

**HC 4016**



**NETLINK Requirements for Interoperability**

NK/2/ZI/A/3/2.1

Task:	
Work-package:	2
Reference:	NK/2/ZI/A/3/2.1
Date of last change:	01.06.2000
Authors:	WP 2 members (Canada/Quebec: D. Morency, J. Sureaud; France: C. Michel, N. Nader, J. Sauret; Germany: G. Brenner, H.-G. Büttner, J. Sembritzki, B. Struif; Italy: G. Meazzini), editors: ZI, H.-G. Büttner, J. Sembritzki
Stage:	Version 2.1

<b>1 TABLE OF CONTENT</b>
---------------------------

<b><i>1 Table of Content</i></b>	<b>2</b>
<b><i>2 Executive Summary</i></b>	<b>4</b>
<b>2.1 Executive Summary</b>	<b>4</b>
<b>2.2 Guidelines how to read the document</b>	<b>4</b>
<b>2.3 Document history</b>	<b>5</b>
<b><i>3 Global overview</i></b>	<b>8</b>
<b><i>4 PDC access (free)</i></b>	<b>9</b>
<b>4.1 Scope</b>	<b>9</b>
<b>4.2 Scenario(s)</b>	<b>10</b>
<b>4.3 Technical components (architectural)</b>	<b>10</b>
<b>4.4 Data and flows</b>	<b>10</b>
<b>4.5 Interoperability needed</b>	<b>10</b>
<b>4.6 Possible evolution</b>	<b>19</b>
<b>4.7 Requirements for technical components</b>	<b>20</b>
<b><i>5 PDC access (protected)</i></b>	<b>21</b>
<b>5.1 Scope</b>	<b>21</b>
<b>5.2 Scenario(s)</b>	<b>22</b>
<b>5.3 Technical components (architectural)</b>	<b>22</b>
<b>5.4 Data and flows</b>	<b>23</b>
<b>5.5 Interoperability needed</b>	<b>35</b>
<b>5.6 Possible evolution</b>	<b>37</b>
<b>5.7 Requirements for technical components</b>	<b>37</b>
<b><i>6 Secure messaging</i></b>	<b>39</b>
<b>6.1 Scope</b>	<b>39</b>
<b>6.2 Scenario(s)</b>	<b>40</b>
<b>6.3 Technical components (architectural)</b>	<b>41</b>
<b>6.4 Data and flows</b>	<b>52</b>
<b>6.5 Interoperability needed</b>	<b>57</b>
<b>6.6 Possible evolution</b>	<b>60</b>
<b>6.7 Requirements for technical components</b>	<b>61</b>
<b><i>7 DB access</i></b>	<b>68</b>
<b>7.1 Scope</b>	<b>68</b>
<b>7.2 Scenarios</b>	<b>70</b>

<b>7.3 Technical components (architectural)</b>	<b>74</b>
<b>7.4 Data and flows</b>	<b>74</b>
<b>7.5 Interoperability needed</b>	<b>75</b>
<b>7.6 Possible evolution</b>	<b>77</b>
<b>7.7 Requirements for technical components</b>	<b>77</b>
<b>8 Procedure simplification</b>	<b>78</b>
<b>8.1 Scope</b>	<b>78</b>
<b>8.2 Scenario</b>	<b>79</b>
<b>8.3 Technical components (architectural)</b>	<b>81</b>
<b>8.4 Data and flows</b>	<b>81</b>
<b>8.5 Interoperability needed</b>	<b>81</b>
<b>8.6 Possible evolution</b>	<b>85</b>
<b>8.7 Requirements for technical components</b>	<b>85</b>
<b>9 Summary of Requirements for technical Components</b>	<b>86</b>
<b>9.1 Scope</b>	<b>86</b>
<b>9.2 Requirements for technical components</b>	<b>86</b>
<i>A Standards, regulations, ongoing work, national projects (informative)</i>	<b>94</b>
<i>B Involved parties nationally (informative)</i>	<b>101</b>
<i>C Glossary (informative)</i>	<b>105</b>
<i>D The EU/G7 Interoperability dataset - Definition (normative) and NETLINK revision marks (informative)</i>	<b>108</b>
<i>E Recommendations for Restrictions for a Core Data Set of EU/G7 - Interoperability - data set (informative)</i>	<b>137</b>
<i>F Presentation/Visualisation of G7-Interoperability-dataset (informative)</i>	<b>142</b>
<i>G Secure messaging- Regulation aspects - France (informative)</i>	<b>149</b>
<i>H DB access - Quebec's example (informative)</i>	<b>150</b>

## 2 EXECUTIVE SUMMARY

### 2.1 *Executive Summary*

This document was prepared by the members of work package 2 of the NETLINK project.

In line with the overall objective of the project to work on recommendations for the implementation of interoperable data card systems and intranet solutions this group took over the task to develop secure communication procedures that can be used in connection with networks and/or card systems in a health care system as well as inside a country or across borders of the countries represented in the consortium (France, Germany, Italy and Canada/Québec).

These solutions shall be based in particular on standards and tools like card consented data sets, healthcare professional cards and encryption algorithms. They are also meant to be simple and based on the real situation of the countries involved, independent from card operating systems, card readers and architectures and using tools available on the market.

Furthermore it is the objective of this document to specify the complete infrastructure: procedures, card terminals, HPC's, PDC's, security architecture, network protocols etc. and if not already existent, to propose to the standardisation bodies these procedures or parts of them as an input for their standardisation work.

The recommendations and guidelines elaborated by WP 2 will be the basis for other work packages for demonstration of interoperability for the provision of confidentiality services at an international level, especially for the NETLINK pilot sites. The WP 2 results will also be used for further dissemination to other European countries and even outside Europe (e.g. G8 SP6).

Even though NETLINK pilot sites or other projects will not fulfil or follow all the recommendations and specifications made in the document it can help to design an application on a certain level and at the same time assure the facility of a gradual migration towards the described cross-border interoperability.

From that point of view it is obvious, that the specifications made in this document can only be an offer to others, inside or outside the project, to ensure or at least support the integration and interoperability of already existing applications and tools. Therefore the document is structured in a modular way, describing scenarios the group felt, that this could be the ones most urgently needed. Each scenario is described by the same chapters, trying to avoid references to other scenarios. References to data sets or others needed by more than one scenario are shifted to annexes. This approach allows the reader to focus on the scenario he is interested in, without reading the whole document.

The group is aware of the fact, that this document has to be worked out or even modified furthermore after having received feedback from the NETLINK pilot sites or users and experts outside the NETLINK project. It therefore describes the possibilities of having interoperable secure communication procedures based on the strategies and existing tools and applications of each country of the consortium, known at the time of creation of this document.

### 2.2 *Guidelines how to read the document*

In order to help the reader of the document to quickly identify his/her approach of interest, it is suggested to choose one of the following:

- **Technical scenarios.** This area includes the chapters describing the technical architecture proposed for getting the interoperability:
  - 04 PDC access (free). PDC emergency data have to be readable by different users independently of their hardware and software.

- 0 5 PDC access (protected). There may be data stored on a PDC which have to be readable and/or writeable in a protected way by different users independently of their hardware and software.
  - 0 6 Secure messaging. The exchange of digitally signed and encrypted e-mails between Health Professionals located in various countries.
  - 0 7 DB access. To extend the storage capacity of the smart card by making use of telecommunication network and remote databases.
  - 0 9 Summary of Requirements for technical Components. To ensure consistency of the whole architecture.
- **Functional scenarios.** This area describes the objectives that can be achieved by introducing the health card as a component of the national health systems.
- 0 8 Procedure simplification. It deals with secure identification of patients and physicians, procedures simplification and usage of internationally recognised health data in emergency and first aid. It is based on the technical architecture and on the data defined in the first and third areas.
- **Data objects.** This area describes the data used in different scenarios.
- *Data – Annex 0.* The interoperability of data is based on the definition of the G7-Interoperability-dataset; this annex lists the dataset with the NETLINK proposals for modification.
- **Informative.** This area includes information useful to better understand the document:
- *Standards – Annex 0.* The annex lists standards, regulations, ongoing works and national projects.
  - *Involved parties nationally – Annex 0.* The annex provides information about persons and/or bodies in charge for the national health cards projects.
  - *Glossary – Annex 0.* It explains the acronyms used in the document.
  - *Core data Set – Annex 0.* A proposal is listed for a reduced dataset, useful for saving space in the card.
  - *Visualisation – Annex 0.* It contains recommendations for the visualisation of the health card data to achieve a common layout.

### 2.3 Document history

NL/2/ZI/A/3/0.2 22.10.98	<ul style="list-style-type: none"> <li>• based on Interoperability document (Struif, Sembritzki) and French and Italian contributions according to NETLINK WP2 meeting on 29./30.09.1998</li> </ul>
NL/2/ZI/A/5/0.25 24.11.98	<ul style="list-style-type: none"> <li>• reformatting according to WP6 guidelines</li> <li>• integrating documents (inclusive some editorial work):             <ul style="list-style-type: none"> <li>- NK/2/MOT/R/1/0.1</li> <li>- contribution_to_Interoperability_v02.doc (2<sup>nd</sup> version)</li> </ul> </li> </ul>
NK/2/ZI/A/3/0.3	<ul style="list-style-type: none"> <li>• renumbering of the document</li> <li>• editorial corrections</li> <li>• integrating documents (inclusive some editorial work):             <ul style="list-style-type: none"> <li>- NK/2/FIN/D/8/2.1</li> <li>- French contribution (concerning secure messaging) (05.01.1999)</li> <li>- German work on chapter 4</li> </ul> </li> </ul>

	<ul style="list-style-type: none"> <li>• integrating decisions of 2<sup>nd</sup> WP 2 meeting</li> </ul>
NK/2/ZI/A/3/0.5	<ul style="list-style-type: none"> <li>• integrating documents (inclusive some editorial work): <ul style="list-style-type: none"> <li>- NK/2/FIN/D/8/2.1 (WP2_procedure.doc instead of WP2_contribution.doc)</li> <li>- German work on chapter 4 taking NK/2/GIE/D/10/1.1 into account</li> <li>- some minor changes in chapter 5</li> </ul> </li> </ul>
NK/2/ZI/A/3/0.51	<ul style="list-style-type: none"> <li>• editorial correction of chapter 8 (tables, numbering of 1.6.2.4 to 8.6.2.4)</li> </ul>
NK/2/ZI/A/3/0.75	<ul style="list-style-type: none"> <li>• integrating decisions of 3<sup>rd</sup> WP 2 meeting</li> <li>• integrating documents (inclusive some editorial work): <ul style="list-style-type: none"> <li>- NK/2/MOT/A/2/0.4</li> <li>- French contribution (concerning secure messaging) (12.02.1999)</li> <li>- German work on chapter 5</li> <li>- NK/2/FIN/D/8/2.2 (WP2_procedure.doc)</li> </ul> </li> </ul>
NK/2/ZI/A/3/0.8	<ul style="list-style-type: none"> <li>• renumbering (ZI instead of ZID)</li> <li>• extending annex B (taking NK/2/MOT/A/2/0.4 into account)</li> <li>• integrating documents (inclusive some editorial work): <ul style="list-style-type: none"> <li>- German work on chapter 3 (executive summary)</li> <li>- German work on chapter 5 (scope)</li> <li>- NK/2/FIN/D/8/2.3 (WP2_procedure.doc)</li> <li>- harmonisation of proposals for modification (annex E)</li> <li>- German work on annex F</li> </ul> </li> </ul>
NK/2/ZI/A/3/0.9	<ul style="list-style-type: none"> <li>• integrating documents (inclusive some editorial work): <ul style="list-style-type: none"> <li>- German work on chapter 4 and 5</li> <li>- NK/2/MOT/A/2/0.5</li> <li>- French contribution (concerning secure messaging) (01.03.1999)</li> <li>- Italian contributions (chapter 2.2, NK/2/FIN/D/8/2.3 (WP2_procedure.doc), annexes A, B, C, D)</li> </ul> </li> <li>• integrating decisions of 4<sup>th</sup> WP 2 meeting</li> </ul>
NK/2/ZI/A/3/0.95	<ul style="list-style-type: none"> <li>• editorial work (changing 0.9 to 0.95) taking the French comments and some peer comments into account</li> </ul>
NK/2/ZI/A/3/1.0	<ul style="list-style-type: none"> <li>• editorial work (changing 0.95 to 1.0) taking the peer comments into account</li> </ul>
NK/2/ZI/A/3/1.1	<ul style="list-style-type: none"> <li>• editorial work (changing 1.0 to 1.1, date, ...)</li> <li>• adding missing pages of table 42</li> <li>• integration of RID</li> <li>• deleting of not existing ISO 7816-11 in annex A</li> <li>• „country of birth“ MANDATORY in all occurrences of the proposed dataset</li> </ul>
NK/2/ZI/A/3/1.25	<ul style="list-style-type: none"> <li>• integrating decisions of 5<sup>th</sup> WP 2 meeting</li> </ul>
NK/2/ZI/A/3/1.3	<ul style="list-style-type: none"> <li>• integrating decisions of 5<sup>th</sup> WP 2 meeting</li> <li>• integrating parts of a minimum command set and new version of chapter</li> </ul>

	6
NK/2/ZI/A/3/2.0	<ul style="list-style-type: none"><li>• editorial work (changing 1.3 to 2.0, date, ...)</li><li>• integrating decisions of 6<sup>th</sup> EC meeting</li></ul>
NK/2/ZI/A/3/2.1	<ul style="list-style-type: none"><li>• correcting tables 41, 42 and 43 of Annex D (refer to G8 Miami meeting results)</li></ul>

For comments or more info, please contact:

Noel Nader – Noel.Nader@sesam-vitale.fr

Juergen Sembritzki - JSembritzki@KBV.DE

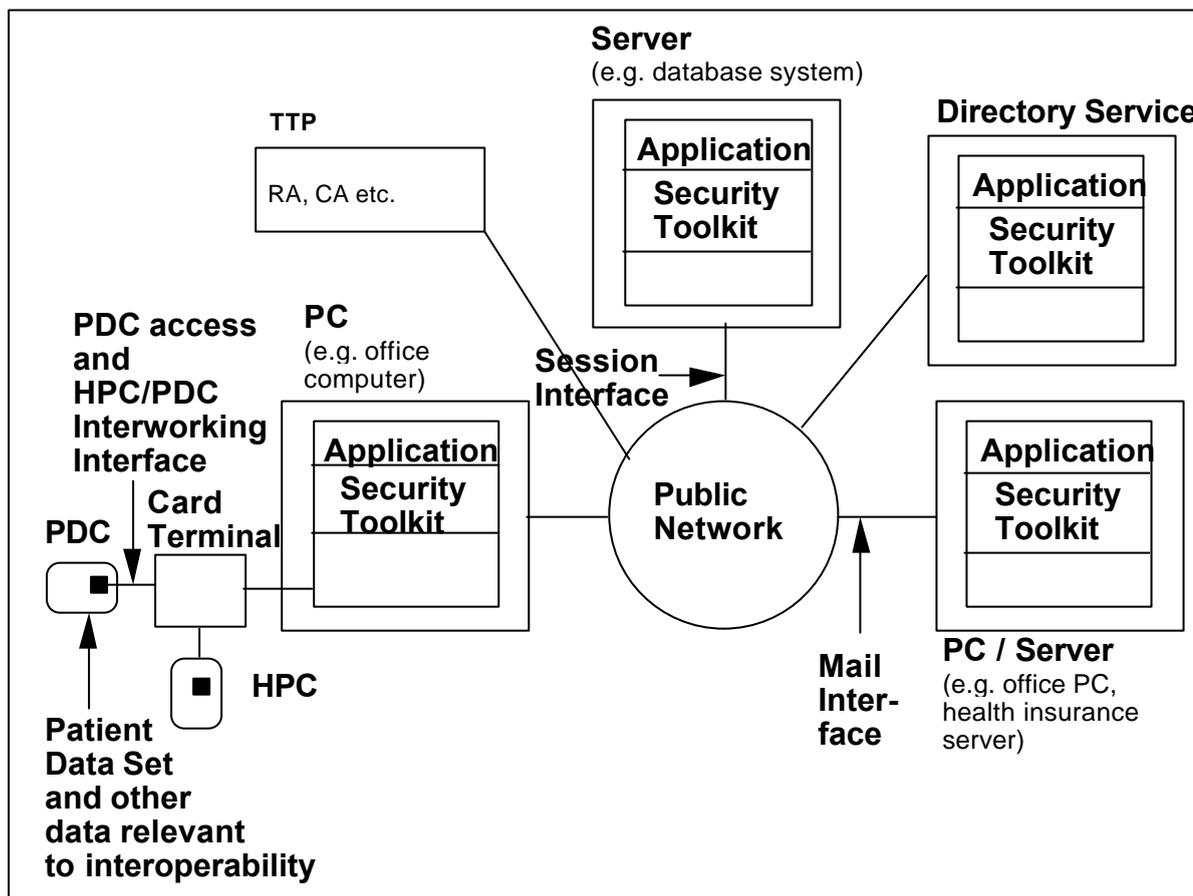
Denis Morency – denis.morency@ramq.gouv.qc.ca

Giulio Meazzini – g.meazzini@finsiel.it

### 3 GLOBAL OVERVIEW

This document describes topics where interoperability is mandatory for achieving the respective service. The basis for the consideration is shown in the subsequent figure. For reasons of simplicity the figure shows only one instance of each component but there might be for example more than one TTP or card terminal.

**Fig. 1 Interoperability Scenario**



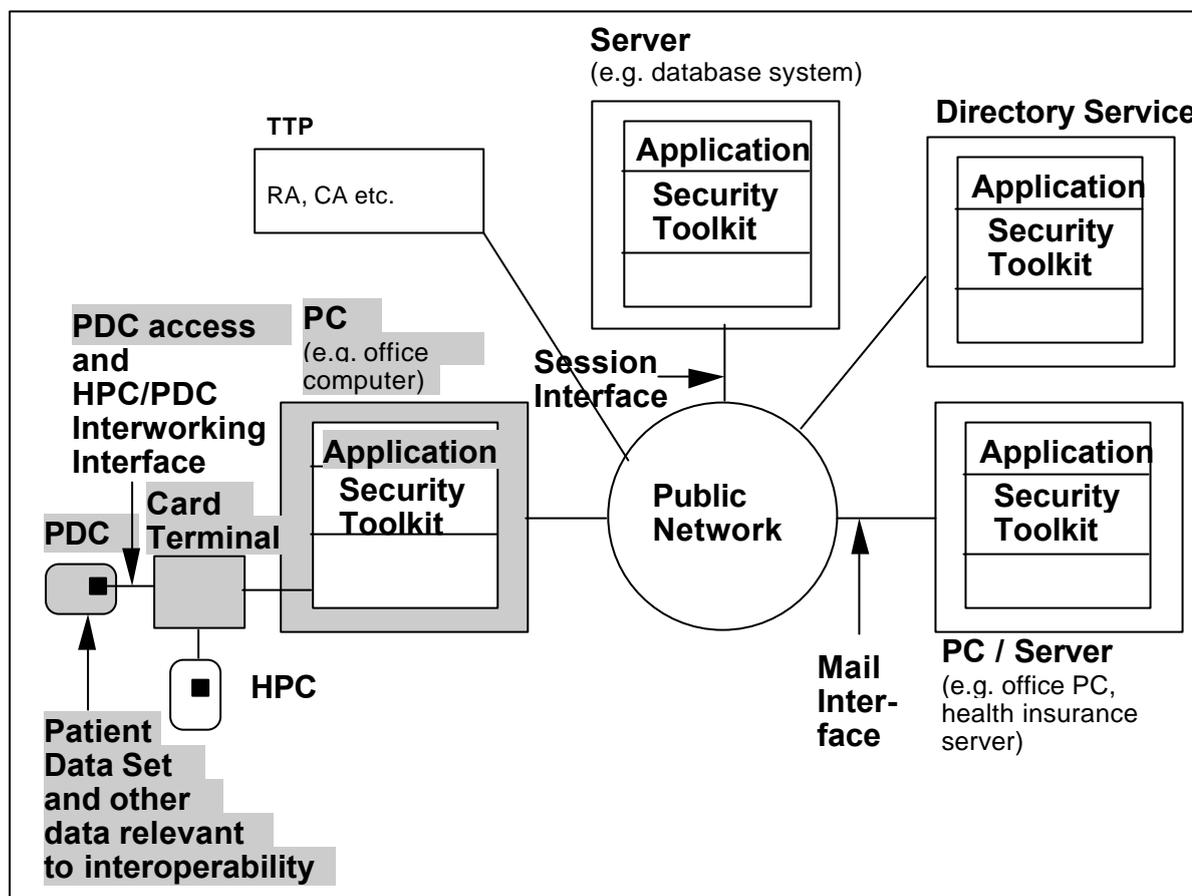
NETLINK has identified five scenarios where interoperability is needed.:

1. PDC access (free)
2. PDC access (protected)
3. secure messaging
4. DB access
5. procedure simplification

Following each scenario is described in detail and recommendations for achieving interoperability are given. Each main chapter starts with the figure above in which for each scenario the relevant components are highlighted.

## 4 PDC ACCESS (FREE)

**Fig. 2 PDC access (free) Interoperability Scenario**



### 4.1 Scope

The issue of healthcard interoperability in the sense of NETLINK is a functional interoperability of healthcard systems. The emergency data of a PDC have to be readable by different users independently of their hardware and software.

In order to achieve this technical interoperability, common functions and/or data requirements and an interoperability agreement must be implemented. In the following chapters the requirements for the technical interoperability will be specified. The other prerequisites (i.e. interpreting data, legislation concerning cross border interoperability etc.) are discussed in „EU/G7 Healthcards - WG7, Interoperability of Healthcard Systems, Part 1 General Concepts“ (see page 98 and annex 0 D The EU/G7 Interoperability dataset - Definition (normative) and ).

Nevertheless it has to be mentioned here that data has to be coded in order to achieve avoiding language problems which may cause problems in the functional interoperability.

Note that it is outside the scope of this chapter to give recommendations concerning

- trusting the data on the card; this includes
  - authentication of the holder of the PDC,
  - the use of a HPC for card to card authentication,

- the reliability of the data (this means the reliability of the original data, it is stated that the integrity of data using smartcards is good)
- the completeness of the patient data; nevertheless all existing data shall be displayable.
- regulations concerning the access of data (the access described here is technically free but there might be organisational additional requirements like an explicit patient consent in some countries)
- non emergency data.

## 4.2 Scenario(s)

The scenario is:

1. The availability of data of a patient coming from a foreign country should be improved in an emergency case by its patient data card with free accessible data.

This means the reading access of data from a PDC without any security feature (writing of data is treated in chapter 0 5 PDC access (protected), this also includes the updating of the free readable data).

## 4.3 Technical components (architectural)

Technical components are:

1. PDC
2. Card terminal
3. PC/Host

## 4.4 Data and flows

The software for reading and visualising the data must be able to handle the complete G7-dataset as mentioned in the scope. The dataset consist of three groups with some sub-groups:

Group	Sub-Groups
Card Data	cardIssuerIdentifier , cardHolderIdentifier, cardIdentifier, cardStatus, cardApplicationIdentification
Administrative Data	patientIdentification, nameDetails, languageDetails, birthDetails, addressDetails, contactDetails, insuringBodies
Clinical Data	codedClinicalDetails, bloodGroupTransfusionDetails, immunisationDetails, medicationDetails, clinicalAddressDetails, opticalPrescriptionDetails, updateDetails

## 4.5 Interoperability needed

### 4.5.1 Subject of Interoperability

Interoperability is needed:

on PDC-side:

- conventions for physical and logical communication with a PDC on the physical layer and the transmission layer
- conventions for reading free accessible data including application selection, file selection etc.

- conventions for the structure and content of the free accessible patient data set (interoperable data set)

on card terminal-side:

- conventions for physical and logical communication with a PDC on the physical layer and the transmission layer

on PC/Host-side:

- conventions for physical and logical communication with a PDC on the physical layer and the transmission layer

on software-side:

- recommendations for displaying the read PDC data

## 4.5.2 Conventions and Standards

### 4.5.2.1 Conventions for the physical layer and the transmission layer

#### 4.5.2.1.1 Physical layer

Today Patient Data Cards mainly are contact based cards with physical characteristics according to ISO/IEC 7816-1. The location and dimensions of the contacts shall comply with ISO/IEC 7816-2. For encoding the data bits on the I/O line the „direct convention“ is recommended.

#### 4.5.2.1.2 ATR, PPS and Transmission Layer

The Answer-to-Reset (ATR) shall comply with ISO/IEC 7816-3 (2<sup>nd</sup> edition).

It is recommended, that PDC's support the Protocol Parameter Selection (PPS) e.g. to be able to transmit data with higher speed.

The transmission protocol supported by the card shall be either

- the half-duplex character transmission protocol T=0 or
- the half-duplex block transmission protocol T=1 or
- both.

If T=1 is used, chaining is mandatory. The following simplifications are allowed:

- NAD Byte: not interpreted (NAD shall be set to '00')
- S-Block ABORT: not used
- S-Block VPP state error: not used

For T=1 the Information Field Size Card (IFSC) shall be indicated in the ATR (Character TA3, recommended value: at least '80' = 128 Bytes).

The Information Field Size Device (IFSD) shall be transmitted by the IFD immediately after ATR, i.e. the IFD shall send at once after ATR the S-Block IFS Request which has to be answered by an HPC with S-Block IFS Response. The recommended value for IFSD is 254 Bytes.

As described in ISO 7816-3, the ATR is composed of one initial character followed by a maximum of 32 characters defined as following :

- one Format Byte describing the ATR format (mandatory)
- Interface Bytes describing communication parameters (optional)
- Historical Bytes (maximum 15 characters) which may help to identify the card (optional)
- one Check Byte (conditional)

ISO 7816-4 describe Historical Bytes when used. They are composed as following :

- Category Indicator (1 mandatory character)
- COMPACT-TLV data objects (optional)
- Status Information (3 characters, conditional)

ISO 7816-4 standard describe the Historical Bytes when the Category Indicator value is '00', '10', or '8X'. When the Category Indicator value is '00', ISO 7816-4 offers 7 data object to be coded in COMPACT-TLV that can be used in the Historical Bytes. These data objects are described in the following table.

Code of the data object	Name of the data object
1	Country code and national data
2	Identification of the card issuer
3	Card service data
4	Initial access data
5	Card issuer's data
6	Pre-issuing data
7	Card capabilities

The data object '3' denotes the methods available for supporting the application-independent card services as defined in ISO 7816-4. When this data object is not present in the Historical Bytes, the card supports only the implicit application selection, while the application-independent card services as defined in ISO 7816-4 may not be supported. As a consequence, it is then necessary to know the card OS specific services to access to it (for instance : the existing Vitale 2 OS does not support the application-independent card services as defined in ISO 7816-4).

NB : When using PC/SC (or similar architecture), it may be envisaged to define an ICC service provider supporting only the application-independent card services as defined in ISO 7816-4. Thus, using such an ICC service provider, it is then possible to access cards of any type compliant to these specifications. When using PC/SC (or similar architecture), to be able to access to cards that do not support the application-independent card services as defined in ISO 7816-4, it is required to have a specific ICC service provider (identified thanks to the ATR).

PDC capabilities (i.e. supported application-independent card services) can be unambiguously determined using Historical Bytes and, when present, the Initial Data String ('4x' object in Historical Bytes).

If the PDC supports application-independent card services as defined in ISO/IEC 7816-4 :

- when the Initial Data String is not present (i.e. only the Historical Bytes can be used), then :
  - 'Card service data' object is present in Historical Bytes (tag '3x') and the other objects can also be used
- when the Initial Data String is present, then :

- Initial Data String should be compliant to ISO/IEC 7816-6
- either 'Card service data' object is present in Historical Bytes (tag '3x') and the other objects can also be used
- or the 'Card service data' object is indicated in the Initial Data String (tag '43')

If the PDC does not support application-independent card services as defined in ISO/IEC 7816-4 :

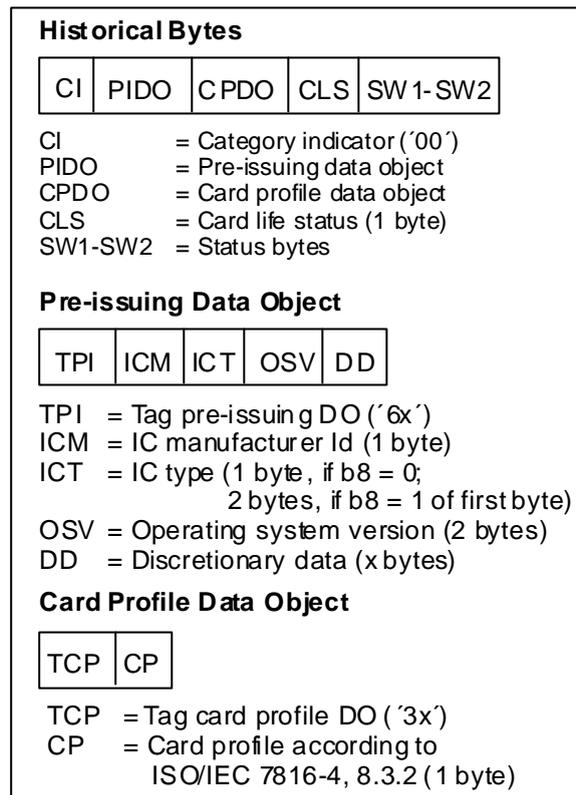
- when the Initial Data String is not present (i.e. only the Historical Bytes can be used), then :
  - 'Card service data' object is not present
  - 'Identification of the card issuer' ('2x' object in Historical Bytes) should value the registered IIN for the PDC as defined in ISO/IEC 7812
  - 'Card Issuer's data' ('5' object in Historical Bytes) or 'Pre-issuing data' ('6x' object in Historical Bytes) objects can be used to uniquely identify the type of card
- when the Initial Data String is present, the previous solution can be used and another one is :
  - Initial Data String should be compliant to ISO/IEC 7816-6
  - 'Card service data object' is not present
  - the registered IIN for the PDC as defined in ISO/IEC 7812 can be found
    - either in the 'Identification of the card issuer' ('42' object in Initial Data String)
    - or in the 'Application Identifier' ('4F' object in Initial Data String) if the AID is based on the IIN
  - additional data can be used to uniquely identify the type of card from Historical Bytes or the Initial Data String according to the PDC issuer's decisions. 'Pre-issuing data' should be preferably used.

Acceptance of PDC that support application-independent card services as defined in ISO/IEC 7816-4 (Netlink preferred solution) can be made possible via „generic“ drivers that follow the rules mentioned above.

Acceptance of PDC that do not support application-independent card services as defined in ISO/IEC 7816-4 is more complex as it requires agreements between PDC issuers and software developers.

For the coding of the Historical Bytes, an example is provided below :

CI	=	'00' according to ISO/IEC 7816-4
TPI	=	'6x' according to ISO/IEC 7816-4 (x codes the length of the DO)
ICM	=	IC Manufacturer Id (see table 1)
ICT	=	Coding manufacturer specific
OSV	=	Coding manufacturer specific
DD	=	Coding manufacturer specific (usually not used)
TCP	=	'3x' according to ISO/IEC 7816-4 (x codes the length of the DO)
CP	=	Coding according to ISO/IEC 7816-4 (i.e. '80' for 'direct application selection')
CLS	=	Card Life Cycle (Default value '00')

**Fig. 3: Structure of the Historical Bytes****table 1: ICM coding**

ICM	IC Manufacturer according to ISO/IEC 7816-6/AM 1
'01'	Motorola
'02'	STMicroelectronics
'03'	Hitachi
'04'	Philips Semiconductors
'05'	Siemens
'06'	Cyline
'07'	Texas Instruments
'08'	Fujitsu
'09'	Matsushita
'0A'	NEC
'0B'	Oki
'0C'	Toshiba
'0D'	Mitsubishi
'0E'	Samsung
'0F'	Hyundai

'10'	LG
------	----

#### 4.5.2.2 Conventions for file selection and data access

There are different possibilities for an interoperable data access:

- using an identical file structure and file id's (and/or names);
- using a special „driver“ for all NETLINK cards:
  - within the G7-Interoperability-study the access of the card data is hidden by the use of proprietary/project-specific health card server; the data interoperability is given on top of the server
  - within the PC/SC-specifications<sup>1</sup> the access of the card data can be hidden by the use of
    - \* a common service provider and agreed file names or
    - \* a NETLINK service provider with the functionality like a G7-health card server.
  - other specifications like OpenCard which hide the access too

Both solutions „identical file structure and file id's (and/or names)“ and „common service provider“ require conventions for storing the data. The data structure on the card has to be identical NETLINK-wide (for example: all data in one EF) or additionally a special software on the PC/Host for interpreting different implementations is needed.

**NETLINK decided to use identical file structure.** This solution permits to use an interface on ISO/IEC 7816-4 level or for an application in the future an interface with a common service provider.

Due to different access conditions for updating the patient's free readable data (Card Data, Administrative Data and Clinical Data), these data might be stored in different files (reading shall be free accessible). For NETLINK an extra EF with the function as a directory-file is used.

The file organisation in a PDC shall be according to ISO/IEC 7816-4. The file structure of the PDC is shown in Fig. 4. The AID is the international application identifier as defined in ISO/IEC 7816-5. An international AID has been applied for by the NETLINK management and is „A000000073“ (see also at the NETLINK web site, URL: „<http://www.sesam-vitale.fr/Projects/Netlink-G7-En/>“). The testsites are in charge of filling the card data.

An EFDIR shall contain 'ApplicationTemplate' data objects as defined in the ISO 7816-5 as described bellow :

```

ApplicationTemplate [61] ::= SET
{
  AID [4F] IMPLICIT OCTET STRING (SIZE (0..16)), -- RID + PIX
  ApplicationLabel [50] IMPLICIT OCTET STRING (SIZE (0..16)) OPTIONAL,
  Path [51] IMPLICIT OCTET STRING (SIZE (1..126)) OPTIONAL,
  CommandToPerform [52] IMPLICIT OCTET STRING (SIZE (4..127)) OPTIONAL,
  FreeData [53] IMPLICIT OCTET STRING OPTIONAL,
  DiscretionaryApplicationData [73] DiscretionaryData OPTIONAL
}

```

The 'ApplicationTemplate' data object as defined in annex 0 to be used with the NETLINK data set is at least stored in the EFDIR of the DFNetlink. The 'ApplicationTemplate' data object is used by NETLINK as

<sup>1</sup> s. annex 0 „A Standards, regulations, ongoing work, national projects (informative)“; at the moment there are different proposals for the further development or extension of the PC/SC-specifications (for example there is a French proposal concerning programmable terminals or the German UCTS (URL: <ftp://ftp.cherry.de>)); since PC/SC is not a health specific topic and currently under development WP 2 recommends to discuss the specifications at least together with the financial sector on European or international level.

follow.

An 'ApplicationTemplate' data object, with the AID NETLINK ('A000000073'), is mandatory in the EFDDir at MF level when the card don't support direct application selection by AID. In this case, the 'ApplicationTemplate' data object is used as follow :

```

ApplicationTemplate [61] ::= SET
{
  AID [4F] IMPLICIT OCTET STRING (SIZE (0...16)), -- 'A000000073' + PIX to be
      defined
  ApplicationLabel [50] IMPLICIT OCTET STRING (SIZE (0...16)) OPTIONAL, -- not used in
      NETLINK by a foreign application
  Path [51] IMPLICIT OCTET STRING (SIZE (1...126)), -- long path to the
      EFNetlink
  CommandToPerform [52] IMPLICIT OCTET STRING (SIZE (4...127)) OPTIONAL, -- not used in
      NETLINK by a foreign application
  FreeData [53] IMPLICIT OCTET STRING OPTIONAL, -- not used in NETLINK by a
      foreign application
  DiscretionaryApplicationData [73] DiscretionaryData OPTIONAL -- as defined in annex D paragraph 4
}

```

The path to the DFNetlink can be calculated from the path EFNetlink : it is the first (n-2) bytes of the path to the EFNetlink.

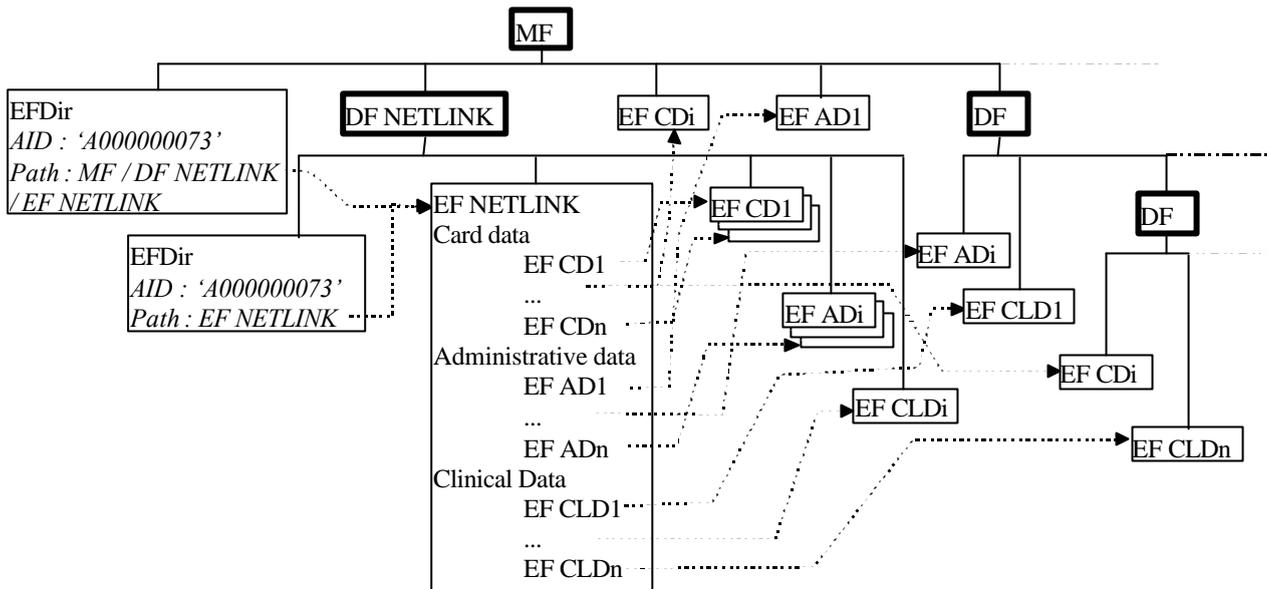
An 'ApplicationTemplate' data object, with the AID NETLINK ('A000000073'), is mandatory in the EFDDir within the DFNetlink. In this case, the 'ApplicationTemplate' data object is used as follow :

```

ApplicationTemplate [61] ::= SET
{
  AID [4F] IMPLICIT OCTET STRING (SIZE (0...16)), -- 'A000000073' + PIX to be
      defined
  ApplicationLabel [50] IMPLICIT OCTET STRING (SIZE (0...16)) OPTIONAL, -- not used in
      NETLINK by a foreign application
  Path [51] IMPLICIT OCTET STRING (SIZE (2)), -- short path to the EFNetlink
  CommandToPerform [52] IMPLICIT OCTET STRING (SIZE (4...127)) OPTIONAL, -- not used in
      NETLINK by a foreign application
  FreeData [53] IMPLICIT OCTET STRING OPTIONAL, -- not used in NETLINK by a
      foreign application
  DiscretionaryApplicationData [73] DiscretionaryData -- as defined in annex D paragraph 4
}

```

**Fig. 4 File structure of a PDC**



The access conditions to the NETLINK mandatory elementary files are :

File	File structure	File size (length of data)	Access conditions	Presence
EFDDir of the DF.NETLINK	Transparent	Open	Read: always Update: protected	Mandatory
EF.NETLINK	Transparent	Open	Read: always Update: protected	Mandatory

The PIX or some other data objects in the eFDir of the DF.NETLINK should be used to provide some administration information such as indication of the data set version.

The EF.NETLINK file size does not need to be fixed. It is possible to read the whole file and then analyse which data are useful or which are not. For that purpose the length of the data needs to be stored in the EF. Using the G7-Interoperability data set this is implicit.

The content of the EF.NETLINK is defined as the ID's and paths of the EF's containing the patient's data of the G7-interoperability-dataset :

```

NETLINK_DataSet_EFPath ::= SEQUENCE
{
  CardFileIdentification          [0] IMPLICIT SEQUENCE OF FileIdentification OPTIONAL,
  AdministrativeFileIdentification [1] IMPLICIT SEQUENCE OF FileIdentification OPTIONAL,
  ClinicalFileIdentification      [2] IMPLICIT SEQUENCE OF FileIdentification OPTIONAL
}

FileIdentification ::= SET
{
  dFName          [0] IMPLICIT OCTET STRING OPTIONAL,
  dFID            [1] IMPLICIT OCTET STRING OPTIONAL,
  eFID           [2] IMPLICIT OCTET STRING
}
    
```

Note: one of dFName and dFID is mandatory.

The coded tag value for NETLINK\_DataSet\_EFPath is '30'.

Splitting the G7-interoperability-dataset it is necessary to store the complete structure of the items (i.e. the

sequence of the TAG's according to the ASN.1-definition from the „highest“ item down to the specific data item) to allow the joining respectively the identification of the data.

The way to access to free readable data depends on the PDC operating system capability. The following gives the algorithm to be followed to access to free readable data ; this can be reused as a base specification to develop a “generic driver” that can be used to access to free readable data stored in a PDC.

- Insertion of the PDC in the IFD
- Reset of the PDC that returns the ATR
- It has to be determined whether or not the PDC supports application-independent card services as defined in ISO/IEC 7816-4 (see all explanations in the text above)<sup>2</sup>
- If the PDC supports the application-independent card services as defined in ISO/IEC 7816-4, then a “generic driver” can be used ; this driver will go through the following steps :

- Select the EF.NETLINK

There are two ways to select it depending on PDC OS capabilities, either :

- Select EFDDir in the MF
- Read EFDDir in the MF
- Get the ApplicationIdentifier object corresponding to NETLINK AID
- Get EF.NETLINK path (n is the length in bytes of the path)
- Select EF.NETLINK (composed of (n-2)/2 select DF to reach the DF NETLINK and 1 select EF)

or :

- Select DF using NETLINK AID (application selection with AID)
- Select EFDDir in DF.NETLINK
- Read EFDDir in the MF
- Get the ApplicationIdentifier object corresponding to NETLINK AID
- Get EF.NETLINK path
- Select EF.NETLINK

For NETLINK the EFDDir under the MF is not mandatory. The PC-application has to know how to select the DF.NETLINK (via name (to be specified) or AID).

- Obtain all paths to the EF's containing free readable data (see NETLINK\_DataSet\_EFPath structure)
- For all the EF's listed in the EF.NETLINK
  - Select the EF (either directly or by selecting first the DF then the EF)
  - Read the EF content
- Return PDC data to the application

When the card support direct application selection, the name of the DF NETLINK is ‘A000000073’, the Id of the DF NETLINK is given by the card issuer (see ISO 7816-5 clause 6.3.1).

---

<sup>2</sup> If the PDC does not support application-independent card services as defined in ISO/IEC 7816-4, then a “specific driver” specified by the card issuer needs to be used to access to patient's data.

Each stored dataset of the EF's is defined as a SET. This means that the first byte of the EF is '31' (i.e. „SET“ according to ISO/IEC 8825) and then the coded length of the following data (i.e. all patient data of this EF) is stored. Therefore it is also possible to read only the first bytes, analyse the number of stored patient data and read exactly the number of the stored data.

The selection of the relevant EF's is needed yet. Depending on the card operating system a selection of an EF is possible for example by path from the MF. Then the coded information can be used for one SELECT FILE. For NETLINK the selection of an EF should be made by explicit selection of DF's and EF but it might be possible to select the EF directly by path from the MF if this is stated in the ATR. It is recommended that the mapping of the DF-names to ID's is coded since the existing card operating systems normally do not support both DF-selection (by name, by ID).

Remark: To solve the selection of EF's in different DF's via a directory file is not yet standardised completely. There might be other solutions using ISO/IEC 7816-5 and/or PKCS#15 but up to now these standards do not apply exactly to the NETLINK requirements.

#### **4.5.2.3 Conventions for the structure and content of the patient data set**

The patient data set (interoperable data set) as defined in „EU/G7 Healthcards - WG7, Interoperability of Healthcard Systems, Part 3 Interoperability Specification“ shall be used. The data shall be encoded using ISO 8825. NETLINK proposes to use a modified dataset as outlined in annex 0 „D The EU/G7 Interoperability dataset - Definition (normative) and “.

Experiences with the complete dataset have shown that using a smartcard with smaller capacity can lead to problems. In this case restrictions for the dataset on the card - i.e. a core data set - have to be defined without changing the definition of the G7-specification. In annex 0 „E Recommendations for Restrictions for a Core Data Set of EU/G7 - Interoperability - data set (informative)“ the recommendations of NETLINK are outlined.

Nevertheless the year of the data element „date“ should be coded with four digits to avoid „year 2000-problems“.

#### **4.5.2.4 Displaying the dataset**

As mentioned in the scope the trustworthiness and completeness of the patient data on the card is not discussed. Nevertheless all data stored on a card have to be displayable. This means that not necessarily all data are displayed automatically but the HP application has to support the whole data model and dataset as defined and there must be a possibility for doing so.

Furthermore it is also important to have a common layout for displaying the dataset. This enables the user to get the needed information (i.e. emergency data) very quickly also if he is using a system unknown to him.

The recommendations for displaying the dataset are outlined in annex 0 „F Presentation/Visualisation of G7-Interoperability-dataset“.

## **4.6 Possible evolution**

The G7-Interoperability-Dataset has been defined in 1996. Having made experiences using the dataset it was decided on G7-level to make a further development. Currently there are proposals for modification coming from Canada, France, Germany and Italy.

The NETLINK-management is also in charge to develop a revised version but that will not be available before autumn 1999.

As mentioned the cards used as PDC's are contact based cards today. In the future it might be possible to use proximity and/or vicinity cards. In that case other standards (partly in development right now) for cards and terminals have to be considered.

Furthermore cards with other operating systems supporting for example ISO/IEC 7816-7 (Identification cards - Integrated circuit(s) cards with contacts - Part 7: Interindustry commands for Structured Card Query Language) or „Javacards“ or EMV compatible cards may be used. The accessing of data might differ from the described solution and other techniques might be needed.

PKCS#15 standard should be taken into consideration when published.

## **4.7 Requirements for technical components**

### **4.7.1 PDC**

PDC's are contact based cards with characteristics according to ISO/IEC 7816-1, 2, 3, 4, 5 and 6. The card size is ID-1. PDC's may be 5Volt- or 3Volt-cards.

PDC will at least support the following minimum subset of ISO 7816 commands with class "00":

- SELECT FILE (CLA='00', INS='A4', P1='04', P2='00', Datafield='A000000073' (Netlink application selection),...)
- SELECT FILE (CLA='00', INS='A4', P1='00', P2='00', Datafield=identifier,...) or
- SELECT FILE (CLA='00', INS='A4', P1='02', P2='00',...)
- READ BINARY (CLA='00', INS='B0', P1-P2='0000' or offset,...)

### **4.7.2 Card terminal**

The card terminals must be able to support contact-based cards with T= 0 and T = 1 transmission protocols.

The terminal shall support 5Volt- and 3Volt-cards (class AB). The terminal should support PPS and be able to transmit data with the highest speed the card indicates (this should at least be configurable).

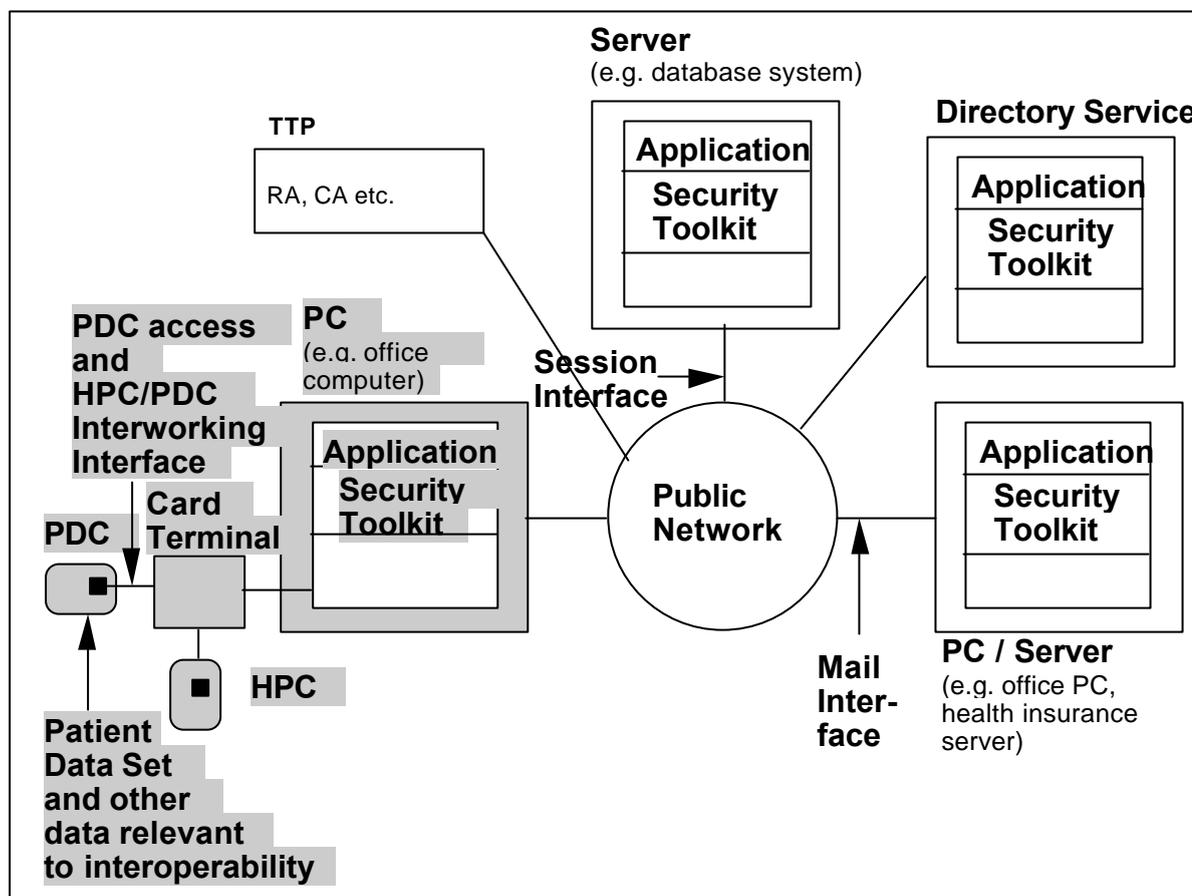
Remark: No further harmonisation is needed for card terminals.

### **4.7.3 PC/Host**

The PC/Host must be able to connect a card terminal and to support the communication with the highest transmission speed the card indicates.

## 5 PDC ACCESS (PROTECTED)

**Fig. 5 PDC access (protected) Interoperability Scenario**



### 5.1 Scope

The issue of healthcard interoperability in the sense of NETLINK is a functional interoperability of healthcard systems. There may be data stored on a PDC which have to be readable and/or writable in a protected way by different users independently of their hard- and software.

Achieving this technical interoperability, common functions and/or data requirements and an interoperability agreement must be implemented. In the following chapters the requirements for the technical interoperability will be specified. The other prerequisites (i.e. interpreting data, legislation concerning cross border interoperability etc.) are discussed in „EU/G7 Healthcards - WG7, Interoperability of Healthcard Systems, Part 1 General Concepts“ (see page 98 and annex 0 D The EU/G7 Interoperability dataset - Definition (normative) and ).

The purpose of this chapter is to show the mechanisms to be used for achieving different levels of security for reading and/or writing PDC-data. This includes holder to card authentication as well as card to card authentication by using a health professional card (HPC). The needed security infrastructure like trusted third parties, certification authorities or revocation lists has to be defined within a security policy. Because of ongoing national discussions and the development of international standards in this area (e.g. card verifiable certificates) it is impossible for NETLINK to make complete recommendations for harmonisation.

It is not in the scope to define the PDC dataset or mechanisms for identification of the patient and/or health professional or to define a harmonised classification of roles of health professionals.

## 5.2 Scenario(s)

The scenario(s) are:

1. The treatment of a patient coming from a foreign country should be supported by its patient data card with data, which require the proof of authenticity of the health professional.  
This means the reading access of data from a PDC with proof of authenticity of the health professional.
2. The writing access of data to a PDC with security feature(s).
3. The patient may have the capability to prove his consent in order to allow the HP to access to his own PDC (either to update or to read protected data).
4. The HP may have the capability to check whether the PDC is still valid or not, thus authenticating it as a PDC or even checking that it is still valid (e.g. accessing to a card revocation list).

For the HPC/PDC interaction two services are required:

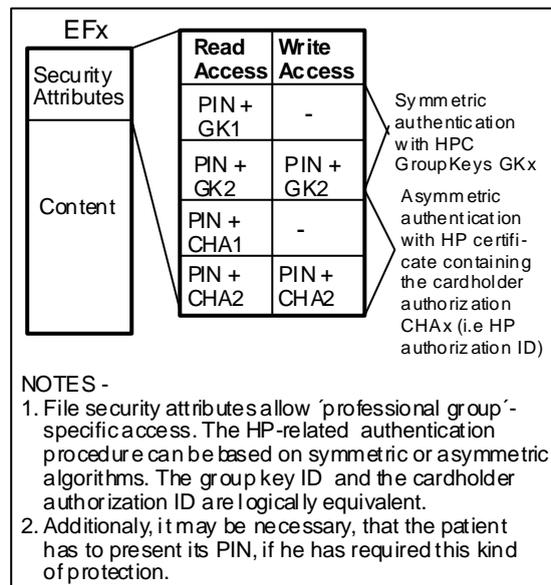
- the PDC has to prove its authenticity
- the health professional has to prove his access rights.

When proving access rights, an authentication procedure has to be performed (PIN presentation according to ISO 7816 is not described), so that in the PDC the related security status can be set, i.e.

- in symmetrical case: group key x has been successfully presented
- in asymmetrical case: certificate holder authorisation y has been successfully presented.

If after successful authentication a read or update command is performed on a file, the PDC has to verify that the respective security condition described in the security attributes of this file is fulfilled, e.g. UPDATE BINARY can only be executed, if group key x or the certificate holder authorisation y was successfully presented. In Fig. 6 an example of security conditions is outlined, whereby or an additional security condition to access the PIN of the patient may be required.

**Fig. 6: PDC file with security attributes and access authorisation (example)**



In the following, the command sequences and the keys needed for these services are described with respect to PDC's supporting symmetric algorithms and/or asymmetric algorithms.

## 5.3 Technical components (architectural)

Technical components are:

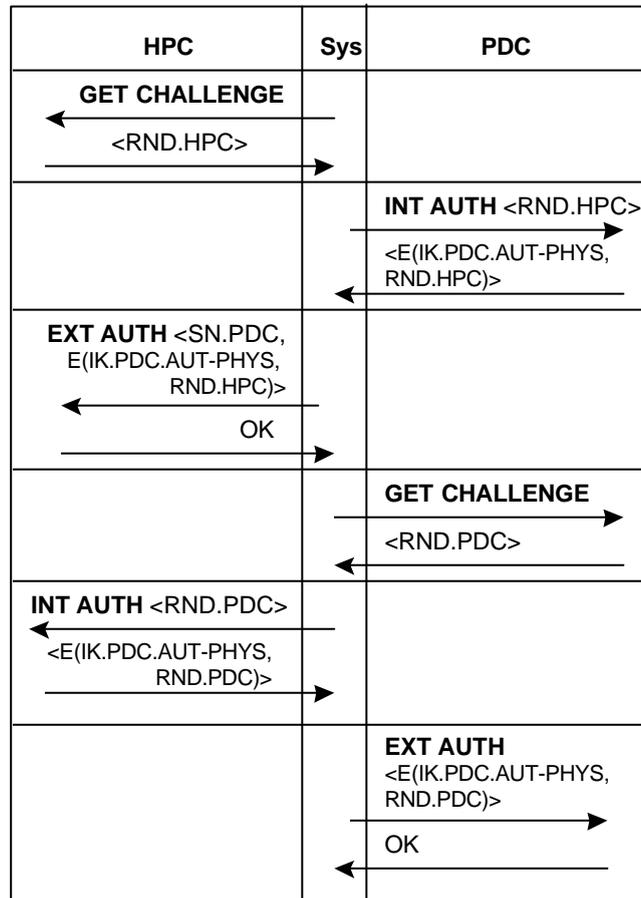
1. PDC
2. HPC
3. Card terminal (depending on the security features there might be the need for secure pin pads etc.)
4. PC/Host
5. Security toolkit

### 5.4 Data and flows

#### 5.4.1 Mutual authentication with symmetric algorithm

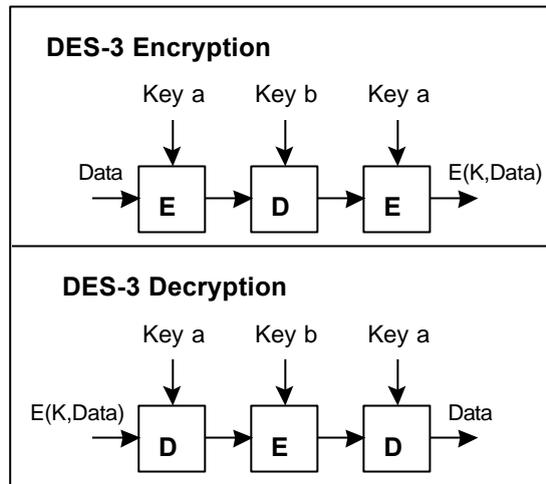
The mutual authentication scheme is shown in Fig. 7.

Fig. 7 Mutual authentication between HPC and PDC



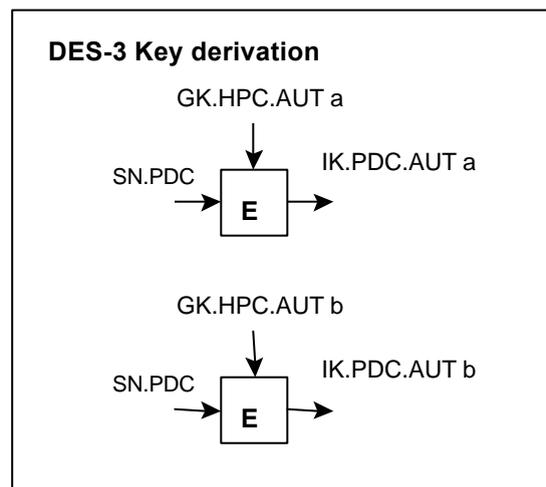
For encryption and decryption of the challenge, DES-3 is applied as Fig. 8 shows.

**Fig. 8 Encryption/Decryption with DES-3**



The derivation of the individual key of the PDC (IK.PDC.AUT-PHYS) with the group key of the physician is shown in Fig. 9.

**Fig. 9 Key derivation**



The first command to be send to the HPC is the GET CHALLENGE command.

table 2: GET CHALLENGE command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'84' = GET CHALLENGE
P1, P2	'0000'
Lc	Empty
Data field	Empty
Le	'08'

table 3: GET CHALLENGE response

Data field	RND.HPC (8 bytes)
SW1-SW2	'9000' or specific status bytes

After GET CHALLENGE follows the command EXTERNAL AUTHENTICATE. In the HPC the individual PDC-key has to be computed, before the cryptogram can be deciphered and compared with the challenge.

table 4: EXT. AUTHENTICATE command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'82' = EXTERNAL AUTHENTICATE
P1	'00'
P2	'00'
Lc	'10' = Length of subsequent data field
Data field	Authentication related data (DES-3 Cryptogram): SN.PDC (8 bytes)    E (GK.PHYS.AUT, RND)
Le	Empty

table 5: EXT. AUTHENTICATE response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Finally the health professional must prove that in the HPC the required key is present.

table 6: INTERNAL AUTHENTICATE command for proving access rights to a PDC

CLA	'00'
INS	'88' = INTERNAL AUTHENTICATE
P1	'00' = Implicit alg. selection (DES-3)
P2	'xx' = KID
Lc	'10' = Length of subsequent data field
Data field	SN.PDC (8 bytes, data item for deriving IK.PDC.AUT-PHYS) followed by a challenge (8 bytes)
Le	'00'

table 7: INTERNAL AUTHENTICATE response

Data field	Enciphered challenge, 8 bytes: E(IK.PDC.AUT-PHYS, RND.PDC)
SW1-SW2	'9000' or specific status bytes

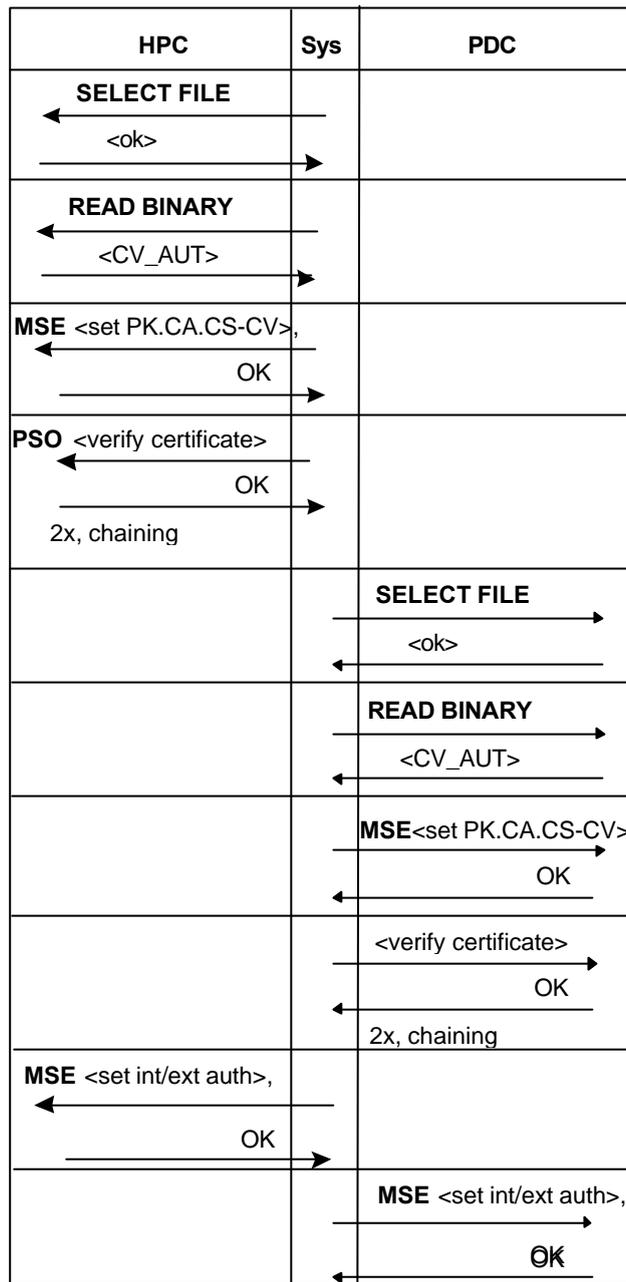
The computed cryptogram is then delivered to the PDC for authentication verification.

#### 5.4.2 Mutual authentication with asymmetric algorithm

The mutual authentication scheme is shown in Fig. 10.

Depending on the content of the PDC and HPC some command do not to be performed. After sending the final MSE-commands the external/internal authentication is being proceeded as described in chapter 0.

**Fig. 10 Mutual authentication between HPC and PDC (draft schema)**



Before performing the authentication procedure, the certificate C.HP.AUT-CV has to be presented to the PDC. It is assumed that the PK.CA.CS-CV is present in the PDC.

For reading the CV AUT certificate out of the HPC the following commands are needed:

table 8: SELECT FILE command for selecting the CV certificate file

CLA	'00'
INS	'A4' = SELECT FILE
P1	'02' = EF file selection
P2	'0C' = No FCI to return
Lc	'02' = Length of subsequent data field
Data field	FID of C.HP.AUT-CV file
Le	Empty

table 9: SELECT FILE response

Data field	Empty
SW1-SW2	'9000' or specific status bytes



table 10: READ BINARY command for reading the CV certificate

CLA	'00'
INS	'B0' = READ BINARY
P1, P2	'0000' or offset
Lc	Empty
Data field	Empty
Le	'00' = Read until end-of-file

table 11: READ BINARY response

Data field	CV certificate
SW1-SW2	'9000' or specific status bytes

Reading the CV certificate of the health professional may be performed only once and then stored in the physicians software for saving time.

The real procedure starts with verifying the PDC CV-certificate. The public key of the CA for verification is expected to be in the HPC (if not then this key has to be delivered in a CV certificate which can be verified with the PK.CA.CS\_AUT present in the HPC). For CV-certificate verification the following commands have to be performed:

- MANAGE SECURITY ENVIRONMENT for setting the public key of the CA (i.e. PK.CA.CS-CV)
- VERIFY CERTIFICATE for checking the CV-certificate of the PDC.

table 12: MSE command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'81' (= SET for verification)
P2	'B6' (= DST)
Lc	'0x' = Length of subsequent data field
Data field	'84 0x ...' (DO for KeyRef of PK.CA.CS-CV)
Le	Empty

table 13: MSE response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

After the PK.CA.CS-CV is set, then the VERIFY CERTIFICATE command is sent whereby command chaining is used (for command chaining, see ISO/IEC 7816-8).

table 14: PSO: VERIFY CERTIFICATE command

CLA	'1x'
INS	'2A' = PERFORM SECURITY OPERATION: VERIFY CERTIFICATE
P1	'00'
P2	'AE' (= Certificate in the data field, signed signature input consists of non-BER-TLV-coded data, i.e. the certificate content is a concatenation of DEs)
Lc	'xx' = Length of subsequent data field
Data field	'5F4E'-L-Certificate content (see 0)
Le	Empty

table 15: PSO: VERIFY CERTIFICATE response

Data field	Empty
SW1-SW2	'9000' or specific status bytes



table 16: PSO: VERIFY CERTIFICATE command

CLA	'0x'
INS	'2A' = PERFORM SECURITY OPERATION: VERIFY CERTIFICATE
P1	'00'
P2	'AE' (= Certificate in the data field, signed signature input consists of non-BER-TLV-coded data, i.e. the certificate content is a concatenation of DEs)
Lc	'xx' = Length of subsequent data field
Data field	'5F37'-L-CA signature (see 0)
Le	Empty

table 17: PSO: VERIFY CERTIFICATE response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

Before the INT/EXT AUTHENTICATE commands are performed the keys to be applied by the HPC for these commands have to be set.

table 18: MSE command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'22' = MANAGE SECURITY ENVIRONMENT
P1	'C1' (= SET for int/ext authentication)
P2	'A4' (= AT)
Lc	'11' = Length of subsequent data field
Data field	'83 0C xx ... xx' (KeyRef of PK.PDC.AUT, i.e. ICCSN.PDC)    '84 01 84' (KeyRef of SK.HP.AUT-CV)
Le	Empty

table 19: MSE response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

table 20: GET CHALLENGE command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'84' = GET CHALLENGE
P1, P2	'0000'
Lc	Empty
Data field	Empty
Le	'08'

table 21: GET CHALLENGE response

Data field	Challenge (8 bytes)
SW1-SW2	'9000' or specific status bytes

After GET CHALLENGE follows the command EXTERNAL AUTHENTICATE, which delivers the digital signature of the PDC to the HPC. The HPC has to verify this signature.

table 22: EXT. AUTHENTICATE command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'82' = EXTERNAL AUTHENTICATE
P1	'00'
P2	'00'
Lc	'xx' = Length of subsequent data field
Data field	Authentication related data: digital signature
Le	Empty

table 23: EXT. AUTHENTICATE response

Data field	Empty
SW1-SW2	'9000' or specific status bytes

The digital signature input based on ISO/IEC 9796-2 and integrating a random number has the following structure:

- Header: 2 bits (= 01)
- More-data bit = 1 (Mn not empty)
- Padding field: bits equal to 0 (amount depending on length of modulus) followed by a single bit set to 1
- Data field: random no. inserted by the card (8 bytes)
- Hash field: hash-code (for SHA-1: 160 bits)
- Trailer: 1 byte: 'BC'

After the CV certificate of the health professional has been presented to the PDC, the software system will require a challenge from the PDC prior to sending the subsequent commands. The random number will be hashed and the DSI format as described will be used.

table 24: INT. AUTHENTICATE command

CLA	As defined in ISO/IEC 7816-4 and -8
INS	'88' = INTERNAL AUTHENTICATE
P1	'00'
P2	'00'
Lc	'08' = Length of subsequent data field
Data field	RND.PDC (8 B)
Le	'00'

table 25: INT. AUTHENTICATE response

Data field	Digital signature
SW1-SW2	'9000' or specific status bytes

### 5.4.3 Secret key files

#### 5.4.3.1 4.1 EF.GK.PHYS.AUT

In EF.GK.HP.AUT the group key of the health professional, i.e. the physician, is stored. It is Ka and Kb for DES-3.

#### 5.4.3.2 EF.SK.HP.AUT-CV

In EF.SK.HP.AUT-CV the secret (private) key of the health professional, i.e. the physician, is stored. It is an RSA key with at least 512 bits.

### 5.4.4 Certificate files

#### 5.4.4.1 Principle structure

This certificate is used in PK-based authentication procedures applied in HPC/PDC interworking.

The principle structure of a card verifiable certificate (CV certificate) shows the subsequent figure. The sequence of data elements can be described by a headerlist as defined in ISO/IEC 7816-8. This requires a fixed length of each data element.

table 26: Certificate content and certificate headerlist

Certificate Content	Certificate Profile Identifier (1 B)	Certification Authority Reference (8 B)	Card-Holder Reference (14 B)	Card-Holder Authorisation (x B)	OID.PK (x B)	PK (modulus tag '81', exponent tag '82') (x B)
Headerlist Content	'5F29 01'	'42 08'	'5F20 0E'	'5F4B 0x'	'06 0x'	'5F49 xx'    '81 xx    '82 xx'

##### 5.4.4.1.1 Certificate Profile Identifier

The "Certificate Profile Identifier (CPI)" has the purpose to denote the exact structure of a CV certificate. It can be considered as an identifier of a card internal headerlist describing the concatenation of the data elements including their length so that e.g. the PK in a CV certificate can be found by the certificate verifying card (patient data card).

##### 5.4.4.1.2 Certification Authority Reference (Authority Key Identifier)

The „Certification Authority Reference (CAR)“ has the purpose of identifying the certificate issuing CA with a distinguished name in such a way that the DE can be used as an authority key identifier for referencing the PK to be applied for the certificate verification. The CAR consists of

- the CA name (country code according to ISO 3166 (2 Bytes) followed by an acronym of the CA (3 Bytes, ASCII characters) and
- an extension for key referencing (3 Bytes).

table 27: Structure of the Certification Authority Reference (Authority Key Identifier)

CA Name (5 B)	Extension for key referencing (3 B)
------------------	---

The extension has the following structure:

table 28: Structure of the extension for key referencing

Service Indicator (1 BCD)	Discretionary Data (1 BCD)	Algorithm Reference (2 BCD)	Date (last two digits of key generation year) (2 BCD)
---------------------------------	----------------------------------	-----------------------------------	---

The Service Indicator has the value 0 = entity authentication according to the key usage in x.509 certificates.

The Discretionary Data may have a value at the discretion of the related CA.

The Algorithm Reference can be individually assigned by a CS for distinguishing different PK algorithms.

The Date consist of the last two digits of the year, in which the key pair for certificate signing was produced. If more than one keypair has been generated, it may be distinguished by using the discretionary data field.

#### 5.4.4.1.3 Certificate Holder Reference (Subject Key Identifier)

The „Certificate Holder Reference (CHR)“ has the purpose to denote the certificate holder uniquely in such a way that the DE can be used as a subject key identifier for referencing the PK of the certificate holder. The CHR consists of

- a CA Reference CAR (5 Bytes) || Extension for key referencing (3 Bytes), if the certificate holder is a CA
- the ICCSN (14 Bytes), if the certificate holder is the card of a health professional.

table 29: Structure of the Certificate Holder Reference, if certificate holder is a CA

Filler (6 B)	CA Name (5 B)	Extension for key referencing (3 B)
-----------------	------------------	---

The „Extension for key referencing“ has the same structure as shown in table 30. The field „date“ contains the last two digits of the year, in which the PK certified in the certificate (i.e. the PK.CA.CS\_AUT) is issued.

table 30: Structure of the extension for key referencing

Service Indicator (1 BCD)	Discretionary Data (1 BCD)	Algorithm Reference (2 BCD)	Date (last two digits of key generation year) (2 BCD)
---------------------------------	----------------------------------	-----------------------------------	---

table 31: Structure of Certificate Holder Reference, if certificate holder is an HPC

ICCSN.ICC
-----------

(14 B)

#### 5.4.4.1.4 Certificate Holder Authorisation

The „Certificate Holder Authorisation (CHA)“ has the purpose to denote the access rights of the health professional with respect to data stored in files in a patient data card. The meaning of CHA can be compared with a role based group key when applying symmetrical algorithms.

The CHA consists of

- a prefix denoting the entity assigning the role id and
- the role identifier of the health professional.

table 32: Structure of Certificate Holder Authorisation

Prefix	Role ID
(x B)	(1B)

The subsequent table shows CHA Role Identifiers relevant for physicians.

table 33: CHA role ID coding

CHA Role ID	Meaning	Relevant for C.CA.AUT	Relevant for C.HP.AUT
'00'	No access right to data	x	
'01'	CHA Role ID for proving the access right of a physician		x

NOTE – If different physicians have different access rights to a PDC, then different role identifiers have to be assigned.

#### 5.4.4.1.5 PK of certificate holder

##### 5.4.4.1.5.1 General construction

The Public Key in a certificate consists of a concatenation of parameters. These parameters, which have a context specific tag, belong to the DO PK (Tag '7F49', constructed) and have to be coded as octet string. In the CV certificate verifying entity (i.e. in the PDC) the occurrence of such a parameter and its length can be described in the headerlist (if a constructed tag occurs in a headerlist, its tag is followed by a length '00', since the embedded tag-length elements carry the length of the respective DE).

##### 5.4.4.1.5.2 Public key RSA

- Tag '81': Modulus
- Tag '82': Public exponent (e.g. 65537)

#### 5.4.4.1.6 Signature formats for the CA signature

##### 5.4.4.1.6.1 General aspects

The data to be signed are the certificate content. The hash function used and the digital signature input (DSI) format are denoted by the OID. For CV AUT certificates in an HPC the RSA algorithm is used for certificate signing.

#### 5.4.4.1.6.2 RSA

##### a) DSI according to ISO/IEC 9796-2

In the DSI for CV AUT certificates based on RSA no random padding is needed, since there are no attacks with dynamically produced DSIs. Therefore the original DSI format according to ISO 9796-2 can be used:

- Header: 2 bits (= 01)
- More-data bit = 0
- Padding field according to 9796-2
- Hash field: hash-code (for SHA-1 and RIPEMD-160: 160 bits)
- Trailer: 1 byte: 'BC'

##### b) DSI according to PKCS #1

The DSI format for PKCS #1 has the following structure:

- Startbyte: '00'
- Block type: '01'
- Padding-String: 'FF ...FF'
- Separator: '00'
- DigestInfo: ASN.1-Sequenz von digestAlgorithm (ASN.1-Sequence of OID and parameter) and digest (ASN.1-DO hash value)

The DigestInfo to be delivered to the card has the following coding:

SHA-1 with OID: { 1 3 14 3 2 26 }

DigestInfo: 3021 3009 06052B0E03021A 0500 0414 || hash value (20 bytes)

#### 5.4.4.2 EF.C.HP.AUT-CV

The EFC.HP.AUT-CV (FID = 'C108') contains the CV AUT certificate of the health professional.

#### 5.4.4.3 EF.C.CA.AUT-CV

The EFC.CA.AUT-CV contains the CV AUT certificate of the CA (to be discussed).

### 5.4.5 Public key file for internal use

#### 5.4.5.1 EF.PK.CA.CS-CV

The EF.PK.CA.CS-CV (FID = 'B100') contains the PK of the CA issuing the CV certificates. This key is applied by the HPC for certificate verification.

## 5.5 Interoperability needed

### 5.5.1 Subject of Interoperability

Beneath the conventions described in chapter 0 interoperability is needed:

on PDC- and HPC-side:

- conventions for physical and logical communication with a smartcard on the physical layer and the transmission layer
- conventions for reading/updating protected data including application selection, file selection etc.

- conventions for the location, structure and content of protected patient data set (interoperable data set)
- conventions for encoding professional roles

on card terminal-side:

- conventions for physical and logical communication with a PDC and HPC on the physical layer and the transmission layer

on PC/Host-side:

- conventions for physical and logical communication with a PDC and HPC on the physical layer and the transmission layer

## 5.5.2 Conventions and Standards

### 5.5.2.1 *Conventions for the physical layer and the transmission layer*

#### 5.5.2.1.1 *Physical layer*

PDC's and HPC's are contact based cards with physical characteristics according to ISO/IEC 7816-1. The location and dimensions of the contacts shall comply with ISO/IEC 7816-2. For encoding the data bits on the I/O line the „direct convention“ is recommended.

#### 5.5.2.1.2 *ATR, PPS and Transmission Layer*

The Answer-to-Reset (ATR) shall comply with ISO/IEC 7816-3 (2<sup>nd</sup> edition).

It is recommended, that PDC's and HPC's support the Protocol Parameter Selection (PPS) e.g. to be able to transmit data with higher speed.

The transmission protocol supported by the card shall be either

- the half-duplex character transmission protocol T=0 or
- the half-duplex block transmission protocol T=1 or
- both.

If T=1 is used, chaining is mandatory. The following simplifications are allowed:

- NAD Byte: not interpreted (NAD shall be set to '00')
- S-Block ABORT: not used
- S-Block VPP state error: not used

For T=1 the Information Field Size Card (IFSC) shall be indicated in the ATR (Character TA3, recommended value: at least '80' = 128 Bytes).

The Information Field Size Device (IFSD) shall be transmitted by the IFD immediately after ATR, i.e. the IFD shall send at once after ATR the S-Block IFS Request which has to be answered by an HPC with S-Block IFS Response. The recommended value for IFSD is 254 Bytes.

### 5.5.2.2 *Conventions for file selection and data access, for the location, structure and content of HPC data*

The standardisation work on card-verifiable certificates is still going on (see annex 0 „A Standards, regulations, ongoing work, national projects (informative)“, German HPC-specification).

Furthermore the standardisation of an European HPC is an open work item within CEN TC 251. After founding the ISO TC 215 „Health Informatics“ it seems to be most likely that there will be an international work item on this topic.

## **5.6 Possible evolution**

The standardisation work on HPC's and card-verifiable certificates has to be taken into account.

Depending on the security level of an application there might be a need for biometrical devices.

Possibly the writing of data to a PDC will require a digital signature. In this case the HPC needs to have the facility to produce such signatures and additionally a security policy on NETLINK level is needed.

Described above there is the possibility of using group keys as role identifier of health professionals. Up to now there are a lot of differences between the roles of health professionals on international and European level. With this background it is obvious that NETLINK can not make any recommendations about roles. But if there is an international/European standardised grouping of health professionals this has to be taken into account for the use of HPC's.

## **5.7 Requirements for technical components**

### **5.7.1 PDC**

PDC's are contact based cards with characteristics according to ISO/IEC 7816-1, 2, 3, 4, 5 and 6. The card size is ID-1. PDC's may be 5Volt- or 3Volt-cards.

In case the patient consent is made by entering a PIN or other techniques, the PDC should have the capability to provide this service.

### **5.7.2 HPC**

HPC's are contact based cards with characteristics according to ISO/IEC 7816-1, 2, 3, 4, 5 and 6. A HPC shall be either a normal size card (ID-001 card) or a plug-in card (ID-000 card). HPC's may be 5Volt- or 3Volt-cards.

### **5.7.3 Card terminal**

The card terminals must be able to support contact-based cards with T= 0 and T = 1 transmission protocols. If PIN-presentation is required, the card terminal with PIN-pad has to be able to deliver the VERIFY-command the way expected by the PDC.

For HPC/PDC interworking a doubleslot card terminal is highly recommended (for example for performance and security reasons) but other solutions are possible. In case of a plug-in HPC there must be a slot for such cards.

The terminal shall support 5Volt- and 3Volt-cards (class AB). The terminal should support PPS and be able to transmit data with the highest speed the card indicates (this should at least be configurable).

In case the patient consent is made by entering a PIN, the card terminal should have the capability to securely handle PIN presentation to PDC.

Remark: No further harmonisation is needed for card terminals.

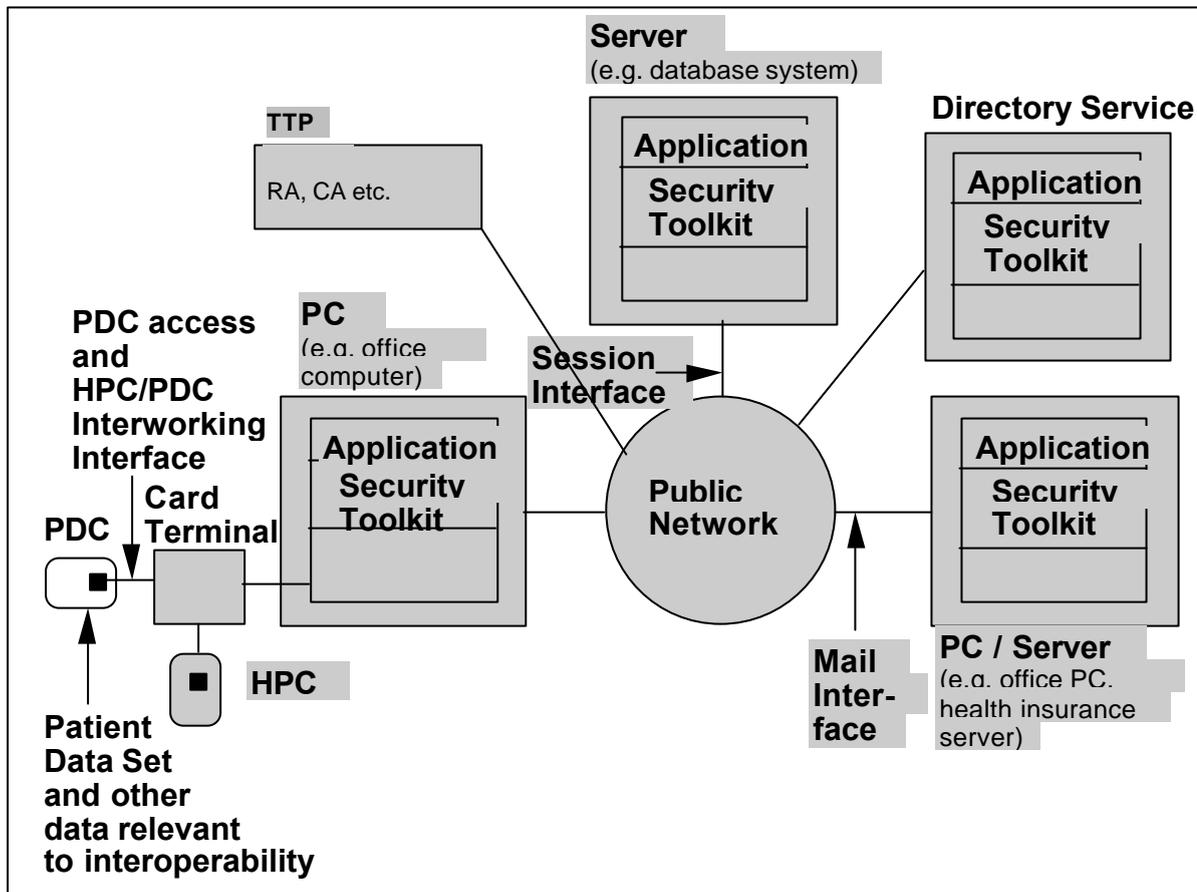
### **5.7.4 PC/Host**

The PC/Host must be able to connect one or more card terminals (depending on the number of slots) and to support the communication with the highest transmission speed the cards indicate.



## 6 SECURE MESSAGING

**Fig. 11 Interoperability Scenario**



### 6.1 Scope

This section focuses on interoperability between secured e-mail systems in the Healthcare sector, i.e. the secure exchange of e-mails (digitally signed for proof of origin and integrity, encrypted for confidentiality) including attachments, between health professionals located in various countries.

Mechanisms to provide exchange of secured messages may be implemented at:

- Network level: network connections provide security services on top of which mail messages can be exchanged; mail protocols or exchanged documents may not be secured (e.g. IP level security services).
- E-mail system level: mail protocols support transport of security fields and the network connections or the document may not be secured (e.g. S/MIME & OPEN PGP security services).
- Document level: documents are secured by themselves, they may be carried over non-secured networks or mail systems (e.g. EDIFACT level security services that allow exchange of secured EDIFACT messages / interchanges over standard SMTP/MIME).

This section gives recommendations for secure messaging at E-mail system level only.

This chapter covers all issues related to the exchange of secured e-mails, i.e. it does not focus only on network protocols and e-mail formats but also on other topics such as key management schemes, interoperability of directory and trusted third party services, as shown in the above figure.

The proposed recommendations should be as much as possible close to the Internet *de facto* standards and further more, easy to bring consistent with the on-going European and / or international *de jure* standards as well as national smart card programs.

The secure messaging specifications only aim at providing guidelines to set up interoperable systems, i.e. these specifications are not complete to solve local / national implementations issues. Additional topics should also be taken into account when designing national Health Information Systems such as: cost of implementation, ergonomics, compliance with standards (industry and *de jure* ones), migration capabilities, compliance to local regulation (e.g. on cryptography).

### 6.1.1 Regulation aspects

The proposed solution should be compliant with the national regulation relevant to France, Germany, Italy and Canada (Quebec) as well as the following European regulation relevant to France, Germany, and Italy: "Data protection " (Ref. 95/46/CE) and "Electronic Signature Recognition" (project).

According to treaty of WIEN and the WASSENAAR arrangement (3 December 1998), the 33 involved countries (including USA Canada, Italy, Germany, and France) may adopt restrictive regulation about exportation of security products using encryption algorithms with key length greater than 56 bits. It seems that export of US products using keys 128 bits long should be allowed toward Europe for the Healthcare sector (with exception for pharmaceuticals industry).

## 6.2 Scenario(s)

The scenario is:

- Any of the actors of the Health Care sector (with the notable exception of patients, i.e. PDC are not involved) should be able to easily exchange secured documents (digitally signed for proof of origin and integrity, encrypted for confidentiality), e.g. physician reports.
- Users involved in the exchange of secured documents should trust the system they use.

The emphasis is to be put on "secured" and "trust".

The recipient of a signed message should have the capability to verify the signed message, i.e.:

- To verify the digital signature.
- To verify the sender's identification and key certificates (including sender's capacity to sign, including public key certificate, attribute certificate, CRL).

The recipient of an encrypted message shall be have the capability to read the received message, i.e.:

- To check the sender's identification and key certificates (including sender's capacity to encrypt a message)
- To decrypt the message.

When TTP services are used (for instance to provide key escrow or key recovery services), conventions need to be defined between TTP's in order to make the management systems interoperable and to allow users to trust the whole system.

Directory services are needed for several system management functions such as:

- retrieval and storage of certificates (including identification)
- retrieval of CRLs

TTP to TTP and Directory server to Directory server protocols have to be described where appropriate.

This scenario addresses how end users are able to reveal (upon request or not) the content of message (i.e. message in clear) starting from the encrypted message (only).

This section does not address encryption of multi-recipient messages.

This section does not address decryption of e-mails by other users than those intended by the originator (e.g. how the HP secretary could handle a message originally sent to the HP).

This section does not give recommendations for the identification of HP.

This section does not give any specification on mail access protocols (e.g. POP3, IMAP 4).

### **6.3 *Technical components (architectural)***

This chapter and the following one (Data and Flows) give a description of the overall architecture that may be used to support the exchange of secured e-mail. Several ways of providing the same service may be described here.

In order to have a good view of the overall Secure Messaging architecture, it is preferable to start by reading the “Data and Flows” chapter and then read this chapter. Readers interested in the recommendations for interoperability only should skip this chapter as well as the following one..

The identified technical components are:

1. HPC (Health Professional Card)
2. Card terminal
3. Workstation
4. Network
5. Directory management system.
6. TTP (Trusted Third Parties)
7. Session Interface

The following chapter describes the overall architecture needed to provide secure mail exchanges.

#### **6.3.1 HPC (Health Professional Card)**

A HPC can be used to provide the services described below.

Access to HPC data or use of some of the services provided by the HPC could be protected by preliminary cardholder authentication (e.g. PIN, biometrics techniques).

##### **6.3.1.1 *HP Identification and personal information***

It is out of the scope of this document to define the content of the HPC.

##### **6.3.1.2 *Digital signature***

The digital signature algorithm is implemented in the HPC (for calculation only). The digital signature algorithm (for verification only) does not need to be implemented in the HPC.

Card holder’s digital signature key certificate may be stored in the HPC, depending on the HP behaviour (i.e. when it is required that the HP always keeps this information with him, e.g. when he makes use of several workstations in several locations with the same credentials).

The certificate may also be stored on the workstation (in this case, it is more complex for the HP to use several workstations with similar credentials).

Public key certificates can be stored according to X509v3.

NB: see next chapter (Data and Flows) for presentation of the format of signed messages.

### 6.3.1.3 *Message encryption*

HPC may be involved in the computing of the session keys needed for message encryption. However, use of HPC for encryption key management has several consequences (advantages and drawbacks) including:

- The only way to decrypt messages is to have an HPC to calculate the session key, thus messages cannot be decrypted with keys stolen on or copied from the workstation.
- Use of HPC leads to some constraints in terms of flexibility ; examples:
  - Messages cannot be decrypted without the HPC, e.g. a secretary may not have access to encrypted messages, unless she uses the HP's card ;
  - Encryption key management has to be strongly co-ordinated with HPC management (CRL, key recovery, etc.).

NB: see next chapter (Data and Flows) for presentation of format of encrypted messages.

#### 6.3.1.3.1 *De facto standard product: S/MIME & OPEN PGP*

Two standards are in competition at this time:

- S/MIME V2 with RFC 2312 (Certificate Handling) and RFC 2311 (Message Specification), which has had the "proposed standard" status since March 23<sup>rd</sup> of 1998.
- OPENPGP, an extension to the well known PGP, RFC 2440 (Message Format), which has had the "draft standard" status since November 1998.
- A new version of S/MIME (V3) with the "Internet draft" status has been available in December 1998.

#### 6.3.1.3.2 *Extensions to de facto standard products*

Existing de facto standard products from major software companies do not make use of smart cards (thus HPC). Some implementations based on smart cards exist but are not widely used nor based on similar architectures.

#### 6.3.1.3.3 *Use of TTP services*

Encryption mechanism may require the use of TTP services, for instance for "data recovery" (see "Trusted Third Party" below in this chapter).

Use of TTP for such services may have consequences on HPC.

### 6.3.1.4 *HPC Certification*

As the HPC hosts several security mechanisms & techniques that are crucial to reach a high level of security, it has to be trusted by all users, thus needs to be secure.

Several ways of evaluating security of HPC exist, including evaluation process compliant to international certification schemes (ITSEC in Europe, ISO Common Criteria, etc.).

The smart card as a whole could be evaluated (i.e. OS and processor in combination) or OS and processor separately.

### 6.3.1.5 *Private keys*

When HPC is used for encryption key management, private keys for session key encryption are generally delivered by the card issuer to the HPC (See "TTP functionality" / "Centralised generation").

Private keys may be delivered at the personalisation phase (in this scenario, the card issuer has a very strong link with the CA) or later during the life card cycle (in this scenario, the card issuer may not be the CA).

There must be a secure way of delivering private keys to HPC: mutual authentication between the HPC and the card issuer and encrypted / signed private key loading.

### 6.3.2 Card Terminal

A card terminal is needed to access to the HPC, thus be compatible with cards standards (see card terminal characteristics for instance in section "4 PDC access (free)").

### 6.3.3 Workstation

#### 6.3.3.1 General

The workstation components are:

- Operating system
- Applications (HPC management software, Local Directory Services, Mail client, Network software, etc.)
- Security toolkit (requires access to card terminal and cards)

Storage of the card holder's public key certificate on the workstation may be needed depending on the HP behaviour (in this case, the HP may use several workstations but with different credentials), the alternative being that the card holder's public key certificate is stored on the HPC (i.e. when it is required that the HP always keeps this information with him, e.g. when he makes use of several workstations in several locations with the same credentials).

Display of certified objects (public key certificates, CRL, etc.) to the end user is needed in a user-friendly way.

#### 6.3.3.2 Digital signature

NB: see next chapter (Data and Flows) for presentation of format of digitally signed messages.

The digital signature algorithm can be implemented on the workstation (for verification only).

The mode of operation for digital signature algorithm can be implemented in the workstation (for calculation and verification).

The hashing algorithm needed for digital signature can be implemented in the workstation.

#### 6.3.3.3 Message encryption

NB: see next chapter (Data and Flows) for presentation of format of encrypted messages.

##### 6.3.3.3.1 De facto standard product: S/MIME & OPEN PGP

All mechanisms can be implemented or stored either onto the workstation or on an external device or service (i.e. smartcard, etc.): security toolkit, keys, etc..

Using S/MIME requires that the e-mail client system on the Workstation support the S/MIME format. The security toolkit may have to be closely linked to it ; this may be a constraint as users may have some difficulties to acquire network agents (e-mail or HTTP client, etc.) with strong security capabilities due to some export restrictions on cryptographic tools.

On the contrary, using OPEN/PGP requires that the e-mail client system on the workstation support the MIME format only, thus the security toolkit can easily be made external to the network agent (e-mail or HTTP client, etc.). This may be an advantage as it would be easy to plug cryptographic tools developed in the end-user's country, thus not constrained by any export restrictions.

#### 6.3.3.3.2 *Extensions to de facto standard products*

Some of the mechanisms may be implemented in the workstation (see above in the HPC chapter).

#### 6.3.3.3 Use of TTP services

All mechanisms can be implemented in the workstation with the exception of encryption keys that may be encrypted using HPC (see above in the HPC chapter).

#### 6.3.3.4 Mail protocols & formats

Protocols and formats that can be used by the workstation for secure mail exchange are:

- either TCP + IP + (E)SMTP + S/MIME
- or TCP + IP + (E)SMTP + MIME + OPEN PGP

This document does not focus on protocols needed to connect to the e-mail system such as POP3, IMAP4, etc.

Today, there is no interoperability between S/MIME compliant software and OPENPGP software. MIME working group is in discussion for a modification of RFC 2015 (MIME), in order to recognise OPENPGP object as attached documents.

Main differences between S/MIME and OPENPGP are:

-	S/MIME	OPENPGP
Protocol	each Transport Protocol which supports MIME protocol	Any protocol: SMTP (MIME), FTP, HTTP, etc., even magnetic or optical media(diskettes, CD, etc.)
Objects secured	Message & attachments	Only attachments
Ergonomic	Transparent to the user	By default, non-transparent to the user. Adding "buttons" in the MIME agent may improve ergonomic. OPENPGP libraries are available for including OPENPGP services into existing (S/)MIME agents. Modification of MIME RFC is in progress in order to include OPENPGP automatic recognition.

#### 6.3.3.5 Workstation local directory

Workstations local directory provides:

- Workstation local directory to store at least e-mail addresses and public key certificates: X509v3, etc.
- Reception from a Certification Authority of public key certificates
- Broadcasting of public key certificates
- Support of public key certificates revocation list

#### 6.3.3.6 API's

API's can be very useful in order to allow the HP application to access to various security services. Some API's also propose some implementation rules for the cryptographic algorithms used.

##### 6.3.3.6.1 PKCS#11

PKCS#11 is one of the CDSA subset components. The PKC#11 industry standard specifies an API to devices that hold cryptographic information and perform cryptographic functions. It proposes four implementation modes:

- Key holder Cards: Keys and certificates are stored into files held by the card. This is the usual card implementation.
- Sign-on Cards: the card provides RSA signatures. The card can do SSL3 (or S/MIME) holder authentication. No data encryption.
- Sign on and data encryption: RSA session key encryption can be provided by the card (i.e. in S/MIME mode).
- Multi service card: RSA data encryption.

PKCS#11 is an API specification that aims at offering to applications a uniform interface to cryptographic token, including smart card. As a consequence, when different cards have to be supported on a single workstation, several PKCS#11 drivers are needed. However, the PKCS#11 specifications do not allow for a dynamic management of multiple smart cards. The solution is then to have a unique PKCS#11 driver that support several cards.

#### *6.3.3.6.2 Common Data Security Architecture (CDSA)*

CDSA is another industry standard specified by the OPEN GROUP (INTEL, IBM, HP, NETSCAPE, RSA Labs., GEMPLUS, etc.). The main benefit provided by CDSA is to split the secure services implemented on the PC into interoperable modules, which are:

- The Cryptographic Service Provider
- Certificate Library
- Data storage Library
- Trust Policy
- Key Recovery

CDSA proposes an architecture based onto the plug-in concept, so it should be easy enhance functionality with new services based on the existing APIs.

CDSA is an evolution of PKCS#11 and X/OPEN API specifications (with ascendant compatibility).

#### *6.3.3.6.3 MS Crypto API*

CryptoAPI is an application programming interface (API) that is provided as part of Microsoft® Windows® 95, 98 and Windows NT®. It provides a framework that programs can use to obtain cryptographic and digital certificate services. Some CDSA implementation include MS CAPI as specific "Crypto modules".

Security Features:

- Support for public-key and shared-secret key cryptographic algorithms.
- Support for certificate handling services.
- Based on industry standards, including cryptographic standards from IETF (PKIX, S/MIME), PKCS, X.509, etc.

#### *6.3.3.7 HP Workstation Certification*

As the workstation hosts several security mechanisms that are important to reach a high level of security, it has to be trusted by all users. Thus implementation of security mechanisms needs to be secure.

Several ways of evaluating security of workstations exist, including evaluation process compliant to international certification schemes (ITSEC in Europe, ISO Common Criteria, etc.). They may be applied to some elements of the workstation (as it is not realistic to plan certification of “commercial” workstations as a whole).

### 6.3.4 Trusted Third Party (TTP)

#### 6.3.4.1 Definitions

##### 6.3.4.1.1 TTP

An organisation of demonstrable probity, offering auditable services in the field of validation, authentication and assurance. A Trusted Third Party provides digital certification to certify that users are who they say they are. TTP certificates must be issued following independent authentication checks on the individuals or organisations seeking to use them. At the application stage, specific information is gathered, which is verified offline or online to ensure that certificate applicants really are whom they say they are.

TTP includes at least two technical subsets: Certification Authority (CA) and Data Recovery Services (DRA)

##### 6.3.4.1.2 Certification Authority

A CA is issuing independently authenticated digital certificates for use by individuals or organisations. Such certificates allow the user to prove their identity, and the integrity of email and/or attachments in transit. Certificates also facilitate the use of encryption to ensure confidentiality.

##### 6.3.4.1.3 CPS (Certification Practice Statement)

In signed e-mail exchanges, there is a strong relationship between the trust related to the digital signature issued by an HP and the trustworthiness of X509 certificate issued by the CA.

Multiple CA maybe used. It is then important that each CA describes the procedures, techniques and mechanisms used to verify the link between an HP identity and his public key.

This is the purpose of the CPS.

The indicative content of a CPS is usually:

CA liability	CA obligations
Subscriber obligations	Financial responsibility
Governing law	Compliance audit
Description of initial Registration	Types of names
Uniqueness of names	Method to prove possession of private key
Authentication of organisation identity	Authentication of individual identity
Revocation Request	Description of operational functions
Certificate Application	Certificate Issuance
Certificate Acceptance	Certificate Suspension and Revocation
CRL issuance frequency (if applicable)	On-line revocation/status checking availability
Security Audit Procedures	Description of physical, procedural and personnel security

Description of technical security controls	Key Pair Generation and Installation
Private Key Protection	Computer Security Controls
Network Security Controls	Cryptographic Module Engineering Controls
Description of certificate profiles	

#### 6.3.4.1.4 Data recovery Services

TTP's are also be able to offer Data recovery Services. At present, if encryption keys are lost, stolen or deliberately withheld by disaffected HP in a hospital for example, then the information remains encrypted and may be lost to its owner for ever. TTP's are in a position to offer recovery of the keys to their clients as they can (in some models of certificates generation) store (or escrow) the keys.

This function may be compulsory in some countries due to local regulation.

#### 6.3.4.2 TTP functionality

The TTP Server shall provide the following functionality:

- Certificate issuing

This is done by the CA. - Certificates are issued for end-users (HP), subordinate CA's lower down the hierarchy and for other root CA's in the case of cross certification . There are two methods. These two methods can be combined in any system and in reality are, because the trusted CA keys are generated by the CA.

##### **Centralised generation**

The private/public key pair is generated by the CA (or some co-located software) and the public key is directly provided to the CA software to create a certificate. The keys & certificate can then be provided to the HP (or other CA) via any suitable channel. The channel must be strongly secured for private key delivery to the HP (not for certificate, because it is a self protecting structure, given the CA's signature)

There are a number of different techniques that can be used:

##### *Manual Distribution*

In this case the HP is registered to the CA (or associated Registration Authority) by an administrator. Depending on the security policy the HP may be required to present himself to the administrator. Part of the process of registering the HP is be the creation of a token for the user (in PKIX terms this is part of the user's Personal Security Environment – PSE). The token contains the HP certificate and the associated private key. The token could then be physically supplied to the user. The token could take the form of a disk file or smart card. For additional security a PIN could be used to “unlock” the token.. This technique does not require the CA to be on-line to the HP.

##### *Request*

The user, using a Web Browser, connects to a CA's Web Page and request a certificate (or in Verisign's language a Digital ID). The user is prompted to enter some personal details, primarily for identification purposes. The user is also prompted to enter some form of Pass Phrase. Having requested the certificate (and also triggered the central generation of the public/private key pair), details on how to fetch the certificate are mailed to the user. This could be of the form of an e-mail containing a URL of a web page the user must visit to fetch the certificate. On visiting the web site the user would be prompted to enter the Pass Phrase (or something derived from it). The certificate would then be sent to the user using a HTTP message encoded perhaps as a special MIME type that the Web Browser recognises and is triggered to enter the certificate into the Browser's certificate database. The user would also have to obtain the CA's Trusted Public Key. Most Browsers already

come installed with some trusted public keys, for instance Verisign. If the CA's trusted public key is not installed within the Browser then using a similar operation to that described can be used to fetch it.

#### *Request with authentication*

This is very similar to the previous technique. The additional (and very sensitive) step is that authentication checks are made. The most convenient technique is the availability of a HPC smart card which can be authenticated (after typing HP' PIN), and tele-loaded with keys & certificate in a secured way (signed & encrypted).. This technique is suited to users of certificates requiring the maximum trust in the certificate.

#### ***Distributed Generation***

In this case the private/public key pair is generated by the HP (more exactly the client software on the workstation). The key pair can also be furnished to the HP pre-loaded in a smart card.

The identity + public key is then sent to the CA requesting that it is certified. If the request is valid then the certificate is returned to the requester, and optionally published on some type of certificate repository (e.g. a X.500 Directory).

Of course, a standalone public key is vulnerable to tampering as it does not have any identity securely associated with it. Therefore the techniques described below are designed to protect the public key in transmission from the workstation to the CA.

In this method, there is one important subject to cover: "Proof of Possession" (POP).

In order to prevent certain attacks and to allow a CA to properly check the validity of the binding between an HP Id and a key pair, an HP needs to prove that it has possession of (i.e., is able to use) the private key corresponding to the public key for which a certificate is requested.

Before examining the various techniques it is useful to describe the protection mechanisms available. These mechanisms are available whatever the type of transport system used, for example HTTP or e-mail. The methods are:

#### *PKCS #10 request: and PKCS #7 response*

Until recently this has been the de-facto standard and is the most wide spread. A PKCS#10 certificate request is sent to the CA and a PKCS#7 certificate response is sent back. The PKCS#10 message has a digital signature, which is used to protect the integrity of the request (especially the public key), and provide authentication of the requester. The secure e-mail standard S/MIME is actually based on PKCS#7. The PKCS#7/#10 protocols do not support POP.

#### *PKCS #10 protected by PKCS #7 request, PKCS #7 response*

This is a variation of the above and is used mainly by Verisign.. The PKCS#10 certificate request is also protected within a PKCS#7 message. The PKCS#7 message is encrypted using the CA's trusted public key. Therefore only the CA can decrypt the PKCS#7 message and extract the certificate request.

#### *PKIX: using PKIMessage*

This is a very new emerging technique for protecting various PKI operational and management messages. It will not be discussed in detail here. The PKIX protocols supports POP as an optional (but highly recommended) feature.

#### *Proprietary*

A number of PKI vendors currently implement proprietary mechanisms, for instance Entrust.

The above mechanisms can be applied in different situations for "distributed generation".

#### *Web Browser*

This is basically the same technique as described previously as "Request" and "Request with

*authentication*". Without the installation of special Browser applets then the protection mechanisms would normally be PKCS #7/#10.

Use of a HPC combined with special browser applet, is a very secure way for "distributed generation".

#### *Helper Application*

In this case the PKI vendor would supply a special "helper application". Typically this would be a GUI application that allows a user to generate key pairs and request certification of public keys. The transport mechanism would be typically HTTP – in both directions – not relying on any "out of band" e-mail communication. This technique is more user friendly than the previous Browser described method (with the disadvantage of having to install the helper application). This technique does depend on having the CA's trusted public key already loaded– perhaps being supplied with the token.

#### *Embedded Application*

In order to hide the PKI from the user completely, some applications generate key material and request certification, at installation phase (or initial start up code).

- Certificate publishing

Once a certificate has been issued, it is published into a directory, so that third parties can access it.

- Certificate revocation

If a user loses the private key corresponding to their public certificate, or it is stolen or compromised, the certificate has to become invalid. The CA makes this information known to the user and other parties by regularly publishing a Certificate Revocation List (CRL). The frequency being part of operational policy, the more frequent the more assurance of certificate validity.

- Certificate archiving

Issued certificates, CRL's and other important information need to be archived, as digitally signed documents frequently "live" a longer time than certificates and still need to be accessed.

- Authorities public keys and/or certificates publication

Most CA's public keys and certificates are pre-defined in major browsers and e-mail clients "security enabled". New CA's must allow users load "in confidence" the appropriate new public key.

- Authorities Revocation Lists (ARL)

Some CA could stop their activity or have their agreement denied by regulation authorities. Other TTP must publish ARL in order to invalidate (revoke) all certificates issued by them.

The TTP Server may also provide the following functionality:

- Private keys recovery for recovery of data encrypted with a lost key (or for legal reason in some countries).

Notice: The Diffie-Hellman encryption scheme is much more convenient for that purpose than RSA scheme. For recovering messages issued by one HP, only one key storage is needed in D-H (HP's secret D-H key), whereas all RSA secret keys of all HP's correspondents are needed in RSA architecture.

- Private agreement escrowing

NB: TTP services may be constrained by national rules.

#### **6.3.4.3 TTP certification**

TTP certification is based on the on the CPS as described above.

#### **6.3.5 Directory management system**

### 6.3.5.1 Architecture

In the previous paragraph, it has been demonstrated the need to “publish” certificate and CRL in directories servers.

In some cases it may be dangerous, from a security point of view, to give free access to those certificate servers. In some countries (e.g. France), to ensure individual privacy rights, it is forbidden to submit non-controlled search request to directories servers

A first prerequisite is that users must be unambiguously identified, i.e. it must exist national and /or supra national Registration Authorities (RA).

Directory architecture includes:

#### *Certificate server*

In order to send encrypted e-mails, HP must be in possession of their correspondent’s certificate and private key.

The usual way, when few users are exchanging secure mail (e.g. in a project), is to initiate the local certificate directories by asking every one to send to every one either a signed mail (S/MIME) or a mail with v-card attachment.

When receiving, a click on the address (or v-card) with the right button of the mouse automatically updates the local certificate directory.

For more extensive use, a certificate server is a HP oriented service, with two functions:

- Submitting a certificate to verify its validity. The answer is VALID/NOT VALID, and could be signed and time stamped.
- Submitting a HP ID (and only one!) and obtaining the appropriate certificate

Many implementations can exist:

- Using the unsecured mode of a X500 directory (LDAP). The main problem is the lack of identification / authentication of the initiator of the request, and the vulnerability of direct “public” exposure of the server.  
*Unfortunately, this is the standard mechanism of most e-mail clients (e.g. button “get certificate of NETSCAPE MESSENGER)*
- Using the secure mode of a X500 directory (LDAP V2 with challenge/response or SSL over LDAP). This is better on a security point of view, but it is not easy to control or make limitations on the requests. The only way would be the use of LDAP access control lists (ACLs) (if supported by the directory) that determine access rights to particular classes of information by particular classes of clients. Access levels include none, compare, search, read, write and delete. Another mechanism is RFC-1558, "A String Representation of LDAP Search Filters," which specifies the syntax for the filters that define the search, but it is not currently available on every directory server
- Some “certificate servers” are based upon a WEB server, acting as a “front-end server” of a X500 directory server. This technology permits: identification / authentication of the users (even strong authentication by HPC), use of a set of pre-defined requests, and secured communication link (SSL).

#### *Synchronisation of Directory servers*

Exchange public key certificates: X509V3, etc.

DISP is the X500 directory servers’ synchronisation protocol (i.e. X593). Most of the existing directory systems implement proprietary protocols for directory synchronisation. Connection of two directory servers require bilateral agreements, developments and validations.

A new feature of LDAP is the “referral capability” to implement cooperating communities of disjoint LDAP servers, and to force all database changes to be referred to certain master LDAP servers. When LDAP

servers use the same naming convention, no matter which LDAP server a client connects to, it sees the same view of the directory; a name presented to one LDAP server references the same entry that it would at another LDAP server. Unfortunately, this feature is not yet available on most directory servers.

Secure connections can be used to provide mutual authentication and integrity services at DISP level (if used) or network level (Virtual Private Networks, IPSEC, IPV6).

Secure network connections can be used to provide confidentiality services when personal information are exchanged (HP identification, name, etc.) using Virtual Private Networks, IPSEC, IPV6.

#### *Synchronisation of Workstation local directory and Directory servers*

There is no standard way to provide this service.

There have been attempts in the past by Microsoft and others to write Personal Address Book synchronisation tools for the Microsoft based clients, but these proved to be unreliable and sometimes even changed the wrong entries

Directory access standard protocol: LDAP, etc.

Synchronisation of local and central directories is under the control of the workstation. A specific mechanism, agreed between the directory server and local workstations, is needed.

#### *Synchronisation of Directory servers and TTP (exchange of public key certificates with a certification authority, etc.)*

There is no standard protocol to provide this service.

Exchange public key certificates: X509V3, etc.

Secure connections can be used to provide mutual authentication and integrity services at DISP level (if used) or network level (Virtual Private Networks, IPSEC, IPV6).

Secure network connections can be used to provide confidentiality services when personal information are exchanged (HP identification, name, etc.) using Virtual Private Networks, IPSEC, IPV6.

### **6.3.5.2 Directory server**

Directory server functionality:

Every "commercial" directory server offers data storage and display functions. In most cases, additional functions must be developed to fulfil application's needs.

Directory server certification:

Today, standard products do not plan to process to certification.(ITSEC or ISO CC).

It does not seem to be a need for that (security is based on structure and signature schemes of X509 certificates).

## **6.4 Data and flows**

This chapter and the previous one give a description of the overall architecture that may be used to support the exchange of secured e-mail. Several **mechanisms** could be used for providing a single service may be described here. Recommendations for interoperability are given in chapters "Interoperability needed" and "Requirements for technical components".

### **6.4.1 Information in HPC**

Refer to annex 0 of this document.

### **6.4.2 Network**

The internetworking architecture is based on a IP network and provides:

- Network services (IP, TCP)
- Mail services (SMTP / ESMTP, MIME, etc.)
- Directory services (LDAP, DISP, etc.)
- Security services, including:
  - Mail oriented services (S/MIME, OPEN PGP, X509v3, etc.)
  - On-line oriented services for Directory and TTP exchange protocols (VPN, IPSEC, IPV6, SSL)

In order to be able to digitally sign a message, it is preferable for the workstation needs to be aware of some of the recipient's capabilities (including e-mail address, capability to verify signatures, etc.).

### 6.4.3

## Certificates

### 6.4.3.1 Public key certificates

S/MIME Standard	OPENPGP Standard
<p>S/MIME compliant agent must support X509 V1, X509 V3 certificates as well as some V2 CRLs.</p> <p>Certificates and Certificate-Revocation Lists (CRL's) are signed by the certificate issuer.</p> <p>According to [RFC 2311-SMIME-MSG], a receiving agent must be capable of verifying the signatures on certificates and CRL's made with md5WithRSAEncryption and sha-1WithRSAEncryption signature algorithms with key sizes from 512 bits to 2048 bits. It should be capable of verifying the signatures on certificates and CRL's made with the md2WithRSAEncryption signature algorithm with key sizes from 512 bits to 2048 bits.</p> <p>According to S/MIME V3, a receiving agent must be capable of verifying signatures on certificates and CRL's made with id-dsa-with-sha1</p>	<p>OPENPGP RFC specifies former PGP certificates for backward compatibility. Additional use of X509 certificates has been proposed, and at least three implementations are available</p>

### 6.4.3.2 Attribute certificates

Certificates do not usually include nor certify information that may be crucial for identification or to establish a reliable contact (i.e. HP's authorisations). They also do not allow for temporary changes of personnel in charge, to cope with, for example, vacation schedules.

To alleviate this problem, Netscape has proposed a new type of certificate, to be used together with X.509 Certificates, called Attribute Certificates. These are signed objects that assert additional properties about a particular identity certificate. An attribute certificate has no associated key pair and consequently cannot be used to establish identity.

Informally, one can think of them as a mechanism for extending the attributes of an identity certificate without requiring that the identity certificate be reissued. Formally, they are a "patch" type of solution -- that may introduce a series of inconsistencies (e.g. revocation lists for either type of certificate, cross dependencies, etc.).

Recent meetings on the X.509 standard have discussed what distinguishes an attribute certificate from a public key (identity) certificate; it was argued that there was not much difference (e.g. no public key in an attribute certificate) and that everything that could be included in an attribute certificate could also be included in a public key certificate, which thus could allow attribute certificates to merge with identity certificates within X.509.

Attribute Certificates are outside the scope of this section as they are considered as "data" (i.e. not carried via e-mail protocols or message formats).

## 6.4.4 Digital signature of messages

### 6.4.4.1 Digital signature

Messages are digitally signed using:

- a mechanism for "compacting" data : hashing ( for example some hashing techniques are SHA-1, MD4,

MD5, RIPEMD 160)

- a mechanism for hash encryption: asymmetric algorithm (for example some techniques are: RSA, DSA, ELC)
- a description of the modes of operation, e.g.: PKCS#1, 1.5, 2 etc.

According to S/MIME and OPENPGP, RSA digital signature technique must be compliant with RFC 2313 (PKCS#1).

S/MIME Standard	OPENPGP Standard
According to S/MIME V3, sending & receiving agents must support digital signatures be performed through id-dsa-with-sha1, should support md5WithRSAEncryption, sha-1WithRSAEncryption and may support md2WithRSAEncryption.	According to OPENPGP, digital signatures techniques must be DSA, should be ElGammal (encrypt / sign key), may be RSA (sign only key or encrypt / sign key).  Hash algorithms are: MD2, MD5, SHA1 RIPEMD-160.

According to S/MIME and OPENPGP, a compliant software must be able of verifying digital signatures with any key length.

## 6.4.5 Message encryption

### 6.4.5.1 Encryption

Messages are encrypted using:

- A data encryption algorithm: DES, RC2, 3-DES, IDEA, CAST5, CAST, Blowfish, , etc.<sup>3</sup> Symmetric encryption algorithms are preferable for performance reasons.
- A mode of operation for the encryption algorithm: CBC, EFB, etc.
- A session encryption key which should be randomly generated (with a good random number generator) and which length may vary from 40 bits to 56 bits, 128 bits or more.
- A way to encrypt the session encryption key which should be based on asymmetric algorithms (RSA, DH, etc.) and the appropriate mode of operation (e.g. X9.42 for DH).

Various implementations are described below.

In order to be able to encrypt a message, it is required that the sending workstation is aware of some of the recipient's capabilities (including e-mail address, capability to decrypt message, etc.).

### 6.4.5.2 De facto standard product: S/MIME

Encrypted messages are exchanged using TCP + IP + (E)SMTP + S/MIME.

For data encryption (i.e. message encryption) and according to S/MIME V3, sending and receiving agents must support encryption and decryption with DES EDE3 CBC, called "tripleDES"; they should support encryption and decryption using the DES (also known as DES40<sup>4</sup>) or RC2 (with key size of 40 bits).

For session key encryption and according to S/MIME V3, sending and receiving agents must support Diffie-

<sup>3</sup> Algorithms mentioned in Open PGP and S/MIME standards. AES won't be defined before 2001.

<sup>4</sup> According to RFC-draft, "shortened keys" are obtained by setting to zero the first four bits of every of the 56 significant byte in the key, starting with the first byte

Hellman X9.42 and Should support rsaEncryption (compatibility with S/MIME V2). S/MIME processes D-H with the variant Static – Static. Works are in progress for the use of Ephemeral – Static mode

It is important to notice that S/MIMEv2 uses the same pair of RSA keys for both digital signature and session key encryption. According to NETSCAPE and MICROSOFT , there is a non-standard link in their products between the length of the RSA key and the length of the encryption key used as described below:

RSA key length	Encryption key length
512 bits	40 bits
768 bits	56 bits
1024 bits	128 bits

#### 6.4.5.3 *De facto standard product: OPEN PGP*

Encrypted messages are exchanged using TCP + IP + (E)SMTP + MIME + OPEN PGP.

For data encryption (i.e. message encryption), OPENPGP supports the following techniques:

- Plain text or unencrypted data
- IDEA
- Triple-DES (DES EDE3 Eccentric CFB), 168 bit key derived from 192
- CAST5 (128 bit key, as per RFC 2144)
- Blowfish (128 bit key, 16 rounds)
- SAFER-SK128 (13 rounds)
- DES/SK
- (reserved) AES with 128-bit key
- Proprietary algorithms

For session key encryption, sending and receiving agents must support Elgammal (encrypt only key), should support RSA (sign only or encrypt / sign key) and may support DH X9.42.

The relevant RFC specifies two way of processing D-H: Static – Static (S-S), and Ephemeral – Static (E-S). In this case, D-H Keys are generated at each session by the sending agent.

#### 6.4.5.4 *Use of TTP*

This scenario introduces a new component in the architecture (TTP) and another key management scheme based on DH algorithm (more convenient than RSA algorithm as for instance digital signature key and session key encryption ones are different, see above). In this scenario, the TTP stores HP private keys and provides key escrow or key recovery services (to allow end users to reveal messages in clear upon request).

TTP's could be used in one country or by both countries.

TTP's can either be national (and then not concerned with interoperability), or "cross-border". In that case, the appropriate specifications (compliant with all national regulations) should be defined.

### 6.4.6 Session interface

#### 6.4.6.1 *General*

Online connections are needed in this scenario to allow:

- a workstation to access to a remote Directory server,
- synchronisation between CA's,

- synchronisation between Directory servers.

The networking architecture is based on IP protocols.

Secure connections can be used to provide mutual authentication and integrity services at network level (Virtual Private Networks, IPSEC, IPV6) or above (SSL).

Secure network connections can be used to provide confidentiality services when personal information are exchanged (HP identification, name, etc.) at network level (Virtual Private Networks, IPSEC, IPV6) or above (SSL3).

#### **6.4.6.2 SSL**

Support of public key certificate is similar to S/MIME.

For data encryption (i.e. message encryption), SSL3 supports the following algorithms: RC4/40, RC4/128, RC2/CBC/40, IDEA, DES 40<sup>5</sup> (CBC mode), DES (CBC mode), DES EDE3 CBC.

For session key encryption, SSL supports RSA-encryption (PKCS#1) and Diffie-Hellman (both variants S-S or E-S). SSL makes “direct” use of these algorithms (the client prepares the appropriate hashing for the digital signature ; X9.42 is not used for D-H).

NB: RFC mention that “exportable” software automatically generate a new RSA key if the RSA key length associated with the agent certificate is too long (more than 512 bits).

SSL uses the same pair of RSA keys for both digital signature and session key encryption.

#### **6.4.6.3 ISec**

Support of public key certificate is not described but X509 is usually supported.

For data encryption (i.e. message encryption), an IPSec tunnel must support DES (CBC mode) and RC5, should support 3-DES (many modes of operation including DES EDE3 CBC), and may support Blowfish & CAST5

For session key encryption, an IPSec software must support Diffie-Hellman (“Ephemeral – Static” variant) with X9.42 mode of operation and should support RSA (PKCS#1).

IPSec uses the same pair of RSA keys for both digital signature and session key encryption.

## **6.5 Interoperability needed**

This chapter gives recommendations to solve interoperability issues in the context of cross-border secure e-mail exchanges. It contains recommendations made on the basis of the information given in the previous chapters.

### **6.5.1 Subject of Interoperability**

Interoperability is needed:

- Format conventions for the exchange of secured documents, including digital signature and message encryption.

Non interoperability between sending and receiving agents from different vendors are often noticed.

Since 4Q'98, two procedures exist:

- “S/MIME Enabled” label by RSA Labs.

---

<sup>5</sup> Cf. supra “S/MIME”

- “Interoperability testing events” organised by Internet Mail Consortium (imc-secureconnect WG)
- Conventions for public key certificates (digital signature, encryption)

Reasons for non interoperability between client software and certificates include:

- ***Incorrect implementation:*** The combination of technicalities of ASN1 and X509 result in frequent incorrectly implementation or misinterpretation of the standards.  

What is currently missing is a formal means of testing certificates against a reference implementation or having the services of an inter-operability laboratory. What often exists is a series of bilateral tests/agreements or groups of vendors working together.
- ***Unsupported Algorithm:*** A HP may receive a certificate that has been signed using an algorithm not supported by his client software (for instance if it only supports RSA , but receives a DSA signed certificate).
- ***Unsupported Extensions:*** A Certificate is a very sophisticated structure and can contain many optional fields. The introduction of version 3 X.509 Certificates added a new sub-structure – that of extensions. A X.509 v3 certificate can have, none, one or more extensions fields, each defined by an OID. A number of standard extensions are defined by ISO/IETF – but various software providers or communities have defined their own extensions. For example the banking community defining their own extensions for defined applications. An example of extensions frequently source of non interoperability is *keyusage* (used to indicate the intended use of the public key, for instance digital signature, encryption or key encryption). The concept of *criticality* ( each extension is marked as to whether it is critical or not) is also misinterpreted by some software.
- ***Unsupported Version:*** There are in fact 3 versions of X.509 certificates, version 1, 2 and 3. Version 1 and 3 certificates are more common, with version 3 being the new de facto standard. Version 2 capable software which are still in use) is not able to process version 3 certificates – however it is normally the case that the opposite situation works.
- If RSA is used for encryption scheme, conventions for key exchange [or key agreement certificates] , including conventions between TTP’s must exists (not needed with Diffie-Hellman scheme).
- Conventions for directory services (certificate retrieval, certificate revocation lists).

## 6.5.2 Conventions and Standards

### *Conventions for protocols*

The internetworking architecture should be based on an IP network and provides services, including:

- Mail services (SMTP / ESMTP)
- Directory services (DISP, LDAP)
- Related security services such as IP tunnelling capabilities, secured sessions, transport of digital signatures and encrypted data, transport of keys and certificates, etc. (IPSEC, SSL).

Since no IPV4 / IPV6 gateway product is able to convert security content of IPV6 (today and in the near future), IPV6 is not recommended for interoperability purpose.

SSL should fully comply with the relevant RFC, with the following restrictions :

- Encryption algorithms using keys smaller than 56 bits should not be used.
- The digital signature key pairs stored in the HPC must never be used for SSL session key encryption.
- Digital signatures made by SSL/RSA should not have any “legal” value as the same key pair is also used for session key encryption.

IPSec should fully comply with the relevant RFC's, with the following restrictions :

- An IPSec implementation should at least support the "aggressive mode" for IKE.
- Encryption algorithms should be DES EDE3 CBC and may be DES (CBC) or RC5.
- The usual session key encryption algorithm is D-H (E-S). When using IPSec protocol in cross-border transmissions, in some cases (not yet exactly defined), RSA should preferably be used to allow legal key recovery<sup>6</sup>.

#### **6.5.2.1 Conventions for mail formats**

As there is no interoperability between a S/MIME compliant software and an OPENPGP compliant one today :

- S/MIME is the recommended format to be used.
- OPENPGP is also to be supported on reception.

#### **6.5.2.2 Conventions for certificates**

Use X509 V3 for public key certificates is mandatory. For calculation of digital signature of certificates and CRL's :

- sha-1WithRSAEncryption signature algorithm should be preferred,
- md5WithRSAEncryption and id-dsa-with-sha1 may also be used,
- md2WithRSAEncryption should not be used.

It is recommended to use 2048 bits<sup>7</sup> keys to calculate RSA digital signatures on certificates. 1024 bits keys could be used in an interim period.

#### **6.5.2.3 Conventions for mail digital signature**

As most of the "S/MIME enabled" software available are S/MIME2 compliant (at this time), digital signature must be computed by sending agents according to sha-1WithRSAEncryption.

Digital signature should be generated with 1024 bits RSA keys. Smaller keys (768 bits, even 512 bits) may be used in intermediate software versions. The digital signature key pair should never be used for session key encryption purpose.

Receiving agent must be able to verify signatures made with sha1WithRSAEncryption and may be able to verify signatures made with md2WithRSAEncryption or md5WithRSAEncryption. Receiving agents should be able to verify digital signature with RSA keys up to 1024 bits.

Sending agents should be able to compute digital signature with at least one of the following RSA modes of operation : PKCS#1 and/or (ISO 9796-1 or ISO 9796-2 with random number).

Receiving agents should be able to verify digital signature made with all the following RSA modes of operation : PKCS#1, ISO 9796-1 and ISO 9796-2.

#### **6.5.2.4 Conventions for mail encryption**

---

<sup>6</sup> No key recovery can be easily done with D-H in E-S variant since the sender's secret key is randomly defined for each session.

<sup>7</sup> There may be national constraints on minimum key length to be used. There are still discussions on this topic at European level.

Sending agents should use “triple DES” DES EDE3 CBC. Sending agents may also support DES 56 bits from 64 bits (because of exportation rules, some countries may not be able to provide “triple DES” encryption).

A sending agent must announce, among other things, its decrypting capabilities in its order of preference.

Receiving agents should support “triple DES” DES EDE3 CBC, DES 56 bits from 64 bits and IDEA.

NB : OPENPGP compliant agents must reference DES EDE3 CBC as “proprietary”.

#### **6.5.2.5 Conventions for encryption key exchange**

Diffie-Hellman X9.42 should be supported in the Static – Static variant.

Because a HP can receive messages from non-HP correspondents, RSA Encryption with encrypt only key may be used when standard products are unable to proceed D-H encryption.

RSA Encryption may be used with encrypt only key. RSA Encryption with encrypt/sign key should not be used.

D-H with the E-S variant may be used. In this last case, D-H cannot be processed by a smart card, and no storage of secret key by a TTP could be processed (implies that data recovery of enciphered texts is impossible )

#### **6.5.2.6 Conventions for directory services**

Directory services include :

- Certificate server :
  - Users should have secured communications (integrity, confidentiality) with certificates servers. Workstations should use SSL / HTTP or SSL / LDAP in order to get their correspondent's certificates.
  - Users could also exchange their certificate with preliminary VCARD transmission.
- Synchronisation of directory servers, if needed, should be specified case by case, due to the number of proprietary protocols that can be found. However, IPSec VPN should be used to encapsulate DIS or proprietary protocols between servers.
- Synchronisation of directory servers and TTP, if needed, should be specified case by case, due to the lack of standardisation. However, IPSec VPN should be used to encapsulate protocols between servers.
- There is no recommendation to provide automatic synchronisation of workstation local directories with directories servers. Each user should have to fetch the new attributes of it's correspondents in case of modification.

## **6.6 Possible evolution**

This chapter gives some indications on possible evolutions for the Secure Messaging specifications.

### **6.6.1 Protection Profiles**

All recommendations made in this section to allow interoperability for Secure Messaging (digital signature of messages, encryption of messages) have been made with „free text“.

According to the discussions held at European and International levels on exchange of secure documents (mainly on digital signature), NETLINK recommends that such specifications should be done using ISO Common Criteria by defining the appropriate Protection Profiles. Nevertheless, it is strongly recommended to put the emphasis onto the security level evaluation when building-up an inter-operable and secure data exchange profile.

This way of describing technical specifications has several advantages:

- It gives objectives for the whole system and neither give a limited description of it nor impose mechanisms
- It follows standards that forces to unique interpretation of the recommendations
- Mutual recognition between countries of the ISO CC certification scheme

### 6.6.2 Encryption

This documents gives recommendations for session key encryption (see above : use of DH, etc.). However, there may be new proposals, still based on DH but with some variants, may emerge. In such a case, these new proposals will need to be further discussed.

In addition to this, there may be some evolutions in national regulations on cryptography that would for instance impose new requirements (e.g. on data recovery or key recovery services). This document has anticipated as much as possible such evolutions. However, if new requirements emerge, they would have to be analysed.

### 6.6.3 Certificates

PKCS#15 is complementary to PKCS#11 and will be designed to enhance support of multiple smart cards on a single workstation. It specifies a syntax for storing credentials (keys, certificates, PINs, etc.) on smart card and for describing how they are accessed. In practice, it defines the structure and content of a specific DF in the card's memory for storing pointers toward the "real" EF's where credentials are stored.

This specification is rather new : RSA Labs has posted the final draft version of this PKCS February 11, 1999, and the first official version is planned for summer '99.

This subject seems interesting, especially for HPC interoperability. However, no proposition can be made today because of the "immaturity" of the draft specification, and the lack of "commercial" implementation.

### 6.6.4 Algorithms

Signature algorithms such as DSA and ELC may be added later.

Hash algorithms such as RIPEMD160 may be added later.

New encryption algorithms will be specified in the near future, e.g. AES in 1999/2000. They may become widely accepted de facto standards.

As encryption algorithms are specified to be implemented in all types of environments, it may be envisaged that new ones, dedicated to smart cards, could be specified to address performance and security issues that are specific to smart cards.

### 6.6.5 TTP

It is likely that some consortium of PKI software vendors will adopt PKIX protection in the near future for certificates distribution instead of proprietary protocols.

## 6.7 Requirements for technical components

Starting from the recommendations given in the "Interoperability needed", this chapter specifies the requirements on all technical components.

## 6.7.1 HPC (Health Professional Card)

HPC have to be compliant with the following recommendations.

### 6.7.1.1 Digital signature

The digital signature algorithm & keys (for calculation only) must be implemented in the HPC.

The digital signature key must be different from other ones that could be used for other purposes such as authentication or session key encryption. "Key Usage" must be explicitly defined, and use of encrypt / sign key should not be allowed.

Digital signature should be generated with 1024 bits RSA keys. Smaller keys (768 bits, even 512 bits) may be used in intermediate software versions.

The mode of operations can be processed in the workstation or in the HPC. At least one of the following RSA modes of operation should be implemented in the HPC : PKCS#1 or [ISO 9796-1 or ISO 9796-2 with random number generated by the HPC].

Public key certificates and attribute certificates can be stored on the HPC or on the workstation depending on the card holder behaviour.

Digital signature computation should only be possible once the HPC has successfully authenticated the card holder (i.e. the HP). Mechanisms such as PIN protection could then be used.

### 6.7.1.2 Message encryption

HPC is not neither used for data encryption (i.e. encryption of the message to be sent) nor for data decryption (i.e. decryption of the received message).

Session key encryption may be processed by the HPC (more specifically when D-H – S-S is used), but processing by the agent on the workstation may also be admitted.

Session key decryption may be processed by the HPC (use of D-H – S-S or RSA), but processing by the agent on the workstation may also be admitted<sup>8</sup>.

When HPC is used for session key encryption / decryption :

- Asymmetric algorithm and private keys must be processed in the HPC,
- Mode of operation (X9.42 for D-H and PKCS#1 for RSA) should be implemented in the HPC with SHA-1 as the minimum set of hashing algorithms,
- HPC should be used to generate random numbers (session key),
- Session key encryption / decryption should only be possible once the HPC has successfully authenticated the card holder (i.e. the HP); mechanisms such as PIN protection could then be used.

The session key encryption key must be different from other ones that could be used for other purposes such as authentication or digital signature. Thus, the X509 public key certificate should include a "key usage" extension.

### 6.7.1.3 HPC Certification

In order to allow interoperability between very large (i.e. national) Information Systems, HPC needs to be trusted thus certified according to ISO Common Criteria. The HPC as a whole should be evaluated (i.e. OS and processor in combination, not separately).

---

<sup>8</sup> It has to be noticed that session key encryption using HPC provides a more secure solution but imposes some constraints in terms of ergonomic features.

A Protection Profile accepted at an international level should be specified (including all, but not limited to, the security mechanisms listed above).

## 6.7.2 Card Terminal

There are no requirements on Card Terminals to solve interoperability issues.

## 6.7.3 Workstation

### 6.7.3.1 Protocols

The internetworking architecture should be based on an IP network and provides services, including:

- Mail services (SMTP / ESMTP)
- Directory services (SSL / LDAP or SSL / HTTP)

Since no IPV4 / IPV6 gateway product is able to convert security content of IPV6 (today and in the near future), IPV6 is not recommended for interoperability purpose.

SSL should fully comply with the relevant RFC, with the following restrictions :

- Encryption algorithms using keys smaller than 56 bits should not be used.
- The digital signature key pairs stored in the HPC must never be used for SSL session key encryption.
- Digital signatures made by SSL/RSA should not have any “legal” value as the same key pair is also used for session key encryption.

### 6.7.3.2 Mail formats

As there is no interoperability between S/MIME compliant software and OPENPGP software today :

- S/MIME is the recommended format to be used.
- OPENPGP is also to be supported on reception.

As automatic recognition of OPENPGP formats by MIME agents is not yet supported, it is highly recommended to add facilities in MIME agents (buttons) for improving ergonomic use of both technologies.

### 6.7.3.3 Messaging agent

#### *Sending agent*

Certificates	<p>Use X509 V3 for public key certificates is mandatory.</p> <p>A sending agent should be able to verify digital signatures on public key certificates and CRL's made with sha-1WithRSAEncryption signature algorithm or md5WithRSAEncryption or id-dsa-with-sha1.</p> <p>It is recommended to use 2048 bits keys to verify digital signatures on certificates. 1024 bits keys could be used in an interim period.</p>
Digital Signature	<p>Digital signature must be computed by sending agents according to sha-1WithRSAEncryption.</p> <p>Digital signature should be generated with 1024 bits RSA keys. Smaller keys (768 bits, even 512 bits) may be used in intermediate software versions.</p> <p>Sending agents should be able to compute digital signature with at least one of the following RSA modes of operation : PKCS#1, and/or [ISO 9796-1 or ISO 9796-2 with random number].</p>

Data Encryption	<p>Data encryption algorithms (i.e. algorithms for the encryption of the message to be sent) must be processed by the agents on the workstation.</p> <p>Depending on recipient capabilities, the sending agents should preferably use “triple DES” DES EDE3 CBC and may also use DES 56 bits from 64 bits (because of exportation rules, some countries may not be able to provide “triple DES” encryption).</p> <p>A sending agent must announce, among other things, its decrypting capabilities in its order of preference.</p> <p>NB : OPENPGP compliant agents must reference DES EDE3 CBC as “proprietary”.</p>
Key Encryption	<p>Diffie-Hellman X9.42 should be supported in the Static – Static variant.</p> <p>RSA Encryption may be used with encrypt only key. RSA Encryption with encrypt/sign key should not be used.</p> <p>D-H with the E-S variant may be used. In this last case, D-H cannot be processed by a smart card, and no storage of secret key by a TTP could be processed (implies that data recovery of enciphered texts is impossible).</p>

Although it is not relevant for interoperability, sending agent should provide ergonomic facilities to users for choosing a secured mode. They may provide “by default” options.

#### *Receiving agent*

Certificates	<p>Use X509 V3 for public key certificates is mandatory.</p> <p>A receiving agent should be able of verifying digital signatures on public key certificates and CRL's made with sha1WithRSAEncryption signature algorithm or md5WithRSAEncryption or id-dsa-with-sha1.</p> <p>It is recommended to use 2048 bits keys to calculate digital signatures on certificates. 1024 bits keys could be used in an interim period.</p>
Digital Signature	<p>Receiving agent must be able to verify signatures made with sha1WithRSAEncryption, and may be able to verify signatures made with sha1WithRSAEncryption, md2WithRSAEncryption, and md5WithRSAEncryption.</p> <p>Receiving agents should be able to compute digital signature with RSA keys from 512 bits up to 1024 bits.</p> <p>Receiving agents should be able to verify digital signature made with all the following RSA modes of operation : PKCS#1, ISO 9796-1 and ISO 9796-2.</p>
Data decryption	<p>Data decryption algorithms (i.e. algorithms for the decryption of received messages) must be processed by the agents on the workstation.</p> <p>Receiving agents should support “triple DES” DES EDE3 CBC, DES 56 bits from 64 bits and IDEA</p>
Key decryption	<p>Diffie-Hellman X9.42 should be supported in the Static – Static variant.</p> <p>Because a HP can receive messages from non-HP correspondents, Rsa with encrypt only key may be used when sender's standard products are unable to proceed D-H encryption.</p> <p>RSA with encrypt/sign key should not be used..</p> <p>D-H with the E-S variant may be used. In this last case, D-H cannot be processed by a smart card, and no storage of secret key by a TTP could be processed (implies that data recovery of enciphered texts is impossible).</p>

Although it is not relevant for interoperability, receiving agent should inform the user of the secured / unsecured characteristics of received messages. They may provide “ignore ” options.

#### *Regulation compliance*

Because of national export / import rules, it is possible that some messaging agents (using 128 bits data encryption for example) will remain in use only in their country. Interoperability with other software in use abroad must be tested, on the basis of the above specifications and “interoperability contests”;

Regulation of some countries may interfere with 128 bits cross-border encryption, without TTP (see infra).

Regulation of some countries may not allow at all 128 bits cross-border encryption. Use of 56 bits encryption key should then be envisaged (with or without TTP).

#### **6.7.3.4 Workstation architecture**

No requirements on the use of API's to solve interoperability issues.

Although it is not directly relevant for interoperability, use of structured / standardised security toolkit's in the workstations (such as CDSA, PKCS#11, etc.) should provide a high level of modularity, and possible use of common cryptoki (reducing thus incompatibility subjects).

Although it is not relevant for interoperability, workstations should provide :

- Storage and management of at least e-mail addresses, X509v3 public keys and attributes certificates of the correspondents (display of the local directory contents must also be provided)
- Display of Health Professional own certificates (either stored on the workstation or in a HPC)
- Storage and display of the list of supported CA's
- Reception from a directory service of the Health Professional Identification and certificates
- Broadcasting of public key certificates (VCARD for example)
- Updating of local directories by certificates revocation list

#### **6.7.3.5 Workstation Certification**

Security evaluation of some software components or hardware (e.g. terminals) of the workstation may be envisaged or even required by some applications but is not mandatory to solve interoperability issues.

#### **6.7.4 Directory management system**

Directory services include :

- Certificate server :
  - Users should have secured communications (integrity, confidentiality) with certificates servers. Workstations should use SSL / HTTP or SSL / LDAP in order to get their correspondent's certificates.
  - Users could also exchange their certificate with preliminary VCARD transmission.
- Synchronisation of directory servers, if needed, should be specified case by case, due to the number of proprietary protocols that can be found. However, IPSec VPN should be used to encapsulate DIS or proprietary protocols between servers.
- Synchronisation of directory servers and TTP, if needed, should be specified case by case, due to the lack of standardisation. However, IPSec VPN should be used to encapsulate protocols between servers.

- There is no recommendation to provide automatic synchronisation of workstation local directories with

directories servers. Each user should have to fetch the new attributes of it's correspondents in case of modification.

Communication must be secured by VPN IPSec, according to § Session interface (Cf. infra).

### 6.7.5 TTP

When a certification authority issues a certificate, it is providing a statement to a certificate user (i.e., a receiving HP) that a particular public key is bound to a particular HP.

However, the extent to which the certificate user should rely on that statement by the CA needs to be assessed by the certificate user. In most CA, different certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes.

Usually, three or four classes are available, with various names :

- Elementary - usually only suitable for SSL
- Basic -, limited assurance for basic commercial security (may be used with SSL & S/MIME)
- Medium - suitable for some types of commercial transactions and non-repudiation
- High(or "gold") - suitable for all applications

An X.509 V3 certificate should contain an indication of certificate policy, which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose.

Each CA must publish its own CPS.

It is recommended to issue only certificates from the highest class.

In a multi-CA project, there is a need for consistency between different policies.

That implies that each CA should be cross-certified with others CA - meaning that all CA's have accepted each other security standards and have also agreed to some type of equivalency between their certificates (this is called "policy mapping").

They may also need that TTP's to agree on the existence of the following services in another country :

- Private keys recovery for recovery of data encrypted with a lost key (or for legal reason in some countries).
- Private agreement escrowing

NB : TTP services may be constrained by national rules.

### 6.7.6 Session Interface

The internetworking architecture should be based on an IP network and provides services, including:

- Mail services (SMTP / ESMTP)
- Directory services (DISP, LDAP)
- Related security services such as IP tunnelling capabilities, secured sessions, transport of digital signatures and encrypted data, transport of keys and certificates, etc. (IPSEC, SSL).

Since no IPV4 / IPV6 gateway product is able to convert security content of IPV6 (today and in the near future), IPV6 is not recommended for interoperability purpose.

SSL should fully comply with the relevant RFC, with the following restrictions :

- Encryption algorithms using keys smaller than 56 bits should not be used.
- The digital signature key pairs stored in the HPC must never be used for SSL session key encryption.

- Digital signatures made by SSL/RSA should not have any “legal” value as the same key pair is also used for session key encryption.

IPSec should fully comply with the relevant RFC's, with the following restrictions :

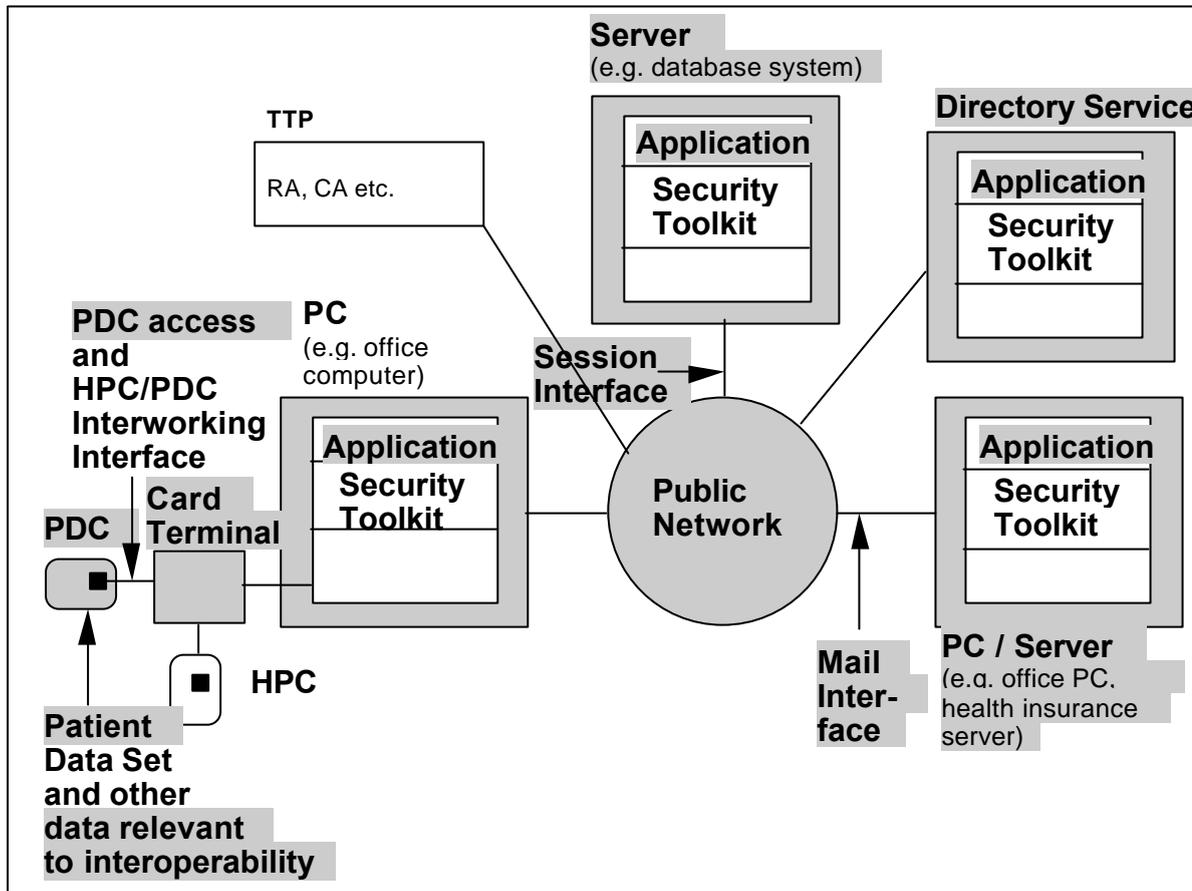
- IPSec implementation should at least support the “aggressive mode” for IKE.
- Encryption algorithms should be DES EDE3 CBC and may be DES (CBC) or RC5.
- The usual session key encryption algorithm is D-H (E-S). When using IPSec protocol in cross-border transmissions, in some cases (not yet exactly defined), RSA should preferably be used to allow legal key recovery<sup>9</sup>.

---

<sup>9</sup> No key recovery can be easily done with D-H in E-S variant since the sender's secret key is randomly defined for each session.

## 7 DB ACCESS

**Fig. 12 DB access Interoperability Scenario**



### 7.1 Scope

The purpose of this chapter is not to dictate the way future medical applications will use databases, but to define a basic concept, that of the card index, which is to extend the storage capacity of the smart card (i.e. external memory) by making use of a telecommunication network and remote databases. This document describes the indexes as pointers to the data stored externally of the card and explains the mechanisms that enable management. Within the scope of Netlink, the applications share and manage this basic concept in the same way.

Interoperability is the result of using the same formal representation of an index in each application, as well as using the same request format to access the relevant database (anonymous database in many cases). Basically, the implementation of the card index concept is based on a Tag-Length-Value combination of the index stored on the card. The way data is stored on the card is described in chapter 0 (4PDC access (free)) and chapter 0 (5 PDC access (protected)).

The secure management of transactions taking place between the card and the databases is not described in this chapter. Public key infrastructure and other features concerning the mode in which the transactions are carried out are described in chapter 0 (6 Secure messaging) or depend on the system developer if there are no interoperability concerns.

In a first version, no online transactions are carried out with foreign databases, but structured secured messages are sent. Online access is not in the scope of this chapter.

In this scheme, a patient or a professional card does not contain all of the administrative and clinical data, but only part of it. The reasons for this are multiple. External memory of the card solves the following problems:

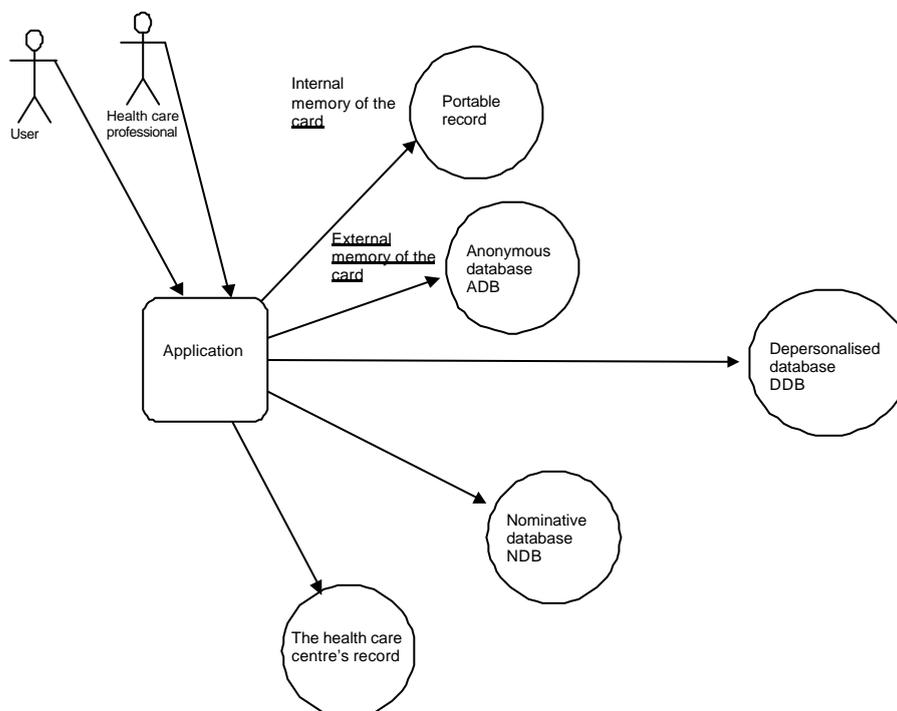
- Limits of the card's physical storage capacity. For instance, telemedicine will require numerous radiography and diagrams.
- Card ubiquity required. The patient data stored in an anonymous database may be accessed from anywhere in the world even if the card, and effectively the patient, are not in the presence of the practitioner, providing the latter has the relevant authorisation from the patient.

The challenge, in terms of implementation, is to access the card's external databases with an appropriate level of security. In fact, microprocessor cards are as well an access key to information highways as a secure data depository.

As shown in Fig. 13, the health smart card system can operate in two modes: a „local mode,, based on the principle of an independent portable record and a „network mode,, based on the principle of remote access and storage. In the local mode, the health smart card holds information which enables it to use off-line administrative and clinical data. In the network operating mode, the system makes the secure access to databases possible, which offers a range of solutions for health insurance (nominative databases of the insurer), clinical decision-making (anonymous databases, also called the card's external memory), the strategic management of health services (depersonalised databases for information on the use of resources).

It is obvious that telecommunication must be efficiently activated by the application making use, for example, of the connection to carry out electronic billing and to simultaneously access the relevant clinical information pointed by indexes.

**Fig. 13 Possible architecture of the health smart card system**



The goal of this chapter is not to dictate how these information databases are to be implemented, this being up to the various system developers, but rather to define a minimum of procedures in order to allow interoperability when needed. These procedures permit to:

- Retrieve the corresponding information by accessing the convenient database

- Update information and distribute it properly to the various databases involved

Imagine these two countries as an example: Healthland and Carekingdom. The architects of both countries may implement their database system as they wish to, but must respect the recommendation of providing a gateway.

When the Carekingdom system discovers a Healthland index on a card, it will know how to send a request to an Healthland server to retrieve and to treat the relative information.

## **7.2 Scenarios**

The goal is to conceive cards with an extended memory, stored on a remote database and to enable practitioners, in telemedicine for example, to retrieve remote data with patient authorisation.

This exchange of information will use the secured messaging, implemented respecting the recommendations of chapter 0.

The scenarios of exchanging information are:

- Retrieving the data pointed by an index (read request)
- Creating a new index (write request)
- Updating data (modification request)
- Deleting data and the index (deletion request)

See below a practical example of database organisation, i.e. Quebec's project, that illustrates the concept of the card index and gives some guidelines to future architects, as well as a generalisation of the scenarios, which is totally independent of the database architecture and which will function in Carekingdom or elsewhere.

### **7.2.1 A Practical Illustration of Health Smart Card System Database Implementation**

As seen above, there are not one but several databases involved in each country. The goal is to have the same access procedures to the Healthland system from any relevant Carekingdom location. Healthland will deal with the requests and localise the appropriate databases using it's own security and data management regulations.

Even if it is, for example, the Healthland system developer's responsibility to choose the appropriate database infrastructure, it is also relevant to give you a example of existing developments, such as the Quebec project (see annex 0).

#### **7.2.1.1 Database Implementation**

The differentiation of the health smart card system's databases is carried out according to their storage and access methods. The storage method concerns the type of information and the way it is divided. The access method concerns the consultation modes of the information and the type of authorisation required. The anonymous database is compared to the depersonalised database in the following table.

table 34: Differentiation of Databases

<i>Storage</i>	Type of information	Dividing the information
<i>Access</i>	Mode of consultation	type of authorisation
<b>ADB</b> <b>Anonymous Database</b>		
<i>Storage</i>	Non nominative information	Record divided into unrelated sections
<i>Access</i>	Consultation of one patient record at a time by an authenticated person	Authorisation of access with the authentication card and the user's card
<b>DDB</b> <b>Depersonalised Database</b>		
<i>Storage</i>	Non nominative information	Record divided into sections that are related to each other
<i>Access</i>	Consultation of one or several records at a time by an authenticated person	Authorisation of access with the authentication card

### 7.2.2 Generalisation of the Scenarios

In the following paragraphs we are going to consider below the case of anonymous databases.

In the anonymous database the record is divided into unrelated sections and no link can be established with the patient's identity. When the database manager reads the information there is no way that he can know to whom the information belongs. The following specifications are a guideline, but each organisation has the choice to use the concept as it deems appropriate.

The general working principle of anonymous databases, is based on the indexing of data stored externally and to which access is only possible with the help of references (indexes) contained in the microprocessor card. Certain data on the card is therefore replaced by an index which can extend the card's storage space and help solve certain data sharing problems (see 0). The use of an anonymous database necessitates a communication link without which the information is not accessible. Several anonymous databases can be used in each country. The localisation of the information must be taken into account during the different cases of use.

Five types of use have been defined to start with:

- read request in the anonymous database
- write request in the anonymous database
- modification request in the anonymous database
- deletion request in the anonymous database

- deletion in the anonymous database by the database manager

Modification request becomes very complex in the case of interoperability between countries, therefore it will not be wholly dealt with.

#### ***7.2.2.1 Read Request in the Anonymous Database***

In this case, a read request accompanied by indexes to read is sent to the IP address corresponding to the index value localisation. The remote server at this address will:

- validate the message according to the secure messaging principles
- extract the index from the message and control it's integrity according to the rule below (paragraph 0)
- access the anonymous database where an index is stored
- pick up the information associated to the index
- Send it back, embedded in the convenient format of secure messaging. All of the information is sent to the client application.

When several indexes are accessed simultaneously, for example several diagnoses for a single card, the client application must be capable of regrouping the indexes by IP address and send one request including all the indexes.

#### ***7.2.2.2 Write Request in the Anonymous Database***

In this case, a write request is accompanied by information to be entered and sent to an acknowledged anonymous database. This generates an index and associates it to the received information. It stores the index and the information and sends the index back to the client application.

The server generates indexes which are held in anonymous database in order to avoid collision.

To keep the maintenance of the system as simple as possible, a Carekingdom practitioner will only be entitled to write Carekingdom indexes, whether the card be from Carekingdom or Healthland.

This means that in the secure messaging system, a remote server will be able to know if the transaction signatures belong to a foreign or domestic requester (see the x.509 structure recommendation).

#### ***7.2.2.3 Modification Request in the Anonymous Database***

In this case, a modification request is accompanied by an index and a new piece of information and is sent to the anonymous database where the index is stored.

It isn't pertinent to authorise a health care professional to modify information that was entered by another health care professional. A validation will be carried out on two levels: one carried out by the country and one by the health care professional himself.

#### ***7.2.2.4 Deletion Request in the Anonymous Database***

An index located on a card issued by Carekingdom, can be deleted only by a Carekingdom application even if the index has been written by Healthland or Carekingdom.

Logically, Carekingdom should delete the index in his anonymous database as well.

#### ***7.2.2.5 Deletion in the Anonymous Database by the Database Manager***

Deletion will be done at a domestic level, therefore the different countries will not be concerned by interoperability. If an index is deleted, further requests for this index will be answered by an error code. Each

country is free to manage it's database, and specifically deletion, by it's own rules. Because the database is anonymous, the probable criteria of deletion will be the date of the last update.

On a practical point of view, a logical deletion is carried out by changing the value of a deletion indicator associated with the index and the information in the anonymous database. A garbage collector will further take care of database maintenance, based on index dates and logical deletions.

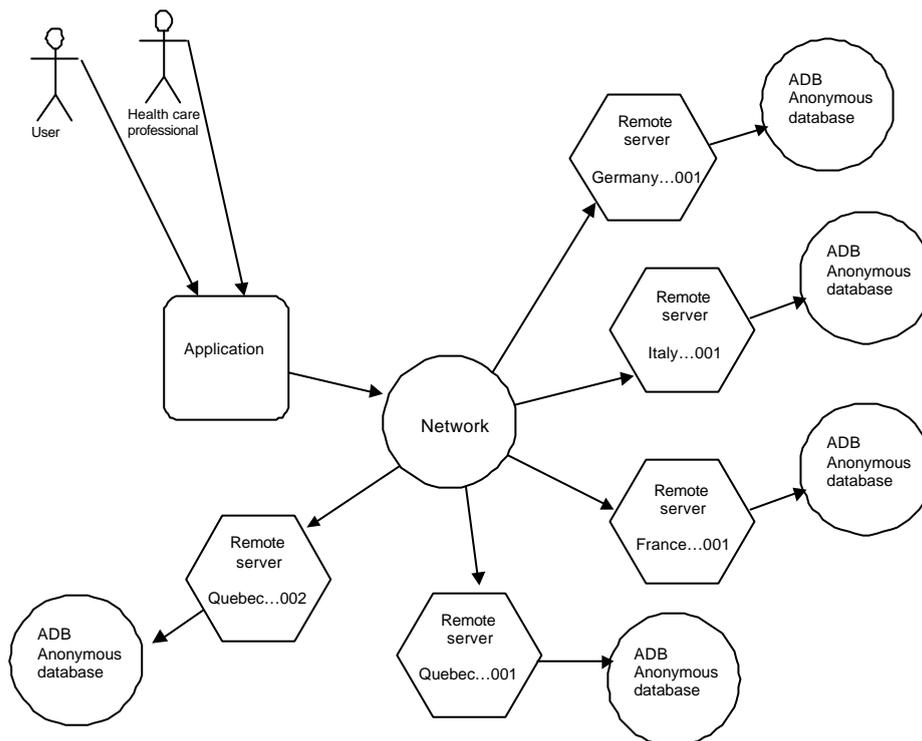
### 7.3

**Technical components (architectural)**

The technical components are:

1. Personal computer
2. Host
3. Network
4. Card
5. Card terminal

**Fig. 14 Architecture of an indexed data system**



**7.4 Data and flows**

The anonymous database (ADB) structure could be as follows:

Name	Data Type	Max Len (bytes)
<b>Anonymous Database</b>		
> Indicators	Byte	1
> Index Number	Binary Number	5
> Index Details	Binary Long Object	undefined
> Details Length	Binary Number	4

**7.5**

## ***Interoperability needed***

### **7.5.1 Subject of Interoperability**

In a first version, no online transactions are carried out with a foreign ADB, but structured secured messages are sent. Secured messaging will therefore be the transport layer of ADB access and so will have to support all interoperability criteria as seen in the previous chapter.

One can conclude that the main concern about interoperability for this chapter is to define a general transaction scheme and to define and then rigorously apply a TLV like structure.

#### **7.5.1.1 General Transaction Scheme**

Both requests shown below use the same type of transaction scheme. One of the request is sent to the remote server and the other comes back from it. All of the „values“ indicated in the tables below are in TLV format and represent a SET in the ASN.1 representation. This chapter deals with the message itself and not with the security attached to it, this being described in the chapter 0 (6 Secure messaging).

General format of the request message (from client to anonymous database):

Note: security needs are not the subject here.

The incoming message is a buffer of bytes of variable length containing the following items:

A request identifier, coming from the client. This identifier shall be joined to the answer message, allowing the client to recognise the request.	long (4 bytes)
A message identifier, specifying the type of request. Each scenario of transaction between the client and the anonymous database is a type of request. See below.	long (4 bytes)
The body of the message containing relevant information. Depending on the current scenario, the body may contain: - a list of indexes (read and deletion requests) number of indexes (long) each index (5 bytes) and / or : - a list of data (write and modification requests) number of data (long) for each data, the length of data (long) + the value (variable length)	long (4 bytes) (body length) + n bytes (body value)

type of request	message identifier
Read	1
Write	2
Modification	3
Deletion	4

General format of the answer message (from anonymous database to client):

Note: security needs are not the subject here.

The outgoing message is a buffer of bytes of variable length containing the following items:

<p>The request identifier, returned to the client. This identifier which is assigned by the client is joined to the answer message, allowing the client to recognise the request.</p>	<p>long (4 bytes)</p>
<p>A message identifier, different from the incoming message identifier. This message identifier permits to interpret correctly the following message body. The returned message identifier will allow the client to know whether the processing of the message in the anonymous database was successful or not. See below.</p>	<p>long (4 bytes)</p>
<p>The body of the message containing the expected returned values. Depending on the current scenario, the body may contain:</p> <ul style="list-style-type: none"> <li>- for a read request, a list of: <ul style="list-style-type: none"> <li>success code (long), index (5 bytes), length of value (long) and value (variable length)</li> <li>or error code (long) and index (5 bytes)</li> </ul> </li> <li>- for a write request, a list of : <ul style="list-style-type: none"> <li>success code (long) and index (5 bytes)</li> <li>or error code (long)</li> </ul> </li> <li>- for a modification request, a list of: <ul style="list-style-type: none"> <li>success code (long) and index (5 bytes)</li> <li>or error code (long) and index (5 bytes)</li> </ul> </li> <li>- for a deletion request, a list of: <ul style="list-style-type: none"> <li>success code (long) and index (5 bytes)</li> <li>or error code (long) and index (5 bytes)</li> </ul> </li> </ul>	<p>long (4 bytes) (body length) + n bytes (body value)</p>

type of error	message identifier
Operation completed with success	0
Operation not carried out	1

### 7.5.1.2 Tag-Length-Value representation

The Tag-Length-Value representation of the data depends on the definition of the information structure. This will be defined in chapter 0 and chapter 0.

The changes that must be carried out on the structure in order to use the indexes concerning the Coded Clinical Details, Immunisation Details and Medication Details are described in annex 0.0 „2 Proposals for Modification (informative)“. The information pointed at by the index is of the same type as the structure in which it is stored.

## **7.6 Possible evolution**

The possible evolutions of the proposed solution are:

concerning the anonymous database:

- simple access with network, differed writing  
In this case, the information is unknown at the time of indexing and the patient authorises the health care professional to differ the writing.
- read pre-authorisation  
In this case, the patient authorises the health care professional to read certain indexed information without his being present. This case is particularly useful for a system of laboratory test requests and results.

in the case of an anonymous database the links between the identity and the data are indirect. In fact the identity and index are in the patient's card's internal memory while the data and index are stored in the anonymous database. Giving pre-authorisation to read enables the health care professional to read information in the anonymous database without the patient's card being present. This case can be useful for a physician who wants to gain access to laboratory test results in the patient's absence. In this case, the identity and the index, contained in the patient's card, are transmitted to the physician's card. The read pre-authorisation can be transmitted from a patient to several health care professionals or from a health care professional to another. For example, a patient can authorise several physicians, therefore not only the prescribing physician, to have access to his laboratory test results. This prescribing physician, who practises medicine in a group, could authorise his colleagues to have access to this information should he be absent. Read pre-authorisation enables the professional to access laboratory test results and is generally appropriate when the patient wants to authorise a health care professional to be able to have access to an element of his record stored in the anonymous database in his absence. Certain rules can be placed in order to limit the access (number of authorised accesses, duration of the pre-authorisation) and to control the transfer (number of authorised transfers, transfers to certain health care professionals only).

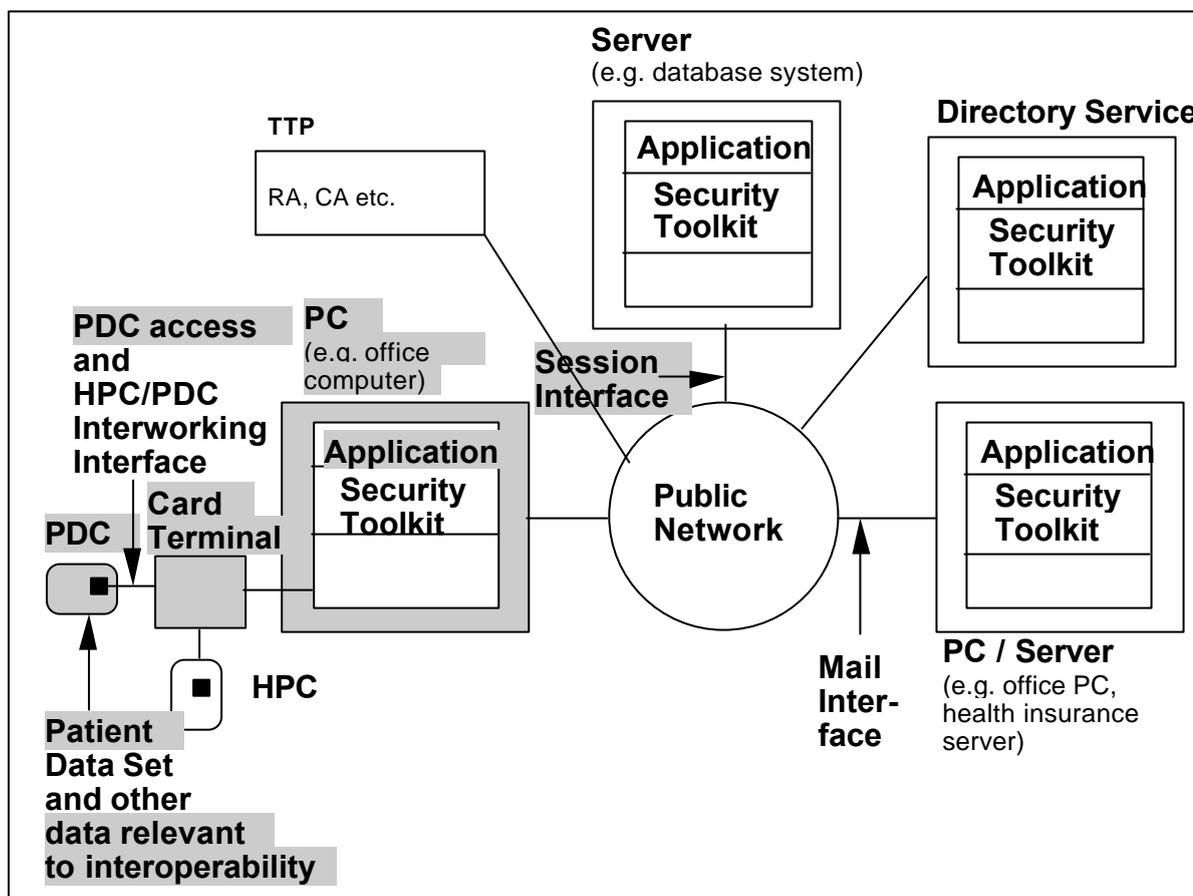
- archiving (meta-indexing)  
In this case, the card storage space can be greatly extended by indexing a set of indexes.

## **7.7 Requirements for technical components**

There are no special requirements for DB access as described.

## 8 PROCEDURE SIMPLIFICATION

**Fig. 15 Interoperability Scenario**



### 8.1 Scope

A key objective of the European Union is to favour the mobility of European citizens also by allowing healthcare to be provided to all, regardless of the location of the healthcare facility or of patient's nationality.

If data cards are to facilitate the availability and exchange of personal medical data across Europe, then the cards must be interoperable.

The introduction of the health card, as a component of the European national health systems, make it possible to simplify the achievement of the following objectives:

- identifying the citizens and their position with respect to the healthcare national systems;
- identifying the national Institution competent for citizens registration and administrative functions management;
- creating a portable personal healthcare file with, among others,
  - administrative elements indicating the general practitioner or paediatrician chosen, the extent to which the citizen contributes to health expenditure, with indication of possible causes for exemption, the insurance coverage and the citizen's entitlement to benefits abroad;
  - fundamental clinical data to be used in case of emergency;
  - references (pointers) to health records available in remotely accessible databases.

The NETLINK project allows to experiment (cross-border):

- secure identification of Patients and doctors;
- procedures and flows simplification;
- reimbursement speed up;
- usage of internationally recognised health data in emergency, first aid and early diagnoses.

Being the health card a proof of the citizen's entitlement to benefits abroad, the information contained in the PDC will be accepted by the health care systems and/or services in the same way as the paper forms E111, E106 and E128 are currently accepted (refer to paragraph 0 below).

The acceptance of the PDC requires mutual trust between the systems of the countries involved and it is based on common verification procedures to be established (refer to paragraph 0).

### 8.1.1 European Regulation and decisions

The EC Regulations N° 1408/71 and N° 118/97 contains the particular provisions to be implemented when international exchanges concerning the reimbursement of health treatment expenses following a medical care supplied to an entitled (wage earner, self-employed, pensioner or student) take place.

The procedure for implementing (EEC) Regulation N° 1408/71 is laid down in (EEC) Regulation N° 574/72. Articles 16 to 34, 93 to 95, 99 to 1078 deal particularly with the health care area.

The Decision 153/93 (refer to annex 0) defines the E-forms that can be used in this area:

a) forms to obtain reimbursement:

E125 actual sum

E127 lump-sum

b) forms to open (or close) a right to reimbursement:

E106, E108, E109, E111, E112, E121, E122,.....

c) "information" forms

E107, E113, E126,...

In the majority of European Member States the health care sector is decentralised. Concerning forms E125 and E127, exchanges take place between (national level) Designated Bodies.

Concerning the E111 form, to be used for emergency care in the case of temporary stay, Article 22 defines "emergency care" as "whose condition that necessitates immediate benefits during the stay in the territory of another Member State".

The judgement of the Court of Justice of the European Communities of 28 April 1998 is related to the interpretation of Articles 30 and 36 of the EC Treaty, in particular concerning the reimbursement of medical expenses occurred in another Member State.

## 8.2 Scenario

With reference to the European Regulation concerning the reimbursement of health treatment expenses provided abroad, the scenario can be depicted as follow:

1. When an European citizen intends to go abroad (for a defined period of time, lower than one year), its local Institution, competent for health administrative issues, instead of providing a paper form E111 or E106 or E128, fills in the areas of the PDC related to the "Entitlement to receive benefits abroad" (refer to [table 35](#) below for the correspondence between the E111 fields and the administrative data in the PDC). If necessary, the physician treating the card holder updates the clinical data contained in the PDC.

2. When the citizen arrives abroad and needs some health service (at hospital or general practitioner office or pharmacies), he can submit its PDC to the service provider to demonstrate its entitlement to receive benefits.
3. The health service provider (hospital doctor or general practitioner or pharmacist) reads the PDC of the citizen and extracts the administrative data necessary for identifying the citizen and for the reimbursement claim (refer to the table in Annex 0 for the *Administrative data* description). The HP can use these data only if he/she trusts the PDC (refer to paragraph 0).
4. In an emergency case (refer to chapter 0) or if the patient gives his/her consensus to access data (see also chapter 0), the health service provider reads the PDC and extracts the emergency data of the citizen (refer to the table in annex 0 for the emergency data description).
5. If necessary, the health service provider can use the pointers contained in the PDC to access remote database containing health records of the citizen (refer to chapter 0).
6. If necessary, the health service provider can use the data contained in the PDC to send a secure e-mail to the physician treating the card holder (refer to chapter 0).
7. Concerning the reimbursement, the citizen can decide which procedure he/she want to apply: usage of E111 or Article 34. In this second case the doctor could directly send an electronic form to the Assurance Body to certify the benefit provided to the citizen. The complete description of the two different scenarios is out of the scope of this document.

The benefits that each country will provide on the basis of the PDC information are the same as for the correspondent paper forms (E111, E106, E128).

### 8.2.1 Project focus and assumptions

The NETLINK project is working in the framework of the current Regulation; this means that this document does not contain proposals for changes.

However changes in regulation are necessary to accept both paper and electronic means; European Commission is strongly recommended to analyse all related aspects and, if necessary, to update the European regulation concerned.

The NETLINK project intends to be a real framework for cross-border experimentation of the organisational, functional and technical aspects related to the usage of PDC as a proof of the citizen's entitlement to benefits abroad, before the European wide implementation and regulation.

Each partner country will promote this solution at national level, making it possible to carry out this experiment in the pilot sites during the project timeframe.

For the purpose of the "Procedure simplification" scenario, it is assumed that the PDC is the citizen smart card to be used for receiving health treatment abroad. This means that the same card should contain international "Administrative" and "Emergency" data.

The international Card, Administrative and Emergency data can be read, and downloaded on the PC, by anybody (HP, Health Insurance Fund, patient) that has a PDC card reader compliant with the technical specification above.

The international Card, Administrative and Emergency data represent the interoperability dataset.

The international Card, Administrative and Emergency dataset are composed of independent objects (refer to paragraph 0) that *can* be present in the PDC, according to the national legislation and the citizen status.

To be *compliant* with the recommendations contained in this document the PC connected to the reader must be able to display all fields belonging to the international Card, Administrative and Emergency dataset.

The patient should have the capability:

- to read by himself data (at least the free-read ones) from his/her PDC, using a kiosk or a dedicated PC

compliant with the technical specification above.

- to control which clinical information are put in the PDC.

The writing of the PDC is out of the scope of this chapter, and it is considered as country-specific (refer to chapter 8.5.2.4 for the basic convention for the PDC acceptance).

### **8.3 Technical components (architectural)**

Technical components are:

- PDC
- Card terminal
- PC/Host

### **8.4 Data and flows**

The software for reading and visualising the data must be able to handle the complete card, administrative and emergency dataset showed below (refer to paragraph 0.2).

### **8.5 Interoperability needed**

#### **8.5.1 Subject of Interoperability**

The subject of interoperability is the “reading” of the administrative and emergency information contained in the PDC. The “writing” of the administrative and emergency information is not addressed by this document as it is considered outside the scope; refer to paragraph 0 for the verification procedures to be put in place.

The approach intends to propose a solution *as much as possible*:

- simple and based on the real situation of the countries involved;
- independent from card operating systems, card readers and architectures;
- using software and tools available on the market;
- based on the already existing international (official and de-facto) standards.

As a consequence, the proposed solution only addresses the *PDC requirements, functions and data*, thus considering the remaining parts of the system (PC, reader, architecture) as a *black-box*.

In this way each country is free to decide its own configuration and architecture: it is only required *to be able to read the PDC according to the following specifications and to respect the minimum set of verification procedures (refer to paragraph 0)*.

The interoperability solution addresses the following items:

- the common administrative and emergency data that can be stored in the PDC;
- the common format of this PDC data;
- the common commands that must be used to read the PDC (free and/or protected access) data.

In order to achieve an European-wide health passport (not to be mixed up with the EC-resolution to introduce an European health passport), it is strongly recommended that all European Member States accept the proposed Administrative data set as the *minimum common* dataset to be stored in the PDC.

In the following paragraphs, the description refers to the PC/SC architecture, but this architecture is not mandatory, as the interoperability is mainly related to the PDC characteristics as defined below (refer to ISO

7816-4 standard).

## 8.5.2

## Conventions and Standards

### 8.5.2.1 Conventions for the physical layer and the transmission layer

Refer to chapter 0.

### 8.5.2.2 Conventions for file selection and data access

Using PC/SC architecture, it is not necessary to provide a health card server; the “PC/SC service provider” component of the card vendor or card issuer can be used.

The access to the card data is hidden by the “service provider” component provided by the card manufacturer, compliant to the PC/SC architecture. This means that it is not necessary to use proprietary/project specific health card server (refer to the Healthcard Client Application calling sequence, using the HS-API and CTM-API, described in EU/G7 Healthcards – WG 7 Interoperability of Healthcard Systems document), and that the file access can be implemented using the standard Client Application calling sequence described in PC/SC.

The following rules apply to the file selection and data access:

- The Administrative, Emergency and Card data structure is coded according to BER-TLV of ASN.1.
- The international *Administrative* data are contained in *one or more* Elementary File of “Transparent” structure. The number and the length of the Administrative EF’s are not fixed, they are country dependent (refer to chapter 0). Each Administrative EF contains *one or more* Groups (refer to 0) belonging to the international Administrative dataset (refer to annex 0).
- The international *Emergency* data are contained in *one or more* Elementary File of “Transparent” structure. The number and the length of the *Emergency* EF’s are not fixed, they are country dependent (refer to chapter 0). Each *Emergency* EF contains *one or more* Groups (refer to 0) belonging to the international *Emergency* dataset (refer to annex 0).
- The international *Card* data are contained in *one or more* Elementary File of “Transparent” structure. The number and the length of the *Card* EF’s are not fixed, they are country dependent (refer to chapter 0). Each *Card* EF contains *one or more* Groups (refer to 0) belonging to the international *Card* dataset (refer to annex 0).
- It is up to the client application to extract and interpret the BER-TLV objects contained in the returned buffers.

### 8.5.2.3 Conventions for the structure and content of the administrative and emergency data set

#### 8.5.2.3.1 Structure

The following rules apply to the structure:

- The data structure is coded according to BER-TLV of ASN.1.
- There are composite data items, called Groups, with tag in the range starting with “A0”, and elementary data items, with tag in the range starting with “80”. The Group items can contain elementary data items and/or composite data items, with tag in the range starting with “A0”, called Sub-groups, in the Value field. All tagged object are defined as IMPLICIT.
- In each EF the first byte is the coded tag for SET (‘31’) followed by the coded length of the groups included in the value field.
- If national data have to be added in the Administrative and Emergency EF’s, it is strongly recommended to use Groups items with tag in the range “B0 to BF”.

8.5.2.3.2 *Content*

With reference to the “EU/G7 Healthcards – WG7 Interoperability of Healthcard Systems” document:

- The Card data that can be stored in the Card EF are listed in table (refer to annex 0).
- The Administrative data that can be stored in the Administrative EF are listed in table (refer to annex 0).
- The Emergency data that can be stored in the Emergency EF are listed in table (refer to annex 0).
- The correspondence between the administrative data and the fields of the E111 form is showed in table 35.

table 35 Correspondence between Administrative data and E111 fields

<i>E111 field number</i>	<i>Administrative data composite tag</i>	<i>Note</i>
1	A0-A0-81	Country
1	A6-A5-82	Professional category
1	A1-82 or A1-87	Surname or Surname at birth
1	A1-83	To be used for supplementary surnames in case of Portuguese and Spanish citizens.
1	A1-85	Forenames
1	A4	Address
1.1	A6-A6-80 or A6-A6-81	Identification number
1.1	A3-80	Date of birth
1.2	A6-A5-83	Scheme
2	A7	Each health card is strictly personal. If the card holder is covered by the insurance policy held by another person (e.g. a relative), his/her card will contain the reference to this person.
3	A6-A5-80	Starting date
3	A6-A5-81	Expiration date
4.1	A6-82	Competent Institution Name
4.1	A6-81	Competent Institution Identifier at national level
4.13-4.11 5.3-5.11	N/A	Stamp and signature requested in the paper copy of the E-form are no more necessary in the electronic flow as the verification procedure is adopted according to the convention below. This means that the modification of the E111 information are only possible for the Insurance organisation; this can be seen as a stamp.
4.2	A6-A3	Competent Institution Address
5	A6	Competent French Institution for non-occupational accidents sustained by self-employed farmers

#### **8.5.2.4 Conventions on common verification procedure**

The acceptance of the PDC requires mutual trust between the systems of the countries involved.

In order to accept a foreign card, at least the following basic conventions should be established to guarantee the mutual trust:

- Robustness of the card itself: it must not be easy to crack the system.
- Data certification level: each PDC must be write protected. Appropriate updating mechanism must assure that only the appropriate body is allowed to modify data in the PDC.
- Revocation list: access to a local or remote revocation list must be made available (may be on line on a national Web site) by each country involved in the project.

Depending on the national legislation, it is up to each country to define the level of protection for PDC writing and the control procedures.

Governments must officially accept these cards as a proof of the citizen's entitlement to benefits abroad. However, in order to avoid many bilateral agreement on this topic, European Commission is strongly recommended to define a common minimum level of protection and verification procedures.

### **8.6 Possible evolution**

In some countries like Italy, the foreign citizen must request a specific administrative paper module at the Local Health Office to obtain general practitioner's treatment. If the general practitioner is able to read the health card, the foreign citizen could avoid to present this administrative paper module. In this case, he will only be requested, at the end of the treatment, to sign the general practitioner coupon stating the service he has received.

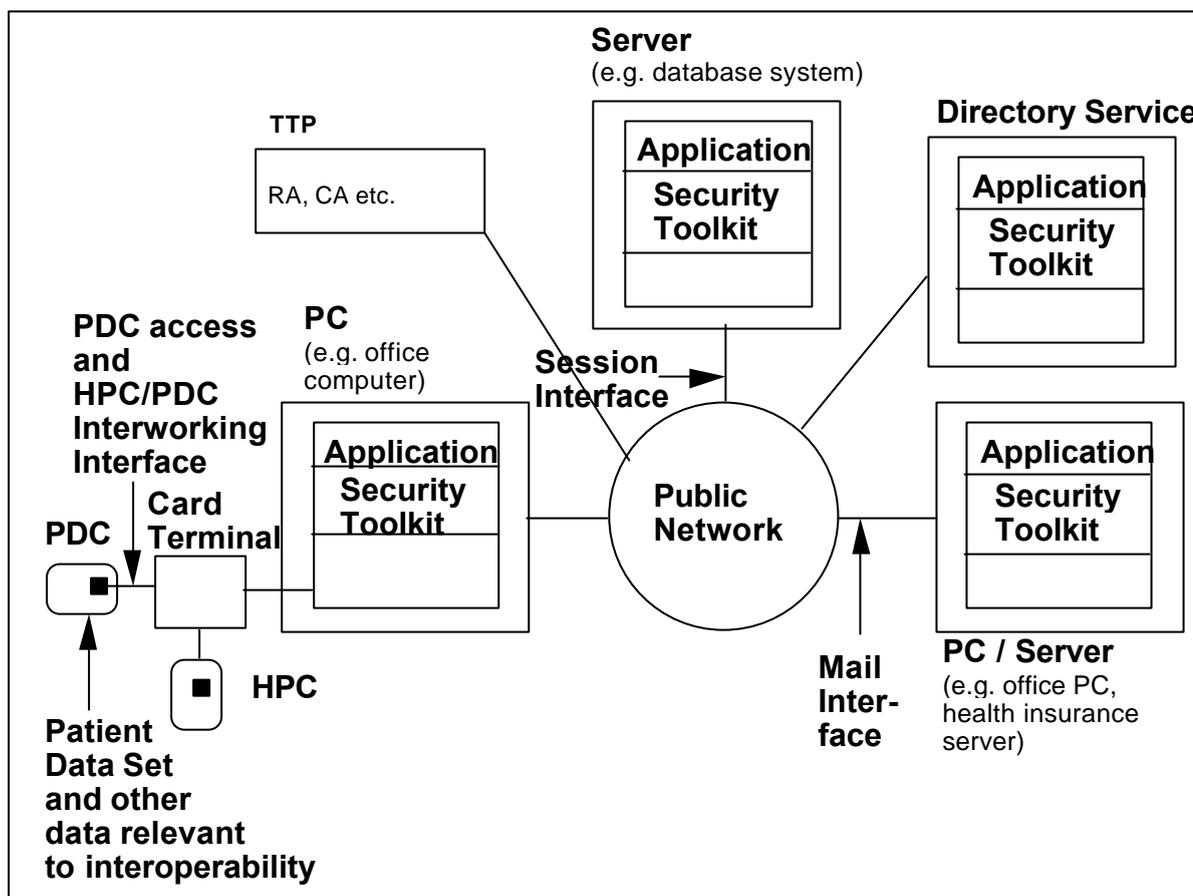
### **8.7 Requirements for technical components**

A detailed definition of the technical aspects can be found in the previous chapters:

- 0 4 PDC access (free)
- 0 5 PDC access (protected)
- 0 7 DB access
- 0 6 Secure messaging

## 9 SUMMARY OF REQUIREMENTS FOR TECHNICAL COMPONENTS

Fig. 16 Consistency Interoperability Scenario



### 9.1 Scope

In this chapter all requirements of the different scenarios are listed. This allows to check whether a specific solution fits to the different scenarios.

This section shall be read having in mind that many possible evolutions have been mentioned (see "Possible evolution" chapters in previous sections).

### 9.2 Requirements for technical components

#### 9.2.1 PDC

PDC's are contact based cards with characteristics according to ISO/IEC 7816-1, 2, 3, 4, 5 and 6. The card size is ID-1. PDC's may be 5Volt- or 3Volt-cards.

In case the patient consent is given by entering a PIN or other techniques, the PDC should have the capability to provide this service.

Refer to chapter 4.5.2.1.2 (ATR, historical bytes,...), 4.5.2.2 (file structure), 8.5.2.3.2 (data) and 8.5.2.4 (robustness and write protection for the PDC characteristics and content).

## 9.2.2 HPC (Health Professional Card)

HPC have to be compliant with the following recommendations.

### 9.2.2.1 Digital signature

The digital signature algorithm & keys (for calculation only) must be implemented in the HPC.

The digital signature key must be different from other ones that could be used for other purposes such as authentication or session key encryption. "Key Usage" must be explicitly defined, and use of encrypt / sign key should not be allowed.

Digital signature should be generated with 1024 bits RSA keys. Smaller keys (768 bits, even 512 bits) may be used in intermediate software versions.

The mode of operations can be processed in the workstation or in the HPC. At least one of the following RSA modes of operation should be implemented in the HPC : PKCS#1 or [ISO 9796-1 or ISO 9796-2 with random number generated by the HPC].

Public key certificates and attribute certificates can be stored on the HPC or on the workstation depending on the card holder behaviour.

Digital signature computation should only be possible once the HPC has successfully authenticated the card holder (i.e. the HP). Mechanisms such as PIN protection could then be used.

### 9.2.2.2 Message encryption

HPC is not neither used for data encryption (i.e. encryption of the message to be sent) nor for data decryption (i.e. decryption of the received message).

Session key encryption may be processed by the HPC (more specifically when D-H – S-S is used), but processing by the agent on the workstation may also be admitted.

Session key decryption may be processed by the HPC (use of D-H – S-S or RSA), but processing by the agent on the workstation may also be admitted<sup>10</sup>.

When HPC is used for session key encryption / decryption :

- Asymmetric algorithm and private keys must be processed in the HPC,
- Mode of operation (X9.42 for D-H and PKCS#1 for RSA) should be implemented in the HPC with SHA-1 as the minimum set of hashing algorithms,
- HPC should be used to generate random numbers (session key),
- Session key encryption / decryption should only be possible once the HPC has successfully authenticated the card holder (i.e. the HP); mechanisms such as PIN protection could then be used.

The session key encryption key must be different from other ones that could be used for other purposes such as authentication or digital signature. Thus, the X509 public key certificate should include a "key usage" extension.

### 9.2.2.3 HPC Certification

In order to allow interoperability between very large (i.e. national) Information Systems, HPC needs to be trusted thus certified according to ISO Common Criteria. The HPC as a whole should be evaluated (i.e. OS and processor in combination, not separately).

---

<sup>10</sup> It has to be noticed that session key encryption using HPC provides a more secure solution but imposes some constraints in terms of ergonomic features.

A Protection Profile accepted at an international level should be specified (including all, but not limited to, the security mechanisms listed above).

### 9.2.3 Card terminal

The card terminals must be able to support contact-based cards with T= 0 and T = 1 transmission protocols.

If PIN-presentation is required, the card terminal with PIN-pad has to be able to deliver the VERIFY-command the way expected by the PDC.

The terminal shall support 5Volt- and 3Volt-cards (class AB).

The terminal should support PPS and be able to transmit data with the highest speed the card indicates (this should at least be configurable).

For HPC/PDC interworking a doubleslot card terminal is highly recommended (for example for performance and security reasons) but other solutions are possible. In case of a plug-in HPC there must be a slot for such cards.

In case the patient consent is made by entering a PIN, the card terminal should have the capability to securely handle PIN presentation to PDC.

### 9.2.4 PC/Host and/or Workstation

#### 9.2.4.1 Interfaces

The PC/Host must be able to connect one or more card terminals (depending on the number of slots) and to support the communication with the highest transmission speed the cards indicate.

#### 9.2.4.2 Protocols

The internetworking architecture should be based on an IP network and provides services, including:

- Mail services (SMTP / ESMTP)
- Directory services (SSL / LDAP or SSL / HTTP)

Since no IPV4 / IPV6 gateway product is able to convert security content of IPV6 (today and in the near future), IPV6 is not recommended for interoperability purpose.

SSL should fully comply with the relevant RFC, with the following restrictions :

- Encryption algorithms using keys smaller than 56 bits should not be used.
- The digital signature key pairs stored in the HPC must never be used for SSL session key encryption.
- Digital signatures made by SSL/RSA should not have any "legal" value as the same key pair is also used for session key encryption.

#### 9.2.4.3 Mail formats

As there is no interoperability between S/MIME compliant software and OPENPGP software today :

- S/MIME is the recommended format to be used.
- OPENPGP is also to be supported on reception.

As automatic recognition of OPENPGP formats by MIME agents is not yet supported, it is highly recommended to add facilities in MIME agents (buttons) for improving ergonomic use of both technologies.

#### 9.2.4.4 Messaging agent

*Sending agent*

Certificates	<p>Use X509 V3 for public key certificates is mandatory.</p> <p>A sending agent should be able to verify digital signatures on public key certificates and CRL's made with sha-1WithRSAEncryption signature algorithm or md5WithRSAEncryption or id-dsa-with-sha1.</p> <p>It is recommended to use 2048 bits keys to calculate digital signatures on certificates. 1024 bits keys could be used in an interim period.</p>
Digital Signature	<p>Digital signature must be computed by sending agents according to sha-1WithRSAEncryption.</p> <p>Digital signature should be generated with 1024 bits RSA keys. Smaller keys (768 bits, even 512 bits) may be used in intermediate software versions.</p> <p>Sending agents should be able to compute digital signature with at least one of the following RSA modes of operation : PKCS#1, and/or [ISO 9796-1 or ISO 9796-2 with random number].</p>
Data Encryption	<p>Data encryption algorithms (i.e. algorithms for the encryption of the message to be sent) must be processed by the agents on the workstation.</p> <p>Depending on recipient capabilities, the sending agents should preferably use "triple DES" DES EDE3 CBC and may also use DES 56 bits from 64 bits (because of exportation rules, some countries may not be able to provide "triple DES" encryption).</p> <p>A sending agent must announce, among other things, its decrypting capabilities in its order of preference.</p> <p>NB : OPENPGP compliant agents must reference DES EDE3 CBC as "proprietary".</p>
Key Encryption	<p>Diffie-Hellman X9.42 should be supported in the Static – Static variant.</p> <p>RSA Encryption may be used with encrypt only key. RSA Encryption with encrypt/sign key should not be used.</p> <p>D-H with the E-S variant may be used. In this last case, D-H cannot be processed by a smart card, and no storage of secret key by a TTP could be processed (implies that data recovery of enciphered texts is impossible).</p>

Although it is not relevant for interoperability, sending agent should provide ergonomic facilities to users for choosing a secured mode. They may provide "by default" options.

*Receiving agent*

Certificates	<p>Use X509 V3 for public key certificates is mandatory.</p> <p>A receiving agent should be able of verifying digital signatures on public key certificates and CRL's made with sha-1WithRSAEncryption signature algorithm or md5WithRSAEncryption or id-dsa-with-sha1.</p> <p>It is recommended to use 2048 bits keys to calculate digital signatures on certificates. 1024 bits keys could be used in an interim period.</p>
Digital Signature	<p>Receiving agent must be able to verify signatures made with sha1WithRSAEncryption, and may be able to verify signatures made with sha1WithRSAEncryption, md2WithRSAEncryption, and md5WithRSAEncryption.</p> <p>Receiving agents should be able to compute digital signature with RSA keys from 512 bits up to 1024 bits.</p> <p>Receiving agents should be able to verify digital signature made with all the following RSA modes of operation : PKCS#1, ISO 9796-1 and ISO 9796-2.</p>

Data decryption	Data decryption algorithms (i.e. algorithms for the decryption of received messages) must be processed by the agents on the workstation.  Receiving agents should support “triple DES” DES EDE3 CBC, DES 56 bits from 64 bits and IDEA
Key decryption	Diffie-Hellman X9.42 should be supported in the Static – Static variant.  Because a HP can receive messages from non-HP correspondents, Rsa with encrypt only key may be used when sender’s standard products are unable to proceed D-H encryption.  RSA with encrypt/sign key should not be used..  D-H with the E-S variant may be used. In this last case, D-H cannot be processed by a smart card, and no storage of secret key by a TTP could be processed (implies that data recovery of enciphered texts is impossible).

Although it is not relevant for interoperability, receiving agent should inform the user of the secured / unsecured characteristics of received messages. They may provide “ignore ” options.

#### *Regulation compliance*

Because of national export / import rules, it is possible that some messaging agents (using 128 bits data encryption for example) will remain in use only in their country. Interoperability with other software in use abroad must be tested, on the basis of the above specifications and “interoperability contests”;

Regulation of some countries may interfere with 128 bits cross-border encryption, without TTP (see infra).

Regulation of some countries may not allow at all 128 bits cross-border encryption. Use of 56 bits encryption key should then be envisaged (with or without TTP).

#### **9.2.4.5 Workstation architecture**

No requirements on the use of API’s to solve interoperability issues.

Although it is not directly relevant for interoperability, use of structured / standardised security toolkit’s in the workstations (such as CDSA, PKCS#11, etc.) should provide a high level of modularity, and possible use of common cryptoki (reducing thus incompatibility subjects).

Although it is not relevant for interoperability, workstations should provide :

- Storage and management of at least e-mail addresses, X509v3 public keys and attributes certificates of the correspondents (display of the local directory contents must also be provided)
- Display of Health Professional own certificates (either stored on the workstation or in a HPC)
- Storage and display of the list of supported CA’s
- Reception from a directory service of the Health Professional Identification and certificates
- Broadcasting of public key certificates (VCARD for example)
- Updating of local directories by certificates revocation list

#### **9.2.4.6 Workstation Certification**

Security evaluation of some software components or hardware (e.g. terminals) of the workstation may be envisaged or even required by some applications but is not mandatory to solve interoperability issues.

#### **9.2.5 Directory management system**

Directory services include :

- Certificate server :
  - Users should have secured communications (integrity, confidentiality) with certificates servers. Workstations should use SSL / HTTP or SSL / LDAP in order to get their correspondent's certificates.
  - Users could also exchange their certificate with preliminary VCARD transmission.
- Synchronisation of directory servers, if needed, should be specified case by case, due to the number of proprietary protocols that can be found. However, IPSec VPN should be used to encapsulate DIS or proprietary protocols between servers.
- Synchronisation of directory servers and TTP, if needed, should be specified case by case, due to the lack of standardisation. However, IPSec VPN should be used to encapsulate protocols between servers.
- There is no recommendation to provide automatic synchronisation of workstation local directories with directories servers. Each user should have to fetch the new attributes of it's correspondents in case of modification.

Communication must be secured by VPN IPSec, according to § Session interface (Cf. infra).

### 9.2.6 TTP

When a certification authority issues a certificate, it is providing a statement to a certificate user (i.e., a receiving HP) that a particular public key is bound to a particular HP.

However, the extent to which the certificate user should rely on that statement by the CA needs to be assessed by the certificate user. In most CA, different certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes.

Usually, three or four classes are available, with various names :

- Elementary - usually only suitable for SSL
- Basic - limited assurance for basic commercial security (may be used with SSL & S/MIME)
- Medium - suitable for some types of commercial transactions and non-repudiation
- High(or "gold") - suitable for all applications

An X.509 V3 certificate should contain an indication of certificate policy, which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose.

Each CA must publish its own CPS.

It is recommended to issue only certificates from the highest class.

In a multi-CA project, there is a need for consistency between different policies.

That implies that each CA should be cross-certified with others CA - meaning that all CA's have accepted each other security standards and have also agreed to some type of equivalency between their certificates (this is called „policy mapping“).

They may also need that TTP's to agree on the existence of the following services in another country :

- Private keys recovery for recovery of data encrypted with a lost key (or for legal reason in some countries).
- Private agreement escrowing

NB : TTP services may be constrained by national rules.

### 9.2.7 Session Interface

The internetworking architecture should be based on an IP network and provides services, including:

- Mail services (SMTP / ESMTP)
- Directory services (DISP, LDAP)
- Related security services such as IP tunnelling capabilities, secured sessions, transport of digital signatures and encrypted data, transport of keys and certificates, etc. (IPSEC, SSL).

Since no IPV4 / IPV6 gateway product is able to convert security content of IPV6 (today and in the near future), IPV6 is not recommended for interoperability purpose.

SSL should fully comply with the relevant RFC, with the following restrictions :

- Encryption algorithms using keys smaller than 56 bits should not be used.
- The digital signature key pairs stored in the HPC must never be used for SSL session key encryption.
- Digital signatures made by SSL/RSA should not have any “legal” value as the same key pair is also used for session key encryption.

IPSec should fully comply with the relevant RFC's, with the following restrictions :

- IPSec implementation should at least support the “aggressive mode” for IKE.
- Encryption algorithms should be DES EDE3 CBC and may be DES (CBC) or RC5.
- The usual session key encryption algorithm is D-H (E-S). When using IPSec protocol in cross-border transmissions, in some cases (not yet exactly defined), RSA should preferably be used to allow legal key recovery<sup>11</sup>.

---

<sup>11</sup> No key recovery can be easily done with D-H in E-S variant since the sender's secret key is randomly defined for each session.

## Annexes

<b><i>A Standards, regulations, ongoing work, national projects (informative)</i></b>	<b>94</b>
<b><i>B Involved parties nationally (informative)</i></b>	<b>101</b>
<b><i>C Glossary (informative)</i></b>	<b>105</b>
<b><i>D The EU/G7 Interoperability dataset - Definition (normative) and NETLINK revision marks (informative)</i></b>	<b>108</b>
<b>1 The EU/G7 Interoperability dataset - Definition (normative)</b>	<b>108</b>
<b>2 Proposals for Modification (informative)</b>	<b>109</b>
Reasons for modifications	109
<b>3 G7-Interoperability-dataset with harmonised NETLINK revision marks</b>	<b>110</b>
1. Coding tables	112
2. Dataset in table form	115
3. Dataset in ASN.1 form	131
4. Card Data in ASN.1 form	131
5. Administrative Data in ASN.1 form	131
6. Clinical Data in ASN.1 form	134
<b><i>E Recommendations for Restrictions for a Core Data Set of EU/G7 - Interoperability - data set (informative)</i></b>	<b>137</b>
<b>1 Usage of the G7-Interoperability-data set</b>	<b>137</b>
Possibilities for reducing the dataset	137
Not using optional data objects	137
Reducing the maximum length of text items	137
Reducing the maximum occurrence of data objects	137
<b>2 Core data set</b>	<b>137</b>
CardData	137
Administrative Data	138
Clinical Data	140
<b><i>F Presentation/Visualisation of G7-Interoperability-dataset (informative)</i></b>	<b>142</b>
<b>1 General remarks</b>	<b>142</b>
<b>2 Card data</b>	<b>142</b>
<b>3 Administrative-Data</b>	<b>143</b>
<b>4 Medical data</b>	<b>143</b>
<b><i>G Secure messaging- Regulation aspects - France (informative)</i></b>	<b>149</b>
<b><i>H DB access - Quebec's example (informative)</i></b>	<b>150</b>

## A Standards, regulations, ongoing work, national projects (informative)

All documents are available in English if not otherwise specified. Standards are structured according to hierarchy (for example: ISO and not CEN).

Coding:	Status:	D	-	European Union Decision	Source:	CAD/Q	-	Canada
		J	-	Judgement of the Court of Justice		FR	-	France
		O	-	Ongoing standard		GER	-	Germany
		P	-	Project		ITA	-	Italy
		R	-	Regulation		Int	-	International
		S	-	Standard				

Card terminal:

Sta-tus	Source	Title	contact address or reference
P	GER	<ul style="list-style-type: none"> <li>MCT - Multifunctional Card Terminal (version 1.0 draft in German)</li> </ul>	<ul style="list-style-type: none"> <li><a href="http://www.darmstadt.gmd.de/TKT/SCT/spec.html">http://www.darmstadt.gmd.de/TKT/SCT/spec.html</a></li> </ul>
P	FR	<ul style="list-style-type: none"> <li>GIE SESAM-VITALE</li> <li>GIP-CPS</li> <li>GIE Cartes Bancaires</li> </ul>	<ul style="list-style-type: none"> <li><a href="http://www.sesam-vitale.fr/">http://www.sesam-vitale.fr/</a> (French)</li> <li><a href="http://www.gip-cps.fr/">http://www.gip-cps.fr/</a> (French)</li> <li><a href="http://www.gie-cartes-bancaires.fr/">http://www.gie-cartes-bancaires.fr/</a></li> </ul>

## Smartcard:

Sta-tus	Source	Title	contact address or reference
P	FR	<ul style="list-style-type: none"> <li>GIE SESAM-VITALE</li> <li>GIP CPS</li> </ul>	<ul style="list-style-type: none"> <li><a href="http://www.sesam-vitale.fr/">http://www.sesam-vitale.fr/</a> (French)</li> <li><a href="http://www.gip-cps.fr/">http://www.gip-cps.fr/</a> (French)</li> </ul>
P	GER	<ul style="list-style-type: none"> <li>German HPC-specification</li> </ul>	<ul style="list-style-type: none"> <li><a href="http://www.zi-koeln.de/">http://www.zi-koeln.de/</a>; chapter „downloads“</li> </ul>
R	FR	<ul style="list-style-type: none"> <li>Ordinance No 96-345 of April 24, 1996 relating to the medical control of the expenditure of care, and in particular its article 8 (French)</li> <li>Decree n°98-275 of 9 April 1998 relative to the health insurance card and modifying the national health service code (French)</li> <li>Decree n°98-271 of 9 April 1998 relative to the health professional card and modifying the national health service code and the public health code (French)</li> </ul>	<ul style="list-style-type: none"> <li><a href="http://www.legifrance.gouv.fr/">http://www.legifrance.gouv.fr/</a></li> <li><a href="http://www.legifrance.gouv.fr/">http://www.legifrance.gouv.fr/</a></li> <li><a href="http://www.legifrance.gouv.fr/">http://www.legifrance.gouv.fr/</a></li> </ul>
S - IS	CEN ISO	<ul style="list-style-type: none"> <li>EN 742</li> <li>ENV 1257 series</li> <li>ENV 1284</li> <li>EN 1387</li> <li>EN 1867</li> <li>ENV 12018</li> <li>ISO/IEC 7816 series</li> </ul>	<ul style="list-style-type: none"> <li></li> </ul>
S - O		<ul style="list-style-type: none"> <li>CEN: „Data logical organisation of patient cards and health care professional cards“</li> </ul>	<ul style="list-style-type: none"> <li></li> </ul>

## Network:

Sta- tus	Source	Title	contact address or reference
P	FR	• <i>RSS Réseau Santé Social: the French healthcare Intranet network</i>	• <a href="http://www.cegetel.rss.fr/">http://www.cegetel.rss.fr/</a>

## Security, Signature, ...:

Sta-tus	Source	Title	contact address or reference
P	FR	<ul style="list-style-type: none"> <li>GIP CPS</li> </ul>	<ul style="list-style-type: none"> <li><a href="http://www.gip-cps.fr/">http://www.gip-cps.fr/</a> (French)</li> </ul>
R	FR	<ul style="list-style-type: none"> <li>Decree n°98-271 of 9 April 1998 relative to the health professional card and modifying the national health service code and the public health code. (French)</li> <li>Decree n°98-275 of 9 April 1998 relative to the health insurance card and modifying the national health service code. (French)</li> </ul>	<ul style="list-style-type: none"> <li><a href="http://www.legifrance.gouv.fr/">http://www.legifrance.gouv.fr/</a></li> <li><a href="http://www.legifrance.gouv.fr/">http://www.legifrance.gouv.fr/</a></li> </ul>
R	GER	<ul style="list-style-type: none"> <li>Information and Communication Services Act (Article 3: Act on Digital Signature)</li> <li>Signaturverordnung (German)</li> <li>Begründung zur Signaturverordnung (German)</li> </ul>	<ul style="list-style-type: none"> <li><a href="http://www.iid.de/rahmen/iukdgeb.html">http://www.iid.de/rahmen/iukdgeb.html</a></li> <li><a href="http://www.iid.de/rahmen/sigv.html">http://www.iid.de/rahmen/sigv.html</a></li> <li><a href="http://www.iid.de/rahmen/sigv_begr.html">http://www.iid.de/rahmen/sigv_begr.html</a></li> </ul>
R	ITA	<ul style="list-style-type: none"> <li>Delegation of power to the Council of Ministers to confer tasks and functions on Regions and local authorities, to pursue the reform of the public administration, and to simplify administrative procedures</li> <li>Regulations establishing criteria and means for implementing Section 15(2) of Law No. 59 of 15 March 1997 concerning the creation, storage and transmission of documents by means of computer-based or telematic systems</li> </ul>	<ul style="list-style-type: none"> <li><a href="http://www.aipa.it/english/law[2/law5997.asp">http://www.aipa.it/english/law[2/law5997.asp</a></li> <li><a href="http://www.aipa.it/english/law[2/pdecree51397.asp">http://www.aipa.it/english/law[2/pdecree51397.asp</a></li> </ul>
S - IS	CEN	<ul style="list-style-type: none"> <li>ENV 12924</li> </ul>	<ul style="list-style-type: none"> <li></li> </ul>
S - O	CEN	<ul style="list-style-type: none"> <li>TC 251: „Framework for Modelling Healthcare Security Policies“</li> </ul>	<ul style="list-style-type: none"> <li><a href="http://www.centc251.org">http://www.centc251.org</a></li> </ul>

Other:

Sta-tus	Source	Title	contact address or reference
P	Int	<ul style="list-style-type: none"> <li>• EU/G7 Healthcards - WG7, Interoperability of Healthcard Systems</li> <li>• PC/SC</li> <li>• OpenCard</li> <li>• Cardlink</li> <li>• Diabcard</li> <li>• ISHTAR</li> <li>• Universal Card Terminal System concept (UCTS)</li> </ul>	<ul style="list-style-type: none"> <li>• <a href="http://www.clinical-info.co.uk/euhci.htm">http://www.clinical-info.co.uk/euhci.htm</a></li> <li>• <a href="http://www.smartcardsys.com">http://www.smartcardsys.com</a></li> <li>• <a href="http://www.opencard.org">http://www.opencard.org</a></li> <li>• <a href="http://www.ehto.org/aim/volume2/cardlink.html">http://www.ehto.org/aim/volume2/cardlink.html</a></li> <li>• <a href="http://www-mi.gsf.de/diabcard/index.html">http://www-mi.gsf.de/diabcard/index.html</a></li> <li>• <a href="http://ted.see.plym.ac.uk/ishtar/">http://ted.see.plym.ac.uk/ishtar/</a></li> <li>• <a href="ftp://ftp.cherry.de">ftp://ftp.cherry.de</a></li> </ul>
R	EU	<ul style="list-style-type: none"> <li>• No 1408/71 of the Council of 14 June 1971 (on the application of Social Security schemes to employed persons, to self-employed persons and to members of their families moving within the Community.)</li> </ul>	<ul style="list-style-type: none"> <li>• Consolidated version Official Journal C 325 of 10 December 1992</li> </ul>
R	EU	<ul style="list-style-type: none"> <li>• No 574/72 of the Council of 21 March 1972 (laying down the procedure for implementing Regulation (EEC) No 1408/71)</li> </ul>	<ul style="list-style-type: none"> <li>• Consolidated version Official Journal C 325 of 10 December 1992</li> </ul>
R	EU	<ul style="list-style-type: none"> <li>• No 118/17 of the Council of 2 December 1996 (amending and updating Regulation (EEC) No 1408/71)</li> </ul>	<ul style="list-style-type: none"> <li>• Official Journal 1997 L 28</li> </ul>
D	EU	<ul style="list-style-type: none"> <li>• No 153/93 (defining the forms (E103-E127) necessary for the application of Regulation (EEC) No 1408/71 and Regulation (EEC) No 574/72)</li> </ul>	<ul style="list-style-type: none"> <li>• Official Journal 1994 L 244</li> </ul>
D	EU	<ul style="list-style-type: none"> <li>• No 165/97 (defining the forms (E128 and e128B) necessary for the application of Regulation (EEC) No 1408/71 and Regulation (EEC) No 574/72)</li> </ul>	<ul style="list-style-type: none"> <li>• Official Journal 1997 L 341</li> </ul>
J	EU	<ul style="list-style-type: none"> <li>• case C-120/95 of 28 April 1998 (proceedings between Nicolas Decker and Caisse de Maladie des Employés Privés)</li> </ul>	<ul style="list-style-type: none"> <li>• n/a</li> </ul>

## Standards:

Source	Year	Status	Title
ISO/IEC 7816 - 1			Identification cards - Integrated circuit(s) cards with contacts - Part 1: Physical characteristics
ISO/IEC 7816 - 2			Identification cards - Integrated circuit(s) cards with contacts - Part 2: Dimension and location of the contacts
ISO/IEC 7816 - 3			Identification cards - Integrated circuit(s) cards with contacts - Part 3: Electronic signals and transmission protocols
ISO/IEC 7816 - 4			Identification cards - Integrated circuit(s) cards with contacts - Part 4: Inter-industry Commands for interchange
ISO/IEC 7816 - 5			Identification cards - Integrated circuit(s) cards with contacts - Part 5: Numbering system and registration procedure for application identifiers
ISO/IEC 7816 - 6			Identification cards - Integrated circuit(s) cards with contacts - Part 6: Inter-industry data elements
ISO/IEC 7816 - 7			Identification cards - Integrated circuit(s) cards with contacts - Part 7: Interindustry commands for Structured Card Query Language
ISO/IEC 7816 - 8			Identification cards - Integrated circuit(s) cards with contacts - Part 8: Security related interindustry commands
ISO/IEC 7816 - 9			Identification cards - Integrated circuit(s) cards with contacts - Part 9: Enhanced interindustry commands
ISO/IEC 7816 - 10			Identification cards - Integrated circuit(s) cards with contacts - Part 10: Operating procedure and ATR for synchronous cards
ISO/IEC 8824			Identification cards - Open Systems Interconnection - Specification of Abstract Syntax Notation One (ASN.1)
ISO/IEC 8825			Identification cards - Open Systems Interconnection - Specification of Basic Encoding Rules for Abstract Syntax Notation One (ASN.1)
CEN EN 742	1993		Identification card systems - intersector ID-1 card location of contacts for cards and devices used in Europe
CEN ENV 1257-1	1994		Identification card system - Rules for PIN - handling in intersection environments - Part 1: PIN presentation
CEN ENV 1257-2	1997		Identification card system - Rules for PIN - handling in intersection environments - Part 2: PIN protection
CEN ENV 1257-3	1997		Identification card system - Rules for PIN - handling in intersection environments - Part 3: PIN verification
CEN ENV 1284	1996		Identification card system - Intersector rules for locking and unlocking of integrated circuit(s) cards
CEN EN 1387	1996		Machine readable Cards - Health care applications - Cards: General characteristics
CEN EN 1867	1997		Machine readable cards - Health care applications - Numbering system and registration procedure for issuer identifiers
CEN ENV 12018	1997		Identification, administrative, and common clinical data structure for intermittently connected devices used in healthcare (including machine readable cards)
CEN ENV 12924	1997		Medical Informatics - Security Categorisation and Protection for Healthcare Information Systems

to be maintained

## B Involved parties nationally (informative)

Co-ordination of national health card project(s) and/or contact address for information about national health card project(s):

Canada	
France	<p><b>GIE SESAM-VITALE</b>  19 Boulevard Alexandre Oyon – 72019 – Le Mans – France  Phone : + 33 2 43 57 42 00  Fax : + 33 2 43 87 78 42  E-mail : gie@sesam-vitale.fr  Web : http://www.sesam-vitale.fr</p>
Germany	<p>There is no central organisation in Germany for the co-ordination of national health card project(s). But there is the „joint panel on HealthCards“, which is a voluntary work group of all health card projects, representatives of ministries and of the local and the national data protection commissioners in Germany. Contact address is:</p> <p><b>Central Research Institute of Ambulatory Health Care in Germany</b>  Höninger Weg 11 5 - 50969 Köln - Germany  Tel.: +49 - 221 - 40 05 - 0  Fax.: +49 - 221 - 40 80 55  e-mail: ZI@KBV.de</p>
Italy	<p>The distribution of the patient cards to the whole Italian population will take place in the next years, under the co-ordination of the:</p> <p><b>Italian Ministry of Health</b>  Lungotevere Ripa 1 - 00152 Roma – Italia</p> <p>Reference persons for the project are:</p> <ul style="list-style-type: none"> <li>• Ms. Nerina Dirindin, General Director Dipartimento Programmazione</li> <li>• Ms. Anna Rita Bove, Senior Project Officer</li> <li>• Mr. Antonio Parrilla, Project Officer</li> <li>• Ms. Alessandra Pastorino, Consultant</li> </ul>

### Regulations

Canada	
France	<p>Both government and congress are in charge of preparing and issuing French regulation (laws, decrees, etc.) that are applicable to the health card information system.</p> <p>The law issued on April 24<sup>th</sup> 1996 (also called “Ordonnance”) gives an overall description of the health card information system as it introduces several concepts : HPC (called “CPS” for “Carte de Professionnel de Santé”), PDC (called “Vitale”), electronic reimbursement claims, etc.</p> <p>Detailed regulation has been published since that date that gives detailed specifications of cards, electronic transactions, etc.</p> <p>A new law will be voted in 1999 to define medical data that can be stored in PDC and the way they will be managed.</p> <p>French Ministry of Health has a specific role in the HP data certification process (with CNAMTS and professional councils)</p>

Germany	Both the Lower and the Upper House of German Parliament are in charge of issuing German regulation (laws, decrees, etc.) that are applicable to the health card information system.  The German Ministry of Health is the highest board of control for the doctor's chambers, the doctor's associations and the health insurances by law.
Italy	Italian Ministry of Health together with national Authorities for „privacy“ (Garante) and IT (AIPA)

### Health Insurances:

Canada	
France	<p>There are many Health Insurance Funds (HIF) in France to insure people from different sectors (employees, farmers, etc.):</p> <ul style="list-style-type: none"> <li>• CNAMTS (Caisse Nationale d'Assurance Maladie des Travailleurs Salariés)</li> <li>MFP (Mutualité de la Fonction Publique)</li> <li>MSA (Mutualité Sociale Agricole)</li> <li>GAMEX (Exploitants Agricoles)</li> <li>AMPI (Assurance Maladie des Professions Indépendantes)</li> <li>UNRS (Union Nationale des Régimes Spéciaux) for Army forces, SNCF, RATP, Bank of France, etc.</li> <li>CAMAC (Cultes)</li> </ul> <p>HIF are in charge of the health expenses reimbursement process (including processing of paper and electronic reimbursement claims).</p> <p>HIF are in charge of issuing PDC (as indicated in the law issued in 1996), thus responsible for data management for the insured persons (and data certification). To maintain the coherence and to help patient data certification process, there is also a central directory (called "RNIAM") operated by CNAVTS (another French Social Security organism) that keeps the identification of all citizens ("social security unique number", name, first name) as well as the identification of the HIF they are affiliated to.</p> <p>CNAMTS has a specific role in the HP data certification process (with FMH and professional councils).</p>
Germany	<p>The health insurances in Germany can be divided into statutory health insurances and private insurances. The statutory health insurances (there are about 1.000) are organised in different federal associations:</p> <ul style="list-style-type: none"> <li>• AOK-Bundesverband K.d.ö.R. (National Association of Local Sickness Funds - public corporation)</li> <li>Bundesverband der Betriebskrankenkassen K.d.ö.R. (National Association of Industrial Sickness Funds - public corporation)</li> <li>IKK-Bundesverband K.d.ö.R. (National Association of Trade Guild Sickness Funds - public corporation)</li> <li>Bundesverband der landwirtschaftlichen Krankenkassen K.d.ö.R. (National Association of Agricultural Sickness Funds - public corporation)</li> <li>Bundesknappschaft K.d.ö.R. (Federal Miners' Guild - public corporation)</li> <li>Seekrankenkasse, Abtlg. der Seekasse K.d.ö.R. (Sailors' Sickness Fund - public corporation)</li> <li>Verband der Angestellten-Krankenkassen e.V. (Association of White Collar Workers' Sickness Funds - registered association)</li> <li>AEV Arbeiter-Ersatzkassen-Verband e.V. (Association of Blue Collar Workers' Substitute Sickness Funds - registered association)</li> </ul> <p>The private health insurances are organised in a different way. There is a voluntary association but not each insurance is member:</p>

	Verband der privaten Krankenversicherung“ Bayenthalgürtel 26 - 50968 Köln - Germany Tel.: +49 - 37662 - 0 Fax.: +49 - 37662 - 10
Italy	Ministry of Health together with Health local offices (USL)

PDC:

Canada	
France	<p>GIE SESAM VITALE objectives are : studies, development, standardisation, implementation, promotion of the of the SESAM-VITALE system, the Vitale Card and related services.</p> <p>GIE SESAM VITALE is in charge of several R&amp;D, design, development, system integration and standardisation activities on Vitale smart card, smart card readers and associated software, servers for HIF, system management tools, telecommunication protocols, security architecture (SESAM-Vitale), etc.</p> <p>GIE SESAM-VITALE is also in charge of several exploitation tasks : issuer of Vitale cards (role given by HIF), Vitale management (CA, etc.), distribution of smart card readers, smart card reader management ,etc.</p>
Germany	<p>The „German health insurance card“ is issued to each insured person of a statutory health insurances on base of § 291, Para. 3, of the German Code of Social Law, Vol. V (SGB V). Each insurance company is issuing its own card based on an agreement of the federal associations mentioned above and the Kassenärztliche Bundesvereinigung K.d.ö.R. (National Association of Panel Doctors - public corporation).</p> <p>The private insurance companies are also issuing an insurance card but on voluntary basis. The contact address is:</p> <p style="padding-left: 40px;">Verband der privaten Krankenversicherung“          Bayenthalgürtel 26 - 50968 Köln - Germany          Tel.: +49 - 37662 - 0          Fax.: +49 - 37662 - 10</p>
Italy	Ministry of Health will define the guidelines at national level.

HPC:

Canada	
France	<p>GIP CPS is in charge of several R&amp;D, design and development on CPS smart card, CPS smart card readers, system management tools, etc.</p> <p>GIP CPS is also in charge of several exploitation tasks : issuer of CPS cards, CPS management (CA, etc.), distribution of smart card readers, smart card reader management ,etc.</p>
Germany	The issuing of a HPC is the task of the national doctor's chambers as an identification card for physicians.
Italy	Ministry of Health will define the guidelines at national level.

Network:

Canada	
--------	--

France	<p>The RSS (for “Réseau Santé Social”) is a “public service” operated by the private company CEGETEL.RSS, i.e. its receives a delegation from FMH to operate the network with many objectives / constraints on security, quality of service, interoperability.</p> <p>The contract signed with FMH is 5 years long.</p> <p>RSS is an IP based network dedicated to HP and other actors from the Health Care sector. It provides TCP/IP connectivity, e-mail and directory services in a secure way. Users are authenticated via their own CPS (i.e. it is not possible to connect to the network without an HPC). Data exchanged over the network are digitally signed and encrypted.</p> <p>HIF have to connect to the network to receive the electronic reimbursement claims. HP may connect to an ISP to send ERC.</p>
Germany	<p>There are several medical networks, one of them is the „DGN“ („Deutsches Gesundheitsnetz“, German health net; <a href="http://www.dgn.de">http://www.dgn.de</a>).</p>
Italy	<p>Ministry of Health together with the Regions.</p>

## C Glossary (informative)

abbreviation	text	comment and/or reference
	Card external memory	synonym of an anonymous database
	Carekingdom	imaginary country
	Healthland	imaginary country
	Index	number or reference that permits the user to find information in the anonymous database
ADB	Anonymous database	shared database which stores non nominative data and whose patient records are divided into unrelated sections
AID	Application Identifier	
ATR	Answer-To-Reset	
AUT	Authentication	
BER	Basic Encoding Rules	
C	Certificate	
CA	Certification Authority	
CAR	Certification Authority Reference	
CH	Cardholder	
CHA	Certificate Holder Authorisation	
CHR	Certificate Holder Reference	
CPI	Certificate Profile Identifier	
CRL	Certificate Revocation List	
CV	Card Verifiable (Certificate)	
DDB	Depersonalised database	shared database which stores non nominative data and whose patient records are divided into related sections
DES		ANSI X3.106, "American National Standard for Information Systems-Data Link Encryption", American National Standards Institute, 1983.
DES-3; 3DES	Data Encryption Standard, triple DES	ANSI X9.52-1998, "Triple Data Encryption Algorithm Modes of Operation" American National Standards Institute, 1998.
DF	Dedicated File	
DO	Data Object	
DS	Digital Signature	
DSI	Digital Signature Input	
DSS		NIST FIPS PUB 186, "Digital Signature Standard", 18 May 1994.
E106	European form related to the entitlement to sickness and maternity insurance benefits in kind for persons residing in a country other than the competent country	
E111	European form related to the entitlement to benefits in kind during a stay in a Member State	
E125	European form related to the	

abbreviation	text	comment and/or reference
	individual record of actual expenditure	
E127	European form related to the individual record of monthly lump-sum payments	
E128	European form related to the benefits in kind required during a stay in a Member State without imposing a condition of immediate need.	
EC	European Commission	
EF	Elementary File	
FCI	File Control Information	
FI	Clock rate conversion factor	
FID	File Identifier	
GK	Group Key	
HB	Historical Bytes	
HP	Health Professional	
HPC	Health Professional Card	
ICC	Integrated Circuit(s) Card	
ICCSN	ICC Serial Number	
ID	Identifier	
IFD	Interface Device	
IFSC	Information Field Size Card	
IFSD	Information Field Size Device	
IIN	Issuer Identification Number	
IK	Individual Key	
KE	Key Encipherment	
KEI	Key Encipherment Input	
MD2		RFC 1319 Kaliski, B., "The MD2 Message-Digest Algorithm", April 1992.
MD4		RFC 1321 Rivest, R., "The MD5 Message-Digest Algorithm," RFC 1321, April 1992.
MD5		"The MD5 Message Digest Algorithm", RFC 1321
MF	Master File	
MII	Major Industry Identifier	
MIME-SPEC		The primary definition of MIME. "MIME Part 1: Format of Internet Message Bodies", RFC 2045; "MIME Part 2: Media Types", RFC 2046; "MIME Part 3: Message Header Extensions for Non-ASCII Text", RFC 2047; "MIME Part 4: Registration Procedures", RFC 2048; "MIME Part 5: Conformance Criteria and Examples", RFC 2049
MSE	MANAGE SECURITY ENVIRONMENT	
NA	Naming Authority	
NDB	Nominative database	shared database which stores parts of the patient record as nominative

abbreviation	text	comment and/or reference
OPENPGP		RFC2440 "OPENPGP", November 1998
P	Patient	
PA	Personalisation Authority	
PC	Personal Computer	
PC/SC	Integrating PC's and Smart Cards	for more information s. annex 0 „A Standards, regulations, ongoing work, national projects (informative)“
PDC	Patient Data Card	
PI	Padding Indicator	
PIN	Personal Identification Number	
PK	Public Key	
PKCS1		“PKCS#1” : RFC2313, Mars 1998
PKCS15		“PKCS#15”, draft RSA Labs. february 11, 1999
PPS	Protocol Parameter Selection	
PSO	PERFORM SECURITY OPERATION	
RC	Retry Counter	
RC2		“A Description of the RC2 ® Encryption Algorithm”, RFC 2268
RCA	Root CA	
RD	Reference Data	
RFC		All RFC can be found at IETF Web server: <a href="http://www.ietf.org">http://www.ietf.org</a> .
RND	Random Number	
RSA	Algorithm of Rivest, Shamir, Adleman	
S	Server	
S/MIME V2		“S/MIME Version 2 Message Specification”, RFC 2311
S/MIMEV3		“S/MIME Version 3 Certificate Handling”, Internet Draft draft-ietf-smime-cert-*.txt.
SHA1		NIST FIPS PUB 180-1, “Secure Hash Standard,” National Institute of Standards and Technology, U.S. Department of Commerce, DRAFT, 31May 1994.
SK	Secret Key (equiv. to private key)	
SN	Serial Number	
SSD	Security Service Descriptor	
TLV	Tag Length Value	
TTP	Trusted Third Party	
UID	User Identification	
VD	Verification Data	

to be maintained

## **D The EU/G7 Interoperability dataset - Definition (normative) and NETLINK revision marks (informative)**

### **1 The EU/G7 Interoperability dataset - Definition (normative)**

To define the data that can be stored in the PDC, NETLINK WP 2 is using the interoperability dataset defined by EU/G7 - WG7. This dataset is normative and may not be changed in his structure and content. Extensions are allowed in the sense of the G7-specifications.

To fit into all scenarios described in this document different modifications of the dataset are necessary and are described in the following subchapter „0 2 Proposals for Modification (informative)“. The status „informative“ may change into „normative“ respectively parts will be shifted from subchapter „0 2

Proposals for Modification (informative)“ to the G7-Interoperability-dataset depending on the decisions of G7 which is in charge of revising the dataset.

The definition of the dataset is given in different representations (ASN.1-definition, tables, ...) in the original G7-specification (see annex 0 A Standards, regulations, ongoing work, national projects (informative)).

Note: Within the interoperability dataset the standard ISO 7826 is used for the registration of coding schemes. Since there is up to now no registration authority working it might be - depending on the future development of this standard and the existence of a working registration authority - necessary to modify the dataset in these points.

## 2 Proposals for Modification (informative)

### Reasons for modifications

#### Modifications concerning general revision

There are the following unsolved points:

1. the definition of "Date" is missing,  
the proposed solution is to replace "Date" with  
"IMPLICIT NUMERIC STRING SIZE(4..8)"
2. the definition of the objects with ISO-tags (7816-6) is syntactic incorrect,  
the proposed solution is to replace the existing text with  
[APPLICATION x] where "x" is the number to get the needed tag (for example x=1 to get the coded tag '4F' according to the ASN.1-BER)
3. to save about 7 KB space all tagged objects should be defined with an IMPLICIT (for example  
„bloodGroupAuthor [3] IMPLICIT Author" instead of „bloodGroupAuthor [3] Author").

An example should make point 3 more clear:

```

BloodGroupTransfusionDetails ::= SET
{
...
bloodGroupAuthor          [3] Author OPTIONAL
}

Author ::= SET
{
...
}

```

The coding would be (in an abridged version)

(Item)	Tag	Length	Content
(bloodGroupAuthor)	A3	zz	31 xx yy

where yy represents the coding of the content of author and xx the length of the coding of yy (according to the basic encoding rules (BER) of ASN.1). According to the BER zz is equal to xx + 1 Byte ('31). 'A3' identifies the item „bloodGroupAuthor" and '31' the information that a SET is following.

Using the proposed definition

```

BloodGroupTransfusionDetails ::= SET
{
...
bloodGroupAuthor          [3] IMPLICIT Author OPTIONAL
}

```

the coding would be

(Item)	Tag	Length	Content
(bloodGroupAuthor)	A3	xx	yy

The bytes for coding the (known) structure „SET" and the length of the SET (zz) won't be needed anymore. The needed informations yy (i.e. the coded content of Author) are still available.

### Modifications concerning the use of indexes

The changes that must be carried out on the structure in order to use the indexes concerning the Coded Clinical Details, Immunisation Details and Medication Details are as follows:

- Concerning the Coded Clinical Details
  - „Clinical Emergency Category“ is 00 when the information that follows concerns an index
  - „Clinical Indicator“ is 07 when the information that follows concerns an index
  - „Author identifier“ contains an IP address that belongs to the server in which the index is stored
  - „Author Name“ can contain additional information about the index origin
  - The item „Index Number“ is added and contains a binary number used as a reference to clinical data or to another index(es). If we take the present structure into consideration, ist tag is 87.
- Concerning the Immunisation Details
  - „Immunisation Emergency Category“ is 00 when the information that follows concerns an index
  - „Immunisation Indicator“ is 07 when the information that follows concerns an index
  - „Author identifier“ contains an IP address that belongs to the server in which the index is stored
  - „Author Name“ can contain additional information about the index origin
  - The item „Index Number“ is added and contains a binary number used as a reference to immunisation data or to another index(es). If we take the present structure into consideration, ist tag is 88.
- Concerning the Medication Details
  - „Medication Emergency Category“ is 00 when the information that follows concerns an index
  - „Medication Indicator“ is 07 when the information that follows concerns an index
  - „Author identifier“ contains an IP address that belongs to the server in which the index is stored
  - „Author Name“ can contain additional information about the index origin
  - The item „Index Number“ is added and contains a binary number used as a reference to medication data or to another index(es). If we take the present structure into consideration, ist tag is 8A.

#### Modifications concerning the use of Exxx-forms

Following changes are proposed:

- change the size of patientIdentifier, surname, alternativeSurnames, insuringBodyName, insuredPersonPolicyNumber, nationalInsuranceNumber to 35; REASON: in analogy with the current Exxx-forms exchange format
- change the size of authorIdentifier to 35; REASON: in analogy with with modifications above
- surname is optional; REASON: in some countries surname at birth only is used to identify a person.
- change the size of insuringBodyIdentifier to 21 and character instead of numbers; REASON: in analogy with with the current Exxx-forms exchange format and due to the needs of some countries
- adding physicianDetails to AdministrativeData; REASON: Each instance specifies a physician treating the card holder
- adding personalPreferences to AdministrativeData; REASON: indicating the status donor
- replacing E111Certificate by entitlementToBenefits; REASON: in analogy with E111 paper form
- deleting the ENUMERATED-status ‘not recorded(8)’ and ‘not supported(9)’ for entries in clinicalIndicator, bloodTransfusionIndicator, immunisationIndicator, medicationIndicator

#### Other Modifications

Following changes are proposed:

- adding „drugBatchNumber“ to medicationDetails

### **3 G7-Interoperability-dataset with harmonised NETLINK revision marks**

All revision marks are printed in bold:

1. Coding tables

table 36 Codes for Clinical Emergency Category

<b>Meaning</b>	<b>Clinical Emergency Category</b>	<b>Notes</b>
<b>Diseases</b>		
Asthma	01	
Heart Disease	02	Including congenital, ischaemic and other heart diseases.
Cardiovascular Disease	03	See also more specific item Heart Disease.
Epilepsy	04	Including any types of fit.
Neurological disorders	05	See also more specific items epilepsy.
Coagulation deficiency	06	Including haemophilia.
Diabetes	07	
Glaucoma	08	
Other significant diseases	00	Valid only if specified in Clinical Text
<b>Procedures</b>		
Dialysis Treatment	31	
Removal of an Organ	32	
Transplanted Organ	33	
Removable Prosthesis	34	
Pacemaker	35	
Other Procedures	30	Valid only if specified in Clinical Text
<b>Allergies</b>		
Analgesics	71	
Animal hair	72	
Antibiotics	73	
Citrus fruits	74	
Dust (or dust mite)	75	
Eggs	76	
Fish or Shellfish	77	
Iodine	78	
Milk	79	
Nuts	80	
Pollen	81	
Other Allergies	70	Valid only if specified in Clinical Text
<b>More or Index</b>	<b>99</b>	

table 37 Codes for Immunisation Emergency Category

Meaning	Immunisation Emergency Category	Notes
Anthrax	01	
BCG	02	
Cholera	03	
Diphtheria	04	
Diphtheria, Pertussis & Tetanus	05	
Diphtheria & Tetanus	06	
Haemophilus Influenza B	07	
Hepatitis A	08	
Hepatitis B	09	
Influenza	10	
Japanese encephalitis	11	
Measles	12	
Measles, Mumps and Rubella	13	
Measles & Rubella	14	
Meningococcal Infection (A&C)	15	
Mumps	16	
Pertussis	17	
Pneumococcus	18	
Polio (inactivated vaccine)	19	
Polio (oral vaccine)	20	
Rabies	21	
Rubella	22	
Tetanus	23	
Tick Borne Encephalitis	24	
Typhoid (oral)	25	
Typhoid (injection)	26	
Yellow Fever	27	
Others	00	Valid only if specified by Immunisation Text.
<b>More or Index</b>	<b>99</b>	

table 38 Codes for Medication Emergency Category

Meaning	Medication Emergency Category	Notes
Anti-arrhythmic	01	See also more specific item for digitalis.
Anti-coagulants	02	
Anti-convulsants	03	
Anti-diabetics	04	See also more specific item for insulin.
Anti-histamines	05	
Anti-hypertensives	06	See also more specific items such as Beta-blockers and Diuretics.
Beta blockers	07	
Corticosteroids	08	
Cytostatics & cytotoxics	09	
Digitalis	10	
Diuretics	11	
Insulin	12	
Monoamine oxidase inhibitors	13	
Psycholeptics	14	
Others	00	Valid only if Drug Name is specified.
<b>More or Index</b>	<b>99</b>	

table 39 Codes for organCategory

Meaning	organ Category	Notes
heart	01	
lungs	02	
liver	03	
kidneys	04	
pancreas	05	
tissus	06	
all	99	this allows to code a general yes or no to organ donation

table 40 Codes for implantCategory

Meaning	implant Category	Notes to be filled by medical specialists
---------	------------------	--

2. Dataset in table form

table 41 International Card data that can be stored in the PDC

Name	Tag Hex	Data Type	Max Len (bytes)	Occurrences Min, max	Notes
<b>Card Issuer Identifier</b>	<b>A0</b>	<b>Group</b>		<b>1,1</b>	
> Major Industry Identifier	80	Number	2 Fixed	1,1	“80” for healthcare
> Country Code	81	Number	3 Fixed	1,1	According to EN23166:1994
> Issuer Identifier	82	Number	8	1,1	Allocated by nationally appointed registration authority. In Europe a fixed length of 5 characters has been accepted (ENV12018 and EN1387). However, the proposed ANSI standard on which US numbering will be based has 8 characters plus a check digit. Therefore, European implementers should be aware of the need to handle this longer form.
> Check Digit	83	Number	1 Fixed	1,1	Luhn modulus ten double-add-double check digit of previous three items.
Card Holder Identifier	81	String	21	0,1	Unique identifier of the card holder by the Card Issuer. The use of this is optional and at the discretion of the Card Issuer. Where law and ethical constraints permit this may be used for a national health/insurance identifier.
Card Identifier	82	String	28	1,1	Unique identifier of the card by the Card Issuer. The number should be unique within the context of the Card Issuer Identifier. May be a built in card serial number or a concatenation of card holder identifier and an card issue number.
Card Status	83	Enumerated	1	1,1	0=Unknown, 1=Test (i.e. not valid for normal use), 2=Normal.
<b>Card Application Identification</b> (ISO7816-5 Application Template)	<b>61</b>	<b>Group</b>		<b>1,1</b>	Each instance specifies an application supported by the card.
> <i>Application Identifier</i> (ISO7816-5 Application Identifier)	31	Sub-group		1,9	
>> Card Application Identifier (ISO7816-5 Application Identifier)	4F	Octet-String	16	1,1	An Identifier that follows the structure specified by ISO7816-5.
>> <i>Discretionary Application Data</i> (ISO7816-5 Discretion Data)	73	Sub-group		1,1	<i>The additional data required to identify healthcard functionality and version numbers should use the ISO7816-5 object “Discretionary data”</i>
>>> Card Application Type	80	Enumerated	1 Fixed	1,1	Specifies the interoperable healthcare application type(s) for this identifier. 0= Administrative and Emergency Clinical, 1= Administrative, 2= Emergency Clinical, 3-8= Reserved for future use, 9= Local use.

Name	Tag Hex	Data Type	Max Len (bytes)	Occurrences Min, max	Notes
>>> Card Application Version	81	Number	2 Fixed	1,1	A version number allocated by the national organisation that specified the healthcard structure for a particular revision of the Card Application.

table 42 International Administrative data that can be stored in the PDC

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
<b>Patient Identification</b>	<b>A0</b>	<b>Group</b>		<b>1,1</b>	<b>Alternative identifier(s) for the same patient issued by different issuers or naming authorities.</b>
>Patient Identification	31	Sub-group		1,3	
>> Issuer of Patient Identifier	A0	Sub-group		1,1	
>>> Major Industry Identifier	80	Number	2 fixed	1,1	“80” for healthcare
>>> Country Code	81	Number	3 fixed	1,1	According to EN23166:1994
>>> Issuer Identifier	82	Number	8	1,1	Allocated by nationally appointed registration authority. In Europe a fixed length of 5 characters has been accepted (ENV12018 and EN1387). However, the proposed ANSI standard on which US numbering will be based has 8 characters plus a check digit.
>>> Check Digit	83	Number	1 fixed	1,1	Luhn modulus ten double-add-double check digit of previous three items.
>> Patient Identifier	81	String	35	1,1	The identifier by which the issuer refers to the patient who holds this card.
<b>Name Details</b>	<b>A1</b>	<b>Group</b>		<b>1,1</b>	
> Title	80	String	7	0,1	E.g. “Mr”, “Prof.”, “Madame”
> Surname prefix	81	String	15	0,1	A prefix to the surname that is typically omitted when calculating alphabetical order (e.g. “von”, “van der”, “de la”)
> Surname	82	String	35	0*,1	* Must be present if Surname at birth is absent.
> Alternative Surnames	A3	Sub-group		0,1	
>> Alternative Surname	04	String	35	1,3	To be used for supplementary surnames in case of Portuguese and Spanish citizens. May also be used for second part of double surnames
> Surname suffix	84	String	15	0,1	A suffix to the surname used as a form of address (e.g. “Senior”, “the III” ).
> Forenames	A5	Sub-group		1,1	
>> Forename	04	String	16	1,3	May hold initials if forenames not specified.
> Preferred forename	86	String	16	0,1	The preferred forename. If not specified the first instance of forenames specifies the preferred forename.
> Surname at birth	87	String	35	0*,1	* Must be present if Surname is absent. Maiden name. In case of adopted persons this may be strictly the name of adoption rather than at birth subject to national conventions
<b>Language Details</b>	<b>A2</b>	<b>Group</b>		<b>0,1</b>	Where more than one language is specified the languages should usually be presented in order of patient preference.
>Language detail	31	Sub-group		1,4	

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
>> Language	80	String	2	1,1	Coded in accordance with ISO 639:1988.
>> Ability in language	81	Enumerated	1	0,1	If more than one language is spoken then this proficiency value is used to distinguish between languages in order of preference. 0=Preferred, 1=fluent, 2=fair, 3= poor.
<b>Birth Details</b>	<b>A3</b>	<b>Group</b>		<b>1,1</b>	
> Date of Birth	80	Date	8	1,1	In full YYYYMMDD
> Sex	81	Enumerated	1	1,1	0=Unknown, 1=Male, 2=Female 3 or 9=Other (usually "other" is represented as 9 as specified by ISO 5218:1977. However, the value 3 should also be treated as other to allow 2 bit storage in the card to be used without further mapping).
> Country of Birth	82	Number	3 fixed	0,1	According to EN23166:1994.
<b>Address Details</b>	<b>A4</b>	<b>Group</b>		<b>0,1</b>	<b>Each instance specifies an address relevant to the card holder.</b>
> Address detail	31	Sub-group		1,2	
>> Address Status	80	Enumerated	1	1,1	An identifier of the status and purpose of the address: 0=Current home address of patient, 1=Previous home address of patient.
>>> Address Structure	A1	Sub-group		0,1	
>>>> Address Text	A0	Sub-sub-group		1,1	
>>>>> Address Text	04	String	35	1,5	Text of the postal address. Each instance contains one line of text. Address Text should include the postcode even if this is also specified separately.
>>>> Address Postcode	81	String	8	0,1	The postal code associated with the address.
>>>> Address Country	82	Number	3 fixed	0,1	The country of the address. According to EN23166:1994.
>>>>> Telecom Structure	A2	Sub-group		0,1	
>>>>>> Telephone number	A0	Sub-sub-group		0,1	
>>>>>>> Telephone number	12	Number	16	1,3	Complete number including country and area code with no separators. If more than one number is given they should be in the order in which they should be tried when attempting to contact the patient.
>>>>>>> Facsimile number	81	Number	16	0,1	Complete number including country and area code with no separators.
>>>>>>> Network Address	82	String	64	0,1	Internet addresses
<b>Contact Details</b>	<b>A5</b>	<b>Group</b>		<b>0,1</b>	<b>Each instance specifies an address relevant to the card holder.</b>
>Contact Detail	31	Sub-group		1,3	
>> Contact Name	80	String	30	1,1	The unstructured name of the next of kin or contact person
>> Contact Relationship	81	String	16	0,1	The relationship of the next of kin or contact person to the card holder.
>>> Contact address structure	A2	Sub-group		0,1	

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
>>> Address Text	A0	Sub-sub-group		1,1	
>>>> Address Text	04	String	35	1,5	Text of the postal address. Each instance contains one line of text. Address Text should include the postcode even if this is also specified separately.
>>> Address Postcode	81	String	8	0,1	The postal code associated with the address.
>>> Address Country	82	Number	3 fixed	0,1	The country of the address. According to EN23166:1994.
>> Contact telecom structure	A3	Sub-group		0,1	
>>> Telephone number	A0	Sub-sub-group		0,1	
>>>> Telephone number	12	Number	16	1,3	Complete number including country and area code with no separators. If more than one number is given they should be in the order in which they should be tried when attempting to contact the patient.
>>> Facsimile number	81	Number	16	0,1	Complete number including country and area code with no separators.
>>> Network Address	82	String	64	0,1	Internet addresses
<b>Insuring Body Details</b>	<b>A6</b>	<b>Group</b>		<b>1,1</b>	
>Insuring Body Detail	31	Sub-group		1,3	
>> Insuring Body Country	80	Number	3 fixed	0,1	The country of the insuring body. According to EN23166:1994.
>> Insuring Body Identifier	81	String	21	1,1	Number identifying the insuring body at national level
>> Insuring Body Name	82	String	35	0,1	
>> Insuring Body Address Structure	A3	Sub-group		0,1	
>>>> Address Text	A0	Sub-sub-group		1,1	
>>>>> Address Text	04	String	35	1,5	Text of the postal address. Each instance contains one line of text. Address Text should include the postcode even if this is also specified separately.
>>>> Address Postcode	81	String	8	0,1	The postal code associated with the address.
>>>> Address Country	82	Number	3 fixed	0,1	The country of the address. According to EN23166:1994.
>> Insuring Body Telecom Structure	A4	Sub-group		0,1	
>>>> Telephone number	A0	Sub-sub-group		0,1	
>>>>> Telephone number	12	Number	16	1,3	Complete number including country and area code with no separators. If more than one number is given they should be in the order in which they should be tried when attempting to contact the patient.
>>>> Facsimile number	81	Number	16	0,1	Complete number including country and area code with no separators.
>>>> Network Address	82	String	64	0,1	Internet addresses
>>Entitlement to benefits abroad	A5	Sub-group		0,1	

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
>>>Starting date	80	Date	8	1,1	Starting date in full YYYYMMDD.
>>>Expiration date	81	Date	8	0,1	Expiration date in full YYYYMMDD.
>>>Professional category	82	Enumerated	1	1,1	1=employed, 2=self-employed, 3=student, 4=pensioner (scheme for employed person), 5=pensioner (scheme for self-employed person), 6=other
>>>Scheme	83	Enumerated	1	1,1	1=Yes, 2=No. The person named above is covered by a scheme for self-employed persons as referred to in Annex 11 to Regulation 574/72
>> <i>Author</i>	<i>A4</i>	<i>Sub-group</i>		<i>0,1</i>	<i>The person responsible for recording this clinical item or the origin of index</i>
>>> Author Country	80	Number	3 fixed	0,1	The country of the author. According to EN23166:1994.
>>> Author Identifier	81	Number	35	0,1	Identifier of the person responsible for the entry (or change) or IP address of the server in which the index is stored. The identification must be either globally or nationally unique.
>>> Author Name	82	String	20	0,1	Optional plain text name of the responsible person or additional information about the index origin..

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
>>Insurance Numbers	A6	Sub-Group		1,1	Reference number issued or recognised by the insuring body for the purpose of identifying the policy and/or the insured person.
>>>Insured Person Policy Number	80	String	35	0*,1	* Must be present if National Insurance Number is absent.
>>>National Insurance Number	81	String	35	0*,1	* Must be present if Policy Number is absent.
>>Insured Person	A7	Sub-Group		0,1	If the card holder is covered by the insurance policy held by another person (e.g. a relative), this sub-group identifies the insured person or main contract holder with the specified insuring body.
>>>Relationship to Patient	80	String	16	0,1	The relationship of the insured person to the card holder.
>>>Insured Person Surname	81	String	35	1,1	It is the Current Surname or the Surname at birth depending on the national legislation
>>>Insured Person Alternative Surnames	A2	String		0,1	Alternative surnames if required.
>>>>Insured Person Alternative Surname	04	String	35	1,3	
>>>Insured Person Forenames	A3	String		1,1	May hold initials if forenames not specified.
>>>>Insured Person Forename	04	String	16	1,3	
>>> Insured Person Address Structure	A4	Sub-sub-group		0,1	
>>>> Insured Person Address Text	A0	Sub-sub-sub-group		1,1	Text of the postal address. Each instance contains one line of text. Address Text should include the postcode even if this is also specified separately.
>>>>> Insured Person Address Text	04	String	35	1,5	
>>>> Insured Person Address Postcode	81	String	8	0,1	The postal code associated with the address.
>>>> Insured Person Address Country	82	Number	3 fixed	0,1	The country of the address. According to EN23166:1994.
>>> Insured Person Telecom Structure	A5	Sub-sub-group		0,1	
>>>> Insured Person Telephone number	A0	Sub-sub-sub-group		0,1	Complete number including country and area code with no separators. If more than one number is given they should be in the order in which they should be tried when attempting to contact the patient.
>>>>> Insured Person Telephone number	12	Number	16	1,3	

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
>>>> Insured Person Facsimile number	81	Number	16	0,1	Complete number including country and area code with no separators.
>>>> Insured Person Network Address	82	String	64	0,1	
<b>Physician details</b>	<b>A7</b>	<b>Group</b>		<b>0,1</b>	<b>Each instance specifies a physician treating the card holder.</b>
>Physician detail	31	Sub-group		1,3	
>> Physician Name	80	String	30	1,1	The unstructured name of the physician
>> Physician kind	81	Enumerated	1	1,1	0=family doctor; 1=paediatrician; 2=other
>> <i>Physician address structure</i>	<i>A2</i>	<i>Sub-group</i>		<i>0,1</i>	
>>> <i>Address Text</i>	<i>A0</i>	<i>Sub-sub-group</i>		<i>1,1</i>	
>>>> <i>Address Text</i>	<i>04</i>	<i>String</i>	<i>35</i>	<i>1,5</i>	<i>Text of the postal address. Each instance contains one line of text. Address Text should include the postcode even if this is also specified separately.</i>
>>> Address Postcode	81	String	8	0,1	The postal code associated with the address.
>>> Address Country	82	Number	3 fixed	0,1	The country of the address. According to EN23166:1994.
>> <i>Physician telecom structure</i>	<i>A3</i>	<i>Sub-group</i>		<i>0,1</i>	
>>> <i>Telephone number</i>	<i>A0</i>	<i>Sub-sub-group</i>		<i>0,1</i>	
>>>> <i>Telephone number</i>	<i>12</i>	<i>Number</i>	<i>16</i>	<i>1,3</i>	<i>Complete number including country and area code with no separators. If more than one number is given they should be in the order in which they should be tried when attempting to contact the patient.</i>
>>> Facsimile number	81	Number	16	0,1	Complete number including country and area code with no separators.
>>> Network Address	82	String	64	0,1	Internet addresses

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
>> Physician Identifier	84	String	35	0,1	An identifier of the physician
>> <i>Physician Certification Authority</i>	<i>A5</i>	<i>Sub-group</i>		<i>0,1</i>	
>>> caX500DirectoryAddress	80	TeletexString	70	1,1	X.500 address of the CA for the physician
>>> physicianDistinguishName	81	TeletexString	237	1,1	distinguish name of the physician used by the CA
<b>Organ donation</b>	<b>A8</b>	<b>Group</b>		<b>0,1</b>	
> Organ category	80	String	2	1,1	Refer to <u>Table x</u>
> Donation	81	Enumerated	1	1,1	1=yes; 2=no; 3=decision is up to a third person

table 43 International emergency data that can be stored in the PDC

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
<b>Coded Clinical Details</b>	<b>A0</b>	<b>Group</b>		<b>0,1</b>	
>Coded clinical detail	31	Sub-group		1,99	
>> Clinical Emergency Category	80	Number	2	1,1	A number identifying key items of emergency clinical data. The category numbers are specified in this document (see <b>table 36</b> ). <b>99 for an index</b> .
>> Clinical Indicator	81	Enumerated	1	1,1	0= Disease or condition indicated by Code recorded as <b>Absent</b> . 1= Disease or condition indicated by Code recorded as <b>Present</b> . 2= Disease or condition indicated by Code recorded as <b>Possible</b> (may be used to indicate uncertainty of the person recording). <b>7=Code replaced by an index</b>
>> Clinical coding structure	A2	Sub-group		0,1	A structure containing more detailed coded information (not used for index)
>>> Coding Scheme Identifier	80	String	6	1,1	Designates the coding scheme from which Clinical Code is derived. Uses identifiers registered in ISO 7826.
>>> Clinical Code	81	String	8	1,1	Code used for representation of clinical data.
>>> Coding Scheme Acronym	82	String	10	0,1	since ISO7826 is not working this field can be used for the common name of the codingscheme
>> Clinical Date	83	Date	8	0,1	Optional date of diagnosis or first occurrence. As full date YYYYMMDD. (not used for index)
>> Clinical Text	84	String	80	0,1	Optional free text associated with the coded (or indexed) information.
>> Clinical Entry Date	85	Date	8	0,1	Date on which this entry was made (or changed). As full date YYYYMMDD.
>> Clinical Author	A6	Sub-group		0,1	The person responsible for recording this clinical item or the origin of index
>>> Author Country	80	Number	3 fixed	0,1	The country of the author. According to EN23166:1994.
>>> Author Identifier	81	Number	35	0,1	Identifier of the person responsible for the entry (or change) or IP address of the server in which the index is stored. The identification must be either globally or nationally unique.

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
>>> Author Name	82	String	20	0,1	Optional plain text name of the responsible person or additional information about the index origin..
>> Index number	87	String	40	0,1	Binary number used as a reference to clinical data or to another index(es).
<b>Blood Group and Transfusion Details</b>	<b>A1</b>	<b>Group</b>		<b>0,1</b>	
> <i>Blood Group</i>	<i>A0</i>	<i>Sub-group</i>		<i>1,1</i>	
>> ABO Blood Group	80	String	2	1,1	“O”, “A”, “B”, “AB” or “U” = Unknown.
>> Rhesus Factor	81	String	1	1,1	“+” or “-” or “U” = Unknown.
>> Date of Last Blood Grouping	82	Date	8	0,1	Full date YYYYMMDD.
>> Blood Grouping Text	83	String	30	0,1	Optional free text description of any additional grouping factors.
> <i>Blood Transfusion</i>	<i>A1</i>	<i>Sub-group</i>		<i>1,1</i>	
>> Blood Transfusion Indicator	80	Enumerated	1	1,1	0= Blood transfusion recorded as Never. 1= Blood transfusion recorded as Once or more than once. 2= Blood transfusion recorded as Unknown.
>> Last Blood Transfusion Date	81	Date	8	0,1	Full date YYYYMMDD, year & month YYYYMM or year only YYYY.
> Blood Group Entry Date	82	Date	8	0,1	Date on which this entry was made (or changed). As full date YYYYMMDD.
> <i>Blood Group Author</i>	<i>A3</i>	<i>Sub-group</i>		<i>0,1</i>	<i>The person responsible for recording the blood transfusion details.</i>
>> Author Country	80	Number	3 fixed	0,1	The country of the author. According to EN23166:1994.
>> Author Identifier	81	Number	35	0,1	Identifier of the person responsible for the entry or change. The identification must be either globally or nationally unique.
>> Author Name	82	String	20	0,1	Optional plain text name of the responsible person.
<b>Immunisation Details</b>	<b>A2</b>	<b>Group</b>		<b>0,1</b>	
> <i>Immunisation detail</i>	<i>31</i>	<i>Sub-group</i>		<i>1,10</i>	

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
>> Immunisation Emergency Category	80	Number	2	1,1	Immunisation identifier. See <b>table 37.99</b> for an index.
>> Immunisation Indicator	81	Enumerated	1	1,1	0= Immunisation recorded as Never done. 1= Immunisation recorded as done at least Once. 2= Immunisation recorded as Unknown. 4= Immunisation recorded as Adverse reaction. 7=Code replaced by an index
>> Immunisation Status	82	Enumerated	1	0,1	Valid only if indicator is 1. 0= Unspecified dose. 1= First dose of course. 2= Second dose of course. 3= Third dose of course. 4= Completed course 5= Booster dose
>> Last Date Immunised	83	Date	8	0,1	The last recorded date of this immunisation. Not used for index. Full date YYYYMMDD, year & month YYYYMM or year only YYYY.
>> <i>Immunisation coding structure</i>	<i>A4</i>	<i>Sub-group</i>		<i>0,1</i>	<i>A structure containing more detailed coded information about an immunisation. (not used for index)</i>
>>> Coding Scheme Identifier	80	String	6	1,1	Designates the coding scheme from which immunisation code is derived. Uses identifiers registered in ISO 7826.
>>> Clinical Code	81	String	8	1,1	Code used to specify the immunisation in more detail.
>>> Coding Scheme Acronym	82	String	10	0,1	since ISO7826 is not working this field can be used for the common name of the codingscheme
>> Immunisation Text	85	String	30	0,1	Optional free text description of any other immunisation or index.

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
>> Immunisation Entry Date	86	Date	8	0,1	Date on which this entry was made (or changed). As full date YYYYMMDD.
>> <i>Immunisation Author</i>	A7	Sub-group		0,1	<i>The person responsible for recording this immunisation or origin of the index.</i>
>>> Author Country	80	Number	3 fixed	0,1	The country of the author. According to EN23166:1994.
>>> Author Identifier	81	Number	35	0,1	Identifier of the person responsible for the entry (or change) or IP address of the server in which the index is stored. The identification must be either globally or nationally unique.
>>> Author Name	82	String	20	0,1	Optional plain text name of the responsible person or additional information about the index origin.
>> Index number	88	String	40	0,1	Binary number used as a reference to immunisation data or to another index(es).
>> Vaccine batch number	89	String	30	0,1	
>> Next date immunised	8A	String	8	0,1	Date of the next immunisation
<b>Medication Details</b>	<b>A3</b>	<b>Group</b>		<b>0,1</b>	
> <i>Medication detail</i>	31	Sub-group		1,30	
>> Medication Emergency Category	80	Number	2	1,1	An identifier of drug categories that enables the emergency information to be conveyed without need for more detailed drug information. See <b>table 38_99</b> for index.
>> Medication Indicator	81	Enumerated	1	1,1	0= Medication with drug in this group recorded as Absent. 1= Medication with at least One drug in this group recorded. 2= Medication with drugs in this group recorded as Unknown. 4= present medication 5= Past or short-term medication with at least one drug in this group recorded but not part of regular current medication. 6= Intermittent medication with at least one drug in this group is recorded (e.g. anti-histamines for hayfever only taken at some times in the year). 7=Code replaced by an index.
>> <i>Medication coding structures</i>	A2	Sub-group		0,1	
>>> <i>Medication coding structure</i>	31	Sub-group		1,6	<i>A structure containing more detailed coded information (not used for index)</i>

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
>>>> Coding Scheme Identifier	80	String	6	1,1	Designates the coding scheme from which Medication Code is derived. Uses identifiers registered in ISO 7826.
>>>> Medication Code	81	String	8	1,1	Code(s) for medication item. In the case of ATC codes several codes may apply to the same item representing different ingredients in this case the coding structure repeats
>>>> Coding Scheme Acronym	82	String	10	0,1	since ISO7826 is not working this field can be used for the common name of the codingscheme
>> Medication Drug Name	83	String	50	0,1	Optional textual representation of a particular drug name. Ideally this should conform to the International Non-proprietary Name (INN). Only valid if the Medication Indicator is 1, 5, 6 or 7. If 7: free text associated with the index.
>> Medication Dosage Codes	A4	Sub-group		0,1	Optional coded representation of dosage. Codes represented as a sequence that constructs a dosage instructions. Not used for index.
>>> Medication Dosage Code	04	String	2	1,4	
>> Medication Dosage	85	String	50	0,1	Optional textual summary of dosage instructions. Not used for index.
>> Medication Started Date	86	Date	8	0,1	Date on which this medication was started. Valid if the Medication Indicator is 1, 5 or 6. Full date YYYYMMDD, year & month YYYYMM or year only YYYY.
>> Medication Ended Date	87	Date	8	0,1	Date on which this medication was stopped. Only valid if the Medication Indicator is 5 (i.e. Past of Short-term). Full date YYYYMMDD, year & month YYYYMM or year only YYYY.
>> Medication Entry Date	88	Date	8	0,1	Date on which this entry was made (or changed). As full date YYYYMMDD.
>> Medication Author	A9	Sub-group		0,1	The person responsible for recording this medication item or origin of index.
>>> Author Country	80	Number	3 fixed	0,1	The country of the author. According to EN23166:1994.
>>> Author Identifier	81	Number	35	0,1	Identifier of the person responsible for the entry (or change) or IP address of the server in which the index is stored. The identification must be either globally or nationally unique.
>>> Author Name	82	String	20	0,1	Optional plain text name of the responsible person or additional information about the index origin.
>> Index number	8A	String	40	0,1	Binary number used as a reference to medication data or another index(es).
>> Amount authorised renewals	8B	String	2	0,1	

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
>> Prescription date	8C	String	8	0,1	Last date on which this medication has been prescribed
>> drugBatchNumber	8D	String	30	0,1	
<b>Clinical Address Details</b>	<b>A4</b>	<b>Group</b>		<b>0,1</b>	<b>Each instance specifies an address at which clinical information relevant to the card holder may be available.</b>
> <i>Clinical address detail</i>	<i>31</i>	<i>Sub-group</i>		<i>1,9</i>	
>> Clinical Address Name	80	String	30	1,1	The unstructured name of the person or clinic
>> Clinical Address Relationship	81	String	16	0,1	The clinical relationship to the patient
>> <i>Clinical Address Structure</i>	<i>A2</i>	<i>Sub-group</i>		<i>0,1</i>	
>>> Clinical Address Text	80	String	35	1,5	Text of the postal address. Each instance contains one line of text. Address Text should include the postcode even if this is also specified separately.
>>> Clinical Address Postcode	81	String	8	0,1	The postal code associated with the address.
>>> Clinical Address Country	82	Number	3 fixed	0,1	The country of the address. According to EN23166:1994.
>> <i>Clinical Telecom Structure</i>	<i>A3</i>	<i>Sub-group</i>		<i>0,1</i>	
>>> Clinical Telephone number	80	Number	16	0,3	Complete number including country and area code with no separators. If more than one number is given they should be in the order in which they should be tried when attempting to contact the patient.
>>> Clinical Facsimile number	81	Number	16	0,1	Complete number including country and area code with no separators.
>>> Clinical Network Address	82	String	64	0,1	
<b>Optical Prescription Details</b>	<b>A5</b>	<b>Group</b>		<b>0,1</b>	
> Optical prescription	80	String	40	1,1	Summary of optical prescription to speed issuing of new glasses or contact lenses.
> Optical Prescription Date	81	Date	8	0,1	Optional date on which this optical prescription was last updated. Full date YYYYMMDD, year & month YYYYMM or year only YYYY.

Name	Tag	Data Type	Max Len (bytes)	Occurrences Min, max	Note
<b>Update Details</b>	<b>A6</b>	<b>Group</b>		<b>1,1</b>	<b>Information about the last update of the Clinical Data.</b>
> Date of Last Clinical Update	80	Date	8	1,1	Date on which the Clinical Data on the card was last updated. Only Full date YYYYMMDD is applicable.
> <i>Responsible Party</i>	<i>A1</i>	<i>Sub-group</i>		<i>1,1</i>	<i>The person or organisation responsible for the last update of the card.</i>
>> Responsible Party Country	80	Number	3 fixed	1,1	The country of the responsible party. According to EN23166:1994.
>> Responsible Party Identifier	81	Number	35	1,1	Identifier of the person or organisation responsible for the update. The identification must be either globally or nationally unique.
>> Responsible Party Name	82	String	20	0,1	Optional plain text name of the responsible person.
<b>Implants</b>	<b>A7</b>	<b>Group</b>		<b>0,1</b>	
> Implant category	80	String	2	0,1	Refer to <b>table 40</b>
<b>Pregnancy details</b>	<b>A8</b>	<b>Group</b>		<b>0,1</b>	
> Pregnancy date	80	Date	8	0,1	Date of last menstruation before pregnancy diagnosis
> <i>Pregnancy author</i>	<i>A1</i>	<i>Sub-group</i>		<i>0,1</i>	<i>Identification of the practitioner who registered the pregnancy</i>
>> Author Country	80	Number	3 fixed	0,1	The country of the author. According to EN23166:1994.
>> Author Identifier	81	Number	35	0,1	Identifier of the person responsible for the entry (or change)
>> Author Name	82	String	20	0,1	Optional plain text name of the responsible person

### 3. Dataset in ASN.1 form

The dataset consists of three groups which are combined as follows. All revision marks are printed in bold:

```
HealthcardServerApiData ::= SET
{
  cardApplicationData      [0] IMPLICIT CardApplicationData,
  administrativeData      [1] IMPLICIT AdministrativeData,
  clinicalData            [2] IMPLICIT ClinicalData
}
```

### 4. Card Data in ASN.1 form

```
CardApplicationData ::= SET
{
  cardIssuerIdentifier     [0] IMPLICIT CardIssuerIdentifier,
  cardHolderIdentifier     [1] IMPLICIT OCTET STRING (SIZE (0..21)) OPTIONAL,
  cardIdentifier           [2] IMPLICIT OCTET STRING (SIZE (0..28)),
  cardStatus              [3] IMPLICIT ENUMERATED
                          {Unknown(0), Test(1), Normal(2)},
  cardApplicationIdentification
}

CardIssuerIdentifier ::= SET
{
  majorIndustryIdentifier [0] IMPLICIT NUMERIC STRING DEFAULT 80 (SIZE(2)),
  countryCode            [1] IMPLICIT NUMERIC STRING (SIZE(3)),
  issuerIdentifier       [2] IMPLICIT NUMERIC STRING (SIZE(5..8)),
  checkDigit            [3] IMPLICIT NUMERIC STRING (SIZE(1))
}

ApplicationTemplate ::= SET
{
  cardApplicationIdentifier [APPLICATION 15] IMPLICIT OCTET STRING (SIZE (0..16)) ; as defined
                          in ISO7816-5
  discretionaryApplicationData [APPLICATION 19] IMPLICIT DiscretionaryData

  DiscretionaryData ::= SET
  cardApplicationType      [0] IMPLICIT ENUMERATED
                          {Administrative and Emergency Clinical(0), Administrative(1), Emergency
                          Clinical(2), Local use(9)},
  cardApplicationVersion   [1] IMPLICIT NUMERIC STRING (SIZE(2))
}
```

### 5. Administrative Data in ASN.1 form

```
AdministrativeData ::= SET
{
  patientIdentification   [0] IMPLICIT SET (SIZE (1..3)) OF PatientIdentification,
  nameDetails             [1] IMPLICIT NameDetails,
  languageDetails        [2] IMPLICIT SEQUENCE (SIZE (0..4)) OF LanguageDetails OPTIONAL,
  birthDetails           [3] IMPLICIT BirthDetails,
  addressDetails         [4] IMPLICIT SET (SIZE (0..2)) OF AddressDetails OPTIONAL,
  contactDetails         [5] IMPLICIT SET (SIZE (0..3)) ContactDetails OPTIONAL,
  insuringBodies         [6] IMPLICIT SET (SIZE (0..3)) OF InsuringBodyDetails OPTIONAL,
  physicianDetails      [7] IMPLICIT SET (SIZE (0..3)) PhysicianDetails OPTIONAL,
  organDonation        [8] IMPLICIT OrganDonation OPTIONAL
}
```

PatientIdentification::= SET	
{	
issuerOfPatientIdentifier	[0] <b>IMPLICIT</b> IssuerOfPatientIdentifier,
patientIdentifier	[1] <b>IMPLICIT</b> OCTET STRING (SIZE (0..35))
}	
NameDetails::= SET	
{	
title	[0] <b>IMPLICIT</b> OCTET STRING (SIZE (0..7)) OPTIONAL,
surnamePrefix	[1] <b>IMPLICIT</b> OCTET STRING (SIZE (0..15)) OPTIONAL,
surname	[2] <b>IMPLICIT</b> OCTET STRING (SIZE (0..35)) <b>OPTIONAL</b> ,
alternativeSurnames	[3] <b>IMPLICIT SEQUENCE (SIZE (1..3)) OF</b> OCTET STRING (SIZE (0..35)) OPTIONAL,
surnameSuffix	[4] <b>IMPLICIT</b> OCTET STRING (SIZE (0..15)) OPTIONAL,
forenames	[5] <b>IMPLICIT SEQUENCE (SIZE (1..3)) OF</b> OCTET STRING (SIZE (1..16)),
preferredForename	[6] <b>IMPLICIT</b> OCTET STRING (SIZE (1..16)) OPTIONAL
surnameAtBirth	[7] <b>IMPLICIT</b> OCTET STRING (SIZE (0..35)) OPTIONAL,
}	
LanguageDetails::= SET	
{	
language	[0] <b>IMPLICIT</b> OCTET STRING (SIZE (2))
abilityInLanguage	[1] <b>IMPLICIT</b> ENUMERATED {preferred(0), fluent(1), fair(2), poor(3)} OPTIONAL,
}	
BirthDetails::= SET	
{	
dateOfBirth	[0] <b>IMPLICIT</b> NUMERIC STRING (SIZE(4..8)),
sex	[1] <b>IMPLICIT</b> ENUMERATED {unknown(0), male(1), female(2), other(3), other(9)}
countryOfBirth	[2] <b>IMPLICIT</b> NUMERIC STRING (SIZE (3)) OPTIONAL
}	
AddressDetails::= SET	
{	
addressStatus	[0] <b>IMPLICIT</b> ENUMERATED {current home address(0), previous home address(1)}
addressStructure	[1] <b>IMPLICIT</b> AddressStructure OPTIONAL,
telecomStructure	[2] <b>IMPLICIT</b> TelecomStructure OPTIONAL
}	
ContactDetails::= SET	
{	
contactName	[0] <b>IMPLICIT</b> OCTET STRING (SIZE (0..30)),
contactRelationship	[1] <b>IMPLICIT</b> OCTET STRING (SIZE (0..30)) OPTIONAL,
contactAddressStructure	[2] <b>IMPLICIT</b> AddressStructure OPTIONAL,
contactTelecomStructure	[3] <b>IMPLICIT</b> TelecomStructure OPTIONAL
}	
PhysicianDetails::= SET	
{	
physicianName	[0] <b>IMPLICIT</b> OCTET STRING (SIZE (0..30)),
physicianKind	[1] <b>IMPLICIT</b> ENUMERATED {Family doctor(0), Paediatrician(1), Other(2)},
contactAddressStructure	[2] <b>IMPLICIT</b> AddressStructure OPTIONAL,
contactTelecomStructure	[3] <b>IMPLICIT</b> TelecomStructure OPTIONAL,
physicianIdentifier	[4] <b>IMPLICIT</b> OCTET STRING (SIZE (0..35)) OPTIONAL,
physicianCertificationAuthority	[5] <b>IMPLICIT</b> PhysicianCertificationAuthority OPTIONAL
}	

**PhysicianCertificationAuthority ::= SET**

```
{
caX500DirectoryAddress      [0] IMPLICIT TeletexString (SIZE (0...70)),
physicianDistinguishName    [1] IMPLICIT TeletexString (SIZE (0...237))
}
```

**OrganDonation ::= SET**

```
{
organCategory                [0] IMPLICIT NUMERIC STRING (SIZE(2)),
donation                      [1] IMPLICIT ENUMERATED    {1=yes, 2=no, 3=decision is up to a third
                                                                    person}
}
```

**InsuringBodyDetails ::= SET**

```
{
insuringBodyCountry          [0] IMPLICIT NUMERIC STRING (SIZE(3)) OPTIONAL,
insuringBodyIdentifier       [1] IMPLICIT NUMERIC OCTET STRING (SIZE(0..21)),
insuringBodyName             [2] IMPLICIT OCTET STRING (SIZE (0...35)) OPTIONAL,
insuringBodyAddressStructure [3] IMPLICIT AddressStructure OPTIONAL,
insuringBodyTelecomStructure [4] IMPLICIT TelecomStructure OPTIONAL,
e111Certificate           [5] IMPLICIT E111Certificate OPTIONAL,
entitlementToBenefitsAbroad  [5] IMPLICIT EntitlementToBenefits OPTIONAL,
insuranceNumbers             [6] IMPLICIT InsuranceNumbers,
insuredPerson                [7] IMPLICIT InsuredPerson OPTIONAL
}
```

**InsuranceNumbers ::= SET**

```
{
insuredPersonPolicyNumber    [0] IMPLICIT OCTET STRING (SIZE (0...35)) OPTIONAL,
nationalInsuranceNumber      [1] IMPLICIT OCTET STRING (SIZE (0...35)) OPTIONAL,
}
```

**InsuredPerson ::= SET**

```
{
relationshipToPatient        [0] IMPLICIT OCTET STRING (SIZE 0...16) OPTIONAL,
insuredPersonSurname         [1] IMPLICIT OCTET STRING (SIZE (0...27)),
insuredPersonAlternativeSurname [2] IMPLICIT OCTET STRING (SIZE (0...27)) OPTIONAL,
insuredPersonForenames       [3] IMPLICIT OCTET STRING (SIZE (0...16)),
insuredPersonAddressStructure [4] IMPLICIT AddressStructure OPTIONAL,
insuredPersonTelecomStructure [5] IMPLICIT TelecomStructure OPTIONAL
}
```

**IssuerOfPatientIdentifier ::= SET**

```
{
majorIndustryIdentifier      [0] IMPLICIT NUMERIC STRING (SIZE(2)),
countryCode                  [1] IMPLICIT NUMERIC STRING (SIZE(3)),
issuerIdentifier              [2] IMPLICIT NUMERIC STRING (SIZE(5...8)),
checkDigit                   [3] IMPLICIT NUMERIC STRING (SIZE(1))
}
```

**AddressStructure ::= SET**

```
{
addressText                   [0] IMPLICIT SEQUENCE (SIZE (1...5)) OF OCTET STRING (SIZE (0...35))
addressPostcode               [1] IMPLICIT OCTET STRING (SIZE (0...8)) OPTIONAL,
addressCountry                [2] IMPLICIT NUMERIC STRING (SIZE (3)) OPTIONAL
}
```

**TelecomStructure ::= SET**

```
{
telephoneNumber               [0] IMPLICIT SEQUENCE (SIZE (0...3)) OF NUMERIC STRING
                                                                    (SIZE(0...16)) OPTIONAL,
facsimileNumber               [1] IMPLICIT NUMERIC STRING (SIZE(0...16)) OPTIONAL,
networkAddress                [2] IMPLICIT OCTET STRING (SIZE (0...32)) OPTIONAL
}
```

```

E111Certificate::= SET
{
expiryDate [0] IMPLICIT NUMERIC STRING (SIZE(4..8))
}

EntitlementToBenefits::= SET
{
startingDate [0] IMPLICIT NUMERIC STRING (SIZE(4..8)),
expirationDate [1] IMPLICIT NUMERIC STRING (SIZE(4..8)) OPTIONAL
professionalCategory [2] IMPLICIT ENUMERATED
{1=employed, 2=self-employed, 3=student, 4=pensioner (scheme for
employed person), 5=pensioner (scheme for self-employed person),
6=other},
scheme [3] IMPLICIT ENUMERATED
1=Yes, 2=No. The person named above is covered by a scheme for self-
employed persons as referred to in Annex 11 to Regulation 574/72,
author [4] IMPLICIT Author
}

```

## 6. Clinical Data in ASN.1 form

```

clinicalData::= SET
{
codedClinicalDetails [0] IMPLICIT SET (SIZE (1...99)) OF CodedClinicalDetails OPTIONAL,
bloodGroupTransfusionDetails [1] IMPLICIT BloodGroupTransfusionDetails OPTIONAL,
immunisationDetails [2] IMPLICIT SET (SIZE (0...10)) OF ImmunisationDetails OPTIONAL,
medicationDetails [3] IMPLICIT SET (SIZE (1...30)) OF MedicationDetails OPTIONAL,
clinicalAddressDetails [4] IMPLICIT SET (SIZE (0...9)) OF ClinicalAddressDetails OPTIONAL,
opticalPrescriptionDetails [5] IMPLICIT OpticalPrescriptionDetails OPTIONAL,
updateDetails [6] IMPLICIT UpdateDetails
implants [7] IMPLICIT SET of Implants OPTIONAL,
pregnancyDetails [8] IMPLICIT Pregnancy OPTIONAL
}

CodedClinicalDetails::= SET
{
clinicalEmergencyCategory [0] IMPLICIT NUMERIC STRING (SIZE(2)),
clinicalIndicator [1] IMPLICIT ENUMERATED
{Absent(0), Present(1), Possible(2), Index(7), Not recorded(8), Not
supported(9)},
clinicalCodingStructure [2] IMPLICIT ClinicalCodingStructure OPTIONAL,
clinicalDate [3] IMPLICIT NUMERIC STRING (SIZE(4..8)) OPTIONAL,
clinicalText [4] IMPLICIT OCTET STRING (SIZE (0..80)) OPTIONAL,
clinicalEntryDate [5] IMPLICIT NUMERIC STRING (SIZE(4..8)) OPTIONAL,
clinicalAuthor [6] IMPLICIT Author OPTIONAL,
indexNumber [7] IMPLICIT OCTET STRING (SIZE (0..40)) OPTIONAL
}

ClinicalCodingStructure::= SET
{
codingSchemeIdentifier [0] IMPLICIT OCTET STRING (SIZE (6)),
clinicalCode [1] IMPLICIT OCTET STRING (SIZE (0..8)),
codingSchemeAcronym [2] IMPLICIT OCTET STRING (SIZE (0..10)) OPTIONAL
{since ISO7826 is not working this field can be used for the common name
of the codingscheme}
}

```

```

BloodGroupTransfusionDetails ::= SET
{
bloodGroup                [0] IMPLICIT BloodGroup,
bloodTransfusion          [1] IMPLICIT BloodTransfusion,
bloodGroupEntryDate       [2] IMPLICIT NUMERIC STRING (SIZE(4..8)) OPTIONAL,
bloodGroupAuthor          [3] IMPLICIT Author OPTIONAL
}

BloodGroup ::= SET
{
aBOBloodGroup             [0] IMPLICIT OCTET STRING (SIZE (1..2)),
rhesusFactor              [1] IMPLICIT OCTET STRING (SIZE (1)),
dateOfLastBloodGrouping   [2] IMPLICIT NUMERIC STRING (SIZE(4..8)) OPTIONAL,
bloodGroupingText         [3] IMPLICIT OCTET STRING (SIZE (0..30)) OPTIONAL
}

BloodTransfusion ::= SET
{
bloodTransfusionIndicator [0] IMPLICIT ENUMERATED
{Never(0), One or more (1), Unknown(2), Not recorded(8), Not supported(9),
lastBloodTransfusionDate [1] IMPLICIT NUMERIC STRING (SIZE(4..8)) OPTIONAL
}

ImmunisationDetails ::= SET
{
immunisationEmergencyCategory [0] IMPLICIT NUMERIC STRING (SIZE(2)),
immunisationIndicator         [1] IMPLICIT ENUMERATED
{Never(0), One or more(1), Unknown(2), Adverse reaction(4), Index(7), Not recorded(8), Not supported(9)},
immunisationStatus           [2] IMPLICIT ENUMERATED
{Unspecified(0), First dose(1), Second dose(2), Third dose(3), Completed course(4), Booster(5), Not supported(9)},
lastDateImmunised            [3] IMPLICIT NUMERIC STRING (SIZE(4..8)) OPTIONAL,
immunisationCodingStructure  [4] IMPLICIT ClinicalCodingStructure OPTIONAL,
immunisationText             [5] IMPLICIT OCTET STRING (SIZE (0..30)) OPTIONAL
immunisationEntryDate        [6] IMPLICIT NUMERIC STRING (SIZE(4..8)) OPTIONAL,
immunisationAuthor           [7] IMPLICIT Author OPTIONAL,
indexNumber                  [8] IMPLICIT OCTET STRING (SIZE (0..40)) OPTIONAL,
vaccinBatchNumber           [9] IMPLICIT OCTET STRING (SIZE (0..30)) OPTIONAL,
nextDateImmunised          [10] IMPLICIT NUMERIC STRING (SIZE(4..8)) OPTIONAL
}

```

MedicationDetails::= SET	
{	
medicationEmergencyCategory	[0] <b>IMPLICIT</b> NUMERIC STRING (SIZE(2)),
medicationIndicator	[1] <b>IMPLICIT</b> ENUMERATED {Absent(0), One or more(1), Unknown(2), Past or short term(5), Intermittent(6), <b>Index(7), Not recorded(8), Not supported(9)</b> ,
medicationCodingStructure	[2] <b>IMPLICIT</b> SET (SIZE (0..6)) OF ClinicalCodingStructure OPTIONAL,
medicationDrugName	[3] <b>IMPLICIT</b> OCTET STRING (SIZE (0..50)) OPTIONAL,
medicationDosageCode	[4] <b>IMPLICIT</b> SET (SIZE (0..4)) OF OCTET STRING (SIZE (0..2)) OPTIONAL,
medicationDosage	[5] <b>IMPLICIT</b> OCTET STRING (SIZE (0..50)) OPTIONAL,
medicationStartedDate	[6] <b>IMPLICIT</b> NUMERIC STRING (SIZE(4..8)) OPTIONAL,
medicationEndedDate	[7] <b>IMPLICIT</b> NUMERIC STRING (SIZE(4..8)) OPTIONAL,
medicationEntryDate	[8] <b>IMPLICIT</b> NUMERIC STRING (SIZE(4..8)) OPTIONAL,
medicationAuthor	[9] <b>IMPLICIT</b> Author OPTIONAL,
<b>indexNumber</b>	[10] <b>IMPLICIT</b> OCTET STRING (SIZE (0..40)) OPTIONAL,
<b>amountAuthorisedRenewals</b>	[11] <b>IMPLICIT</b> NUMERIC STRING (SIZE(2)) OPTIONAL,
<b>prescriptionDate</b>	[12] <b>IMPLICIT</b> NUMERIC STRING (SIZE(4..8)) OPTIONAL,
<b>drugBatchNumber</b>	[13] <b>IMPLICIT</b> OCTET STRING (SIZE (0..30)) OPTIONAL
}	
ClinicalAddressDetails::= SET	
{	
clinicalAddressName	[0] <b>IMPLICIT</b> OCTET STRING (SIZE (0..30)),
clinicalAddressRelationship	[1] <b>IMPLICIT</b> OCTET STRING (SIZE (0..16)) OPTIONAL,
clinicalAddressStructure	[2] <b>IMPLICIT</b> AddressStructure OPTIONAL,
clinicalTelecomStructure	[3] <b>IMPLICIT</b> TelecomStructure OPTIONAL
}	
OpticalPrescriptionDetails::= SET	
{	
opticalPrescription	[0] <b>IMPLICIT</b> OCTET STRING (SIZE (0..40)),
opticalPrescriptionDate	[1] <b>IMPLICIT</b> NUMERIC STRING (SIZE(4..8)) OPTIONAL
}	
UpdateDetails::= SET	
{	
dateOfLastClinicalUpdate	[0] <b>IMPLICIT</b> NUMERIC STRING (SIZE(4..8)),
responsibleParty	[1] <b>IMPLICIT</b> Author OPTIONAL
}	
Author::= SET	
{	
authorCountry	[0] <b>IMPLICIT</b> NUMERIC STRING (SIZE(3)) OPTIONAL,
authorIdentifier	[1] <b>IMPLICIT</b> NUMERIC STRING (SIZE(0..35)) OPTIONAL,
authorName	[2] <b>IMPLICIT</b> OCTET STRING (SIZE (0..20)) OPTIONAL
}	
<b>Implants::= SET</b>	
{	
<b>implantCategory</b>	[0] <b>IMPLICIT</b> NUMERIC STRING (SIZE(2))
}	
<b>Pregnancy::= SET</b>	
{	
<b>pregnancyDate</b>	[0] <b>IMPLICIT</b> NUMERIC STRING (SIZE(4..8)) OPTIONAL,
<b>pregnancyAuthor</b>	[1] <b>IMPLICIT</b> Author
}	

## E Recommendations for Restrictions for a Core Data Set of EU/G7 - Interoperability - data set (informative)

### 1 Usage of the G7-Interoperability-data set

The G7-Interoperability-dataset consist of three groups of data: card data, administrative and clinical data. These are specified using ASN.1 (ISO 8824) and must be coded according to the basic encoding rules (BER, ISO 8825).

To achieve full interoperability each data item must be readable by each system using the G7-dataset. But it is possible to make project specific restrictions.

#### Possibilities for reducing the dataset

In principle there are three different possibilities for reducing the data set:

1. not using optional data objects
2. reducing the maximum length of text items
3. reducing the maximum occurrence of data objects

#### Not using optional data objects

Different objects are specified as „OPTIONAL“, i.e. the useage is free. It should be discussed project specific which objects are needed or can be left out.

#### **Guideline 1**

**The G7-Interoperability-data set has to be checked concerning the need of objects. Not needed optional data objects can be left out project specific.**

#### Reducing the maximum length of text items

All (primitive) data objects are specified with a maximum length. If the length is not fixed it can be reduced.

#### **Guideline 2**

**In the G7-Interoperability-data set the maximum length of the data objects has to be checked project specific and if necessary reduced.**

#### Reducing the maximum occurrence of data objects

Some data object can be repeated. Sometimes the specific project requires less instances than possible.

#### **Guideline 3**

**In the G7-Interoperability-data set the maximum occurrence of the data objects has to be checked project specific and if necessary reduced.**

### 2 Core data set

Remark: The proposed core data set is based on the G7-interoperability-dataset and not on the dataset with the NETLINK proposals for modification. Following only revised definitions are listed.

#### CardData

data set-Definition	Reduction
CardApplicationData ::= SET {	<ul style="list-style-type: none"> <li>• no use of cardholderIdentifier</li> </ul>

<pre> cardIssuerIdentifier [0] CardIssuerIdentifier, cardHolderIdentifier [1] OCTET STRING (SIZE (0...21)) OPTIONAL, cardIdentifier [2] OCTET STRING (SIZE (0...28)), cardStatus [3] ENUMERATED {Unknown(0), Test(1), Normal(2)}, cardApplicationIdentification [64] SET SIZE (1...9) OF ApplicationTemplate cardApplicationIdentification [64] SET SIZE (1...2) OF ApplicationTemplate } </pre>	<p>(Id is also in the Administrative Data)</p> <ul style="list-style-type: none"> <li>number of ApplicationTemplate : 2</li> </ul>
--	--

### Administrative Data

data set-Definition	Reduction
---------------------	-----------

AdministrativeData ::= SET { <del>patientIdentification [0] SET SIZE (1...3) OF PatientIdentification,</del> patientIdentification [0] SET SIZE (1...1) OF PatientIdentification, nameDetails [1] NameDetails, <del>languageDetails [2] SEQUENCE SIZE (0...4) OF LanguageDetails OPTIONAL,</del> languageDetails [2] SEQUENCE SIZE (0...1) OF LanguageDetails OPTIONAL, birthDetails [3] BirthDetails, <del>addressDetails [4] SET SIZE (0...2) OF AddressDetails OPTIONAL,</del> addressDetails [4] SET SIZE (0...1) OF AddressDetails OPTIONAL, <del>contactDetails [5] SET SIZE (0...3) ContactDetails OPTIONAL,</del> contactDetails [5] SET SIZE (0...2) ContactDetails OPTIONAL, <del>insuringBodies [6] SET SIZE (0...3) OF InsuringBodyDetails OPTIONAL,</del> } 	<ul style="list-style-type: none"> <li>only one instance of patientIdentification, LanguageDetails and AddressDetails</li> <li>only one address</li> <li>no insurance data</li> </ul>
NameDetails ::= SET { title [0] OCTET STRING (SIZE (0...7)) OPTIONAL, surnameprefix [1] OCTET STRING (SIZE (0...15)) OPTIONAL, surname [2] OCTET STRING (SIZE (0...27)), <del>alternativeSurname [3] OCTET STRING (SIZE (0...27)) OPTIONAL,</del> <del>surnameSuffix [4] OCTET STRING (SIZE (0...15)) OPTIONAL,</del> <del>forenames [5] SEQUENCE SIZE (1...3) OF OCTET STRING (SIZE (1...16)),</del> forenames [5] SEQUENCE SIZE (1...1) OF OCTET STRING (SIZE (1...16)), <del>preferredForename [6] OCTET STRING (SIZE (1...16)) OPTIONAL</del> surnameAtBirth [7] OCTET STRING (SIZE (0...27)) OPTIONAL } 	<ul style="list-style-type: none"> <li>no use of alternativeSurname, surnameSuffix and preferredForename</li> <li>only one forename</li> </ul>
LanguageDetails ::= SET { language [0] OCTET STRING (SIZE (2)) <del>abilityInLanguage [1] ENUMERATED {preferred(0), fluent(1), fair(2), poor(3)} OPTIONAL,</del> } 	<ul style="list-style-type: none"> <li>no use of abilityInLanguage</li> </ul>
BirthDetails ::= SET { dateOfBirth [0] NUMERICSTRING (SIZE (4..8)), sex [1] ENUMERATED {unknown(0), male(1), female(2), other(3), other(9)} <del>countryOfBirth [2] OCTET STRING (SIZE (3)) OPTIONAL</del> } 	<ul style="list-style-type: none"> <li>no use of countryOfBirth</li> </ul>
ContactDetails ::= SET { contactName [0] OCTET STRING (SIZE (0...30)), <del>contactRelationship [1] OCTET STRING (SIZE (0...30)) OPTIONAL,</del> contactRelationship [1] OCTET STRING (SIZE (0...16)) OPTIONAL, contactAddressStructure [2] AddressStructure OPTIONAL, contactTelecomStructure [3] TelecomStructure OPTIONAL } 	<ul style="list-style-type: none"> <li>length of contactRelationship: 16</li> </ul>

data set-Definition	Reduction
---------------------	-----------

<pre> AddressStructure ::= SET { addressText          [0] SEQUENCE SIZE (1..5) OF OCTET STRING (SIZE                         (0..35)) <del>addressPostcode    [1] OCTET STRING (SIZE (0..8)) OPTIONAL,</del> addressCountry       [2] OCTET STRING (SIZE (0..3)) OPTIONAL } </pre>	<ul style="list-style-type: none"> <li>no use of addressPostcode (coding in addressText)</li> </ul>
<pre> TelecomStructure ::= SET { <del>telephoneNumber    [0] SEQUENCE SIZE (0..3) OF NUMERIC STRING                         (SIZE(0..16)) OPTIONAL,</del> telephoneNumber      [0] SEQUENCE SIZE (0..1) OF NUMERIC STRING                         (SIZE(0..16)) OPTIONAL, facsimileNumber      [1] NUMERIC STRING (SIZE(0..16)) OPTIONAL, <del>networkAddress     [2] OCTET STRING (SIZE (0..32)) OPTIONAL</del> } </pre>	<ul style="list-style-type: none"> <li>only one telephoneNumber</li> <li>no use of networkAddress</li> </ul>

### Clinical Data

data set-Definition	Reduction
<pre> ClinicalData ::= SET { <del>codedClinicalDetails [0] SET SIZE (1..99) OF CodedClinicalDetails,</del> codedClinicalDetails [0] SET SIZE (1..40) OF CodedClinicalDetails, bloodGroupTransfusionDetails [1] BloodGroupTransfusionDetails, immunisationDetails [2] SET SIZE (0..10) OF ImmunisationDetails                         OPTIONAL, <del>medicationDetails   [3] SET SIZE (1..30) OF MedicationDetails,</del> medicationDetails [3] SET SIZE (1..20) OF MedicationDetails, <del>clinicalAddressDetails [4] SET SIZE (0..9) OF ClinicalAddressDetails                         OPTIONAL,</del> <del>opticalPrescriptionDetails [5] OpticalPrescriptionDetails OPTIONAL,</del> updateDetails [6] UpdateDetails } </pre>	<ul style="list-style-type: none"> <li>only 40 codedClinicalDetails</li> <li>only 30 medicationDetails</li> <li>no use of clinicalAddressDetails and opticalPrescriptionDetails</li> </ul>
<pre> CodedClinicalDetails ::= SET { clinicalEmergencyCategory [0] NUMERIC STRING (SIZE(2)), clinicalIndicator [1] ENUMERATED {Absent(0), Present(1), Possible(2),                                 Not recorded(8), Not supported(9)}, <del>clinicalCodingStructure [2] ClinicalCodingStructure OPTIONAL,</del> <del>clinicalDate [3] NUMERICSTRING (SIZE (4..8)) OPTIONAL,</del> <del>clinicalText [4] OCTET STRING (SIZE (0..80)) OPTIONAL,</del> clinicalText [4] OCTET STRING (SIZE (0..40)) OPTIONAL, <del>clinicalEntryDate [5] NUMERICSTRING (SIZE (4..8)) OPTIONAL,</del> <del>clinicalAuthor [6] Author OPTIONAL</del> } </pre>	<ul style="list-style-type: none"> <li>no use of clinicalCodingStructure, clinicalDate, clinicalEntryDate, clinicalAuthor</li> <li>only 40 character text</li> </ul>
<pre> BloodGroupTransfusionDetails ::= SET { bloodGroup [0] BloodGroup, <del>bloodTransfusion [1] BloodTransfusion,</del> - wird über API bereitgestellt <del>bloodGroupEntryDate [2] NUMERICSTRING (SIZE (4..8)) OPTIONAL,</del> <del>bloodGroupAuthor [3] Author OPTIONAL</del> } </pre>	<ul style="list-style-type: none"> <li>no use of bloodTransfusion, bloodGroupEntryDate and bloodGroupAuthor</li> </ul>

data set-Definition	Reduction
<pre> BloodGroup ::= SET {   abOBloodGroup      [0] OCTET STRING (SIZE (1..2)),   rhesusFactor       [1] OCTET STRING (SIZE (1)),   <del>dateOfLastBloodGrouping [2] NUMERICSTRING (SIZE (4..8)) OPTIONAL,</del>   <del>bloodGroupingText [3] OCTET STRING (SIZE (0..30)) OPTIONAL</del> } </pre>	<ul style="list-style-type: none"> <li>no use of dateOfLastBloodGrouping and bloodGroupingText</li> </ul>
<pre> ImmunisationDetails ::= SET {   immunisationEmergencyCategory [0] NUMERIC STRING (SIZE(2)),   immunisationIndicator [1] ENUMERATED {Never(0), One or more(1),   Unknown(2), Adverse reaction(4), Not recorded(8), Not supported(9)},   immunisationStatus [2] ENUMERATED {Unspecified(0), First dose(1), Second dose(2), Third dose(3), Completed course(4),   Booster(5), Not supported(9)},   lastDateImmunised [3] NUMERICSTRING (SIZE (4..8)) OPTIONAL,   <del>immunisationCodingStructure [4] ClinicalCodingStructure OPTIONAL,</del>   <del>immunisationText [5] OCTET STRING (SIZE (0..30)) OPTIONAL</del>   immunisationText [5] OCTET STRING (SIZE (0..20)) OPTIONAL   <del>immunisationEntryDate [6] NUMERICSTRING (SIZE (4..8)) OPTIONAL,</del>   <del>immunisationAuthor [7] Author OPTIONAL</del> } </pre>	<ul style="list-style-type: none"> <li>no use of immunisationCodingStructure, immunisationEntryDate and immunisationAuthor</li> <li>only 20 character text</li> </ul>
<pre> MedicationDetails ::= SET {   medicationEmergencyCategory [0] NUMERIC STRING (SIZE(2)),   medicationIndicator [1] ENUMERATED {Absent(0), One or more(1),   Unknown(2), Past or short term(5), Intermittent(6), Not recorded(8), Not supported(9)},   <del>medicationCodingStructure [2] SET SIZE (0..6) OF ClinicalCodingStructure OPTIONAL,</del>   <del>medicationDrugName [3] OCTET STRING (SIZE (0..50)) OPTIONAL,</del>   medicationDrugName [3] OCTET STRING (SIZE (0..26)) OPTIONAL,   <del>medicationDosageCode [4] SET SIZE (0..4) OF OCTET STRING (SIZE (0..2)) OPTIONAL,</del>   medicationDosage [5] OCTET STRING (SIZE (0..50)) OPTIONAL,   <del>medicationStartedDate [6] NUMERICSTRING (SIZE (4..8)) OPTIONAL,</del>   <del>medicationEndedDate [7] NUMERICSTRING (SIZE (4..8)) OPTIONAL</del>   medicationEntryDate [8] NUMERICSTRING (SIZE (4..8)) OPTIONAL,   <del>medicationAuthor [9] Author OPTIONAL</del> } </pre>	<ul style="list-style-type: none"> <li>no use of medicationCodingStructure, medicationDosageCode, medicationDosage, medicationStartedDate, medicationEndedDate, medicationEntryDate and medicationAuthor</li> <li>only 26 character text</li> </ul>
<pre> UpdateDetails ::= SET {   dateOfLastClinicalUpdate [0] NUMERICSTRING (SIZE (4..8)),   <del>responsibleParty [1] Author OPTIONAL</del> } </pre>	<ul style="list-style-type: none"> <li>no use of responsibleParty</li> </ul>

size of the reduced data set: ca. 3000 Byte

Note: The number of characters in this annex are calculated on G7-base, not on the NETLINK recommended interoperability dataset.

## **F Presentation/Visualisation of G7-Interoperability-dataset (informative)**

Remark: The recommendations are based on the G7-interoperability-dataset and not on the dataset with the NETLINK proposals for modification.

### **Recommendations for the Visualisation of the G7-Interoperability-dataset**

The G7-Interoperability-dataset consists of three different groups of data:

1. Card Data
2. Administrative Data
3. Medical Data

Following the recommendations for the presentation are listed. They are described regardless of the platform used, to achieve a common layout.

#### **1 General remarks**

For all presentations the following applies:

- For each coded information the belonging text is retrievable directly.
- For ENUMERATED-values the respective meaning will be displayed. A list of possible entries has to be retrievable (e.g. for cardStatus „Unknown, Test, Normal“).
- For objects that will not be presented completely, it must be possible to display the more detailed data on demand. (Example: It is mentioned that an address for emergency cases is stored. On the users demand these data are listed completely.)
- In case there are no additional data for an object, this has to be stated clearly by a corresponding text or an optical highlighting.

An introductory screen is defined for which the following applies:

- On the introductory screen the most important medical information, stored on the card, is displayed.
- The list of the "important" medical data can be set by parameters. Recommendations are enclosed.
- The medical data consist of the seven groups CodedClinicalDetails, BloodGroupTransfusionDetails, ImmunisationDetails, MedicationDetails, ClinicalAddressDetails, OpticalPrescriptionDetails und UpdateDetails. On the introductory screen it is displayed additionally to the above mentioned data, if there is data stored for a group or not.
- For the groups CodedClinicalDetails, ImmunisationDetails und MedicationDetails the number of existing entries has to be displayed
- For CodedClinicalDetails the groups „Diseases“, „Procedures“ and „Allergies“ are displayed separately.
- On the introductory screen only single data items of the card owner shall be displayed (again by parameter setting, suggestion is name, surname and date of birth). More detailed information will be presented on user demand.

#### **2 Card data**

- Card data will only be displayed on demand.
- The data have to be visible on one single screen ( by consideration of the following rule).

- The data of „cardApplicationIdentification“ ( occurrences 1..9) are presented in groupes. It must be possible to display only one group at a time (number of characters for each group: max. 19).

### 3 Administrative-Data

- First the data object „NameDetails“ (comprised of title, surnamePrefix, surname, alternativeSurname, surnameSuffix, forenames, preferredForename und surnameAtBirth) (number of characters: max. 182) including date of birth (maximum number of characters 12) shall be displayed.

Additionally at least one card holders address (number of characters max. 283) and data of a contact person (maximum number of characters 342) will be presented.

Further address or contact data can be displayed separately.

- Data of PatientIdentification and LanguageDetails can be displayed separately.
- The insurance data will be displayed on separate screens. Groups must be displayable one by one (maximum number of characters 732).

### 4 Medical data

For the medical data CodedClinicalDetails, ImmunisationDetails und MedicationDetails the following applies:

- The data belonging to the same data entry must be displayed in groups.
- For the data of the author it is sufficient to display the name only. The additional data can be retrievable on demand.
- For each data entry the value of the category, the indicator and the status will be displayed in its corresponding meaning (e.g. instead of „Category=23, Indicator=1 and Status=1“ regarding ImmunisationDetails, „Category=Cholera (23), Indicator=One or More (1) und Status=First Dose (1)“ is displayed).

For ClinicalAddressDetails the following applies:

- This group will be displayed separately.
- The number of entries has to be stated.
- All data of one corresponding data entry have to be displayed in groups.(storage capacity 254 characters)

Furthermore:

- All data of BloodGroupTransfusionDetails will be presented together (storage capacity 93 characters)
- All data of OpticalPrescriptionDetails will be presented together (storage capacity 48 characters)

All data of UpdateDetails will be presented together (storage capacity 43 characters)

G7-Interoperability-dataset	max. length	max. occurencies	single length
CardApplicationData	235	1	
cardIssuerIdentifier	14	1	14
majorIndustryIdentifier	2	1	2
countryCode	3	1	3
issuerIdentifier	8	1	8
checkDigit	1	1	1

<b>G7-Interoperability-dataset</b>	<b>max. length</b>	<b>max. occurrences</b>	<b>single length</b>
cardHolderIdentifier	21	1	21
cardIdentifier	28	1	28
cardStatus	1	1	1
cardApplicationIdentification	171	9	19
cardApplicationIdentifier	16	1	16
discretionaryApplicationData	3	1	3
cardApplicationType	1	1	1
cardApplicationVersion	2	1	2
AdminData	4099		
patientIdentification	105	3	35
issuerOfPatientIdentifier	14	1	14
majorIndustryIdentifier	2	1	2
countryCode	3	1	3
issuerIdentifier	8	1	8
checkDigit	1	1	1
patientIdentifier	21	1	21
nameDetails	182	1	182
title	7	1	7
surnamePrefix	15	1	15
surname	27	1	27
alternativeSurname	27	1	27
surnameSuffix	15	1	15
forenames	48	3	16
preferredForename	16	1	16
surnameAtBirth	27	1	27
languageDetails	12	4	3
language	2	1	2
abilityInLanguage	1	1	1
birthDetails	12	1	12
dateOfBirth	8	1	8
sex	1	1	1
countryOfBirth	3	1	3
addressDetails	566	2	283
addressStatus	1	1	1
addressStructure	186	1	186
addressText	175	5	35
addressPostcode	8	1	8

<b>G7-Interoperability-dataset</b>	<b>max. length</b>	<b>max. occurrences</b>	<b>single length</b>
addressCountry	3	1	3
telecomStructure	96	1	96
telephoneNumber	48	3	16
facsimileNumber	16	1	16
networkAddress	32	1	32
contactDetails	1026	3	342
contactName	30	1	30
contactRelationship	30	1	30
contactAddressStructure	186	1	186
addressText	175	5	35
addressPostcode	8	1	8
addressCountry	3	1	3
contactTelecomStructure	96	1	96
telephoneNumber	48	3	16
facsimileNumber	16	1	16
networkAddress	32	1	32
insuringBodies	2196	3	732
insuringBodyCountry	3	1	3
insuringBodyIdentifier	9	1	9
insuringBodyName	20	1	20
insuringBodyAddressStructure	186	1	186
addressText	175	5	35
addressPostcode	8	1	8
addressCountry	3	1	3
insuringBodyTelecomStructure	96	1	96
telephoneNumber	48	3	16
facsimileNumber	16	1	16
networkAddress	32	1	32
e111Certificate	8	1	8
expiryDate	8	1	8
insuranceNumbers	42	1	42
insuredPersonPolicyNumber	21	1	21
nationalInsuranceNumber	21	1	21
insuredPerson	368	1	368
insuredPersonAddressStructure	186	1	186
addressText	175	5	35
addressPostcode	8	1	8

<b>G7-Interoperability-dataset</b>	<b>max. length</b>	<b>max. occurrences</b>	<b>single length</b>
addressCountry	3	1	3
insuredPersonTelecomStructure	96	1	96
telephoneNumber	48	3	16
facsimileNumber	16	1	16
networkAddress	32	1	32
relationshipToPatient	16	1	16
insuredPersonSurname	27	1	27
insuredPersonAlternativeSurname	27	1	27
insuredPersonForenames	16	1	16
ClinicalData	26398	1	26398
codedClinicalDetails	14652	99	148
clinicalEmergencyCategory	2	1	2
clinicalIndicator	1	1	1
clinicalCodingStructure	14	1	14
codingSchemeIdentifier	6	1	6
clinicalCode	8	1	8
clinicalDate	8	1	8
clinicalText	80	1	80
clinicalEntryDate	8	1	8
clinicalAuthor	35	1	35
authorCountry	3	1	3
authorIdentifier	12	1	12
authorName	20	1	20
bloodGroupTransfusionDetails	93	1	93
bloodGroup	41	1	41
aBOBloodGroup	2	1	2
rhesusFactor	1	1	1
dateOfLastBloodGrouping	8	1	8
bloodGroupingText	30	1	30
bloodTransfusion	9	1	9
bloodTransfusionIndicator	1	1	1
lastBloodTransfusionDate	8	1	8
bloodGroupEntryDate	8	1	8
bloodGroupAuthor	35	1	35
authorCountry	3	1	3
authorIdentifier	12	1	12
authorName	20	1	20

<b>G7-Interoperability-dataset</b>	<b>max. length</b>	<b>max. occurrences</b>	<b>single length</b>
immunisationDetails	990	10	99
immunisationEmergencyCategory	2	1	2
immunisationIndicator	1	1	1
immunisationStatus	1	1	1
lastDateImmunised	8	1	8
immunisationCodingStructure	14	1	14
codingSchemeIdentifier	6	1	6
clinicalCode	8	1	8
immunisationText	30	1	30
immunisationEntryDate	8	1	8
immunisationAuthor	35	1	35
authorCountry	3	1	3
authorIdentifier	12	1	12
authorName	20	1	20
medicationDetails	7620	30	254
medicationEmergencyCategory	2	1	2
medicationIndicator	1	1	1
medicationCodingStructure	84	6	14
codingSchemeIdentifier	6	1	6
clinicalCode	8	1	8
medicationDrugName	50	1	50
medicationDosageCode	8	4	2
medicationDosage	50	1	50
medicationStartedDate	8	1	8
medicationEndedDate	8	1	8
medicationEntryDate	8	1	8
medicationAuthor	35	1	35
authorCountry	3	1	3
authorIdentifier	12	1	12
authorName	20	1	20
clinicalAddressDetails	2952	9	328
clinicalAddressName	30	1	30
clinicalAddressRelationship	16	1	16
clinicalAddressStructure	186	1	186
addressText	175	5	35
addressPostcode	8	1	8
addressCountry	3	1	3

<b>G7-Interoperability-dataset</b>	<b>max. length</b>	<b>max. occurrences</b>	<b>single length</b>
clinicalTelecomStructure	96	1	96
telephoneNumber	48	3	16
facsimileNumber	16	1	16
networkAddress	32	1	32
opticalPrescriptionDetails	48	1	48
opticalPrescription	40	1	40
opticalPrescriptionDate	8	1	8
updateDetails	43	1	43
dateOfLastClinicalUpdate	8	1	8
responsibleParty	35	1	35
authorCountry	3	1	3
authorIdentifier	12	1	12
authorName	20	1	20

Note: The number of characters in this annex are calculated on G7-base, not on the NETLINK recommended interoperability dataset.

## G Secure messaging- Regulation aspects - France (informative)

The French legal framework changed significantly in January 99 after the French Prime Minister announced the liberalisation of the use of cryptography in France. The major changes within the French regulation focus on three main issues:

- free the usage of cryptography. (i.e. to allow citizens to make a free choice for data encryption products, software and tools). Nevertheless, an export trading control will be maintained as far as France is engaged through international trade agreements.
- Suppress the obligation to use a state certified TTP for legal key recovering purposes. (i.e. to suppress the compulsory steps of TPC registration for ciphering keys deposit). Therefore, the TPC role could be enhanced to various missions (e.g. digital signature).
- legislation changes to oblige anyone to decrypt any encrypted material when asked to do so by judicial authorities

Still the different use, conditions to provide, import or export products using cryptography is classified in four different categories :

- free
- submitted to simplified declaration
- submitted to declaration
- submitted to authorisation

The table hereafter summaries the new legal framework for cryptography in France :

**table 41 French legal framework for cryptography**

	Non-repudiation and authentication	Confidentiality		
		key ≤ 40 bits	key > 40 bits key ≤ 128 bits	key > 128 bits
Usage	Free	Free	Authorisation but free if with key recovery	authorisation
Providing	Simplified declaration	Declaration	Authorisation	
Importation	Free	Free	Authorisation	
Exportation	Free	Authorisation	Authorisation	

For non-repudiation and authentication only the provider is submitted to a simplified administrative declaration. For confidentiality the usage is free for keys up to 128 bits as long as you put in place a key recovery mechanism for keys longer than 40 bits. Otherwise the usage of confidentiality services using keys longer than 128 bits are submitted to authorisation.

## H DB access - Quebec's example (informative)

This will give an idea of what kind of databases exist and how they are accessed.

The health smart card system is used to supply and operate a group of databases (including the cards as part of the global database system):

- the portable patient record in the card's internal memory. In a local operating mode, the health smart card is used as a portable record. The clinical data in this record represents a summary portraying the user's state of health. It can also be used to check the user's status and his eligibility to certain services based on his administrative data. Last but not least, it can contain a „patient index,, which indicates the presence of external records;
- the patient's minimal clinical record in the card's external memory. The system operates an anonymous database which makes the access and secure communication possible between several health care professionals situated in different areas of practice. This database contains health information that the different health care professionals deem relevant to share depending on the patient's consent. It can regroup past examinations, prescribed drugs, medical and surgical history and other indications: it is the user's history of health or a minimal clinical record. Both the health care professional's and the user's card are needed in order to have access to the record, nevertheless not necessarily concomitantly. The patient has some control over the access rights to this database, such as is the case with the internal memory. Each record is secured by protected keys and indexes that are unique to each card and which de/encrypt and de/personalise the information. Without these keys and indexes, the personal information stored in this database appears as a string of incoherent codes that cannot be decrypted nor associated to the patient; therefore the term anonymous database.
- the insurer's record or nominative database. The health smart card system favours the interactive management of health insurance programs. Through secure access to the insurer's nominative databases, the system notably enables the insurer to check in real-time the patient's eligibility to programs and to certify the services offered by the health care professionals. By presenting the card, the patient can benefit from health insurance programs and establish, if necessary, his or the insurer's financial contribution. When the professional and the patient both connect themselves to the system by presenting their cards, they certify that the services have been offered. Furthermore, the patient will be able to view the cost of the services he uses.
- the health care centre's record. The patient's card, and more particularly the patient index, indicates to the health care professional the existence of a user's health record and where it is stored. In other words, if records for this patient exist in other health care centres, the professional is made aware of this. Access to the computerised patient records of various health care centres can be gained with the health care professional's card. Once set up in health care centres, the health smart card system would eventually replace the existing health care centre's cards.
- the depersonalised database. The health smart card system can also be used to set up a depersonalised database in order to gain information on the health care services that the population uses. This in turn supports research activities and strategic management: planning, monitoring and co-ordinating the resources used on a given territory; epidemiological research on the population's state of health; comparing health care centres; etc. The users of this database (managers, planners, researchers) hold cards which differentiate and certify their access.