COUNCIL OF THE EUROPEAN UNION

Brussels, 12 October 2010

14558/10 ADD 1

LIMITE

COPEN 204 EJUSTICE 85 JURINFO 43

ADDENDUM TO NOTE

from:	General Secretariat of the Council
to:	Delegations
Subject:	Inception Report on the implementation of ECRIS

Delegations will find in the Annex the revised text of the Inception Report on the implementation of ECRIS, as resulting from the observations submitted by the Member States and examined during the discussions at the Working Party on Cooperation in Criminal Matters which met on 27 September 2010. Changes are indicated by underlined text as against the initial Inception Report.

ECRIS Technical Specifications

Glossary

Document Information

AUTHOR	iLICONN – Intrasoft International S.A.
OWNER	European Commission – DG Justice
ISSUE DATE	04/10/2010
VERSION	1.0
APPROVAL STATUS	Final

Authors

NAME	ACRONYM	ORGANISATION	ROLE
Nicholas YIALELIS	NYI	iLICONN – Intrasoft International S.A.	Manager Reviewer
Ludovic COLACINO DIAS	LCO	iLICONN – Intrasoft International S.A.	Main Author
Panos ATHANASIOU	PAT	iLICONN – Intrasoft International S.A.	Contributor
Daniel COMAN	DCO	iLICONN – Intrasoft International S.A.	Contributor
Ann Mennens	AME	iLICONN – Unisys Belgium	Reviewer
Marc Lombaerts	MLO	iLICONN – Unisys Belgium	Contributor

Document History

VERSION	DATE	AUTHOR	DESCRIPTION
0.1	20/08/2010	LCO	First draft
0.2	29/08/2010	LCO	Revision of all sections, consolidation of all comments received from all reviewers and contributors
0.3	02/08/2010	LCO	Minor corrections
0.4	03/08/2010	LCO	Addition of entries for Inception Phase Questionnaire
0.5	26/08/2010	LCO	Minor corrections
0.6	27/08/2010	LCO	Addition of entries for Inception Report document
0.7	10/09/2010	LCO/PAT	Addition of entries for Technical Architecture proposals
0.8	13/09/2010	LCO/MLO	Addition of entries for Security proposals
0.9	26/09/2010	LCO	Addition of entries for Technical Architecture and Security Analysis documents
1.0	04/10/2010	LCO	Update of entries together with the final version of the Inception Report document

The following table aims at providing definitions for most of the specific terms that are used throughout the *ECRIS Technical Specifications* project. The aim is to bring all contributors to the same level of understanding and avoid ambiguities. The terms are sorted alphabetically.

Term	Abbreviation/Acronym	Definition
	X. 509	An ITU-T standard for a public key infrastructure (PKI) for single sign-on (SSO) and Privilege Management Infrastructure (PMI). X.509 specifies, amongst other things, standard formats for public key certificates, certificate revocation lists, attribute certificates, and a certification path validation algorithm.
Address **R**esolution **P**rotocol	ARP	A computer networking protocol for determining a network host's link layer or hardware address, when only it's Internet Layer (IP) or Network Layer address is known.
ARP Poisoning		A technique used to attack an Ethernet wired or wireless network. ARP Spoofing may allow an attacker to sniff data frames on a local area network (LAN), modify the traffic, or stop the traffic altogether. The attack can only be used on networks that actually make use of ARP and not another method of address resolution.
Base64		A group of similar encoding schemes that represent binary data in an ASCII string format by translating it into a radix-64 representation. The Base64 term originates from a specific MIME content transfer encoding. Base64 encoding schemes are commonly used when there is a need to encode binary data that needs be stored and transferred over media that are designed to deal with textual data. This is to ensure that the data remains intact without modification during transport. Base64 is used commonly in a number of applications including email via MIME, and storing complex data in XML.
Canonicalisation		A process for converting data that has more than one possible representation into a "standard", "normal", or canonical form. This can be done to compare different representations for equivalence, to count the number of distinct data structures, to improve the efficiency of various algorithms by eliminating repeated calculations, or to

		make it possible to impose a meaningful sorting order.
Certification **A**uthority	CA	An entity that issues digital certificates for use by other parties.
Cipher Suite		The negotiated algorithm identifiers that are agreed during the SSL "handshake negotiation".
CIRCA		CIRCA is an extranet tool, developed under the European Commission IDA programme, and tuned towards Public Administrations' needs. It enables a given community (e.g. committee, working group, project group etc.) geographically spread across Europe (and beyond) to maintain a private space on the Internet where they can share information, documents, participate in discussion forums and benefit from various other functionalities. Such a private space is called an 'Interest Group'. The CIRCA tool is accessible at the following location: https://circa.europa.eu (Note: it is not to be confused with the CIRCABC tool which is a separate service)
Command Message		A Message used to reliably invoke a procedure in another application.
Confidentiality		As defined in ISO-17799: "ensuring that information is accessible only to those authorised to have access"
Convicting Member State		In the context of ECRIS, the "convicting Member State" is an EU Member State in which a conviction is handed down against a national of another Member State.
Conviction		(*According to the ECRIS legal basis – 2009/315/JHA*) Any final decision of a criminal court against a natural person in respect of a criminal offence, to the extent these decisions are entered in the criminal record of the convicting Member State.
Criminal Proceedings		(*According to the ECRIS legal basis – 2009/315/JHA*) The pre-trial stage, the trial stage itself and the execution of the conviction.
Criminal Record		(*According to the ECRIS legal basis – 2009/315/JHA*) The national register or registers recording convictions in accordance with national law.
Cross site scripting	XSS	A type of computer security vulnerability typically found in web applications that enables malicious attackers to inject client-side script into web pages viewed by other

		users. An exploited cross-site scripting vulnerability can be used by attackers to bypass access controls such as the same origin policy. Cross-site scripting carried out on websites were roughly 80% of all security vulnerabilities documented by Symantec as of 2007. Their impact may range from a petty nuisance to a significant security risk, depending on the sensitivity of the data handled by the vulnerable site, and the nature of any security mitigations implemented by the site's owner.
Cryptography		The principles, means and methods for securing information
Denial-of-Service	DoS	A denial-of-service attack (DoS attack) or distributed denial-of-service attack (DDoS attack) is an attempt to make a computer resource unavailable to its intended users. Although the means to carry out, motives for, and targets of a DoS attack may vary, it generally consists of the concerted efforts of a person or people to prevent an Internet site or service from functioning efficiently or at all, temporarily or indefinitely. Perpetrators of DoS attacks typically target sites or services hosted on high-profile web servers such as banks, credit card payment gateways, and even root name-servers. The term is generally used with regards to computer networks, but is not limited to this field, for example, it is also used in reference to CPU resource management. One common method of attack involves saturating the target (victim) machine with external communications requests, such that it cannot respond to legitimate traffic, or responds so slowly as to be rendered effectively unavailable. In general terms, DoS attacks are implemented by either forcing the targeted computer(s) to reset, or consuming its resources so that it can no longer provide its intended service or obstructing the communication media between the intended users and the victim so that they can no longer communicate adequately.
	DG	Directorate General
DIME		See ***D**irect **I**nternet **M**essage **E**ncapsulation*
Direct **I**nternet **M**essage **E**ncapsulation	DIME	A Microsoft-proposed internet standard in the early 2000s for the streaming of binary and other encapsulated data over the

		Internet. According to the IETF web site, the standard has been withdrawn and never made RFC status. However, Microsoft did at one time recommend DIME for transmitting files via Web services. It was also used in Java EE, but differences in the implementation of the protocol made it difficult.
Directory **A**ccess **P**rotocol	DAP	A computer networking standard promulgated by ITU-T and ISO in 1988 for accessing an X.500 directory service. DAP was intended to be used by client computer systems, but was not popular as there were few implementations of the full OSI protocol stack for desktop computers available to be run on the hardware and operating systems typical of that time. The basic operations of DAP: *Bind*, *Read*, *List*, *Search*, *Compare*, *Modify*, *Add*, *Delete* and *ModifyRDN*
Document Message		A Message, used to reliably transfer a data structure between applications.
Expression des **B**esoins et **I**dentification des **O**bjectifs de **S**écurité	EBIOS	EBIOS (In French: Expression des Besoins et Identification des Objectifs de Sécurité) is a methodology that allows to evaluate and act on risks relative to information systems security, and proposes a security policy adapted to the needs of an organization. This risk analysis method has been created by the DCSSI (Direction Centrale de la Sécurité des Systèmes d'Information), a department of the French Ministry of Defence. The 5 steps of the EBIOS method are: circumstantial study, security requirements, risk study, identification of security goals, and determination of security requirements.
ebXML **M**essage **S**ervice	ebMS	Standard for sending e-business messages. The specification, which builds on the SOAP web services message format, aims to act as a neutral format for carrying messages between different systems, such as between legacy systems and web services applications. It is designed to work with any communications protocol, and the content (or "payload") of messages carried over ebMS can be in any format. It interacts with other ebXML and OASIS standards, such as XML-Signature, Reliable Messaging Protocol and Collaboration Protocols and Agreements, to add security and reliability features.

ECRIS	ECRIS	Please refer to the definition of "**E**uropean **C**riminal **R**ecords **I**nformation **S**ystem".
ECRIS application		Synonym of "ECRIS software".
ECRIS Reference Implementation	ECRIS RI	The software implementation of ECRIS which is to be procured by the European Commission and produced based on the *ECRIS Technical Specifications*. It is a full standalone software product that can be installed in any Member State for exchanging data using the ECRIS formats, standards and protocols. ~~It features a user interface that allows end users to use all ECRIS functionality, independently of their infrastructure managing the criminal records.~~ The *ECRIS Reference Implementation* is meant to become an application that will comply with the *ECRIS Technical Specifications* and that will be able to send and receive (1) notifications of information on convictions and their subsequent alterations or deletions, (2) requests for information on convictions and (3) replies to such requests. It is intended to be only a messaging system, and not a replacement for any national criminal records register. When indicating that the ECRIS RI is a "standalone" product, it is meant that this messaging application will need to be able to run and be operated by Member States central authorities as such, without requiring major additional technical developments for integrating the ECRIS RI with the national criminal records register. Therefore it needs to have a user interface where end users can display the incoming notifications, incoming requests and incoming responses to requests as well as send outgoing notifications, outgoing requests and outgoing responses to requests, in compliance with the ECRIS detailed technical specifications. The ECRIS RI is to be considered as "standalone" from a purely technical point of view. Obviously, the ECRIS RI is not to be considered as "standalone" from a business point of view because the information is and remains in the national criminal records register. The ECRIS RI is only an intermediate messenger between the national criminal records register and the ECRIS applications of other

		Member States. In essence, the ECRIS RI has the same purpose than the current *NJR Reference Implementation*, with the exception that it implements the ECRIS technical specifications and not the NJR technical specifications.
ECRIS software		ECRIS is defined as a system composed of a piece of interconnection software and a communication infrastructure. The term "ECRIS software" refers specifically to the piece of interconnection software of ECRIS. Synonym of "ECRIS application".
ECRIS Technical Specifications		The technical specifications define the protocols, standards, formats and structures for the computerised exchanges of information extracted from criminal records between the Member States' central authorities. It is mainly constituted of a set of files that define the common technical interface between the ECRIS applications.
Electronic **B**usiness using e**x**tensible **M**ark-up **L**anguage	ebXML	A family of XML based standards sponsored by OASIS and UN/CEFACT whose mission is to provide an open, XML-based infrastructure that enables the global use of electronic business information in an interoperable, secure, and consistent manner by all trading partners. The ebXML architecture is a unique set of concepts; part theoretical and part implemented in the existing ebXML standards work.
Encryption		The process of transforming information using an algorithm (called cipher) to make it unreadable to anyone except those possessing special knowledge, usually referred to as a key.
Enterprise **A**rchitecture	EA	A rigorous description of the structure of an enterprise, its decomposition into subsystems, the relationships between the subsystems, the relationships with the external environment, the terminology to use, and the guiding principles for the design and evolution of an enterprise. This description is comprehensive, including enterprise goals, business functions, business process, roles, organisational structures, business information, software applications and computer systems.
Enterprise Integration		*Enterprise Integration* is a technical field of

		Enterprise Architecture, which focuses on the study of subjects like system interconnection, electronic data interchange, product data exchange and distributed computing environments, and it's possible other solutions.
Enterprise **I**ntegration **P**atterns	EIP	A number of design patterns for the use of enterprise application integration and message-oriented middleware. These patterns provide a consistent vocabulary and visual notation to describe large-scale integration solutions across many implementation technologies.
Enterprise **S**ervice **B**us	ESB	An event-driven and standards-based messaging-engine (the bus) which provides fundamental services for complex architectures. An ESB generally provides an abstraction layer on top of an implementation of an enterprise messaging system, which allows integration architects to exploit the value of messaging without writing code.
Etch		A new open source, cross-platform framework for building network services, first announced in May 2008 by Cisco Systems. Etch encompasses a service description language, a compiler, and a number of language bindings. It is intended to supplement SOAP and CORBA as methods of communicating between networked pieces of software, especially where there is an emphasis on portability, transport independence, small size, and high performance. Etch is designed to be easily incorporated into existing applications and systems, enabling a natural and easy transition to a service oriented architecture. It originally was derived from work on the Cisco Unified Application Environment.
European **C**riminal **R**ecords **I**nformation **S**ystem	ECRIS	(*According to the ECRIS legal basis – 2009/316/JHA*) ECRIS is a decentralised information technology system based on the criminal records databases in each Member State. It is composed of the following elements: (a) an interconnection software built in compliance with a common set of protocols enabling the exchange of information between Member States' criminal records databases; (b) a common communication infrastructure that provides an

		encrypted network.
Event Message		A Message used for reliable, asynchronous event notification between applications.
E**x**tensible **M**ark-up **L**anguage	XML	A set of rules for encoding documents in machine-readable form. It is defined in the XML 1.0 Specification produced by the W3C, and several other related specifications, all gratis open standards. XML's design goals emphasise simplicity, generality, and usability over the Internet. It is a textual data format, with strong support via Unicode for the languages of the world. Although XML's design focuses on documents, it is widely used for the representation of arbitrary data structures, for example in web services.
E**x**tensible **S**tyle-sheet **L**anguage **T**ransformations	XSLT	A declarative, XML-based language used for the transformation of XML documents into other XML documents. The original document is not changed; rather, a new document is created based on the content of an existing one. The new document may be serialised (output) by the processor in standard XML syntax or in another format, such as HTML or plain text. XSLT is often used to convert XML data into HTML or XHTML documents for display as a web page
Hyper**t**ext **T**ransfer **P**rotocol	HTTP	The Hypertext Transfer Protocol (HTTP) is a networking protocol for distributed, collaborative, hypermedia information systems. HTTP is the foundation of data communication for the World Wide Web
HTTPS Specification		See "**H**yper**t**ext **T**ransfer **P**rotocol **S**ecure" In the context of ECRIS, whenever HTTPS Specification is mentioned, it refers to the complete specification RFC 2818 "HTTPS over TLS"
Hyper**t**ext **T**ransfer **P**rotocol **S**ecure	HTTPS	A combination of the Hypertext Transfer Protocol with the SSL/TLS protocol to provide encryption and secure identification of the server.
Internet **C**ontrol **M**essage **P**rotocol	ICMP	The Internet Control Message Protocol (ICMP) is one of the core protocols of the Internet Protocol Suite. It is chiefly used by the operating systems of networked computers to send error messages—indicating, for instance, that a requested service is not available or that a host or router could not be reached
Injection		Also known as Code injection, is the exploitation of a computer bug that is caused by processing invalid data. Code

		injection can be used by an attacker to introduce (or "inject") code into a computer program to change the course of execution. The results of a code injection attack can be disastrous. For instance, code injection is used by some computer worms to propagate.
Integrity		A concept of consistency of actions, values, methods, measures, principles, expectations and outcomes. In the context of data communication it refers to the ability to verify whether the data received is identical to the data sent by the claimed sender.
Internet **P**rotocol Suite	IP	The Internet Protocol Suite is the set of communications protocols used for the Internet and other similar networks. It is commonly also known as TCP/IP. It consists of four layers. From lowest to highest, these are the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer.
Internet **P**rotocol **Sec**urity	IPSec	Internet Protocol Security (IPsec) is a protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session. IPsec also includes protocols for establishing mutual authentication between agents at the beginning of the session and negotiation of cryptographic keys to be used during the session. IPsec is an end-to-end security scheme operating in the Internet Layer of the Internet Protocol Suite. It can be used in protecting data flows between a pair of hosts (host-to-host), between a pair of security gateways (network-to-network), or between a security gateway and a host (network-to-host).[1] Some other Internet security systems in widespread use, such as Secure Sockets Layer (SSL), Transport Layer Security (TLS) and Secure Shell (SSH), operate in the upper layers of the TCP/IP model. Hence, IPsec protects any application traffic across an IP network. Applications do not need to be specifically designed to use IPsec. The use of TLS/SSL, on the other hand, must be designed into an application to protect the application protocols.
ISO 17799	ISO 17799	An information security standard published by the International Organisation for

		Standardisation (ISO) and by the International Electro-technical Commission (IEC) as **ISO/IEC 17799:2005**. It was subsequently renumbered ISO/IEC 27002:2005 in July 2007, bringing it into line with the other ISO/IEC 27000-series standards. It is entitled *Information technology - Security techniques - Code of practice for information security management*. The current standard is a revision of the version first published by ISO/IEC in 2000, which was a word-for-word copy of the British Standard (BS) 7799-1:1999. ISO/IEC 27002 provides best practice recommendations on information security management for use by those who are responsible for initiating, implementing or maintaining Information Security Management Systems (ISMS).
ISO 27033	ISO 27033	ISO 27033 is a multi-part standard. Much of it based upon or derived from the existing ISO 18028 standard. The first part, ISO/IEC 27033 1, was published in 2009 (revision of ISO 18028-1:2006). ISO/IEC 27033-1 defines/describes the concepts associated with, and provides management guidance on, network security. It is intended to provide a roadmap an overview of the other parts of the ISO 27033 standard. Part 1 also: • Offers guidance on identification and analysis of network security risks • Offers definition of network security requirements based on the above • Provides an overview of security controls to support network technical security architectures • Embraces other technical controls not limited to networks, thus linking to ISO 2700 and ISO 27002 • Explains a route to introduce quality network technical security architectures • Covers the implementation and operation of network security controls, and on-going monitoring and review
Java**S**cript **O**bject **N**otation	JSON	A lightweight text-based open standard designed for human-readable data interchange. It is derived from the JavaScript programming language for

		representing simple data structures and associative arrays, called objects. Despite its relationship to JavaScript, it is language-independent, with parsers available for virtually every programming language.
JSON-RPC	JSON-RPC	An RPC protocol encoded in JSON. It is a very simple protocol (and very similar to XML-RPC), defining only a handful of data types and commands. In contrast to XML-RPC or SOAP, it allows for bidirectional communication between the service and the client, treating each more like peers and allowing peers to call one another or send notifications to one another. It also allows multiple calls to be sent to a peer that may be answered out of order. A JSON invocation can be carried on an HTTP request where the content-type is application/json. Besides using HTTP for transport, one may use TCP/IP sockets. Using sockets, one can create much more responsive web applications with JSON-RPC, compared to polling data from a service with JSON-RPC over HTTP.
Judicial decision		This term is used throughout the *ECRIS Technical Specifications* project as a generic term referring to any decision taken by a competent judicial authority, such as the conviction of a person, a decision modifying a previous conviction, decisions affecting the execution of a penalty, decisions grouping previously sentenced sanctions, etc.
Kerberos		A computer network authentication protocol, which allows nodes communicating over a non-secure network to prove their identity to one another in a secure manner. Its designers aimed primarily at a client–server model, and it provides mutual authentication — both the user and the server verify each other's identity. **Kerberos** protocol messages are protected against eavesdropping and replay attacks.
Kinematics (Also choreography)		A form of service composition in which the interaction protocol between several partner services is defined from a global perspective. It specifies the expected messaging behaviour of the participants that will play it in terms of the sequencing and timing of the messages that they can consume and produce.
Lightweight **D**irectory	LDAP	An application protocol for querying and

Access **P**rotocol		modifying data of directory services implemented in Internet Protocol (IP) networks. A directory is a set of objects with attributes organised logically in a hierarchical manner. A simple example is the telephone directory, which consists of a list of names (of either persons or organisations) organised alphabetically, with each name having an address and phone number associated with it. A directory information tree often reflects various political, geographic, and/or organisational boundaries, depending on the model chosen. LDAP deployments today tend to use Domain Name System (DNS) names for structuring the topmost levels of the hierarchy. Deeper inside the directory might appear entries representing people, organisational units, printers, documents, groups of people or anything else that represents a given tree entry (or multiple entries). The latest version of LDAP is Version 3, which is specified in a series of Internet Engineering Task Force (IETF) Standard Track Requests for comments (RFCs) as detailed in RFC 4510.
Memorandum **o**f **U**nderstanding	MoU	A memorandum of understanding (MOU or MoU) is a document describing a bilateral or multilateral agreement between parties. It expresses a convergence of will between the parties, indicating an intended common line of action. It is often used in cases where parties either do not imply a legal commitment or in situations where the parties cannot create a legally enforceable agreement. It is a more formal alternative to a gentlemen's agreement.
Message		A message in its most general meaning is an object of communication. It is a vessel which provides information. Yet, it can also be this information. Therefore, its meaning is dependent upon the context in which it is used; the term may apply to both the information and its form.
Message Channel		A logical channel in a messaging system. That is, sending messages to different message channels provides an elementary way of sorting messages into different message types. For example, message queues and message topics are examples of

		message channels. A logical channel is *not* the same as a physical channel. There may be several different ways of physically realising a logical channel.
Message Endpoint		A client of the messaging system that the application can then use to send or receive messages.
Message Queue		A software-engineering component used for inter-process communication, or for inter-thread communication within the same process. They use a queue for messaging – the passing of control or of content. Group communication systems provide similar kinds of functionality.
Message **T**ransmission **O**ptimization **M**echanism	MTOM	MTOM is a W3C recommendation defining a method for efficiently sending binary data to and from *web services*. MTOM is usually used with XOP (XML-binary Optimized Packaging). In the lead up to the approval of MTOM as a W3C Recommendation, several different alternatives for handling binary data in SOAP messages were submitted to the W3C: SOAP with Attachments (SwA) and DIME attachments. MTOM supersedes those other proposals.
MTOM		**M**essage **T**ransmission **O**ptimization **M**echanism
Network of **J**udicial **R**egisters	NJR	NJR is a project of several EU Member States that aims at interconnecting their criminal/judicial registers on electronic base and, in this way, at speeding up the exchange of information about offenders and at improving prosecution. The main products of the NJR project are: - judicial agreements on the set of information to be exchanged, how to exchange it and how to represent and structure it - IT-technical agreements supporting the judicial agreements and materialised in a set of IT-technical specifications defining the exchange protocols, standards and exchange formats (in the form of WSDL, XSD and XML files) - Software implementations of the interconnection systems that respect the NJR technical specifications and allow effective criminal record data exchanges between the Member States administrations

Network of **J**udicial **R**egisters – **R**eference **I**mplementation	NJR-RI	The software implementation of NJR produced by the European Commission, based on the NJR technical specification. It is a full standalone software product that can be installed in any Member State for exchanging data using the NJR formats, standards and protocols. It features a user interface that allows end users to use all NJR functionality, independently of their infrastructure managing the criminal records.
Non-**R**epudiation of **O**rigin	NRO	A security feature that can be used to ensure that the original sender of information cannot successfully deny that he has sent the information.
Non-**R**epudiation of **R**eceipt	NRR	A security feature that can be used to ensure that the sender of information is protected against the denial of the receiver, who may claim that the information was never sent or that it was not sent on time.
Novell eDirectory (formerly known as **N**ovell **D**irectory **S**ervices, sometimes referred to as **N**etware **D**irectory **S**ervices)	NDS	An X.500-compatible directory service software product initially released in 1993 by Novell for centrally managing access to resources on multiple servers and computers within a given network. eDirectory is a hierarchical, object oriented database used to represent certain assets in an organisation in a logical tree, including people, positions, servers, workstations, applications, printers, services, and groups.
Offence		A violation or breach of the penal law. An offence can range from a simple misdemeanour (e.g. a traffic violation) to a felony (e.g. capital murder).
Open **S**ystems **I**nterconnection model	OSI	A standard for subdividing a communication system in layers. It consists of 7 layers (from bottom to top): the physical layer, the data link layer, the network layer, the transport layer, the session layer, the presentation layer and the application layer.
Open **W**eb **A**pplication **S**ecurity **P**roject	OWASP	A non-profit worldwide charitable organisation focused on improving the security of application software.
Payload		Material transmitted over a network (either computer or telecommunications network) includes both data and information that identifies the source and destination of the material. The *payload* is the actual data, or the cargo, carried by the headers. In the context of ECRIS, *payload* refers to the functional data contained in the XML messages to be transmitted between the

		Member States' central authorities, excluding the technical meta-data used for the transmission itself.
PEAR		See "PHP Extension and Application Repository"
Peer-**to**-**p**eer	PSP	*Peer-to-peer* (P2P) computing or networking is a distributed application architecture that partitions tasks or work-loads between peers. *Peers* are equally privileged, equipotent participants in the application. They are said to form a peer-to-peer network of nodes.
Penalty		A legal or official decree of punishment issued by a court or judge (such as for example a term of imprisonment).
PHP **E**xtension and **A**pplication **R**epository	PEAR	The PHP Extension and Application Repository, or PEAR, is a repository of PHP software code. Stig S. Bakken founded the PEAR project in 1999 to promote the re-use of code that performs common functions. The project seeks to provide a structured library of code, maintain a system for distributing code and for managing code packages, and promote a standard coding style. Though community-driven, the PEAR project has a PEAR Group which serves as the governing body and takes care of administrative tasks. Each PEAR code package comprises an independent project under the PEAR umbrella. It has its own development team, versioning-control and documentation.
Point **o**f **C**ontact	PoC	
Point-to-Point Channel		Is a *Message Channel* with the addition that a *Point-to-Point Channel* ensures that only one receiver consumes any given message.
Register		In the context of the *ECRIS Technical Specifications* project, the term *Register* refers specifically to the national criminal records archives operated by a Member State.
Remote **P**rocedure **C**all	RPC	An inter-process communication that allows a computer program to cause a subroutine or procedure to execute in another address space (commonly on another computer on a shared network) without the programmer explicitly coding the details for this remote interaction. That is, the programmer writes essentially the same code whether the subroutine is local to the executing program, or remote. When the software in question uses object-oriented principles,

		RPC is called **remote invocation** or **remote method invocation**. Note that there are many different (often incompatible) technologies commonly used to accomplish this
Representational **S**tate **T**ransfer	REST	A style of software architecture for distributed hypermedia systems such as the World Wide Web. Roy Fielding, the creator of the term REST, is one of the principal authors of the Hypertext Transfer Protocol (HTTP) specification versions 1.0 and 1.1. Conforming to the REST constraints is referred to as being 'RESTful'. In contrast to SOAP RPC over HTTP, REST does not encourage each application designer to define a new and arbitrary vocabulary of nouns and verbs (for example "getUsers()", "savePurchaseOrder(...)"), usually overlaid onto the HTTP 'POST' verb. This disregards many of HTTP's existing capabilities such as authentication, caching, content type negotiation, etc. and may leave the application designer re-inventing many of these features within the new vocabulary.
Reverse Proxy		A proxy server installed on a server network, usually in front of Web Servers. All connections coming towards the Web Servers are routed through the proxy, which may either deal with the request itself or pass the request to the main web servers.
Risk Assessment		Risk assessment is the identification of risks, their evaluation and the definition of measure to address them. See also Risk Treatment Plan.
Risk Treatment Plan		It is an output of the Risk Assessment and defines how to handle the risks identified.
Sanction		A sanction is a penalty or other means of enforcement used to provide incentives for obedience with the law, or with rules and regulations.
secured **T**rans **E**uropean **S**ervices for **T**elematics between **A**dministrations	sTESTA	An extension to the TESTA network, which delivers enhanced performance, stronger security and higher availability.
Security **A**ssertion **M**arkup **L**anguage	SAML	An XML-based standard for exchanging authentication and authorization data between security domains, that is, between an *identity provider* (a producer of assertions) and a *service provider* (a consumer of assertions). SAML is a product of the OASIS Security Services Technical Committee.

Service Contract		In the context of ECRIS, it is the WSDL file and technical artefacts on which it relies (such as XSD files) that define the set of common technical interfaces to be implemented by software systems for electronically exchanging messages and data.
Service **O**riented **A**rchitecture	SOA	A flexible set of design principles used during the phases of systems development and integration. A deployed SOA-based architecture will provide a loosely-integrated suite of *services* that can be used within multiple business domains. SOA also generally provides a way for consumers of services, such as web-based applications, to be aware of available SOA-based services. For example, several disparate departments within a company may develop and deploy SOA services in different implementation languages; their respective clients will benefit from a well understood, well defined interface to access them. XML is commonly used for interfacing with SOA services, though this is not required.
Simple **O**bject **A**ccess **P**rotocol	SOAP	A protocol specification for exchanging structured information in the implementation of Web Services in computer networks. It relies on eXtensible Mark-up Language (XML) as its message format, and usually relies on other Application Layer protocols (most notably Remote Procedure Call (RPC) and HTTP) for message negotiation and transmission. SOAP can form the foundation layer of a web services protocol stack, providing a basic messaging framework upon which web services can be built. This XML based protocol consists of three parts: an envelope (which defines what is in the message and how to process it), a set of encoding rules for expressing instances of application-defined data types, and a convention for representing procedure calls and responses.
SOAP **w**ith **A**ttachments	SwA	The term refers to the method of using Web Services to send and receive files using a combination of SOAP and MIME, primarily over HTTP. Note that SwA is not a new specification, but rather a mechanism for using the existing SOAP and MIME facilities

		to perfect the transmission of files using Web Services invocations.
Technical Specifications		In the context of the *ECRIS Technical Specifications* project, the *Technical Specifications* are a set of documents and files that define in details the common protocols, standards and formats to be respected by the software systems realising the exchanges of information extracted from criminal records between the competent authorities of the Member States.
	TAP	Turn-key access point of sTESTA
Trans **E**uropean **S**ervices for **T**elematics between **A**dministrations	TESTA	A telecommunications interconnection platform for secure information exchange between the European public administrations. TESTA is not a single network, but a network of networks, composed of the Euro-Domain backbone and Local Domain networks.
Transport **L**ayer **S**ecurity	TLS	A cryptographic protocol that provide security for communications over networks, such as the Internet
Unicode		A computing industry standard for the consistent representation and handling of text expressed in most of the world's writing systems. Developed in conjunction with the Universal Character Set standard and published in book form as *The Unicode Standard*, the latest version of Unicode consists of a repertoire of more than 107,000 characters covering 90 scripts, a set of code charts for visual reference, an encoding methodology and set of standard character encodings, an enumeration of character properties such as upper and lower case, a set of reference data computer files, and a number of related items, such as character properties, rules for normalisation, decomposition, collation, rendering, and bidirectional display order.
Universal **B**usiness **L**anguage	UBL	A library of standard electronic XML business documents such as purchase orders and invoices. UBL was developed by an OASIS Technical Committee with participation from a variety of industry data standards organisations. UBL is designed to plug directly into existing business, legal, auditing, and records management practices. It is designed to eliminate the re-keying of data in existing fax- and paper-

		based business correspondence.
Universal **D**escription, **D**iscovery and **I**ntegration	UDDI	A platform-independent, Extensible Markup Language (XML)-based registry for businesses worldwide to list themselves on the Internet. UDDI is an open industry initiative, sponsored by the Organisation for the Advancement of Structured Information Standards (OASIS), enabling businesses to publish service listings and discover each other and define how the services or software applications interact over the Internet. UDDI was originally proposed as a core Web service standard. It is designed to be interrogated by SOAP messages and to provide access to Web Services Description Language (WSDL) documents describing the protocol bindings and message formats required to interact with the web services listed in its directory.
User **I**nterface	UI	A place where interaction between humans and machines occurs. The goal of interaction between a human and a machine at the user interface is effective operation and control of the machine, and feedback from the machine which aids the operator in making operational decisions. In IT software, this term frequently refers to windows on the computer screen that allow a human user to interact with the software system.
Verdict		The findings of a jury on the issues of fact submitted to it for examination and trial; judgment.
Web **A**pplication **D**escription **L**anguage	WADL	An XML-based file format that provides a machine-readable description of HTTP-based web applications. These applications are typically REST web services. WADL is a W3C Member Submission. The purpose of WADL is to allow services on the internet (or any other IP network) to be described in a machine process-able way, to make it easier to create Web 2.0 style applications and create a dynamic way of creating and configuring services. Prior to this, it was necessary to go to an existing web service, study it and write the application manually. WADL can be thought of as the REST equivalent of Web Services Description Language version 1.1. Version 2.0 of WSDL can be used to describe REST Web services, thus competing with WADL.

Web Services		Web services are typically application programming interfaces (API) or "Web APIs" that are accessed via Hypertext Transfer Protocol (HTTP) and executed on a remote system hosting the requested services. These allow for software systems to support interoperable machine-to-machine interaction over a network.
Web **S**ervices **A**ddressing	WS-Addressing	Provides transport-neutral mechanisms to address Web services and messages. Specifically, it defines XML elements to identify Web service endpoints and to secure end-to-end endpoint identification in messages. This specification enables messaging systems to support message transmission through networks that include processing nodes such as endpoint managers, firewalls, and gateways in a transport-neutral manner.
Web **S**ervices **D**escription **L**anguage	WSDL	An XML format for describing network services as a set of endpoints operating on messages containing either document-oriented or procedure-oriented information. The operations and messages are described abstractly, and then bound to a concrete network protocol and message format to define an endpoint. Related concrete endpoints are combined into abstract endpoints (services). WSDL is extensible to allow description of endpoints and their messages regardless of what message formats or network protocols are used to communicate.
Web Services Endpoint		The *web services endpoint* is the piece of the software that actually implements the *web services*.
Web **S**ervices **P**olicy	WS-Policy	A specification that allows web services to use XML to advertise their policies (on security, Quality of Service, etc.) and for web service consumers to specify their policy requirements.
Web **S**ervices **S**ecurity	WS-Security WSS	A flexible and feature-rich extension to SOAP to apply security to Web services
XML	XML	Please refer to the definition of "E**x**tensible **M**ark-up **L**anguage".
XML Encryption	XML-Enc	A specification, governed by a W3C recommendation, which defines how to encrypt the contents of an XML element
XML **S**chema **D**efinition	XSD	One of several XML schema languages. It was the first separate schema language for XML to achieve Recommendation status by the W3C. Because of confusion between

		XML Schema as a specific W3C specification, and the use of the same term to describe schema languages in general, some parts of the user community referred to this language as **WXS**, an initial naming for W3C XML Schema, while others referred to it as **XSD**, an initial naming for XML Schema Document—a document *written in* the XML Schema language, typically containing the "xsd" XML namespace prefix and stored with the ".xsd" filename extension. In the draft of the next version, 1.1, the W3C has chosen to adopt XSD as the preferred name.
XML Signature	XML-Sig	A W3C recommendation that defines an XML syntax for digital signatures
XML-RPC	XML-RPC	An RPC protocol which uses XML to encode its calls and HTTP as a transport mechanism. It works by sending a HTTP request to a server implementing the protocol. The client in that case is typically software wanting to call a single method of a remote system. Multiple input parameters can be passed to the remote method, one return value is returned. The parameter types allow nesting of parameters into maps and lists, thus larger structures can be transported. Therefore XML-RPC can be used to transport objects or structures both as input and as output parameters. XML-RPC is simpler to use and understand than SOAP because it • allows only one method of method serialisation, whereas SOAP defines multiple different encodings • has a simpler security model • does not require (nor support) the creation of WSDL service descriptions, although XRDL provides a simple subset of the functionality provided by WSDL JSON-RPC is similar to XML-RPC.