INTERNATIONAL STANDARD

ISO 21549-2

Second edition
2014-02-15

Health informatics — Patient healthcard data —

Part 2: Common objects

Informatique de santé — Données relatives aux cartes de santé des patients —

Partie 2: Objets communs

Reference number
ISO 21549-2:2014(E)

COPYRIGHT PROTECTED DOCUMENT

ISO copyright office
Case postale 56 • CH-1211 Geneva 20
Tel. + 41 22 749 01 11
Fax + 41 22 749 09 47
E-mail copyright@iso.org
Web www.iso.org

Published in Switzerland

Contents

Page

Foreword

ISO (the International Organization for Standardization) is a worldwide federation of national standards bodies (ISO member bodies). The work of preparing International Standards is normally carried out through ISO technical committees. Each member body interested in a subject for which a technical committee has been established has the right to be represented on that committee. International organizations, governmental and non-governmental, in liaison with ISO, also take part in the work. ISO collaborates closely with the International Electrotechnical Commission (IEC) on all matters of electrotechnical standardization.

The procedures used to develop this document and those intended for its further maintenance are described in the ISO/IEC Directives, Part 1. In particular the different approval criteria needed for the different types of ISO documents should be noted. This document was drafted in accordance with the editorial rules of the ISO/IEC Directives, Part 2 (see www.iso.org/directives).

Attention is drawn to the possibility that some of the elements of this document may be the subject of patent rights. ISO shall not be held responsible for identifying any or all such patent rights. Details of any patent rights identified during the development of the document will be in the Introduction and/or on the ISO list of patent declarations received (see www.iso.org/patents).

Any trade name used in this document is information given for the convenience of users and does not constitute an endorsement.

For an explanation on the meaning of ISO specific terms and expressions related to conformity assessment, as well as information about ISO's adherence to the WTO principles in the Technical Barriers to Trade (TBT) see the following URL: Foreword - Supplementary information.

The committee responsible for this document is ISO/TC 215, *Health informatics*.

This second edition cancels and replaces the first edition (ISO 21549-2:2004), which has undergone a minor revision. The following changes have been made.

— Foreword: mention of CEN collaboration is removed.

— Scope: first paragraph is reworded.

— Normative references: references that are not cited normatively are moved to the Bibliography.

— Terms and definitions: unused terms are removed.

— Symbols and abbreviated terms: unused abbreviated terms are removed.

— Subclause 6.3.2, Table 2: data type of codeIdentifier is corrected to match ASN.1 definition.

— Clauses 5, 6, and 7: the figures and tables are renumbered sequentially, references to the figures and tables are added.

— Bibliography: dates from the references are removed where not applicable.

ISO 21549 consists of the following parts, under the general title *Health informatics — Patient healthcard data*:

— *Part 1: General structure*

— *Part 2: Common objects*

— *Part 3: Limited clinical data*

— *Part 4: Extended clinical data*

— *Part 5: Identification data*

— *Part 6: Administrative data*

— *Part 7: Medication data*

— *Part 8: Links*

Introduction

This part of ISO 21549 provides data structures and definitions for limited clinical data for use within patient-held healthcare data cards.

With a more mobile population, greater healthcare delivery in the community and at patients' homes, together with a growing demand for improved quality of ambulatory care, portable information systems and stores have increasingly been developed and used. Such devices are used for tasks ranging from identification, through portable medical record files, and on to patient-transportable monitoring systems.

The functions of such devices are to carry and to transmit person-identifiable information between themselves and other systems; therefore, during their operational lifetime they may share information with many technologically different systems which differ greatly in their functions and capabilities.

Healthcare administration increasingly relies upon similar automated identification systems. For instance prescriptions may be automated and data exchange carried out at a number of sites using patient transportable computer readable devices. Healthcare insurers and providers are increasingly involved in cross-region care, where reimbursement may require automated data exchange between dissimilar healthcare systems.

The advent of remotely accessible data bases and support systems has led to the development and use of "Healthcare Person" identification devices that are also able to perform security functions and transmit digital signatures to remote systems via networks.

With the growing use of data cards for practical everyday healthcare delivery, the need has arisen for a standardized data format for interchange.

The person-related data carried by a data card can be categorized in three broad types: identification (of the device itself and the individual to whom the data it carries relates), administrative and clinical. It is important to realize that a given healthcare data card "de facto" has to contain device data and identification data and may in addition contain administrative, clinical, prescription and linkage data.

Device data is defined to include:

— identification of the device itself;

— identification of the functions and functioning capabilities of the device.

Identification data may include:

— unique identification of the device holder or of all other persons to whom the data carried by the device are related.

Administrative data may include:

— complementary person(s)-related data;

— identification of the funding of healthcare, whether public or private, and their relationships i.e. insurer(s), contract(s) and policy(ies) or types of benefits;

— other data (distinguishable from clinical data) that are necessary for the purpose of healthcare delivery.

Clinical data may include:

— items that provide information about health and health events;

— their appraisal and labeling by a healthcare provider (HCP);

— related actions planned requested or performed.

Because a data card essentially provides specific answers to definite queries while having at the same time a need to optimize the use of memory by avoiding redundancies, “high level” Object Modeling Technique (OMT) has been applied with respect to the definition of healthcare data card data structures.

Data in the four categories above share many features. For instance, each may need to include ID numbers, names and dates. Some information may also have clinical as well as administrative uses. Therefore it has been considered inadequate to provide a simple list of items carried by healthcare data cards without applying a generic organization, based upon the existence of basic data elements. These may be defined by their characteristics (e.g. their format), and from them compound data objects may be constructed; several such objects may also share attributes.

This part of ISO 21549 describes and defines the Common Data objects used within or referenced by patient held health data cards using UML, plain text and Abstract Syntax Notation (ASN.1).

These data objects are utilized in all forms of healthcare data cards and are used to construct compound data objects as defined in Parts 3 to 8 of ISO 21549.

Health informatics — Patient healthcard data —

Part 2: Common objects

1 Scope

This part of ISO 21549 establishes a common framework for the content and the structure of common objects used to construct data held on patient healthcare data cards. It is also applicable to common objects referenced by other data objects.

This part of ISO 21549 is applicable to situations in which such data is recorded on or transported by patient healthcards compliant with the physical dimensions of ID-1 cards defined by ISO/IEC 7810.

This part of ISO 21549 specifies the basic structure of the data, but does not specify or mandate particular data-sets for storage on devices.

The detailed functions and mechanisms of the following services are not within the scope of this part of ISO 21549, (although its structures can accommodate suitable data objects elsewhere specified):

— the encoding of free text data;

— security functions and related services which are likely to be specified by users for data cards depending on their specific application, for example: confidentiality protection, data integrity protection, and authentication of persons and devices related to these functions;

— access control services which may depend on active use of some data card classes such as microprocessor cards;

— the initialization and issuing process (which begins the operating lifetime of an individual data card, and by which the data card is prepared for the data to be subsequently communicated to it according to this part of ISO 21549).

The following topics are therefore beyond the scope of this part of ISO 21549:

— physical or logical solutions for the practical functioning of particular types of data cards;

— how the message is processed further 'downstream' of the interface between two systems;

— the form which data takes for use outside the data card, or the way in which such data is visibly represented on the data card or elsewhere.

2 Normative references

The following documents, in whole or in part, are normatively referenced in this document and are indispensable for its application. For dated references, only the edition cited applies. For undated references, the latest edition of the referenced document (including any amendments) applies.

ISO 21090:2011, *Health informatics — Harmonized data types for information interchange*

3 Terms and definitions

For the purposes of this document, the following terms and definitions apply.

3.1
country
code that identifies the country of origin of the device issuer

Note 1 to entry: This may not necessarily be the same as the nationality of the device holder.

3.2
data integrity
property that data has not been altered or destroyed in an unauthorized manner

[SOURCE: ISO 7498-2:1989]

3.3
data object
collection of data that has a natural grouping and may be identified as a complete entity

3.4
data sub-object
component of a data object that itself may be identified as a discrete entity

3.5
device holder
individual transporting a data card which contains a record with themselves identified as the major record person

3.6
entity authentication
corroboration that an entity is the one claimed

[SOURCE: ISO/IEC 9798-1:2010]

3.7
erasure
process whereby access to a data entity after a given point in time is permanently removed or access denied thereafter to all parties

Note 1 to entry: This may not involve physical removal from the device and may merely be the result of altering security such that access is permanently denied to all parties.

3.8
healthcard holder
individual transporting a healthcare data card which contains a record with themselves identified as the major record person

3.9
healthcare data card
machine readable card conformant to ISO/IEC 7816 intended for use within the healthcare domain

3.10
record
collection of data

3.11
record person
individual about whom there is an identifiable record containing person-related data

3.12
security
combination of confidentiality, integrity and availability

4 Symbols and abbreviated terms

ASN.1 Abstract Syntax Notation version 1

HCP Healthcare person

UML Unified Modeling Language

UTC Universal Time Coordinated

5 Basic data object model for a healthcare data card - Patient healthcard data object structure

A set of basic data objects have been designed to facilitate the storage of clinical data in a flexible structure, allowing for future application specific enhancements. These tools should help the implementation of common accessory characteristics of stored data in a way that allows efficient use of memory, an important feature for many types of data cards.

The tools consist of a generic data structure based on an object-oriented model represented as an UML class diagram as shown in Figure 1.

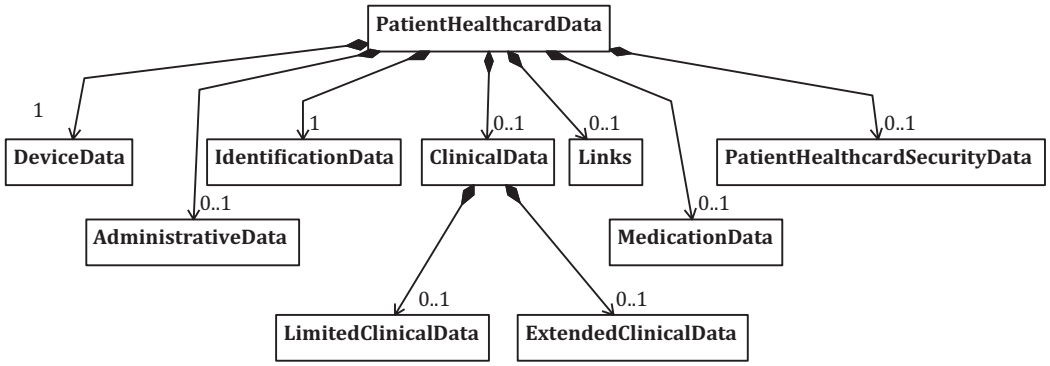

Figure 1 — Patient healthcard data: overall structure

The content of this object-oriented structure is described below and intrinsically will also require the use of data objects not defined within this part of ISO 21549.

NOTE 1 This part of ISO 21549 is purely applicable to patient healthcards containing health data. Data objects containing financial and healthcare reimbursement data are not defined within this International Standard.

NOTE 2 It is possible to take the data objects and recombine them while preserving their context-specific tags, and to define new objects, while still preserving interoperability.

In addition to the capability of building complex aggregate data objects from simpler building blocks, this part of ISO 21549 allows for associations between certain objects so that information can be shared. This feature is mainly used to allow, for example, a set of accessory attributes to be used as services to several stored information objects.

6 Basic data objects for referencing

6.1 Overview

A series of generally useful data type definitions have been made that have no intrinsic value in themselves, but which are used to define other objects within this multi-part standard. Operations may be performed with these objects in association with other information objects to “add value”.

6.2 Internal links

6.2.1 General

A number of objects in the data model of this part of ISO 21549 are used mainly as a reference to other objects. In many situations constructed objects contain a general pointer called a RefPointer that is a sequence of tags allowing a reference to any object, including sub-objects that can only be referenced as part of a constructed object, using an application-specific tag and a number of context-specific tags to sufficient depth.

6.2.2 The "ReferencePointer" and "ReferenceTag" data objects

A general reference pointer is defined in this part of ISO 21549 as an ordered list of tags pointing to the object or sub-object that is referenced. The data object "RefPointer" shall consist of a sequence of "RefTag" (of integer type). The "RefTag" is the application-specific tag of the object as defined in this part of ISO 21549. Each following "RefTag" in Table 1 specifies the context-specific tag in increasing depth.

Table 1 — The specification of individual entities within the object RefPointer

Object name	Data Type	Multiplicity	Comments
RefTag	Integer	1..*	This is a sequence of references to other objects. The Reference is the ASN.1 Tag of another data object.

6.3 Coded data

6.3.1 General

Coded values are understood by reference to the coding scheme to which they apply. The general principle in this part of ISO 21549 is that it is not mandatory to use a particular coding scheme, unless specified within this part of ISO 21549, when such codes act as parameters. One example is the use of ISO 3166-1 for country codes.

When a coding scheme is exclusively specified within this part of ISO 21549 no alternative coding scheme shall be allowed. Any references to coding schemes not so specified may however be modified in the future independent of the rest of this part of ISO 21549.

6.3.2 The data object CodingSchemesUsed

A coding scheme in accordance with ISO 21090 shall be referred to by a unique identifier, which allows unambiguous reference to standard code systems and other local code systems. Where either ISO or HL7 have assigned the unique identifiers to coding schemes, then these identifiers shall be used. Otherwise implementations shall use an appropriate ISO Object Identifier (OID) or UUID to construct a globally unique local coding scheme identifier.

The data object CodingSchemesUsed shall consist of an ordered sequence of the sub-object CodingScheme, which shall itself consist of a code identifier, a code length (of integer type), and an optional free text comment (an octet string with a length of between 1 and 20 characters). Figure 2 and Table 2 define CodingScheme data object.

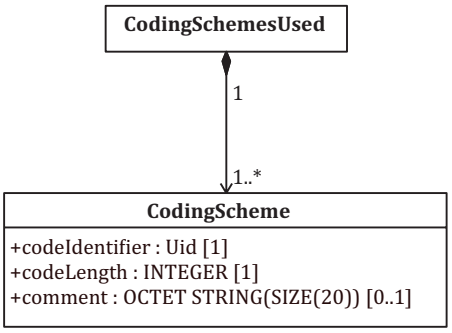

Figure 2 — The structure of CodingScheme

Table 2 — The specification of individual entities within the object CodingScheme

Object name	Data Type	Multiplicity	Comments
codeIdentifier	OCTET STRING (SIZE (64))	1	This identifies the particular coding scheme being referenced.
codeLength	INTEGER	1	This identifies the length of the code.
comment	OCTET STRING (SIZE(20))	0..1	This optional element of free text allows the qualification in text of the coding scheme.

6.3.3 The data object CodedData

The data object CodedData shall include both a reference to coding schemes used and a code data value as well as optional free text.

The object codingSchemeRef is a RefPointer pointing at a value that identifies a particular coding scheme within the object coding schemes used. If codingSchemeRef = 0 then the coding scheme is implicit in this part of ISO 21549.

The object codeDataValue has been defined to indicate the actual code value in a particular coding scheme. Figure 3 and Table 3 define CodedData data object.

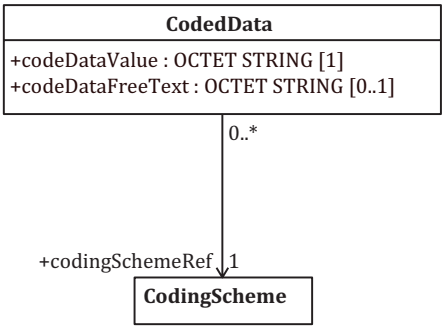

Figure 3 — The structure of CodedData

Table 3 — The specification of individual entities within the object CodedData

Object name	Data Type	Multiplicity	Comments
codingSchemeRef	RefPointer	1	This is a reference pointer to a value that identifies a particular coding scheme within the data object CodingSchemesUsed. If CodingSchemeRef = 0 then the following code set is used: A = Admininstrative-data free text, C = Clinical-data free text.
codeDataValue	OCTET STRING	1	This string contains the value of the coded data.
codeDataFreeText	OCTET STRING	0..1	This optional element of free text allows the qualification in text of the coding scheme.

6.4 Accessory attributes

The data object "AccessoryAttributes" shall consist of an ordered set of data that is essential to record an audit trail regarding both the originator of the information and the means via which it arrives to the recipient. It shall consist of:

— date1 which shall represent the time/date of data being communicated to the data card across the interface;

— date2 which shall represent the time/date of data being available to the originator of the message;

— place1 which shall represent the identity/locator of the sender of the message and is linked with "person1";

— place2 which shall represent the identity/locator of the original author of the data;

— personid3 shall be either the code or representation of the person/device/system that provided the information that was added to a system to become the data within the "message";

— securityLevels which shall be constructed according to the ASN.1 definition contained in Annex A and shall represent the rights in relation to reading, writing, updating and erasing the data contained within the data object to which these accessory attributes are attached;

— compressionMethodData shall be constructed according to the ASN.1 definition contained in Annex A and shall consist of a reference pointer pointing at a defined compression methodology within a compression methodology table. This represents the methodology applied to the data contained within the data object to which the accessory attributes are attached;

— object security attributes.

The object security attributes "SecurityServices" shall each consist of a sequence of digital signatures, as well as algorithms and keys for signature and encryption.

None of the above attributes is mandatory, however all are highly desirable. It is recommended that all (with the possible exception of personid3) should be delivered every time that the media/system allows. A list of priorities in groupings follows and in principle should be followed as groups:

{date1, date2, place1, place2, personid3, SecurityLevels, CompressionMethodData, objSecAttributes}

{date1, place1, place2, SecurityLevels, CompressionMethodData, objSecAttributes}

{date1, place2, SecurityLevels, CompressionMethodData, objSecAttributes}

{date1, SecurityLevels, CompressionMethodData, objSecAttributes}

{SecurityLevels, CompressionMethodData, objSecAttributes}

{objSecAttributes}

NOTE This "AccessoryAttributes" data object can be associated to any other data object.

Figure 4 and Table 4 define AccessoryAttributes data object. Table 5 defines PersonCode data object. Figure 5 and Table 6 define SecurityServices data object. Table 7, Table 8, and Table 9 define SecurityLevels, CompressMethodData, and SecAttData data object respectively.

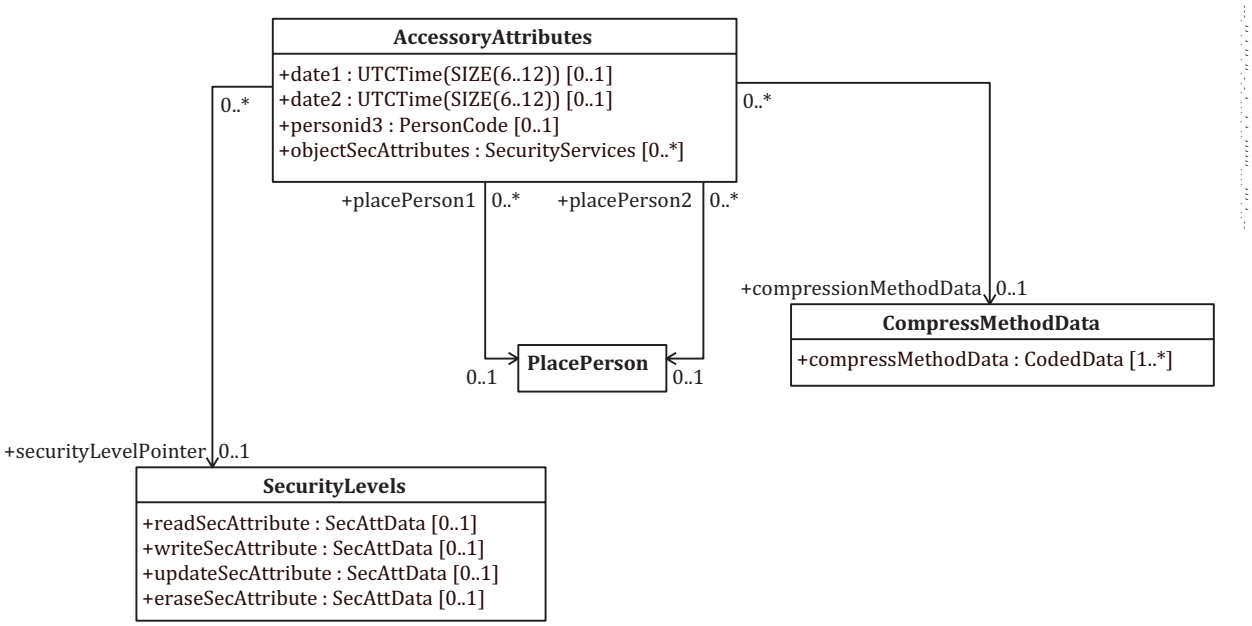

Figure 4 — The structure of Accessory Attributes

Table 4 — The specification of individual entities within the object AccessoryAttributes

Object name	Data Type	Multiplicity	Comments
date1	UTCTime	0..1	
date2	UTCTime	0..1	
personid3	PersonCode	0..1	
objectSecAttributes	SecurityServices	0..*	
securityLevelPointer	RefPointer	0..1	This is a reference pointer to an object SecurityLevels.
placePerson1	RefPointer	0..1	This is a reference pointer to an object PlacePerson.
placePerson2	RefPointer	0..1	This is a reference pointer to an object PlacePerson.
compressionMethodData	RefPointer	0..1	This is a reference pointer to an object CompressionMethodData.

Table 5 — The specification of individual entities within the object PersonCode

Object name	Data Type	Multiplicity	Comments
personCode	RefPointer	1	
personText	OCTET STRING	0..1	

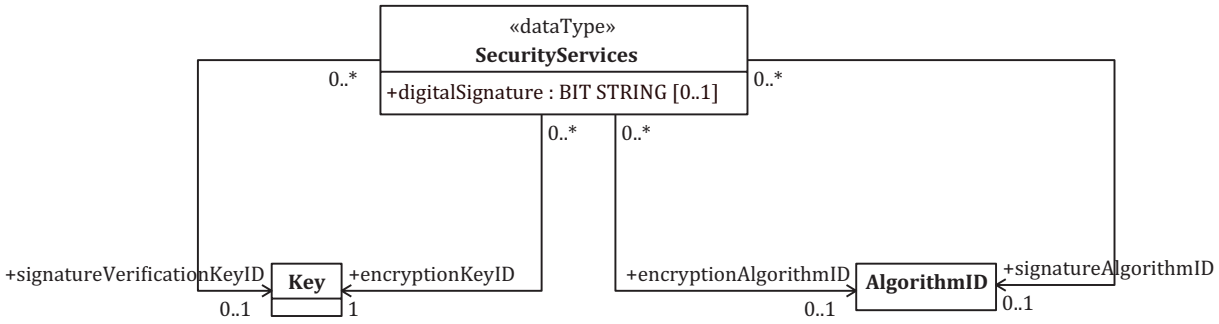

Figure 5 — The structure of SecurityServices

Table 6 — The specification of individual entities within the object SecurityServices

Object name	Data Type	Multiplicity	Comments
digitalSignature	BIT STRING	0..1	This contains the computed bit string of the digital signature.
signatureAlgorithmID	RefPointer	0..1	This is a reference pointer to a line in the signature algorithm table.
signatureVerificationKeyID	RefPointer	0..1	This is a reference pointer to a line in the signature verification key ID table.
encryptionAlgorithmID	RefPointer	0..1	This is a reference pointer to a line in the Encryption Algorithm ID table.
encryptionKeyID	RefPointer	0..1	This is a reference pointer to a line in the encryption key table.

Table 7 — The specification of individual entities within the object SecurityLevels

Object name	Data Type	Multiplicity	Comments
readSecAttribute	SecAttData	0..1	This attribute sets a rule for reading an object.
writeSecAttribute	SecAttData	0..1	This attribute sets a rule for writing data to an object.
updateSecAttribute	SecAttData	0..1	This attribute sets a rule for updating object data.
eraseSecAttribute	SecAttData	0..1	This attribute sets a rule for erasing object data.

Table 8 — The specification of individual entities within the object CompressMethodData

Object name	Data Type	Multiplicity	Comments
compressMethodData	CodedData	1..*	This contains coded data value representation of the compression methodology utilized.

Table 9 — The specification of individual entities within the object SecAttData

Object name	Data Type	Multiplicity	Comments
always	BOOLEAN	1	True = always available, if false functionality is protected and is controlled by one or more of the underlying parameters.
extAuth	BOOLEAN	1	True = requires external authentication.
holdAg	BOOLEAN	1	True = requires data-card holder agreement.
origAg	BOOLEAN	1	True = can only be done by originator of data element.

7 Device and data security attributes

7.1 General

Data stored in data cards used in healthcare may be personally sensitive. For this reason this part of ISO 21549 provides a series of security attributes in the form of data objects that may be required for the provision of security functions. The actual data content (value) is not within the scope of this part of ISO 21549, nor are the mechanisms that make use of these data elements. It is emphasized that the security attributes cannot satisfy given security requirements without the implementation of the appropriate security functions and mechanisms within the data card.

Such access privileges are attributable to specific individuals with respect to discrete data items. These privileges will be defined by application developers and can be controlled by automated systems such as healthcare professional cards. The privileges may be defined at the application level thereby providing application and potential country specificity.

The data object SecurityServices provides for the storage of data required to deliver these security functions and mechanisms. These data can be "attached" to individual data elements thereby preserving the original author's security requirements when the data object is transferred between different forms of data card. This mechanism may therefore ensure that in the process of transferring data from active to passive media and then back to active media, the original security requirements are re-generated. This ability also allows exact replication of a data card such as on regeneration after failure.

7.2 Specific data cards' security services-related data objects

7.2.1 General

All the security service objects required to deliver security related to patient data held on and transmitted by data cards shall be constructed according to the following definitions.

7.2.2 Patient devices security-related data

Patient-held data cards may require the following security services:

— authentication of the device;

— authentication of the data card holder;

— authentication of the HCP attempting to access data contained in the data card.

These services shall be provided by the objects:

— data card holder verification and its associated data PatCardHolderVer;

— data card Authentication and its associated DevClassAuthenticateData;

— data card Authenticating HCP-class for access control and its associated HCPAuthenticateData.

7.2.3 Data from data cards held by healthcare persons

Data objects from data cards held by healthcare persons shall provide for the functions of identification, access control and signature. These functions are provided by a discrete number of sub-objects. The identification information related to a healthcare person and his or her responsible agency shall be provided by the data object HcpData. This data object shall be constructed as an implicit sequence of healthcare person identification data, of healthcare site location data, and of optional accessory attributes.

7.2.4 Patient healthcard security-related data

Healthcare cards require security services to control access to the medical data contained within them. These services are determined and controlled by PatientHealthcardSecurityData. Figure 6 and Table 10 define the PatientHealthcardSecurityData data object. Table 11, Table 12, Table 13, Table 14, Table 15, Table 16 and Table 17 define DevClassAuthenticateData, HcpAuthenticateData, PatCardHolderVer, PatSignatureFunctionData, PatEncryptionData, Keytable and AlgorithmTable data objects respectively.

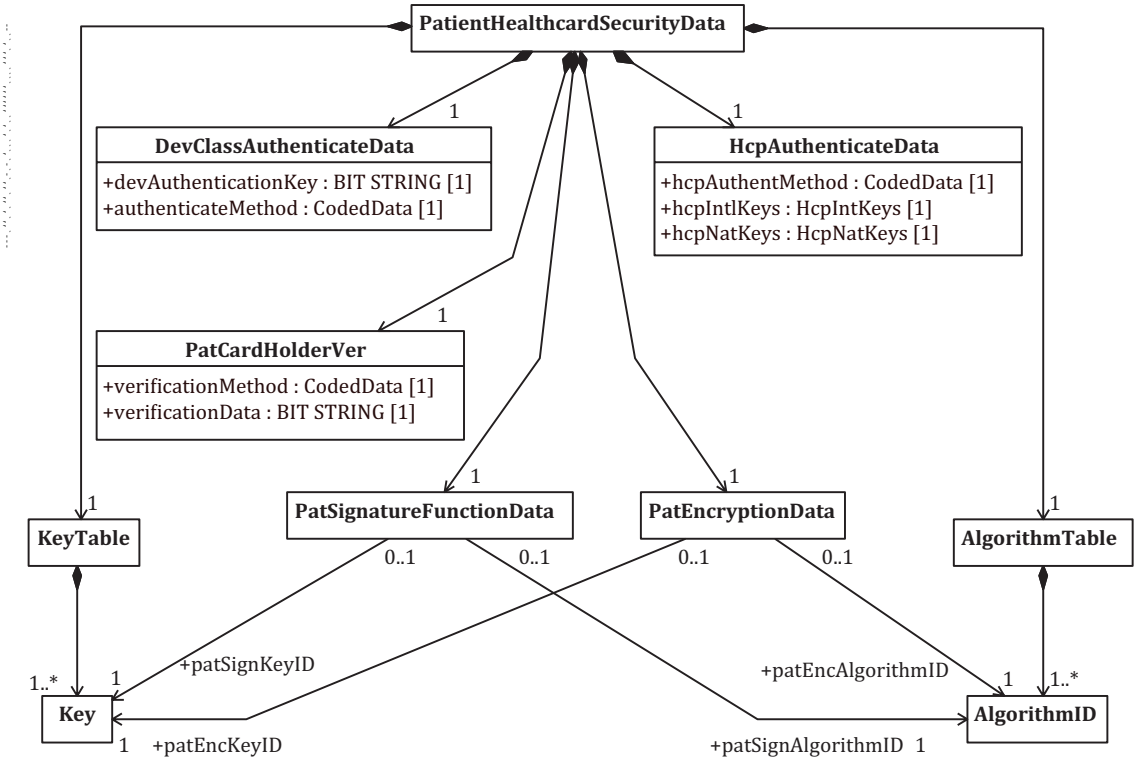

Figure 6 — The structure of PatientHealthcardSecurityData

Table 10 — The specification of individual entities within the object PatientHealthcardSecurity

Object name	Data Type	Multiplicity	Comments
DevClassAuthenticateData	Class	1	
HcpAuthenticateData	Class	1	
PatCardHolderVer	Class	1	
PatSignatureFunctionData	Class	1	
PatEncryptionData	Class	1	
KeyTable	Class	1	
AlgorithmTable	Class	1	

Table 11 — The specification of individual entities within the object DevClassAuthenticateData

Object name	Data Type	Multiplicity	Comments
devAuthenticationKey	BIT STRING	1	Contains the device authentication Key.
authenticateMethod	CodedData	1	Coded data specifying the methodology to be used to authenticate the card.

Table 12 — The specification of individual entities within the object HcpAuthenticateData

Object name	Data Type	Multiplicity	Comments
hcpAuthentMethod	CodedData	1	Coded Data specifying the authentication methodology to be used to authenticate a Healthcare Person.
hcpIntKeys	HcpIntKeys	1	Containing a set of International access keys.
hcpNatKeys	HcpNatKeys	1	Containing a set of national access keys. NOTE The national access keys are limited to use within the country of issue of the health-care card.

Table 13 — The specification of individual entities within the object PatCardHolderVer

Object name	Data Type	Multiplicity	Comments
verificationMethod	CodedData	1	Contains coded data specifying the methodology to be used in conjunction with the data contained within verificationData to obtain verification that the identity of the record person is as claimed.
verificationData	BIT STRING	1	

Table 14 — The specification of individual entities within the object PatSignatureFunctionData

Object name	Data Type	Multiplicity	Comments
patSignAlgorithmID	RefPointer	1	This points to a line in the algorithm table.
patSignKeyID	RefPointer	1	This points to a line in the key table.

Table 15 — The specification of individual entities within the object PatEncryptionData

Object name	Data Type	Multiplicity	Comments
patEncAlgorithmID	RefPointer	1	This points to a line in the algorithm table.
patEncKeyID	RefPointer	1	This points to a line in the key table.

Table 16 — The specification of individual entities within the object KeyTable

Object name	Data Type	Multiplicity	Comments
Key	OCTET STRING	1..*	

Table 17 — The specification of individual entities within the object AlgorithmTable

Object name	Data Type	Multiplicity	Comments
Algorithm	OCTET STRING	1..*	

Annex A
(normative)

ASN.1 data definitions

```
CommonDataTypes DEFINITIONS ::= BEGIN
EXPORTS AccessoryAttributes, CodingSchemesUsed, CodedData, RefPointer
PatientHealthCardSecurityData;
-- RefPointer data object
RefPointer ::= SEQUENCE OF RefTag
RefTag ::= INTEGER   -- This object can hold the ASN.1-tag of another object
-- CodingSchemesUsed and CodingScheme data objects
CodingSchemesUsed ::= SEQUENCE OF CodingScheme
CodingScheme ::= SEQUENCE
{
   codeIdentifier  [0] OCTET STRING  (SIZE (64)), -- Size is changed from 6 to 64 to
                                                  -- allow OIDs here
   codeLength      [1] INTEGER,
   comment         [2] OCTET STRING (SIZE (1..20)) OPTIONAL
}
-- CodedData data object
CodedData ::= SET
{
   codingSchemeRef  [0] RefPointer, -- CodingSchemeRef is a RefPointer pointing at a
                     -- value that identifies a particular coding scheme
                     -- within the object coding schemes used.
                     -- If CodingSchemeRef = 0, then the coding scheme
                     -- is implicit in this International Standard.
   codeDataValue    [1] OCTET STRING,
   codeDataFreeText [2] OCTET STRING   OPTIONAL
}

-- AccessoryAttributes data object

AccessoryAttributes ::= SET
{
   date1               [0] UTCTime     OPTIONAL,
   placePerson1        [1] RefPointer  OPTIONAL, -- This is a pointer to a person/place
                                                 -- identifier
                                                 -- stored elsewhere
   placePerson2        [2] RefPointer OPTIONAL,  -- This is a pointer to a person/place
                                                 -- identifier
                                                 -- stored elsewhere
   personid3           [3] PersonCode OPTIONAL,
   securityLevelPointer[4] SecurityLevels OPTIONAL, -- Points to SecurityLevels
                                                    -- table
   compressionMethod   [5] CompressMethodData OPTIONAL, -- Points to CompressMethodData
   objectSecAttributes [6] SET OF SecurityServices OPTIONAL
}
PersonCode ::= SET
   {
      personCode    [0] RefPointer, -- This is a pointer to a person identifier
                                    -- stored elsewhere
      personText    [1] OCTET STRING (SIZE(0..30))
   }
SecurityServices ::= SEQUENCE
{
   signatureAlgorithmID      [0] RefPointer  OPTIONAL, -- This points to the
                                                       -- algorithm table.
   signatureVerificationKeyId [1] RefPointer OPTIONAL, -- This points to the
                                                       --signature
                                                       -- verification key.
   digitalSignature           [2] BIT STRING,
   encryptionAlgorithmID      [3] RefPointer, -- This points to the algorithm table.
   encryptionKeyId            [4] RefPointer  -- This points to the encryption key.
```

```
}
SecurityLevels ::= SEQUENCE
{
   readSecAttribute           [0] SecAttData OPTIONAL,
   writeSecAttribute          [1] SecAttData OPTIONAL,
   updateSecAttribute         [2] SecAttData OPTIONAL,
   eraseSecAttribute          [3] SecAttData OPTIONAL
}
SecAttData ::= SEQUENCE
{
   always             [0] BOOLEAN,   -- True = Always available, if false
                                     -- functionality is protected
                                     -- and is controlled by one or more of
                                     -- the underlying parameters.
   extAuth            [1] BOOLEAN,   -- True = Requires external authentication.
   holdAg             [2] BOOLEAN,   -- True = Requires data-card holder agreement.
   origAg             [3] BOOLEAN    -- True = Can only be done by originator
                                     -- of data element.
}
CompressMethodData ::= SET OF CodedData
--  Patient Healthcard Security data set
PatientHealthCardSecurityData ::= SET
{
   patCardHolderVer           [0] PatCardHolderVer,
   devClassAuthenticateData   [1] DevClassAuthenticateData,
   patEncryptionData          [2] PatEncryptionData,
   patSignatureFunctData      [3] PatSignatureFunctData,
   hcpAuthenticateData            [4] HcpAuthenticateData,
   keyTable                   [5] KeyTable,
   algorithmTable             [6] AlgorithmTable
}
PatCardHolderVer ::= SET
{
   verificationMethod         [0] CodedData,
   verificationData           [1] BIT STRING
}
DevClassAuthenticateData ::= SET
{
   authenticationMethod       [0] CodedData,
   devAuthenticationKey       [1] BIT STRING
}
PatEncryptionData ::= SET
{
   patEncAlgorithmID [0] RefPointer, -- This points to a line in the algorithm table.
   patEncKeyID       [1] RefPointer -- This points to a line in the key table.
}
PatSignatureFunctData ::= SET
{
   patSignAlgorithmID [0] RefPointer, -- This points to a line in the algorithm table.
   patSignKeyID       [1] RefPointer -- This points to a line in the key table.
}
HcpAuthenticateData ::= SET
{
   hcpAuthentMethod    [0] CodedData,
   hcpIntKeys          [1] HcpIntKeys,
   hcpNatKeys          [2] HcpNatKeys
}
HcpIntKeys ::= SEQUENCE
{
   hcpIntKey           [0] BIT STRING
}
HcpNatKeys ::= SEQUENCE
{
   hcpNatKey           [0] BIT STRING
}
AlgorithmTable ::= SEQUENCE OF AlgorithmID
AlgorithmID ::= OCTET STRING
KeyTable ::= SEQUENCE OF Key
Key ::= OCTET STRING
HcpKeyID ::= OCTET STRING (SIZE (1))
END
```

Bibliography

[1] ISO 3166-1, *Codes for the representation of names of countries and their subdivisions — Part 1: Country codes*

[2] ISO 7498-2:1989, *Information processing systems — Open Systems Interconnection — Basic Reference Model — Part 2: Security Architecture*

[3] ISO/IEC 7810, *Identification cards — Physical characteristics*

[4] ISO/IEC 7816, *Identification cards — Integrated circuit(s) cards with contacts*

[5] ISO/IEC 9798-1:2010, *Information technology — Security techniques — Entity authentication — Part 1: General*

[6] ISO 639-1, *Codes for the representation of names of languages — Part 1: Alpha-2 code*

[7] ISO 639-2, *Codes for the representation of names of languages — Part 2: Alpha-3 code*

[8] ISO 4217, *Codes for the representation of currencies and funds*

[9] ISO/IEC 5218, *Information technology — Codes for the representation of human sexes*

[10] ISO 6093, *Information processing — Representation of numerical values in character strings for information interchange*

[11] ISO/IEC 6523-1, *Information technology — Structure for the identification of organizations and organization parts — Part 1: Identification of organization identification schemes*

[12] ISO 8601, *Data elements and interchange formats — Information interchange — Representation of dates and times*

[13] ISO/IEC 8824-1, *Information technology — Abstract Syntax Notation One (ASN.1): Specification of basic notation — Part 1*

[14] ISO/IEC 8859-1, *Information technology — 8-bit single-byte coded graphic character sets — Part 1: Latin alphabet No. 1*

[15] ISO/IEC 9594-8, *Information technology — Open Systems Interconnection — The Directory: Public-key and attribute certificate frameworks — Part 8*

[16] ISO/IEC 10181-2, *Information technology — Open Systems Interconnection — Security frameworks for open systems: Authentication framework — Part 2*.

[17] ISO 20301, *Health informatics — Health cards — General characteristics*

[18] CCITT, Numbering plan for the international telephone service

ICS 35.240.80

Price based on 15 pages