# ETSI TR 103 690 V1.1.1 (2012-02)


**Lawful Interception (LI);**
**eWarrant Interface**

Reference
DTR/LI-00069

Keywords
eWarrant, interception, retention, security

***ETSI***

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

***Important notice***

Individual copies of the present document can be downloaded from:
http://www.etsi.org

The present document may be made available in more than one electronic version or in print. In any case of existing or perceived difference in contents between such versions, the reference version is the Portable Document Format (PDF). In case of dispute, the reference shall be the printing on ETSI printers of the PDF version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status. Information on the current status of this and other ETSI documents is available at
http://portal.etsi.org/tb/status/status.asp

If you find errors in the present document, please send your comment to one of the following services:
http://portal.etsi.org/chaircor/ETSI_support.asp

***Copyright Notification***

# Contents

# Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://ipr.etsi.org).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

# Foreword

This Technical Report (TR) has been produced by ETSI Technical Committee Lawful Interception (LI).

# 1 Scope

The present document presents a high-level description of an interface mechanism - the eWarrant Interface - for receipt of requests for measures producing real-time or stored information by an issuing authority possessing lawful authorization to initiate such a request. The eWarrant Interface is a generic, extensible interface intended to be fully compatible with all existing kinds of requests for these purposes - as well as support future ones, including local requirements and languages or character sets. The eWarrant Interface is not intended to replace existing implementation-specific mechanisms found, for example, in the Retained Data Handover Interface.

The present document describes an electronic interface. Annex B describes work flow for an eWarrant in different jurisdictions and a means for discovering related information. Annex C describes how this interface may be adapted and made interoperable for manual and legacy techniques. The present document provides a high-level description of the interface mechanism. It defines basic principles of interoperability, and provides recommendations for the types of data that are delivered. It provides a recommendation on the choice of data modelling languages, but the present document does not give a normative structure for the delivery of eWarrant messages. It is envisaged that a later Technical Specification will add the required details for a full implementation.

# 2 References

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the reference document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at http://docbox.etsi.org/Reference.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

## 2.1 Normative references

The following referenced documents are necessary for the application of the present document.

Not applicable.

## 2.2 Informative references

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] ETSI TS 102 657: "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".

[i.2] FIPS PUB 186-2: "Digital Signature Standard (DSS)".

[i.3] ETSI TS 102 042: "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates".

[i.4] Trusted Network Connect. Trusted Computing Group.

Integrity Measurement Collectors - TCG Version (IF-IMC, Specification ver. 1.2 Rev. 8, 5 February 2007).

Integrity Measurement Verifiers - TCG Version (IF-IMV Specification ver. 1.2 Rev. 8, 5 February 2007).

Trusted Network Connect Client-Server - TCG Version (IF-TNCCS TLV Binding Specification ver. 2.0 Rev. 16, 22 January 2010).

Trusted Network Connect Client-Server Statement of Health - TCG Version (IF-TNCCS-SOH TLV Binding Specification Ver. 2.0 Rev. 10, 23 January 2008).

Policy Enforcement Point - TCG Version (IF-PEP Protocol Bindings for RADIUS Specification ver. 1.1 Rev. 0.7, 5 February 2007).

Binding for SOAP - TCG Version (IF-MAP Specification ver. 2.0 Rev. 36, 30 July 2010).

Platform Trust Services Interface - TCG Version (IF-PTS Specification ver. 1.0 Rev. 1.0, 17 November 2006).

Clientless Endpoint Support Profile - TCG Version (CESP Specification ver. 1.0 Rev. 13, 18 May 2009).

[i.5] Trusted Platform Modules. Trusted Computing Group.

Design Principles - TCG Version (TPM Main, Part 1, Specification ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-2, 2009-05-15, Information technology - TPM - Part 2).

TPM Structures - TCG Version (TPM Main, Part 2. Specification ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-3, 2009-05-15, Information technology - TPM - Part 3).

Commands - TCG Version (TPM Main, Part 3, Specification ver. 1.2, Level 2 Rev. 103, 9 July 2007), ISO/IEC Version (11889-4, 2009-05-15, Information technology - TPM - Part 4).

The TPM 1.2 specifications have also been adopted as ISO/IEC 11889. Overview - TCG Version (N/A), ISO/IEC Version (11889-1, 2009-05-15, Information technology - TPM - Part 1).

[i.6] NIST SP 800-137: "Information Security Continuous Monitoring for Federal Information Systems and Organizations, December 2010".

[i.7] "CAESARS Framework Extension: An Enterprise Continuous Monitoring Technical Reference Architecture", NIST Interagency Report 7756, February 2011.

[i.8] ITU-T Recommendation X.1500 (04/2011): "Overview of Cybersecurity information exchange (CYBEX)".

[i.9] OASIS: "7 Steps to Electronic Filing with Electronic Court Filing 4.0".

[i.10] IETF RFC 2818: "HTTP Over TLS".

# 3 Definitions and abbreviations

## 3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

**authority:** any organization or official possessing the legal authority to issue or approve an eWarrant

NOTE: Authorities can be divided into Issuing Authority or Approving Authority.

**approving authority:** any organization or official possessing the legal authority to approve an eWarrant, frequently a judicial official

**Communications Service Provider (CSP):** generic description covering Access Provider, Service Provider and Network Operator

**eWarrant:** request for the production of information pursuant to the present document

**eWarrant interface:** physical and logical interface across which the production measures are requested from a CSP, and the results are delivered from a CSP to a designated location

NOTE: The interface also includes chained message flows associated with the request.

**Handover Interface 1 (HI1):** data interface supporting the receipt of eWarrant requests pursuant to the present document

**issuing authority:** any organization or official possessing the legal authority to issue an eWarrant, frequently a LEA official

**lawful authorization:** permission granted to an Issuing Authority under certain conditions to intercept specified telecommunications and requiring co-operation from a CSP

**Law Enforcement Agency (LEA):** organization or official authorized by a lawful authorization based on the applicable jurisdiction to request and receive the results of telecommunications interceptions or retained data

**trusted third party:** entity lawfully acting on behalf an authorized organization, LEA, or CSP for the purposes of facilitating the implementation of an eWarrant

## 3.2 Abbreviations

For the purposes of the present document, the following abbreviations apply:

| | |
|---|---|
| ASN.1 | Abstract Syntax Notation One |
| CSP | Communications Service Provider |
| EVCP | Extended Validation Certificates Policy |
| EVCP+ | enhanced Validation Certificate Policies |
| HI | Handover Interface |
| HTTP | HyperText Transfer Protocol |
| ICT | Information and Communications Technology |
| LEA | Law Enforcement Agency |
| LEMF | Law Enforcement Monitoring Facility |
| LI | Lawful Interception |
| OS | Operating System |
| TCG | Trusted Computing Group |
| TLS | Transport Layer Security |
| TNC | Trusted Network Connect |
| TPM | Trusted Platform Module |
| TTP | Trusted Third Party |
| XML | eXtensible Markup Language |

# 4 The eWarrant Interface

## 4.1 Reference model

In order to implement the eWarrant Interface capabilities, a one-port structure between the Issuing Authorities or Approving Authorities and Communications Service Providers (CSPs) is established such that eWarrant request information is logically distinguished from all other interfaces. The eWarrant requests and responses occur through HI1.

Figure 1 is the eWarrant Interface reference model for the request of production of real-time or stored information and a response indicating receipt and the action taken, including messages in a flow change described in clause 5.

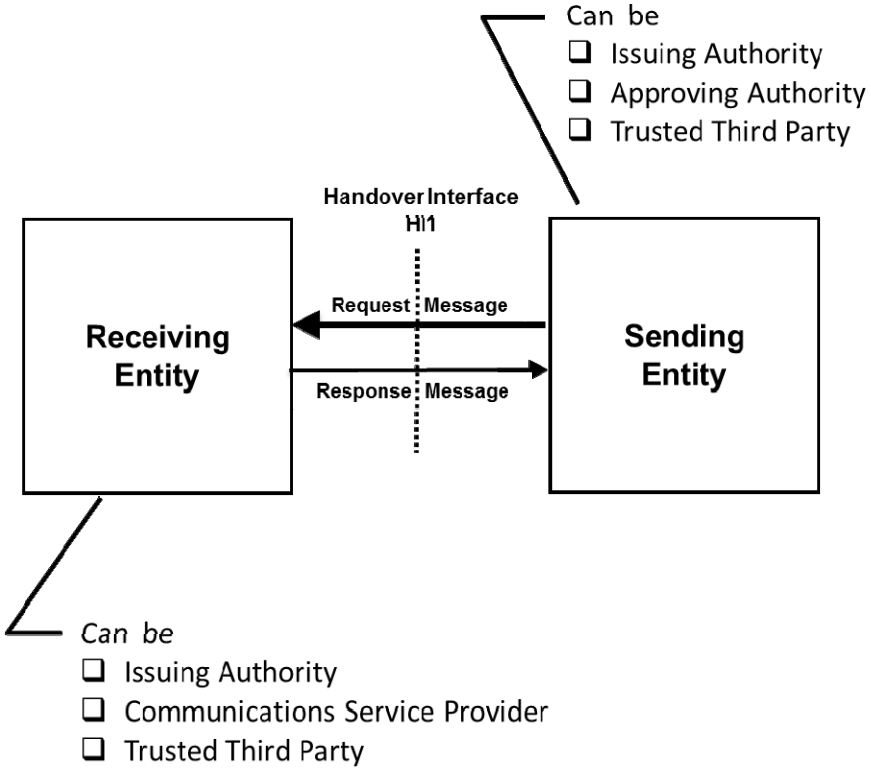



**Figure 1: Functional handover diagram showing eWarrant Interface**

Each of these two parties can be expanded to show some of their internal functions. This is not to prescribe how implementations of the present document must be organized, and is purely informational. Any internal functions and the interfaces between them are not part of the present document.

## 4.2 Outsourcing to Trusted Third Party

A CSP or Issuing Authority or Approving Authority may outsource some of their functions to a Trusted Third Party (TTP). It is a jurisdictional option whether or not outsourcing is allowed, or additional conditions apply.

## 4.3 The eWarrant Interface port

Handover Interface port 1 (HI1) supports eWarrant implementations by enabling administrative, request and response information to be conveyed in the form of messages from/to the Issuing Authority or Approving Authority and the organization at the CSP responsible for accepting eWarrants. The present document does not describe XML or ASN.1 encoded message content.

The HI1 interface may cross borders between countries. This possibility is subject to corresponding local/jurisdictional jurisdiction and/or inter-jurisdictional agreements.

## 4.4 Framework for the interface

The present document describes a framework that can apply to eWarrant implementations. It defines no services - only a means for specifying and conveying specific information as depicted in figure 2. These details consist of a *RequestMessage and Response Message*. The responses are intended only for simple acknowledgement of receipt of requests or approvals, as well as reporting significant error conditions.

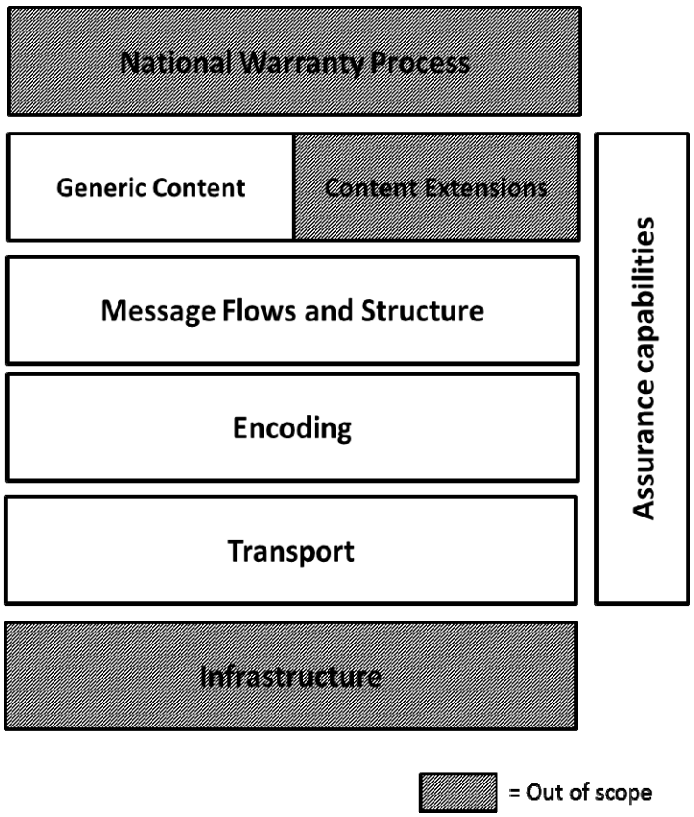



**Figure 2: Interface Framework**

The framework defines the message procedures, the basic information for each message, data exchange techniques, recommended security/assurance measures, including the means for requesting real-time or stored information across the interface. It is an open structure that will allow for national adaptations.

The present document is extensible - providing for national, local or special content extensions. Additional capabilities may be added in future. A version structure will allow for co-existence of different versions. Retained Data handling in some jurisdictions may be accomplished entirely using TS 102 657 [i.1] rather than the present document.

It is essential that authenticity of the eWarrant be capable of verification in a standalone environment (e.g. no connection to an on-line server is needed, with a root certificate being sufficient). The eWarrant can be transported and stored on any digital network or media. No particular data protocol or operating system is needed. Interoperability with paper-based media is described in annex C.

Security recommendations for eWarrant use provide for tamperproof capabilities, that is, to prevent any modifications to the eWarrant without this being noticeable.

Because the potential eWarrant life cycle - from the creation of an eWarrant (including the internal process between Judge and Police Officer) to the usage in the equivalent of a national supreme court may be 10 to 20 years, consideration is given to specification provisions that enable storage and use over long periods of time.

# 5 eWarrant interface messages and flows

This clause identifies the messages that are conveyed over the eWarrant interface. The message flows covered include the request and approval of production of real-time or stored information and a response indicating receipt and initiation of action.

## 5.1 Normal message flows

eWarrant interface message flows assume a single situation where there is a transport mechanism that supports a full two-way transport of messages between Approving or Issuing Authorities and CSPs for the purposes of initiating production as depicted in figure 3. The message flows may be either simple or chained as described in clause 5.2.

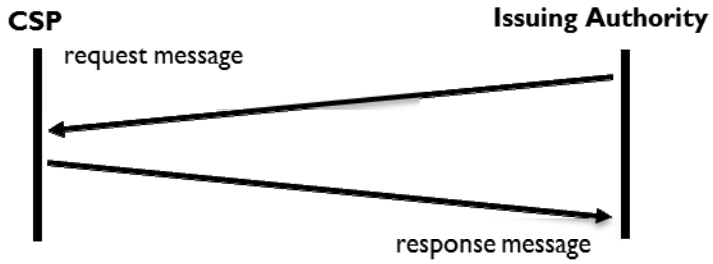



**Figure 3: Normal message flow**

## 5.2 Chained message flows

Entities will only response to the requesting entity. Acknowledgements received can be forwarded down the chain.

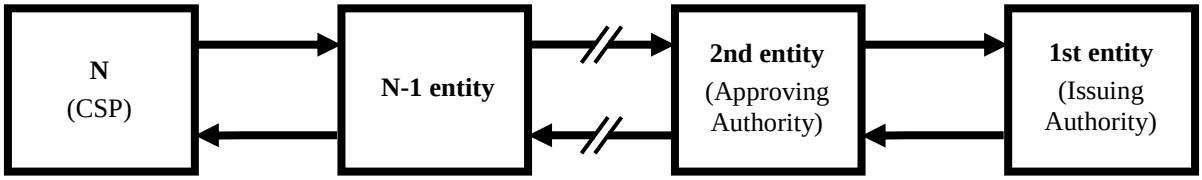



**Figure 4: eWarrant Message chain**

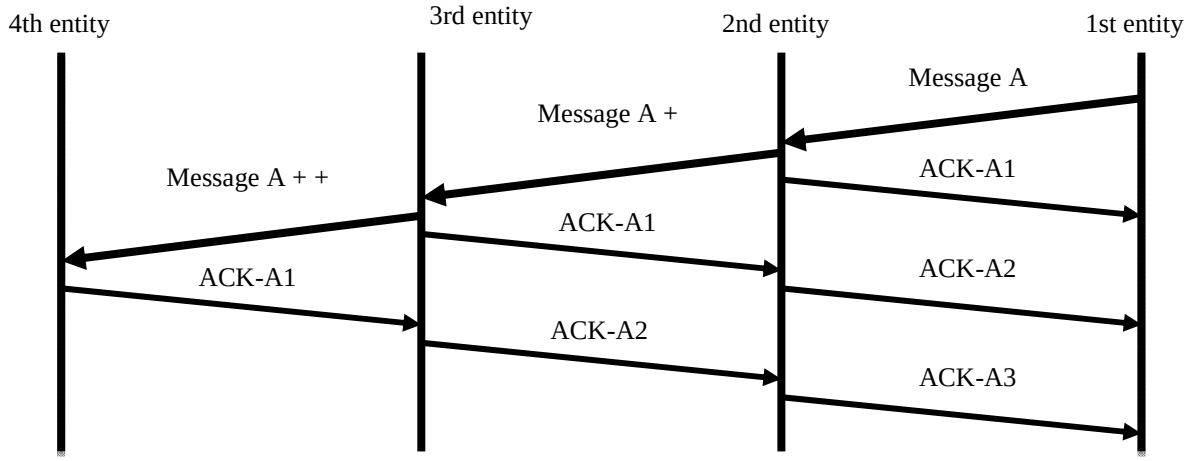
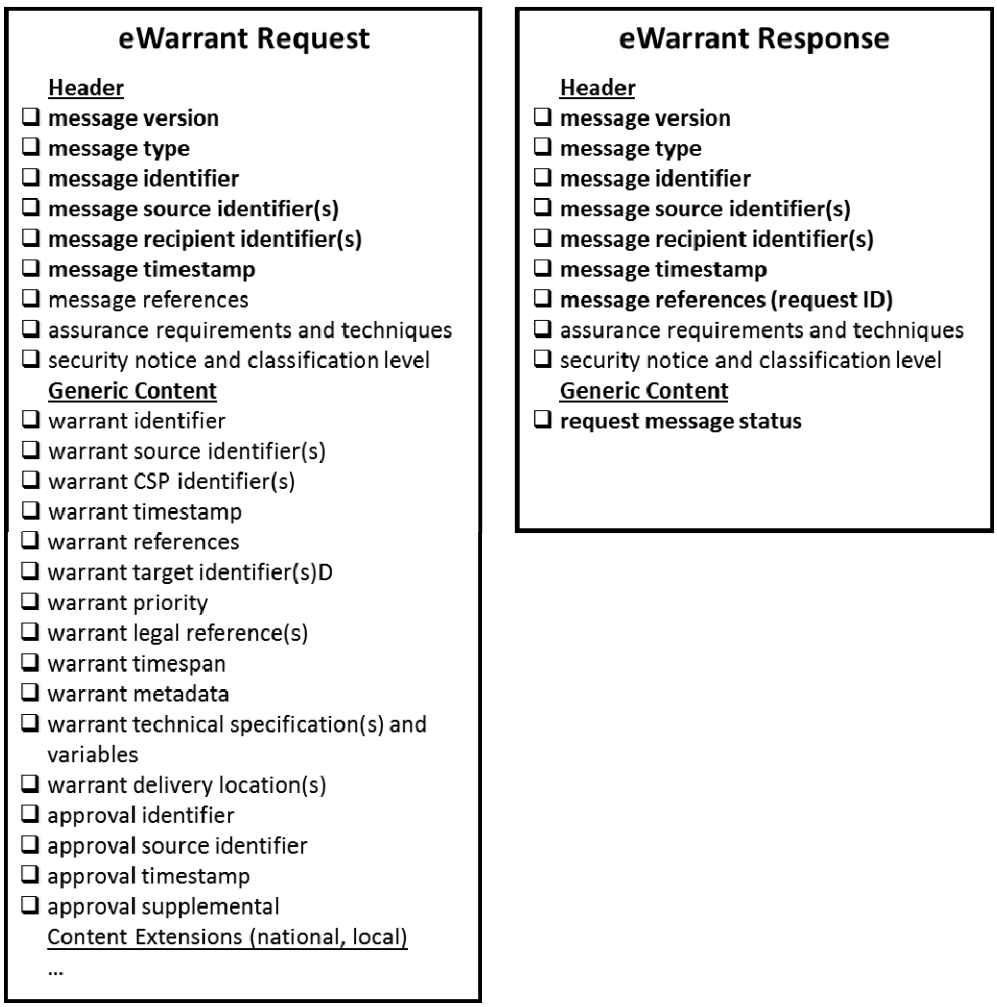



**Figure 5: eWarrant Message flow chain with layered acknowledgement**

# 6 eWarrant Interface messages

This clause describes the structure of messages conveyed in the flows at the eWarrant interface. The general form of the eWarrant Message and content are depicted in figure 6 and described in clauses 6.1 to 6.4.

The main body of the message contains elements for executing an eWarrant. Extensions or attachment can be added to show the required authorisations which may be nested. Attachments can be scanned paper documents.




Required elements are shown in bold.

**Figure 6: eWarrant Messages and their content**

## 6.1 Messages - common header

When writing message headers, the following information types should be considered.

### 6.1.1 *MessageVersion*

Each message has to contain a message version of the eWarrant schema or module used for encoding the information.

### 6.1.2 *MessageType*

Each message has to contain a Message type enumeration.

### 6.1.3 *MessageID*

Each message has to contain a globally unique, verifiable eWarrant message identifier.

### 6.1.4 *MessageSourceID*

Each message has to contain globally unique, verifiable identifier(s) sufficient to uniquely identify the specific entity that was the source of the message. In some instances, this may require a hierarchical layering of identifiers.

### 6.1.5 *MessageRecipientID*

Each message has to contain globally unique, verifiable identifier(s) sufficient to uniquely identify the specific entity that is the intended recipient of the message. In some instances, this may require a hierarchical layering of identifiers.

### 6.1.6 *MessageTimestamp*

Each message has to contain a timestamp indicating the time the message was sent.

NOTE: Each message will contain a timestamp and a qualifier indicating the type of timestamp used.

### 6.1.7 *MessageRef*

Each message may contain references to other MessageIDs.

### 6.1.8 *MessageAssurance*

Each message may contain enumerated assurance requirements and techniques for authenticating the entities associated with the message as well as the message itself.

### 6.1.9 *MessageSecurity*

Each message may contain security notices and classification levels recognizable by the recipient entity.

## 6.2 Generic Content for Request Messages

When writing Request Messages, the following sorts of information should be considered.

### 6.2.1 *WarrantID*

Each message may contain a globally unique, verifiable Warrant identifier. If this identifier is the same as the MessageID, it is omitted.

### 6.2.2 *WarrantSourceID*

Each message may contain globally unique, verifiable identifier(s) sufficient to uniquely identify the specific Issuing Authority entity that was the source of the Warrant. In some instances, this may require a hierarchical layering of identifiers. In most jurisdictions, this entity will be a LEA. If these identifier(s) are the same as the MessageSourceID, they may be omitted.

### 6.2.3 *Warrant*CspID

Each message may contain a globally unique, verifiable identifier(s) sufficient to uniquely identify the specific CSP entity that is requested to implement the Warrant. If these identifier(s) are the same as the MessageRecipientID, they may be omitted.

### 6.2.4 WarrantTimestamp

Each message may contain a timestamp indicating the time the Warrant was created. If this timestamp is the same as the Message timestamp, it is omitted.

NOTE: Each timestamp may contain a qualifier indicating the type of timestamp used.

### 6.2.5 *WarrantRef*

Each message may contain references to one or more other Warrants. If this reference is the same as the MessageRef, they may be omitted.

### 6.2.6 *WarrantTargetID*

Each message may describe one or more target entity identifiers in sufficient detail for the Warrant execution.

### 6.2.7 *WarrantPriority*

Each message may contain a priority.

### 6.2.8 *WarrantLegalRef*

Each message may contain a legal reference, i.e. an article of the law that provides the basis for the Warrant.

### 6.2.9 *WarrantTimespan*

Each message may contain an execution timespan which provides the time period during which the interception or preservation of information will occur.

### 6.2.10 *WarrantMetadata*

Each message may contain any other kinds of information necessary for executing the Warrant.

### 6.2.11 *WarrantTechspec*

Each message may contain any technical specifications and related variables necessary for executing the Warrant.

### 6.2.12 *WarrantDelivery*

Each message may contain sufficient address information for delivery of the information produced by the Warrant.

### 6.2.13 *ApprovalID*

Each message may contain a globally unique, verifiable Approval identifier. If this identifier is the same as the Message Identifier, it is omitted.

### 6.2.14 *ApprovalSourceID*

Each message may contain globally unique, verifiable identifier(s) sufficient to uniquely identify the specific Approval Authority entity that was the source of the Approval. In some instances, this may require a hierarchical layering of identifiers. In many jurisdictions, this entity will be a court. If these identifier(s) are the same as the MessageSourceID, they are omitted.

### 6.2.15 *ApprovalTimestamp*

Each message may contain a timestamp indicating the time the Approval was created. If this timestamp is the same as the Message timestamp, it is omitted.

NOTE: Each timestamp may contain a qualifier indicating the type of timestamp used.

### 6.2.16 *ApprovalSupplemental*

Each message may contain information associated with and supplementing the approval.

## 6.3 Generic Content for Response Messages

An eWarrant Response message is intended to provide an issuing or approving authority with a simple acknowledgement of receipt and disposition.

### 6.3.1 *RequestStatus*

Each Response Message has to provide acknowledgement of receipt and disposition.

# 7 Information exchange

## 7.1 General

An XML data exchange encoding technique is described in annex A, which contains the encoded data fields for XML implementations. Annex C contains the application of the encoding techniques to legacy media.

# 8 Security and Assurance Methods

The following security and assurances methods should be considered when implementing an eWarrant Interface mechanism.

## 8.1 Application level security and assurance

### 8.1.1 Digital signatures

The use of digital signatures for eWarrant interface messages and Production Warrants is recommended. Minimally, signatures should meet applicable provisions of FIPS PUB 186-2 [i.2], or TS 102 042 [i.3]. Use of Extended Validation Certificate (EVCP) or enhanced Validation Certificate (EVCP+) Policies as described in TS 102 042 [i.3] are preferred.

A layering of signatures for the information will be provided. This provides the capability to check the authorisation and authenticity of the individual information elements. This also provides the capability to leave out elements not required for the next step in the eWarrant process.

The information added to a message sent by an entity in the eWarrant interface will be signed. If applicable the message can also contain information from the previous entity. This information will contain also the original signature from the previous entity if authorisation and authenticity is required in the eWarrant process. The total information in the message that is sent on will be signed as well, see figure 7.

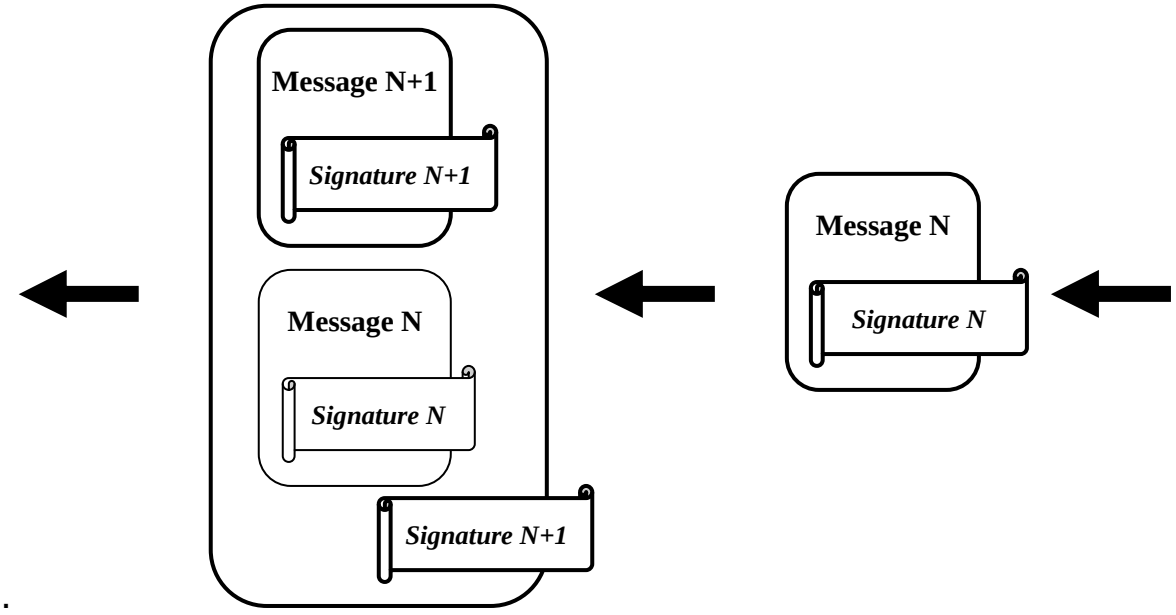



**Figure 7: Layering of signing information in the eWarrant process**

## 8.2 Transport, Connection and Device level security and assurance measures

Most practical implementations of such secure connections are at the hardware level, and sometimes at the software level. For securing these connections at the HI1 interface, it is recommended to consider the following security measures:

- Mutual authentication, i.e. the communicating parties have verified and confirmed each other's identities,
- Confidentiality, i.e. it is impossible to interpret the data by eavesdropping on the communication link,
- Integrity, i.e. any alteration or mutilation of the transported data can be detected.

At the transport level, the use of some manner of Transport Layer Security (TLS) for HTTP, as specified in RFC 2818 [i.10], as amended, is highly recommended - ideally using EVCP or EVCP+ policies. Additional continuous assurance measures described in clause 8.3 are also highly recommended.

At the connection level, use of ICT security operations to discover the state of Operating System (OS)-level and the application software used by the supporting network is highly recommended. For example, when systems lack OS security patches or antivirus signatures, reliable notification is crucial to containing the damage associated with network- based attacks. Making this appraisal requires reliable information that a connected system is in a particular state. Use of the Trusted Network Connect (TNC) suite of specifications is recommended to provide an open architecture for network access control and endpoint integrity at every network connection. [i.4].

At the device platform level, it is recommended to consider the use of computing and communications products with embedded Trusted Platform Modules (TPMs) - as defined by the specifications developed and maintained by the Trusted Computing Group (TCG), alongside with a protection profile for security evaluation against the Common Criteria [i.5].

## 8.3 Additional Assurance Measures

### 8.3.1 Continuous Security Monitoring

Additional assurance measures for the integrity of the eWarrant Interface can be instituted by implementing Information Security Continuous Monitoring capabilities - defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. See NIST SP 800-137 [i.6]. A well-designed continuous monitoring strategy for information security addresses both and incorporates processes to respond to findings with response actions as necessary. Continuous monitoring helps ensure ongoing situational awareness and control of the security of systems across the organization and ongoing knowledge of associated threats and vulnerabilities, despite inevitable changes to organizational information systems and their environments of operation.

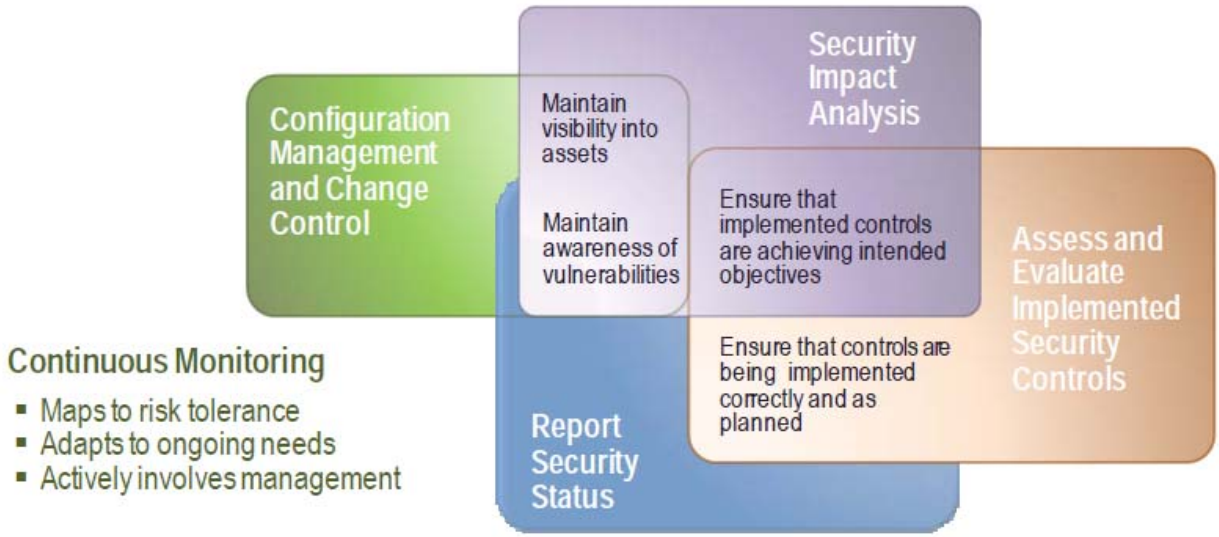



**Figure 8: Elements of an Effective Continuous Monitoring Program**

Implementation of high-level architectures and techniques for achieving these capabilities for law enforcement agency and other high assurance information exchange interfaces such as the eWarrant Interface are recommended; CAESARS Framework Extension [i.7] and ITU-T Recommendation X.1500 [i.8].

# Annex A:
# Encoded Data Elements

## A.1 Summary

### A.1.1 Use of this annex

This annex provides a suggestion of data types which may be present in an eWarrant message. It is envisaged that a later Technical Specification will provide a full normative definition and XML schema.

### A.1.2 Choice of data modelling language

It is recommended that eWarrant messages are encoded using XML. However the present document recommends the use of an ASN.1 representation for the presentation of the data structure to help readability.

The present document does not supersede national legislation or approved practices.

NOTE: In formal XML listings, the word OPTIONAL is used as defined in the XML languages for interoperability, and is not directly linked to national requirements.

### A.1.3 Overview

The data structure is broken down in the following way:

- Information that is present in all eWarrant Request messages (definitions in clauses 6.1, 6.2 and 6.3).
- Information that is present in all eWarrant Response messages (clause 6.4).

### A.1.4 Schematic representation of data

Here is an example of how the eWarrant data may be represented.

```
eWarrant Request message
├ MessageVersion
├ MessageType
├ MessageID
├ MessageSourceID
├ MessageRecipientID
├ MessageTimestamp
├ MessageRef
├ MessageAssurance
├ MessageSecurity
├ WarrantID
├ WarrantSourceID
├ WarrantCspID
├ WarrantTimestamp
├ WarrantRef
├ WarrantTargetID
├ WarrantPriority
├ WarrantLegalRef
├ WarrantTimespan
├ WarrantMetadata
├ WarrantTechspec
├ WarrantDelivery
├ ApprovalID
├ ApprovalSourceID
├ ApprovalTimestamp
├ ApprovalSupplemental
└ [Content Extensions]
```

```
eWarrant Response message
├ MessageVersion
├ MessageType
├ MessageID
├ MessageSourceID
├ MessageRecipientID
├ MessageTimestamp
├ MessageRef
├ MessageAssurance
├ MessageSecurity
└ RequestStatus
```

**Figure A.1: Schematic representation of the eWarrant messages**

## A.2 XML definitions

### A.2.1 General

#### A.2.1.1 Introduction

The present document does not contain any further details of an XML schema. It is anticipated that at a later time, a Technical Specification may be created with an XML schema attached, together with an object identifier tree.

# Annex B:
# Warrant process flow

a. An investigator may have the need for Lawful Interception or Retained Data information in an investigation. In order to get this information a Warrant is needed. To obtain a Warrant the investigator will provide a report instituting the Warrant.

   The report might contain:

   i. the investigation for which the information is needed,

   ii. which article in the law permits this Warrant,

   iii. why this information is needed,

   iv. target identification(s),

   v. provider(s) involved,

   vi. period,

   vii. signature.

b. The Warrant might be checked by a senior person, an expert or a coordinator in the investigators organisation (team) before it is sent to the Approving Authority.

c. The Approving Authority (e.g. Public Prosecutor or court) will check a request legally.

   If granted, Warrant parameters can be modified, added and removed.
   If not granted the Warrant is sent back with a motivation of the denial.

d. For some type of Warrants, where the Public Prosecutor checks the Warrant, additional approval of the court might be legally necessary.

   The court will check a Warrant legally.

   Additional information might be requested.
   If granted parameters from the Warrant can be modified, added and removed.
   If not granted the Warrant is sent back with a motivation of the denial.

e. Depending on the approval process described above:

   - the Warrant might be sent directly to the provider by the authorised authority or via the coordinator or the investigator. The request/warrant will also contain the delivery address for the information.

   - the delivery information for the Law Enforcement Monitoring Facility (LEMF) will be added to the Warrant. This might be done by the investigator, coordinator or LEMF, who then will send it on to the CSP.

f. The CSP might send a confirmation that the request is received or is accepted. The CSP will always send a reply if the request is rejected completely with the reason.

g. The CSP might provide, for example, administrative information on the status of the intercepted service after the request is accepted.

In a paper process it might be difficult for the involved parties to know the status in the process.

In a paper process, it might be necessary to print, fax and retype information several times. Although this ensures a careful legal process, it might administratively cause mistakes.

# Annex C:
# Interoperability with manual and legacy techniques

## C.1 Introduction

The eWarrant interface should be structured in a way that partial implementations can also be supported. Although the full implementation of the eWarrant interface might be the goal there will always be situation where this cannot be fulfilled. Reasons for this are:

- Migration: the implementation of a eWarrant interface is likely done by an evolution process rather than a revolution process.
- Change of participants: New parties in the warrant process should be able to participate although an eWarrant interface is not implemented yet.
- Availability: The warrant process is independent of the availability of the eWarrant interface. In the case of outage it should continue.
- In the case of emergencies access to the eWarrant process might not always be available.

## C.2 Description

Manual started requests can be imported/incorporated in the electronic process. Electronic started requests can be exported/extracted and handled manually. Manual techniques can include:

- use of phone, fax, paper mail or email for HI1.

For partly manual use the process is likely to be similar to the complete electronic process. This will mean that:

- the message flows (clause 5) are broadly followed;
- the content of the messages will broadly follow the messages defined in clause 6;
- lower layers (encoding, transport, etc.) (clause 7) in general would not be followed;
- in all steps of the process transformations between the manual and electronic domain are possible.

The transformation from the manual to the electronic domain could contain:

- the transformation into an electronic attachment to the eWarrant message;
- extraction of the manual presentation of the parameters into electronic domain;
- signing of the manual authorisation into the electronic domain.

The transformation from the electronic to the manual domain could contain:

- the transformation into manual messages (fax, paper, email);
- the transformation of electronic signatures into printable versions (checking might only be possible by back transformation into the electronic domain).

Implementation guidelines such as those of the OASIS Court Filing Technical Committee that describe integration of legacy paper based and contemporary XML based interfaces may be useful [i.9].

# Annex D:
# eWarrant requirements

## D.1 General

**Existing standards:** the eWarrant and eWarrant interface should use already existing mechanisms and standards if possible (e.g. ETSI, ISO, …).

**Open structure:** the eWarrant and eWarrant interface will have an open structure that will allow for (national) adaptations.

**Future proof:** changes can be made and new features can be added. A version structure will allow for co-existence of different versions.

**Flexibility:** the eWarrant and eWarrant interface support partial implementations. It may be used in a subset of the involved parties.

**Security:** authentication, integrity protection and confidentiality shall be supported.

## D.2 eWarrant

**Self containing:** it has to be possible to check the authenticity of the eWarrant in a standalone environment (e.g.: no connection to an on line server needed, root certificate can be enough).

**Media independent:** the eWarrant can be transported and stored on any digital network or media. No particular data protocol or operating system is needed.

**Life Cycle Information:** life cycle means from the creation of a warrant (internal process between Judge and Police Officer in the French system in the creation) to the usage in front of the equivalent of the supreme court/some international / European court sometime 10/20 years after its creation (problem of the storage and of the viewer maintenance on a long term basis).

**Authenticity:** the authenticity of the eWarrant and its signer can be checked throughout the interface.

## D.3 eWarrant interface

**Message:** the eWarrant interface supports messages from the issuing authority and approving authority to the CSP. For example request & approval messages and Information Request messages.
The eWarrant interface supports messages from the issuing authority to the approving authority.
The eWarrant interface supports messages from the CSP to the issuing authority and approving authority. For example Acknowledgement, Status Change, Information Message messages and Information Request messages.

**Workflow control:** authorized users have to be able to monitor the progress of the request and associated actions.

**Authenticity:** the authenticity of the eWarrant and its sender can be checked throughout the interface.

**Interoperability:** the eWarrant interface will be structured in a way that partial implementations can also be supported. Manual started requests can be imported/incorporated in the electronic process. Electronic started requests can be exported/extracted and handled manually.

**Migration:** the eWarrant interface allows for (seamless) migration with manual interfaces.

# Annex E:
# Change Request History

| Status of the present document<br>TR 103 690 eWarrant Interface | | |
|---|---|---|
| **TC LI approval date** | **Version** | **Remarks** |
| January 2012 | 1.1.1 | First publication of the TR after approval by ETSI/TC LI#29 (24-26 January 2012, Dun Laoghaire)<br><br>Version 1.1.1 prepared by Tony Rutkowski (Yaana Technologies) (rapporteur) |

# History

| Document history | | |
|---|---|---|
| V1.1.1 | February 2012 | Publication |
| | | |
| | | |
| | | |
| | | |