

ETSI TS 103 120 V1.17.1 (2024-08)



TECHNICAL SPECIFICATION

Lawful Interception (LI); Interface for warrant information



Reference

RTS/LI-00264

KeywordseWarrant, lawful disclosure, lawful interception,
warrant, warantry**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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Important notice

The present document can be downloaded from the
ETSI [Search & Browse Standards](#) application.

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the prevailing version of an ETSI deliverable is the one made publicly available in PDF format on [ETSI deliver](#).

Users should be aware that the present document may be revised or have its status changed,
this information is available in the [Milestones listing](#).

If you find errors in the present document, please send your comments to
the relevant service listed under [Committee Support Staff](#).

If you find a security vulnerability in the present document, please report it through our
[Coordinated Vulnerability Disclosure \(CVD\)](#) program.

Notice of disclaimer & limitation of liability

The information provided in the present deliverable is directed solely to professionals who have the appropriate degree of experience to understand and interpret its content in accordance with generally accepted engineering or other professional standard and applicable regulations.

No recommendation as to products and services or vendors is made or should be implied.

No representation or warranty is made that this deliverable is technically accurate or sufficient or conforms to any law and/or governmental rule and/or regulation and further, no representation or warranty is made of merchantability or fitness for any particular purpose or against infringement of intellectual property rights.

In no event shall ETSI be held liable for loss of profits or any other incidental or consequential damages.

Any software contained in this deliverable is provided "AS IS" with no warranties, express or implied, including but not limited to, the warranties of merchantability, fitness for a particular purpose and non-infringement of intellectual property rights and ETSI shall not be held liable in any event for any damages whatsoever (including, without limitation, damages for loss of profits, business interruption, loss of information, or any other pecuniary loss) arising out of or related to the use of or inability to use the software.

Copyright Notification

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI 2024.
All rights reserved.

Contents

Intellectual Property Rights	10
Foreword.....	10
Modal verbs terminology.....	10
Executive summary	10
Introduction	11
1 Scope	12
2 References	12
2.1 Normative references	12
2.2 Informative references.....	14
3 Definition of terms, symbols and abbreviations.....	14
3.1 Terms.....	14
3.2 Symbols.....	15
3.3 Abbreviations	15
4 Structure and model.....	16
4.1 Structure of the standard.....	16
4.2 Structure of the present document	17
4.3 Reference model.....	17
5 Message Exchange	18
6 Message Structure	19
6.1 Overview	19
6.2 MessageHeader	19
6.2.1 Overview	19
6.2.2 Structure.....	19
6.2.3 Version.....	20
6.2.4 EndpointID	20
6.2.5 Transaction Identifiers	21
6.3 Message Payload.....	21
6.3.1 Overview	21
6.3.2 Request Payload.....	21
6.3.3 Response Payload	22
6.4 Action Request and Responses.....	22
6.4.1 Overview	22
6.4.2 Action Requests	22
6.4.3 Action Responses.....	22
6.4.4 Action Identifiers	23
6.4.5 GET	23
6.4.6 CREATE.....	23
6.4.7 UPDATE	24
6.4.8 LIST.....	25
6.4.9 Action Unsuccessful Information	26
6.4.10 DELIVER	26
6.4.11 GETCSPCONFIG.....	27
6.4.11.1 Overview.....	27
6.4.11.2 TargetFormatTypeDefinition	27
6.4.11.3 TargetingConfiguration.....	28
6.4.11.4 SupportedLIWorkflowEndpoint.....	28
6.4.11.5 SupportedLPWorkflowEndpoint.....	29
7 Data Definitions	29
7.1 HIObject.....	29
7.1.1 Overview	29
7.1.2 ObjectIdentifier.....	30

7.1.3	Generation.....	30
7.1.4	AssociatedObjects.....	30
7.1.5	LastChanged	31
7.1.6	NationalHandlingParameters	31
7.2	AuthorisationObject	31
7.2.1	Overview	31
7.2.2	AuthorisationReference	32
7.2.3	AuthorisationLegalType	32
7.2.4	AuthorisationPriority	32
7.2.5	AuthorisationStatus.....	33
7.2.6	AuthorisationDesiredStatus	33
7.2.7	AuthorisationTimespan.....	34
7.2.8	AuthorisationCSPID	34
7.2.9	AuthorisationCreationTimestamp	34
7.2.10	AuthorisationServedTimestamp	34
7.2.11	AuthorisationApprovalDetails	34
7.2.12	AuthorisationFlags.....	35
7.2.13	AuthorisationJurisdiction.....	35
7.2.14	AuthorisationTypeOfCase	35
7.2.15	AuthorisationLegalEntity.....	36
7.2.16	AuthorisationManualInformation	36
7.3	DocumentObject.....	36
7.3.1	Overview	36
7.3.2	DocumentReference.....	37
7.3.3	DocumentName	37
7.3.4	DocumentStatus	37
7.3.5	DocumentDesiredStatus.....	37
7.3.6	DocumentTimespan	38
7.3.7	DocumentType	38
7.3.8	DocumentProperties.....	38
7.3.9	DocumentBody	39
7.3.10	DocumentSignature	39
7.4	NotificationObject.....	39
7.4.1	Overview	39
7.4.2	NotificationDetails.....	40
7.4.3	NotificationType.....	40
7.4.4	NewNotification	40
7.4.5	NotificationTimestamp	41
7.4.6	NationalNotificationParameters.....	41
7.4.7	StatusOfAssociatedObjects.....	41
7.5	TrafficPolicyObject	41
7.5.1	Overview	41
7.5.2	Order.....	42
7.6	TrafficRuleObject.....	42
7.6.1	Overview	42
7.6.2	TrafficCriteria.....	42
7.6.2.1	Overview.....	42
7.6.2.2	IPPolicyCriteria.....	42
7.6.2.2.1	Overview	42
7.6.2.2.2	BothDirections.....	43
7.6.2.3	MobileAccessPolicyCriteria.....	43
7.6.2.3.1	Overview	43
7.6.2.4	EthernetPolicyCriteria.....	43
7.6.2.4.1	Overview	43
7.6.2.4.2	BothDirections.....	44
7.6.2.5	RCSPolicyCriteria.....	44
7.6.3	Action	44
7.6.4	Parameters.....	45
7.6.4.1	Overview	45
7.6.4.2	Truncate Action Parameters	45
8	Task Objects.....	45

8.1	Overview	45
8.2	LITaskObject.....	46
8.2.1	Overview	46
8.2.2	Reference	47
8.2.3	Status	47
8.2.4	DesiredStatus	47
8.2.5	TimeSpan	48
8.2.6	TargetIdentifier	48
8.2.6.1	Overview	48
8.2.6.2	TargetIdentifierValues Field	48
8.2.6.3	FormatType	49
8.2.6.4	Task Service Type.....	49
8.2.7	DeliveryType	50
8.2.8	TaskDeliveryDetails	50
8.2.8.1	Overview	50
8.2.8.2	DeliveryDestination	50
8.2.8.3	DeliveryAddress.....	51
8.2.8.4	HandoverFormat	51
8.2.9	ApprovalDetails	51
8.2.10	CSPID	51
8.2.11	HandlingProfile.....	51
8.2.12	Flags.....	52
8.2.13	ListOfTrafficPolicyReferences	52
8.2.13.1	Overview	52
8.2.13.2	Order	52
8.3	LDTaskObject	52
8.3.1	Overview	52
8.3.2	Reference	53
8.3.3	Status	53
8.3.4	DesiredStatus	54
8.3.5	RequestDetails	54
8.3.5.1	Overview	54
8.3.5.2	RequestType.....	55
8.3.5.3	RequestValues.....	55
8.3.5.4	FormatType	56
8.3.5.5	Subtype	56
8.3.5.6	TargetIdentifierSubtype	57
8.3.6	DeliveryDetails	57
8.3.6.1	Overview	57
8.3.6.2	LDDeliveryDestination	58
8.3.6.3	HandoverFormat	58
8.3.7	Flags.....	58
8.3.8	AlternativePreservationReferences.....	59
8.4	LPTaskObject.....	59
8.4.1	Overview	59
8.4.2	Status	60
8.4.3	DesiredStatus	60
8.4.4	RequestDetails	61
8.4.4.1	General	61
8.4.4.2	Subtype	61
8.4.5	DesiredPreservationExpiration	61
8.4.6	PreservationExpiration.....	62
9	Transport and Encoding	62
9.1	Overview	62
9.2	Encoding.....	62
9.2.0	Encoding schemes	62
9.2.1	XML Schema.....	62
9.2.2	Error conditions	62
9.2.3	Message signing and encryption.....	62
9.2.4	JSON Schema	62
9.3	HTTP Transport	63

9.3.1	Use of HTTP	63
9.3.2	Client/Server architecture	63
9.3.3	HTTP Configuration	63
9.3.4	Transport security	63
9.4	Nationally-defined Transport	63
10	Delivery Object	63
10.1	Overview	63
10.2	DeliveryObject	64
10.2.1	Overview	64
10.2.2	Manifest	64
10.2.3	Delivery	65
Annex A (informative): Example usage scenarios for HI-1		67
A.1	Overview	67
A.2	Direct communication	67
A.3	Single "Central Authority"	67
A.4	Multiple Approving Authorities	68
A.4.1	Overview	68
A.4.2	"Serial" interaction	69
A.4.3	"Parallel" interaction	69
Annex B (informative): Example Template National Profile		71
B.1	Introduction	71
B.1.1	Overview	71
B.1.2	Structure of this annex	71
B.1.3	Checklist for National Profile authors	71
B.1.4	Details of the fictional national jurisdiction	73
B.2	Example National Profile	73
B.2.1	Approach and reference model	73
B.2.1.1	Overview	73
B.2.1.2	Warrants	73
B.2.1.3	Tasking Instructions	74
B.2.1.4	Representation by HI-1 Objects	74
B.2.2	Message Structure	74
B.2.2.1	Overview	74
B.2.2.2	Version information	74
B.2.2.3	Sender and Receiver Identifiers	75
B.2.2.4	LIST semantics	75
B.2.3	Data Definitions	75
B.2.3.1	Overview	75
B.2.3.2	Object Identifiers	75
B.2.3.3	Generic Object Fields	75
B.2.3.4	Authorisation Objects	75
B.2.3.5	Document Objects	76
B.2.3.6	Notification Objects	78
B.2.3.7	LITaskObjects	78
B.2.4	Transport and Encoding	79
B.2.5	Example XML	79
B.2.5.1	Introduction	79
B.2.5.2	Void	80
B.2.5.3	Void	80
B.2.5.4	Void	80
B.2.5.5	Void	80
B.2.5.6	Void	80
B.2.5.7	Void	80
Annex C (normative): ETSI Target Identifier and Request Value Format Definitions		81

C.1	Overview	81
C.2	Definitions	81
Annex D (normative): Error Codes		83
D.1	Detailed error codes	83
Annex E (normative): Approval Details		85
E.1	Overview	85
E.2	ApprovalType	85
E.3	ApprovalDescription	85
E.4	ApprovalReference	85
E.5	ApproverDetails	86
E.5.1	Overview	86
E.5.2	ApproverIdentity	86
E.5.3	ApproverContactDetails	86
E.6	ApprovalTimestamp	86
E.7	ApprovalIsEmergency	87
E.8	ApprovalDigitalSignature	87
E.8.1	Overview	87
Annex F (normative): Dictionaries		88
F.1	Overview	88
F.2	DictionaryEntry type	88
F.3	Definition and use of dictionaries	88
F.3.1	Overview	88
F.3.2	Owner	89
F.3.3	Name	89
F.3.4	Use of dictionaries	89
F.3.5	Machine-readable dictionary definitions	89
Annex G (normative): Drafting conventions for National Parameters		90
G.1	Overview	90
G.2	Drafting conventions	90
Annex H (normative): Workflow Profiles		91
H.1	Basic information about Workflow Profiles	91
H.2	Simple disclosure request Workflow Profile	91
H.2.1	Definition	91
H.2.2	Constraints on structure of objects	91
H.2.3	Constraints on the contents of objects	91
H.2.3.1	Authorisation Object contents	91
H.2.3.2	Task Object contents	91
H.2.3.3	Document Object contents	91
H.2.4	Constraints on flow of messages	92
H.3	Multi-endpoint Workflow Profile	92
H.3.1	Definition	92
H.3.2	Constraints on the structure and contents of objects	92
H.3.3	Message flow	93
H.3.3.1	Overview	93
H.3.3.2	Create Authorisation	93
H.3.3.3	Adding of documents and tasks	93

H.3.3.4	Submit Authorisation	93
H.3.3.5	Cancel Authorisation	93
H.4	Conversion between Simple and Multi-Endpoint Workflow Profiles (informative)	94
H.4.1	Description	94
H.4.2	Shim between a Simple Workflow LEA and a Multi-Endpoint at CSP	94
H.4.3	Shim between a Multi-Endpoint LEA and a Simple Workflow at CSP	94
H.5	Workflow Profile for the LI lifecycle.....	95
H.5.1	Overview and scope	95
H.5.2	Common procedures and definitions	95
H.5.2.1	Object Model	95
H.5.2.2	Common procedure.....	96
H.5.2.2.1	Overview	96
H.5.2.2.2	LEA Request	96
H.5.2.2.3	Initial CSP Response	96
H.5.2.2.4	CSP review and action	97
H.5.2.3	Common constraints	97
H.5.2.3.1	Overview	97
H.5.2.3.2	Authorisation Object	97
H.5.2.3.3	LI Task Object	97
H.5.2.3.4	Document Object	97
H.5.3	New Authorisation Workflow Endpoint.....	98
H.5.3.1	Description.....	98
H.5.3.2	Message flow	98
H.5.3.3	Message contents	98
H.5.3.4	Constraints on objects.....	98
H.5.4	Authorisation Extension Workflow Endpoint	98
H.5.4.1	Description.....	98
H.5.4.2	Message flow	98
H.5.4.3	Message contents	98
H.5.4.4	Constraints on objects	99
H.5.4.4.1	Authorisation Object	99
H.5.4.4.2	LITask Objects	99
H.5.4.4.3	Document Objects	99
H.5.5	Authorisation Cancellation Workflow Endpoint	99
H.5.5.1	Description.....	99
H.5.5.2	Message flow	99
H.5.5.3	Message contents	99
H.5.5.4	Constraints on objects.....	100
H.5.5.4.1	Authorisation Object	100
H.5.5.4.2	Document Objects	100
H.5.6	Task Addition Workflow Endpoint	100
H.5.6.1	Description.....	100
H.5.6.2	Message flow	100
H.5.6.3	Message contents	100
H.5.6.4	Constraints on objects.....	100
H.5.6.4.1	LITask Object	100
H.5.6.4.2	Document Objects	100
H.5.7	Task Cancellation Workflow Endpoint	101
H.5.7.1	Description.....	101
H.5.7.2	Message flow	101
H.5.7.3	Message contents	101
H.5.7.4	Constraints on objects.....	101
H.5.7.4.1	LITask Object	101
H.5.7.4.2	Document Objects	101
H.5.8	Change of Delivery Endpoint.....	101
H.5.8.1	Description.....	101
H.5.8.2	Message flow	101
H.5.8.3	Message contents	101
H.5.8.4	Constraints on objects.....	102
H.5.8.4.1	LITask Object	102

H.5.8.4.2	Document Objects.....	102
H.6	Workflow Profile for the LP lifecycle.....	102
H.6.1	Overview and Scope.....	102
H.6.2	Common procedures and definitions.....	103
H.6.2.1	Object Model.....	103
H.6.2.2	Common procedure.....	103
H.6.2.2.1	Overview.....	103
H.6.2.2.2	LEA Request.....	103
H.6.2.2.3	Initial CSP Response.....	104
H.6.2.2.4	CSP review and action.....	104
H.6.2.3	Common constraints.....	104
H.6.2.3.1	Overview.....	104
H.6.2.3.2	Authorisation Object.....	104
H.6.2.3.3	LP Task Object.....	104
H.6.2.3.4	Document Object.....	104
H.6.3	New Preservation Workflow Endpoint.....	105
H.6.3.1	Description.....	105
H.6.3.2	Message contents.....	105
H.6.3.3	Constraints on objects.....	105
H.6.4	Preservation Extension Workflow Endpoint.....	105
H.6.4.1	Description.....	105
H.6.4.2	Message contents.....	105
H.6.4.3	Constraints on objects.....	106
H.6.4.3.1	Authorisation Object.....	106
H.6.4.3.2	LP Task Objects.....	106
H.6.4.3.3	Document Objects.....	106
H.6.5	Preservation Cancellation Workflow Endpoint.....	106
H.6.5.1	Description.....	106
H.6.5.2	Message contents.....	106
H.6.5.3	Constraints on objects.....	106
H.6.5.3.1	Authorisation Object.....	106
H.6.5.3.2	Document Objects.....	107
Annex I (normative):	Signing JSON documents.....	108
I.1	Overview.....	108
I.2	Signing procedure.....	108
I.3	Verification procedure.....	108
I.4	Worked example.....	109
I.5	Implementation guidance.....	110
I.5.1	Guidance on IETF RFC 7515 and IETF RFC 7797.....	110
I.5.2	Guidance on implementing clauses I.2 and I.3.....	110
Annex J (informative):	Bibliography.....	111
Annex K (informative):	Change history.....	112
History.....		114

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 (<https://ipr.etsi.org/>).

Pursuant to the ETSI Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM®** and the GSM logo are trademarks registered and owned by the GSM Association.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Lawful Interception (LI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](#) (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Executive summary

The present document defines a protocol for the electronic exchange of legal and technical information for the purposes of establishing and managing lawfully required actions (e.g. Lawful Interception). In this phase, the present document is intended to provide the underlying functionality for HI-1, as defined in the ETSI LI Reference Model, and it has been designed for applicability beyond LI in future phases.

Introduction

The present document was constructed in multiple phases. The first phase of the present document consisted of a reference architecture. It was created by investigating current practices and procedures across TC LI. It makes clear the distinction between the process of communicating with the Communication Service Provider to inform them about the interception details (commonly called "tasking") and also communication among government/law enforcement/judiciary to establish the warrant (commonly called "warrantry"). The second phase of the present document provided a standardized detailed interface based on the architecture in the first phase, in particular for LI. The present document anticipates that future phases will add other requests for legal action.

1 Scope

The present document defines an electronic interface between two systems for the exchange of information relating to the establishment and management of lawful required action, typically Lawful Interception. Typically this interface would be used between on one side, a Communications Service Provider and on the other side, a Government or Law Enforcement Agency who is entitled to request a lawful action.

The present document is a specific and detailed example of one particular Warrantry interface for eWarrants [i.1].

The ETSI reference model for LI (ETSI TS 102 232-1 [i.11]) defines three interfaces between law enforcement and CSPs, called HI-1, HI-2 and HI-3. The protocol defined in the present document is designed to provide a large part of the functionality for HI-1. It is not designed to be used for HI-2 (delivery of intercept related information) or HI-3 (delivery of communications content). The protocol designed in the present document may also be used for interfaces which require structured exchange of information relating to the establishment and management of Lawful Interception. The general view is that the HI-1 concept can also be used for other legal actions than LI. For that reason the present document could, besides LI, also be applied for retained data requests, seized data requests, data preservation orders and other similar legal requests.

2 References

2.1 Normative 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 referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at <https://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.

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

- [1] Void.
- [2] Void.
- [3] [IETF RFC 4122](#): "A Universally Unique IDentifier (UUID) URN Namespace".

NOTE: Obsoleted by IETF RFC 9562.

- [4] [W3C® Recommendation 26 November 2008](#): "Extensible Markup Language (XML) 1.0".
- [5] [IETF RFC 2818](#): "HTTP over TLS".

NOTE: Obsoleted by IETF RFC 9110.

- [6] [IETF RFC 4279](#): "Pre-Shared Key Ciphersuites for Transport Layer Security (TLS)".
- [7] [ETSI TS 103 280](#): "Lawful Interception (LI); Dictionary for common parameters".
- [8] [IETF RFC 1738](#): "Uniform Resource Locators (URL)".

NOTE: Obsoleted by IETF RFC 4248 and IETF RFC 4266.

- [9] [IETF RFC 2045](#): "Multipurpose Internet Mail Extensions (MIME) Part One: Format of Internet Message Bodies".
- [10] [IETF RFC 2046](#): "Multipurpose Internet Mail Extensions (MIME) Part Two: Media Types".
- [11] [IETF RFC 1321](#): "The MD5 Message-Digest Algorithm".

- [12] W3C®: "[HTML 5.2](#)".
- [13] [IEEE POSIX 1003.1™-2017](#): "IEEE Standard for Information Technology -- Portable Operating System Interface (POSIX™) Base Specifications, Issue 7".
- [14] [ISO 3166-1](#): "Codes for the representation of names of countries and their subdivisions -- Part 1: Country code".
- [15] [ETSI TS 102 232-2](#): "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 2: Service-specific details for messaging services".
- [16] [ETSI TS 102 232-3](#): "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 3: Service-specific details for internet access services".
- [17] [ETSI TS 102 232-4](#): "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 4: Service-specific details for Layer 2 services".
- [18] [ETSI TS 102 232-5](#): "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 5: Service-specific details for IP Multimedia Services".
- [19] [ETSI TS 102 232-6](#): "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 6: Service-specific details for PSTN/ISDN services".
- [20] [ETSI TS 102 232-7](#): "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 7: Service-specific details for Mobile Services".
- [21] [ETSI TS 123 501](#): "5G; System architecture for the 5G System (5GS) (3GPP TS 23.501)".
- [22] [ETSI TS 102 657](#): "Lawful Interception (LI); Retained data handling; Handover interface for the request and delivery of retained data".
- [23] [IETF RFC 6234](#): "US Secure Hash Algorithms (SHA and SHA-based HMAC and HKDF)".
- [24] [ETSI TS 103 707](#): "Lawful Interception (LI); Handover Interface for HTTP delivery".
- [25] [IETF RFC 6530](#): "Overview and Framework for Internationalized Email".
- [26] [IANA](#): "Hash Function Textual Names".
- [27] [IETF RFC 8259](#): "The JavaScript Object Notation (JSON) Data Interchange Format".
- [28] [IETF Draft draft-bhutton-json-schema-01](#): "JSON Schema: A Media Type for Describing JSON Documents".
- [29] [IETF RFC 7515](#): "JSON Web Signature (JWS)".
- [30] [IETF RFC 7518](#): "JSON Web Algorithms (JWA)".
- [31] [IETF RFC 7797](#): "JSON Web Signature (JWS) Unencoded Payload Option".
- [32] [IETF RFC 4648](#): "The Base16, Base32, and Base64 Data Encodings".
- [33] [ETSI TS 103 976](#): "LEA support services; Interface for Lawful Disclosure of vehicle-related data".
- [34] [GSMA SGP.02 v4.2](#): "Remote Provisioning Architecture for Embedded UICC Technical Specification".
- [35] [ETSI TS 103 705](#): "Lawful Interception (LI); Data Structures for Lawful Disclosure".

2.2 Informative 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 referenced document (including any amendments) applies.

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

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 TR 103 690: "Lawful Interception (LI); eWarrant Interface".
- [i.2] IETF RFC 3261: "SIP: Session Initiation Protocol".
- [i.3] IETF RFC 3966: "The tel URI for Telephone Numbers".
- [i.4] IETF RFC 3508: "H.323 Uniform Resource Locator (URL) Scheme Registration".
- [i.5] IETF RFC 4282: "The Network Access Identifier".
- [i.6] ETSI TS 123 003: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; Numbering, addressing and identification (3GPP TS 23.003)".
- [i.7] ETSI TS 124 229: "Digital cellular telecommunications system (Phase 2+) (GSM); Universal Mobile Telecommunications System (UMTS); LTE; 5G; IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3 (3GPP TS 24.229)".
- [i.8] IEEE Std 802TM-2001: "IEEE Standard for Local and Metropolitan Area Networks: Overview and Architecture".
- [i.9] Recommendation ITU-T E.164: "The international public telecommunication numbering plan".
- [i.10] Recommendation ITU-T E.212: "The international identification plan for public networks and subscriptions".
- [i.11] ETSI TS 102 232-1: "Lawful Interception (LI); Handover Interface and Service-Specific Details (SSD) for IP delivery; Part 1: Handover specification for IP delivery".
- [i.12] GSMA RCC.07: "Rich Communication Suite - Advanced Communications Services and Client Specification".

3 Definition of terms, symbols and abbreviations

3.1 Terms

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

base64url: base64 encoding using the URL- and filename-safe character set as defined in IETF RFC 4648 [32] Section 5, without trailing padding per IETF RFC 4648 [32], Section 3.2

NOTE See also IETF RFC 7515 [29], Appendix C.

Communications Service Provider (CSP): Network Operator (NWO) or Access Provider (AP) who is obliged by law to perform a lawful action in response to a Warrant (e.g. perform Lawful Interception)

Law Enforcement Agency (LEA): government or Law Enforcement Agency who is entitled to request a lawful action

shim: extra piece of software or software modification inserted into a process in order to help with compatibility or add additional functionality

warrant: legal authorisation to perform an action or set of actions

3.2 Symbols

Void.

3.3 Abbreviations

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

AP	Access Provider
API	Application Programming Interface
APN	Access Point Name
ASN	Abstract Syntax Notation
CC	Content of Communication
CGI	Cell Global ID
CIDR	Classless InterDomain Routing
CSP	Communication Service Provider
CSPID	Communication Service Provider Identifier
CYBER	Cybersecurity Technical Committee (ETSI)
DNN	Data Network Name
ECGI	E-UTRAN Cell Global ID
EID	eUICC Identifier
ERE	Extended Regular Expression
eUICC	Embedded Universal Integrated Circuit Card
FQDN	Fully Qualified Domain Name
FTP	File Transfer Protocol
HI	Handover Interface
HI-1	Handover Interface 1
HI-2	Handover Interface 2
HI-3	Handover Interface 3
HI-B	Handover Interface B
HMAC	Hash-based Message Authentication Code
HTML	Hypertext Markup Language
HTTP	HyperText Transfer Protocol
HTTPS	HyperText Transfer Protocol Secure
IANA	Internet Assigned Number Association
ICCID	Integrated Circuit Card ID
ID	Identifier
IEEE	Institute of Electrical and Electronics Engineers
IMEI	International Mobile station Equipment Identity
IMEISV	International Mobile station Equipment Identity Software Version
IMPI	IP Multimedia Private Identity
IMPU	IP Multimedia PUBlic identity
IMSI	International Mobile Subscriber Identity
IP	Internet Protocol
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IRI	Intercept Related Information
ISO	International Organization for Standardization
JPEG	Joint Photographic Experts Group
JSON	JavaScript Object Notation
JWS	JSON Web Signature
LD	Lawful Disclosure
LDID	Lawful Disclosure IDentifier
LEA	Law Enforcement Agency
LEMF	Lawful Interception Monitoring Facility

LI	Lawful Intercept
LIID	Lawful Intercept Identifier
LP	Lawful Preservation
MAC	Media Access Control
MD5	Message Digest 5
MIME	Multipurpose Internet Mail Extensions
MSISDN	Mobile Station International Subscriber Directory Number
NAI	Network Access Identifier
NCGI	NR Cell Global Identifier
NR	New Radio
NWO	Network Operator
PDHR	Packet Data Header Reporting
PDSR	Packet Data Summary Reporting
POSIX	Portable Operating System Interface
RCS	Rich Communications Services
RFC	Request For Comments
SHA	Secure Hash Function
SIP	Session Initiation Protocol
SV	Software Version
TC	Technical Committee
TCLI	Technical Committee Lawful Interception
TCP	Transmission Control Protocol
TIFF	Tagged Image File Format
TLS	Transport Layer Security
UDP	User Datagram Protocol
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTF	Unicode Transformation Format
UTRAN	UMTS Terrestrial Radio Access Network
UUID	Universally Unique IDentifier
VIN	Vehicle Identification Number
VLAN	Virtual Local Area Network
WI	Warrant Information
XML	eXtensible Markup Language
XSD	XML Schema Definition

4 Structure and model

4.1 Structure of the standard

The present document defines an interface and data structures that can be used to enable electronic warrant and tasking information to be exchanged. The processes for creating, approving and implementing a warrant are national matters. The present document does not attempt to dictate or define these processes, but provides an interface and data structures on which such processes can be built. Likewise, the present document assumes that a suitable physical network infrastructure is available. Figure 4.1 shows the conceptual structure of the standard.

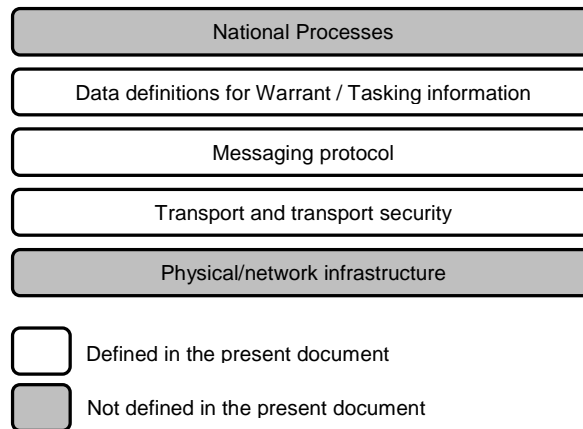


Figure 4.1: Conceptual structure of the standard

4.2 Structure of the present document

Clause 5 defines how messages are exchanged in the messaging protocol.

Clause 6 defines the format of the messages exchanged in the messaging protocol.

Clause 7 describes the data definitions and structures for HI-1 Objects that are exchanged and used as part of the warrant and tasking processes.

Clause 8 describes the data definitions and structures for HI-1 Task Objects.

Clause 9 describes the transport mechanism(s) used by the messaging protocol.

Clause 10 describes the definition and usage of the Delivery Object.

4.3 Reference model

The present document defines an interface between two participants.

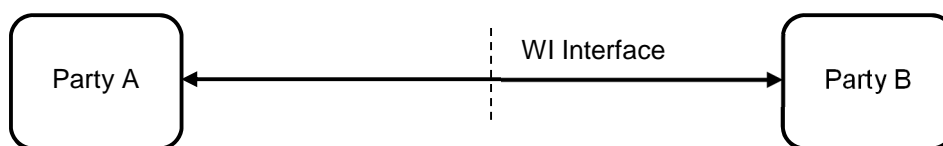


Figure 4.2: Reference model for WI interface

The process of approving or enacting a warrant will often involve more than two participants. Multi-party or multi-step interactions can, by national agreement, be composed of multiple two-party interactions. For example:

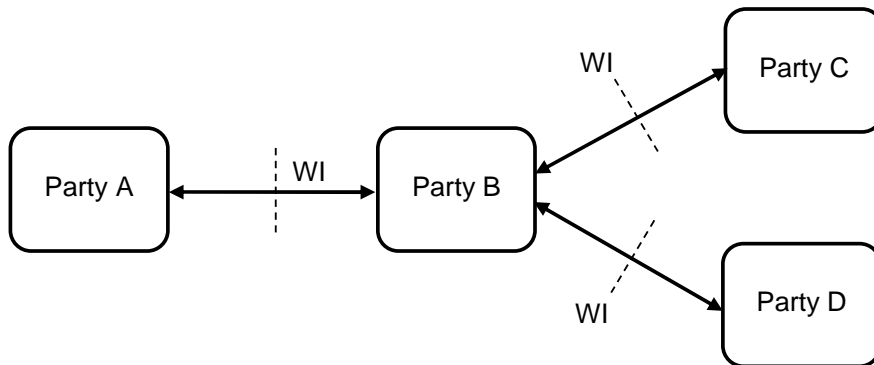


Figure 4.3: Example national process composed of WI interactions

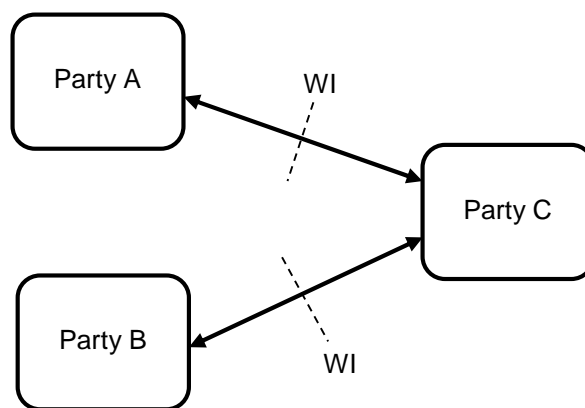


Figure 4.4: Further example national process composed of WI interactions

The nature of these "higher-level" multi-party processes will be dictated by national legislation, and as such are not defined in the present document.

5 Message Exchange

HI-1 defines two roles in an HI-1 communication:

- The Sender generates a Request Message and transmits it.
- The Receiver receives the Request Message, processes it, and returns a Response Message to the Sender.

HI-1 message exchange therefore follows a simple Request-Response pattern between Sender and Receiver.

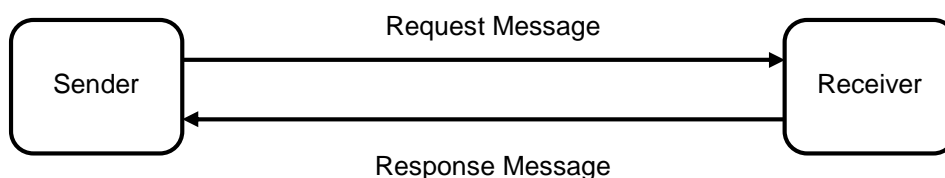


Figure 5.1

Note that the roles of Sender and Receiver are logical ones. A given node may act as both a Sender and Receiver for different exchanges, depending on the specifics of the relevant national processes, network configuration and implementation details.

Clause 6 describes the structure of Request and Response messages.

6 Message Structure

6.1 Overview

The high-level structure for HI-1 Request and Response messages is shown in figure 6.1.

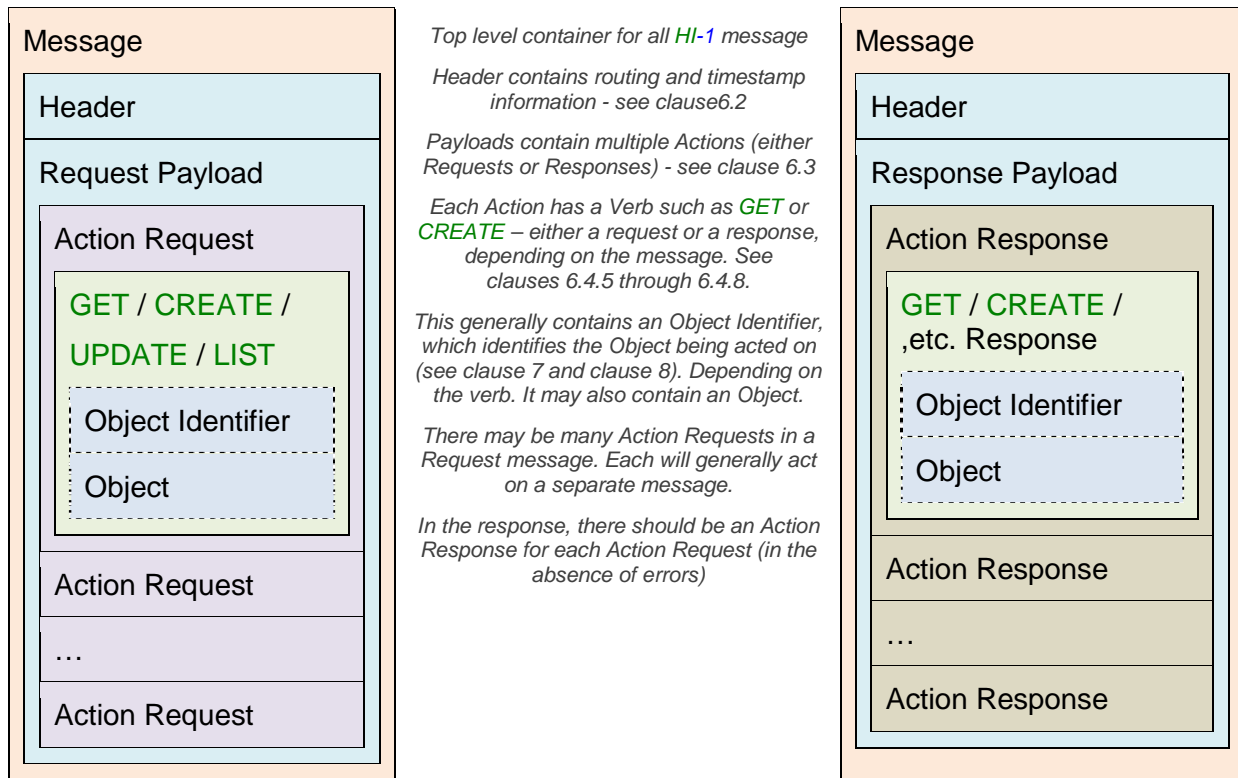


Figure 6.1: High-level message structure

Each message consists of two parts:

- Message Header.
- Message Payload (either a Request Payload or a Response Payload).

6.2 MessageHeader

6.2.1 Overview

Every HI-1 Message shall contain a MessageHeader structure that is the same for all messages and contains basic routing and identification information.

If a Receiver receives a message containing a MessageHeader that does not follow the format and rules given in this clause, the Receiver shall reject the entire message with a top-level Action Unsuccessful response (see clause 6.4.9).

If a Sender receives a message containing a MessageHeader that does not follow the format and rules given above, the Sender shall disregard the message. Implementers are encouraged to alert the local user.

6.2.2 Structure

Table 6.1 shows the structure of every valid MessageHeader within an HI-1 message.

Table 6.1: MessageHeader

Field	Format	Description
SenderIdentifier	EndpointID (see clause 6.2.4 for details)	Nationally unique identifier and country code, sufficient to uniquely identify the Sender node in the message exchange. See clause 6.2.4 for details.
ReceiverIdentifier	EndpointID (see clause 6.2.4 for details)	Nationally unique identifier and country code, sufficient to uniquely identify the intended Receiver in the message exchange. See clause 6.2.4 for details.
TransactionIdentifier	UUID (see ETSI TS 103 280 [7]) in IETF RFC 4122 [3] canonical form	Identifier that uniquely identifies the message exchange between a given Sender and Receiver. See clause 6.2.5 for details.
Timestamp	QualifiedMicrosecondDateTime (see ETSI TS 103 280 [7])	Timestamp indicating the time the message was sent.
Version	Version (see clause 6.2.3 for details)	Version of the present document and relevant national profile used for interpreting the message.

6.2.3 Version

The Version structure indicates the version of the present document that should be used to interpret this message, as well as identifying the relevant national profile version that should be used.

Table 6.2: Version

Field	Format	Description
ETSIVersion	ShortString of the form "VX.Y.Z" (X gives major version, Y gives minor version, Z gives revision)	Version of the present document that should be used to interpret this message.
NationalProfileOwner	National profile owner (see clause F.3.2 for a definition of owners)	Identifies the owner of the relevant national profile. See clause F.3.2 for further details.
NationalProfileVersion	ShortString (see ETSI TS 103 280 [7])	Version of the national profile that should be used to interpret this message. National profile shall define the valid format and values for this field.

The present document does not specify any requirements for interoperability between systems using different versions of the present document or a national profile. The required behaviour of systems under such circumstances is a matter for national agreement.

6.2.4 EndpointID

An EndpointID is used to provide a nationally unique identifier for a Sender or Receiver.

Table 6.3: EndpointID

Field	Format	Description
CountryCode	ISOCountryCode (see ETSI TS 103 280 [7]) giving 3166-1 alpha-2 code	Two-letter country code for the country. The reserved Country Code XX shall be used for international organizations.
UniquelIdentifier	LongString (see ETSI TS 103 280 [7])	Unique identifier sufficient for identifying the object/field within the country.

Sender and Receiver Identifiers are used within a MessageHeader to uniquely identify Sender and Receiver entities. As such, they have to be unique within the country specified by their respective country codes.

The Receiver shall populate the Receiver Identifier in all Response messages with its assigned Receiver Identifier. The Receiver shall also populate the Sender Identifier with the value specified in the original Request message, unless the Receiver is responding with a top level Action Unsuccessful payload and is unable to determine the original Sender Identifier. This means, for example, that a Receiver sending back a Response message still sets the Sender Identifier to the identifier of the original Sender, and the Receiver Identifier to its own identifier. If a Receiver cannot determine the original Sender Identifier, then the Receiver shall populate the Sender Identifier with the reserved value "UNKNOWN" (all capitals). This value may not be used as a valid Sender or Receiver Identifier.

If a Receiver receives a message with a valid but unexpected Receiver Identifier, the Receiver shall reject the entire message with a top-level Error Response.

If a Receiver cannot determine the original Sender Identifier Country Code, then the Receiver shall populate the Sender Identifier Country Code with the reserved value "ZZ" (all capitals) in the Response. This value may not be used as a value Sender or Receiver country code.

The precise format of Sender and Receiver Identifiers is for national agreement.

6.2.5 Transaction Identifiers

The Transaction Identifier is a UUID in IETF RFC 4122 [3] canonical form used within a MessageHeader that uniquely identifies a particular HI-1 message exchange between a particular Sender and Receiver. As such, the Transaction Identifier is unique for a pair of Request and Response messages.

Senders are responsible for creating Transaction Identifiers and maintaining their uniqueness between that Sender and a given Receiver. A Receiver that receives a duplicate Transaction Identifier from a given Sender may respond with a top-level Action Error if such duplication causes a system error, but is otherwise not required to check the uniqueness of the Transaction Identifier.

A Receiver creating a Response message shall populate the Transaction Identifier as specified in the original Request message, unless the Receiver is responding with a DELIVER Response (see clause 6.4.10) or Error payload or is unable to determine the original Sender, Receiver and Transaction Identifiers (e.g. the Request message is corrupted and unreadable). If a Receiver cannot determine the original Transaction Identifier, then the Receiver shall assign the Response message a new unique Transaction Identifier.

6.3 Message Payload

6.3.1 Overview

Every HI-1 Message shall contain a Message Payload structure. A Request Message shall contain a Request Payload, while a Response message shall contain a Response payload. For a definition of Request and Response messages, see clause 5.

6.3.2 Request Payload

A Request Payload contains the information sent from a Sender to Receiver. It consists of a collection of Action Requests (see clause 6.4.2).

To improve processing efficiency and responsiveness, it is recommended that Action Requests in a Request Payload be limited to a single related set of objects, e.g. an Authorisation Object and its dependent Task Objects.

To ensure error-free and predictable processing of Task Objects, it is recommended that Action Requests concerning Authorisation Objects be placed ahead of its associated Action Requests concerning Task Objects. The easiest way to ensure that this takes place is to put all Action Requests concerning Authorisation Objects before any Action Requests concerning Tasking Objects in the Request Payload.

It is also recommended that Action Requests concerning Warrant documentation referenced within a Document Object be submitted prior to Action Requests concerning Authorisation Objects which reference that documentation.

6.3.3 Response Payload

A Response Payload contains information sent back from a Receiver to a Sender, in response to a Request Message.

The result of processing multiple Action Requests in a given Request message shall be as if they were processed in order of Action Identifier (see clause 6.4.4).

On receiving an Action Unsuccessful response, the Sender shall consider that particular Action Request as not having been understood or acted on. On receiving a top-level Action Unsuccessful structure, the Sender shall consider none of the original Request Message to have been understood or acted on. See clause 6.4.9 for more details.

6.4 Action Request and Responses

6.4.1 Overview

Clause 6.4 defines a set of verbs to aid the two parties in creating, updating, exchanging and reporting on the HI-1 Objects. It does not dictate business processes that vary nationally.

6.4.2 Action Requests

Each Action Request in the Request Payload shall be assigned an Action Identifier (see clause 6.4.4). Each Action Request appears in ascending order of the Action Identifier.

An Action Request shall be one of the following "verbs".

Table 6.4: Action Request types

Verb	Description	Definition
GET	Retrieve HI-1 Object	See clause 6.4.5
CREATE	Create new HI-1 Object	See clause 6.4.6
UPDATE	Update existing HI-1 Object	See clause 6.4.7
LIST	List identifiers of HI-1 Objects	See clause 6.4.8
DELIVER	Deliver an HI-1 Object	See clause 6.4.10
GETCSPCONFIG	Retrieve the CSP Capability Configuration	See clause 6.4.11

The list of verbs is deliberately limited, as they are not intended to describe the business processes. Such higher level processes should instead be represented by the state of the relevant HI-1 Object. The present document simply provides a mechanism for transferring objects between participants in the process.

6.4.3 Action Responses

A response message sent from a Receiver to a Sender describes the legibility of the Request message received. An Action Response is generated for each Action Request provided in a Request, providing the Request Message as a whole could be understood. Each Action Response contains an Action Identifier that correlates with the Action Identifier provided in the Request. For the avoidance of doubt, in the case of a DELIVER Response, the Action Identifier shall match the one given in the DELIVER Request, and not any associated with the creation of related objects.

An Action Response shall be one of the following "verbs".

Table 6.5: Action Response types

Verb	Description	Definition
GET RESPONSE	Successful retrieval of HI-1 Object of given identifier in Action Request.	See clause 6.4.5
CREATE RESPONSE	Receipt of legible Create Request of given identifier in Action Request.	See clause 6.4.6
UPDATE RESPONSE	Receipt of legible Update Request of given identifier in Action Request.	See clause 6.4.7
LIST RESPONSE	Successful retrieval of identifiers of given type from Action Request.	See clause 6.4.8
ERROR INFORMATION	Action Request could not be successfully processed. On receipt of this, the Sender shall regard the Action Request as not having been processed.	See clause 6.4.9
DELIVER RESPONSE	Successful receipt of an HI-1 Object.	See clause 6.4.10
GETCSPCONFIGRESPONSE	Successful retrieval of the CSP Capability Configuration information.	See clause 6.4.11

6.4.4 Action Identifiers

Action Identifiers are used in Message Payloads, within Action Requests and Action Responses. The Action Identifier correlates an Action Request and Action Response between a given Sender and Receiver. Action Identifiers are generated by the Sender. The Action Identifier shall be a zero-based integer counter that is unique for each Action Request and corresponding Action Response for a given Transaction Identifier. The Sender shall populate the Request Payload with Action Requests in ascending order of Action Identifier. On receiving a Request Message, the Receiver shall check that the Action Identifiers are correctly in sequence, starting at zero and increasing by one for each Action Identifier. If the Action Identifiers are not correctly in sequence, the Receiver shall reject the Request Message with a top-level Error. Systems with a manual step should take particular care here to check for duplicates before performing any actions.

6.4.5 GET

A GET Request represents a request for the Receiver to return a particular HI-1 Object.

A GET Request shall have the following parameters.

Table 6.6: GET Request fields

Field	Format	Description	Mandatory?
Identifier	ObjectIdentifier (see clause 7.1.2)	Uniquely identifies the HI-1 Object that the Sender wishes to retrieve.	Yes

The Receiver shall respond to a successful GET Request with a GET Response with the following parameters.

Table 6.7: GET Response fields

Field	Format	Description	Mandatory?
HI1Object	HI1Object	Object that is identified by the identifier.	Yes

If the Receiver is unable to retrieve an Object with the defined ObjectIdentifier, then an Action Error response with an appropriate error code is returned.

6.4.6 CREATE

A CREATE Request represents a request for the Receiver to create a new HI-1 Object.

A CREATE Request shall have the following parameters.

Table 6.8: CREATE Request fields

Field	Format	Description	Mandatory?
HI1Object	HI1Object	Representation of the HI-1 Object to be created by the Receiver.	Yes

The Receiver shall respond to a successful CREATE Request with a CREATE Response with the following parameters.

Table 6.9: CREATE Response fields

Field	Format	Description	Mandatory?
Identifier	ObjectIdentifier (see clause 7.1.2)	Value provided in the CREATE Request.	Yes
HI1Object	HI1Object	HI-1 Object that is identified by the identifier.	No

If the Receiver is unable to create an HI-1 Object with the defined identifier, then an Action Error response with an appropriate error code is returned. Unsuccessful creations could be as a result of an already used identifier.

The Receiver may, optionally, return an updated version of the Object as part of the CREATE Response (see table 6.9). This may be useful in situations where the Receiver populates or updates additional fields as part of processing the CREATE request.

The Receiver shall set the Generation of a created Object to 1 (see clause 7.1.3).

6.4.7 UPDATE

An UPDATE Request represents a request for the Receiver to update values in an existing HI-1 Object.

An UPDATE Request shall have the following parameters.

Table 6.10: UPDATE Request fields

Field	Format	Description	Mandatory?
HI1Object	HI1Object	Representation of the HI-1 Object to be updated by the Receiver.	Yes

The Receiver shall respond to a successful UPDATE Request with an UPDATE Response with the following parameters.

Table 6.11: UPDATE Response fields

Field	Format	Description	Mandatory?
Identifier	ObjectIdentifier (see clause 7.1.2)	Value provided in the UPDATE Request.	Yes
HI1Object	HI1Object	HI-1 Object that is identified by the identifier.	No

If the Receiver is unable to update an Object with the defined identifier, then an Action Error response is returned. Unsuccessful updates could be as a result of using an identifier that does not exist.

Receivers shall observe the following on performing an UPDATE Request:

- If a single-valued field is present in the UPDATE Request Object, the Receiver should set the value of the equivalent field to match.
- If a list-field is present in the UPDATE Request Object, the Receiver should set the contents of the equivalent list field to match, i.e. overwrite the entire list and not append to it.
- If a field is absent in the UPDATE Request Object, the Receiver should leave the value of the equivalent field unchanged.

If the request can be understood and parsed, but cannot be acted upon, then the Receiver shall return an Error Information as described in clause 6.4.9.

The Receiver shall update the Generation of an Object that has been updated (see clause 7.1.3).

6.4.8 LIST

A LIST Request represents a request for the Receiver to list records of HI-1 Object identifiers that the Sender is permitted to have knowledge of, optionally depending on the type requested. Although no business processes are defined in the present document, the Receiver is responsible for listing only the identifiers that a Sender is allowed to access. Details of how to determine this shall be specified in the relevant national profile.

This method shall only be allowed if explicitly required by the relevant national profile. Use of the capability on a national basis should be carefully considered for its security implications. If the Receiver does not allow the use of the LIST verb, then it shall respond to a LIST Request with an Action Error response.

The list of objects provided in a response message may be limited subject to national agreement, for example to only Active objects, or to a configured number of most recent objects. This is needed to prevent potentially many years worth of data being dumped on the requestor in a message too large for the requestor system to handle. Such details shall be specified in the relevant national profile.

A LIST Request shall have the following parameters.

Table 6.12: LIST Request fields

Field	Format	Description	Mandatory?
ObjectType	ObjectType dictionary entry (see below)	Specifies the type of identifiers to be listed.	No
LastChanged	QualifiedDateTime (see ETSI TS 103 280 [7])	If specified, the Receiver shall return only records of Objects whose LastChanged field is equal to or later than the value specified.	No

The Receiver shall respond to a successful LIST Request with a list of LIST Response records, one for each HI-1 Object matching the request constraints (e.g. ObjectType). Each LIST Response record shall have the following parameters.

Table 6.13: LIST ResponseRecord fields

Field	Format	Description	Mandatory?
ObjectType	ObjectType dictionary entry (see below)	Value provided in the LIST Request.	Yes
Identifier	ObjectIdentifier (see clause 7.1.2)	Identifier of the Object.	Yes
CountryCode	ISOCountryCode (see ETSI TS 103 280 [7]) giving ISO 3166-1 [14] Alpha-2 code [14]	See clause 7.1.1.	No
OwnerIdentifier	ShortString (see ETSI TS 103 280 [7])	See clause 7.1.1.	No
Generation	Positive integer	See clause 7.1.3.	Yes
ExternalIdentifier	LongString (see ETSI TS 103 280 [7])	See clause 7.1.1.	No
LastChanged	QualifiedDateTime (see ETSI TS 103 280 [7])	Indicates the last time an Object was altered, either via HI-1 or locally.	No

The ObjectType dictionary is defined as follows (see annex F for more details on Dictionaries).

Table 6.14: ObjectType Dictionary

Dictionary Owner	Dictionary Name
ETSI	ObjectType
Defined DictionaryEntries	
Value	Meaning
Authorisation	An Authorisation Object as defined in clause 7.2
Document	A Document Object as defined in clause 7.3
Notification	A Notification Object as defined in clause 7.4
Task	An LI Task Object as defined in clause 8.2
LDTask	An LD Task Object as defined in clause 8.3
Delivery	A Delivery Object as defined in clause 10
LPTask	An LP Task Object as defined in clause 8.4

If the Receiver contains no Objects of the defined type, then an empty list is returned.

If the Request can be understood and parsed, but cannot be acted upon, then the Receiver shall return an Error Information as described in clause 6.4.9.

In the particular case that the ObjectType is set to "Notification", the Receiver shall only return the Object Identifiers of instances of a NotificationObject whose NewNotification flag is set (see clause 7.4.4 for more details). Implementations may need additional rules or logic to restrict the association of instances of a NotificationObject. Where needed, such logic shall be specified by the relevant national profile.

6.4.9 Action Unsuccessful Information

The Receiver shall respond to unsuccessful requests with an Action Unsuccessful Information structure with the following parameters.

Table 6.15: Action Unsuccessful Information fields

Field	Format	Description	Mandatory?
ErrorCode	Integer	Integer code specifying the type of error.	Yes
ErrorInformation	LongString (see ETSI TS 103 280 [7])	Detail of the error that occurred.	Yes

If the message received by the Receiver is understood and parsed, but an individual Action Request cannot be acted on, then the response shall contain an individual Action Unsuccessful Response. On receiving this Action Unsuccessful Response, a Sender shall consider the associated request to have not been acted on.

If the message received by the Receiver as a whole cannot be understood, then the response shall contain a top-level Action Unsuccessful structure explaining the nature of the error, instead of a collection of Action Responses. This shall only be used in error conditions which prevent any of the Action Requests being understood - for example, a fatal syntax error that makes the entire request message illegible. On receiving this top-level Action Unsuccessful Error structure, a Sender shall consider none of the original request to have been understood or acted on.

6.4.10 DELIVER

A DELIVER Request represents a mechanism to deliver information in response to a lawful request represented by another HI-1 Object, for example where a LEA creates an LDTaskObject and the CSP discloses data by sending one or more DeliveryObject(s).

A DELIVER Request shall have the following parameters.

Table 6.16: DELIVER Request fields

Field	Format	Description	Mandatory?
Identifier	ObjectIdentifier (see clause 7.1.2)	Uniquely identifies the Delivery Object that the Responder (i.e. CSP) wishes to deliver.	Yes
HI1Object	HI1Object	HI-1 Object that is identified by the identifier.	Yes

A DELIVER Response indicates successful receipt of the object. It contains the following parameters.

Table 6.17: DELIVER Response fields

Field	Format	Description	Mandatory?
Identifier	ObjectIdentifier (see clause 7.1.2)	Identifier of the HI-1 Object delivered in the DELIVER request.	Yes

While the DELIVER verb may be used to deliver any HI-1 Object, it is primarily intended for delivering Delivery Objects (see clause 10).

6.4.11 GETCSPCONFIG

6.4.11.1 Overview

A GETCSPCONFIG Request represents a request to retrieve information about the capabilities of a CSP. It allows querying the dictionaries supported by the CSP, the workflow endpoints supported by the CSP, the permitted formats for targets, and the services or products that can be requested for LI, LD, or LP for a given target format.

A GETCSPCONFIG Request has no parameters.

A GETCSPCONFIG Response indicates successful retrieval of the capability information. It has the following structure.

Table 6.18: GETCSPCONFIG Response fields

Field	Format	Description	Mandatory?
LastChanged	QualifiedDateTime (see ETSI TS 103 280 [7])	Indicates the time this configuration was last changed.	Yes
DictionaryDefinitions	List of Dictionary values (see annex F)	Defines supported Dictionaries.	No
TargetFormatTypeDefinitions	TargetFormatTypeDefintions (see clause 6.4.11.2)	Defines supported Target FormatTypes.	No
TargetingConfigurations	List of TargetingConfiguration values (see clause 6.4.11.3)	Defines valid target identifier formats and associated services or products that can be requested for that format.	Yes
SupportedLIWorkflowEndpoints	List of SupportedLIWorkflowEndpoint values (see clause 6.4.11.4)	LI Workflow Endpoints that are supported by the CSP.	No
SupportedLPWorkflowEndpoints	List of SupportedLPWorkflowEndpoint values (see clause 6.4.11.5)	LP Workflow Endpoints that are supported by the CSP.	No

6.4.11.2 TargetFormatTypeDefinition

The TargetFormatTypeDefinition defines the FormatType values (see clauses 8.2.6.3 and 8.3.5.4) owned by this CSP.

TargetFormatTypeDefinition has the following structure.

Table 6.19: TargetFormatTypeDefinition

Field	Format	Description	Mandatory?
FormatOwner	ShortString (see ETSI TS 103 280 [7])	The owner of these format definitions.	Yes
TargetFormatTypeDefinitionEntries	List of TargetFormatTypeDefinitionEntry (see Table 6.20)	The format definitions introduced by the CSP.	Yes

TargetFormatTypeDefinitionEntry has the following structure.

Table 6.20: TargetFormatTypeDefinitionEntry

Field	Format	Description	Mandatory?
FormatName	ShortString (see ETSI TS 103 280 [7])	The name of this format.	Yes
Description	LongString (see ETSI TS 103 280 [7])	Provides additional guidance about this format type.	Yes
FormatRegex	LongString (see ETSI TS 103 280 [7])	A regular expression that can be applied to the identifier value for this format type.	Yes

6.4.11.3 TargetingConfiguration

The TargetingConfiguration defines the valid format types for LITask, LDTask, or LPTask Objects sent to the CSP. It also defines the valid services associated with that format type.

TargetingConfiguration has the following structure.

Table 6.21: TargetingConfiguration

Field	Format	Description	Mandatory?
FormatOwner	ShortString (see ETSI TS 103 280 [7])	The valid FormatOwner this entry is associated with (see clauses 8.2.6.3 and 8.3.5.4).	Yes
FormatName	ShortString (see ETSI TS 103 280 [7])	The valid FormatName this entry is associated with (see clauses 8.2.6.3 and 8.3.5.4).	Yes
Guidance	LongString (see ETSI TS 103 280 [7])	Provides additional guidance about this format type.	No
AssociatedLIServiceTypes	List of TaskServiceType DictionaryEntries (see clause 8.2.6.4)	Provides valid TaskServiceType values for the given format.	No
AssociatedLDSubtypes	List of LDRequestSubtype DictionaryEntries (see clause 8.3.5.5)	Provides valid LDRequestSubtype values for the given format.	No
AssociatedLPSubtypes	List of LPRequestSubtype DictionaryEntries (see clause 8.4.4.2)	Provides valid LPRequestSubtype values for the given format.	No

6.4.11.4 SupportedLIWorkflowEndpoint

Including a SupportedLIWorkflowEndpoint in the SupportedLIWorkflowEndpoints field indicates that the CSP supports that endpoint. See clause H.5 for LI Workflow Profile Endpoints and their restrictions. The CSP shall specify an entry associated with a given endpoint at most once.

The SupportedLIWorkflowEndpoint has the following structure.

Table 6.22: SupportedLIWorkflowEndpoint

Field	Format	Description	Mandatory?
LIWorkflowEndpoint	LIWorkflowEndpoint DictionaryEntry (see table 6.23)	The supported LI Workflow Endpoint this entry is associated with.	Yes
Guidance	LongString (see ETSI TS 103 280 [7])	Provides additional guidance about this workflow endpoint.	No
URL	LongString (see ETSI TS 103 280 [7])	The URL to access this endpoint.	Yes

Table 6.23: LIWorkflowEndpoint Dictionary

Dictionary Owner	Dictionary Name
ETSI	LIWorkflowEndpoint.
Defined DictionaryEntries	
Value	Meaning
NewAuthorisation	CSP supports the "New Authorisation" Endpoint.
AuthorisationExtension	CSP supports the "Authorisation Extension" Endpoint.
AuthorisationCancellation	CSP supports the "Authorisation Cancellation" Endpoint.
TaskAddition	CSP supports the "Task Addition" Endpoint.
TaskCancellation	CSP supports the "Task Cancellation" Endpoint.
ChangeOfDelivery	CSP supports the "Change of Delivery" Endpoint.

6.4.11.5 SupportedLPWorkflowEndpoint

Including a SupportedLPWorkflowEndpoint in the SupportedLPWorkflowEndpoints field indicates that the CSP supports that endpoint. See clause H.6 for LP Workflow Profile Endpoints and their restrictions. The CSP shall specify an entry associated with a given endpoint at most once.

The SupportedLPWorkflowEndpoint has the following structure.

Table 6.24: SupportedLPWorkflowEndpoint

Field	Format	Description	Mandatory?
LPWorkflowEndpoint	LPWorkflowEndpoint DictionaryEntry (see table 6.25)	The supported LP Workflow Endpoint this entry is associated with.	Yes
Guidance	LongString (see ETSI TS 103 280 [7])	Provides additional guidance about this workflow endpoint.	No
URL	LongString (see ETSI TS 103 280 [7])	The URL to access this endpoint.	Yes

Table 6.25: LPWorkflowEndpoint Dictionary

Dictionary Owner	Dictionary Name
ETSI	LPWorkflowEndpoint.
Defined DictionaryEntries	
Value	Meaning
NewPreservation	CSP supports the "New Preservation" Endpoint.
PreservationExtension	CSP supports the "Preservation Extension" Endpoint.
PreservationCancellation	CSP supports the "Preservation Cancellation" Endpoint.

7 Data Definitions

7.1 HI1Object

7.1.1 Overview

HI1Objects represent the current state of a particular national process. The relevant national profile shall specify which fields are required for a particular HI1Object to be valid within the relevant national processes.

All HI1Objects have the following top-level structure.

Table 7.1: HI1Object

Field	Format	Description
ObjectIdentifier	UUID (see ETSI TS 103 280 [7]) given in IETF RFC 4122 [3] canonical form	Uniquely identifies the Object (see clause 7.1.2).
CountryCode	ISOCountryCode (see ETSI TS 103 280 [7]) giving ISO 3166-1 [14] Alpha-2 code [14]	Two-letter country code for the country. If the Owner Identifier identifies an international organization, the reserved Country Code XX.
OwnerIdentifier	ShortString (see ETSI TS 103 280 [7])	String to represent the agency/organization involved. Format for national agreement.
Generation	Positive integer	Indicates the generation or version of the Object (see clause 7.1.3).
ExternalIdentifier	LongString (see ETSI TS 103 280 [7])	Optional identifier for the Object, as assigned by the Receiver. For correlation with legacy or pre-HI-1 systems.
AssociatedObjects	List of ObjectIdentifiers (see clause 7.1.4)	Indicated other Objects which are associated with a given Object.
LastChanged	QualifiedDateTime (see ETSI TS 103 280 [7])	Indicates the last time this Object was altered, either via HI-1 or locally.
NationalHandlingParameters	Defined by the relevant national profile	Nationally-defined information concerning the handling of the Object.

7.1.2 ObjectIdentifier

An ObjectIdentifier is an identifier that is used to uniquely identify and refer to a particular HI1Object. To follow RESTful principles, an HI1Object should be identified by a persistent identifier to refer to or locate the HI1Object. This identifier is essential to the automated handling and management of the lifecycle of the object, and is therefore not permitted to change for the lifetime of the HI1Object as it is used to uniquely identify the HI1Object.

7.1.3 Generation

The Generation parameter indicates how many times the HI1Object has been changed or updated.

The Receiver shall set the Generation of an HI1Object to 1 when it is created. A Sender shall not specify the Generation as part of a CREATE Request, and a Receiver shall return an Action Unsuccessful Information response if it attempts to.

The Receiver shall increment the Generation of an Object by 1 each time it is altered or updated, either via HI-1 or by other means. A Sender may optionally specify the Generation as part of an UPDATE Request. In this case, the Receiver shall check whether the Generation matches the current Generation of the Object. If so, the Receiver shall process the UPDATE Request normally, and then increment the Generation. If not, the Receiver shall respond with an Action Unsuccessful Information response. If the Sender omits the Generation as part of the UPDATE Request, then the Receiver shall process the UPDATE normally and increment the Generation.

7.1.4 AssociatedObjects

The AssociatedObjects field gives a list of other HI1Objects which are related or associated in some way with this HI1Object. Examples include TaskObjects associated with an AuthorisationObject or DocumentObjects associated with an AuthorisationObject or TaskObject.

Table 7.2: AssociatedObjects

Field	Format	Description
AssociatedObjects	List of ObjectIdentifiers	List of other HI1Objects which are related or associated with the current HI1Object.

7.1.5 LastChanged

The LastChanged field indicates the date and time that the HIObject was last changed, either as a result of an HI-1 Action, or as the result of local activity at the Receiver (e.g. local operator intervention, or a change of workflow state).

This field shall be set by the Receiver when an HIObject is first created, and each time it is modified as a result of either an HI-1 Action or local activity.

Only the Receiver may change the content of the LastChanged field. A Receiver shall reject an Action which attempts to modify or set the LastChanged field.

7.1.6 NationalHandlingParameters

The NationalHandlingParameters structure is provided to allow the relevant national profile to specify nationally-specific handling information (e.g. routing information or security labelling).

The format and use of the NationalHandlingParameters structure shall be defined in the relevant national profile.

7.2 AuthorisationObject

7.2.1 Overview

An AuthorisationObject represents the state of an authorisation - that is, a legal instrument by which legal action is permitted. It has the following fields (following the categories defined in ETSI TR 103 690 [i.1]).

Table 7.3: AuthorisationObject

Field	Format	Description	Reference
AuthorisationReference	LongString (see ETSI TS 103 280 [7]).	Nationally defined reference for the Authorisation. This is provided to allow correlation with non-HI1 processes.	Clause 7.2.2
AuthorisationLegalType	AuthorisationLegalType DictionaryEntry.	Indicates the type and legal basis under which the Authorisation is sought e.g. a reference to the relevant legal code or statutory purpose. The format and acceptable values for this field shall be defined by the relevant national profile.	Clause 7.2.3
AuthorisationPriority	AuthorisationPriority DictionaryEntry.	Usage for national agreement When used, a default dictionary is provided in clause 7.2.4.	Clause 7.2.4
AuthorisationStatus	AuthorisationStatus DictionaryEntry.	The current status of the Authorisation according to the Receiver.	Clause 7.2.5
AuthorisationDesiredStatus	AuthorisationDesiredStatus DictionaryEntry.	The desired status of the Authorisation, as specified by the Sender.	Clause 7.2.6
AuthorisationTimespan	AuthorisationTimespan.	The period of validity for the Authorisation.	Clause 7.2.7
AuthorisationCSPID	List of EndpointIDs (see clause 6.2.4).	Identifies the CSP(s) required to implement the Authorisation.	Clause 7.2.8
AuthorisationCreationTimestamp	QualifiedDateTime (see ETSI TS 103 280 [7]).	Indicates when the Authorisation was created.	Clause 7.2.9
AuthorisationServedTimestamp	QualifiedDateTime (see ETSI TS 103 280 [7]).	Indicates when the Authorisation was served on the CSP.	Clause 7.2.10
AuthorisationTerminationTimestamp	QualifiedDateTime (see ETSI TS 103 280 [7]).	Indicates when an Authorisation was terminated, in the event that it is explicitly terminated prior to the end of its validity.	

Field	Format	Description	Reference
AuthorisationApprovalDetails	ApprovalDetails (see annex E).	Gives details of who approved or signed the Authorisation, and when.	Clause 7.2.11
AuthorisationInvalidReason	ActionUnsuccessful structure.	Optional information for the Receiver to indicate why the Object is in the Invalid state. Usage for national agreement.	Clause 6.4.9
AuthorisationFlags	AuthorisationFlags.	Set of flags associated with the Authorisation Object.	Clause 7.2.12
AuthorisationManuallInformation	LongString (see ETSI TS 103 280 [7]).	Any additional human-readable information regarding the Authorisation.	Clause 7.2.16
NationalAuthorisationParameters	See annex G.	See annex G.	Annex G
AuthorisationJurisdiction	LongString (see ETSI TS 103 280 [7]).	Indication of the relevant jurisdiction for the Authorisation.	Clause 7.2.13
AuthorisationTypeOfCase	AuthorisationTypeOfCase DictionaryEntry.	Informative for the CSP, to give an indication of the type of case involved.	Clause 7.2.14
AuthorisationLegalEntity	ShortString (see ETSI TS 103 280 [7]).	Identifies the specific legal or procedural entity that the Authorisation requires action from.	Clause 7.2.15

7.2.2 AuthorisationReference

The AuthorisationReference field provides a nationally defined reference for the Authorisation. This is provided to allow correlation with non-HII processes. The format and permissible values for the AuthorisationReference field shall be defined by the relevant national profile.

7.2.3 AuthorisationLegalType

The AuthorisationLegalType field indicates the type and legal basis for the Authorisation. Examples include references to the relevant legal code or statutory purpose.

Given as an AuthorisationLegalType DictionaryEntry. The valid set of values for this field is likely to be closely coupled to national legislation. It is therefore expected that most national profiles will need to define their own extensions to this dictionary.

Table 7.4: AuthorisationLegalType Dictionary

Dictionary Owner	Dictionary Name
ETSI	AuthorisationLegalType
Defined DictionaryEntries	
Value	Meaning
Manual	The implementation should consult the AuthorisationManuallInformation field for details on the type of legal Authorisation

7.2.4 AuthorisationPriority

The AuthorisationPriority field gives an indication of the priority of the authorisation. Usage is for national agreement. The meaning of a given priority shall be specified by the national profile. The AuthorisationPriority, if used, shall be given as an AuthorisationPriority DictionaryEntry. The AuthorisationPriority Dictionary is defined in table 7.5 (see annex F for more details on Dictionaries).

Table 7.5: AuthorisationPriority Dictionary

Dictionary Owner	Dictionary Name
ETSI	AuthorisationPriority.
Defined DictionaryEntries	
Value	Meaning
High	The Authorisation has a high priority.
Routine	The Authorisation has a routine priority.

7.2.5 AuthorisationStatus

The AuthorisationStatus field indicates the current status of the authorisation as determined by the Receiver. A Sender shall not attempt to set the AuthorisationStatus as part of a CREATE or UPDATE Request, and a Receiver shall return an Action Unsuccessful Information response if it attempts to.

The Status field provides a key mechanism for mapping the content of the AuthorisationObject to the relevant nationally-defined processes. The rules for evaluating the correct value of the Status field shall be defined in the relevant national profile.

Given as an AuthorisationStatus Dictionary Entry. The AuthorisationStatus Dictionary is defined in table 7.6 (see annex F for more details on Dictionaries).

Table 7.6: AuthorisationStatus Dictionary

Dictionary Owner	Dictionary Name
ETSI	AuthorisationStatus.
Defined DictionaryEntries	
Value	Meaning
AwaitingApproval	The Authorisation is still waiting approval from one or more relevant authorities.
EmergencyApproval	The Authorisation has been approved under emergency procedures.
Approved	The Authorisation has been approved by the relevant authorities.
Rejected	The Authorisation has been explicitly denied or rejected by one or more relevant authorities.
Suspended	The Authorisation has been suspended temporarily.
Cancelled	The Authorisation has been permanently cancelled.
Expired	The expiry date for this Authorisation has passed, meaning that the Authorisation has lapsed.
Invalid	The Authorisation is not active due to a problem with the current information populated in the Authorisation Object.
CreatingForCSP	The LEA is in the process of creating the Authorisation with the CSP (i.e. in the process of uploading the relevant components). For example, it could be used as described in clause H.3.3.
SubmittedToCSP	The LEA has now uploaded all the relevant objects for this Authorisation to the CSP e.g. it could be used as described in clause H.3.3. This is intended to convey that the CSP can now proceed.

7.2.6 AuthorisationDesiredStatus

The AuthorisationDesiredStatus field indicates the current status of the authorisation as determined by the Sender.

Given as an AuthorisationDesiredStatus Dictionary Entry. The AuthorisationDesiredStatus Dictionary is defined in table 7.7 (see annex F for more details on Dictionaries).

Table 7.7: AuthorisationDesiredStatus Dictionary

Dictionary Owner	Dictionary Name
ETSI	AuthorisationDesiredStatus.
Defined DictionaryEntries	
Value	Meaning
AwaitingApproval	The Authorisation is still waiting approval from one or more relevant authorities.
EmergencyApproval	The Authorisation has been approved under emergency procedures.
Approved	The Authorisation has been approved by the relevant authorities.
Rejected	The Authorisation has been explicitly denied or rejected by one or more relevant authorities.
Suspended	The Authorisation has been suspended temporarily.
Cancelled	The Authorisation has been permanently cancelled.
Expired	The expiry date for this Authorisation has passed, meaning that the Authorisation has lapsed.
CreatingForCSP	The LEA is in the process of creating the Authorisation with the CSP (i.e. in the process of uploading the relevant components). For example, it could be used as described in clause H.3.3.
SubmittedToCSP	The LEA has now uploaded all the relevant objects for this Authorisation to the CSP e.g. it could be used as described in clause H.3.3. This is intended to convey that the CSP can now proceed.

7.2.7 AuthorisationTimespan

The AuthorisationTimespan field gives the period of time for which the authorisation is valid. This may not necessarily be the time that the legal action is active. The timestamps shall include a time-zone specifier.

Table 7.8: AuthorisationTimespan

Field	Format	Description
StartTime	QualifiedDateTime (see ETSI TS 103 280 [7])	Start time for the authorisation.
EndTime	QualifiedDateTime (see ETSI TS 103 280 [7])	End time for the authorisation.

7.2.8 AuthorisationCSPID

The AuthorisationCSPID field gives a list of globally unique CSP Identifiers that identify the CSPs required to implement the authorisation.

In some jurisdictions, authorisations may be required to be specific to an identified CSP. In those cases, this field may become a required field for Authorisation Objects to be valid and may be restricted from changing during the authorisation lifecycle. Also, validation checks may determine if the CSP exists, and searches associated with a CSP may be possible.

7.2.9 AuthorisationCreationTimestamp

The AuthorisationCreationTimestamp field indicates the time that the authorisation was created. The timestamp shall include a time-zone specifier. If necessary, the precise meaning of this field should be clarified by the relevant national profile.

7.2.10 AuthorisationServedTimestamp

The AuthorisationServedTimestamp indicates the time that the authorisation was served on the CSP. The timestamp shall include a timezone specifier.

7.2.11 AuthorisationApprovalDetails

The AuthorisationApprovalDetails field provides details of who approved the Authorisation.

See annex E for further details.

7.2.12 AuthorisationFlags

The AuthorisationFlags field allows a set of multiple flags to be associated with the Authorisation Object. Each flag is given as an AuthorisationFlag Dictionary Entry. If a flag is present in the Flags field, then the meaning given as part of that flag's definition shall be taken to apply.

The AuthorisationFlag Dictionary is defined in table 7.9 (see annex F for more details on Dictionaries).

Table 7.9: AuthorisationFlag Dictionary

Dictionary Owner	Dictionary Name
ETSI	AuthorisationFlag.
Defined DictionaryEntries	
Value	Meaning
IsEmergency	Indicates if the authorisation was issued under nationally-defined emergency procedures (e.g. orally). The circumstances and consequences for setting the field shall be defined by the relevant national profile.
IsConsensual	Indicates that the current authorisation is for consensual interception. This may alter the process or documentation accompanying the authorisation.
IsTest	Indicates that the current authorisation is given for test purposes. This may alter the process or documentation accompanying the authorisation.

7.2.13 AuthorisationJurisdiction

The AuthorisationJurisdiction field indicates the relevant jurisdiction for the Authorisation, given as a human-readable free text field. The presence and precise usage of this field is subject to the relevant profile.

7.2.14 AuthorisationTypeOfCase

Informative for the CSP, to give an indication of the type of case involved. The LEA may choose not to use it or may choose "not specified" if they wish not to provide a classification.

Given as an AuthorisationTypeOfCase DictionaryEntry. The present document defines the dictionary shown in table 7.10. Other dictionaries may be created, including ones with CSP-defined entries which are chosen unilaterally by a CSP. Use of this dictionary or a custom dictionary, as well as the values contained therein, is subject to bilateral agreement between CSP and LEA.

Table 7.10: AuthorisationTypeOfCase Dictionary

Dictionary Owner	Dictionary Name
ETSI	AuthorisationTypeOfCase
Defined DictionaryEntries	
Value	Meaning
ChildExploitationOrChildSexualAbuse	The case relates to a child exploitation or child sexual abuse investigation
Corruption	The case relates to a corruption investigation
Cybercrime	The case relates to a cybercrime investigation
Defamation	The case relates to a defamation investigation
DrugsOrDrugTrafficking	The case relates to a drugs or drug trafficking investigation
HarassmentOrThreatToPersonalSafety	The case relates to a harassment or threat to personal safety investigation
HateSpeech	The case relates to a hate speech investigation
HumanTrafficking	The case relates to a human trafficking investigation
MissingPerson	The case relates to a missing person investigation
MoneyLaundering	The case relates to a money laundering investigation
OtherFinancialCrimeOrFraud	The case relates to a financial crime or fraud investigation, other than money laundering
SexualAbuseOrExploitation	The case relates to a sexual abuse or exploitation investigation, other than those relating to minors
Theft	The case relates to a theft investigation
TerrorismOrThreatToPublicSafety	The case relates to a terrorism or threat to public safety investigation

Defined DictionaryEntries	
Value	Meaning
ViolenceOrCrimeAgainstAPerson	The case relates to a violent crime or crime against a person investigation
Other	The case relates to an investigation that does not fall under any other type of case
NotSpecified	The type of case is not specified or not provided by the LEA

7.2.15 AuthorisationLegalEntity

The AuthorisationLegalEntity field provides an indication of the specific legal or procedural entity that the Authorisation is being used to seek assistance from. Examples include the specific subsidiary or department of a commercial company.

7.2.16 AuthorisationManualInformation

The AuthorisationManualInformation field provides any additional human-readable information regarding the Authorisation. This field shall only be used if required information cannot be contained in any other field. CSPs and LEAs should be aware that the information carried in this field cannot be guaranteed to be machine-processable and may negatively affect processing times.

7.3 DocumentObject

7.3.1 Overview

A DocumentObject represents a particular legal document or instrument related to a given AuthorisationObject or TaskObject. Examples may include the original warrant documentation, or subsequent modification or renewal documents.

The DocumentObject has the following fields.

Table 7.12: DocumentObject

Field	Format	Description	Reference
DocumentReference	LongString (see ETSI TS 103 280 [7]).	Nationally-defined reference for the Document. This is provided to allow correlation with non-electronic processes.	Clause 7.3.2
DocumentName	LongString (see ETSI TS 103 280 [7]).	Name for a specific document.	Clause 7.3.3
DocumentStatus	DocumentStatus Dictionary Entry.	The current status of the Document as determined by the Receiver.	Clause 7.3.4
DocumentDesiredStatus	DesiredDocumentStatus Dictionary Entry.	The current status of the Document as specified by the Sender.	Clause 7.3.5
DocumentTimespan	TimeSpan.	Optional start and end datetimes indicating the period of validity of the Document.	Clause 7.3.6
DocumentType	Document Type.	Indicates the type of document that this Object represents. The list of permissible Document Types is defined by national agreement.	Clause 7.3.7
DocumentProperties	Document Properties.	A list of key-value pairs that define additional properties of the Document in a machine-readable manner. Permissible document properties for each Document Type are defined by national agreement.	Clause 7.3.8
DocumentBody	Complex type.	Contains an electronic copy of the original document e.g. a scanned image.	Clause 7.3.9
DocumentSignature	ApprovalDetails (see annex E).	Details of the approval given for the present document, including any necessary signature information.	Clause 7.3.10

Field	Format	Description	Reference
DocumentInvalidReason	ActionUnsuccessful structure (see clause 6.4.9).	Optional information for the Receiver to indicate why the Document Object is in the Invalid state. Usage for national agreement.	Clause 6.4.9
NationalDocumentParameters	See annex G.	See annex G.	Annex G

7.3.2 DocumentReference

The DocumentReference field gives a nationally-defined reference for the Document. This is provided to allow correlation with non-electronic processes.

7.3.3 DocumentName

The DocumentName field allows a nationally defined name for the Document to be specified. The permissible values and format of this field shall be specified by the relevant national profile.

7.3.4 DocumentStatus

The DocumentStatus field gives the status of the Document as determined by the Receiver. A Sender shall not attempt to set the DocumentStatus as part of a CREATE or UPDATE Request, and a Receiver shall return an Action Unsuccessful Information response if the Sender attempts to do so.

The Status field provides a key mechanism for mapping the content of the Object to the relevant nationally-defined processes. The rules for evaluating the correct value of the Status field shall be defined in the relevant national profile.

Given as a DocumentStatus Dictionary Entry. The DocumentStatus Dictionary is defined in table 7.13 (see annex F for more details on Dictionaries).

Table 7.13: DocumentStatus Dictionary

Dictionary Owner	Dictionary Name
ETSI	DocumentStatus.
Defined DictionaryEntries	
Value	Meaning
AwaitingApproval	The Document is still waiting approval from one or more relevant authorities.
Approved	The Document has been approved by the relevant authorities.
Rejected	The Document has been explicitly denied or rejected by one or more relevant authorities.
Suspended	The Document has been suspended temporarily.
Cancelled	The Document has been permanently cancelled.
Expired	The expiry date for this Document has passed.
Invalid	The Document is invalid due to a problem with the current information populated in the Document Object.

7.3.5 DocumentDesiredStatus

The DocumentDesiredStatus field gives the status of the Document as specified by the Sender.

Given as a DocumentDesiredStatus Dictionary Entry. The DocumentDesiredStatus Dictionary is defined in table 7.14 (see annex F for more details on Dictionaries).

Table 7.14: DocumentDesiredStatus Dictionary

Dictionary Owner	Dictionary Name
ETSI	DocumentDesiredStatus.
Defined DictionaryEntries	
Value	Meaning
AwaitingApproval	The Document is still waiting approval from one or more relevant authorities.
Approved	The Document has been approved by the relevant authorities.
Rejected	The Document has been explicitly denied or rejected by one or more relevant authorities.
Suspended	The Document has been suspended temporarily.
Cancelled	The Document has been permanently cancelled.
Expired	The expiry date for this Document has passed.

7.3.6 DocumentTimespan

The DocumentTimespan field gives the period of time for which the Document is valid. The precise meaning may depend on the type of document being represented. The timestamps shall include a timezone specifier.

Table 7.15: DocumentTimespan

Field	Format	Description
StartTime	QualifiedDateTime (see ETSI TS 103 280 [7]).	Start time for the document.
EndTime	QualifiedDateTime (see ETSI TS 103 280 [7]).	End time for the document.

7.3.7 DocumentType

Indicates the type of document that this Document Object represents. Given as a DocumentType DictionaryEntry. The DocumentType Dictionary is defined below (see annex F for more details on Dictionaries). Since each jurisdiction is likely to have its own particular set of documents, it is expected that most national profiles will need to extend this dictionary.

Table 7.16: DocumentType Dictionary

Dictionary Owner	Dictionary Name
ETSI	DocumentType.
Defined DictionaryEntries	
Value	Meaning
Warrant	This Document represents a legal warrant.

7.3.8 DocumentProperties

A list of key-value pairs that define additional properties of the Document in a machine-readable manner. Permissible property types shall be specified in a dictionary defined by the relevant national profile.

Table 7.17: DocumentProperty

Field	Format	Description
PropertyType	Dictionary entry (see below).	Type of the property. The dictionary of permissible document properties shall be defined by the relevant national profile.
PropertyValue	LongString (see ETSI TS 103 280 [7]).	Value of the property.

7.3.9 DocumentBody

Binary representation of the original paper documentation (e.g. TIFF or JPEG).

Table 7.18: DocumentBody

Field	Format	Description
Contents	Binary data, represented in base64 encoding.	Binary representation of the original paper authorisation documentation.
ContentType	ShortString containing a MIME type as per IETF RFC 2045 [9] and IETF RFC 2046 [10]. The details of permissible MIME types shall be defined by the relevant national profile.	Encoding of the binary Contents file (e.g. "image/jpeg").
Checksum	<p>UTF-8 string containing a checksum of the binary data, given as hexadecimal digits.</p> <p>In version 1.11.1 the ChecksumType field was introduced. New implementations shall support at least the "sha-256" function as defined in IANA Hash Function Textual Names [26].</p> <p>If no ChecksumType is provided, the Checksum field shall contain an MD5 checksum as per IETF RFC 1321 [11].</p>	<p>Checksum to ensure that the Contents field has been transmitted correctly.</p> <p>This mechanism is not intended as a signature.</p>
ChecksumType	UTF-8 string containing a Hash Function Name as defined in IANA Hash Function Textual Names [26].	The type of checksum provided in the Checksum field.

7.3.10 DocumentSignature

The DocumentSignature field gives approval details for the Document represented by the Document Object. This may include signature information.

The DocumentSignature field is specified using the ApprovalDetails structure. See annex E for more details.

7.4 NotificationObject

7.4.1 Overview

The NotificationObject is a means for a Receiver to notify a Sender of any change or update to an HI1Object or set of HI1Objects that was not due to a direct HI-1 Action from the Sender. Such changes may occur for a number of reasons, for example local user interaction at the Receiver.

The use of NotificationObjects are subject to national agreement.

When a Receiver wishes to notify a Sender of changes to an HI1Object or set of HI1Objects, it may create a NotificationObject associated to that Object via the AssociatedObjects field. A NotificationObject may be associated to more than one Object. Similarly, an HI1Object may be associated to multiple NotificationObjects as it may be subject to a number of changes over time.

NotificationObjects may only be created by the Receiver. A Receiver that receives a CREATE Action attempting to create a NotificationObject shall return an error.

The NotificationObject consists of the following fields. Further details are given in clause 7.4.2.

Table 7.19: NotificationObject

Field	Format	Description	Reference
NotificationDetails	LongString (see ETSI TS 103 280 [7]).	Human readable information regarding the notification.	Clause 7.4.2
NotificationType	NotificationType Dictionary Entry (see clause 7.4.3).	Identifies the type of notification, for use in automating workflow processes. The format and acceptable values for this field shall be defined by the relevant national profile.	Clause 7.4.3
NewNotification	Boolean.	Indication that this is a new notification. See clause 7.4.4 for more details.	Clause 7.4.4
NotificationTimestamp	QualifiedDateTime (see ETSI TS 103 280 [7]).	Timestamp indicating the time of the Notification.	Clause 7.4.5
StatusOfAssociatedObjects	ListOfAssociatedObjectStatus (see clause 7.4.7).	Provides a list of references to associated objects together with the status of the associated objects.	Clause 7.4.7
NationalNotificationParameters	See annex G.	See annex G.	Clause 7.4.6

7.4.2 NotificationDetails

The NotificationDetails field shall carry human-readable information regarding the nature of the notification (for example, a summary of any changes, or the reason for the notification).

A Receiver shall ignore any attempt by a Sender to UPDATE the value of the Notification details field.

7.4.3 NotificationType

The NotificationType field indicates the type of Notification being given. It is given as a NotificationType Dictionary Entry. The NotificationType Dictionary is defined in table 7.20 (see annex F for more details on Dictionaries). Since the list of notification types is tightly coupled to national processes and workflow, it is expected that each national profile will need to extend this dictionary.

Table 7.20: NotificationType Dictionary

Dictionary Owner	Dictionary Name
ETSI	NotificationType.
Defined DictionaryEntries	
Value	Meaning
General	A general notification that a change has occurred with the specified Objects.

7.4.4 NewNotification

The NewNotification flag is used to indicate whether the notification is new, and therefore whether it should be returned in a query for New Notifications (see clause 6.4.8).

When a Receiver creates a new NotificationObject, the NewNotification flag shall be set to True. The NewNotification Flag may be set to False, thereby removing it from the Notification Objects returned by the Receiver when queried for new Notifications, in any of the following ways:

- Once a Sender is satisfied that it has been notified, it may UPDATE the NewNotification field to False explicitly.
- Once a Receiver is satisfied that the Sender has been notified (e.g. upon Receiving a GET or UPDATE for all AssociatedObjects) the Receiver may change the NewNotification field to False. The logic and circumstances under which the Receiver makes such a change shall be specified by the relevant national profile.

Archiving and persistence of Notification Objects once the NewNotification flag has been cleared is a matter for national agreement.

7.4.5 NotificationTimestamp

The NotificationTimestamp field shall be set by the Receiver to the time at which the notification event occurred.

The Receiver shall ignore any attempt by a Sender to UPDATE the value of the NotificationTimestamp field.

7.4.6 NationalNotificationParameters

The use and definition of the NationalNotificationParameters structure is for national agreement. See annex G.

7.4.7 StatusOfAssociatedObjects

The StatusOfAssociatedObjects field can be used to inform the Sender of an HIObject or set of HIObjects that the status of these objects has changed to value given by this field to avoid that Sender has to send a GET Message to retrieve the new status value. The values are defined in the dictionaries for the status value for the HIObjects. The StatusOfAssociatedObjects is a ListOfAssociatedObjectStatus that contains one or more AssociatedObjectStatus elements.

The following table defines the structure of AssociatedObjectStatus.

Table 7.20a: AssociatedObjectStatus

Field	Format	Description
AssociatedObject	ObjectIdentifier (see clause 7.1.2).	Specifies the associated object that the notification applies to.
Status	AuthorisationStatus Dictionary (see clause 7.2.5), DocumentStatus Dictionary (see clause 7.3.4), TaskStatus Dictionary (see clause 8.2.3), LDTaskStatus Dictionary (see clause 8.3.3), LPTaskStatus Dictionary (see clause 8.4.2).	Indicates the new status value of the associated object. The dictionary to use depends on the type of the associated object.
Details	LongString (see ETSI TS 103 280 [7]).	Optional human readable information regarding the status change of the associated object.

7.5 TrafficPolicyObject

7.5.1 Overview

The TrafficPolicyObject represents a policy from an LEA which is to be applied to the intercepted materials as part of an LITaskObject. An LEA may associate multiple TrafficPolicyObjects to an LITaskObject, using the LITaskObject's ListOfTrafficPolicyObjects field (see clause 8.2.13.2).

A change to a traffic policy should be reflected in the data delivered by LITasks which use that policy in a timely fashion and not require re-tasking.

A Traffic Policy is an ordered list of rules (represented by TrafficRuleObjects, see clause 7.6) where the action of the first matching rule is applied to the traffic.

The TrafficPolicyObject consists of the fields shown in table 7.21.

Table 7.21: TrafficPolicyObject

Field	Format	Description	Reference	M/C/O
TrafficPolicyName	ShortString	Optional human readable name for TrafficPolicy	ETSI TS 103 280 [7], clause 6.29	O
TrafficRules	List of TrafficRuleReferences	Ordered list of references to TrafficRule objects	Table 7.22	M

The TrafficPolicyObject shall include at least one TrafficRuleReference. Each TrafficRuleReference consists of the fields shown in table 7.22.

Table 7.22: TrafficRuleReference

Field	Format	Description	Reference	M/C/O
Order	Positive Integer	Determines the order in which rules are considered	Clause 7.5.2	M
ObjectIdentifier	ObjectIdentifier	Object Identifier of associated TrafficRuleObject	Clause 7.6	M

7.5.2 Order

TrafficRuleReferences are considered in ascending order according to the Order field. If all of the criteria listed in the TrafficRuleObject referenced by the ObjectIdentifier field are matched (see clause 7.6.2), then the action described in the referenced TrafficRuleObject's Action field is taken (see clause 7.6.3) and no further TrafficRuleReferences are considered. Otherwise, the next TrafficRuleReference is evaluated.

The value of Order shall be unique within the context of a TrafficPolicyObject.

7.6 TrafficRuleObject

7.6.1 Overview

Table 7.23: TrafficRule

Field	Format	Description	Reference	M/C/O
Criteria	List of TrafficCriteria	List of rule criteria all of which shall match for this rule to apply	Clause 7.6.2	M
Action	TrafficAction Dictionary Entry	The action to take with matching criteria	Clause 7.6.3	M
Parameters	ActionParameters	Parameters that are applicable to the action	Clause 7.6.4	C

At least one filter criteria shall be given, along with a TrafficAction. Parameters are only applicable to specific types of action.

7.6.2 TrafficCriteria

7.6.2.1 Overview

The TrafficCriteria structure defines whether a TrafficRule applies to a particular piece of intercepted traffic or not.

If multiple TrafficCriteria are given, they are logically ANDed together - that is, the intercepted traffic shall match all of them in order for the TrafficRule to be considered matching.

7.6.2.2 IPPolicyCriteria

7.6.2.2.1 Overview

IPPolicyCriteria is one type of TrafficCriteria. The IPPolicyCriteria structure defines a set of IP based criteria which can be used to determine if a rule applies.

Table 7.24: IPPolicyCriteria

Field	Format	Description	Reference	M/C/O
IPProtocol	IPProtocol	IP Protocol of the traffic.	ETSI TS 103 280 [7], clause 6.55	O
SourceIPRange	IPCIDR	Match IP packets with a source address within this range.	ETSI TS 103 280 [7], clause 6.16	O
SourcePortRange	PortRange	Match TCP/UDP packets with a source port within this range.	ETSI TS 103 280 [7], clause 6.22	O
DestinationIPRange	IPCIDR	Match IP packets with a destination address within this range.	ETSI TS 103 280 [7], clause 6.16	O
DestinationPortRange	PortRange	Match TCP/UDP packets with a destination port within this range.	ETSI TS 103 280 [7], clause 6.22	O
BothDirections	Boolean	Also match packets in the other direction.	Clause 7.6.2.2.2	O

At least one of SourceIPRange, SourcePortRange, DestinationIPRange or DestinationPortRange shall be given.

Where IPProtocol and PortRanges (SourcePortRange or DestinationPortRange) are included, all shall indicate the same protocol type. Use IPProtocol value 6 for TCP and value 17 for UDP.

7.6.2.2.2 BothDirections

The presence of the BothDirections field indicates that packets matching in both directions match the criteria.

If the BothDirections field is present, the packet is considered a match if either:

- all of the SourceIPRange, SourcePortRange, DestinationIPRange, and DestinationPortRange IPPolicyCriteria that are present match their respective packet headers per table 7.24; or
- the SourceIPRange and SourcePortRange IPPolicyCriteria that are present match their respective packet destination headers, and the DestinationIPRange and DestinationPortRange IPPolicyCriteria that are present match their respective packet source headers.

7.6.2.3 MobileAccessPolicyCriteria

7.6.2.3.1 Overview

MobileAccessPolicyCriteria defines a criteria based on the APN or DNN of a particular traffic flow.

Table 7.24a: MobileAccessPolicyCriteria

Field	Format	Description	Reference	M/C/O
APN	APN Network Identifier	Match traffic sent to or from the specified APN	Presentation format specified in 3GPP TS 23.003 [i.6], clause 9.1	O
DNN	DNN Network Identifier	Match traffic sent to or from the specified DNN	Presentation format specified in 3GPP TS 23.003 [i.6], clause 9A	O

One of APN or DNN shall be given in a particular MobileAccessPolicyCriteria.

7.6.2.4 EthernetPolicyCriteria

7.6.2.4.1 Overview

EthernetPolicyCriteria is one type of TrafficCriteria. The EthernetPolicyCriteria structure defines a set of Ethernet based criteria which can be used to determine if a rule applies.

Table 7.24b: EthernetPolicyCriteria

Field	Format	Description	Reference	M/C/O
SourceMACAddress	MACAddress	Match Ethernet frames with this source MAC address.	ETSI TS 103 280 [7], clause 6.25	O
DestinationMACAddress	MACAddress	Match Ethernet frames with this destination MAC address.	ETSI TS 103 280 [7], clause 6.25	O
VLANCriteria	VLANCriteria	Match Ethernet frames with the VLANCriteria.	Table 7.24c	O
BothDirections	Boolean	Also match frames in the other direction.	Clause 7.6.2.4.2	O

At least one of SourceMACAddress, DestinationMACAddress or VLANCriteria shall be given.

Table 7.24c: VLANCriteria

Field	Format	Description	Reference
OuterVLANs	VLANIDList	Match Ethernet frames with the outer VLAN IDs. When more than one VLAN ID is provided, the VLAN IDs shall be matched from outermost to innermost in order of the sequence sent in the OuterVLANs element	ETSI TS 103 280 [7], clause 6.56

7.6.2.4.2 BothDirections

The presence of the BothDirections field indicates that frames matching in both directions match the criteria.

If the BothDirections field is present, the frame is considered a match if either:

- all of the SourceMACAddress, DestinationMACAddress or VLANCriteria that are present match their respective frame headers per table 7.24b; or
- the SourceMACAddress, VLANCriteria or EthernetPolicyCriteria that are present match their respective frame destination header, and the DestinationMACAddress, VLANCriteria or EthernetPolicyCriteria that are present match their respective frame source header.

7.6.2.5 RCSPolicyCriteria

RCSPolicyCriteria defines a criterion based on the communication service identifier of an RCS (Rich Communication Suite) service flow.

Table 7.24d: RCSPolicyCriteria

Field	Format	Description	Reference	M/C/O
CommunicationServiceID	ShortString	Match service flows of a specific RCS communication service identified by CommunicationServiceID. The value given shall be any of the feature tags of RCS services listed in GSMA RCC.07 [i.12] clause 2.4.4.1, table 3.	ETSI TS 103 280 [7], clause 6.29	M

7.6.3 Action

Action to be applied to the policy. Given as an Action DictionaryEntry. The TrafficAction Dictionary is defined below (see annex F for more details on Dictionaries).

Table 7.25: TrafficAction Dictionary

Dictionary Owner	Dictionary Name
ETSI	TrafficAction.
Defined DictionaryEntries	
Value	Meaning
PDSR	Traffic that matches this policy is delivered as Packet Data Summary Reports.
PDHR	Traffic that matches this policy is delivered as Packet Data Header Reports.
NotDelivered	Traffic that matches this policy is not delivered.
Delivered	Traffic that matches this policy is delivered.
Truncate	Deliver only a specified number of the first octets of each IP or ethernet datagram. The Truncate Action Parameters (see clause 7.6.4.2) shall be provided when this TrafficAction is used.

NOTE: Traffic Policies are evaluated in the order defined within TrafficRuleReference. This allows the TrafficAction Deliver to be used to define in a TrafficRuleObject that delivers a specific flow within a broader flow that would otherwise be summarized or suppressed by a later TrafficRuleObject.

7.6.4 Parameters

7.6.4.1 Overview

Parameters that are applicable to an action. Given as an action-specific choice of parameters.

7.6.4.2 Truncate Action Parameters

TruncateActionParameters defines the parameters that are applicable to the Truncate action.

Table 7.26: TruncateActionParameters

Field	Format	Description	Reference	M/C/O
NumberOfOctets	Non-negative Integer	Request to deliver only the specified number of the first octets of all the intercepted IP or ethernet datagrams pertaining to the target.	ETSI TS 102 232-3 [16], clause 7.2 [16], ETSI TS 102 232-4 [17], clause 7.2 [17].	M
ProvideOriginalLength	Boolean	Request the delivery of the original length in octets of the IP datagrams before the applied truncation, if applicable. The indication shall be provided if the required functionality in the referenced clause should be enabled or not.	ETSI TS 102 232-3 [16], clause 7.2 [16].	C

8 Task Objects

8.1 Overview

This clause defines a set of HI1Object definitions that can be used to describe "Tasks". These Objects are intended to describe the technical details of a request or instruction, and will typically be associated with an AuthorisationObject which represents the legal basis for the technical request.

The present document defines three types of Task Objects; the LITaskObject, which represents a technical request to perform Lawful Intercept, the LDTaskObject, which represents a technical request to perform Lawful Disclosure, and the LPTaskObject, which represents a technical request to perform Lawful Preservation.

Implementers should refer to applicable law to determine the lawful retention period of the Task Objects when Task processing is completed. If and for how long Tasks are required to be stored is out of scope of the present document.

8.2 LITaskObject

8.2.1 Overview

An LITaskObject represents the state of an LI task - that is, the act of intercepting of a communication. This corresponds to the WarrantTargetID and WarrantTechSpec elements defined in ETSI TR 103 690 [i.1]. In general, multiple tasks may be authorised by a single warrant.

The LITaskObject consists of the following fields. Further details are given in clause 8.2.2.

Table 8.1: LITaskObject

Field	Format	Description	Reference
Reference	LIID (see ETSI TS 103 280 [7]).	LIID assigned to the product of task.	Clause 8.2.2
Status	TaskStatus Dictionary Entry.	The current status of the task as determined by the Receiver.	Clause 8.2.3
DesiredStatus	TaskDesiredStatus Dictionary Entry.	The current status of the task as specified by the Sender.	Clause 8.2.4
TimeSpan	Collection of QualifiedDateTimes (see ETSI TS 103 280 [7]).	Indicated the period of time for which task should occur, as well as provisioning and deprovisioning times.	Clause 8.2.5
TargetIdentifier	TargetIdentifier (see clause 8.2.6).	The communication address or technical identifier used to identify the target of task. Given as a list of TargetIdentifier types (see clause 7.3.6) which are combined (with ordering and Boolean ANDed together) to identify the target's traffic.	Clause 8.2.6
DeliveryType	DictionaryEntry (see clause 8.2.7).	Typically for interception indicates whether the interception should contain IRI, CC or both.	Clause 8.2.7
DeliveryDetails	List of DeliveryDestination structures (see clause 8.2.8).	Destination(s) for the intercepted LI traffic.	Clause 8.2.8
ApprovalDetails	ApprovalDetails (see annex E).	Details regarding the approval for this Task, including dates and signatures where appropriate.	Clause 8.2.9
CSPID	EndpointID (see clause 6.2.4).	Describes the CSP required to implement the Task.	Clause 8.2.10
HandlingProfile	DictionaryEntry (see clause 8.2.11).	A dictionary entry which gives the name of a handling profile that represents a set of configuration information associated with this task.	Clause 8.2.11
InvalidReason	ActionUnsuccessful structure (see clause 6.4.9).	Optional information for the Receiver to indicate why the Object is in a certain state (such as Invalid or Rejected). Usage for national agreement. See note.	Clause 6.4.9
Flags	TaskFlags (see clause 8.2.12).	A set of flags associated with the Task Object.	Clause 8.2.12
NationalLITaskingParameters	See annex G.	See annex G.	Annex G

Field	Format	Description	Reference
ListOfTrafficPolicyReferences	ListOfTrafficPolicyReferences.	Ordered list of TrafficPolicyReferences to be applied to the LITaskObject.	Clause 8.2.13
NOTE: For backwards-compatibility reasons this field is named InvalidReason even though it is permitted to indicate the reasons for other states. The definition above does not preclude the use of this field for non-error-related states, but such use should be clearly signalled by the relevant national agreement.			

8.2.2 Reference

The Reference field gives a reference identifier for the Task, for correlation with other processes. For LI, this shall be set to the LIID that will be assigned to the product of interception. Format will be as per ETSI TS 103 280 [7].

8.2.3 Status

The Status field gives the status of the LITaskObject as determined by the Receiver. A Sender shall not attempt to set the Status as part of a CREATE or UPDATE Request, and a Receiver shall return an Action Unsuccessful Information response if the Sender attempts to do so.

The Status field provides a key mechanism for mapping the content of the Object to the relevant nationally-defined processes. The rules for evaluating the correct value of the Status field shall be defined in the relevant national profile.

Given as a TaskStatus Dictionary Entry. The TaskStatus Dictionary is defined in table 8.2 (see annex F for more details on Dictionaries).

Table 8.2: TaskStatus Dictionary

Dictionary Owner	Dictionary Name
ETSI	TaskStatus.
Defined DictionaryEntries	
Value	Meaning
AwaitingApproval	The Task is still waiting approval from one or more relevant authorities.
AwaitingProvisioning	The Task is approved, but is not yet provisioned in the LI system.
Active	The Task is active and can produce LI traffic.
Rejected	The Task has been explicitly denied or rejected by one or more relevant authorities.
Suspended	The Task has been suspended temporarily.
Cancelled	The Task has been permanently cancelled.
Expired	The expiry date for this Task has passed, meaning that the Task has lapsed.
Error	The Task is not active due to a problem with the underlying LI system.
Invalid	The Task is not active due to a problem with the current information populated in the Task Object.

8.2.4 DesiredStatus

The DesiredStatus field gives the status of the LITaskObject as determined by the Sender.

Given as a TaskDesiredStatus Dictionary Entry. The TaskDesiredStatus Dictionary is defined in table 8.3 (see annex F for more details on Dictionaries).

Table 8.3: TaskDesiredStatus Dictionary

Dictionary Owner	Dictionary Name
ETSI	TaskDesiredStatus.
Defined DictionaryEntries	
Value	Meaning
AwaitingApproval	The Task is still waiting approval from one or more relevant authorities.
AwaitingProvisioning	The Task is approved, but is not yet provisioned in the LI system.
Active	The Task is active and can produce LI traffic.
Rejected	The Task has been explicitly denied or rejected by one or more relevant authorities.
Suspended	The Task has been suspended temporarily.
Cancelled	The Task has been permanently cancelled.
Expired	The expiry date for this Task has passed, meaning that the Task has lapsed.

8.2.5 TimeSpan

The period for which the interception is active. May not be identical to the AuthorisationTimespan (although it is likely that national laws will require it to be within the AuthorisationTimespan). Given as a TaskTimeSpan structure as defined in table 8.4.

Table 8.4: TaskTimeSpan

Field	Format	Description
StartTime	QualifiedDateTime (see ETSI TS 103 280 [7]).	Start time for the interception.
EndTime	QualifiedDateTime (see ETSI TS 103 280 [7]).	End time for the interception.
TerminationTime	QualifiedDateTime (see ETSI TS 103 280 [7]).	Termination or cancellation timestamp, in the event that the Task is terminated prior to its scheduled end time.
Provisioning Time	QualifiedDateTime (see ETSI TS 103 280 [7]).	Provisioning time for the interception.
DeprovisioningTime	QualifiedDateTime (see ETSI TS 103 280 [7]).	Deprovisioning time for the interception.

8.2.6 TargetIdentifier

8.2.6.1 Overview

The TargetIdentifier specifies the communications address or technical identifier used to identify the target of the Task in conjunction with TargetIdentifierSubtype. It consists of the following fields.

Table 8.5: TargetIdentifier

Field	Format	Description
TargetIdentifierValues	List of TargetIdentifierValue structures (see clause 8.2.6.2).	Specifies the technical identifier(s) used to identify the target of the Task.
ServiceType	ServiceType (see clause 8.2.6.4).	Specifies the service(s) to be intercepted.
TargetIdentifierSubtype	TargetIdentifierSubtype (see clause 8.3.5.6).	Indicates the kind of CSP entity (such as kind of account) targeted by this request. Used to limit the disclosure of data to the that kind of CSP entity known to the requestor, if applicable.

8.2.6.2 TargetIdentifierValues Field

The TargetIdentifierValues field contains a list of TargetIdentifierValue structures, which are combined (with ordering and Boolean ANDed together) to identify the target's traffic. Each TargetIdentifierValue structure contains the following fields.

Table 8.6: TargetIdentifierValue

Field	Format	Description
FormatType	As defined below.	Specifies a Target Identifier Format (see below) which defines the format for the Target Identifier Value fields. See annex C for the list of Target Identifier Formats defined by ETSI. Other definitions may be managed on a national basis.
Value	LongString (see ETSI TS 103 280 [7]).	Additional formatting information is given by the Target Identifier Format.

The TargetIdentifier FormatType and format descriptions are given in annex C.

The Receiver is responsible for checking that the format of the Target Identifier Value matches the format defined for the Target Identifier Format Type. If any of the Target Identifier Values are not correctly formatted, the Action should be rejected.

8.2.6.3 FormatType

A TargetIdentifier FormatType uniquely identifies a particular TargetIdentifier Format. It can be used to retrieve the correct Target Identifier Format definition for a given Target Identifier. It consists of the following fields.

Table 8.7: TargetIdentifier FormatType

Field	Format	Description
FormatOwner	ShortString (see ETSI TS 103 280 [7]).	Name of the Owner of the Format definition. See below.
FormatName	ShortString (see ETSI TS 103 280 [7]).	Uniquely identifies the format definition within the Owner.

A Format owner is specified by a string value. The following owners are defined by the present document:

- "ETSI": The Format is owned by ETSI, and defined in the present document in annex C.
- A valid ISO 3166-1 [14] country code: The Format is owned and defined by the relevant national authority for the country specified by the country code.

A Format definition shall contain, at a minimum, the following information.

Table 8.8: TargetIdentifier Format Definition

Field	Format	Description
FormatOwner	ShortString (see ETSI TS 103 280 [7]).	Identifies the Owner of the Format definition. See above.
FormatName	ShortString (see ETSI TS 103 280 [7]).	Identifies the format, unique within the Format Owner.
Description	LongString (see ETSI TS 103 280 [7]).	Human-readable description associated with the Format.
Format	IEEE POSIX 1003.1™ [13] ERE Regular Expression.	Regular expression defining the permissible contents of the field. If absent, any UTF-8 string is permitted, subject to the length restriction of the field.

See annex C for the list of TargetIdentifier Formats defined by ETSI. Other definitions may be managed on a national basis.

8.2.6.4 Task Service Type

Type of service or services to intercept using the specified TargetIdentifiers.

Given as a list of TaskServiceType DictionaryEntries. The usage and meaning of the Service Type is likely to be closely coupled to national legislation, as will the permissible combinations of TargetIdentifier Types and Service Types. It is therefore expected that most national profiles will need to define their own extensions to this dictionary.

Table 8.9: TaskServiceType Dictionary

Dictionary Owner	Dictionary Name
ETSI	TaskServiceType.
Defined DictionaryEntries	
Value	Meaning
The present document does not define any dictionary entries for this dictionary.	

8.2.7 DeliveryType

Delivery type of the Task. Given as a TaskDeliveryType DictionaryEntry. The TaskDeliveryType Dictionary is defined below (see annex F for more details on Dictionaries).

Table 8.10: TaskDeliveryType Dictionary

Dictionary Owner	Dictionary Name
ETSI	TaskDeliveryType.
Defined DictionaryEntries	
Value	Meaning
IRIOnly	Only IRI is delivered.
CCOnly	Only CC is delivered.
IRIandCC	Both IRI and CC are delivered.

8.2.8 TaskDeliveryDetails

8.2.8.1 Overview

The TaskDeliveryDetails field indicates where intercepted traffic should be delivered.

The TaskDeliveryDetails field consists of a list of DeliveryDestination structures. Each entry in the list represents a desired destination for traffic related to the Task.

Limits on the type, number or combinations of DeliveryDestination for a given type of Task shall be specified by the relevant national profile.

8.2.8.2 DeliveryDestination

The DeliveryDestination structure contains the following fields.

Table 8.11: DeliveryDestination

Field	Format	Description
DeliveryAddress	DeliveryAddress (see clause 8.2.8.3).	The address to which the traffic for this Task should be delivered.
EncryptionDetails	NationalEncryptionDetails.	Details regarding the encryption to be applied to traffic delivered to this destination. Shall be defined by the relevant national profile.
IRIorCC	TaskDeliveryType (see clause 8.2.7).	Specifies whether IRI, CC, or IRI and CC should be delivered to this destination.
HandoverFormat	HandoverFormat DictionaryEntry (see clause 8.2.8.4).	Specifies the handover format to be used.
DeliveryProfile	DictionaryEntry.	A dictionary entry which gives the name of a delivery profile that represents a set of configuration information associated with the destination and delivery of the traffic from this Task. If used, the dictionary shall be defined by the relevant national profile.
NationalDeliveryParameters	See annex G.	See annex G.

8.2.8.3 DeliveryAddress

The DeliveryAddress is specified in one of the following formats.

Table 8.12: DeliveryAddress

Field	Format	Description
IPv4Address	IPv4Address (see ETSI TS 103 280 [7]).	IPv4 destination.
IPv6Address	IPv6Address (see ETSI TS 103 280 [7]).	IPv6 destination.
IPAddressPort	IPAddressPort (see ETSI TS 103 280 [7]).	Combination of an IP Address (IPv4 or IPv6) and a Port number.
IPAddressPortRange	IPAddressPortRange (see ETSI TS 103 280 [7]).	Combination of an IP Address (IPv4 or IPv6) and a Port Range.
E164number	InternationalE164 (see ETSI TS 103 280 [7]).	E.164 destination.
FTPAddress	URL as per xs:anyURI but conformant to the FTP scheme defined in IETF RFC 1738 [8].	IETF RFC 1738 [8] allows specification of hostname, port, path and username.
URL	xs:anyURI.	URL destination.
FQDN	LongString (see ETSI TS 103 280 [7]).	FQDN of the destination.
EmailAddress	EmailAddress (see ETSI TS 103 280 [7]).	Email address of the destination.
EndpointID	EndpointID (see clause 6.2.4).	EndpointID of the destination.
DeliveryInformationID	LongString (see ETSI TS 103 280 [7]).	This value, which shall be locally unique for a given LEA, is provided by the LEA to the CSP to identify delivery destination information that has been provided by the LEA to the CSP out-of-band of the present document, e.g. identifying preconfigured LEMF destinations.

8.2.8.4 HandoverFormat

The HandoverFormat dictionary is defined in table 8.13 (see annex F for more details on Dictionaries).

Table 8.13: HandoverFormat Dictionary

Dictionary Owner	Dictionary Name
ETSI	HandoverFormat.
Defined DictionaryEntries	
Value	Meaning
TS102232-2	Handed over in ETSI TS 102 232-2 [15] format.
TS102232-3	Handed over in ETSI TS 102 232-3 [16] format.
TS102232-4	Handed over in ETSI TS 102 232-4 [17] format.
TS102232-5	Handed over in ETSI TS 102 232-5 [18] format.
TS102232-6	Handed over in ETSI TS 102 232-6 [19] format.
TS102232-7	Handed over in ETSI TS 102 232-7 [20] format.
TS103707	Handed over in ETSI TS 103 707 [24] format.

8.2.9 ApprovalDetails

The ApprovalDetails field gives details regarding the approval for the Task. The information is specified in using the ApprovalDetails structure given in annex E.

8.2.10 CSPID

The CSPID field gives a globally unique CSP Identifier that identifies the CSP required to implement the Task.

8.2.11 HandlingProfile

The HandlingProfile field gives a dictionary entry which gives the name of a handling profile that represents a set of configuration information associated with this task.

The use of this field is for national agreement. If used, the dictionary of permissible values shall be defined by the relevant national profile.

8.2.12 Flags

The Flags field allows a set of multiple flags to be associated with the LITaskObject. Each flag is given as a TaskFlag Dictionary Entry. If a flag is present in the Flags field, then the meaning given as part of that flag's definition shall be taken to apply.

The TaskFlag Dictionary is defined in table 8.14 (see annex F for more details on Dictionaries).

Table 8.14: TaskFlag Dictionary

Dictionary Owner	Dictionary Name
ETSI	TaskFlag.
Defined DictionaryEntries	
Value	Meaning
IsTest	Indicates that the current Task is for test purposes. This may alter the process or documentation accompanying the authorisation.
IsEmergency	Indicates if the LI Task was issued under nationally-defined emergency procedures. The circumstances and consequences for setting the field shall be defined by the relevant national profile (see clause B.1.3).
IsNonLocal	Indicates that the current Task shall be intercepted as a non-local identity.
IsLocal	Indicates that the current Task shall be intercepted as local identity. If both the IsNonLocal and IsLocal flag are absent, the Task shall be intercepted as a local identity unless otherwise agreed.

8.2.13 ListOfTrafficPolicyReferences

8.2.13.1 Overview

The ListOfTrafficPolicyReferences fields gives an ordered list of TrafficPolicyReferences that shall be applied to the intercepted traffic (see clause 7.6). The TrafficPolicyReference fields contain elements defined in table 8.14a.

Table 8.14a: TrafficPolicyReference

Field	Format	Description	Reference	M/C/O
Order	Positive Integer	Determines the order in which TrafficPolicyObjects are considered	Clause 8.2.13.2	M
ObjectIdentifier	ObjectIdentifier	Object Identifier of associated TrafficPolicyObject	Clause 7.1.2	M

8.2.13.2 Order

TrafficPolicyReferences are considered in ascending order according to the Order field. Once a rule in the TrafficPolicyObject referenced by the ObjectIdentifier field is matched and the action in the referenced TrafficPolicyObject is taken (see clause 7.6.3), then no further TrafficPolicyReferences are evaluated. If no rules are matched in any of the referenced TrafficPolicyObjects, then the traffic shall be delivered as-is.

The value of Order shall be unique within the context of a LITaskObject.

8.3 LDTaskObject

8.3.1 Overview

An LDTaskObject represents the state of an LD Task - that is, the act of disclosing information. This corresponds to the WarrantTargetID and WarrantTechSpec elements defined in ETSI TR 103 690 [i.1]. In general, multiple tasks may be authorised by a single warrant.

The LDTaskObject consists of the following fields.

Table 8.15: LDTaskObject

Field	Format	Description	Reference
Reference	LDID (see ETSI TS 103 280 [7]).	LDID assigned to the product of task.	Clause 8.3.2
Status	LDTaskStatus Dictionary Entry.	The current status of the task as determined by the Receiver.	Clause 8.3.3
StatusReason	ActionUnsuccessful structure (see clause 6.4.9).	Optional information for the Receiver to indicate why the Object is in a certain state (such as Invalid or Rejected). Usage for national agreement.	Clause 6.4.9
DesiredStatus	LDTaskDesiredStatus Dictionary Entry.	The current status of the task as specified by the Sender.	Clause 8.3.4
RequestDetails	LDRequestDetails (see clause 8.3.5).	Details regarding the content of the disclosure request, such as identifiers and dates.	Clause 8.3.5
DeliveryDetails	List of LDDeliveryDestination structures (see clause 8.3.6).	Destination(s) for the disclosure product.	Clause 8.3.6
ApprovalDetails	ApprovalDetails (see annex E).	Details regarding the approval for this Task, including dates and signatures where appropriate.	Clause 8.2.9
CSPID	EndpointID (see clause 6.2.4).	Describes the CSP required to implement the Task.	Clause 8.2.10
HandlingProfile	LDHandlingProfile (see clause 8.2.11).	A dictionary entry which gives the name of a handling profile that represents a set of configuration information associated with this task.	Clause 8.2.11
Flags	LDTaskFlags (see clause 8.3.7).	A set of flags associated with the Task Object.	Clause 8.3.7
AlternativePreservationReferences	List of AlternativePreservationReference values (see clause 8.3.8).	Indication of any prior preservation requests related to this disclosure, where appropriate.	Clause 8.3.8
NationalLDTaskingParameters	See annex G.	See annex G.	Annex G

8.3.2 Reference

The Reference field gives a reference identifier for the Task, for correlation with other processes. For LD, this shall be set to the LDID that will be assigned to the product of the disclosure. Format will be as per ETSI TS 103 280 [7].

8.3.3 Status

The Status field gives the status of the LDTaskObject as determined by the Receiver. A Sender shall not attempt to set the Status as part of a CREATE or UPDATE Request, and a Receiver shall return an Action Unsuccessful Information Response if the Sender attempts to do so.

The Status field provides a key mechanism for mapping the content of the Object to the relevant nationally-defined processes. The rules for evaluating the correct value of the Status field shall be defined in the relevant national profile.

Given as a LDTaskStatus Dictionary Entry. The LDTaskStatus Dictionary is defined in table 8.16 (see annex F for more details on Dictionaries).

Table 8.16: LDTaskStatus Dictionary

Dictionary Owner	Dictionary Name
ETSI	LDTaskStatus.
Defined DictionaryEntries	
Value	Meaning
AwaitingApproval	The Task is still awaiting approval from one or more relevant authorities.
AwaitingDisclosure	The Task is approved by the relevant authorities, but is not yet approved and/or processed by the LD system.
Disclosed	The Task has been processed and the product has been disclosed by the LD system.
DisclosureNotAvailable	The Task has been processed and the CSP has determined there is no product available to disclose.
Rejected	The Task has been explicitly denied or rejected by one or more relevant authorities or by the CSP.
Cancelled	The Task has been permanently cancelled.
Error	The Task has not been processed due to a problem with the underlying LD system.
Invalid	The Task has not been processed to a problem with the current information populated in the Task Object.

8.3.4 DesiredStatus

The DesiredStatus field gives the status of the LDTaskObject as determined by the Sender.

Given as a LDTaskDesiredStatus Dictionary Entry. The LDTaskDesiredStatus Dictionary is defined in table 8.17 (see annex F for more details on Dictionaries).

Table 8.17: LDTaskDesiredStatus Dictionary

Dictionary Owner	Dictionary Name
ETSI	LDTaskDesiredStatus.
Defined DictionaryEntries	
Value	Meaning
AwaitingApproval	The Task is still awaiting approval from one or more relevant authorities.
AwaitingDisclosure	The Task is approved by the relevant authorities, but is not yet approved and/or processed by the LD system.
Disclosed	The Task has been processed and the product has been disclosed by the LD system.
Rejected	The Task has been explicitly denied or rejected by one or more relevant authorities or by the CSP.
Cancelled	The Task has been permanently cancelled.

8.3.5 RequestDetails

8.3.5.1 Overview

The RequestDetails structure specifies the content of the disclosure request. It consists of the following fields.

Table 8.18: LDRequestDetails

Field	Format	Description
Type	RequestType (see clause 8.3.5.2).	Specifies the products to be disclosed.
StartTime	QualifiedDateTime (see ETSI TS 103 280 [7]).	If a date/time range needs to be applied to the request, the StartTime and EndTime shall be provided.
EndTime	QualifiedDateTime (see ETSI TS 103 280 [7]).	If a date/time range needs to be applied to the request, the StartTime and EndTime shall be provided.
ObservedTime	QualifiedDateTime (see ETSI TS 103 280 [7]).	If an observed date/time needs to be applied to the request. This field may be used to indicate at which date/time a certain value was observed by the requestor. If multiple observed dates/times need to be applied to the request, the ObservedTimes field shall be used instead of this field.
ObservedTimes	List of QualifiedDateTime (see ETSI TS 103 280 [7]).	If multiple observed dates/times all need to be applied to the request. This field may be used to indicate at which dates/times a certain value was observed by the requestor. This field shall only be used if multiple dates/times need to be applied to the request.
RequestValues	List of RequestValue structures (see clause 8.3.5.3).	Specifies the value(s) used to define the disclosure request.
Subtype	List of LDRequestSubtype DictionaryEntries.	Indicates the subtype of CSP product or products to be disclosed, for use in cases where this cannot be sufficiently well-determined from the RequestType field. Optional.
TargetIdentifier Subtype	TargetIdentifierSubtype (see clause 8.3.5.6).	Indicates the kind of CSP entity (such as kind of account) targeted by this request. Used to limit the disclosure of data to the that kind of CSP entity known to the requestor, if applicable. Optional.

8.3.5.2 RequestType

Type of disclosure or disclosures to produce using the specified RequestDetails.

Given as a list of RequestType DictionaryEntries. The usage and meaning of the Request Type is likely to be closely coupled to national legislation, as will the permissible combinations of Request Values and Request Types. It is therefore expected that most national profiles will need to define their own extensions to this dictionary.

Table 8.19: RequestType Dictionary

Dictionary Owner	Dictionary Name
ETSI	RequestType.
Defined DictionaryEntries	
Value	Meaning
SubscriberData	Refers to 'subscriber data' in the European Production or Preservation order.
UserIdentifyingData	Refers to 'data requested for the sole purpose of identifying a user' in the European Production or Preservation order.
TrafficData	Refers to 'traffic data' in the European Production or Preservation order.
StoredContentData	Refers to 'content data' in the European Production or Preservation order.
Other	Used in all other cases.

NOTE: The description of the meaning of these values is part of the European Production and Preservation order and not of the present document.

8.3.5.3 RequestValues

The RequestValues field contains a list of RequestValue structures, which are combined (with ordering and Boolean ANDed together) to identify the requested disclosure. Each RequestValue structure contains the following fields.

Table 8.20: RequestValue

Field	Format	Description
FormatType	As defined below.	Specifies a Request Value Format (see below) which defines the format for the Request Value fields. See annex C for the list of Request Value Formats defined by ETSI. Other definitions may be managed on a national basis.
Value	LongString (see ETSI TS 103 280 [7]).	Additional formatting information is given by the Request Value Format.

The RequestValue FormatType and format descriptions are given in annex C.

The Receiver is responsible for checking that the format of the RequestValue matches the format defined for the Request Value Format Type. If any of the RequestValues are not correctly formatted, the Action should be rejected.

8.3.5.4 FormatType

A RequestValue FormatType uniquely identifies a particular Request Value Format. It can be used to retrieve the correct RequestValue Format definition for a RequestValues structure. It consists of the following fields.

Table 8.21: RequestValue FormatType

Field	Format	Description
FormatOwner	ShortString (see ETSI TS 103 280 [7]).	Name of the Owner of the Format definition. See below.
FormatName	ShortString (see ETSI TS 103 280 [7]).	Uniquely identifies the format definition within the Owner.

A Format owner is specified by a string value. The following owners are defined by the present document:

- "ETSI": The Format is owned by ETSI, and defined in the present document in annex C.
- A valid ISO 3166-1 [14] alpha-2 country code: The Format is owned and defined by the relevant national authority for the country specified by the country code.

A Format definition shall contain, at a minimum, the following information.

Table 8.22: RequestValue Format Definition

Field	Format	Description
FormatOwner	ShortString (see ETSI TS 103 280 [7]).	Identifies the Owner of the Format definition. See below.
FormatName	ShortString (see ETSI TS 103 280 [7]).	Identifies the format, unique within the Format Owner.
Description	LongString (see ETSI TS 103 280 [7]).	Human-readable description associated with the Format.
Format	IEEE POSIX 1003.1™ ERE [13] Regular Expression.	Regular expression defining the permissible contents of the field. If absent, any UTF-8 string is permitted, subject to the length restriction of the field.

See annex C for the list of Request Value Formats defined by ETSI. Other definitions may be managed on a national basis.

8.3.5.5 Subtype

Subtype of CSP product or products to disclose information about. This field is for use in cases where this cannot be sufficiently well-determined from the Type field (see clause 8.3.5.2). This field is optional.

Given as a list of LDRequestSubtype DictionaryEntries. More than one entry may be chosen. The usage and meaning of the Product Subtype are likely to be closely coupled to the products offered by the Receiver; in these circumstances the Receiver should define its own extensions to this dictionary. The Receiver may choose not to define any entries i.e. meaning that field is not used.

Table 8.22a: LDRequestSubtype Dictionary

Dictionary Owner	Dictionary Name
ETSI	LDRequestSubtype.
Defined DictionaryEntries	
Value	Meaning
The present document does not define any dictionary entries for this dictionary.	

8.3.5.6 TargetIdentifierSubtype

The kind of CSP entity to disclose information about. For use in cases where multiple kinds of CSP entities exist that possibly share a RequestValue, and the Requestor knows what kind of CSP entity they are targeting for the disclosure request. This additional granularity is used to accurately identify specific targets when the CSP has several kinds of CSP entities that share an identifier space.

EXAMPLE: As an example, consider a CSP which supports personal accounts and business accounts, but a given numeric identifier can be shared across a personal account and business account (even if the underlying account owners are different people). In this case, the TargetIdentifierSubtype would be provided to target either the personal account or business account.

Given as a TargetIdentifierSubtype DictionaryEntry. The usage and meaning of any TargetIdentifierSubtype is likely to be closely coupled to the products offered by the Receiver; in these circumstances the Receiver should define its own extensions to this dictionary.

Table 8.23: TargetIdentifierSubtype Dictionary

Dictionary Owner	Dictionary Name
ETSI	TargetIdentifierSubtype.
Defined DictionaryEntries	
Value	Meaning
The present document does not define any dictionary entries for this dictionary.	

8.3.6 DeliveryDetails

8.3.6.1 Overview

The LDTaskDeliveryDetails field indicates where disclosed product should be delivered.

The LDTaskDeliveryDetails field consists of a list of LDDeliveryDestination structures. Each entry in the list represents a desired destination for product related to the Task.

Limits on the type, number or combinations of LDDeliveryDestination for a given type of Task shall be specified by the relevant national profile.

8.3.6.2 LDDeliveryDestination

The LDDeliveryDestination structure contains the following fields.

Table 8.23: LDDeliveryDestination

Field	Format	Description
DeliveryAddress	DeliveryAddress (see clause 8.2.8.3).	The address to which the product for this Task should be delivered.
EncryptionDetails	NationalEncryptionDetails.	Details regarding the encryption to be applied to product delivered to this destination. Shall be defined by the relevant national profile.
HandoverFormat	LDHandoverFormat DictionaryEntry (see clause 8.3.6.3).	Specifies the handover format to be used.
DeliveryProfile	LDDeliveryProfile DictionaryEntry.	A dictionary entry which gives the name of a delivery profile that represents a set of configuration information associated with the destination and delivery of the product from this Task. If used, the dictionary shall be defined by the relevant national profile.
NationalDeliveryParameters	See annex G.	See annex G.

8.3.6.3 HandoverFormat

The LDHandoverFormat dictionary is defined in table 8.24 (see annex F for more details on Dictionaries).

Table 8.24: LDHandoverFormat Dictionary

Dictionary Owner	Dictionary Name
ETSI	LDHandoverFormat.
Defined DictionaryEntries	
Value	Meaning
TS102657	Handed over in ETSI TS 102 657 [22] format, using HI-B as described in ETSI TS 102 657 [22].
EncapsulatedTS102657	Handed over as ETSI TS 102 657 [22] format, using the DeliveryObject as described in clause 10.
TS103120	Handed over using the DeliveryObject as described in clause 10.
TS103705	Handed over as ETSI TS 103 707 [24], using the DeliveryObject as described in clause 10.
TS103707	Handed over as ETSI TS 103 707 [24], using the DeliveryObject as described in clause 10.

8.3.7 Flags

The Flags field allows a set of multiple flags to be associated with the LDTaskObject. Each flag is given as a LDTaskFlag Dictionary Entry. If a flag is present in the Flags field, then the meaning given as part of that flag's definition shall be taken to apply.

The LDTaskFlag Dictionary is defined in table 8.25 (see annex F for more details on Dictionaries).

Table 8.25: LDTaskFlag Dictionary

Dictionary Owner	Dictionary Name
ETSI	LDTaskFlag.
Defined DictionaryEntries	
Value	Meaning
IsTest	Indicates that the current Task is for test purposes. This may alter the process or documentation accompanying the authorisation.
IsEmergency	Indicates if the LD Task was issued under nationally-defined emergency procedures. The circumstances and consequences for setting the field shall be defined by the relevant national profile (see clause B.1.3).
IsNonLocal	Indicates that the current Task shall disclose information about a non-local identity.
IsLocal	Indicates that the current Task shall disclose information about a local identity. If both the IsNonLocal and IsLocal flag are absent, the identity provided within the Task shall be considered as a local identity unless otherwise agreed.

8.3.8 AlternativePreservationReferences

In situations where an LDTask Object is related to one or more prior preservation request exchanged via a mechanism outside of those described in the present document (i.e. an out-of-band process), this field shall be used to provide references to those prior preservation requests. The field is given as a list of AlternativePreservationReference structures. Each AlternativePreservationReference has the structure given in table 8.26.

Table 8.26: AlternativePreservationReference

Field	Format	Description
ReferenceValue	LongString (see ETSI TS 103 280 [7])	Reference in a format defined by or agreed with the CSP.
NatureOfReference	Dictionary	Optional indication of the nature of the referenced preservation. Format and usage for agreement between LEA and CSP.

In situations where the prior preservation request is represented as an HI1 Object, then this field shall not be used and the relationship shall be signalled using the AssociatedObjects field (see clause 7.1.4).

8.4 LPTaskObject

8.4.1 Overview

An LPTaskObject represents the state of an LPTask - that is, the act of preserving information. In general, multiple tasks may be associated with a single Authorisation.

The LPTask is intended to be used only for preserving historical data, not for ordering the preservation of data generated in the future. CSPs and LEAs shall refer to applicable law to determine the lawful retention period of the preserved data. If and for how long preserved data is required to be stored is out of scope of the present document.

Where an LDTask requests the disclosure of data preserved by an LPTask, the LDTask shall list the ObjectID of the related LPTask in its AssociatedObjects field.

The LPTaskObject consists of the following fields.

Table 8.27: LPTaskObject

Field	Format	Description	Clause
Status	LPTaskStatus Dictionary Entry.	The current status of the task as determined by the Receiver.	Clause 8.4.2
StatusReason	ActionUnsuccessful structure (see clause 6.4.9).	Optional information for the Receiver to indicate why the Object is in a certain state (such as Invalid or Rejected). Usage for national agreement.	Clause 6.4.9
DesiredStatus	LPTaskDesiredStatus Dictionary Entry.	The current status of the task as specified by the Sender.	Clause 8.4.3
RequestDetails	LPRequestDetails.	Details regarding the content of the preservation request, such as identifiers and dates.	Clause 8.4.4
DesiredPreservationExpiration	QualifiedDateTime (see ETSI TS 103 280 [7]).	Set by the LEA to indicate to the CSP the desired time to live for the preserved data archive retained by the CSP.	Clause 8.4.5
PreservationExpiration	QualifiedDateTime (see ETSI TS 103 280 [7]).	Set by the CSP to indicate to the LEA the time to live for the preserved data archive retained by the CSP.	Clause 8.4.6
CSPID	EndpointID (see clause 6.2.4).	Describes the CSP required to implement the Task.	Clause 8.2.10
NationalLPTaskingParameters	See annex G.	See annex G.	Annex G

8.4.2 Status

The Status field gives the status of the LPTaskObject as determined by the Receiver. A Sender shall not attempt to set the Status as part of a CREATE or UPDATE Request, and a Receiver shall return an Action Unsuccessful Information Response if the Sender attempts to do so. The Status field provides a key mechanism for mapping the content of the Object to the relevant nationally-defined processes. The rules for evaluating the correct value of the Status field shall be defined in the relevant national profile. Given as an LPTaskStatus Dictionary Entry. The LPTaskStatus Dictionary is defined in table 8.28 (see annex F for more details on Dictionaries).

Table 8.28: LPTaskStatus Dictionary

Dictionary Owner	Dictionary Name
ETSI	LPTaskStatus.
Defined DictionaryEntries	
Value	Meaning
AwaitingPreservation	The Task is approved by the relevant authorities, but the Task has not yet been approved and/or actioned by the CSP.
Preserved	The Task has been processed and the data has been preserved by the LP system.
PreservationNotAvailable	The Task has been processed and the CSP has determined there is no data available to preserve.
Rejected	The Task has been explicitly denied or rejected by one or more relevant authorities or by the CSP.
Cancelled	The Task has been permanently cancelled.
Expired	The retention period of the preserved data has expired.
Error	The Task has not been processed due to a problem with the underlying LP system.
Invalid	The Task has not been processed due to a problem with the current information populated in the Task Object.

8.4.3 DesiredStatus

The DesiredStatus field gives the status of the LPTaskObject as determined by the Sender. Given as an LPTaskDesiredStatus Dictionary Entry. The LPTaskDesiredStatus Dictionary is defined in table 8.29 (see annex F for more details on Dictionaries).

Table 8.29: LPTaskDesiredStatus Dictionary

Dictionary Owner	Dictionary Name
ETSI	LPTaskDesiredStatus.
Defined DictionaryEntries	
Value	Meaning
AwaitingPreservation	The Task is approved by the relevant authorities, but the Task has not yet been approved and/or actioned by the CSP.
Preserved	The Task has been processed and the data has been preserved by the LP system.
Cancelled	The Task has been permanently cancelled.

8.4.4 RequestDetails

8.4.4.1 General

The RequestDetails structure specifies the content of the disclosure request. It consists of the following fields.

Table 8.30: LPRequestDetails

Field	Format	Description
Type	RequestType (see clause 8.3.5.2).	Specifies the products to be preserved.
StartTime	QualifiedDateTime (see ETSI TS 103 280 [7]).	If a date/time range needs to be applied to the request, the StartTime and EndTime shall be provided.
EndTime	QualifiedDateTime (see ETSI TS 103 280 [7]).	If a date/time range needs to be applied to the request, the StartTime and EndTime shall be provided.
RequestValues	List of RequestValue structures (see clause 8.3.5.3).	Specifies the value(s) used to define the preservation request.
Subtype	List of LPRequestSubtype DictionaryEntries	Indicates the subtype of CSP product or products to be preserved, for use in cases where this cannot be sufficiently well-determined from the RequestType field. Optional.

8.4.4.2 Subtype

Subtype of CSP product or products to preserve information about. This field is for use in cases where this cannot be sufficiently well-determined from the Type field (see clause 8.3.5.2). This field is optional. Given as a list of LPRequestSubtype DictionaryEntries. More than one entry may be chosen. The usage and meaning of the Product Subtype are likely to be closely coupled to the products offered by the Receiver; in these circumstances the Receiver should define its own extensions to this dictionary. The Receiver may choose not to define any entries i.e. meaning that field is not used.

Table 8.31: LPRequestSubtype Dictionary

Dictionary Owner	Dictionary Name
ETSI	LPRequestSubtype.
Defined DictionaryEntries	
Value	Meaning
The present document does not define any dictionary entries for this dictionary.	

8.4.5 DesiredPreservationExpiration

The DesiredPreservationExpiration field indicates the time at which the LEA desires the data retained in response to the preservation request to expire. This field is set by the LEA. When requesting an extension of a preservation, the LEA shall update this field to indicate the new desired expiration time of the retained data.

8.4.6 PreservationExpiration

The PreservationExpiration field indicates the time at which the data retained in response to the preservation request will expire. This field is set by the CSP. When extending a preservation, the CSP shall update this field to indicate the new expiration time of the retained data.

9 Transport and Encoding

9.1 Overview

This clause describes the transport and encoding mechanisms used in exchanging WI messages.

9.2 Encoding

9.2.0 Encoding schemes

ETSI TS 103 280 [7] messages shall be encoded in either XML (see clauses 9.2.1) or JSON (see clauses 9.2.4). Clauses 9.2.2 and 9.2.3 apply to both encodings. A Receiver that receives a WI message in a given encoding shall either respond in the same encoding or return an error message indicating that it does not support the given encoding.

9.2.1 XML Schema

Messages encoded in XML format [4] shall conform to the WI XSD Schema, which is provided as an XML XSD Schema Set that accompanies the present document. Each National Profile may, subject to national agreement, specify additional schema files that give definitions for national parameters (see annex G) that shall be considered as part of the schema set.

The Sender and Receiver shall only send messages that are successfully validated against the schema.

9.2.2 Error conditions

If a Receiver receives a WI Message which does not conform to the relevant schema (either XSD or JSON), or fails due to some other transport-related issue (e.g. it is too large for the receiver to process or the version is not supported), it shall not attempt to process any of the contents. It shall respond with a top-level Action Unsuccessful message containing a suitable error code.

9.2.3 Message signing and encryption

Implementations may choose to digitally sign and/or encrypt XML-encoded messages for security and assurance purposes. If used, the signature information shall be placed in element as the last child element of the root message element.

If this is required, the relevant national profile shall specify the relevant details for populating the signature element.

Implementations may choose to sign JSON-encoded messages; if so, the procedures in annex J shall be followed.

9.2.4 JSON Schema

Messages encoded in JSON format [27] shall conform to the WI JSON Schema, which is provided as a set of JSON Schema files [28] that accompanies the present document.

NOTE: This schema set is derived from the XSD schema set (see clause 9.2.1) following the translation specified in ETSI TS 103 280 [7], annex C.

Each National Profile may, subject to national agreement, specify additional schema files that give definitions for national parameters (see annex G) that shall be considered as part of the schema set.

The Sender and Receiver shall only send messages that are successfully validated against the schema.

9.3 HTTP Transport

9.3.1 Use of HTTP

HTTP Transport is the defined transport mechanism for WI messages in the present document, unless a nationally-defined transport mechanism is to be used (see clause 9.4). For security details relating to the HTTP exchange, see clause 9.3.4.

9.3.2 Client/Server architecture

When using HTTP for WI message exchange, the Sender acts as an HTTP client while the Receiver acts as an HTTP server.

9.3.3 HTTP Configuration

The POST method shall be used for all HTTP requests. The body of the POST message shall contain a single HI1 Request Message, as defined in clause 5 and clause 6.3.1, and encoded as per clause 9.2.

The Content-Type shall be set to text/xml or application/json as appropriate (see clause 9.2.0).

Caching shall not be used.

In the absence of HTTP transport level errors, the Receiver shall respond with an HTTP 200 OK response. The body of the response shall contain a single HI-1 Response Message, as defined in clause 5 and clause 6.3.1, and encoded as per clause 9.2. HTTP Status Codes shall not be used to indicate WI application layer errors. Well-formed WI Response messages containing the appropriate error codes shall be used.

9.3.4 Transport security

Implementations shall support HTTPS as defined in IETF RFC 2818 [5], including the support for mutual authentication through bidirectional certificate usage. Implementations shall use HTTPS unless specifically directed otherwise in the relevant national profile.

The use of pre-shared keys may be considered for authentication at the transport layer. If this option is selected, the specifications set forth in IETF RFC 4279 [6] shall be followed.

The relevant national profile shall provide details for the agreed security requirements for the transport layer, including specification of any necessary encryption, signatures or hash functions.

Issues such as key management, key length, key exchange, choice of cryptographic algorithm, etc. are outside of the scope of the present document. It is expected that future versions of the present document will include best practice recommendation as defined by ETSI TC CYBER.

9.4 Nationally-defined Transport

If HTTP transport as defined in the above clause is not to be used in a particular country, a nationally-defined alternative may be agreed on a national basis. Such a transport mechanism shall not break any of the requirements of clause 9.2.

10 Delivery Object

10.1 Overview

A delivery Object represents the delivery of information to a request for that information as part of a task.

10.2 DeliveryObject

10.2.1 Overview

The DeliveryObject consists of the following fields. Where the DeliveryObject is created in response to a Task Object, that Task Object shall be referenced in the AssociatedObjects field of the DeliveryObject.

Table 10.1: DeliveryObject

Field	Format	Description	Reference
Reference	LDID or LIID (see ETSI TS 103 280 [7])	LDID or LIID assigned by the corresponding LDTaskObject or LITaskObject, respectively.	Clauses 8.3.2, and 8.2.2
DeliveryID	UUID (see ETSI TS 103 280 [7]) in IETF RFC 4122 [3] canonical form	A DeliveryID uniquely identifies this delivery. The delivery may be split using the SequenceNumber mechanism. The Manifest field applies to the aggregate content for all sequences delivered under a single DeliveryID.	
SequenceNumber	Positive integer	An incremental and unique number within the scope of a DeliveryID. Starts with 1. May be omitted if there is only one SequenceNumber in the delivery (see definition of LastSequence below).	
LastSequence	Boolean	A boolean that indicates whether this was the last sequence for a DeliveryID. If there is only one SequenceNumber, the LastSequence field shall either be set to true, or both the LastSequence and SequenceNumber field shall be omitted.	
Manifest	Manifest	The Manifest describes the format used in the delivery. It is recommended to transmit the manifest at the first sequence.	Clause 10.2.2
Delivery	Delivery	The actual delivery (or sequence of) the requested information.	Clause 10.2.3

10.2.2 Manifest

A Manifest structure is used to describe the format of a Delivery structure. The Manifest either points to existing formats (such as the format specified in ETSI TS 102 657 [22]) for the delivery of information but also supports a mechanism to attach a manifest to that delivery. An example of this is where a manifest is attached in the form of an XSD that describes the XML in the Delivery structure.

The Manifest consists of one of the following fields.

Table 10.2: Manifest

Field	Format	Description	Reference
Specification	Specification dictionary	A dictionary describing the applicable ETSI TC-LI specifications that can be used in the Delivery structure.	Table 10.3
ExternalSchema	ExternalSchema structure	Information on the external schema that describes the contents of the Delivery structure.	Table 10.4

Table 10.3: ManifestSpecification Dictionary

Dictionary Owner	Dictionary Name
ETSI	ManifestSpecification.
Defined DictionaryEntries	
Value	Meaning
TS102657-ASN.1	The delivery is according to ETSI TS 102 657 [22] using ASN.1 encoding.
TS102657-XML	The delivery is according to ETSI TS 102 657 [22] using XML encoding.
TS103705	The delivery is according to ETSI TS 103 705 [35] using JSON encoding.
TS103707	The delivery is according to ETSI TS 103 707 [24].
TS103976	The delivery is according to ETSI TS 103 976 [33] using JSON encoding.

Table 10.4: ExternalSchema

Field	Format	Description	Reference
ManifestID	LongString that uniquely identifies a certain manifest	Instead of delivering ManifestContents, a ManifestID may be used to identify a certain manifest.	
ManifestContents	ExternalSchema structure (see table 10.4a).	Contains a copy of the schema that describes the content of the overall Delivery. The ExternalSchema structure provides a choice of three formats, described in table 10.4a.	Table 10.4a

Table 10.4a: ManifestContents

Field	Format	Description	Reference
BinaryData	EmbeddedBinaryData	Shall contain a binary representation of the relevant manifest contents.	Table 10.5
XMLSchema	An XML document conforming to the W3C schema format.	Shall contain an XML schema. Shall only be used if the HI-1 message is encoded in XML.	
JSONSchema	A JSON document conforming to the JSON schema specification.	Shall contain a JSON schema. Shall only be used if the HI-1 message is encoded in JSON	

10.2.3 Delivery

A Delivery structure is used to deliver information as part of the DeliveryObject. If the sequencing mechanism in the DeliveryObject is used, the content in each Delivery structure may be a part of a file.

The Delivery structure allows data to be provided either as XML data (if the HI-1 Message is encoded as XML), JSON data (if the HI-1 Message is encoded as JSON) or as binary data. The available fields are described in table 10.4b below.

Table 10.4b: Delivery

Field	Format	Description
XMLData	EmbeddedXMLData (permits any valid XML)	Shall only be used if the HI-1 Message is encoded in XML. May contain any valid XML elements in any namespace other than the target namespace. If XML data is required to be sent in a non-XML-encoded HI1 message, the EmbeddedBinaryData field shall be used.
BinaryData	EmbeddedBinaryData (see table 10.5)	May be used to carry binary data.
JSONData	EmbeddedJSONData (permits any valid JSON)	Shall only be used if the HI-1 Message is encoded in JSON. May contain any valid JSON document. If JSON data is required to be sent in a non-JSON- encoded HI1 message, the EmbeddedBinaryData field shall be used.

Table 10.5: EmbeddedBinaryData

Field	Format	Description
Data	Binary data, represented using base64 encoding.	Binary representation of the delivered data.
Content Type	ShortString containing a MIME type as per IETF RFC 2045 [9] and IETF RFC 2046 [10].	Encoding of the binary Data field (e.g. "image/jpeg").
Checksum	<p>UTF-8 string containing a checksum of the binary data, given as hexadecimal digits.</p> <p>In version 1.11.1 the ChecksumType field was introduced. New implementations shall use the ChecksumType field and shall support at least "sha-256".</p> <p>If no ChecksumType is provided, the Checksum field shall contain an SHA-256 checksum as per IETF RFC 6234 [23].</p>	<p>Checksum to ensure that the Data field has been transmitted correctly.</p> <p>This mechanism is not intended as a signature.</p>
ChecksumType	UTF-8 string containing a Hash Function Name as defined in IANA Hash Function Textual Names [26].	The type of checksum provided in the Checksum field.

Annex A (informative): Example usage scenarios for HI-1

A.1 Overview

This annex shows some characteristic message flows for eWarrant exchange.

A.2 Direct communication

In this scenario the LEA directly requests warrant authorisation from a competent Warrant Approving Authority, and then passes the technical details for the interception on to the CSP for action.

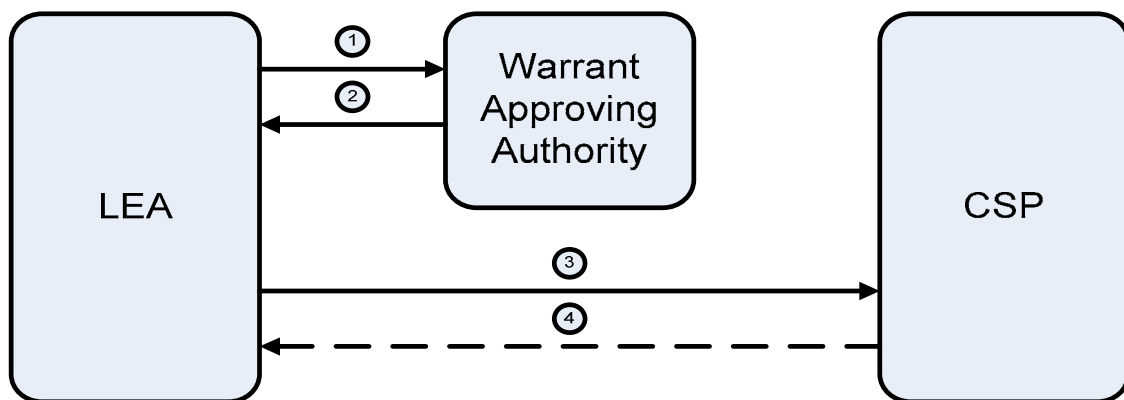


Figure A.1: Simple architecture for exchange of warrant and tasking information

The numbered message flows are as follows.

Table A.1: Message flows in Direct Communication

Message flow	Description	Information carried	Notes
1	Request for warrant approval.	Warrant information, plus any technical tasking information required.	
2	Approved/rejected warrant.	Warrant information.	If the warrant is not approved, #1 and #2 may be repeated.
3	Request for interception.	Tasking information, plus whatever subset of the warrant information is required.	
4	Intercepted product.	Intercepted product.	Covered by HI-2/3.

A.3 Single "Central Authority"

In this scenario, LEAs interact with the CSPs via a central broker authority. LEAs still interact with the warrant granting authorities directly.

The Central Authority may also take responsibility for fanning out an LEA's request to multiple CSPs, if appropriate.

Depending on the details of the jurisdiction, CSPs may or may not require a subset of the warrant information to be passed along with the tasking information.

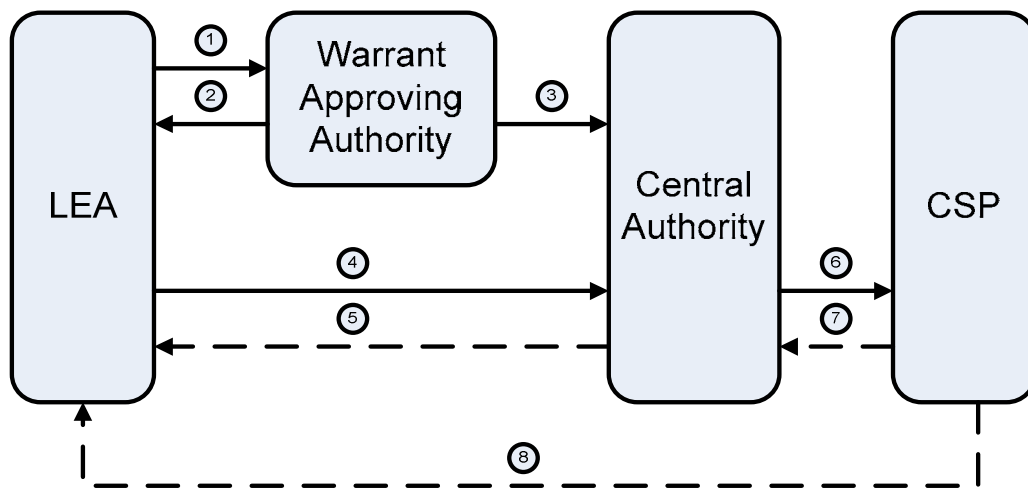


Figure A.2: Scenario including a Central Authority

The numbered message flows are as follows.

Table A.2: Message flows with a Central Authority

Message flow	Description	Information carried	Notes
1	Request for warrant approval.	Warrant information, plus any technical tasking information required.	
2	Approved/rejected warrant.	Warrant information.	If the warrant is not approved, #1 and #2 may be repeated.
3	Notification of approved warrant.	Warrant information.	Sent if the Central Authority requires some kind of external notification that the warrant is approved.
4	Request for interception.	Tasking information, plus any required subset of warrant information.	May include requests for tasking multiple CSPs.
5	Product of interception.	Intercepted product (if product is passed back via the Central Authority).	Covered by HI-2/3.
6	Request for interception.	Tasking information, plus any required subset of warrant information.	May be a subset of the information carried in #4.
7	Product of interception.	Intercepted product (if product is passed back via the Central Authority).	Covered by HI-2/3.
8	Product of interception.	Intercepted product (if product is passed back to the LEA directly).	Covered by HI-2/3.

A.4 Multiple Approving Authorities

A.4.1 Overview

In this scenario, the LEA's request for interception passes through two separate Approving Authorities for approval. In principle, this could be generated for three or more Approving Authorities.

A.4.2 "Serial" interaction

This may happen "serially", such that the first of the Warrant Approving Authorities is responsible for passing the relevant information on to the next Warrant Approving Authority. Information regarding the warrant is then passed back from the CSP in a similar way. In this scenario, the results of interception are passed directly to the LEA. Although it is not shown here, it is possible that results of interception could also be mediated through one or more authorities, as in scenario A.2 above.

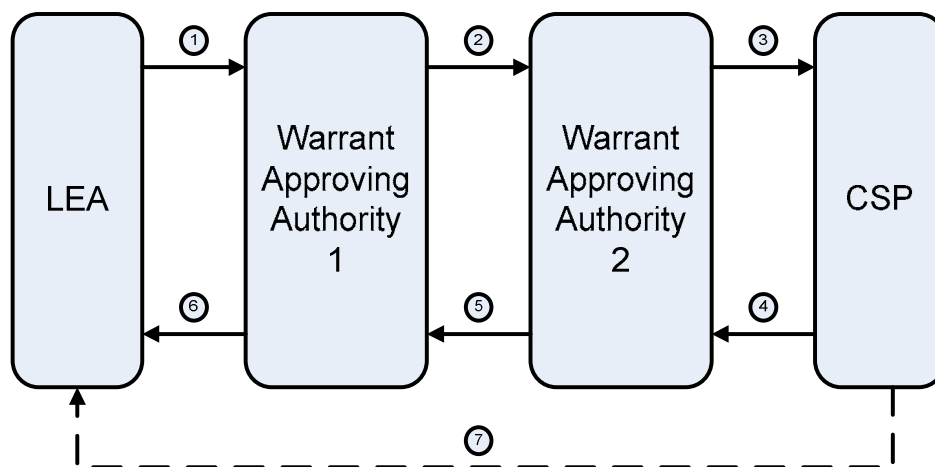


Figure A.3: Scenario with multiple Approving Authorities

The numbered message flows are as follows.

Table A.3: Message flows with multiple serial approving authorities

Message flow	Description	Information carried	Notes
1	Request for warrant approval.	Warrant information, plus any technical tasking information required.	
2	Request for warrant approval.	Warrant information (including approval from Warrant Approving Authority 1), plus any technical tasking information required.	If the warrant is not approved, a rejection may be sent back to the LEA.
3	Request for interception.	Tasking information, plus any required subset of warrant information.	Here, the last Approving Authority serves the warrant on the CSP.
4	Notification of activated warrant.	Tasking information.	Confirmation from the CSP that the warrant/task has been activated.
5	Notification of activated warrant.	Tasking information.	Confirmation from the CSP that the warrant/task has been activated.
6	Notification of activated warrant.	Tasking information.	Confirmation from the CSP that the warrant/task has been activated.
7	Product of interception.	Intercepted product (if product is passed back to the LEA directly).	Covered by HI-2/3.

A.4.3 "Parallel" interaction

This scenario may also happen "in parallel", where the LEA is responsible for presenting the warrant information to each of the Warrant Approving Authorities. Once the approvals have been collected, the LEA then submits the details of the interception required to the CSP directly.

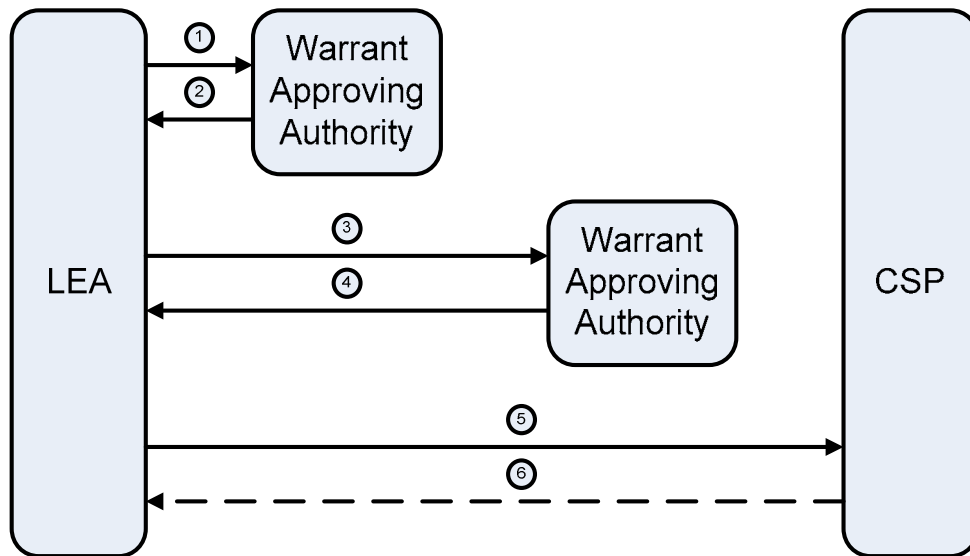


Figure A.4: Scenario with multiple Approving Authorities

The numbered message flows are as follows.

Table A.4: Message flows with multiple parallel approving authorities

Message flow	Description	Information carried	Notes
1	Request for warrant approval.	Warrant information, plus any technical tasking information required.	
2	Approved/rejected warrant.	Warrant information.	If the warrant is not approved, #1 and #2 may be repeated.
3	Request for warrant approval.	Warrant information, plus any technical tasking information required.	
4	Approved/rejected warrant.	Warrant information.	If the warrant is not approved, #3 and #4 may be repeated.
5	Request for interception.	Tasking information, plus any required subset of warrant information.	
6	Product of interception.	Intercepted product (if product is passed back to the LEA directly).	Covered by HI-2/3.

Annex B (informative): Example Template National Profile

B.1 Introduction

B.1.1 Overview

National tasking and warrant processes are tightly coupled to national legislation. While there are many broad similarities between different countries, the processes are subtly different in each country. The present document does not attempt to dictate these processes, but rather support whatever processes are required by national law.

To do so, the standard defines a common set of definitions for representing and exchanging authorisation and task information, but does not define the national business logic or rules that are applied to them. These are left to national jurisdictions to define in their national profiles of the present document.

This annex gives an example, or template, national profile. The purpose of this annex is as follows:

- To illustrate to readers of the standard how HI-1 can be used to build national processes.
- To demonstrate how the present document and a national profile are intended to interact.
- To give drafting guidance to those who are writing national profiles.

Clause B.1.2 gives a suggested structure and content for a national profile.

B.1.2 Structure of this annex

Clause B.2 contains an Example National Profile. It is written from the perspective of a fictional national jurisdiction, such that if the text in clause B.2 were made a separate document, it would form an illustrative example of a fictional national profile.

The content of clause B.1 should be read as part of the present document. It provides the necessary explanation and background for the text in clause B.2.

B.1.3 Checklist for National Profile authors

The following list is provided as an informative checklist of the information that should be provided as part of a complete National Profile. The Example National Profile follows this checklist.

Table B.1: Requirements for national profiles

Item	ETSI Reference
The relevant national processes and reference model should be described or referenced, taking particular care to explain the desired mapping between HI-1 Objects and the things they represent in those national processes.	Clause 4
The correct value for the NationalProfileOwner has to be specified.	Clause 6.2.3
The correct value for the NationalProfileVersion field has to be specified.	Clause 6.2.3
The desired interoperability behaviour should be described.	Clause 6.2.3
The correct EndpointID country codes have to be specified.	Clause 6.2.4
The format or list of valid values for EndpointID Unique Identifiers have to be specified.	Clause 6.2.4
The profile has to specify whether use of the LIST verb is permitted.	Clause 6.4.8
If LIST is permitted, the rules for determining which Object Identifiers are returned have to be specified.	Clause 6.4.8
If LIST is permitted, any additional rules relating to LIST responses (e.g. size of response, caching behaviour) may be specified.	Clause 6.4.8
If LIST is permitted, any additional logic related to listing Notification Objects may be specified.	Clause 6.4.7

Item	ETSI Reference
The national profile has to make a statement about whether each field in each HI-1 Object definition are required in order for an instance of the object to be valid.	Clause 7.1
The valid format or values for Owner Identifier have to be specified.	Clause 7.1.1
NationalHandlingParameters may be defined.	Clause 7.1.6
The correct format or values for AuthorisationReference have to be specified.	Clause 7.2.2
The correct format or values for AuthorisationLegalType have to be specified.	Clause 7.2.3
The usage of AuthorisationPriority has to be specified. Any additional clarifications or DictionaryEntries may be specified.	Clause 7.2.4
The rules for determining the value of the AuthorisationStatus field have to be specified. The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Clause 7.2.5
The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Clause 7.2.6
Usage and meaning of the IsEmergency flag have to be specified.	Clause 7.2.12
Any additional clarifications or DictionaryEntries for Flags field may be specified.	Clause 7.2.12
The correct format or values of the DocumentReference field have to be specified.	Clause 7.3.2
The correct usage of the DocumentName field has to be specified.	Clause 7.3.3
The rules for determining the value of the DocumentStatus field have to be specified. The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Clause 7.3.4
The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Clause 7.3.5
The list of permissible of DocumentTypes has to be specified.	Clause 7.3.7
The list of permissible of DocumentProperties has to be specified.	Clause 7.3.8
The list of permissible MIME types for the DocumentBody field has to be specified.	Clause 7.3.9
The profile has to specify whether use of Notification Objects is permitted.	Clause 7.4.1
If NotificationObjects are used, the format and usage of the NotificationType field have to be specified.	Clause 7.4.3
If NotificationObjects are used, the correct archiving and persistence behaviour for NotificationObjects once the NewNotification flag has been cleared have to be specified.	Clause 7.4.4
If NotificationObjects are used, the definition of NationalNotificationParameters may be specified.	Clause 7.4.6
The rules for determining the value of the LIObject Status field have to be specified. The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Clause 8.2.3
The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Clause 8.2.4
Additional TargetIdentifier FormatTypes may be defined.	Clause 8.2.6.3
The list of valid TaskServiceTypes has to be specified.	Clause 8.2.6.4
Additional clarifications and DictionaryEntries for the DeliveryType may be defined.	Clause 8.2.7
EncryptionDetails applicable for the LI delivery may be specified.	Clause 8.2.8.2
DeliveryProfile representing a set of configuration information associated with the destination and delivery of the LI traffic.	Clause 8.2.8.2
NationalDeliveryParameters may be defined.	Clause 8.2.8.2
Additional clarifications and DictionaryEntries for the HandoverFormat may be defined.	Clause 8.2.8.4
DictionaryEntries for the HandlingProfile may be defined.	Clause 8.2.11
Additional clarifications and DictionaryEntries for the Flags field may be defined.	Clause 8.2.12
The rules for determining the value of the LDTaskObject Status field have to be specified. The business meaning of each Status should be specified. Any additional clarifications or DictionaryEntries may be specified.	Clause 8.3.3
The list of valid RequestType DictionaryEntries has to be specified.	Clause 8
EncryptionDetails applicable for the LD delivery may be specified.	Clause 8.3.6.2
DeliveryProfile representing a set of configuration information associated with the destination and delivery of the LD traffic.	Clause 8.3.6.2
NationalDeliveryParameters for LD may be defined.	Clause 8.3.6.2
Additional clarifications and DictionaryEntries for the LDHandoverFormat Dictionary may be defined.	Clause 8.3.6.3
DictionaryEntries for the LDHandlingProfile may be defined.	
Additional clarifications and DictionaryEntries for the LDTaskFlag Dictionary may be defined.	Clause 8.3.7
Additional schema fields may be specified.	Clause 9.2.1
Use of message signature and message encryption may be specified. If they are, the required signature and encryption details have to be specified.	Clause 9.2.3
Implementers may be directed not to use HTTPS.	Clause 9.3.4
National requirements for transport encryption and authentication have to be specified.	Clause 9.3.4
Additional error codes may be specified.	Annex D
The usage and valid format for ApprovalType have to be specified.	Clause E.2
The usage and valid format for ApprovalDescription may be specified.	Clause E.3

Item	ETSI Reference
The usage and valid format for ApprovalReference have to be specified.	Clause E.4
The usage and valid format for ApprovalRole have to be specified.	Clause E.5.1
NationalApproverIdentity may be defined.	Clause E.5.2
Definition of the usage of ApprovalsEmergency has to be specified.	Clause E.7
NationalDigitalSignature details may be defined.	Clause E.8

B.1.4 Details of the fictional national jurisdiction

For the purposes of the Example National Profile, it is assumed there is a fictional national jurisdiction.

This jurisdiction has a country code of "XX", which is a reserved ISO 3166-1 [14] alpha-2 country code.

The jurisdiction has a national process which follows the model given in clause A.2 of the present document. For simplicity and brevity, the jurisdiction is only using the present document to exchange information between the LEA and the CSP. It is assumed that the earlier interactions between the LEA and the warrant signing authority have occurred.

B.2 Example National Profile

B.2.1 Approach and reference model

B.2.1.1 Overview

This national profile follows ETSI TS 103 120 (the present document). The approach, structure of this national profile, and reference model follow the details given in clause 4, subject to the following clarifications and additions.

This national profile defines how ETSI TS 103 120 (the present document) is to be used for interactions between an LEA and a CSP. Specifically, the interactions covered by this national profile are as follows:

- Communication of a new Warrant, and associated Tasking instructions.
- Cancellation of an existing Warrant.
- Communication of a new Tasking Instruction under an existing Warrant.

B.2.1.2 Warrants

A new Warrant is created by obtaining a Warrant Instrument from the Warrant Issuing Authority. A Warrant Instrument is represented by a Document Object. For a Warrant Instrument to be valid, it has to contain:

- A Warrant Reference, consisting of the letter "W" followed by a six-digit number.
- The name of the person signing the Warrant Instrument.
- A signature date, in the past.
- An end date, later than the start date.

A Warrant is cancelled by obtaining a Cancellation Instrument from the Warrant Issuing Authority. A cancelled Warrant automatically stops all Tasking Instructions related to that Warrant. For a Cancellation Instrument to be valid, it has to contain:

- A valid Cancellation Reference, consisting of the letter "C", followed by a six-digit number.
- The name of the person signing the Cancellation Instrument.
- A signature date, in the past.

B.2.1.3 Tasking Instructions

A Tasking Instruction is issued as part of a Warrant by the LEA.

For a Tasking Instruction to be valid, it has to:

- Be part of a valid Warrant.
- Have a valid LIID.
- Specify the communications address to be intercepted. The only valid type of communications address is MSISDN.
- Specify the time period inside which interception is sought, which has to be within the period of validity of the Warrant.

B.2.1.4 Representation by HI-1 Objects

Figure B.1 shows how the concepts described in the previous clauses are represented by HI-1 Objects.

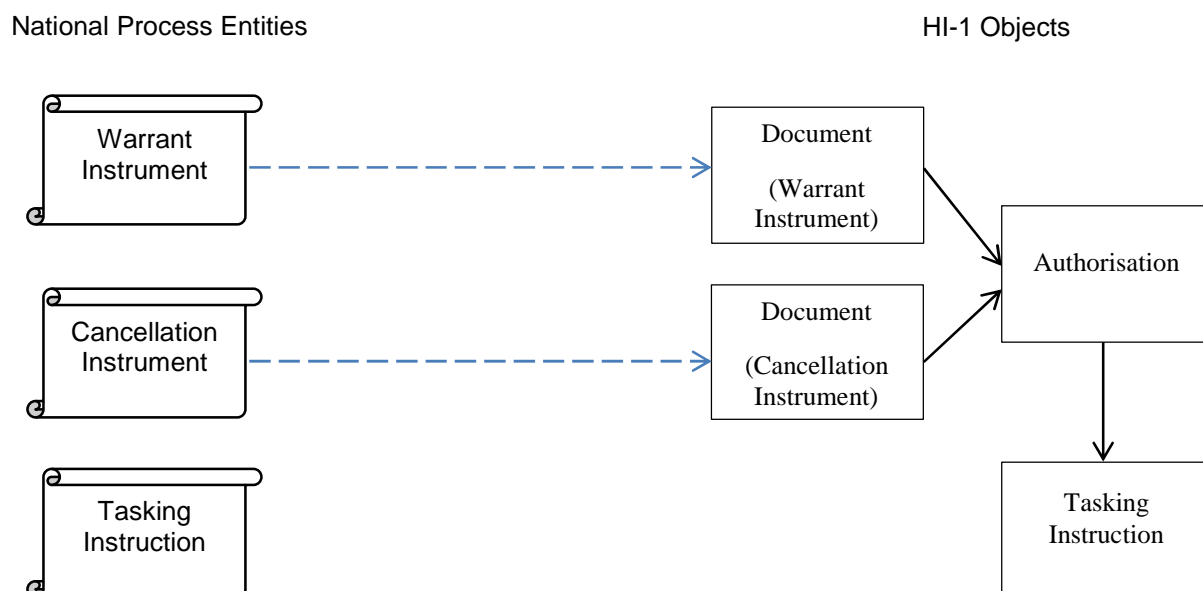


Figure B.1: Mapping of concepts to HI-1 Objects

B.2.2 Message Structure

B.2.2.1 Overview

The details in clause 6 have to be followed, subject to the following clarifications and additions in this clause.

B.2.2.2 Version information

The NationalProfile Owner is set to "XX".

The NationalProfileVersion is set to "v1.0".

Future versions of this national profile will specify interoperability requirements.

B.2.2.3 Sender and Receiver Identifiers

The Sender Identifier and Receiver Identifiers have a country code of "XX".

The Sender and Receiver Unique Identifier fields consist of eight alphanumeric characters.

B.2.2.4 LIST semantics

The Receiver has to support the LIST verb.

The Receiver can only return Object Identifiers for HI-1 Objects that are owned by the Sender (that is, the Sender Identifier matches the Object's Owner Identifier).

The number of matches returned is not to be limited.

B.2.3 Data Definitions

B.2.3.1 Overview

The details in clause 7 are followed, subject to the following clarifications and additions.

B.2.3.2 Object Identifiers

Object Identifiers are created with a country code of "XX".

The Object Identifier Owner Identifier is set to the Sender Identifier of the Sender that created the Object.

The Object Identifier External Identifier field is not populated.

B.2.3.3 Generic Object Fields

The National Handling Parameters is not to be used.

B.2.3.4 Authorisation Objects

The Authorisation Object is to be subjected to the following additional guidance.

Table B.2: Authorisation Object

Field	Usage	Additional guidance
AuthorisationReference	Used	Set to the Warrant Reference of the associated Warrant Instrument, in the same format (see Document Object, clause B.2.3.5).
AuthorisationLegalType	Not Used	
AuthorisationPriority	Not Used	
AuthorisationStatus	Used	No additional AuthorisationStatus DictionaryEntries are defined. The rules for calculating the correct AuthorisationStatus value are given below in table B.2.
AuthorisationDesiredStatus	Not Used	
AuthorisationTimespan	Used	Set to match the validity period of the associated Warrant Instrument Document Object.
AuthorisationCSPID	Not Used	
AuthorisationCreationTimestamp	Not Used	
AuthorisationServedTimestamp	Not Used	
AuthorisationTerminationTimestamp	Used	If the Authorisation Object is associated with a Cancellation Instrument Document Object, this field is set to the signature date of the associated Cancellation.
AuthorisationApprovalDetails	Not Used	
AuthorisationInvalidReason	Used	Populated by the Receiver if the AuthorisationStatus is "Invalid", absent otherwise.
AuthorisationFlags	Not Used	
NationalAuthorisationParameters	Not Used	

The Status field of an Authorisation Object is set according to the following rules, applied in the order given:

- If any of the other fields in the Authorisation Object do not conform to the relevant format as defined in this national profile, then the Status is "Invalid".
- If the Authorisation Object is not associated with a valid Document Object representing a Warrant Instrument, then the Status is "Invalid".
- If the Authorisation Object is associated with a valid Document Object representing a Cancellation Instrument, then the Status is "Cancelled".
- If the Authorisation does not have an AuthorisationTimespan StartTime after the date of the signature of the associated Warrant Instrument Document Object, the Status is "Invalid".
- If the Authorisation does not have an AuthorisationTimespan EndTime before the end date of the associated Warrant Instrument Document Object, the Status is "Invalid".
- If the Authorisation has an AuthorisationTimespan end time in the past, then the Status has to be set to "Expired".
- In all other cases, the Authorisation Status is "Approved".

B.2.3.5 Document Objects

The Document Object is subject to the following additional guidance.

Table B.3: Document Object

Field	Usage	Additional guidance
DocumentReference	Used	For Warrant Instruments, this field is set to the Warrant Reference, given as the letter "W" followed by a six digit number. For Cancellation Instruments, this field is set to the Cancellation Reference, given as the letter "C" followed by a six digit number.
DocumentName	Not Used	Name for a specific document.
DocumentStatus	Used	No additional DocumentStatus DictionaryEntries are defined. The rules for calculating the correct DocumentStatus value are given below.
DocumentDesiredStatus	Not Used	
DocumentTimespan	Used	Start time is set to the date of signature. For Warrant Instruments, the End time is set to the end of the validity of the Warrant. For Cancellation Instruments, the End time is absent.
DocumentType	Used	Additional guidance and DictionaryEntry definitions are given below.
DocumentProperties	Not Used	
DocumentBody	Not Used	
DocumentSignature	ApprovalDetails (see annex E)	Additional guidance given below table B.3.
NationalDocumentParameters	Not Used	

The DocumentStatus field of a Document Object is set according to the following rules, applied in the order given:

- If the Document does not have a valid DocumentSignature block, the Status is "Invalid".
- If the DocumentType is set to anything other than "Warrant Instrument" or "Cancellation Instrument", then the Status is "Invalid".
- If the DocumentType is "Warrant Instrument", and the Document does not have a DocumentTimespan EndDate, then the Status is "Invalid".
- In all other cases, the Status is "Approved".

The following additional DocumentType DictionaryEntries are defined.

Table B.4: National DocumentType Dictionary

Dictionary Owner	Dictionary Name
CountryXX	DocumentType.
Defined DictionaryEntries	
Value	Meaning
Cancellation	This Document represents a Cancellation Instrument.

The ETSI-defined DocumentType DictionaryEntries have the following additional meaning.

Table B.5: ETSI DocumentType Dictionary

ETSI-Defined DictionaryEntries	
Value	Additional Meaning
Warrant	This Document represents a Warrant Instrument.

The ApprovalDetails fields are populated as follows.

Table B.6: ETSI Document ApprovalDetails

Field	Used	Additional Guidance
ApprovalType	Not Used	
ApprovalDescription	Not Used	
ApprovalReference	Not Used	
ApproverDetails	ApproverDetails	See table B.7.
ApprovalTimestamp	Used	Given as the time of the signature.
ApprovalIsEmergency	Not Used	
ApprovalDigitalSignature	Not Used	
ApprovalNationalDetails	Not Used	

Table B.7: ETSI Document ApproverDetails

Field	Used	Description
ApproverName	Used	Name or other identifier of the approver.
ApproverRole	Not Used	
ApproverIdentity	Not Used	

B.2.3.6 Notification Objects

Notification Objects are not used.

B.2.3.7 LITaskObjects

The LITaskObject is subject to the following additional guidance.

Table B.8: LITaskObject

Field	Used	Additional guidance
Reference	Used	LIID assigned to the product of task.
Status	Used	No additional Status DictionaryEntries defined. The rules for calculating the correct Status value are given below table B.8.
DesiredStatus	Not Used	
TimeSpan	Not Used	
TargetIdentifier	Used	Contains the desired Target Identifier. Contains a single Target Identifier of type InternationalE164.
DeliveryType	Used	No additional guidance.
DeliveryDetails	Used	No additional guidance.
ApprovalDetails	Not Used	
CSPID	Used	No additional guidance.
HandlingProfile	Not Used	
InvalidReason	Used	Populated by the Receiver if the AuthorisationStatus is "Invalid", absent otherwise.
Flags	Not Used	
NationalLITaskingParameters	Not Used	

The Status field of a LITaskObject is set according to the following rules, applied in the order given:

- If the LITaskObject is not associated with an AuthorisationObject, then the Status is "Invalid".
- If the LITaskObject is associated with an AuthorisationObject whose status is "Cancelled", then the LITaskObject's Status is "Cancelled".
- If the LITaskObject is associated with an AuthorisationObject's whose status is anything other than "Approved", then the LITaskObject's Status is "Invalid".
- If the LITaskObject does not have a valid LIID, then the Status is "Invalid".
- If the LITaskObject does not have a Target Identifier, then the Status is "Invalid".

- If the LITaskObject has a Target Identifier which is not of type "MSISDN", then the Status is "Invalid".
- If the LITaskObject does not have a TaskTimeSpan StartTime equal to or later than the associated Authorisation Start Time, then the Status is "Invalid".
- If the LITaskObject does not have a TaskTimeSpan EndTime equal to or earlier than the associated Authorisation End Time, then the Status is "Invalid".
- If the LITaskObject 's TaskTimeSpan EndTime is in the past, then the Status is "Expired".
- If the Task requests data outside the bounds of the associated Authorisation (e.g. CC for IRI only warrant), then the LITaskObject Status is "Rejected".
- If the underlying LI system has an error related to this Task, then the Status is "Error".
- In all other cases, the LITaskObject Status is "Active".

B.2.4 Transport and Encoding

The details in clause 9 are followed.

XML encoding is used. XML message is not signed nor encrypted.

The present document does not specify any nationally-defined transport mechanisms.

HTTPS is used. For details on the current security requirements and considerations for the transport layer, contact the national regulator.

B.2.5 Example XML

B.2.5.1 Introduction

The following example XML messages illustrate both the principles of HI-1 and the application to this national profile. The scenario is not an example of good programming practice or application design, but is intended to highlight some of the key aspects of HI-1.

The example messages consist of following transactions:

Request 1: In the first request message, the Sender asks to CREATE an AuthorisationObject, and an associated LITaskObject which is associated to it.

Response 1: The Receiver responds, indicating that both CREATE Requests were accepted, but not returning any further information.

Request 2: The Sender asks to retrieve the current state of the AuthorisationObject and the LITaskObject.

Response 2: The Receiver supplies the current state of both. It can be seen that both are "Invalid", since the AuthorisationObject is not associated with a valid Document Object, as per the details AuthorisationStatus rules given above.

Request 3: The Sender issues a CREATE request to create the relevant Document Object, and an UPDATE to associate the AuthorisationObject with the newly created Document Object.

Response 3: The Receiver indicates that both requests succeeded. Further, in the UPDATE Response, it provides an updated view of the state, which shows that the Authorisation is now in the "Active" state.

Request 4: In the first request message, the Sender asks to CREATE an AuthorisationObject, and an associated LITaskObject which is associated to it.

Response 4: The Receiver responds, indicating that both CREATE Requests were accepted, but not returning any further information.

Request 5-Binary-Delivery: The Receiver responds, returning a DeliveryObject in response to the lawful disclosure request in the LDTaskObject provided within Request 4. The binary Delivery structure is used to forward the delivery content.

Request 5-XML-Delivery: The Receiver responds, returning a DeliveryObject in response to the lawful disclosure request in the LDTaskObject provided within Request 4. The XML based Delivery structure is used to forward the delivery content.

Response 5: The Receiver responds, indicating that the DELIVER Requests were received successfully. The response fits both Request 5-Binary-Delivery4 as well as Request 5-XML-Delivery, meaning it is Delivery structure agnostic.

The example XML can be found in in the attachment provided with the present document and contained in archive ts_103120v011701p0.zip.

B.2.5.2 Void

Void.

B.2.5.3 Void

Void.

B.2.5.4 Void

Void.

B.2.5.5 Void

Void.

B.2.5.6 Void

Void.

B.2.5.7 Void

Void.

Annex C (normative): ETSI Target Identifier and Request Value Format Definitions

C.1 Overview

This annex details the baseline set of Target Identifier and Request Value Formats that are defined and managed by ETSI. This list covers the majority of identifier formats used in the ETSI TC LI family of LI and LD handover standards. It is expected that some Target Identifier and Request Value Formats will need to be used in combination with each other (e.g. UDPPortRange and IPv4Address).

C.2 Definitions

Table C.1: ETSI Target Identifier and Request Value Format Definitions

Format Name	Description	Format
InternationalE164 (was E.164)	Recommendation ITU-T E.164 [i.9] Number in full international format, excluding the '+' prefix, written as decimal digits. In version 1.16.1, the Format Name was corrected from "E.164" to "InternationalE164". To maintain backwards compatibility, implementations shall accept either form.	Regular expression as per ETSI TS 103 280 [7]
IMSI	International Mobile Subscriber Identity, following the Recommendation ITU-T E.212 [i.10] numbering scheme, written as decimal digits.	Regular expression as per ETSI TS 103 280 [7]
IMEI	International Mobile station Equipment Identity, following the numbering plan defined in 3GPP TS 23.003 [i.6], written as decimal digits without the Luhn check digit.	Regular expression as per ETSI TS 103 280 [7]
IMEICheckDigit	International Mobile station Equipment Identity, following the numbering plan defined in 3GPP TS 23.003 [i.6], written as decimal digits with the Luhn check digit.	Regular expression as per ETSI TS 103 280 [7]
IMEISV	International Mobile station Equipment Identity Software Version, following the numbering plan defined in 3GPP TS 23.003 [i.6], written as decimal digits including the two SV digits.	Regular expression as per ETSI TS 103 280 [7]
MACAddress	A MAC address in IEEE Std 802™-2001 [i.8] 48-bit format, written as six pairs of hexadecimal digits separated by colons.	Regular expression as per ETSI TS 103 280 [7]
IPv4Address (was Ipv4Address)	IPv4 address in dotted decimal notation. In version 1.11.1, the start of the Format Name was corrected from "Ipv4" to "IPv4". To maintain backwards compatibility, implementations shall accept either form.	Regular expression as per ETSI TS 103 280 [7]
IPv6Address (was Ipv6Address)	IPv6 address as colon-separated hexadecimal digits. In version 1.11.1, the start of the Format Name was corrected from "Ipv6" to "IPv6". To maintain backwards compatibility, implementations shall accept either form.	Regular expression as per ETSI TS 103 280 [7]
IPv4CIDR (was Ipv4CIDR)	IPv4CIDR, written in dotted decimal notation followed by CIDR notation. In version 1.11.1, the start of the Format Name was corrected from "Ipv4" to "IPv4". To maintain backwards compatibility, implementations shall accept either form.	Regular expression as per ETSI TS 103 280 [7]

Format Name	Description	Format
IPv6CIDR (was Ipv6CIDR)	IPv6CIDR written as eight groups of four hexadecimal digits separated by a colon, followed by CIDR notation. In version 1.11.1, the start of the Format Name was corrected from "Ipv6" to "IPv6". To maintain backwards compatibility, implementations shall accept either form.	Regular expression as per ETSI TS 103 280 [7]
TCPPort	TCP Port number, written in decimal notation.	Regular expression as per ETSI TS 103 280 [7]
TCPPortRange	Range of TCP Ports, written as decimal numbers separated by a colon.	Regular expression as per ETSI TS 103 280 [7]
UDPPort	UDP Port number, written in decimal notation.	Regular expression as per ETSI TS 103 280 [7]
UDPPortRange	Range of UDP Ports, written as decimal numbers separated by a colon.	Regular expression as per ETSI TS 103 280 [7]
Port	Port number given as a decimal number.	Regular expression as per ETSI TS 103 280 [7]
PortRange	Range of port numbers, given as decimal numbers separated by a colon.	Regular expression as per ETSI TS 103 280 [7]
EmailAddress	Email address following W3C [®] HTML 5 Recommendation [12].	Regular expression as per ETSI TS 103 280 [7]
Internationalized EmailAddress	Email address following IETF RFC 6530 [25].	Regular expression as per ETSI TS 103 280 [7]
SIP-URI	SIP-URI according to the SIP URI scheme (see IETF RFC 3261 [i.2]/3GPP TS 24.229 [i.7]).	Regular expression as per ETSI TS 103 280 [7]
TEL-URI	tel-URI according to the tel URI scheme (see IETF RFC 3966 [i.3]).	Regular expression as per ETSI TS 103 280 [7]
H323-URI	H323 URI according to the H323 URI scheme (see IETF RFC 3508 [i.4]).	h323:[a-zA-Z0-9!#\$%&-'=?~\[\]_~%]+
IMPU	IP Multimedia Public Identity, as per 3GPP TS 23.003 [i.6].	[a-zA-Z0-9!#\$%&-'=?~\[\]_~%]+
IMPI	IP Multimedia Private Identity, as per 3GPP TS 23.003 [i.6].	[a-zA-Z0-9!#\$%&-'=?~\[\]_~%]+
NAI	Network Access Identifier following IETF RFC 4282 [i.5] format.	Regular expression as per ETSI TS 103 280 [7]
SUPIIMSI	Subscription Permanent Identifier in IMSI representation as defined in 3GPP TS 23.501 [21].	Regular expression as per ETSI TS 103 280 [7]
SUPINAI	Subscription Permanent Identifier in NAI representation as defined in 3GPP TS 23.501 [21].	Regular expression as per ETSI TS 103 280 [7]
PEIIMEI	Permanent Equipment Identifier in IMEI representation as defined in 3GPP TS 23.501 [21].	Regular expression as per ETSI TS 103 280 [7]
PEIIMEICheckDi git	Permanent Equipment Identifier in IMEI Check Digit representation as defined in 3GPP TS 23.501 [21].	Regular expression as per ETSI TS 103 280 [7]
PEIIMEISV	Permanent Equipment Identifier in IMEI SV representation as defined in 3GPP TS 23.501 [21].	Regular expression as per ETSI TS 103 280 [7]
GPSIMSISDN	General Public Subscription Identifier as defined in 3GPP TS 23.501 [21] in MSISDN representation.	Regular expression as per ETSI TS 103 280 [7]
GPSINAI	General Public Subscription Identifier as defined in 3GPP TS 23.501 [21] in NAI representation.	Regular expression as per ETSI TS 103 280 [7]
EUI64	EUI64 as defined in ETSI TS 103 280 [7], clause 6.50.	Regular expression as per ETSI TS 103 280 [7]
CGI	Cell Global Identification as defined in ETSI TS 103 280 [7], clause 6.51.	Regular expression as per ETSI TS 103 280 [7]
ECGI	E-UTRAN Cell Global Identification as defined in ETSI TS 103 280 [7], clause 6.52.	Regular expression as per ETSI TS 103 280 [7]
NCGI	NR Cell Global Identification as defined in ETSI TS 103 280 [7], clause 6.53.	Regular expression as per ETSI TS 103 280 [7]
ICCID	Integrated circuit card identifier as defined in ETSI TS 103 280 [7], clause 6.54.	Regular expression as per ETSI TS 103 280 [7]
VIN	Vehicle Identification number as defined in ETSI TS 103 280 [7], clause 6.57	Regular expression as per ETSI TS 103 280 [7]
ServiceAccessId entifier	ServiceAccessIdentifier as defined in ETSI TS 103 280 [7], clause 6.58.	Regular expression as per ETSI TS 103 280 [7]
EUICCID	eUICC Identifier, corresponding to the EID as defined in GSMA SGP.02 [34], clause 2.2.2.	Regular expression as per ETSI TS 103 280 [7]

Annex D (normative): Error Codes

D.1 Detailed error codes

Table D.1: Detailed Error Codes

Error Code	Error Description	Message Element
3000	General Business Logic Error.	
3001	Feature Not Supported.	
3002	Duplicate ActionID detected.	
3003	Transient Technical Error.	"Call us if this persists"
3004	Configuration Issue - <Customize element>.	Indicates portal element to configure (Example: Legal Order Type configuration)
	Message Element Checks.	
3005	Required element missing. (Mandatory per national profile.) (Example: Valid CSPID present.)	Specific element type from the messageheader or object structure is cited. (Object reference if applicable) ObjectID: <Object_Value>: <Element name>
3006	Value change not allowed. (Update operations.)	Specific element type from the messageheader or object structure is cited. (Object reference if applicable) ObjectID: <Object_Value>: <Element name>
3007	Improper value. (Semantic value does not fit context. Schema validation catches syntactic.)	Specific element type from the messageheader or object structure is cited. (Object reference if applicable) ObjectID: <Object_Value>: <Element name>
3008	Improper value change. (New value not allowed.)	Specific element type from the messageheader or object structure is cited. (Object reference if applicable) ObjectID: <Object_Value>: <Element name>
3009	Value not found in system. (Reference to previous system value.)	Specific element type from the messageheader or object structure is cited. (Object reference if applicable) ObjectID: <Object_Value>: <Element name>
	Object Reference Checks.	
3010	Attempt to Create an Object that already exists.	Object_ID: <Object_Value>
3011	Attempt to Update an Object that does not exist.	Object_ID: <Object_Value>
3012	Attempt to Update an Object that has Expired. (Question on reuse and impact on audits.)	Object_ID: <Object_Value>
3013	Attempt to Cancel an Object that does not exist.	Object_ID: <Object_Value>
3014	Attempt to Get an Object that cannot be found.	Object_ID: <Object_Value>
3015	Attempt to Get an Object that was found but not deliverable via tasking interface. (Object may have been archived.)	Object_ID: <Object_Value>
3016 (3200)	Attempt to link an Object to an Associated Object that does not exist.	Linked_From_Object_ID: <Object_Value> Linked_To_Object_ID: <Object_Value>
3017	Attempt to link an Object to an Associated Object that has Expired. (Question on reuse and impact on audits.)	Linked_From_Object_ID: <Object_Value> Linked_To_Object_ID: <Object_Value>
3018	Attempt to link an Object to an Associated Object that failed. (Two objects sent in same message.) (Example: <3106> Warrant doc delivery.)	Linked_From_Object_ID: <Object_Value> Linked_To_Object_ID: <Object_Value>

Error Code	Error Description	Message Element
3019	Unsupported encoding used.	
3020	Validation error.	The application shall deliver more information about the cause of the validation error in the error message.
3021	Version not supported.	The application shall deliver the supported versions in the error message.
3022	Message too large.	The application shall deliver the supported maximum size in the error message.
3023-3999	Reserved for future Errors.	
4000-4999	Reserved for nationally-defined Error Codes.	The relevant national profile may specify additional error codes in this range

Annex E (normative): Approval Details

E.1 Overview

An individual approval may be represented by the ApprovalDetails structure, defined by table E.1. This structure documents the nature of an approval and the details of the signatures on such actions.

Table E.1: ApprovalDetails

Field	Format	Description	Reference
ApprovalType	LongString (see ETSI TS 103 280 [7])	Defines the nature of the approval: e.g. Creation, Renewal, Modification, Cancellation.	Clause E.2
ApprovalDescription	LongString (see ETSI TS 103 280 [7])	Human readable description of what elements of the authorisation were changed.	Clause E.3
ApprovalReference	LongString (see ETSI TS 103 280 [7])	Nationally defined reference for the Approval, provided to allow correlation with non-HI-1 processes.	Clause E.4
ApproverDetails	ApproverDetails	Gives details of who gave the Approval.	Clause E.5
ApprovalTimestamp	QualifiedDateTime (see ETSI TS 103 280 [7])	Indicates when the Approval was given or signed.	Clause E.6
ApprovalsEmergency	Boolean	Flag to indicate that this was an emergency change.	Clause E.7
ApprovalDigitalSignature	Complex Type (see clause E.8)	Provides digital signature information relating to the approval.	Clause E.8
ApprovalNationalDetails	Complex Type	Provides national-specific data elements associated with an approval.	

E.2 ApprovalType

The ApprovalType field is used to indicate the type of approval being given. The acceptable values and business meaning of this field shall be defined by the relevant national profile.

E.3 ApprovalDescription

The ApprovalDescription field is used to provide a human readable description of the contents of authorisation. This may include a human-readable description of what is being authorised, or other process or legal information (e.g. "boilerplate" text) that may be relevant to the approval. The precise contents and meaning of this field will be defined by the relevant national profile.

E.4 ApprovalReference

The ApprovalReference field is a nationally-defined reference for the Approval, provided to allow correlation with non-HI-1 processes. The precise contents and meaning of this field will be defined by the relevant national profile.

E.5 ApproverDetails

E.5.1 Overview

The ApproverDetails gives details of the person, role or other entity that is granting the Approval. It consists of the following fields.

Table E.2: ApproverDetails

Field	Format	Description
ApproverName	LongString (see ETSI TS 103 280 [7]).	Name or other identifier of the Approver.
ApproverRole	LongString (see ETSI TS 103 280 [7]).	Nationally-defined role of the Approver (e.g. rank, post or office).
ApproverIdentity	ApproverIdentity (see clause E.5.2).	Identity of the Approver given in a machine-readable format.
ApproverContactDetails	List of ApproverContactDetails (see clause E.5.3).	Contact details of the Approver.

E.5.2 ApproverIdentity

The ApproverIdentity field asserts the identity of the approver in a machine-readable form.

The ApprovalIdentity field contains one of the following structures.

Table E.3: ApproverIdentity

Field	Format	Description
NationalApproverIdentity	Defined by the relevant national profile.	Nationally-defined digital signature details.

It is important that on a national basis appropriate measures are in place, either digitally or through other processes, to provide appropriate identity details. It is expected that future versions of the present document will include digital signature recommendation as defined by ETSI TC CYBER.

E.5.3 ApproverContactDetails

The ApproverContactDetail gives contact details of the person, role or other entity that is granting the Approval. It consists of the following fields.

Table E.4: ApproverContactDetail

Field	Format	Description
ApproverAlternateName	LongString (see ETSI TS 103 280 [7]).	Alternate name or other identifier of the Approver.
ApproverEmailAddress	EmailAddress (see ETSI TS 103 280 [7]).	E-mail address of the Approver.
ApproverPhoneNumber	InternationalE164 (see ETSI TS 103 280 [7]).	Phone number of the Approver.

E.6 ApprovalTimestamp

The ApprovalTimestamp field is used to indicate when the Approval was given, in ISO date-time format with an explicit timezone indication.

E.7 ApprovalIsEmergency

The ApprovalIsEmergency field is used to indicate whether the Approval has been given under emergency circumstances. The definition of "emergency circumstances" and the use of this field will be given in the relevant national profile.

E.8 ApprovalDigitalSignature

E.8.1 Overview

The ApprovalDigitalSignature field is used to provide a digital signature which covers all or part of one or more HI-1 Objects, including other Approvals. Implementers should note that the ApprovalDigitalSignature field is **not** used to digitally sign an HI-1 Message or Action - this is done using the appropriate Message Security procedures given in clause 9.

For the avoidance of doubt, the following aspects of the ApprovalDigitalSignature are not in scope of the present document, and shall be defined by the relevant national profile:

- The circumstances and processes surrounding the use of digital signatures to indicate or assert approval of a given Object.
- Which parts of which HI-1 Objects have to be signed for a given HI-1 Object to be considered valid.
- Issues surrounding key management and distribution.

The ApprovalDigitalSignature contains one of the following structures.

Table E.5: Approval Digital Signature

Field	Format	Description
NationalDigitalSignature	Defined by the relevant national profile.	Nationally-defined digital signature details.

It is important that on a national basis appropriate measures are in place, either digitally or through other processes, to provide appropriate signature details. It is expected that future versions of the present document will include digital signature recommendation as defined by ETSI TC CYBER.

Annex F (normative): Dictionaries

F.1 Overview

The DictionaryEntry type is used to provide for fields that can be easily and unambiguously extended by national implementers without needing to change the underlying schema or the HI-1 message parsing and storing aspects of an implementation (e.g. a database).

This annex describes the following:

- The definition of the DictionaryValue type and associated dictionaries.
- Definitions, procedures and conventions concerning the definition and use of dictionaries.

F.2 DictionaryEntry type

The DictionaryEntry type is intended to represent a single string value chosen from an extensible enumerated list. It is defined as follows.

Table F.1: DictionaryEntry

Field	Format	Description
Owner	ShortString (see ETSI TS 103 280 [7]).	Name of the owner of the dictionary (see clause F.3.2).
Name	ShortString (see ETSI TS 103 280 [7]).	Name of the dictionary from which the value is chosen (see clause F.3.3).
Value	ShortString (see ETSI TS 103 280 [7]).	Value chosen from the dictionary.

A dictionary of DictionaryEntry values shall consist of the following definitions.

Table F.2: Required information when defining a dictionary

Field	Format	Description
Owner	ShortString (see ETSI TS 103 280 [7]).	Name of the owner of the dictionary (see clause F.3.2).
Name	ShortString (see ETSI TS 103 280 [7]).	Name of the dictionary from which the value is chosen (see clause F.3.3).
Value	ShortString (see ETSI TS 103 280 [7]).	A label which is unique within the dictionary, and assigned a meaning.
Meaning	LongString (see ETSI TS 103 280 [7]).	A human-readable definition of the meaning associated with the Value.

For more details on the definition and use of dictionaries, see clause F.3.

F.3 Definition and use of dictionaries

F.3.1 Overview

This clause defines the definition and use of dictionaries.

F.3.2 Owner

Each dictionary has a defined owner. The owner of a dictionary is responsible for the definition of the dictionary, as well as the maintenance and publication of the dictionary. All dictionaries shall contain at least the information specified in clause F.2.

A dictionary owner is specified by a string value. The following owners are defined by the present document:

- "ETSI": The dictionary is owned by ETSI, and defined in the present document.
- A valid ISO 3166-1 [14] country code: The dictionary is owned and defined by the relevant national authority for the country specified by the country code.

F.3.3 Name

Each dictionary shall have a defined name which is unique within the owner of that dictionary. A name may be any valid ShortString.

F.3.4 Use of dictionaries

Any field which the present document defines as a DictionaryEntry shall either specify an ETSI dictionary of default values, or specify that the permissible values shall be given in a nationally-defined dictionary.

If an ETSI dictionary is specified, then each national profile may specify additional dictionaries that contain additional permissible types and values, as well as confirming or clarifying the handling of ETSI defined values. If an ETSI dictionary is not specified, then each national profile shall either specify a dictionary of permissible values, or state that the field shall not be used.

It is strongly discouraged to introduce ambiguity by duplicating ETSI-defined values in nationally-owned dictionaries. Should ETSI choose to adopt a value already defined in a nationally-owned dictionary, the owner is strongly encouraged to consider whether to retain the nationally-defined value.

A national profile shall not modify any dictionary that it is not the owner of by adding or removing values. However, it is permissible for a national profile to define the handling of ETSI-defined values.

F.3.5 Machine-readable dictionary definitions

Implementers are encouraged to allow Dictionary definitions to be easily updated to e.g. storing them in a database table, or ingesting them as a configuration file.

In order to facilitate this, an XML XSD schema is provided alongside the present document that defines a machine-readable format for Dictionary definitions ("ts_103120v011701p0.zip"). Additionally, the dictionary definitions given in the present document are supplied as an XML file which conforms to the dictionary specification ("ts_103120v011701p0.zip").

National profiles may specify additional dictionaries in additional XML files.

Annex G (normative): Drafting conventions for National Parameters

G.1 Overview

This clause gives normative drafting conventions and guidelines that shall be used when drafting National Parameters for use in the National Parameter extension points.

G.2 Drafting conventions

National profiles are encouraged to restrict the number of national extensions to a minimum, and use standard fields and/or extended dictionary types where possible (see annex F for more details on dictionaries).

A national profile shall specify whether a National Parameter definition exists for each of the extension points defined in the standard. An extension point can be identified in the following way:

- The element name begins with "National".
- The element is defined as being "abstract" in the schema.
- The abstract definition contains a single "CountryCode" field.

A National Parameter definition shall follow these drafting conventions:

- It shall be defined in a schema with a namespace specific to, and defined in, the relevant national profile.
- It shall be defined as an extension of the relevant base type via XSD's `xs:extension` mechanism or the equivalent translation as described in ETSI TS 103 280 [7].
- In instance documents, the "CountryCode" field shall be populated with the country code of the relevant national profile, to indicate the source of the extension.

Annex H (normative): Workflow Profiles

H.1 Basic information about Workflow Profiles

This annex defines some Workflow Profiles. Each Workflow Profile provides extra constraints.

If both parties agree that a profile shall be adopted, then all provisions of that profile shall be followed.

H.2 Simple disclosure request Workflow Profile

H.2.1 Definition

This Workflow Profile may be used for situations complying with the structure in clause H.2.2.

This Workflow Profile shall not be used for situations which necessarily require an ongoing answer i.e. situations which necessarily require some answers to be supplied at one point in time and then some further answers to be given later.

H.2.2 Constraints on structure of objects

There shall be one Authorisation Object.

There shall be one or more Task Objects. Each Task Object shall contain within its AssociatedObjects field (defined in clause 7.1.4) the identifier of the Authorisation Object to which it belongs.

There shall be one or more Document Objects. Each Document Object shall contain within its AssociatedObjects field (defined in clause 7.1.4) the identifier of the Authorisation Object to which it belongs.

H.2.3 Constraints on the contents of objects

H.2.3.1 Authorisation Object contents

This Workflow Profile does not describe any constraints on the contents of the Authorisation Object.

H.2.3.2 Task Object contents

The Task Object shall have the constraints described in this clause.

There shall be a parameter supplied by the LEA side in the Reference field (see clauses 8.2.2 or 8.3.2). There is no assurance about the uniqueness of this parameter (some LEAs may choose to make this unique, but uniqueness is not required or guaranteed by the present document). This parameter shall be attached to the results that are created from this request.

The CSP shall also create an identifier for a task. It may make this unique to the extent that is required for its purposes. The identifier shall be put in the ExternalIdentifier (see table 7.1) field (wherever it is present).

H.2.3.3 Document Object contents

This Workflow Profile does not define any constraints on the contents of the Document Objects.

H.2.4 Constraints on flow of messages

When using the Workflow Profile in this clause, the following message flow shall be observed:

- 1) **START:** LEA initiates the process. The LEA shall send a single Request Message (as defined in clause 5) containing a CREATE for the items listed in clause H.2.2.
- 2) **CSP syntax check.** The CSP performs a check on the Request Message to ensure it complies syntactically with the schema and Workflow Profile. If it complies, the CSP shall send a Response Message (as defined in clause 5) as a positive acknowledgement and move to step 3. If not, or there is a technical error, send a Response Message with the appropriate error (further details in annex D) and the message flow is terminated.
- 3) **The CSP either:**
 - a) States there is a results set (this case includes the situation where there are zero results, which shall be signalled clearly in the results). In this case, delivery takes place using mechanisms outside the scope of this annex. The status of the task object is now Disclosed. To inform the LEA that the delivery was created a notification objects for the tasks shall be created. All the disclosed task objects shall be included in the field StatusOfAssociatedObjects which contains a list of AssociatedObjectStatus. The field Status of the AssociatedObjectStatus structure shall contain the status value Disclosed.
 - b) States there is not a results set (this case does not include the situation where there are zero results). The status of task object is now Rejected. To inform the LEA that the delivery will not be created. Notification objects for the rejected tasks shall be created to prevent the LEA from polling to get the status information. All the rejected task objects shall be included in the field StatusOfAssociatedObjects which contains a list of AssociatedObjectStatus. The field Status of the AssociatedObjectStatus structure shall contain the status value Rejected. The optional field Details of the AssociatedObjectStatus structure may contain a description why the task has been rejected.

Step 3 takes place within the present document (i.e. part of this Workflow Profile) based on a way for the CSP to inform the LEA about the change in status.

Where there is more than one task (see clause H.2.2), step 3 shall take place independently for each task.

H.3 Multi-endpoint Workflow Profile

H.3.1 Definition

This Workflow Profile may be used for situations complying with the structure in clause H.3.2. It differs from the simple Workflow Profile in that there are multiple Workflow Endpoints (on the CSP side). A Workflow Endpoint is defined as an HTTPS URL which accepts only HI-1 messages that comply with a specific subset of the HI-1 message syntax, as described by the relevant stage of this Workflow Profile. Which URLs map to which stages or profiles is a matter for onboarding between an LEA and a CSP.

This Workflow Profile shall not be used for situations which necessarily require an ongoing answer i.e. situations which necessarily require some answers to be supplied at one point in time and then some further answers to be given later.

NOTE: This means that LI lifecycle operations are not covered by the present document.

Clause H.4 describes how the Workflow Profiles in clauses H.2 and H.3 can be made interoperable through the use of a small function or "shim".

H.3.2 Constraints on the structure and contents of objects

The contents and structure of the objects provided in the stages above shall conform to the constraints set out in clauses H.2.2 and H.2.3.

H.3.3 Message flow

H.3.3.1 Overview

When using the Workflow Profile in this clause, the following message flow shall be observed.

H.3.3.2 Create Authorisation

LEA initiates the process by invoking the "Create Authorisation" Workflow Endpoint.

The "Create Authorisation" Workflow Endpoint shall accept an HI-1 message containing a single CREATE request for an Authorisation Object (see clause 7.2) with AuthorisationDesiredStatus set to CreatingForCSP (see clause 7.2.6).

H.3.3.3 Adding of documents and tasks

The required information that is part of the Authorisation shall be added as followed. Any order shall be permitted.

- Documents. The LEA adds one or more documents to the Authorisation. Documents are added by invoking the "Add Document" Workflow Endpoint. The Add Document Workflow Endpoint accepts an HI-1 message containing one or more CREATE Requests for a Document Object (see clause 7.3). There may be more than one invocation of the Add Document Workflow Endpoint for the documents within each Authorisation. Each Document shall reference the Authorisation via the AssociatedObjects field (see clause 7.1.4).
- Tasks. The LEA adds one or more LDTasks to the Authorisation, referencing the Authorisation. LDTasks are added by invoking the "Add LD Task" Workflow Endpoint. The Add LD Task Workflow Endpoint accepts an HI-1 message containing one or more CREATE Requests for an LDTask Object (see clause 8.3). There may be more than one invocation of the Add LD Task Workflow Endpoint for the tasks within each Authorisation. Each LDTask shall reference the Authorisation via the AssociatedObjects field (see clause 7.1.4).

If an invocation of one of these Workflow Endpoints fails, the Receiver shall return an Action Unsuccessful Information Response with appropriate error information (see clause 6.4.9), and shall disregard the invocation. The Sender may, at the Sender's discretion, decide to continue with the Authorisation and attempt further invocations, or to cancel the Authorisation (see clause H.3.3.5).

H.3.3.4 Submit Authorisation

When all the relevant objects (Documents and Tasks) have been added to the Authorisation, the LEA submits them by invoking the Submit Authorisation Workflow Endpoint. This Workflow Endpoint accepts an HI-1 message containing a single UPDATE for the Authorisation which sets the AuthorisationDesiredStatus field to "SubmittedToCSP" (see clause 7.2.6).

The CSP shall now proceed as described in clause H.2.4, step 3 onwards. If there is an error with the Authorisation structure, the CSP shall set the Status of the Authorisation to "Invalid" as appropriate (see clause 7.2.5).

H.3.3.5 Cancel Authorisation

At any stage prior to "Submit Authorisation", the LEA may cancel the Authorisation by invoking the "Cancel Authorisation" Workflow Endpoint. This Workflow Endpoint accepts an HI-1 messaging containing a single UPDATE for the Authorisation which sets the AuthorisationDesiredStatus field to "Cancelled" (see clause 7.2.6).

H.4 Conversion between Simple and Multi-Endpoint Workflow Profiles (informative)

H.4.1 Description

This clause defines an informative approach for how to interoperate between the Workflow Profiles in clauses H.2 and H.3. It is not normative: there is no assurance that following this clause necessarily gives a compliant solution.

The conversion functionality is called a shim. The present document does not specify whether the shim is hosted at the LEA or CSP.

H.4.2 Shim between a Simple Workflow LEA and a Multi-Endpoint at CSP

The shim would:

- 1) Take in the CREATE (from step 1 of clause H.2.4). If there is a problem with the CREATE (badly formed, not understandable) the shim would reply immediately with an error.
- 2) Using information received in step 1, create an Authorisation (clause H.3.3.2).
- 3) Split the remaining information (from step 1) into the relevant structures of clause H.3.3.3, making the appropriate series of invocations. If the shim receives errors for the invocations in clause H.3.3.3, the shim could choose to re-send or could choose to cancel the Authorisation (clause H.3.3.5) (if cancelled, move to step 6).
- 4) If the Authorisation, Task(s) and Document(s) have been successfully sent, the shim would invoke the Submit Authorisation Workflow Endpoint.
- 5) If the shim gets positive confirmation of an invocation to the Submit Authorisation Workflow Endpoint, it would send a positive acknowledgement back to the LEA side and the function of the shim is complete (all further stages are identical between the two Workflow Profiles).
- 6) If the shim does not manage to get a positive confirmation of an invocation to the Submit Authorisation Workflow Endpoint, it would send an error back to the LEA side. In this situation, it would (if appropriate) make sure that the Cancel Authorisation Workflow Endpoint had been invoked. This ends the function of the shim.

H.4.3 Shim between a Multi-Endpoint LEA and a Simple Workflow at CSP

The shim would:

- 1) Take in the calls from clauses H.3.3.2 and H.3.3.3. It would respond to each of them individually, with a positive acknowledgement unless it is already clear that something is not correct. If something is identified as being incorrect with the calls in clause H.3.3.3, the shim would respond with the appropriate error message and behave as described in clause H.3.3.3 (i.e. make that single invocation null and void and then allow further invocations).
- 2) Once it receives an invocation on the Submit Authorisation Workflow Endpoint, it would create one message (as per step 1 of clause H.2.4) and send this to the CSP:
 - a. If the shim gets a positive acknowledgement from the CSP, then the shim would reply with a positive acknowledgement to the LEA's invocation of the Submit Authorisation Workflow Endpoint. The work of the shim is complete as further steps are identical between the two Workflow Profiles.
 - b. If the shim gets an error from the CSP, it would reply with an error to the LEA's invocation of the Submit Authorisation Workflow Endpoint. This completes the function of the shim.

H.5 Workflow Profile for the LI lifecycle

H.5.1 Overview and scope

This Workflow Profile may be used between an CSP and LEA to support common operations in the lifecycle of an ongoing LI warrant.

This Workflow Profile is intended to support operations between CSP and LEA. It is not intended to cover the warrant approval procedures within the LEA or relevant warrant granting department that are required prior to each of these operations, although it may be used in any instance where an organization can adopt the role of a CSP.

Likewise, any considerations regarding what authorisation is required for each operation, or which operations may be authorised or otherwise in any given jurisdiction, are out of scope of the present document. Not all operations may be required or supported by a given CSP or LEA.

This Workflow Profile covers the following operations, each of which is exposed as a Workflow Endpoint (see clause H.3.1) with a default relative URL path in table H.0:

Table H.0: LI Workflow Profile Endpoints

Endpoint	Relative URL Path	Clause
New Authorisation	/li/authorisation/new	H.5.3
Authorisation Extension	/li/authorisation/extension	H.5.4
Authorisation Cancellation	/li/authorisation/cancellation	H.5.5
Task Addition	/li/task/addition	H.5.6
Task Cancellation	/li/task/cancellation	H.5.7
Change of Delivery	/li/task/change-delivery	H.5.8

The URL path is specified relative to the API base URL. For example, if the API base URL is example.com, the "New Authorisation" endpoint would be example.com/li/authorisation/new. The API base URL could include the version of the specification used. Usage of the relative URL path is the default for the endpoint but is not required; different URL paths may be provided by the CSP when onboarding the LEA.

Details which apply to all of the above operations are given in clause H.5.2.

H.5.2 Common procedures and definitions

H.5.2.1 Object Model

This Workflow Profile assumes the following object model, equivalent to the one described in clause H.2.

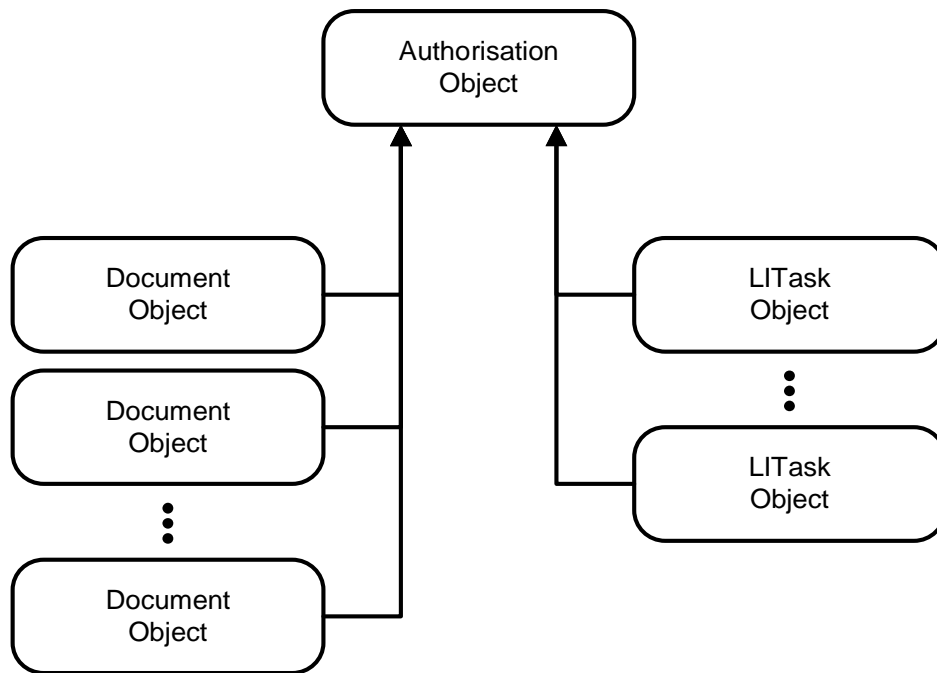


Figure H.1: Object model for the LI lifecycle workflow profile

There is a single Authorisation Object that represents the current overall state of the lawful authority covering the interception.

There are zero or more Document Objects that represent the lawful instruments and orders used to authorise the interception. The net effect of the combination of these instruments and orders is represented by the Authorisation Object. Each Document Object shall be related to a single relevant Authorisation via the Document Object's AssociatedObjects field (see clause 7.1.4).

There are zero or more Task Objects that represent the instruction to intercept a particular identifier. Each LITaskObject shall be related to a single relevant Authorisation via the LITaskObject's AssociatedObjects field (see clause 7.1.4).

The Workflow Profile operations described in the following clauses provide mechanisms to create, maintain and terminate interception by creating, altering and removing elements in this object model.

H.5.2.2 Common procedure

H.5.2.2.1 Overview

Unless otherwise specified, each of the Workflow Endpoints defined in clause H.5.3 follows the procedure as outlined below.

H.5.2.2.2 LEA Request

The LEA initiates the procedure by issuing a single Request Message (see clause 5) containing the verbs and objects required by the Workflow Endpoint.

H.5.2.2.3 Initial CSP Response

The CSP verifies the syntax of the request. If the request is syntactically correct and meets the requirements of the Workflow Endpoint, then it shall send a Response Message (as defined in clause 5) as a positive acknowledgement and move to clause H.5.2.2.4. In all other circumstances it shall respond with a top-level Error Response (see clause 6.3.3) describing the nature of the error. Both CSP and LEA shall consider the transaction to be terminated, and no action is taken. The state of the Authorisation, Document and LITask Objects on the CSP side remains unchanged.

H.5.2.2.4 CSP review and action

The CSP updates the state of the Authorisation, Document and Task Objects as outlined in the relevant Workflow Endpoint definition to signal that it is processing the requested changes.

The CSP follows any necessary internal procedures to review the changes requested via the Workflow endpoint. If these are successful, the CSP makes the changes requested to the Authorisation, Document and LITask Objects as described in the Workflow Endpoint and where appropriate actions the necessary requests e.g. by starting or stopping interception. The CSP shall issue a Notification Object (see clause 7.4) to the LEA informing them that the requested changes have been actioned. If, as a result of the changes, the status of an Authorisation, Document or LITask Object is updated, this shall be reflected via the StatusOfAssociatedObjects structure (see clause 7.4.7).

If the CSP established that some or all of the changes cannot take place, then all the requested changes are rejected. The CSP shall revert the status of the Authorisation, Document and LITask Objects to their original values, and issue a Notification Object (see clause 7.4) to the LEA informing them of the rejection. The NotificationDetails field (see clause 7.4) shall contain a reference to the Transaction Identifier (see clause 6.2.5) of the original Request message, and an explanation of why the changes could not be made.

H.5.2.3 Common constraints

H.5.2.3.1 Overview

Unless otherwise specified, objects provided to the Workflow Endpoints defined in clause H.5.3 shall obey the following constraints, in addition to any specified in the relevant Workflow Endpoint description.

H.5.2.3.2 Authorisation Object

No common constraints are specified.

H.5.2.3.3 LI Task Object

No common constraints are specified.

H.5.2.3.4 Document Object

Where a Document Object is provided without a DocumentBody (see clause 7.3.9) e.g. because it is necessary to transport the content of the document via other means, then the DocumentReference field (see clause 7.3.2) shall be populated such that the CSP can associate the object with the appropriate contents.

Where a Document Object is provided with a DocumentBody (see clause 7.3.9), the ContentType shall be one of the following, or any other MIME type as agreed between the CSP and LEA:

- application/pdf.
- application/vnd.openxmlformats-officedocument.wordprocessingml.document.
- image/png.
- image/jpeg.
- text/plain.

If a ContentType is provided that is not on the list of acceptable MIME types for a CSP, that CSP shall reject the request as part of its initial response (see clause H.5.2.2.3).

H.5.3 New Authorisation Workflow Endpoint

H.5.3.1 Description

This endpoint covers the act of serving a new warrant, or other lawful authorisation for Lawful Interception, together with supporting documentation and a set of authorised tasking instructions, on a CSP. It provides the initial set of Authorisation, Document and LITask objects considered in the object model given in clause H.5.2.1.

NOTE: For the purposes of these workflows, a warrant is considered "new" from the perspective of the CSP. The LEA may have served the same authorisation (with different LITasks) on one CSP, before including additional LITasks that involve a second CSP. This workflow endpoint would be used in both cases for the LEA to provide the authorisation and the appropriate subset of LI Tasks for each CSP, since the warrant is "new" to each respective CSP.

H.5.3.2 Message flow

The message flow shall be as described in clause H.5.2.2.

H.5.3.3 Message contents

The LEA request message shall contain the following:

- A CREATE Request for an Authorisation Object that represents the new authorisation.
- One or more CREATE Requests for LITask Objects that represent the technical instructions for interception.
- One or more CREATE Requests for Document Objects that represent the actual legal documents used to form the authorisation.

The relationships between the objects shall be as described in clause H.5.2.1.

H.5.3.4 Constraints on objects

This endpoint does not place any additional constraints on the contents of objects.

H.5.4 Authorisation Extension Workflow Endpoint

H.5.4.1 Description

This endpoint covers the act of extending the end date of the lawful authorisation to perform interception. It does so by modifying the AuthorisationTimespan field of the Authorisation Object, and the Timespan field of selected LITaskObjects.

H.5.4.2 Message flow

The message flow shall be as described in clause H.5.2.2.

H.5.4.3 Message contents

The LEA request message shall contain the following:

- An UPDATE Request for the relevant Authorisation Object.
- Zero or more UPDATE Requests for the LITask Objects for which the LEA wishes to extend interception (updating the Authorisation End Time does not implicitly extend Tasks associated to the Authorisation).
- One or more CREATE Requests for Document Objects that represent the legal documents used to authorise the extension.

The relationships between the objects shall be as described in clause H.5.2.1.

H.5.4.4 Constraints on objects

H.5.4.4.1 Authorisation Object

The following fields shall be present in the UPDATE request for the Authorisation Object.

Table H.1: Authorisation fields in the Warrant Extension Workflow Endpoint

Field	Description	M/C/O	Reference
AuthorisationTimespan	Shall be populated to provide the new end date of the authorisation. Only the endTime member shall be populated.	M	Clause 7.2.7

H.5.4.4.2 LITask Objects

The following fields shall be present in each UPDATE request for an LITask Object.

Table H.2: LITaskObject fields in the Warrant Extension Workflow Endpoint

Field	Description	M/C/O	Reference
Timespan	Shall be populated to provide the new end date of the interception. Only the endTime member shall be populated. Shall be earlier than or equal to the AuthorisationTimespan endTime given in table H.1.	M	Clause 8.2.5

H.5.4.4.3 Document Objects

This workflow endpoint does not define any restrictions on the content of the Document objects. They should provide sufficient information to the CSP to verify that the extension of the Authorisation and LITask Objects is permitted.

H.5.5 Authorisation Cancellation Workflow Endpoint

H.5.5.1 Description

This endpoint covers the act of terminating a warrant prior to the scheduled end-date of that warrant. This shall be considered as a request to terminate any active interceptions authorised under that warrant, and means that no further interceptions can be started under that warrant. This is different from terminating an interception under **§** authorisation (see clause H.5.7), and different from allowing an authorisation to reach its expiry date.

H.5.5.2 Message flow

The message flow shall be as described in clause H.5.2.2.

H.5.5.3 Message contents

The LEA request message shall contain the following:

- An UPDATE Request for the relevant Authorisation Object to set the status to cancelled.
- Zero or more CREATE Requests for Document Objects that represent the legal documents that give effect to the cancellation.

The relationships between the objects shall be as described in clause H.5.2.1.

If this workflow succeeds, then both the CSP and LEA shall consider all LITask Objects associated with the Authorisation to be cancelled too.

H.5.5.4 Constraints on objects

H.5.5.4.1 Authorisation Object

The following fields shall be present in the UPDATE request for the Authorisation Object.

Table H.3: Authorisation fields in the Warrant Cancellation Workflow Endpoint

Field	Description	M/C/O	Reference
AuthorisationDesiredStatus	Shall be set to "Cancelled".	M	Clause 7.2.6

H.5.5.4.2 Document Objects

This workflow endpoint does not define any restrictions on the content of the Document Objects beyond those given in clause H.5.2.1. They should provide sufficient information to the CSP to verify that the cancellation of the Authorisation and LITask Objects is required.

H.5.6 Task Addition Workflow Endpoint

H.5.6.1 Description

This endpoint covers the act of adding a new interception instruction under a warrant or other lawful authorisation that has already been given to the CSP.

H.5.6.2 Message flow

The message flow shall be as described in clause H.5.2.2.

H.5.6.3 Message contents

The LEA request message shall contain the following:

- A CREATE Request for the new LITask Object.
- One or more CREATE Requests for Document Objects that represent the legal documents that authorise the new interception under the existing warrant or lawful order.

The relationships between the objects shall be as described in clause H.5.2.1.

H.5.6.4 Constraints on objects

H.5.6.4.1 LITask Object

This workflow endpoint does not define any restrictions on the content of the LITask Objects beyond those given in clause H.5.2.1.

H.5.6.4.2 Document Objects

This workflow endpoint does not define any restrictions on the content of the Document Objects beyond those given in clause H.5.2.1. They should provide sufficient information to the CSP to verify that the addition of the new interception under the existing authorisation is permitted.

H.5.7 Task Cancellation Workflow Endpoint

H.5.7.1 Description

This endpoint covers the termination of an interception, without affecting the warrant or lawful order. This is used in situations where other interception under the same warrant is required to continue. This is different to the situation in which the authorisation and all related interceptions are cancelled, which is covered by clause H.5.4.

H.5.7.2 Message flow

The message flow shall be as described in clause H.5.2.2.

H.5.7.3 Message contents

The LEA request message shall contain the following:

- An UPDATE Request for the LITask Object that is to be cancelled.
- Zero or more CREATE Requests for Document Objects that represent the legal documents that authorise the new interception under the existing warrant or lawful order.

H.5.7.4 Constraints on objects

H.5.7.4.1 LITask Object

The following fields shall be present in the UPDATE request for each LITask Object that the LEA requires to terminate interception for.

Table H.4: LITaskObject fields in the Task Cancellation Workflow Endpoint

Field	Description	M/C/O	Reference
DesiredStatus	Shall be set to "Cancelled"	M	Clause 8.2.4

H.5.7.4.2 Document Objects

This workflow endpoint does not define any restrictions on the content of the Document Objects beyond those given in clause H.5.2.1. They should provide sufficient information to the CSP to verify that the termination of the interception is required.

H.5.8 Change of Delivery Endpoint

H.5.8.1 Description

This endpoint covers updating information given to the CSP regarding where and how interception product should be delivered.

H.5.8.2 Message flow

The message flow shall be as described in clause H.5.2.2.

H.5.8.3 Message contents

The LEA request message shall contain the following:

- One or more UPDATE Requests for LITask Objects.

- Zero or more UPDATE Requests for Document Objects.

H.5.8.4 Constraints on objects

H.5.8.4.1 LITask Object

The following fields shall be present in the UPDATE request for each LITask Object that the LEA wishes to change the delivery details for.

Table H.5: LITaskObject fields in the Change Of Delivery Workflow Endpoint

Field	Description	M/C/O	Reference
DeliveryDetails	Shall contain the new delivery details for the LITask Object	M	Clause 8.2.8

H.5.8.4.2 Document Objects

This workflow endpoint permits Documents Objects to be provided where necessary. In situations where an LEA is free to alter the delivery details as a technical matter, it may be that no Document Objects are required or provided. In situations where Document Objects are provided, this workflow endpoint does not define any restrictions on the content of the Document Objects beyond those given in clause H.5.2.1.

H.6 Workflow Profile for the LP lifecycle

H.6.1 Overview and Scope

This Workflow Profile may be used between a CSP and LEA to support common operations in the lifecycle of an LP request. It is not intended to cover the preservation approval procedures within the LEA or relevant authorisation granting department that are required prior to each of these operations, although it may be used in any instance where an organization can adopt the role of a CSP.

Likewise, any considerations regarding what authorisation is required for each operation, or which operations may be authorised or otherwise in any given jurisdiction, are out of scope of the present document. Not all operations may be required or supported by a given CSP or LEA.

This Workflow Profile covers the following operations, each of which is exposed as a Workflow Endpoint (see clause H.3.1) with a default relative URL path in table H.6.1-1.

Table H.6.1-1: LP Workflow Profile Endpoints

Endpoint	Relative URL Path	Clause
New Preservation	/lp/new	H.6.3
Preservation Extension	/lp/extension	H.6.4
Preservation Cancellation	/lp/cancellation	H.6.5

The URL path is specified relative to the API base URL. For example, if the API base URL is example.com, the "New Preservation" endpoint would be example.com/lp/new. The API base URL could include the version of the specification used. Usage of the relative URL path is the default for the endpoint but is not required; different URL paths may be provided by the CSP when onboarding the LEA.

Details which apply to all of the above operations are given in clause H.6.2.

H.6.2 Common procedures and definitions

H.6.2.1 Object Model

This Workflow Profile assumes the following object model, equivalent to the one described in clause H.2.

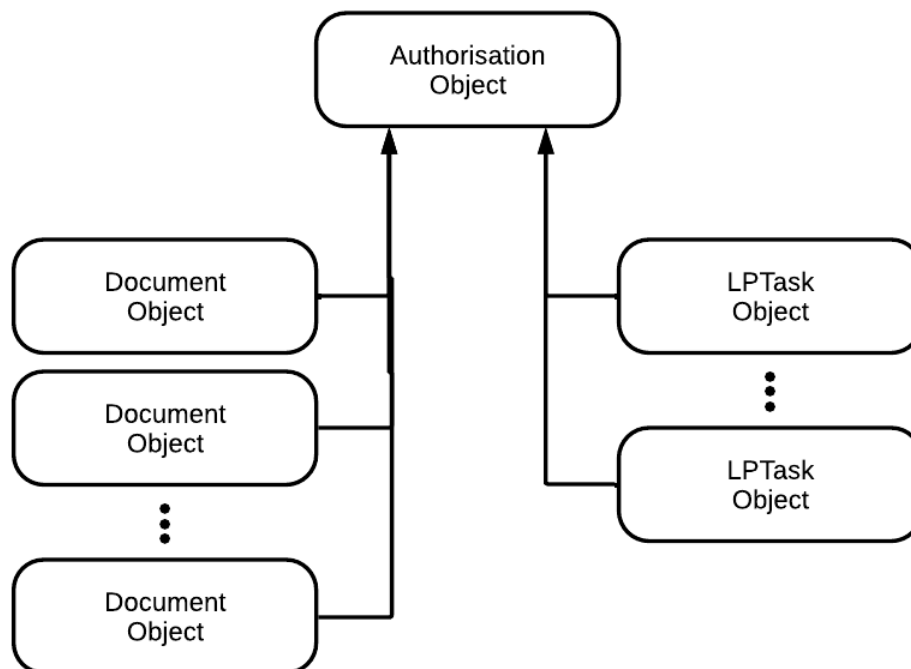


Figure H.2: Object model for the LP lifecycle workflow profile

There is a single Authorisation Object that represents the current overall state of the lawful authority covering the preservation.

There are zero or more Document Objects that represent the warrant relevant to the preservation. The net effect of the combination of these instruments and orders is represented by the Authorisation Object. Each Document Object shall be related to a single relevant Authorisation via the Document Object's AssociatedObjects field (see clause 7.1.4).

There are zero or more Task Objects that represent the instruction to preserve data relating to a particular identifier. Each LPTaskObject shall be related to a single relevant Authorisation via the LPTaskObject's AssociatedObjects field (see clause 7.1.4).

The Workflow Profile operations described in the following clauses provide mechanisms to create, maintain and terminate preservation by creating, altering and removing elements in this object model.

H.6.2.2 Common procedure

H.6.2.2.1 Overview

Unless otherwise specified, each of the Workflow Endpoints defined in clause H.6.3 follows the procedure as outlined below.

H.6.2.2.2 LEA Request

The LEA initiates the procedure by issuing a single Request Message (see clause 5) containing the verbs and objects required by the Workflow Endpoint.

H.6.2.2.3 Initial CSP Response

The CSP verifies the syntax of the request. If the request is syntactically correct and meets the requirements of the Workflow Endpoint, then it shall send a Response Message (as defined in clause 5) as a positive acknowledgement and move to clause H.6.2.2.4. In all other circumstances it shall respond with a top-level Error Response (see clause 6.3.3 and clause D.1) describing the nature of the error. Both CSP and LEA shall consider the transaction to be terminated, and no action is taken; the state of the Authorisation, Document and LPTask Objects on the CSP side remains unchanged.

H.6.2.2.4 CSP review and action

The CSP updates the state of the Authorisation, Document and Task Objects as outlined in the relevant Workflow Endpoint definition to signal that it is processing the requested changes.

The CSP follows any necessary internal procedures to review the changes requested via the Workflow endpoint. If these are successful, the CSP makes the changes requested to the Authorisation, Document and LPTask Objects as described in the Workflow Endpoint and where appropriate actions the necessary requests e.g. by starting or stopping preservation. The CSP shall issue a Notification Object (see clause 7.4) to the LEA informing them that the requested changes have been actioned. If, as a result of the changes, the status of an Authorisation, Document or LPTask Object is updated, this shall be reflected via the StatusOfAssociatedObjects structure (see clause 7.4.7).

If the CSP established that some or all of the changes cannot take place, then all the requested changes are rejected. The CSP shall revert the status of the Authorisation, Document and LPTask Objects to their original values, and issue a Notification Object (see clause 7.4) to the LEA informing them of the rejection. The NotificationDetails field (see clause 7.4) shall contain a reference to the Transaction Identifier (see clause 6.2.5) of the original Request message, and an explanation of why the changes could not be made.

H.6.2.3 Common constraints

H.6.2.3.1 Overview

Unless otherwise specified, objects provided to the Workflow Endpoints defined in clause H.6.3 shall obey the following constraints, in addition to any specified in the relevant Workflow Endpoint description.

H.6.2.3.2 Authorisation Object

No common constraints are specified.

H.6.2.3.3 LP Task Object

No common constraints are specified.

H.6.2.3.4 Document Object

Where a Document Object is provided without a DocumentBody (see clause 7.3.9) e.g. because it is necessary to transport the content of the document via other means, then the DocumentReference field (see clause 7.3.2) shall be populated such that the CSP can associate the object with the appropriate contents.

Where a Document Object is provided with a DocumentBody (see clause 7.3.9), the ContentType shall be one of the following, or any other MIME type as agreed between the CSP and LEA:

- application/pdf
- application/vnd.openxmlformats-officedocument.wordprocessingml.document
- image/png
- image/jpeg
- text/plain

If a ContentType is provided that is not on the list of acceptable MIME types for a CSP, that CSP shall reject the request as part of its initial response (see clause H.5.2.2.3).

H.6.3 New Preservation Workflow Endpoint

H.6.3.1 Description

This endpoint covers the act of serving a new Lawful Preservation request, together with supporting documentation and a set of authorised tasking instructions, on a CSP. It provides the initial set of Authorisation, Document and LPTask objects considered in the object model.

H.6.3.2 Message contents

The LEA request message shall contain the following:

- A CREATE Request for an Authorisation Object that represents the new authorisation.
- One or more CREATE Requests for LPTask Objects that represent the technical instructions for preservation.
- One or more CREATE Requests for Document Objects that represent the actual legal documents used to form the authorisation.

The relationships between the objects shall be as described in a previous clause.

H.6.3.3 Constraints on objects

None given.

H.6.4 Preservation Extension Workflow Endpoint

H.6.4.1 Description

This endpoint covers the act of extending the end date of the lawful authorisation to preserve data. It does so by modifying the AuthorisationTimespan field of the Authorisation Object, and the DesiredPreservationExpiration field of selected LPTaskObjects.

H.6.4.2 Message contents

The LEA request message shall contain the following:

- An UPDATE Request for the relevant Authorisation Object.
- Zero or more UPDATE Requests for the LPTask Objects for which the LEA wishes to extend preservation, moving the DesiredPreservationExpiration date to the new date for preservation (see note).
- Zero or more CREATE Requests for Document Objects that represent the legal documents used to authorise the extension.

The relationships between the objects shall be as described in a previous clause

NOTE: Unless otherwise agreed, the LEA is required to explicitly update the DesiredPreservationExpiration for each LPTask Object that it wishes to extend preservation for.

H.6.4.3 Constraints on objects

H.6.4.3.1 Authorisation Object

The following fields shall be present in the UPDATE request for the Authorisation Object.

Table H.6: Authorisation fields in the Extension Workflow Endpoint

Field	Description	M/C/O	Reference
AuthorisationTimespan	Shall be populated to provide the new end date of the authorisation. Only the endTime field shall be populated, and shall be later than the existing endTime value.	M	Clause 7.2.7

H.6.4.3.2 LPTask Objects

The following fields shall be present in each UPDATE request for an LPTask Object.

Table H.7: LPTaskObject fields in the Extension Workflow Endpoint

Field	Description	M/C/O	Reference
DesiredPreservationExpiration	Shall be populated to provide the new end date of the preservation. Shall be earlier than or equal to the AuthorisationTimespan endTime given in table H.6, but later than the existing value.	M	Clause 8.4.5

H.6.4.3.3 Document Objects

This workflow endpoint does not define any restrictions on the content of the Document objects. If given, they should provide sufficient information to the CSP to verify that the extension of the Authorisation and LPTask Objects is permitted.

H.6.5 Preservation Cancellation Workflow Endpoint

H.6.5.1 Description

This endpoint covers the act of terminating a preservation prior to the preservation expiration date.

H.6.5.2 Message contents

The LEA request message shall contain the following:

- An UPDATE Request for the relevant Authorisation Object to set the status to cancelled.
- Zero or more CREATE Requests for Document Objects that represent the legal documents that give effect to the cancellation.

If this workflow succeeds, then both the CSP and LEA shall consider all LPTask Objects associated with the Authorisation to be cancelled too.

H.6.5.3 Constraints on objects

H.6.5.3.1 Authorisation Object

The following fields shall be present in the UPDATE request for the Authorisation Object.

Table H.8: Authorisation fields in the Cancellation Workflow Endpoint

Field	Description	M/C/O	Reference
AuthorisationDesiredStatus	Shall be set to "Cancelled"	M	Clause 7.2.6

H.6.5.3.2 Document Objects

This workflow endpoint does not define any restrictions on the content of the Document objects. They should provide sufficient information to the CSP to verify that the cancellation of the Authorisation and LPTask Objects is required.

Annex I (normative): Signing JSON documents

I.1 Overview

This annex provides the procedures to be followed when signing or verifying the signature of a JSON-encoded HI-1 message as specified in clause 9.2.3.

The signature mechanism is based on the JSON Web Signature (JWS) with Detached Content, as described in IETF RFC 7515 [29], Appendix F. It is modified to allow the JWS header and signature to be included as part of the HI-1 message.

For signing documents two basic procedures need to be observed, which are the generation of a signature (as described in clause I.2) and the verification of a signature (as described in clause I.3).

I.2 Signing procedure

The signing procedure is as follows:

- 1) Start with JSON document containing the unsigned HI-1 Message.
- 2) Add a JSON object named "Signature" into the root HI-1 Message object, after the Payload member. The "Signature" object has a structure based on the JWS JSON Serialization object in IETF RFC 7515 [29], Section 3.2, and the following object members shall be present:
 - a) "protected": An empty string when generating the signature, the base64url protected value once signed.
 - b) "signature": An empty string when generating the signature, the JWS Signature once calculated.
- 3) Compute the JWS Protected Header from the JWS Header Parameters to use for the signing, per IETF RFC 7515 [29], Section 4. The JWS Protected Header shall contain the "alg" JWS Header Parameter. Other JWS Header Parameters may be provided as required, such as those to support the JWS Unencoded Payload option as per IETF RFC 7797 [31], Section 3.
- 4) Take the JWS Payload to be the octets of the UTF-8 encoding of the modified JSON document containing the HI-1 Message.
- 5) Compute the JWS Signing Input from the JWS Protected Header and JWS Payload, using the algorithm in IETF RFC 7515 [29], Section 5.1, and optionally IETF RFC 7797 [31], Section 5.
- 6) Compute the JWS Signature by performing the HMAC calculation on the JWS Signing Input per IETF RFC 7515 [29], Section 5.1. The JWS Signature shall use an appropriate JSON Web Algorithm (JWA) key per IETF RFC 7518 [30].
- 7) Set the values of the following members of the "Signature" JSON object that was added in step 2:
 - a) "protected": The base64url encoded JWS Protected Header from step 3.
 - b) "signature": The base64url encoded JWS Signature from step 6.

I.3 Verification procedure

The verification procedure verifies the JWS Protected Header and it verifies the JWS Signature. The verification procedure is only considered successful if both verifications succeed.

The verification procedure, which included both of these steps, is as follows:

- 1) Start with JSON document containing the signed HI-1 Message, containing the "Signature" object in the root HI-1 Message object.
- 2) Modify the values of the following members of the "Signature" JSON object:
 - a) "protected": Temporarily store the value as the encoded JWS Protected Header, and set the "protected" member to the empty string.
 - b) "signature": Temporarily store the value as the JWS Signature, and set the "signature" member to the empty string.
- 3) Decode the JWS Protected Header JSON object from the encoded JWS Protected Header from step 2)a.
- 4) Verify the JWS Protected Header is supported by the implementation, per IETF RFC 7515 [29], Section 5.2 step 5.
- 5) Take the JWS Payload to be the octets of the UTF-8 encoding of the modified JSON document containing the HI-1 Message.
- 6) Compute the JWS Signing Input from the JWS Protected Header and JWS Payload, using the algorithm in IETF RFC 7515 [29], Section 5.2 or optionally IETF RFC 7797 [31], Section 5.
- 7) Compute the JWS Signature by performing the HMAC calculation on the JWS Signing Input per IETF RFC 7515 [29], Section 5.2. The JWS Signature uses an appropriate JSON Web Algorithm (JWA) key as per IETF RFC 7518 [30].
- 8) Verify the result of step 7 matches the JWS Signature stored in step 2)b.

Implementations shall ensure that the removal of the values in step 2 does not alter any other part of the JSON document. In particular, implementers should take care that the resulting JSON document is not reformatted, and that no changes are made to the indenting or whitespace. Such changes will result in a different payload at step 5 to the one that the signer signed in clause I.2 step 4, and will therefore result in a verification failure.

I.4 Worked example

This clause gives a worked example of the signing procedure given in clause I.2.

Step 1 begins with a JSON-encoded HI-1 message taken from the "request1.json" example given in the TCLIForge repository (<https://forge.etsi.org/rep/li/schemas-definitions/-/blob/main/103.20/examples/json/request1.json>). An abbreviated version is given below:

```
{
  "Header":{ ... },
  "Payload":{ ... }
}
```

Step 2 inserts a placeholder Signature object as a root member of the JSON document. The new Signature object has the members specified in IETF RFC 7515 [29], Section 3.2 with blank values:

```
{
  "Header":{ ... },
  "Payload":{ ... },
  "Signature":{
    "protected":"","
    "signature":""
  }
}
```

Step 3 creates the JWS Protected Header based on the chosen algorithm and any other configuration.

NOTE: Implementers are encouraged to use existing JWS libraries instead of implementing their own, and as such it may be that Steps 3 through 6 are performed as part of a single library call i.e. by a function which takes the payload and signing parameters as arguments and returns the complete JWS including the JWS Protected Header and JWS signature as return values.

For simplicity, this example uses HS256 and base64-encoded payload rather than using the option described in IETF RFC 7797 [31]. This results in the following JWS Protected Header:

```
{"alg" : "HS256"}
```

Step 4 asserts that the JWS Payload is considered to be the modified HI-1 message from Step 2. No computation is required.

Step 5 computes the JWS Signing Input. Following IETF RFC 7515 [29], Section 5 for our example, this requires taking the base64url encoding of the JWS Protected Header from Step 3, the base64url encoding of the JWS Payload from Step 4, and concatenate them with a period (".") character. For our example values, this results in the following JWS Signing Input (where "..." indicated characters omitted for brevity):

```
eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.ewogICJAeGlsbnMiOiAiaHR0cDovL3V...AgICJzaWduYXR1cmUiOiAiIgowIH0KfQ
```

Step 6 computes the JWS Signature over the JWS Signing Input, following IETF RFC 7515 [29], Section 5. For our example, calculated under a secret key of "secret", this gives a value of:

```
RImkRSJkh46537Bh4LpNbkL2064jInUv0JLGeoKJ-2M
```

Step 7 uses the values from step 2 and step 6 to populate the Signature object in the root of the HI-1 message from Step 2.

```
{
  "Header":{ ... },
  "Payload":{ ... },
  "Signature":{
    "protected":"eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9",
    "signature":"RImkRSJkh46537Bh4LpNbkL2064jInUv0JLGeoKJ-2M"
  }
}
```

1.5 Implementation guidance

1.5.1 Guidance on IETF RFC 7515 and IETF RFC 7797

Implementers are encouraged to note IETF RFC 7515 [29], Appendix C on the difference between base64url encoding and base64 encoding.

Implementers are encouraged to follow the principles set out in IETF RFC 7515 [29], Appendix D on key selection.

If implementers elect to follow the options set out in IETF RFC 7797 [31], the implementation shall set the proper fields in the protected header.

1.5.2 Guidance on implementing clauses I.2 and I.3

It is not recommended to implement the procedures in IETF RFC 7515 [29] directly. Instead, where possible implementers are encouraged to leverage existing libraries to perform the procedures given in clauses I.2 and I.3. In many cases, multiple steps of the procedure may be accomplished with a single library call.

When implementing the verification procedure in clause I.3, implementers shall pay particular attention to the directions on ensuring that formatting and whitespace are not altered in step 2 of clause I.3.

Annex J (informative): Bibliography

- W3C® Recommendation 10 June 2008: "XML Signature Syntax and Processing (Second Edition)".
- IETF RFC 2822: "Internet Message Format".
- W3C® Working Group Note 11 April 2013: "XML Signature Best Practices".

Annex K (informative): Change history

Status of the present document Lawful Interception (LI); Interface for warrant information		
TC LI approval date	Version	Remarks
September 2015	1.1.1	First publication of the TS after approval by ETSI TC LI#40
		Included Change Requests agreed by ETSI TC LI#41
February 2016	1.2.1	CR001, LI(16)P41013r1 (Cat C) Tasking Delivery IP Address and Port CR002, LI(16)P41019r1 (Cat A) Initial corrections to ETSI TS 103 120 CR003, LI(16)P41021r2 (Cat B) Addition of Task IsEmergency flag
		Included Change Requests agreed by ETSI TC LI#50
February 2019	1.3.1	CR004, LI(19)P50012r1 (Cat B) CR to support 3GPP 5G work
		Included Change Requests agreed by ETSI TC LI#52
October 2019	1.4.1	CR005, LI(19)P52032r1 (Cat B) Support for Lawful Disclosure in ETSI TS 103 120
		Included Change Requests agreed by ETSI TC LI#53
February 2020	1.5.1	CR006, LI(20)P53030r3 (Cat B) Native XML Delivery CR007, LI(20)P53031r4 (Cat B) Making DELIVER Verb consistent CR008, LI(20)P53029 (Cat F) Minor editorial changes to ETSI TS 103 120
		Included Change Requests agreed by ETSI TC LI#54e
June 2020	1.6.1	CR009, LI(20)P54013r1 (Cat F) Fixing Object Dictionary CR010, LI(20)P54015 (Cat F) Fixing Specification Dictionary CR011, LI(20)P54027r1 (Cat B) Adding Non-Local Identifier
		Included Change Requests agreed by ETSI TC LI#55e
October 2020	1.7.1	CR012, LI(20)P55017 (Cat F) Multiple Approval Details
		Included Change Requests agreed by ETSI TC LI#56e
February 2021	1.8.1	CR013, LI(21)P56021r1 (Cat F) Reference to Approval Details corrected CR014, LI(21)P56036r3 (Cat F) Correction of dictionary entries and names, references and corresponding XML files
		Included Change Requests agreed by ETSI TC LI#57e
June 2021	1.9.1	CR015, LI(21)P57016 (Cat B) Addition of InternationalizedEmailAddress type CR016, LI(21)P57019 (Cat F) Correction of normative references in scope CR017, LI(21)P57026r1 (Cat B) Namespace of signature element
		Included Change Requests agreed by ETSI TC LI#58e
October 2021	1.10.1	CR018, LI(21)P58037r2 (Cat B) Extension of ApproverDetails CR019, LI(21)P58038r2 (Cat B) Extension of RequestDetails CR020, LI(21)P58039r1 (Cat B) Extension of DeliveryAddress CR021, LI(21)P58041r1 (Cat C) Aligning use of Invalid/StatusReason fields
		Included Change Request agreed by ETSI TC LI#59e
February 2022	1.11.1	CR022, LI(22)P59029r2 (Cat B) Support for additional checksum types CR023, LI(22)P59030r2 (Cat B) Addition of EUI64, CGI, ECGI, NCGI and ICCID to annex C
May 2022	1.11.2	Revision for an editorial update to the attachments.
		Included Change Requests agreed by ETSI TC LI#61
November 2022	1.12.1	CR027, LI(22)P61019r3 (Cat B) Additional fields from discussion CR028, LI(22)P61020r4 (Cat B) Additional profile CR029, LI(22)P61009r4 (Cat B) Traffic Policy Object feature addition to ETSI TS 103 120

Status of the present document		
Lawful Interception (LI); Interface for warrant information		
TC LI approval date	Version	Remarks
March 2023	1.13.1	<p>Included Change Requests agreed by ETSI TCLI#62</p> <p>CR033, LI(23)P62029r5 (Cat B) Traffic Policy Object feature addition to ETSI TS 103 120 CR034, LI(23)P62023r3 (Cat B) Status changes in notifications CR035, LI(23)P62024r2 (Cat B) Adding notifications to the simple profile CR036, LI(23)P62025r4 (Cat B) Introducing data categories from the European production and preservation order CR037, LI(23)P62012r1 (Cat B) Additional DeliveryAddress Value CR038, LI(23)P62013r5 (Cat C) AuthorisationTypeOfCase Dictionary Values CR039, LI(23)P62022r3 (Cat B) Multi-endpoint Workflow Profile CR040, LI(23)P62034r3 (Cat F) DELIVER Request Clarification – 120 CR041, LI(23)P62035r3 (Cat F) AuthorisationObject Reference Update - 120</p>
June 2023	1.14.1	<p>Included Change Requests agreed by ETSI TCLI#63</p> <p>CR042, LI(23)P63009r1 (Cat B) Addition of ETSI TS 103 707 to the ManifestSpecification Dictionary CR043, LI(23)P63036r2 (Cat B) Including link to preservation request CR044, LI(23)P63035r3 (Cat B) Workflow Profile for LI CR045, LI(23)P63034r2 (Cat B) JSON encoding CR046, LI(23)P63032r3 (Cat C) Refactoring Traffic Policies CR047, LI(23)P63029r1 (Cat C) Specify linking of objects in the simple workflow profile CR049, LI(23)P63040r3 (Cat B) LPTask Object CR050, LI(23)P63042r2 (Cat F) LDTask Status Dictionaries Corrections</p>
December 2023	1.15.1	<p>Included Change Requests agreed by ETSI TCLI#64</p> <p>CR052, LI(23)P64013r2 (Cat B) Signing JSON documents CR053, LI(23)P64014r1 (Cat B) Transporting JSON CR054, LI(23)P64027r3 (Cat B) Traffic Policy for Ethernet data flows CR055, LI(23)P64011r4 (Cat B) Traffic Policy for RCS services CR056, LI(23)P64030r1 (Cat C) Optimizing DeliveryObject CR057, LI(23)P64035r2 (Cat B) Workflow Profile for LPTask</p>
February 2024	1.16.1	<p>Included Change Requests agreed by ETSI TCLI#65</p> <p>CR058, LI(24)P65015r5 (Cat B) Traffic Policy for Truncating Data Packets CR059, LI(24)P65021 (Cat B) Changes to support publication of ETSI TS 103 976 CR060, LI(24)P65019r1 (Cat C) Standard Endpoint Paths for LI Workflow Profile CR061, LI(24)P65024r1 (Cat C) Introduction of the format name ServiceAccessIdentifier CR062, LI(24)P65025r1 (Cat B) Adding error codes for technical errors CR063, LI(24)P65026r3 (Cat B) Adding the additional format name InternationalE164</p>
June 2024	1.17.1	<p>Included Change Requests agreed by ETSI TCLI#66</p> <p>CR065, LI(24)P66007 (Cat C) Default LP Workflow Endpoints CR066, LI(24)P66008 (Cat F) AuthorisationLegalEntity Correction CR067, LI(24)P66009r2 (Cat B) Capability Discovery CR068, LI(24)P66013r1 (Cat B) Addition of the eUICC identifier (EID) CR069, LI(24)P66022r1 (Cat F) Adding \$schema keyword to JSON schema CR070, LI(24)P66030r5 (Cat C) Improving Target Identification CR071, LI(24)P66024r3 (Cat B) Adding TS 103 707 for LI handover CR072, LI(24)P66029r1 (Cat F) AuthorisationManualInformation Correction CR073, LI(24)P66038r2 (Cat B) Addition of ETSI TS 103 705 to the HandoverFormat and the ManifestSpecification</p>

History

Document history		
V1.1.1	January 2016	Publication
V1.2.1	March 2016	Publication
V1.3.1	May 2019	Publication
V1.4.1	December 2019	Publication
V1.5.1	March 2020	Publication
V1.6.1	August 2020	Publication
V1.7.1	October 2020	Publication
V1.8.1	March 2021	Publication
V1.9.1	July 2021	Publication
V1.10.1	December 2021	Publication
V1.11.1	March 2022	Publication
V1.11.2	May 2022	Publication
V1.12.1	December 2022	Publication
V1.13.1	March 2023	Publication
V1.14.1	August 2023	Publication
V1.15.1	January 2024	Publication
V1.16.1	April 2024	Publication
V1.17.1	August 2024	Publication