is a fundamental step in securing meaningful information sharing. Once a technical solution has been put in place these contact points will have the ability to carry out automated searches to obtain data relating to owners or operators as well as data relating to vehicles. The national contact point will also act as the conduit for all incoming requests.

Advantages	**Disadvantages**
• Allows for an immediate response. • Source data is only held in one place. • Resource burden is shifted to the requesting state. • Direct access to the registers of participant countries ensures that up-to-date information is being obtained. • It is also beneficial that national registration authorities can remain responsible for their own data and that no inputting onto a central system is required.	• Countries that lack a central driving licence registration system are unable to participate in the exchange of driver information. • Sovereign laws would need to be amended/introduced to allow this type of access • Solutions will need to be devised to prevent the need to re-search periodically for searches which do not generate a match • No cold hit capacity (i.e. the ability to obtain an unexpected match without prior information). • If data is not visual or numeric, translations tools will need to be incorporated into the network, or data will have to start being stored in common languages.

iii. Access to information of another Member State through a central index on a hit-no-hit basis

This model already exists in respect of lost and stolen vehicles on the SIS. This index is easy to use, accurate and well populated. It is a powerful and useful tool for identifying stolen vehicles.

However, for the wider purpose of law enforcement a central index containing a limited range of data on vehicle registrations, and linked to Member States' own vehicle registration databases could be established.

Advantages	**Disadvantages**
• Principles and models already exist • Standard response and data fields will result in a simpler IT (and less expensive) solution • Can be established comparatively quickly • It is also beneficial that national registration authorities can remain responsible for their own data and that no inputting onto a central system is required.	• Only limited information could be made available through this solution • It may be difficult to agree the levels of data and access to be shared • This solution will require indirect support • The data held may not be as up-to-date and accurate as in the national systems • Standard protocols for populating the database would need to be agreed • It is dependent on all countries populating the index • Matches will be on a hit no/hit basis on the limited data available, so will require human follow-up for more personal data to be provided

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

A central database for stolen vehicles already exists at Interpol. This database is easy to use, accurate (Member States repopulate their data every 24 hours) and well populated. The Interpol database also has the added and important advantage that it can reach beyond the borders of the EU. As vehicles stolen from within Europe often appear outside Europe it is important for Member States to ensure that their stolen vehicle data is made available to Interpol. Work is underway to roll-out access to this database to police stations country-wide. In addition the Europol Information System (EIS) will contain a data object on vehicles.

However, for the wider purpose of law enforcement a central database of vehicle registrations could be created.

Advantages	**Disadvantages**
• Little need for national implementation work apart from providing access to the data • Central application will provide an option for central governance and validation of searches • Filters can be provided to restrict the countries that can access each depositing state's data	• National sovereign control of data is shared with a third (external) party • Requires an overhead of maintaining the data both locally as well as centrally • Information in central application may be significantly out of date compared with national databases • Scale of the operation may be overwhelming and prohibitively expensive to sustain • Common language and data format required. This may require either a conversion tool for uploading or manual conversion and inputting of data.

v. Enhanced access to police data rendered public by Member States' law enforcement authorities

In some Member States such as Finland, Sweden and Latvia, a certain amount of information on vehicle registrations is already publicly available from the appropriate administrative agencies via telephone, email and SMS communications. The data available varies but on submitting a vehicle registration or VIN can include details of the vehicle (including brand and model); the name of the current and previous owners and the city of their residence; and tax and insurance details.

Such resources, where (and this is not always the case) available to international enquirers and providing the response to the enquiry is rapid, provide a useful additional resource to law enforcement officers in other Member States. Unfortunately access to such information may necessitate the payment of a fee and the amount of personal data released may be limited. Their value as a primary channel for data exchange to the international law enforcement community may therefore be questionable, but as an additional resource their existence should be publicised. Their value could be increased by ensuring that access is allowed to law enforcement officials from other Member States free of charge and preferably in a range of languages.

7.3 Recommendations

Short term: Initially use should be made of existing links and IT infrastructure and in particular EUCARIS. The IT platform constructed for EUCARIS is already an operational reality in participating states. It delivers practical, direct, international information exchange. Widening the number of states participating in the system and broadening the amount of data shared should be encouraged. EUCARIS can and is being developed further and this too should be welcomed.

However EUCARIS does not (at least currently) provide for the sharing of personal data. To follow up leads identified from EUCARIS, obtain information not available on EUCARIS or to obtain information from states who do not participate in EUCARIS, a national contact point / gateway team should be designated in each Member State who can follow up hit-no-hit queries indirectly and interact with other organisations in the sharing of intelligence and best practice.

For stolen vehicles the SIS and Interpol database will continue to have a valuable role to play. Member States should ensure access is made available at a local level countrywide, so that they can be populated and interrogated at the point of need.

- **Medium term:** Full direct access to the national vehicle registration databases should be established via a search engine / search request network. Various different options exist which could potentially deliver this integrated IT platform. An enhanced version of EUCARIS is one option; the solution developed to facilitate direct access under the Prüm Treaty will be an alternative.

In undertaking work on REGNET the Commission is already investigating the means to deliver such an information exchange network. EUCARIS is a proven system that can be developed (EUCARIS II) as the platform for REGNET. As a result of its availability it has been included in the REGNET feasibility study and should be considered as the preferred option. If EUCARIS is not chosen as the IT platform for REGNET, any other IT platform will need to be developed and tested and would therefore not be operational for some years.

Whatever platform is chosen it would be beneficial if a direct link, if technically possible, is established between the network and the stolen vehicle information held on SIS and the Interpol database to ensure cross-population. The connection and relationship between RESPER and REGNET should also be considered and the possibilities for their interconnection should be encouraged.

- **Long term:** Once the data exchange network has been identified and developed it should be rolled out to all Member States to become the primary tool for international information exchange in this field.

8. Telephone Numbers and other Communications Data

8.1 The Current Position – Practice and Initiatives

- Law enforcement authorities benefit from the exchange of information related to telephone numbers and a range of other communications data. For the purposes of this report this is deemed to cover:

  (i) reverse directory enquiries, identifying the name and address of a subscriber from a given telephone number or IP address;
  (ii) identifying other account related information (billing address, installation address, payment method);
  (iii) identifying call related data of outgoing calls made from a given telephone number;
  (iv) identifying call related data of incoming calls made to a given telephone number;
  (v) identifying call related data for a specific mobile telephone handset (the IMEI number)
  (vi) historic location data for specific mobile telephones; and
  (vii) calling line identity (telephone number) for a given dial-up access IP address.

- It is recognised that in many Member States communications data is not held by law enforcement authorities themselves but by privately and publicly owned companies. This adds an additional complexity to proposals to share this data, but the group felt it would be useful to highlight and explore the variety of information and intelligence of use to law enforcement authorities and how it might be better exchanged. Such companies who hold such data do so because of their provider-customer relationship and they have an explicit duty of confidence to their customer. Whilst a limited amount of data (usually restricted to the ability to provide a telephone number for a named individual) may be made publicly available via directory enquiry services, the vast majority of the data is held subject to a duty of confidence which may be overridden but only by the exercise of a legal authority requiring the disclosure of data to a judicial body or other public authority. Therefore fundamentally the databases of communications data are held by the various communications service providers, each provider holding data in relation to their customers. Such data is not readily available and instantly accessible to law enforcement authorities (some service providers will apply a charge for providing such data) and it is important to maintain good relationships with the communications service provider industry. Good relationships are critical to the effectiveness of certain national security and law enforcement work. Any initiatives intended to improve availability should not jeopardise existing relationships with service providers in any way.

- However, disclosure of communications data between Member States already takes place to some extent. Exchange is by means of indirect access to information upon request and can be by way of Interpol, Europol or Sirene bureaux. In some Member States the transmission of this information requires the use of formal mutual legal assistance mechanisms. Any initiatives intended to improve availability should be without prejudice to the national security interests of Member States.

8.2 The Future – options for enhancing information exchange

In considering options to enhance data exchange it is important to draw a distinction between:
(a) Communications data that is publicly available; and
(b) Communications data that can be obtained but is held by third parties.

Where data is already publicly available it is not necessary to consider modalities to facilitate data exchange. However, efforts could be made with service providers to ensure efficient access.

For all other forms of communications data the current mode of exchange is via **indirect access to information upon request**.

The Friends of the Presidency group has considered a variety of options in order to improve the exchange of communications data:

i. Indirect access to information upon request.

Indirect access to information upon request is the most commonly used mechanism by which communications data is currently exchanged. It is also the most appropriate means given that the data is not usually held by law enforcement agencies directly but rather by companies and third parties. The efficiency (and especially the timeliness of responses) could be improved. The ability of the Interpol National Central Bureaux, the Europol National Unit or the Sirene bureaux to obtain this data quickly can be enhanced if there are electronic links between them and telecommunications data service providers.

The Framework Decision on simplifying the exchange of information between the law enforcement authorities of the EU will, once adopted and in as far as communications data meets the criteria of information and intelligence held by or accessible without the use of coercive means to competent law enforcement authorities, improve the efficiency of such exchanges and will specify timescales.

The Prüm Treaty (Article 27) provides for co-operation between signatory states, upon request, to ascertain the identity of telephone subscribers and subscribers to other telecommunications services, where this information is publicly accessible. This limited provision reinforces the existing modalities for the exchange of telecommunications data.

ii. Direct access to the databases of another Member State

Direct access provides that the law enforcement authorities of one Member State could directly query the law enforcement (or administrative) database of another Member State. Law enforcement authorities in Member States do not routinely hold communications data except where it has been obtained from third parties pursuant to specific investigations. Such data is not therefore available upon a specific database to which law enforcement authorities of other Member States could be granted direct access. And in most cases the requested communications data will be held by communications service providers and access to such data is only available via means of indirect access upon request.

iii. Access to information of another Member State through a central index on a hit-no-hit basis

This option would also be difficult to implement by law enforcement authorities in Member States given the nature of the data, its current storage and access arrangements.

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

In the case of communications data, this modality could not be applied for practical reasons.

v. Enhanced access to police data rendered public by Member States' law enforcement authorities.

In the case of communications data, this modality could not be applied for practical reasons.

Recommendations

- The nature of communications data and its current storage arrangements by communications service providers determines that the current mode for exchange of this type of data, indirect access to information upon request, is and shall remain the only feasible approach to data exchange (except where this data is publicly available). Efforts should be made to improve the efficiency of this mode of transmission. This could be assisted, where possible within national law, by granting the relevant contact point(s) within each Member State direct access to the relevant databases of the communications services providers within their Member State.

- A questionnaire could be circulated in order to gather information regarding the position in each Member State for obtaining the data referred to above in the paragraph entitled "the Current Position – Practice and Initiatives".

- Exchange of open-source information containing telephone numbers and communications data could be facilitated, although the service provided by www.ediq.org may already prove adequate.

9. Minimum Data for the Identification of Persons (Civil Registers)

9.1 The Current Position – Practice and initiatives

- The need to consider data exchange in this field for law enforcement purposes was first raised at the Article 36 Committee on 4 April 2005. The mandate of the Friends of the Presidency is to discover whether this area provides scope for any further work, decide how this might be taken forward and make a recommendation to the Multi-Disciplinary Group.

- Discussions of the Friends of the Presidency focused on the possible repositories for such data and how this data is exchanged. Two main sources were identified: civil registers (varying from the comprehensive registers held in certain Member States to other administrative task-specific registers such as electoral registers) and ID card databases. The existence of such registers, who administers and how information can be exchanged from these registers was considered in some detail.

- Certain Member States, notably the Nordic countries hold very comprehensive civil registers. In Finland the civil register is owned by the state insurance authority and domestically police officers have direct access. Similar registers, accessible directly by the police in combating crime, exist in other Member States such as Belgium and Slovenia. Other Member States such as Spain hold a national identity cards database, which stores similar details. The police manage this database but it is an administrative database and information cannot be extracted without judicial authority.

- However not all Member States have ID cards or such comprehensive central civil registers. In Member States where such central civil registers do not exist the police consult less comprehensive sources. In Ireland for example, the electoral register, the land register, the birth and deaths register and the social security database can all be consulted. Such registers and databases are owned by non-law enforcement authorities and held primarily for non-law enforcement related purposes. In some instances such registers, or an edited version, are publicly available.

- If another Member State wished to obtain information from these registers, except where the registers are publicly accessible, access would be indirect with information provided on request. The data could be channelled via Interpol, Europol national units or the SIRENE bureaux. In certain Member States, such as Belgium and Spain, the release of the information would be subject to judicial authorisation.

- There is no Community competence concerning ID cards making it difficult to make recommendations concerning ID cards or the databases that support them. All Member States which have ID card databases have rules about who may access them and in what circumstances. However, work is underway at the intergovernmental level, on producing a minimum set of security standards for national ID cards in the EU. This work is being led by the Presidency, and facilitated by the Commission and the Council.

9.2 The Future – options for enhancing information exchange

The current model for data exchange between Member States of information held within civil registers is by means of **indirect access to information upon request.** In certain Member States such transmissions are subject to judicial authorisation. The disparity in available information and access regimes hinders exchange but also does not lend itself to simple solutions. The Friends of the Presidency group has considered a variety of options in order to improve the exchange of this data:

(i) Indirect access to information upon request

This is the current model for information exchange with information being channelled via the existing communication channels. The efficiency of this means of transmission could be improved by ensuring that the national units for each of these possible channels of exchange are housed in the same agency, in the same location and under the same management. Where internationally agreed service standards exist these should be followed and may provide a mechanism for improving response times. The Framework Decision on simplifying the exchange of information between the law enforcement authorities of the EU will, once adopted, also improve the efficiency of such exchanges and will specify timescales. The speed of access will continue to be influenced by the judicial process where judicial authorisation is required.

Where possible within national law, the speed of exchange of this data could also be enhanced by ensuring these national units have direct access to the civil registers and ID cards databases. Where this is not possible an arrangement should exist between these national units and the authority in a Member State which is the guardian of the civil register / ID cards database to provide for an effective chain for the transmission and receipt of data.

(ii) Direct access to the databases of another Member State

This option, once operational, would shift the resource burden to the requesting state. However, the technical and linguistic difficulties in linking the variety of registers and databases that exist would make this an unattractive option. There are also likely to be significant and probably insurmountable political objections to such a proposal.

(iii) Access to information of another Member State through a central index on a hit/no-hit basis

A central index searchable on a hit-no-hit basis might overcome some of the political and data protection objections. It would also, once operational, shift the resource burden to the requesting state. However significant technical obstacles, complicated further by the diversity of data held in Member States, may make this an unattractive and costly option. It would also be difficult to determine what reference data should be stored and the added value from such an index.

(iv) The creation or extended use of central European and international databases

No such database exists. Any proposal to establish any new central databases would need to be considered critically. The Friends of the Presidency do not foresee a need or value in this field for such a database and note that there would likely be significant political objections to any proposals to create such a database.

(v) Enhanced access to police data rendered public by Member States' law enforcement authorities.

In certain Member States some civil registers, or at least an edited version, will be publicly available (whether at the initiative of the law enforcement authorities or other public bodies). Access regimes to these vary. Providing access is free and data can be obtained rapidly, this may provide a useful additional resource for law enforcement officials in other Member States. Access via the internet is desirable. The value of such open sources also depends on awareness and promotion of their existence.

9.3 Recommendations

- Information contained within civil registers should, taking into account the need for confidentiality in specific cases, be available within the EU on the basis of equivalent access. This means that the access regime for this data should be the same for other Member States law enforcement officers as it is for the domestic law enforcement authorities in the Member State concerned. Therefore where data from such registers is available to a law enforcement officer domestically without judicial authorisation, the transmission of such data overseas should not be subject to judicial authorisation. In the longer term those Member States who require judicial authorisation should revisit this requirement in light of the principle of availability.

- Indirect access upon request will remain the principle modality for data exchange. The existing channels for data exchange will continue to be used. However the efficiency of data exchange via indirect access upon request should be improved by implementing agreed service standards. Efficiency would be increased were the various national units for each of the possible channels of exchange to be housed nationally in the same agency, in the same location and under the same management and Government Ministry.

- Work should also be undertaken to catalogue and promote the various open sources which might be of value. Access to data through these sources should be quick and free (unless a charge is made to domestic law enforcement officials) to law enforcement officials from other Member States.

10. Other Data Fields to which the Principle of Availability could usefully be applied

10.1 Explosives, trade registers and the forensic profile of synthetic drugs[xviii] are all fields to which the principle of availability could be applied.

11. Concluding Remarks – towards a coherent strategy

11.1 The report considers options for improving information exchange in each of the data areas, either by enhancing the efficiency of the existing mechanisms or by adopting alternative modalities. The recommendations include complementary short and long term strands. However, the long term objectives are:

- DNA – direct access to Member States national DNA databases via a search request network
- Fingerprints – direct access to Member States AFIS databases via a search request network
- Ballistics – full direct access to Member States IBIS databases via a search request network (subject to confirmation of added value)
- Vehicle Registrations – full direct access to Member States vehicle registration and driving licence databases via a search request network
- Telephone numbers and other Communication data – (more efficient) indirect access to information upon request via existing communication channels
- Minimum data for the Identification of Persons (Civil Registers) – (more efficient) indirect access to information upon request via existing communication channels; promotion of open sources

11.2 These modalities are considered the most practical and beneficial means by which to realise the principle of availability in these fields. However it should be emphasised that the findings do not purport to be a full and thorough business case. Detailed assessments of business needs, considering functional requirements (general, investigation and intelligence) and technical requirements (standards, security, audit management information / service levels / future proofing) should now be undertaken. There are also outstanding issues concerning data protection requirements and other legal considerations which will need to be addressed. Ultimately there is also a need to review procedures regarding judicial decision making in instances where it proves to be overly slow and cumbersome.

11.3 The report can provide a basis for future discussion of improving information exchange within these particular data fields and other fields. It is clear that there are generic advantages and disadvantages to the different modalities, but the applicable approach will depend on:

- the type of data;
- its ownership; and
- existing storage and access arrangements within Member States.

The recommended approach must further be proportional to the law enforcement need and the sensitivity of the data. The speed at which the recommendations can be implemented will also be influenced by these factors. These considerations will also apply to any other data areas where modalities are being sought to implement the principle of availability. The modality will determine where the data is stored and how it is transmitted, but it need not determine the level of access which can be controlled by the individual Member State.

11.4 In taking forward the recommendations it is clear that there is a need for co-ordination and consolidation. It is vital that there is a consolidation exercise to ensure that the various initiatives under way in each field are compatible and that duplication of effort does not occur. A cataloguing exercise to establish what databases and other knowledge banks exist, the types of data stored, the retention periods and the various access regimes would assist. This could be accompanied by an assessment of the tasks, inter-connection and inter-operability of the already established and functioning systems in order to ensure the capabilities of these systems are fully exploited and avoid overlapping mechanisms and duplication. Such an assessment should build upon the 2003 study of 3rd pillar information systems to consider other national and international information systems.[xix] These initiatives should assist and underline the need for a coherent policy in IT development. A paper outlining some suggested guidelines was drawn up by some members of the Friends of the Presidency group and is set out at Annex B. The Friends of the Presidency group did not have time to consider these in detail but included them as a spur for future work and the development of future policy in this area.[xx]

11.5 The objective must be 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. The technical solution must be designed to meet current and future business needs, taking into account functional and technical requirements. Its functionality and interoperability should be maximised and it must be easy to expand and modify.

11.6 Most importantly of all the chosen modality must seek to enable and not constrain information exchange, to empower Member States and not to diminish Member State control. The modality must therefore provide for a flexible and diversified approach both now and in the future, and should be designed to allow for a continuous improvement in data exchange and to allow individual Member States to pursue enhanced co-operation should they see fit.

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

The applicable approach will depend on the availability and access regime to the database.

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.

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.

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:

- "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."
- "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."
- "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:**
  - 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.
  - 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.

  - *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.

- *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.

- *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.

- *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.

- *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.

- *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.

- *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.

- *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.

- *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.

- *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.

[i] Council Resolution of 9 June 1997 on the exchange of DNA analysis results (97/C/193/02)

[ii] Details of the national databases, the legislation and the DNA systems used are available on the ENFSI DNA WG website (http://www.enfsi.org/ewg/dnawg/). The criteria for DNA sampling of individuals and the data retention periods vary according to national legislation. Details of legislation, profile retention and removal are available on the ENFSI DNA WG website at http://www.enfsi.org/ewg/dnawg/db/exfile.2004-09-20.5914860034. In February this year the Commission issued a questionnaire to all Member States to collate information on national DNA databases. The questionnaire asked for details of these databases their technical specifications, their control and access regimes, their searching and matching capabilities and their ability to exchange data with other Member States. The collated responses to this questionnaire, accompanied by a synthesis of the results, was published by the Commission on 3 August 2005. This provides a valuable inventory of the DNA capabilities of Member States.

[iii] Council Resolution of 25 June 2001 on the exchange of DNA analysis results (2001/C 187/01) invited Member States to use specific DNA markers in forensic DNA analysis, to use a particular form for exchange of DNA analysis results and to exchange such results electronically. This reinforced the standard already in use in other international organisations such as Interpol.

[iv] It should be noted that not all Member States yet have access to the Schengen Information System.

[v] Interpol have advised that, of transmissions via the I-24/7 system, Germany is the only Member State to be applying this standard.

[vi] At the Interpol General Assembly in 2004 all EU members present agreed to upload fingerprints related to identified and arrested criminals onto the Interpol AFIS system.

[vii] Figure supplied by Interpol (of which 17758 are from EU states), September 2005.

[viii] Council Regulation 2252/2004 of 13 December 2004 on standards for security features and biometrics in passports and travel documents issued by Member States, requires that by 2008 such documents shall contain fingerprints in an interoperable format.

[ix] It is interesting to note that Article 22 of the 1959 European Convention on Criminal Matters requires Member States to exchange data in relation to convictions of individuals from other Member States, but it does not require the conviction to be supported with fingerprints. In the absence of this, it is impossible to prove that the conviction relates to a particular person rather than someone who may have assumed their identity.

[x] Interim Report for the European Commission Directorate-General of Justice & Home Affairs: Funded by AGIS, '*A Study into a networked firearms intelligence database*'. Forensic Pathways Ltd ©. Document ID: Draft 2004 AGIS/Ballistics/Leary, R.M. 112/04.

[xi] One project, the Markings of Firearms project, will assist the police and practitioners in identifying and classifying unknown markings on firearms. A second (2004/AGIS/094), a Feasibility study of a common European standard format for describing class characteristics on cartridge cases and bullets from firearms

[xii] Figues provided by Finland indicate that their Crime Laboratory of the National Bureau of Investigation handle some 250 firearms statements per year, but less than 20 concern ballistic analysis. In total they estimate that they have only 20 – 30 unsolved cases which concern the question of what firearm a bullet or cartridge was fired from.

[xiii] There are currently 5 EUCARIS-participating countries; within the European Union 11 countries have two way links where enquiries can be made of them and vice versa (Belgium, Estonia, Germany, Hungary, Latvia, Lithuania, Luxembourg, The Netherlands, Romania, Sweden and the United Kingdom), and 6 have "one way links" where they are able to make enquiries but not receive enquiries.

[xiv] More information on the EUCARIS system is available on the EUCARIS internet site, www.eucaris.net.

[xv] The Council Framework Decision on the application of the principle of mutual recognition to financial penalties provides for the application of the principle of mutual recognition to financial penalties. The Framework Decision was specifically extended to include financial penalties imposed in respect of road traffic offences. It will come into force in 2007. Work is currently being taken forward in the EU funded VERA2 project to identify a data exchange network (ENFORCE) which will allow the authorities to carry out cross border enforcement of financial penalties – the earlier VERA project established the principle that penalties should be dealt with in the country in which they were invoked or where the vehicle's driver / owner is resident.

[xvi] The Electronic Fee Control project is another EU funded project which is intended to look at ways of automating the collection of road tolls and to facilitate cross-border enforcement action against non-payers.

[xvii] This work is being taken forward in CAPTIVE, a project which will analyse the current multi-lateral and bi-lateral instruments and propose recommendations as to how to overcome problems in this field.

[xviii] Forensic laboratories have developed methods to identify the profile of synthetic drugs. This can usefully establish with a high probability the connections samples of amphetamine seized and establish whether they came from the same batch and / or the same production facility. Work has already been undertaken in this field at EU level, commencing in May 2001 with the CASE Pilot Project (which sought to prepare a scientific and practical way for the establishment of a system for profiling synthetic drugs). In 2002 an Analytical Work File was opened at Europol to facilitate the sharing of profiles and accompanying intelligence. The EU Drugs Action Plan

identifies the development of the forensic profiling of synthetic drugs as an important instrument for intelligence led drugs enforcement and calls for the development of a long term solution at EU level for the use of synthetic drugs profiling results for strategic and operational purposes. This will require a harmonised method for analysis and a vehicle for accurately and efficiently sharing data.

[xix] Report of the ad hoc group for the study of the 3rd pillar information systems, 8857/03 JAI 118.

[xx] The content of Annex B was not considered substantively by the Friends of the Presidency Group, but is annexed to the report in view of further considerations by the Multidisciplinary Group on Organised Crime.