EUROPEAN COMMISSION
DIRECTORATE-GENERAL FOR HEALTH AND FOOD SAFETY

General Affairs
Information systems

eHealth DSI
Patient Summary and ePrescription

Audit Trail Profiles

DOCUMENT VERSION 2.2.0

DATE 08/06/2018

STATUS Wave 2 Operation ready

COVER AND CONTROL PAGE OF DOCUMENT	
Document old name:	epSOS Architecture and Design EED DESIGN – epSOS Audit Trail Profiles
Document name:	Audit Trail Profiles
Distribution level*:	PU
Status:	Wave 1 Operation ready
Author(s): Organization:	eHealth DSI provider

* Distribution level: PU = Public, PP = Restricted to other programme participants, RE = Restricted to a group specified by the consortium, CO = Confidential, only for members of the consortium.

ABSTRACT
This normative binding specifies the capture of auditable events within any eHealth DSI service invocation, as well as NCP-internal functionality.

CHANGE HISTORY				
Version	Date	Status Changes	From	Review
V1.1	15/09/2015	Publish	Fraunhofer FOKUS	
V2.0.0	28/03/2017	Remove all references to epSOS and requirements	eHealth DSI provider	
V2.0.1	21/04/2017	Integrate the modifications linked to the CP-002	eHealth DSI provider	
V2.0.2	27/04/2017	Integrate the modifications linked to the CP-001 (Evidence emitter)	eHealth DSI provider	
V2.0.3	04/05/2017	Integrate the Non repudiation Evidence	eHealth DSI provider	
V2.1.0	01/06/2017	Released for eHMSEG adoption	eHealth DSI Solution Provider	
V2.2.0	08/06/2018	Wave 2 Operation Ready	eHealth DSI Solution Provider	

TABLE OF CONTENTS

1 Introduction

This normative binding specifies the capture of auditable events within any eHealth DSI service invocation, as well as NCP-internal functionality.

1.1 eHealth DSI Audit Trail

The protection of patient privacy and the integrated implementation of adequate security measures are fundamental foundations of the eHealth DSI architecture and design. Therefore a holistic network of security services is required for serving eHealth DSI requirements on privacy and security. Among these services ~~– as specified in [Interoperability Specification] –~~ is an Audit Trail, where all events related to the processing of identity data and medical data are logged. ~~While [Interoperability Specification] only specifies the core requirements and logical outline of the eHealth DSI Audit Trail,~~ this specification provides a binding of that logical outline to the [RFC 3881] standard which is well established for logging auditable events in health IT.

The eHealth DSI Audit Trail specification consists of three parts:

- Chapter 2 specifies the contents and structure of the eHealth DSI audit trail. This specification is normative and each eHealth DSI NCP implementation MUST generate an audit trail that captures the specified contents. This specification does not define a normative format for generating and storing the audit trail but requires that each implementation is able to transform the audited data to the format and coding as specified in this document.

- Chapter 3 imposes constraints in eHealth DSI audit trail implementation and operation which MUST be followed by each NCP in order to respect the eHealth DSI required level of security and privacy. These constraints are normative and verifications on proper implementation MUST be part of the eHealth DSI projectathon testing and security auditing.

- While eHealth DSI services can trigger the writing of an audit trail, it is the responsibility of an Audit Trail Repository to accept and store single audit trail entries and to provide functionalities for their designated use (e.g. assessment of privacy-aware operation). As such a repository does not affect interoperability within the eHealth DSI NCP-to-NCP zone, the transactions for writing audit trail entries into the Audit Trail repositories are out of the eHealth DSI scope. However, for preserving a common level of trust among all NCPs, several security considerations related to the audit trail processing environment and the applied security measures need to be followed. These are specified in section 3 of this document.

1.2 ETSI REM

ETSI Registered Electronic Mail, REM, (ETSI, 2011) provides an architectural approach to achieve interoperability, and for defining additional security services, when exchanging Electronic mail for business and administration. REM is an enhanced form of mail transmitted by electronic means (email), which provides evidence relating to the handling of an email, including proof of submission and delivery. Evidence is a set of signed data created within a specific context, which proves that a certain event has occurred at a certain time.

1.2.1 Why ETSI REM in eHealth

Although ETSI REM architecture is made for the asynchronous communication model of the email, the REM set of evidence is the de-facto standard used by

industry and public administrations implementing the ISO 13888 regulatory framework. In fact, the adoption of ETSI REM provides:

- Interoperability with other sectors of the European Digital Agenda
- Compliance with ISO 13888
- Schema-driven implementation (e.g., JAXB)

1.2.2 Evidence structure

The message is *delivered* from actor to actor, and for this event the framework produces the following evidence: the *SubmissionAcceptanceRejection (SAR)* (REM, Section 5.1.1), and the *AcceptanceRejectionByRecipient (ARbR)* (REM, Section 5.1.7). SAR is acting as an NRO token, while ARbR is acting as NRR token.
The purpose of the SAR is to prove that a certain message was/was not successfully submitted, at the time indicated in the evidence, to the authenticated sender. The purpose of the ARbR is to prove that the given message was accepted by the recipient or by a delegate.
If the couple (SAR, ARbR) can be chained from the first actor sending the message to the last one receiving, the evidence of *submission* can be constructed[1].
The SAR and ARbR tokens follow ISO 13888 standard as NRO and NRR, respectively. ISO 13888 defines the NRO token as:

$$\text{NRO}=text1||z1||Sa(z1),$$

where *Sa(z1)* is the signature of

$$z1 = Pol||fNRO||A||B||TTP||T||Tsent||Q||SHA(m).$$

Pol is a policy governing non-repudiation in this context, *TTP* is the trusted third party, *Tissue* and *Tsent* are the timestamps, *Q* additional elements, and *m* the message. *Text1* is part of the message. *A* is the sender, and *B* is the recipient. fNRO is the type of token.

$$\text{NRR}=text2||z2||Sb(z2)$$

where $z2 = Pol||fNRR||A||B||TTP||Tissue||Treceived||Q||SHA(m)$.
The structure of the REM evidence follows the NRO, and NRR token definition as above. The REM evidence implementation used MUST be XML.
For this exchange, the value of the PolicyID is set to: "urn:oid:epsos:nonrepudiation:policyid:1".

Non-Repudiation of Origin

The NRO is implemented as REM *SubmissionAcceptanceRejection (SAR)* as defined in (ETSI, Section 5.1.1). The value of the fields is here described.

Token Element	Optionality	Usage Convention
@Version	R	It MUST be "2"
EventCode	R	"Acceptance" if the message has been successfully delivered, "Rejection" otherwise.
EvidenceIdentifier	R	It MUST be an UNIQUE identifier for the evidence, in the form of UUID
EvidenceIssuerPolicyID		
PolicyID	R	The distinguishing identifier of the non-repudiation policy (or policies), which apply to the evidence. It MUST be in the form of OID.
EvidenceIssuerDetails		
CertificateDetails		
X509Certificate	R	The Base64-encoded certificate of the issuer of the REM evidence. In case of NCPs this MUST be the TLS certificate.
SenderAuthenticationDetails		
AuthenticationTime	O	Since the authentication of the sender is made by establishing the TLS handshake, this

[1] This fact leds to the Weak Fairness property of the Non Repudiation protocol

			value MAY be omitted. However to achieve compliance with the ETSI REM schema, the current time is placed.
	AuthenticationMethod	R	It MUST be "http:uri.etsi.org/REM/AuthMethod#Strong", the client is authenticated using TLS.
EventTime		R	This value MUST be the time of the evidence created. In the workflow this is evaluated by the Evidence Emitter (strict synchronization with the message sent)
SubmissionTime		R	This value MUST be the time when the message is sent.
SenderDetails			
	CertificateDetails		
	X509Certificate	R	This is the Base64-encoded value of the sender's certificate (e.g., "my" certificate). It usually is the certificate of the actor. For the NCP it MUST be the TLS certificate.
RecipientDetails			
	CertificateDetails		
	X509Certificate	R	This is the Base64-encoded value of the recipient's certificate. For NCP-B it MUST be the certificate of NCP-A and vice versa
SenderMessageDetails			
	@isNotification	R	MUST be "false"
	MessageSubject	R	This value represents the epSOS-encoded message type (e.g., epSOS-31)
	UAMessageIdentifier	R	This value MUST be the WS-Addressing Message UUID.
	MessageIdentifierByREMMD	R	This value MUST be the same of UAMessageIdentifier
	DigestMethod @Algorithm	R	It MUST be "SHA256"
	DigestValue	R	This is the digest value of the whole message, with the algorithm defined DigestMethod/@Algorithm. The digest value MUST be evaluated as follows: • Over the canonicalized XML of the SOAP envelope (the algorithm http://www.w3.org/TR/2001/REC-xml-c14n-20010315 MUST be used). • Over the attachments as byte array
Signature		R	This is the XMLDSG field of the Evidence. It MUST • Be signed using the actor identity • Contain the certificate Base64-encoded as KeyInfo/KeyData/X509Certificate

The ISO 13888 token is mapped in the following table. The source of the token can be either loaded from the Obligation or from the transaction Context.

ISO 13888	**ETSI REM SAR**	**Obligation / Context**
PoI	*EvidenceIssuerPolicyID*	Obligation
A	*SenderDetails*	Context
B	*RecipientDetails*	Context
TTP	*EvidenceIssuerDetails*	Context / Obligation
T_{issue}	*EventTime*	Context
T_{sent}	*SubmissionTime*	Context
fNRO	*SubmissionAcceptanceByRecipient*	Context

Non-Repudiation of Receipt

The NRO is implemented as REM *AcceptanceRejectionByRecipient (ARbR)* as defined in (ETSI, Section 5.1.7). The value of the fields is here described. It is worth noticing that the values are almost the same of the *SAR*, but mirrored (ARbR is the "receiving" part).

Token Element	Optionality	Usage Convention
@Version	R	It MUST be "1"
EventCode	R	"Acceptance" if the message has been successfully delivered, "Rejection" otherwise.
EvidenceIdentifier	R	It MUST be an UNIQUE identifier for the evidence, in the form of UUID
EvidenceIssuerPolicyID		
PolicyID	R	The distinguishing identifier of the non-repudiation policy (or policies), which apply to the evidence. It MUST be in the form of OID.
EvidenceIssuerDetails		
CertificateDetails		
X509Certificate	R	The Base64-encoded certificate of the issuer of the REM evidence. In case of NCPs this MUST be the TLS certificate.
SenderAuthenticationDetails		
AuthenticationTime	O	Since the authentication of the sender is made by establishing the TLS handshake, this value MAY be omitted. However to achieve compliance with the ETSI REM schema, the current time is placed.
AuthenticationMethod	R	It MUST be "http:uri.etsi.org/REM/AuthMethod#Strong", the client is authenticated using TLS.
EventTime	R	This value MUST be the time of the evidence created. In the workflow this is evaluated by the Evidence Emitter (strict synchronization with the message sent)
SubmissionTime	R	This value MUST be the time when the message is sent.
SenderDetails		
CertificateDetails		
X509Certificate	R	This is the Base64-encoded value of the sender's certificate. It usually is the certificate of the actor. For the NCP it MUST be the TLS certificate.
RecipientDetails		
CertificateDetails		
X509Certificate	R	This is the Base64-encoded value of the recipient's certificate (e.g., "my" certificate"). For NCP-B it MUST be the certificate of NCP-A and vice versa
SenderMessageDetails		
@isNotification	R	MUST be "false"
MessageSubject	R	This value represents the epSOS-encoded message type (e.g., epSOS-31)
UAMessageIdentifier	R	This value MUST be the WS-Addressing Message UUID.
MessageIdentifierByREMMD	R	This value MUST be the same of UAMessageIdentifier.
DigestMethod @Algorithm	R	It MUST be "SHA256"
DigestValue	R	This is the digest value of the whole message, with the algorithm defined DigestMethod/@Algorithm. The digest value MUST be evaluated as follows: • Over the canonicalized XML of the SOAP envelope (the algorithm http://www.w3.org/TR/2001/REC-xml-c14n-20010315 MUST be used).

			• Over the attachments as byte array
Signature		R	This is the XMLDSG field of the Evidence. It MUST • Be signed using the actor identity • Contain the certificate Base64-encoded as KeyInfo/KeyData/X509Certificate

The ISO 13888 token is mapped in the following table. The source of the token can be either loaded from the Obligation or from the transaction Context.

ISO 13888	ETSI REM SAR	Obligation / Context
PoI	*EvidenceIssuerPolicyID*	Obligation
A	*SenderDetails*	Context
B	*RecipientDetails*	Context
TTP	*EvidenceIssuerDetails*	Context / Obligation
T_{issue}	*EventTime*	Context
T_{sent}	*SubmissionTime*	Context

1.2.3 Flow of events

The evidence messages are triggered immediately after the execution of an event, in order to keep timeliness with the message flows.

Flow from NatInfrB to NatInfrA

- National Infrastructure B MAY issue the SAR token
- The message is received by NCPeH-B, which MUST issue a ARbR token
- NCPeH-B performs internal operations
- NCPeH-B MUST issue a SAR token when the message is sent
- All the tokens MAY be stored in the Evidence Recording Service
- NCPeH-A receives the message, and it MUST issue a ARbR token
- NCPeH-A performs internal operations
- NCPeH-A MUST issue a SAR token before sending the new message to the national infrastructure
- National Infrastructure A MAY issue a ARbR token

A mirrored flow is valid for vice versa operations (e.g., dispensations).

1.3 Related Documents

The integration of the eHealth DSI Audit Trail into the overall eHealth DSI Security Framework is defined in [Interoperability Specification] which is the normative foundation for all binding specifications. eHealth DSI countries' implementation of the audit trail technical components MUST make use of several security mechanisms and objects in order to fulfil the eHealth DSI security requirements on secure and privacy aware audit trails (see chapter 4). All cryptographic mechanisms and objects used for safeguarding eHealth DSI audit trails MUST provide a level of technical security that MUST NOT be lower than the security level implemented through the normative eHealth DSI algorithm catalogue provided in [Cryptographic Algorithms].

1.4 Conventions

The keywords MUST, SHOULD, MAY, SHOULD NOT and MUST NOT are used as defined in [RFC 2119].

eHealth DSI requirements are managed within a central requirements management tool and serialized into [Requirements and Recommendations]. For references to requirements, always use the identifiers as used with the central requirements.

Newly defined requirements are handed over to the central requirements management. In case of doubt or conflict, [Requirements and Recommendations] MUST be considered to be the normative phrasing of a requirement.

1.5 Terms and Definitions

The country which holds information about a patient, where the patient can be univocally identified and where his data may be accessed is called “country-A” (country of affiliation) [eHealth DSI Glossary]. The country of treatment where cross-border health care is provided when the patient is seeking care abroad is called “country-B” (country of care) [eHealth DSI Glossary].
The term “Healthcare Professional (HP)” denotes a doctor of medicine, a nurse responsible for general care, a dental practitioner, a midwife or a pharmacist within the meaning of Directive 2005/36/EC, or another professional exercising activities in the healthcare sector which are restricted to a regulated profession as defined in Article 3(1)(a) of Directive 2005/36/EC, or a person considered to be a health professional according to the legislation of the country of treatment [eHealth DSI Glossary]. Health professionals are allowed to process medical patient data according to the legislation of the country of the health professional’s residence. An “eHealth DSI Point of Care (PoC)” is a location where an eHealth DSI patient may seek healthcare services [eHealth DSI Glossary].
A “National Contact Point (NCP)” is an entity in each particular country to act as a bidirectional technical, organizational and legal interface between the existing national functions and infrastructures [eHealth DSI Glossary]. In this document the term “NCP” emphasizes the technical aspects of this interface and as such refers to a gateway which facilitates various aspects of cross-border data sharing (e.g. message forwarding, signature verification). From an architectural perspective NCPs denote the boundary between the eHealth DSI infrastructure and a country’s existing national eHealth infrastructure (see [Interoperability Specification] for details).

1.6 Status of this Binding

The binding as defined in this document is a normative binding. All eHealth DSI countries MUST implement this binding within their NCP.
Other eHealth DSI documents must refer to this binding as [Audit Trail Profiles]. Unless a version number is given, references to [Audit Trail Profiles] always refer to the most current version that is published on the eHealth DSI website.
Additional or alternative bindings for logging auditable events MUST NOT be defined and implemented for the eHealth DSI.

2 eHealth DSI Audit Trail Contents and Structure

2.1 Referenced Standards

The eHealth DSI Audit Trail specification builds upon the following set of standards and profiles:

- RFC3881: Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications [RFC 3881]

Regarding the concrete use of [RFC 3881] eHealth DSI relies on the codes and mechanisms from:

- DICOM Supplement 95: Audit Trail Messages [DICOM Sup 95]
- [ASTM E2147-01]
- IHE ATNA: IHE IT Infrastructure Technical Framework – Audit Trail and Node Authentication Profile [IHE ITI TF-2a]

Wherever possible, the eHealth DSI Audit Trail encodings make use of their original counterparts of the IHE transactions as laid out within such transaction profiles [IHE ITI-2a, IHE ITI TF-2b]. However, due to specific shortcomings regarding integrity and

non-repudiation safeguards, the eHealth DSI Audit Trail is extending the original provisions whenever required.
Following the conventions of IHE, coded values within audit trail entries are restricted to the attributes "`@code`", "`@codeSystemName`" and "`@displayName`" and denoted as EV(code, codeSystemName, displayName).

2.2 RFC 3881 Overview and eHealth DSI Audit Schemas

Every HP Identity Assertion MUST be signed by its issuer (i.e., the NCP-B). The XML signature MUST be applied by using the *saml:Assertion/ds:Signature* element as defined in [Cryptographic Algorithms].
The RFC 3881:
"… defines the format of the data to be collected and minimum set of attributes that need to be captured by healthcare application systems for subsequent use by an automation-assisted review application. The data includes records of who accessed healthcare data, when, for what action, from where, and which patients' records were involved. The data definition is an XML schema to be used as a reference by healthcare standards developers and application designers." [RFC3881]
The standard defines five categories that are subject to audit activity, as shown in Figure 2, and detailed in the following table:

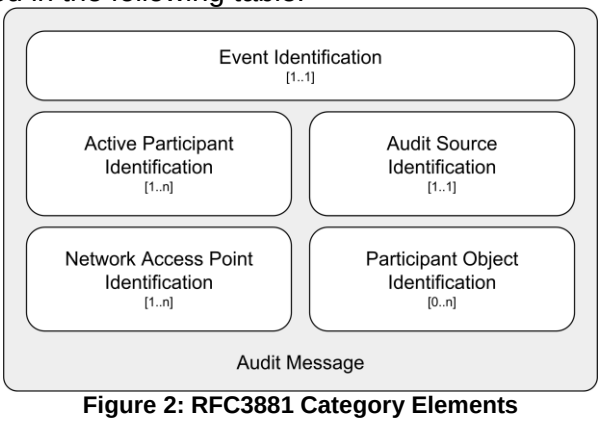

Figure 2: RFC3881 Category Elements

RFC3881 Category	Description[2]
Event Identification	What was done? "*The following data identifies the name, action type, time, and disposition of the audited event. There is only one set of event identification data per audited event*"
Active Participant Identification	By whom? "*The following data identify a user for the purpose of documenting accountability for the audited event. A user may be a person, or a hardware device or software process for events that are not initiated by a person.*"
Audit Source Identification	Using which server? "*Identifier of the source where the event originated.*"
Network Access Point Identification	Initiated from where? "*The network access point identifies the logical network location for application activity. These data are paired 1:1 with the Active Participant Identification data.*"
Participant Object Identification	To what resource (patient, record, etc.)? "*The following data assist the auditing process by indicating specific instances of data or objects that have been accessed.*"

[2] taken from RFC3881

Within eHealth DSI, all Audit Trail schemata are aligned to the categories as outlined above. eHealth DSI specifies two mandatory Audit Trail schemata and one optional in case that patient mapping mechanisms are used that require further protection (see figure 3).

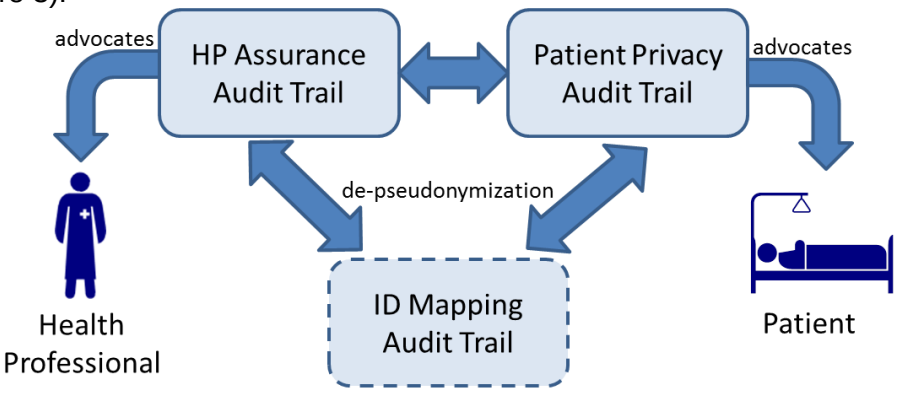

Figure 3: eHealth DSI Audit Trail Schemata

The following table shows how these advocating roles apply to the concrete eHealth DSI audit trail schemas.

Schema	Provided By	Description
HP Assurance	Service Consumer (country B)	The HP Assurance audit schema is used by the service consumer at the country of care and written in that country. The main purpose of this audit trail is to document all actions of this country's HPs in order to protect them against false accusations for not properly using the features of eHealth DSI (e. g. a patient claiming that a HP did not access his data even though he authorised him to do so).
Patient Privacy	Service Provider (country A)	The Patient Privacy audit schema is used by the service provider at the patient's CoA and written in this country. The primary objective of this audit is to document the responsibilities the data controller has regarding the rights of the data subject and the proper execution of such duties. Consequently, this audit trail is also used to enable the patient to get knowledge on all usages of his medical data. By analysing this audit trail the patient is able to evaluate the legitimacy of all accesses to his data.
Patient ID Mapping (OPTIONAL)	Service Provider (country A)	During patient identification the identifier provided by the patient is mapped onto a patient identifier that is to be used for subsequent calls. The patient ID mapping audit schema MAY be written to a log file that is separated from the Patient Privacy Audit Log in cases where a country makes use of pseudonyms (by separating the logs the Patient Privacy Audit trail is pseudonymous while the Patient ID Audit trail can be used for resolving pseudonyms for further privacy assessments).

Table 1: eHealth DSI Audit Trail Schemata

Each schema is used to write a separate Audit Trail. Whenever the optional Patient ID Mapping Audit Trail Schema is used, it SHOULD be written and stored within a separate system to avoid disclosure of the patient ID mapping in sensitive patient ID issuing authorities or pseudonymisation environments. A linkage of audit trails that are written by different NCPs in different countries MUST comply with the respective eHealth DSI security regulations, communities, and service level agreements.
The payload of each auditable event (written as of RFC 3881 as a whole) MUST be safeguarded by a payload signature that is protecting the integrity and originator authenticity of each individual auditable event. NCPs writing audit trail entries SHALL use the NCP Signature for this purpose (see [X.509 Certificate Profiles] for the respective certificate schema).

2.3 eHealth DSI Audit Schema Instances

The following chapter presents the instances of the eHealth DSI Audit Schemata that MUST be applied to all eHealth DSI operations as specified.

2.3.1 eHealth DSI HP Assurance Audit Schema

The HP Assurance Audit schema consists of the following subcategories of the original categories as defined by RFC 3881:

RFC 3881 Category	eHealth DSI Object/Subject	Description
Event	Event	Audited event according to [RFC 3881]
Active Participant	Requesting Point of Care	Point of Care that is the origin of the event
	Human Requestor	HP who triggered the event
	Service Consumer NCP	Service consumer NCP that triggered the event
	Service Provider NCP	Destination of the event
Audit Source	Audit Source	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants.
Participant Object	Patient	Patient whose data is affected from the event
	Event Target	Target resource of the event
	Error Message	**Optional:** Information on errors that occurred during transaction processing

Entries according to this schema MUST only be written after receipt of the response to the transaction that is target to auditing.

In the following sections the required (R) and optional (O) fields of these categories are listed. Fields not listed here but defined in [RFC 3881] MAY be defined by the operator of the service consumer nodes or by the NCP of the country of care. In cases where audit trail entries are exchanged between NCPs, these fields SHOULD be blanked.

2.3.1.1 Event Identification

Field Name	Opt.	Value Constraints
EventID	R	MUST be set to EV(num, “IHE Transactions”, name) where num is the number of the transaction including the “ITI-“ prefix and name is set to the transaction name as specified in ITI TF-2. Example for XCA: EV(“ITI-38”, “IHE Transactions”, “Cross Gateway Query”). See ITI TF-2a: 3.18.5.1.2. MUST be set to EV(*num*, “eHealth DSI Transaction”, *name*) where *num* is the number of the transaction including the “epSOS-“ prefix and *name* is the name of the transaction as written in the respective Use Case Roles diagram. See section 2.3.5.7 for a full list of all EventIDs defined for eHealth DSI.
EventActionCode	R	Acc. RFC 3881. See section 2.3.5.7 for a mapping of EventIDs and EventActionCodes.
EventDateTime	R	Acc. RFC 3881. Time MUST be provided by a node that is grouped with a Consistent Time Consumer Actor.
EventOutcomeIndicator	R	Acc. RFC 3881. MUST be “0” on full success, “1” in case of a partial delivery, “4” for temporal or recoverable failures, and “8” for permanent failures.

2.3.1.2 Active Participant Identification: Point of Care

Field Name	Opt.	Value Constraints
UserID	R	Identifier of the point of care that initiated the event. This field MUST contain the name of the point of care as provided by the HP Identity Assertion (see [SAML Profile]).
UserIsRequestor	R	“true”
RoleIDCode	R	RFC 3881 compliant encoding of the kind of HCPO as defined in the “HCPO Type” attribute of the Authentication Assertion that was issued for the user.

2.3.1.3 Active Participant Identification: Human Requestor

Field Name	Opt.	Value Constraints
UserID	R	Identifier of the HP who initiated the event. This field MUST contain the name identifier as given in the respective element of the Authentication Assertion that was issued for this user. See section 2.3.5.9 for the mandatory encoding scheme for user identifiers.
AlternativeUserID	R	Human readable name of the HP as given in the XSPA Subject-ID attribute of the HP identity assertion (see [SAML Profile]).
AlternativeUserID	O	UUID of the original Authentication Assertion that was issued for this user. This field SHOULD only be used if the issued eHealth DSI Authentication Assertion is an attest for an Assertion that was issued by the national infrastructure. In this scenario the UUID might be useful to univocally link these two assertions.
UserIsRequestor	R	"true"
RoleIDCode	R	RFC 3881 compliant encoding of the user's role as defined in the "role" attribute of the Identity Assertion that was issued for this user.

2.3.1.4 Active Participant Identification: Service Consumer NCP

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded CN of the TLS certificate of the NCP that triggered the eHealth DSI operation that corresponds to the event
UserIsRequestor	R	"true"
RoleIDCode	R	Coded value for "eHealth DSI Service Consumer"

2.3.1.5 Active Participant Identification: Service Provider NCP

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded CN of the TLS certificate of the NCP that processed the eHealth DSI operation that corresponds to the event
UserIsRequestor	R	"false"
RoleIDCode	R	Coded value for "eHealth DSI Service Provider"

2.3.1.6 Audit Source

Field Name	Opt.	Value Constraints
AuditSourceID	R	Identifies the authority that is legally responsible for the audit source. In the case of eHealth DSI this element MUST provide the ISO 3166-2 code of the country/region where the audit source is located OR the specific OID of the entity authenticating and vouching for this auditable event.

2.3.1.7 Participant Object: Patient

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "1" (Person)
ParticipantObjectTypeCodeRole	R	MUST be "1" (Patient)
ParticipantObjectIDTypeCode	R	EV(2, RFC-3881, "Patient Number")
ParticipantObjectID	R	Patient identifier encoded in HL7v2 CX format. Only the patient identifier that is issued during the patient identification handshake MUST be used for this field.

2.3.1.8 Participant Object: Error Message

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be "2" (System Object)
ParticipantObjectTypeCodeRole	R	MUST be "3" (Report)
ParticipantObjectIDTypeCode	R	MUST be "9" (Report Number)
ParticipantObjectID	R	String-encoded error code that was included with the response message.
ParticipantObjectDetail	R	Error message as included with the response message as

		a type-value pair acc to [RFC 3881]. As a type qualifier “errormsg” MUST be used. The value MUST contain the base64 encoded error message.

A single error message section MUST be given for each error code/message that is included with a response message.

2.3.1.9 Participant Object: Event Target

This subcategory MUST be defined individually for each transaction.

2.3.2 eHealth DSI Patient Privacy Audit Schema

The Patient Privacy Audit schema consists of the following subcategories of the original categories as defined by RFC 3881.

RFC 3881 Category	eHealth DSI Instance	Description
Event	Event	Audited event according to [RFC 3881]
Active Participant	Human Requestor	HP who triggered the event
	Service Consumer NCP	Service consumer NCP that triggered the event
	Service Provider NCP	Destination of the event
Audit Source	Audit Source	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Participant Object	Patient	Patient whose data is affected from the event
	Event Target	Target of the event
	Error Message	Optional: Information on errors that occurred during transaction processing

Entries according to this schema MUST only be written after the response to the transaction that is target to auditing has been successfully transmitted to the requesting gateway.

2.3.2.1 Event Identification

Field Name	Opt.	Value Constraints
EventID	R	MUST be set to EV(*num*, “epSOS Transaction”, *name*) where *num* is the number of the transaction including the “epSOS-“ prefix and *name* is the name of the transaction as written in the respective Use Case Roles diagram. See section 2.5.3.7 for a full list of all eventIDs defined for eHealth DSI.
EventActionCode	R	Acc. RFC 3881. See section 2.5.3.7 for a mapping of EventIDs and EventActionCodes.
EventDateTime	R	Acc. RFC 3881. Time MUST be provided by a node that is grouped with a Consistent Time Consumer Actor.
EventOutcomeIndicator	R	Acc. RFC 3881. MUST be “0” on full success, “1” in case of a partial delivery, “4” for temporal or recoverable failures, and “8” for permanent failures.

2.3.2.2 Active Participant Identification: Human Requestor

Field Name	Opt.	Value Constraints
UserID	R	Identifier of the HP who initiated the event. This field MUST contain the name identifier as given in the respective element of the Authentication Assertion that was issued for this user. See section 2.5.3.9 for the mandatory encoding scheme for user identifiers.
AlternativeUserID	R	Human readable name of the HP as given in the Subject-ID attribute of the HP identity assertion (see [SAML Profile]).
UserIsRequestor	R	“true”
RoleIDCode	R	RFC 3881 compliant encoding of the user’s role as defined in the “role” attribute of the Identity Assertion that was issued for this user.

2.3.2.3 Active Participant Identification: Service Consumer NCP

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded CN of the TLS

		certificate of the NCP that triggered the eHealth DSI operation that corresponds to the event
UserIsRequestor	R	“true”
RoleIDCode	R	Coded value for “eHealth DSI Service Consumer”

2.3.2.4 Active Participant Identification: Service Provider NCP

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded CN of the TLS certificate of the NCP that processed the eHealth DSI operation that corresponds to the event
UserIsRequestor	R	“false”
RoleIDCode	R	Coded value for “eHealth DSI Service Provider”

2.3.2.5 Audit Source

Field Name	Opt.	Value Constraints
AuditSourceID	R	Identifies the authority that is legally responsible for the audit source. In the case of eHealth DSI this element MUST provide the ISO 3166-2 code of the country/region where the audit source is located OR the specific OID of the entity authenticating and vouching for this auditable event.

2.3.2.6 Participant Object: Patient

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “1” (Person)
ParticipantObjectTypeCodeRole	R	MUST be “1” (Patient)
ParticipantObjectIDTypeCode	R	EV(2, RFC-3881, “Patient Number”)
ParticipantObjectID	R	Patient identifier encoded in HL7v2 CX format. Only the patient identifier that is issued during the patient identification handshake MUST be used for this field.

2.3.2.7 Participant Object: Error Message

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “2” (System Object)
ParticipantObjectTypeCodeRole	R	MUST be “3” (Report)
ParticipantObjectIDTypeCode	R	MUST be “9” (Report Number)
ParticipantObjectID	R	String-encoded error code that was included with the response message.
ParticipantObjectDetail	R	Error message as included with the response message as a type-value pair acc to [RFC 3881]. As a type qualifier “errormsg” MUST be used. The value MUST contain the base64 encoded error message.

A single error message section MUST be given for each error code/message that is included with a response message.

2.3.2.8 Participant Object: Event Target

This subcategory MUST be defined individually for each transaction.

2.3.3 eHealth DSI Patient ID Mapping Audit Schema

The Patient ID Mapping Audit schema consists of the following subcategories of the original categories as defined by RFC 3881.

RFC 3881 Category	eHealth DSI Instance	Description
Event	Event	Audited event according to [RFC 3881]
Active Participant	Human Requestor	HP who triggered the event
	Service Consumer NCP	Service consumer NCP that triggered the event
	Service Provider NCP	Destination of the event
	Mapping Service	Service that provided the mapping
Audit Source	Audit Source	Legal entity that ensures the uniqueness of the identifiers that are used to identify active participants
Participant Object	Patient Source	Patient whose identifier was mapped

	Patient Target	Result of the mapping operation
	Error Message	Optional: Information on errors that occurred during transaction processing

Entries according to this schema MUST only be written after the response to the mapping transaction that is target to auditing has been successfully transmitted to the requesting gateway.

2.3.3.1 Event Identification

Field Name	Opt.	Value Constraints
EventID	R	MUST be set to EV(*num*, “epSOS Transaction”, *name*) where *num* is the number of the transaction including the “epSOS-“ prefix and *name* is the name of the transaction as written in the respective Use Case Roles diagram. See section 2.5.3.7 for a full list of all eventIDs defined for eHealth DSI.
EventActionCode	R	Acc. RFC 3881. See section 2.5.3.7 for a mapping of EventIDs and EventActionCodes.
EventDateTime	R	Acc. RFC 3881. Time MUST be provided by a node that is grouped with a Consistent Time Consumer Actor.
EventOutcomeIndicator	R	Acc. RFC 3881. MUST be “0” on successful patient identification, “1” in case of multiple matches, “4” in case of insufficient traits data, and “8” for permanent failures.

2.3.3.2 Active Participant Identification: Human requestor

Field Name	Opt.	Value Constraints
UserID	R	Identifier of the HP who initiated the event. This field MUST contain the name identifier as given in the respective element of the Authentication Assertion that was issued for this user. See section 2.5.3.9 for the mandatory encoding scheme for user identifiers.
AlternativeUserID	R	Human readable name of the HP as given in the Subject-ID attribute of the HP identity assertion (see [SAML Profile]).
UserIsRequestor	R	“true”
RoleIDCode	R	RFC 3881 compliant encoding of the user’s role as defined in the “role” attribute of the Identity Assertion that was issued for this user.

2.3.3.3 Active Participant Identification: Service Consumer NCP

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded CN of the TLS certificate of the NCP that triggered the eHealth DSI operation that corresponds to the event
UserIsRequestor	R	“true”
RoleIDCode	R	Coded value for “eHealth DSI Service Consumer”

2.3.3.4 Active Participant Identification: Service Provider NCP

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded CN of the TLS certificate of the NCP that processed the eHealth DSI operation that corresponds to the event
UserIsRequestor	R	“false”
RoleIDCode	R	Coded value for “eHealth DSI Service Provider”

2.3.3.5 Active Participant Identification: Mapping Service

Field Name	Opt.	Value Constraints
UserID	R	This field MUST contain the string-encoded OID of the service instance that performed the mapping (e. g. a national MPI)
UserIsRequestor	R	“false”
RoleIDCode	R	Coded value for “Master Patient Index” or “Pseudonymisation”

2.3.3.6 Audit Source

Field Name	Opt.	Value Constraints
AuditSourceID	R	Identifies the authority that is legally responsible for the audit source. In the case of eHealth DSI this element MUST provide the ISO 3166-2 code of the country/region where the audit source is located OR the specific OID of the entity authenticating and vouching for this auditable event.

2.3.3.7 Participant Object: Patient Source

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “1” (Person)
ParticipantObjectTypeCodeRole	R	MUST be “1” (Patient)
ParticipantObjectIDTypeCode	R	EV(2, RFC-3881, “Patient Number”)
ParticipantObjectID	R	Patient identifier encoded in HL7v2 CX format. Only the patient identifier that was the source for the mapping MUST be used for this field.

2.3.3.8 Participant Object: Patient Target

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “1” (Person)
ParticipantObjectTypeCodeRole	R	MUST be “1” (Patient)
ParticipantObjectIDTypeCode	R	EV(2, RFC-3881, “Patient Number”)
ParticipantObjectID	R	Patient identifier encoded in HL7 II format. Only the patient identifier that was the result for the mapping MUST be used for this field.

2.3.3.9 Participant Object: Error Message

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “2” (System Object)
ParticipantObjectTypeCodeRole	R	MUST be “3” (Report)
ParticipantObjectIDTypeCode	R	MUST be “9” (Report Number)
ParticipantObjectID	R	String-encoded error code that was included with the response message.
ParticipantObjectDetail	R	Error message as included with the response message as a type-value pair acc to [RFC 3881]. As a type qualifier “errormsg” MUST be used. The value MUST contain the base64 encoded error message.

A single error message section MUST be given for each error code/message that is included with a response message.

2.3.4 Audit Trail Data for Non-Repudiation

For traceability and non-repudiation of message exchange operations, [Interoperability Specification] requires that the full security headers (including body signature and security token) of all messages MUST be written to audit trails at both NCP-A and NCP-B.

NCP implementers MUST add respective Participant Object sections (see 2.3.4.1 and 2.3.4.2) to the message audit trail entries of all eHealth DSI audit schemas.

2.3.4.1 Participant Object: Request Message

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “4” (Other)
ParticipantObjectIDTypeCode	R	MUST be EV(“req”, “eHealth DSI Msg”, “Request Message”)
ParticipantObjectID	R	String-encoded UUID of the request message
ParticipantObjectDetail	R	Full security header of the request message as a type-value pair acc. to [RFC 3881]. As a type qualifier “securityheader” MUST be used. The value MUST contain the base64 encoded security header. For Internal NCP activities (see 2.3.5), static value "No Security Header Used" might be used.

2.3.4.2 Participant Object: ResponseMessage

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “4” (Other)
ParticipantObjectIDTypeCode	R	MUST be EV(“rsp”, “ehealth DSI Msg”, “Response Message”)
ParticipantObjectID	R	String-encoded UUID of the response message
ParticipantObjectDetail	R	Full security header of the response message as a type-value pair acc. to [RFC 3881]. As a type qualifier “securityheader” MUST be used. The value MUST contain the base64 encoded security header. For Internal NCP activities (see 2.3.5), static value "No Security Header Used" might be used.

2.3.5 Audit Trail Entries on NCP-Internal Activities

Many eHealth DSI operations take place within the NCP and serve as foundation for a subsequent message exchange but feature not inter-NCP characteristics. However, since the NCP may take over additional responsibilities as a data controller, a full traceability, non-repudiation, and originator authenticity regarding the internal operations MUST be achieved.

2.3.5.1 Issuance of a HP Identity Assertion

The national Identity Provider service MUST write an audit trail entry for the confirmation of a HP authentication (e. g. after the attesting signature has been applied to the Identity Assertion). The audit message MUST be assembled according to the HP Assurance audit schema as defined in section 2.3.1. The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

eHealth DSI Instance	Opt.	Description
Event	R	Audited event. See section 2.5.3.7 for the respective values.
Requesting Point of Care	R	Organisation that performed the initial identification and authentication of the HP (e. g. a hospital)
Human Requestor	R	HP whose authenticity was attested
Source Gateway	O	Service that performed the original authentication of the HP
Target Gateway	R	NCP-B that attested the authenticity of the Identity Assertion
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are uses to identify active participants
Patient	X	
Event Target	R	See below

Table 2: Country-B Identity Provider Audit Message Categories

For the event target, a reference to the assertion MUST be kept in order to allow for a linkage of assertions used within messages to their issuing act.

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “2” (System Object)
ParticipantObjectIDTypeCode	R	MUST be EV(“IdA”, “eHealth DSI Security”, “HP Identity Assertion”)
ParticipantObjectID	R	String-encoded UUID of the assertion

2.3.5.2 Issuance of a Treatment Relationship Confirmation Assertion

The NCP at the country of care MUST write an audit trail entry for the confirmation of a treatment relationship between a HP/HCPO and a patient. The audit message MUST be assembled according to the HP Assurance audit schema as defined in section 2.3.1. The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

eHealth DSI Instance	Opt.	Description
Event	R	Audited event. See section 2.5.3.7 for the respective values.
Requesting Point of Care	R	Organisation that established a treatment relationship with

		the patient (e.g. a hospital)
Human Requestor	R	HP who acts on behalf of the HCPO.
Source Gateway	O	System at the HPCO that requested the issuance of the TRC assertion
Target Gateway	R	NCP-B that attested the existence of the treatment relationship
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are uses to identify active participants
Patient	R	Patient who is treated by the HPCO
Event Target	R	See below

Table 3: Country-B TRC Assertion Provider Audit Message Categories

For the event target, a reference to the assertion MUST be kept in order to allow for a linkage of assertions used within messages to their issuing act.

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “2” (System Object)
ParticipantObjectIDTypeCode	R	MUST be EV(“TrcA”, “epSOS Security”, “TRC Assertion”)
ParticipantObjectID	R	String-encoded UUID of the assertion

2.3.5.3 Security Audit Considerations

The service consumer MUST write an audit trail entry according to the *Audit Trail Entries for Internal NCP Activities* after performing SMP queries. The service provider MUST write an audit trail entry according to the *Patient Privacy Audit Schema* when pushing a SMP record.
The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

eHealth DSI Instance	Opt.	Description
Event	R	MUST BE EV(“SMP”, “ehealth-193”, “SMP::Query”) when querying as NCP-B and EV(“SMP”, “ehealth-194”, “SMP::Push”) when pushing to SMP server.
Requesting Point of Care	X	
Human Requestor	X	
Source Gateway	R	URL of the SMP server
Target Gateway	R	NCP that imported the SignedServiceMetadata
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are uses to identify active participants
Patient	X	
Event Target	R	See below

Table 4: eHealth DSI NSL Import Audit Message Categories

For the event target, a reference to the SMP MUST be written.

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “2” (System Object)
ParticipantObjectIDTypeCode	R	MUST be EV(“SMP”, “eHealth DSI Security”, “SignedServiceMetadata”)
ParticipantObjectID	R	Base64 encoded list of endpoints that has been affected by the SMP update, separated by comma.

2.3.5.4 Pivot Translation of a Medical Document

A NCP MUST write an audit trail entry for the pivot translation of a medical document. The audit message MUST be assembled according to the HP Assurance audit schema as defined in section 2.3.1. The following table defines which categories MUST be filled (R), which MAY be filled (O) and which categories MUST NOT be used (X).

eHealth DSI Instance	Opt.	Description
Event	R	Audited event. See section 2.5.3.7 for the respective values.
Requesting Point of Care	X	
Human Requestor	X	
Source Gateway	X	
Target Gateway	R	Identification of the NCP Translation Service
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers

		that are uses to identify active participants
Patient	X	
Event Target	R	See below

Table 5: eHealth DSI Pivot Translation Audit Message Categories

An event target MUST be defined for both the source data of the translation and the result of the translation.

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “4” (other)
ParticipantObjectDataLifeCycle	R	MUST be “5” (translation)
ParticipantObjectIDTypeCode	R	MUST be EV(“in”, “eHealth DSI Translation”, “Input Data”)
ParticipantObjectID	R	Identifier that allows to univocally identifying the source document or source data entries.

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “4” (other)
ParticipantObjectDataLifeCycle	R	MUST be “5” (translation)
ParticipantObjectIDTypeCode	R	MUST be EV(“out”, “eHealth DSI Translation”, “Output Data”)
ParticipantObjectID	R	Identifier that allows to univocally identifying the target document.

2.3.5.5 Documentation of the Patient Information Notification (PIN)

The NCP at the country of care MUST write an audit trail entry documenting the confirmation of the HP concerning the issuance and approval of the Patient Information Notification (PIN) between a HP/HPCO and a patient. The audit message MUST be assembled according to the HP Assurance audit schema.

eHealth DSI Instance	Opt.	Description
Event	R	Audited event. See section 2.5.3.7 for the respective values.
Requesting Point of Care	R	Organisation that established a treatment relationship with the patient (e. g. a hospital) and is responsible for collecting the PIN.
Human Requestor	R	HP who acts on behalf of the HPCO.
Source Gateway	O	System at the HPCO
Target Gateway	R	NCP-B that attested the existence of the treatment relationship
Audit Source	R	Legal entity that ensures the uniqueness of the identifiers that are uses to identify active participants
Patient	R	Patient who is treated by the HPCO
Event Target	R	See below

Table 6: Country-B TRC Assertion Provider Audit Message Categories

For the event target, a reference to the assertion MUST be kept in order to allow for a linkage of assertions used within messages to their issuing act.

Field Name	Opt.	Value Constraints
ParticipantObjectTypeCode	R	MUST be “4” (Other)
ParticipantObjectIDTypeCode	R	MUST be EV(“PIN”, “epSOS Security”, “Privacy Information Notice”)
ParticipantObjectDataLifecycle	R	MUST be “12” (Receipt of Disclosure)
ParticipantObjectID	R	string-encoded of either “PINack” for consent given OR “PINdny” for consent denied

2.3.5.6 eHealth DSI-specific Codes and Encodings

In the following sections eHealth DSI-specific code lists and encoding conventions for use within audit trail entries are defined.

2.3.5.7 eHealth DSI EventIDs

Interaction Pattern	Operation	Transaction / Event ID	Event Name	Action
“**Request of Data**”	Fetch Request	ITI-63	XCF::CrossGatewayFetchRequest	“R”

according to [Interoperability Specification]				
	Query	ITI-38	XCA::CrossGatewayQuery	R
	Retrieve	ITI-39	XCA::CrossGatewayRetrieve	R
"**Provisioning of Data**" according to [Interoperability Specification]	Provide	ITI-41	XDR::ProvideandRegisterDocumentSet-b	U
	BPPC-RegisterUpdate	ITI-41	XDR::BPPCProvideandRegisterDocumentSet-b	C/U
"**Patient Identification and Authentication**" according to [Interoperability Specification]	XCPD	ITI-55	XCPD::CrossGatewayPatientDiscovery	E
Country-B Identity Provider	Issuance of HP Identity Assertion	epSOS-91	identityProvider::HPAuthentication used for proprietary issuance	"E"
	Issuance of HP Identity Assertion	ITI-40	XUA::ProvideX-UserAssertion used for IHE ITI XUA-compliant issuance	E
Country-B NCP	Issuance of a TRC Assertion	epSOS-92	ncp::TrcAssertion	"E"
Configuration Manager	NSL Import	epSOS-93	ncpConfigurationManager::ImportNSL	"E"
Transformation Manager	Pivot Translation	epSOS-94	ncpTransformationMgr::Translate	"E"
"**Patient Access**" according to [Interoperability Specification]	PA-AuthN	epSOS-95	Proprietary	E
	PA-Fetch	epSOS-96	Proprietary	E
	PA-Translate	epSOS-97	ncpTransformationMgr::Translate	E

Table 7: eHealth DSI EventIDs

In error cases where NCP-A cannot decode the requested operation an event ID of EV(epSOS-00, "unknown", unknown) MUST be written to the Patient Privacy Audit Trail.

2.3.5.8 Active Participant Role ID Codes

Codesystem	Code	DisplayName
eHealth DSI	ServiceProvider	eHealth DSI Service Consumer
eHealth DSI	ServiceConsumer	eHealth DSI Service Provider
eHealth DSI	Pseudonymisation	Pseudonymisation Service
eHealth DSI	MasterPatientIndex	Master Patient Index
eHealth DSI	IdentityProvider	NCP Identity Provider
eHealth DSI	NCP-B	NCP-B
eHealth DSI	Configuration Manager	NCP Configuration Manager
eHealth DSI	Transformation Manager	NCP Transformation Manager

2.3.5.9 Encoding of the User Identifier

The HP identifier entry MUST be taken from the subject field of the identification assertion that is transmitted together with a request. For conformance with [IHE XUA++] the following encoding MUST be used:

`SPProvidedID<saml:SubjectNameID@saml:Issuer>`

The SPProvidedID is needed because there are situations where identity federation is in place. The SPProvidedID is a name identifier established by a service provider

or affiliation of providers for the entity in the NameID different from the primary name identifier given in the content of the element.

2.3.6 Non Repudiation Evidence

NCPeH MUST provide electronic evidence for non-repudiation purposes.
Non-repudiation services are mandated to generate, collect, maintain, make available and validate evidence concerning a claimed event or action in order to resolve disputes about the occurrence or non-occurrence of the event or action. Non-Repudiation protocols have been exhaustively studied in the literature and by industry practices[3]. In particular both literature and ISO 13888 define four types of Non-Repudiation evidence: Non Repudiation of Origin (NRO), Non Repudiation of Receipt (NRR), Non Repudiation of Delivery (NRD), and Non Repudiation of Submission (NRS). [Section II – Security Services], section 5.2 highlights the need to have in eHealth DSI message exchanges NRO and NRD type of evidence, for all the levels of the eHealth DSI message stack, by allowing technologies such as IPSec, TLS, Message Payload Signatures, possible usage of trusted third parties, and Audit Trails.
Audit trail content is insufficient with respect to disputes that can arise during operations. Examples are[4]:

- In ePrescription, the patient returns to the home country and claims reimbursement of 3 packages of the drug purchased abroad. The dispensation only shows that 1 package was dispensed. The organization of NCPeH A now needs to prove that erroneous information was received from NCPeH B and was not generated while processing the dispensation information in the NCPeH or NI software. A similar case arises when the patient claims they only purchased 1 package out of 3, and there should be still some available amount on the prescription. The NCPeH A needs to show that the information received from NCPeH B was wrong.
- In Patient Summary, a drug is administered to the patient, and the patient suffers a severe allergic reaction. The allergy to the drug was mentioned on the patient summary, but the doctor claims that this information was not delivered and shown to them. Now NCPeH B wants to demonstrate that this information was indeed not received from Country A.

This specification provides a solution for the non-repudiation requirements stated in [Interoperability Specification] section 5.7, adapting the ETSI Registered Electronic Mail (REM) set of evidence to the need of the eHealth DSI synchronous, RegRep-based message exchange pattern. The solution proposed, highly inspired by the eHealth DSI Extended Security Safeguards (ESS) provides a policy-based mechanism that, inspecting the incoming message or flow, feeds data the chosen sector-specific evidence emitter (e.g., for the eHealth domain, IHE ATNA and [Interoperability Specification] section 4.5). The benefits of this approach are:

- Provide a technology-agnostic path towards evidence interoperability in all the sectors, while *preserving* the current specifications (i.e., the content of the ATNA audit trails is unchanged)
- Align eHealth DSI specifications with CEF building blocks on evidence, by enabling additional and forthcoming evidence formats (e.g., ETSI REM)
- Defines a set of extensible templates reflecting all mandatory auditable events for any cross-border use case
- Provide anchor points for national extensions as required/desired by the operating nations (e.g., enabling the use of controlled vocabularies or ontologies for automated processing)
- Aligns eHealth DSI to ISO 13888 "Non Repudiation" requirements

[3] http://wiki.ds.unipi.gr/display/ESENS/Whitepaper+-+Non+Repudiation

[4] See https://openncp.atlassian.net/wiki/pages/viewpage.action?pageId=51413101

- Provide a formalized testing facility to warrant a complete traceability and reconstructability using templates in any combination, by using the Gazelle Test Assertion Markup Language (TAML) model
- No storage of private healthcare information in the NCPeH

3 Security Considerations

3.1 Audit Trail Implementation

Regarding the implementation of eHealth DSI audit trails, the following requirements MUST be considered.

- NCP implementations MUST ensure that audit trail data is not lost, cannot be altered and is not disclosed in between the NCP and the audit trail repository. In cases where audit trail data is transmitted among system boundaries, adequate protection means MUST be applied. If TLS is used, configuration, algorithms and key length MUST be used as specified in [Messaging Profile] for NCP-to-NCP secure messaging.
- A NCP MAY cache audit trail data for performance improvement or in case that the audit trail repository is temporarily not available. If caching at the NCP is used,
    - the NCP MUST ensure that audit trail data does not get lost at the NCP even in case of NCP operational failures
    - the NCP MUST not accept or issue further service requests in case that it cannot ensure the writing of the respective audit trail
    - the NCP MUST ensure that audit trail data cannot be altered
    - the NCP MUST prevent audit trail entries from disclosure

3.2 Audit Trail Repository

The audit trail repository that is used for the persistent storage of eHealth DSI audit trail entries

- MUST prevent audit trail entries from disclosure to unauthorized persons.
- MUST prevent audit trail entries from being deleted or altered. In addition it MUST be possible to detect the alteration or deletion of single audit trail entries.
- MUST provide functionality to authorized users (e.g., prosecutors) to inspect the audit trail and to query for audit trails affecting identified patients, HPs or documents.

4 Audit Trail Implementation Guidelines (non-normative)

As [RFC5424] defines a recommended message size of 2048 bytes a NCP implementation should consider to store the ParticipantObjectDetail attribute value data outside the audit trail and just place a reference to this data into the audit trail entry.

5 References

5.1 Normative References

[RFC 2119] Bradner, S.: Key words for use in RFCs to Indicate Requirement Levels. Harvard University, Boston, Massachusetts, 1997.

[RFC 3881] RFC3881: Security Audit and Access Accountability Message XML Data Definitions for Healthcare Applications, http://tools.ietf.org/html/rfc3881

[ETSI REM] ETSI TS 102 640-2 v2.2.1, 2011

5.2 Non-Normative References

[ASTM E2147-01] ASTM Subcommittee E31.25: *ASTM E2147 - Standard Specification for Audit and Disclosure Logs for Use in Health Information Systems.* January 2009.

[DICOM Sup 95] DICOM Standards Committee: *DICOM Supplement 95: Audit Trail Messages*. August 2010.

[IHE ITI TF-2a] IHE International*: IT Infrastructure Technical Framework Volume 2a – Transactions ITI-29 – ITI-51*. Revision 9.0, August 2012. http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Vol2a.pdf

[IHE ITI TF-2b] IHE International*: IT Infrastructure Technical Framework Volume 2 – Transactions ITI-29 – ITI-51*. Revision 9.0, August 2012. http://www.ihe.net/Technical_Framework/upload/IHE_ITI_TF_Vol2b.pdf

[IHE XUA++] IHE International*: IT Infrastructure Technical Framework Cross-Entreprise User Assertion – Attribute Extension (XUA++) – Trial Implementation* August 2011. http://www.ihe.net/Technical_Framework/upload/IHE_ITI_Suppl_XUA-_Rev1-2_TI_2011-08-19.pdf