Ensuring trust and security in electronic communication

Theodor W. Schlickmann
Commission of the European Communities
Directorate-General XIII - Telecommunications, Information Market and Exploitation of Research
Security of telecommunications and information systems
Theodor.Schlickmann@bxl.dg13.cec.be

1. Introduction

This paper is on European Commission (EC) projects researching and piloting the provision of trusted services to meet the needs of the Single European Market. These projects, in the main, address topics related to the market demand for these services and the technological options for satisfying this demand. However, there is one other critical area that needs to be addressed to develop a rounded assessment of the situation. This is that of the legal and regulatory environment with which service providers need to be compliant.

The control of access to high quality technology for encryption of information has been goal of leading industrial countries for many years. This is evidenced by a variety of controls on either the use, import or export of these technologies which are imposed by different countries in Europe and elsewhere.

The justification for controlling the availability of high quality encryption technologies has been based on the premise that its widespread proliferation could be prejudicial to the interest of the State. Ready access to these technologies to criminal, terrorist or potential military adversaries is viewed as having the potential to make it more difficult to protect national interests.

Control of encryption technology fall within the scope of the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies. This Arrangement, drawn up in 1996, views encryption technology as a dual-use item, i.e. one that has potential military as well as civil uses, and as such one which should be subject to export controls. At least 31 countries have signed this Arrangement, including most European countries.

The result of these, and the earlier COCOM measures, to control the export of encryption technologies have been several. One of the more serious consequences has been the growth of legal and regulatory regimes that vary from country to country. And, in turn, this has inhibited the growth of international markets for advanced security products.

In the light of this situation the EC has set up several projects which are researching the issues surrounding the provision of trusted services on a pan-European basis with a need to pay attention to the legal and regulatory situations in the countries involved

2. Background of trusted services

2.1 General

When different actors need to co-operate electronically and grant information access rights to one another, they need some level of assurance that their counterparts will pay for the services, will refrain from using the access rights for unfriendly actions, and will not violate other business agreements that are valid for the access.

The business agreements between service providers engaged in co-operative management will be substantially simpler than those for joint management. As a minimum, however, providers will require registration and authentication of their counterparts in advance, in order to ensure that authorisation, access control and accounting can be properly taken care of.

The level of trust one provider places in a particular counterpart is reflected in the access rights granted to this party. Such a party to party trust may be mutual, but not necessarily so. If the level of trust is low, very limited access will be granted, although Open Network Provisioning (ONP) requirements for non-discriminatory access must be kept in mind. Moreover, one will be required to record proofs of the performed actions (i.e. accountability requirements) in order to ensure non-repudiation.

Such recordings may be performed by a trusted services acting as a notary, and disputes may be settled by a trusted services in an adjudicator role. When no direct agreement exists between two actors, it may be possible to use a trusted services as a mediator. This trusted services must be trusted by both sides, and must vouch for their accountability. In this case, the two actors do not even need to know each other, and anonymous access is possible.

2.2 Trusted Third Parties (TTPs)

Several research syndicates have proposed the introduction of Trusted Third Parties as an optional solution to the need for trusted services within the field of electronic commerce. The definition of TTPs developed by the International Standards Organisation is as follows :

A Trusted Third Party is a security authority or its agent which is trusted by other entities for the security functions it provides. When a Trusted Third Party is the security authority for a domain, it can be trusted within that domain.

Many other research syndicates developed their own definition of Trusted Third Parties. In a definition that is more workable and which gives more insight into the features and tasks, a Trusted Third Party is described as follows:

A Trusted Third Party is an impartial organisation delivering business confidence, through commercial and technical security, to electronic transactions. It supplies *technically and legally reliable means of carrying out, facilitating, producing independent evidence about and/or an electronic transaction. Its services are provided and underwritten by technical, legal, financial and/or structural means.*

2.3 General functional requirements for Trusted Services

The Security Group of G4 (Law enforcement members from Germany, England, France, The Netherlands) with Sweden also, have issued a list of functional requirements that the Trusted Third Parties would have to comply with to be agreed. These requirements are based on the implementation of the so called Royal Holloway Protocol (see also Section 6).

The fourteen minimal requirements as defined for an international TTP architecture are listed hereafter[1]:

1. The framework should provide benefits to legitimate user. It must support electronic business transactions in terms of integrity, authenticity, and confidentiality.

2. It should provide for both national and international working.

3. It should be public and unclassified.

4. It should use well known techniques.

5. It should support all forms of electronic communication.

6. It should be compatible with different laws and regulations of participating countries concerning interception, use, supply and export.

7. It should not impede the due process of law and order. In particular, it should allow near-real-time access when a warrant is held. The system must not allow the user to detect that warranted access is taking or has taken place;

8. It should provide access under warrant (or other legally-constituted form of authority) to both incoming and outgoing communications from a single TTP in the country in which the warrant was granted. The system should limit warranted access to that which is authorised and no more, i.e. to communications to and from the user against whom the warrant has been granted for the time when the warrant is extant. It must provide for warranted access to confidentiality keys, but should not permit access to keys used for digital signature; there is no requirement for escrow of such keys.

9. It should enable the sender to limit the length of time for which any key is used.

[1] This list of requirements does not necessarily reflect the opinion of the EC

10. It should provide for the use of a variety of cryptographic algorithms whether in hardware or in software.

11. It should not enable those with a warrant to fabricate false evidence.

12. It should ensure that attempted abuse by the sender can be noticed by the receiver. It should be impractical for the/a user to subvert or bypass the legal access system.

13. It should not require a user to deal with a Trusted Third Party in another country.

14. It should not require either regular or on-line communication between Trusted Third Parties.

The European Commission has published recently a communication[2] which tries to create awareness about the risks and implications of establishment of key recovery/escrow schemes. It also shows, based on the findings of the projects, that some of the requirements from above can not be met at all

2.4 Trusted functionality

A secure communication channel between two parties cannot be established unless there exists at least one component which both parties unquestionably trust. Effectively, secure communication is based on trust between the two end-users, the third party has a referee role. In his absence, one of the two entities could create an insecurity or claim its partner to have created one, without any proof, this creating conflict and an insecurity. A typical example of the third party role is to insure that a party is who they say they are and not another end-user that pretends to be the right person.

The third party is usually the starting point for an authentication process, for example the signature key for a public-key certificate. It may also be a shared secret key, where both parties trust that this key is not revealed to any outside party.

TTPs may be used to realise points of trust. TTPs may have a role in different kinds of security related services, for example as authentication, access control, key management, or non-repudiation (notary) servers.

From the communication point of view, TTPs can be:

- on-line services, interacting in real time with one or both of the management systems, for example an authentication server;

[2] http://www.ispo.cec.be/eif/policy/97503toc.html

- in-line services, intercepting the path between the two management systems, for example a "black box" translating between two encryption algorithms (decrypt and re-encrypt);
- off-line services, which are needed to enable communication, but do not take part in the actual communication, for example a certification authority.

2.5 Commercial requirements

2.5.1 General

Commercial requirements, also known as accounting management, consists of a set of functions which:

- enables the activation and use of the service feature to be measured and the cost to the customer for each use to be determined, including facilities to generate, collect, store and process accounting information to generate cost advice, billing and invoices for customers. Accounting management also provides functions for the setting of tariffs, accounting limits and billing parameters for the usage of the services and resources;
- enables the measurement of the attaining of business objectives with regard to profitability and cost control;
- enables the exchange of information with other accounting management systems in other domains for accounting purposes.

Accounting management, enables the administration to keep the operating company on a sound financial footing.

The recording process will have facilities to collect, store and process accounting information. The accounting management function has the following sub functions, which are described below:

- charging and billing;
- cost accounting

The charging and billing function enables the usage of resources and services, by each customer, to be measured and the subsequent generation of cost advice, billing and invoices for customers. The receipt of payments is registered. This function also alerts the administration of non payment of bills, so that service can be discontinued.

The cost accounting function has two main purposes: it enables the administration to constantly evaluate its financial position and it enables the administration to alter its tariff plans by first running trials of proposed tariffs and elasticity of demand, on simulated computer programmes.

Section 2.5.2 and 2.5.3 detail the requirements for these two functions.

2.5.2 Basic requirements for charging

To perform the charging function it is best to consider and keep to some basic principles, which are summarised as follows:

- it should be fair, to both the user and network operator;
- it should be user-friendly;
- it should be objective in the sense that in the event of conflict between the operator and the subscriber, some measurable and specific parameters, used as the base information for charging, can be utilised when negotiating differences of opinion;
- it should be flexible enough to allow the operator to change and select the charging parameters to suit his specific regulatory and commercial requirements;
- it should be easy and cheap to implement. This is also an important aspect, because of the large hardware and software cost associated with the collection and processing of the charging information;
- it should consider and reflect the real costs invested by the operator to provide the services;
- it should be independent of the specific teleservice or of the user information which is transported in the cell user payload;
- it should be used to promote an efficient usage of the network.

2.5.3 Basic requirements for billing

Depending on the functional area, billing may be viewed :

- as a service provided to customers, which is the same as any service managed by the other functional areas;

- as a management activity in its own right. For example, performance management may monitor the activity of the "billing service" and check whether the required Quality of Service is being achieved. On the other hand, Provisioning will communicate details of new customers directly to the billing activity, treating billing as part of network management

4. Threads and counter-measures

Selection of countermeasures.

The selection of security countermeasures is the result of a complex process which includes the aforementioned analysis of the threats, the vulnerability of the service management assets, and of the potential impact of a security breach. The resulting assessment of the risk leads to the decision to counteract all or most of the identified threats. That process will be iterative. The selection of the countermeasures is followed by a cost/benefit evaluation, which might conclude that the cost of the selected measures is too high compared to the potential damage.

Security measures can be of various sorts: administrative, physical or logical. These measures aim at protection of the management services and management information when stored in or transmitted between management systems. Here only logical measures are considered. Physical protection is outside the scope of the projects. Administrative measures, to the extent that those fall within the scope, are for further study.

When an interface between management systems belonging to different actors is considered, the authorities responsible for the security domains must agree on the measures to use. To some extent the provider of the management services (on the server side) can impose a given set of measures. The ONP regulations recognise the right for a provider to deny a management service request from another provider, when that provider is not able to guarantee the required level of security in the operations. For external access however, the provider of the management services can only impose security measures and security profiles which are standardised..

5. Project description

What follows is a short description of each project to give an overview of their objectives and pilot tests. A more detailed description can be found on the Internet[3].

5.1 KRISIS (Key Recovery In Secure Information Systems)

The project has the objective to derive commercial requirements for a confidentiality service with ability for key recovery. But in contrast to the US Clipper Chip approach, the project will install an architecture, that allows the commercial enterprises a control on the key recovery techniques used while maintaining the possibility to integrate law enforcement requirements. A pilot will be implemented, which allows to demonstrate the use of the confidentiality service including the key recovery technique to a wide user community.

A pilot will be set up in the project to demonstrate key and data recovery techniques in Europe using Data Recovery Centres in five different European countries.

5.2 OSCAR (Trusted services support for name authentication, certification and directory management)

This project will specify the functional requirements and design of a pan European network of trusted services centres. and for the assessment of this design with pilot certification and directory management. This infrastructure is aimed at supporting

[3] http://www.cordis.lu/infosec/home

user authentication primarily in support to secure messaging. However, the certification infrastructure can be used to provide other forms of certified keys including public keys for confidentiality key encryption or in a key agreement mechanism.

The pilot will show authority of certification can work, and how entities can communicate using certified keys in a certified-based asymmetric key management architecture.

5.3 MANDATE II(Secure cheques)

The MANDATE I project, funded under the TEDIS programme in 1994/5, set out to develop a generic solution, both technical and legal, to the problem of electronic negotiability. A demonstration system was produced, but no actual pilot testing were planned for, nor carried out.

The objective of MANDATE II is to take the generic solution produced in MANDATE I and, in line with the functions (key management, inter-domain communication and document transactions), develop a prototype of a new financial electronic negotiable instrument. Particular emphasis is put on providing and piloting a solution which is not only technical sound, but which also addresses the legal and commercial issues involved in the project in the sense that the necessary framework to form a realistic legal basis for the pilot will be provided as well.

5.4 AEQUITAS (Legal Study on Trusted Services)

The objective of the project is the elaboration of a study on the legality that encrypted electronic messages, signed by digital signature and certified by a service of trust can have in criminal litigation. For that the project will specify:

judicial and technological possibilities to ensure that encrypted messages be decrypted, and
the juridical rules to fulfil by a trusted service.

The study will establish on the experience made during one year by a public (experimental) trusted service. This service will include certification of established relations made between a group of lawyers, judges and prosecutors in different European countries in their daily practice.

5.5 EURO-TRUST (Provision of a Public Key Certification Infrastructure)

EURO-TRUST is a project to investigate the establishment of trusted service centres in four countries within the EU. These national activities will be aligned with and bound to a common European framework which will be defined within the project. A limited pilot across the four countries will be used to validate the designs produced. They will focus on designing and implementing a trusted service infrastructure which uses appropriate cryptographic techniques and addresses legal implications and interoperability issues.

5.6 EUROMED (Trusted Services for medical applications)

The main objective of EUROMED is to exploit all aspects (operational, technical, regulatory, legal) of trusted services for telemedical applications over the WWW[4]. They will achieve this objective building on existing results from various European projects. The project will concentrate on the establishment of trusted services for ensuring that all health actors can communicate in a secure way. In this project the wealth of existing results will be reviewed and a pilot will be set up in order to effectively assess the acceptability, effectiveness, and economics of these services in health care.

5.7 EAGLE (Key management for trusted services with key escrow/recovery)

The EAGLE project will address the following objectives:

to investigate the commercial issues associated with offering trusted services over a pan-European network of trusted service centres, including the service offered, mechanism to provide them, and the means of charging for them;
to investigate licensing and other regulatory issues associated with offering such services, including the current regulatory position in each of the participating European countries;
to research the practicality and feasibility of operating and managing a pan-European network of trusted service centre, providing services on a commercial basis.

These objectives will be met by carrying out work in two technical strands. The first of these is a study of schemes, looking at technical, commercial and regulatory issues. This study will investigate potential services and features which could be offered by networked trusted services over Europe. The second strand centres around the development and use of a research tool, based on a confidentiality scheme including a mechanism for government lawful access. Its implementation will involve the setting up of a network of trusted services. Assessment will be done with respect to feasibility and commercial aspects.

5.8 OPARATE (Operational and Architectural aspects of Trusted Services)

This project will concentrate on the investigation of the following specific areas relating to trusted service provision:

- how such service should be organised and operated to provide services effectively

[4] World Wide Wait

- how different trusted service systems may be combined or made interwork together, and in particular:
- how an trusted service network may be extended to provide confidentiality/key recovery service
- how interworking may be achieved between heterogeneous trusted service networks

The project will include the conduct of a field trial which will concentrate on investigating practical/operational aspects of trusted service provision. Assessment criteria will be developed to evaluate the results of the field trial.

6. Analysis of Results

Assessment of the outcome of the studies and the performance of the pilots is a task which each of the projects had to accomplish. In this paper a compressed review of a selected subset of leading schemes for Key Backup/Recovery Schemes is presented. The four selected schemes are:

- the Royal Holloway College scheme,
- the RecoverKey scheme from Trusted Information Systems,
- the SecureKees scheme from CertCo, and
- the SecureWay scheme from IBM.

The projects analysed the schemes in relation to 12 different attributes from which the results for the first and the last will be presented here.

Attribute:

A1: compatibility with use of confidentiality services on an international basis.

A12: ability to limit adverse resource and performance impacts.

Royal Holloway College Scheme

Goals:

The original paper[5] purports to accommodate two widely debated - and apparently conflicting - requirements: The necessity to (1) protect the confidentiality of electronic private or commercial communications by resorting to strong cryptography, whilst (2) preserving the right of legal authorities to intercept such communications in the interest of law enforcement. The paper further articulates a

[5] Royal Holloway Trusted Third Party Services. This proposed architecture for a public key infrastructure requires that the TTPs associated with pairs of communicating users share parameters and a secret key. Nigel Jefferies, Chris Mitchell, and Michael Walker, "A Proposed Architecture for Trusted Third Party Services," Royal Holloway, University of London, 1995.

list of 13 requirements which any scheme should satisfy, but recognises that not all of these are met by the RHC scheme. The analysis for the first and last attribute showed the following.

A1: The escrowing TTP is able to comply with a warrant to disclose a bilateral confidentiality key used for incoming or outgoing traffic between two parties, when one of them belongs to its own domain. Authorities are therefore technically able to intercept international traffic to/from one of their nationals, provided they are registered with one of the country's licensed TTPs. As with many escrow or recovery schemes, the weakness is that there is no technical means to prevent a user (e.g. mobile) to register with another country's TTP over which the local authority have no jurisdiction.

A12: Again, resource and performance impacts are very implementation-dependent. There is the issue of scaleability of the scheme to meet enterprise level needs for confidentiality services. For instance, it is not clear whether the certificate management and key refresh needs of the scheme will scale in an economical manner. In the instance of the Communications Electronic Security Group (CESG) proposed implementation, the projects assume that the Confidentiality Key Infrastructure (CKI) is simply integrated into an existing Public Key Infrastructure . This will still entail deploying the Certificate Management Authority (CMA) and top level CMA, establish frequent confidential channels between CKI User Agent and/or store a considerable number of frequently (daily) updated public key certificates.

Trusted Information Systems (TIS) scheme:

Goals:

The scheme offers an approach to key recovery that is independent of any particular key management infrastructure and any associated relationships between keys. It provides a means of creating cryptographically protected copies of those keys that are used to control the encryption process. These copies of the so-called session keys are retained in the user's system. Only when key recovery is invoked is it necessary to involve a third party key recovery centre to decipher one of these key copies.

A1:

The definition of the schemes makes no choices or assumptions regarding the nature of the applications employing key recovery, the geographical location of the parties (to such applications) or the security policies which these parties may wish to adopt. Specific implementations of the scheme will, however, seek to comply both with national regulatory frameworks and corporate security policies. Such compliance could result in restrictions on cross-border use of confidentiality services.

A12:

The major impact on normal operations come from the inclusion of the key recovery field in each network transfer. This can add 200 (or more) bytes to each transfer. In addition, there is the overhead of cryptographic computations in client workstations,

- which may add the equivalent of say 3-4 RSA public key operations times per message.

CERTCO Scheme

Goals:
The main goal of the CertCo scheme is to support companies in their own key recovery policy as well as providing a mechanism to enable law enforcement agencies to encryption keys. To avoid the need to trust a single key escrow agent the SecureKees scheme uses the method of fair cryptosystems developed by Silvio Micali which allow the keys to be split up into several parts and stored with different key escrow agents.

A1:
The scheme has been designed to be compliant with the export restrictions of the US and is claimed to have sufficient flexibility to be adaptable to the law enforcement requirements within different countries. Whether the usage of the scheme will be allowed in countries with usage restrictions like France and Russia is still an open question.

A12:
The scheme adds a message header containing the key recovery information to each message, thereby increasing the size of each message. The actual size of the key recovery information in the header is not specified in the documentation available in the public. Additionally the size is dependent on the number of escrow agents. As a whole the size of this information may be between 100 and 200 byte per message. There is also the overhead of additional encryption operations for parts of the key recovery information. A major factor for the operational costs are the number of escrow agents and the additional devices needed to operate the scheme.

SecureWay Scheme

Goals:
SecureWay is a cryptographic infrastructure developed by IBM. It contains the SecureWar key management framework, SecureWay key recovery and other components. SecureWay key recovery was in the Beta testing phase starting at 21 May 1997 with version number 1.0

The SecureWay Key Management Architecture is a set of layered security services suitable for use in operating systems as middleware in embedded applications, or provided as a component of cryptographic security tool-kits developed by IBM or other developers producing security solutions. The architecture focuses upon security in peer-to-peer, store-and-forward, and archival applications.

A1:
The issue is whether the scheme can be implemented in a way that satisfies the law enforcement agencies in both end user countries. The scheme itself makes no choices or assumptions regarding the location of Key Recovery Agents (KRA) or Key Requesting Party (KRP). It is not clear whether the key recovery profile features of SecureWay are powerful enough to support, for example, the generation of two key recovery fields, that is one for each country involved. With the information to hand, it appears that the scheme in its present from only supports the generation of a single recovery field and so all KRPs have to make use of the same set of KRAs.

A12:
The major cost is the generation and transmission of the data necessary for processing the key recovery field. This includes: exchange of the random seed S as a master secret between any pair of users, generation of random numbers S_i and secondary keys K_i, the encryption of each S_i using i-th KRA's public key and the encryption of session key K using every K_i.

6.1 Remarks on the analysis of results

The analyses showed that each scheme satisfied business needs to varying degrees. The projects do, however, express reservations concerning this analysis.

In conducting the analysis they were acutely aware that implementations of these schemes are very thin on the ground. For instance, the projects believes that the RHC and SecureWay schemes have only been deployed in demonstrations, field trials and beta test versions at present including the pilot of their own projects. In fact, the projects believe that only the TIS scheme has deployed commercially to any significant extent. This lack of extensive practical experience, especially with enterprise-scale situations, injects a degree of uncertainty into any assessment of the schemes' acceptability from a business perspective.

They have a related concern that there are few practical example of key recovery policies, coming either from industry or Administration background. Of course, they recognised that representatives of both camps have made numerous statements that have implications for policy development. But the have been unable to form a clear view as to which of the schemes provide an adequate level of support of recovery policy needs. At face value, the RecoverKey, SecureKees and SecureWay appear to offer a wide range of policy flexibility, although this is not so true of their current implementations. The RHC scheme appears somewhat less flexible but, if it were to satisfy practical needs, then this would be of little account.

However, on the basis of their analysis we consider that each scheme provides a technically feasible means for key recovery when used in combination with symmetric encryption algorithm. Each scheme does, of course, have its particular strengths and weaknesses in relation to the projects understanding of business needs.

Matters of cost, risks and liabilities are obviously important and are a clear underlying concern of their understanding of business needs. However, the analysis of scheme designs, as undertaken by some projects, is unable to shed much light on these issues although some of the other project sought to undertake such an analysis. Their finding was that it would require a more mature regulatory environment and product marketplace to address these matters effectively.

7. Exploitation of results

Part of the tasks given to the projects has been to review these schemes in the light of understanding of business requirements for key recovery. What follows are a number of issues that have become apparent to the projects during the course of their work.

Firstly, bearing in mind the relatively untried nature of these schemes they believe that they should express reservations about the extent of any of them is able to support enterprise -scale business needs. This is not to suggest that any of the schemes is necessarily inadequate in this respect. But they are concerned they have seen little evidence of scheme proponents, other than IBM, tackling the systems and key management issues that occur in large scale deployment of cryptographic technology. And neither have they seen much evidence of consideration of scaleability from a recovery protocol perspective.

Second, the projects doubt the extent to which the schemes address business concerns over the protection of escrowed key material. Starting on a positive note, the projects are of the opinion that each of the schemes could be implemented for intra-company use in a way that satisfies business demands for control over, and the physical location of escrowed material. However, when they look at inter-company communications or intra-company communications that cross national boundaries things start to get more complicated. In this scenario the RHC scheme would naturally involve Trusted Services in both domains. But it is also quite likely that national or corporate cryptography policies would also force a similar arrangement on users of the other schemes. And, of course, when there are Trusted Services in both domains, the implication is that escrowed material is, for all intents and purposes, accessible independently in either domain. This replication and distribution of sensitive material would, as the projects believe, heighten business anxieties over the potential for key compromise.

Third, they are concerned that piecemeal deployment of scheme implementations could raise barriers to interoperability at a technical level. Each scheme has its own requirements either for initialisation protocol exchanges between communicating parties or for protocol elements that need to be added to the "normal" communication stream. But what is the receiving party to do with protocol messages and elements it cannot interpret ? And what if it expected to receive protocol messages defined by a different scheme ? Irrespective of whether key recovery aims are served in such a case, it is clear that the prospects for successful communication are likely be jeopardised.

In raising these issues they are aware that they have reviewed the schemes from a business perspective. But they also recognise that much of the interest in key recovery is attributable to Administrations' wishes to find ways of balancing the interests of industry and law enforcement agencies as regards the use of strong encryption. However, they have not reviewed the schemes from a law enforcement perspective.

In conclusions, they note that the adoption (or not) of any of these key recovery schemes, or indeed other schemes, will be a result of market forces which are as much commercial and regulatory as they are technical. One result of regulatory developments could be the creation of a market for key recovery products. For instance, current US export regulations for cryptographic products are one driver for key recovery capabilities. But they are aware that the business community, while recognising the need for key recovery in some situations, is anxious about the costs and risks associated with its widespread use. Until issues of these kinds are resolved in a satisfactory manner they believe that interest in particular key recovery technologies will be limited. Nevertheless, the higher level regulatory and policy debates do need to be informed by an understanding of technology capabilities and limitations. The EC hopes that these projects prove to be a step towards satisfying this need.

EuroIntel '98 PROCEEDINGS 1 st Annual Conference & Exhibit European Intelligence & European Electronic Security: Open Source Solu - Link Page

Previous	Economic Intelligence
Next	Open Sources and Law Enforcement - Learning Curves and Pain Barriers

Return to Electronic Index Page