




Smart Open Services for European Patients
Open eHealth initiative for a European large scale pilot of
Patient Summary and electronic Prescription

eADC Specifications

Appendix 6

D3.10.1

WORK PACKAGE	WP3.10
DOCUMENT NAME	eADC Specifications
SHORT NAME	D3.10.1- eADC Specifications
DOCUMENT VERSION	0.1
DATE	31/01/2012

	eADC Specifications	Document Short name:	D3.10.1- eADC Specifications
	WP3.10: eADC Specifications	Version:	0.1
		Date:	31/01/2012

COVER AND CONTROL PAGE OF DOCUMENT	
Document name:	eADC Specifications
Document Short name:	D3.10.1- eADC Specifications
Distribution level	PU-when released
Status	Final
Author(s): Organization:	Sören Bittins, Jörg Caumanns // FhG ISST ; Gottfried Heider // ELGA GmbH; Tobias Pass, MK, WW // Tiani Spirit GmbH WP3.10 Core Team

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

ABSTRACT
<p>“eADC Specifications” it collects the three documents prepared by the CCD team for the component foreseen for the Automatic Data Collection and Evaluation:</p> <ol style="list-style-type: none"> 1. The change proposal picturing this new component able to provide the functionality requested by the epsos Evaluation work package 2. The Administrators guide of eADC. 3. The end-user guide of eADC.

Change History					
Version	Date	Status Changes	From	Details	Review
V0.1	31/01/2012	Draft	Lombardy	First draft merging prepared for eADC	created material core team



	eADC Specifications	Document Short name:	D3.10.1- eADC Specifications
		Version:	0.1
	WP3.10: eADC Specifications	Date:	31/01/2012

TABLE OF CONTENTS

	1 INTRODUCTION	4
	1.1 Readers' Instructions	4
	2 eADC Change Proposal	5
10	3 Administrators guide of eADC	10
	4 The end-user guide of eADC	26

	eADC Specifications	Document Short name:	D3.10.1- eADC Specifications
		Version:	0.1
	WP3.10: eADC Specifications	Date:	31/01/2012

15 **1 INTRODUCTION**

1.1 **Readers' Instructions**

This deliverable collects the three documents prepared by the CCD team for the component foreseen for the Automatic Data Collection and Evaluation:

- 20
1. The change proposal picturing this new component able to provide the functionality requested by the epSOS Evaluation work package.
 2. The Administrators guide of eADC.
 3. The end-user guide of eADC.



Smart Open Services for European Patients

Open eHealth initiative for a European large scale pilot of
patient summary and electronic prescription

CCD Team – Change Proposal

Automatic Data Collection / Evaluation

WORK PACKAGE	CCD
DOCUMENT VERSION	1.0
DATE	04.05.11

COVER AND CONTROL PAGE OF DOCUMENT	
Document name:	
Distribution level	
Status	
Author(s):	Sören Bittins, Jörg Caumanns // FhG ISST
Organization:	Gottfried Heider // ELGA GmbH

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

ABSTRACT
<p>This change proposal is picturing a new component that is able to provide the requested functionality of the epSOS Evaluation work package. While the current reference implementation may only collect certain performance data points, the enhanced component may also extract important evaluation information from epSOS consumer documents (CDA).</p>

History of Alteration				
Version	Date	Status Changes	From	Review
1.0	April, 11 th , 2011		SB	

1. Introduction and Objective

In order to assess the success and performance of the epSOS large scale pilot, certain performance, scalability, and operational information is about to be collected from the NCP's and the data that is exchanged by the means of epSOS. The current epSOS reference implementation already supports a limited collection of statistical data, such as the total number of epSOS consumer document passed through the NCP network, error statistics, and human actors.

However, individual participating nations, as well as the epSOS evaluation work package, wish to collect a more sophisticated and flexible collection of data points within epSOS and, if applicable, the affected national infrastructures. Such behaviour was not anticipated during the original specification phase of epSOS and is therefore not included and implemented in the current release. The principle of the Monitoring Manager was the extraction of anonymous audit trail data and its presentation in a dedicated graphical user interface (GUI). Since many of the newly requested data points are not being processed within the Audit Repository, they cannot be extracted and re-used. The current list of the requirements with regards to the automatic data collection, as derived by the WP 1.2, can be found here: <https://service.projectplace.com/pp/pp.cgi/r578974834>

As a result, the epSOS CCD Team, in close cooperation with the epSOS working package 3.10, is proposing the introduction of a new component: the evaluation manager (EM). In contrast to the current evaluation means, the EM specifically understand epSOS consumer documents and may therefore extract an arbitrary set of data from any epSOS common component.

2. Evaluation Manager

2.1. Description

Two options have been identified in order to provide the requested enhanced evaluation functionality within the existing reference implementation:

1. an adaption of the existing Transformation Manager that intercepts and exports certain data sets, while performing the translation/transcoding or
2. the creation of a new, "floating" component that can be freely integrated at any interception point within the NCP or compatible environments.

While option 1 is rather simple to be implemented, any extension of the TM may also bear significant risks. The TM is specified to provide the semantic services and considered to be a critical component of epSOS. Keeping it self-contained might be a major requirement. It is also one of the few components that has full access and understanding of the processed data: Adding a new functionality to this component may prove problematic from a data safety and security standpoint. It may also hinder certain deployment scenarios in which the TM is not initiated from within the NCP but externally under the responsibility of the data providing HCP.

Option 2 is clearly causing a higher effort in implementation, however, provides a higher flexibility concerning data safety, data security, and deployment scenarios. It also facilitates the data protection assessments by being contained in an individual component that then may be evaluated and restricted accordingly to the concrete data protection demands of the operator. The EM may be integrated into the existing NCP by assigning it to any of the interceptor points in the NCP-internal data and control flow. Each participating nation as potential operator of the EM may decide, on which point, if any, the EM is to be invoked and what specific evaluation data sets are to be collected.

In any case, the EM is able to collect an arbitrary data set that is defined in advance and tailored to the specific requirements of each operator by the means of XPath and/or XSLT.

2.2. Requirements

The following requirements MUST be met by the implementation of the Evaluation Manager:

Number	Description
1	The Evaluation Manager MUST be able to arbitrarily export data points from any epSOS consumer document coded in CDA.
2	The Evaluation Manager MUST be able to detect the format of any input document by its format or type code.
3	The Evaluation Manager MUST report into a secure repository.
4	The Evaluation Manager MUST offer the possibility to search the result data sets and provide common exporting functionalities.
5	The Evaluation Manager MUST understand XPath and XSLT for data selection and transformation.

3. Commercial Setting

All commercial efforts are stated in person days (PD) and are assigned to each individual CCD Team Member. The daily rates, as presented in the original CCD proposal, are still valid. All efforts are transparently assigned to each activity and separated for each CCD Team member. FhG ISST may either perform the development on its own or subcontract one of the available Industry team partners as done in the original development work.

Organisation	Key Personnel	Rate / PD
FhG ISST	Jörg Caumanns, Sören Bittins, Raik Kuhlisch, Andreas Billig	721,50€ / PD
Tiani Spirit GmbH	Martin Tiani, Roland Maurer	980,00€ / PD

Organisation	Description of Work	Effort
FhG ISST	Specification of the Evaluation Manager	5 PD
FhG ISST	Development, documentation, and testing of the Evaluation Manager	18 PD
Tiani Spirit GmbH	Implementation, documentation, and testing of the interceptor interface in order to enable floating components	3 PD

Activity	ISST Effort PD	Cost / Activity
Specification & Development	23 PD	Max. 17.000,00€
Extension of the NCP Backbone	3 PD	Max. 3.000,00€
TOTAL	26 PD	Max. 20.000,00€



Smart Open Services for European Patients

Open eHealth initiative for a European large scale pilot of
patient summary and electronic prescription

CCD Team – Common Component Automatic Data Collection / Evaluation

WORK PACKAGE	CCD
DOCUMENT VERSION	1.1
DATE	15/12/2011

COVER AND CONTROL PAGE OF DOCUMENT	
Document name:	
Distribution level	
Status	Final
Author(s): Organization:	Tobias Pass, MK, WW // Tiani Spirit GmbH Sören Bittins // FhG ISST

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

ABSTRACT
Administrators guide of eADC.

History of Alteration				
Version	Date	Status Changes	From	Review
1.0	Dec., 6 th , 2011		SB	TP, MK, WW
1.1	Dec., 12 th , 2011	DB Change	SB	TP, MK, WW

1. Introduction and Objective

In order to assess the success and performance of the epSOS large scale pilot, certain performance, scalability, and operational information is about to be collected from the NCP's and the data that is exchanged by the means of epSOS. The current epSOS reference implementation already supports a limited collection of statistical data, such as the total number of epSOS consumer document passed through the NCP network, error statistics, and human actors.

However, individual participating nations, as well as the epSOS evaluation work package, wish to collect a more sophisticated and flexible collection of data points within epSOS and, if applicable, the affected national infrastructures. Such behaviour was not anticipated during the original specification phase of epSOS and is therefore not included and implemented in the current release. The principle of the Monitoring Manager was the extraction of anonymous audit trail data and its presentation in a dedicated graphical user interface (GUI).

Since many of the newly requested data points are not being processed within the Audit Repository, they cannot be extracted and re-used. The current list of the requirements with regards to the automatic data collection, as derived by the WP 1.2, can be found here:

<https://service.projectplace.com/pp/pp.cgi/r578974834>

2. epSOS Automatic Data Collection (eADC)

The epSOS Automatic Data Collection is designed in order to facilitate:

- the automatic, unsupervised information gathering and data extraction from every NCP transaction or consumer document that passes the NCP
- persistent storage of the resulting data sets in a RDBMS, available within each NCP
- the flexible definition of extraction rules and their specific application onto transactions or consumer documents

2.1. Prerequisites

The eADC requires a specific runtime and operation environment:

- a fully configured and operational epSOS NCP of version 6.02 or higher
- a suitable SQL-capable RDBMS and database instance within the NCP
- administrative permissions within the DB for initial setup of the eADC
- user access permissions for each DB unload and result data set export
- disk space within the DB' machine for continuous gathering of the desired data sets
- a data extraction drop point within the file system of the DB's virtual machine
- secure shell access or a scheduled operation manager (such as cron)
- result data set data transfer facilities (such as sftp, ssh, or a push mechanism)
- only administrators are anticipated to be interacting with any of the eADC functionality, end users are merely provided with results data sets in CSV files

2.2. Security Considerations

The eADC is considered to gather, store, and process highly sensitive information. The following sub-section may serve as a functionality and process description for security and data protection assignees within your organisation. Please note that security and data protection assignees may be required to review this section before this common component may be used within your organisation.

Scope and Extend Data Disclosure

The eADC is designed to flexibly extract any information that is contained in any epSOS transaction and its enclosed consumer documents. As such, the eADC potentially may have access to all information that is transported between NCP's, creating a piece of software that may be subject to a full disclosure of sensitive personal medical information.

Limitation of Use to Specific Circumstances

The eADC may only be used for enabling the designated evaluation task force to fulfill its assigned task as agreed by the epSOS decision bodies and in full compliance to the epSOS FWA and the individual regulatory setting at the point of operation.

Furthermore, the eADC may only be used after the prior authorization of the affected data protection assignees of the organization that is operating the NCP. It may also be necessary to document a prior authorization of the affected data subject (patient) under certain circumstances or regulatory settings, depending on your specific configuration and extent of the actual data extraction and collection.

Data Economy, Avoidance, and Minimisation

The eADC is potentially collecting and storing a redundant data set (copy of medical information) in relation to its individual configuration. Without manual intervention, the eADC is potentially storing the collected data sets for an indefinite period of time.

Information Security

The eADC result data sets and persistent data storage facilities within the RDBMS MUST be adequately protected from unauthorised access. The configuration and extraction rules MUST be adequately integrity protected.

2.3. eADC Provision

The eADC common component has been released and published as part of the NCP-in-the-Box version 6.02 and higher. However, without a specific installation by the administrative personnel the functionality remains dormant.

The required parts of the eADC are located within the directory:

`/opt/spirit/jboss/bin/EADC_resources/`

2.4. eADC Installation

Prerequisites:

- the ability to transfer files and directories to the target system

- access to the target system's RDBMS for executing SQL Scripts
- the ability to execute shell commands at the target system
- all steps need to be performed by an administrator and not a regular end-user

Installation:

- locate the RDBMS that is chosen to have eADC installed
- use the SQL-script ***create_EADC.sql*** provided in the directory ***EADC_resources/db*** on your local NCP to initially create the required tables within this database
- copy the directory ***EADC_resources*** to your ***jboss*** working directory "***../jboss/bin***"

2.5. eADC Configuration

Prerequisites:

- XML-Editor installed on your local computer that supports XML-Schemas and may display annotations (such as Eclipse-IDE, Oxygen or XMLSpy)
- working knowledge of XML and XPath
- all steps need to be performed by an administrator and not a regular end-user

Configuration:

- copy the directory ***EADC_resources*** from the target system to your workstation
- configure the extraction rules by editing the file ***EADC_resources/config/config.xml*** with your XML-Editor:
 - *Hint* – each XML node contains additional information on:
 - what content is allowed within that XML-Node
 - how this node affects the data extraction
- move your edited local copy of ***EADC_resources/config/config.xml*** back to the target system by updating/overwriting ***EADC_resources/config/config.xml***

Exemplary Configuration:

This sub-section contains an exemplary configuration for extracting and collecting the gender of a patient that is coded by the property ***administrativeGenderCode*** within an epSOS CDA consumer document.

- determine the XML-Node within the CDA-Documents that contains the property to be extracted and collected → **cda:administrativeGenderCode**
- create an XPath expression that points to that property. This expression is used to navigate within the document that contains the data to be extracted:

```
/proxy:Transaction/cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:patient/cda:administrativeGenderCode
```

- open **EADC_resources/config/config.xml** and navigate to the **childTable** node
- within that node insert the following **extractionRule** node:

```
<extractionRule matchXPath=
"/proxy:Transaction/cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:patient/cda:administrativeGenderCode">
  <mapping targetColumn="DataType" sourceXPath="'0815'"/>
  <mapping targetColumn="DataTypeName" sourceXPath="'Gender Code'"/>
  <mapping targetColumn="DataValue" sourceXPath="."/ />
  <mapping targetColumn="ValueDisplay" sourceXPath="."/ />
</extractionRule>
```

- the **matchXPath** attribute is targeting the **administrativeGenderCode** node. This extraction rule is being processed for every match of this XPath within the transaction-xml.
- every **mapping** node specifies a customizable part of the resulting sql-insert statement that stores the collected information in the database:
 - the **targetColumn** attribute specifies into which table-column within the database the value should be stored.
 - the **sourceXPath** attribute specifies the content that should be stored. It must contain a valid XPath expression. This expression is evaluated within the context of the currently processed node that was matched by **matchXPath**

2.6. Exporting the Result Data Sets

Prerequisites:

- the ability to transfer files and directories to the target system
- access to the target system's RDBMS for executing SQL Scripts
- the ability to execute shell commands at the target system
- all steps need to be performed by an administrator and not a regular end-user

Export:

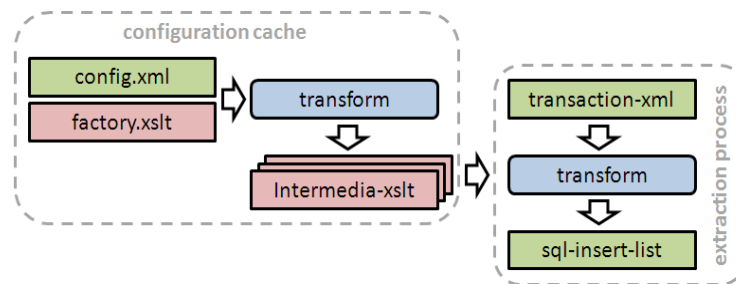
- log in to the target system via ssh
- execute the following command (copy&paste):

```
mysql -utmed -ptmed -e "select 'Transaction_PK','Direction','HomeISO','HomeNCP_OID','HomeHCID','HomeHost','HomeAddress','SndISO','SndNCP_OID',
'SndHCID','SndAddress','SndHost','SndMsgID','ReceivingISO','ReceivingNCP_OID','ReceivingHost','receivingAddr','ReceivingMsgID','TransactionCounter',
'HumanRequestor','UserId','POC','POC_ID','AuthenticationLevel','RequestAction','ResponseAction','ServiceType','ServiceName','StartTime','EndTime',
```

```
'Duration','TransactionData_PK','Transaction_FK','DataType','DataTypeName','DataValue','ValueDisplay','Void0','Void1','Void2','Void3','Void4','Void5',
'Void6','Void7','Void8','Void9' \
union select * INTO OUTFILE '/tmp/etransactiondata_`hostname`_`date`+%Y%m%d%H%M%S`' FIELDS TERMINATED BY ',' OPTIONALLY ENCLOSED BY '\"
LINES TERMINATED BY '\n' \
from tmed.etransaction left join tmed.etransactiondata on etransaction.Transaction_PK=etransactiondata.Transaction_FK"
```

- The above command unloads the content of the tables **etransaction** and **etransactiondata** to the CSV file **/tmp/etransactiondata_`hostname`_`date`+%Y%m%d%H%M%S`** i.e. **/tmp/etransactiondata_ncp-at_20111102123839**

2.7. eADC Extraction Workflow



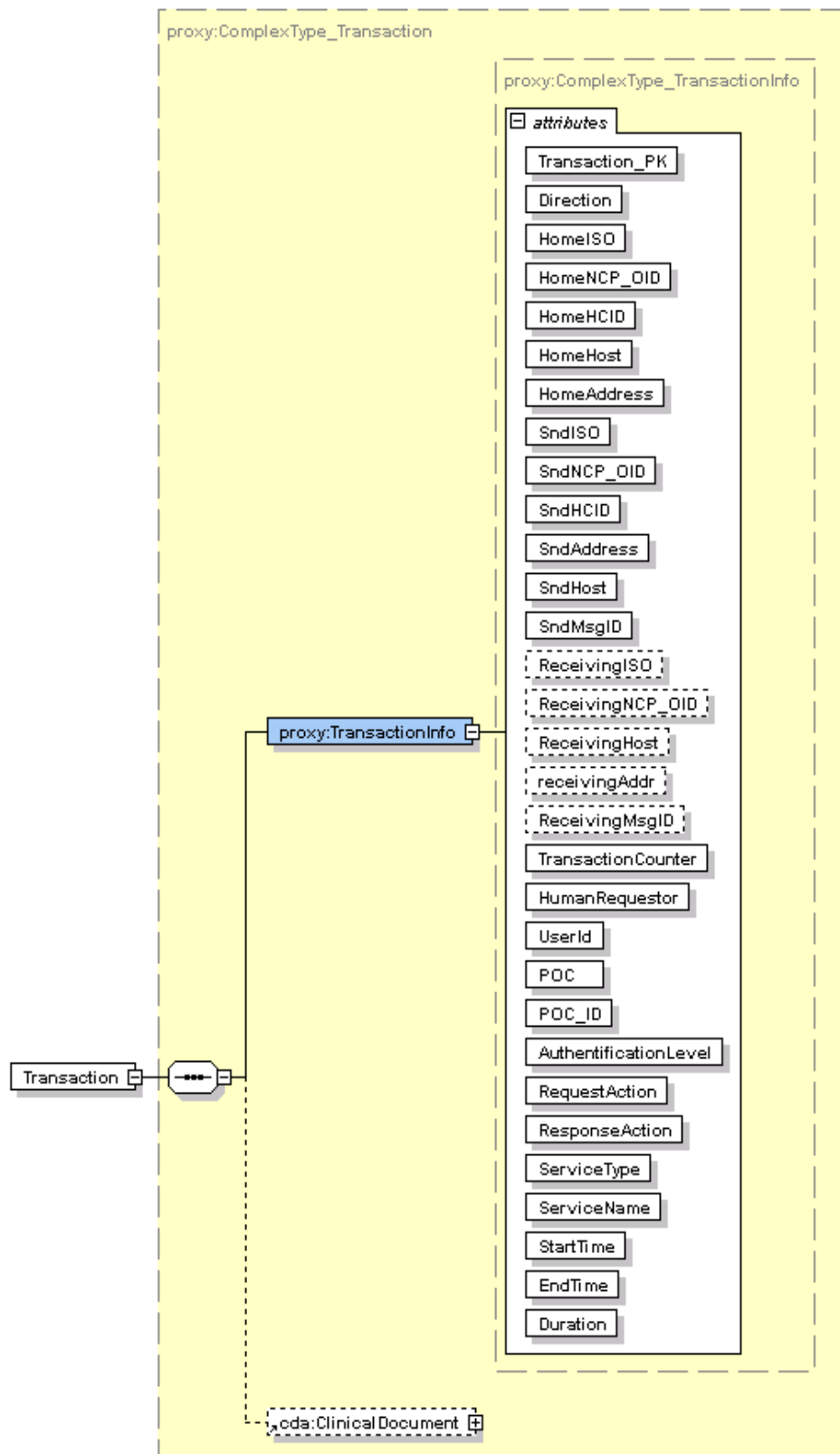
The workflow consists of two branches, which are described in detail as follows:

- **Extraction Process:**
 - The spirit proxy feeds the eADC with a transaction-xml as specified in the section XML-Schema Diagrams.
 - If the transaction has an appended CDA-document, the class-code of that document is extracted, otherwise "null" is used as classcode.
 - An XML-stylesheet, that is customized for being used along with that class-code, is then retrieved from the configuration cache.
 - The retrieved XML-stylsheet is applied to the transaction-xml.
 - The resulting plaintext output is a list of SQL-insert-statements.
 - Those statements are then executed by using the JDBC-connector
- **Configuration Cache:**
 - Extraction rules are specified in the file config.xml. (Every extraction rule can be configured for being applied to a specific subset of CDA-document-types.)
 - A stylesheet request from the extraction process always contains a specific CDA classcode.
 - The factory.xslt, the config.xml, and this classcode are used to generate an intermedia-xslt, which is then cached.
 - This cache can be cleared by reloading the proxy configuration

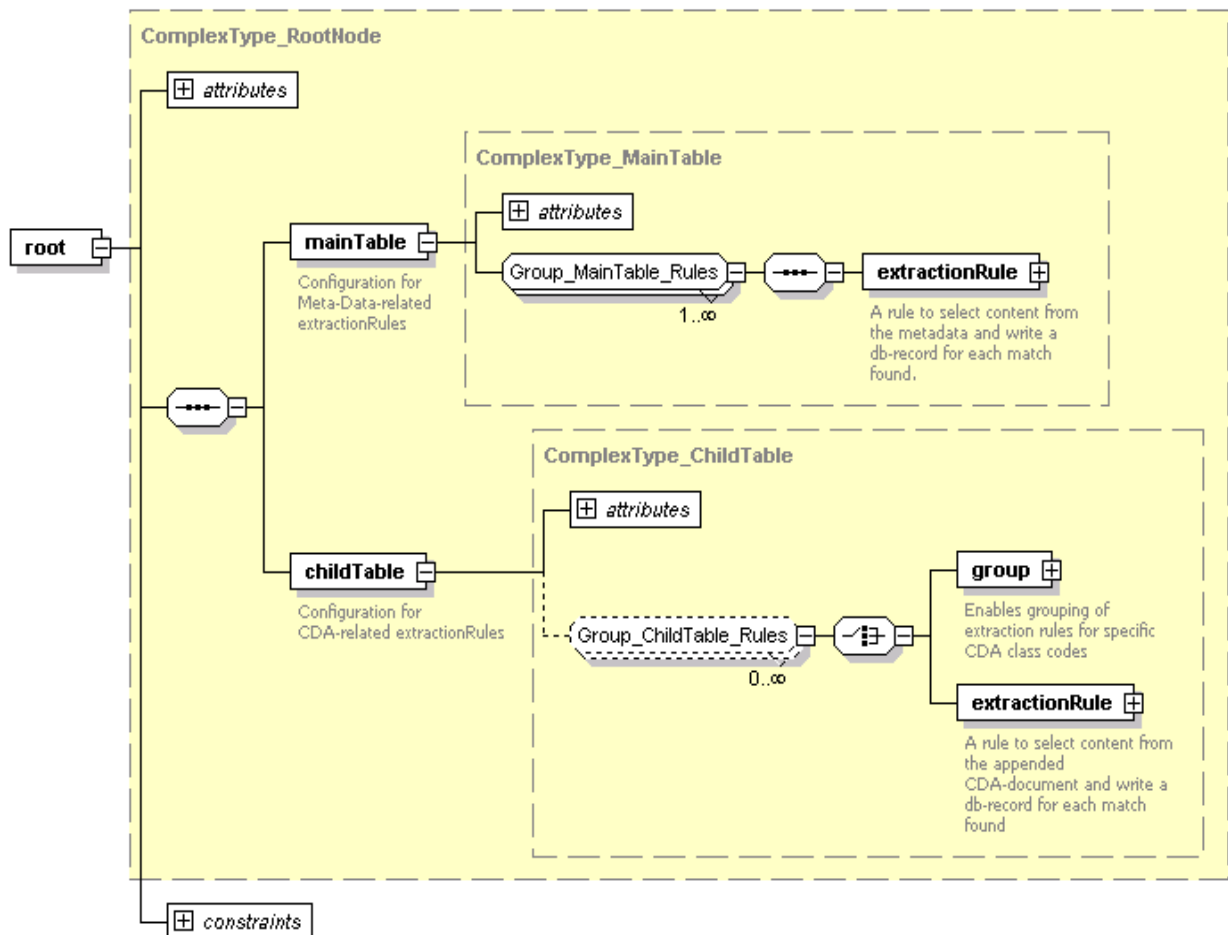
2.8. Additional Developers and Administrators Resources

Input Data Structure:

The following XML-Structure is used to feed the EADC

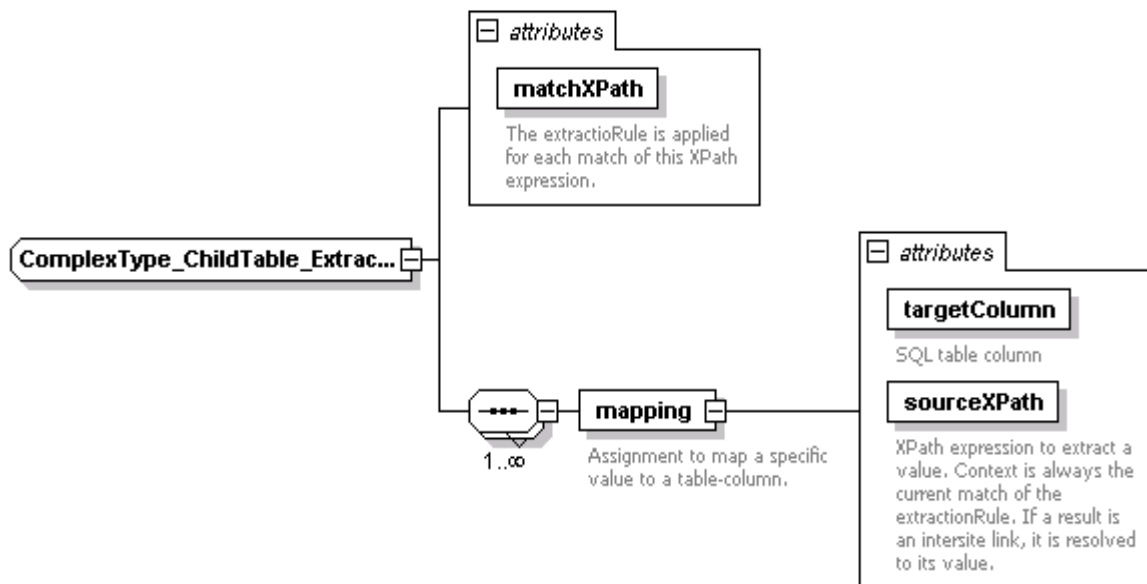


Configuration Root Node:



- The maintable and childtable have a similar specification for extractionRule. Every NCP-transaction is parsed by the **MainTable-extractionRule** and by the **ChildTable-extractionRules**:
 - The **MainTable-extractionRule** translates the parsed transaction-message into an SQL-query that inserts the data into the MainTable.
 - Every **ChildTable-extractionRule** generates an SQL-insert-statement for every match of any **extractionRule**. The extracted data is inserted into the **ChildTable** by those insert statements.

Extraction Rule:



2.9. Manual Data Source and Database Configuration

Within the default deployment, the eADC is residing in the same RDBMS as other functions of the NCP. However, due to concerns of the separation of responsibilities, general security policy, and purpose binding, it might be required to move the eADC to another physical RDBMS.

The following sub-section is guiding administrators through preparation and configuration of using a separate or other database for all eADC concerns.

Prerequisites:

- the ability to transfer files and directories to the target system
- availability of an operational RDBMS w/ sufficient capacity of enabling eADC (>4GB)
- administrative access to the target system's RDBMS for executing SQL Scripts
- the ability to execute shell commands at the target system
- all steps need to be performed by an administrator and not a regular end-user

Preparing the RDBMS, Database, and Users

1. open the configuration and management interface to the RDBMS to be used
2. create a database instance within that RDBMS for eADC:
 - a. execute “`CREATE DATABASE <database-name>;`” `eADCDokuTestDB` is used as example
→ “`Query OK, 1 row affected (0.05 sec)`”
 - b. perform initial check by executing: “`SHOW DATABASES`”
→ “

```
+-----+
| Database          |
+-----+
| eADCDokuTestDB    |
| eFAPerfLogInterceptor |
+-----+
3 rows in set (0.00 sec)
```

”
3. create and configure the user and access rights for the newly created database:
 - a. execute “`GRANT ALL PRIVILEGES ON eADCDokuTestDB.* TO eADCTstUsr@localhost IDENTIFIED BY 'password';`”
 - b. check the successful operation by executing “`SELECT User,Host,Password from mysql.User;`”

Preparing the Data Source, JNDI, and JDBC

1. provide the JDBC data driver classes according to your RDBMS (MySQL in example)
2. provide the deployment by creating/editing “`mysql-ds.xml`” in the `deploy` directory:

```
<datasources>
  <local-tx-datasource>
    <jndi-name>eADCTsTDoc</jndi-name>
    <connection-url>jdbc:mysql://localhost:1234/eADCDokuTestDB </connection-url>
    <driver-class>com.mysql.jdbc.Driver</driver-class>
    <user-name> eADCTstUsr </user-name>
    <password>password</password>
  </local-tx-datasource>
</datasources>
```

The current default configuration of the NCP-in-the-Box is using the following data sources and configuration: `/opt/spirit/jboss/server/spirit/deploy/mysql-ds.xml`

```
<datasources>
  <local-tx-datasource>
    <jndi-name>eADCTsTDoc</jndi-name>
    <connection-url>jdbc:mysql://localhost:1234/eADCDokuTestDB </connection-url>
    <driver-class>com.mysql.jdbc.Driver</driver-class>
    <user-name> eADCTstUsr </user-name>
```

```

    <password>password</password>
  </local-tx-datasource>
</datasources><datasources>
  <local-tx-datasource>
    <jndi-name>MySQLDS</jndi-name>
    <connection-url>jdbc:mysql://localhost:3306/tmed</connection-url>
    <driver-class>com.mysql.jdbc.Driver</driver-class>
    <user-name>tmed</user-name>
    <password>tmed</password>
  </local-tx-datasource>
  <local-tx-datasource>
    <jndi-name>MySQLxdsDS</jndi-name>
    <connection-url>jdbc:mysql://localhost:3306/xds3</connection-url>
    <driver-class>com.mysql.jdbc.Driver</driver-class>
    <user-name>tmed</user-name>
    <password>tmed</password>
  </local-tx-datasource>
  <local-tx-datasource>
    <jndi-name>MySQLDS_PIXV3</jndi-name>
    <connection-url>jdbc:mysql://localhost:3306/PIXV3</connection-url>
    <driver-class>com.mysql.jdbc.Driver</driver-class>
    <user-name>tmed</user-name>
    <password>tmed</password>
  </local-tx-datasource>
</datasources>

```

Configuration of the eADC2DataSource Link in Proxy/Injection Handler

1. navigate to the configuration file:
/opt/spirit/jboss/bin/proxy/ProxyCodeMapper/InjectionHandlerMappings.xml
2. locate the provision of the data source configuration within the Injection Handler:
<Code key="datasource" value="java:<currentConfigValue"/>
3. edit the key according to your individual needs and save the configuration file
4. restart the instance

Exemplary and default configuration:

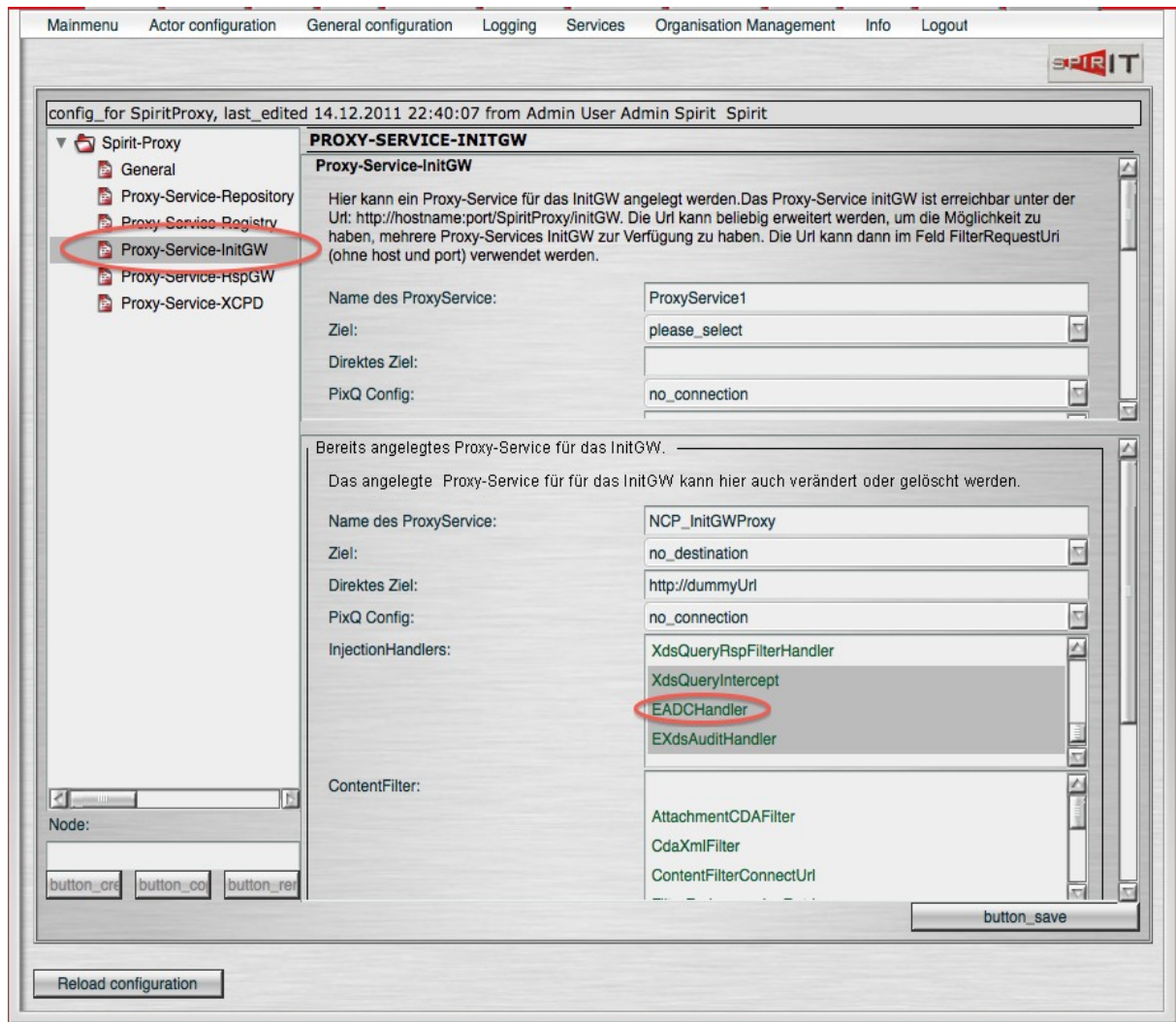
```

<!-- call Handler for AutomaticDataCollector -->
<CodeType name="EADCHandler_HandlerInjection" >
  <Code key="active" value="true"/>
  <Code key="supportedServices" value=""/>
  <Code key="injectionPlace" value="RSP,ERROR"/>
  <Code key="executionClass" value="com.spirit.proxy.handler.general.EADCHandler"/>
  <Code key="datasource" value="java:/MySQLDS"/>
  <!-- Code key="useFQ" value="false"/-->
  <!-- Code key="usedADCReceiverImpl" value="com.spirit.epsos.cc.adc.EADCReceiverImpl"/-->
  <!-- Code key="usedADCEntryImpl" value="com.spirit.epsos.cc.adc.EADCEntryImpl"/-->
</CodeType>

```

Configuration of the eADC2DataSource Link in Transaction Broker

1. open the Transaction Broker and log-on using your credentials
2. navigate to “**Spirit-Proxy**” and then to “**Proxy-Service-RspGW**”
3. select “**EADCHandler**” in the selection box named “**InjectionHandlers**”
4. navigate to “**Spirit-Proxy**” and then to “**Proxy-Service-InitGW**”
5. select “**EADCHandler**” in the selection box named “**InjectionHandlers**”



Mainmenu Actor configuration General configuration Logging Services Organisation Management Info Logout

SPRIT

config_for SpiritProxy, last_edited 14.12.2011 22:40:07 from Admin User Admin Spirit Spirit

- Spirit-Proxy
 - General
 - Proxy-Service-Repository
 - Proxy-Service-Registry
 - Proxy-Service-InitGW
 - Proxy-Service-RspGW**
 - Proxy-Service-XCPD

PROXY-SERVICE-RSPGW

Proxy-Service-RspGW

Hier kann ein Proxy-Service für das RspGW angelegt werden. Das Proxy-Service-RspGW ist erreichbar unter der Url: http://hostname:port/SpiritProxy/rspGW. Die Url kann beliebig erweitert werden, um die Möglichkeit zu haben, mehrere Proxy-Services RspGW zur Verfügung zu haben. Die Url kann dann im Feld FilterRequestUri (ohne host und port) verwendet werden.

Name des ProxyService: ProxyService1
Ziel: please_select
Direktes Ziel:
PixQ Config: no_connection

Bereits angelegtes Proxy-Service für das RspGW

Das angelegte Proxy-Service für für das RspGW kann hier auch verändert oder gelöscht werden.

Name des ProxyService: NCP_RespGWProxy
Ziel: no_destination
Direktes Ziel: http://dummyURL
PixQ Config: no_connection
InjectionHandlers:
XdsQueryRspFilterHandler
XdsQueryIntercept
EADCHandler
EXdsAuditHandler

ContentFilter:
Error :null

Node:
button_cre button_co button_re

button_save

Reload configuration



Smart Open Services for European Patients

**Open eHealth initiative for a European large scale pilot of
patient summary and electronic prescription**

CCD Team – Common Component

Automatic Data Collection / Evaluation

End-User's Reference

WORK PACKAGE	CCD
DOCUMENT VERSION	1.0
DATE	18/12/2011

COVER AND CONTROL PAGE OF DOCUMENT	
Document name:	
Distribution level	
Status Final	
Author(s):	Tobias Pass, MK, WW // Tiani Spirit GmbH
Organization:	Sören Bittins // FhG ISST

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

ABSTRACT
End-user reference of eADC.

History of Alteration				
Version	Date	Status Changes	From	Review
1.0 Dec.,	16 th , 2011		SB	TP, MK, WW

1. Introduction and Objective

In order to assess the success and performance of the epSOS large scale pilot, certain performance, scalability, and operational information is about to be collected from the NCP's and the data that is exchanged by the means of epSOS. The current epSOS reference implementation already supports a limited collection of statistical data, such as the total number of epSOS consumer document passed through the NCP network, error statistics, and human actors.

However, individual participating nations, as well as the epSOS evaluation work package, wish to collect a more sophisticated and flexible collection of data points within epSOS and, if applicable, the affected national infrastructures. Such behaviour was not anticipated during the original specification phase of epSOS and is therefore not included and implemented in the current release. The principle of the Monitoring Manager was the extraction of anonymous audit trail data and its presentation in a dedicated graphical user interface (GUI).

Since many of the newly requested data points are not being processed within the Audit Repository, they cannot be extracted and re-used. The current list of the requirements with regards to the automatic data collection, as derived by the WP 1.2, can be found here:

<https://service.projectplace.com/pp/pp.cgi/r578974834>

This document is targeted at the end-users of the eADC as reference material explaining the extracted data points, and facilitating the assessment and interpretation of such.

2. References

The data base for the eADC is specified and formalised within the following documents:

Document Type		Contents
D3.4.2v2.2	Spec. Normative	Transaction specification, available meta-data, and usage constraints
D3.9.1 Appendix B1	Spec, Guide	CDA elements, restrictions, epSOS extensions and purpose of use
CDA, POCD_MT000040 (extended), core and extended schemata	XSD Normative	Validation and formalised purpose of use, dependencies and organisation, valid codomain and parameters, data compartmentalisation, deployment

3. epSOS Automatic Data Collection (eADC)

The epSOS Automatic Data Collection is designed in order to facilitate:

- the automatic, unsupervised information gathering and data extraction from every NCP transaction or consumer document that passes the NCP
- persistent storage of the resulting data sets in a RDBMS, available within each NCP
- the flexible definition of extraction rules and their specific application onto transactions or consumer documents

The eADC is designed to be able to extract and compile any transactional data from any specified epSOS business operation. Please note that this only scopes NCP2NCP transactions as defined in epSOS, while country-internal operations, such as portal delivery and foreign Identity Provider, are considered private operations that may not be reflected in eADC.

The eADC is extracting the desired data sets in an immediate fashion and in real-time. This means that the eADC has a direct, unfiltered access to the transactional and CDA information without any intermediaries, such as the auditable events or performance data collectors. As a result, the eADC may operate independently from any other means within the NCP by its interceptor character and needs to be safeguarded as such.

The extracted data itself represents raw data points in general, however, may also contain simple eADC-internal aggregations and calculations, such as calculating the current age of a data subject by subtracting the birthdate from the transaction date. Please note that those calculations and aggregations may impact the final assessment as the calculations are performed at the time of extraction, which is not necessarily the time of evaluation. If advanced features of the eADC are operated, the assessment time needs to be adjusted accordingly in order to avoid fuzzy data such as an incorrect patient age: if the patient was 30 at the point of extraction but 31 at the point of assessment, the data contained in the export file is principally unable to reflect this fact.

3.1. eADC Data Extraction

The eADC toolset needs to be configured in order to be able to extract and export any data. The tool itself has no end-user interface at all and is designed to be configured by an administrator exclusively. The configuration permits flexible scenarios that also enable a PN to operate their own data extraction in excess of the epSOS-wide extraction rules.

For details or questions concerning the capabilities, configurations, and operation of the eADC, please refer to the document “*epSOS CCD eADC Administrators Guide*” or your local NCP administrator.

3.2. eADC Transaction Data Points

Medical and administrative information, such as authorisation and authentication statements, originators and targets, are communicated between the affected NCP's by a set of sanctioned messages. The term sanctioned in this circumstance means that only a well-defined set of messages in a certain order may be issued and received by each NCP at any point in time. Furthermore, each message contains one transaction that is directly related to an epSOS service, such as the epSOS Patient Service or epSOS Identification Service.

Each transaction is containing administrative information as transaction meta-data in addition to the service pay load (which is generally the CDA that is displayed to the HP). The meta-data contains significant information, such as the transaction time, target, human actor, and status. Those data points may be significant for an evaluation of the overall epSOS system and are therefore fully assessable by the eADC.

The following sub-section is introducing and listing the available transaction data points, as well as briefly describing the purpose of each term. It is also categorising each term primary domain, which is indicated by a **E** for Evaluation Team, **A** for Administrative Data, and **B** for both. Administrative data is primarily used to ensure that the extracted data may be directly mapped to the original transaction and its context may be re-established. Evaluation data is primarily aimed at the Evaluation team for their assessment of the NCP performance. It is safe to assume that, unless a fatal error has occurred, the Evaluation Team may ignore the Administrative data points.

Figure 1 is illustrating the available data points within each transaction, while Table 1 is briefly introducing and explaining the meaning of each data point.

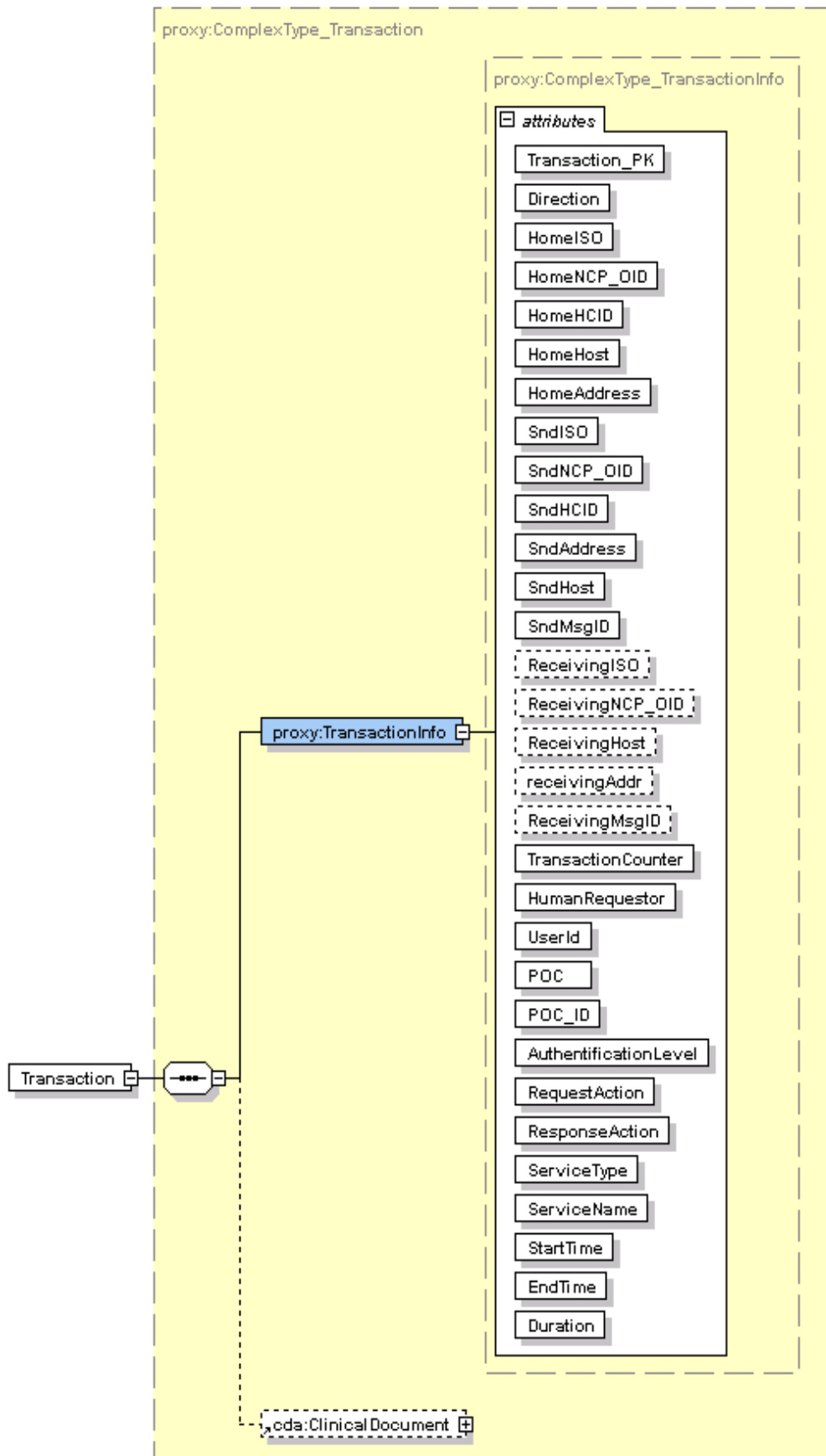


Figure 1: Available Transactional Data Points

Data Point	Type	Description
Transaction_PK	A	This field is the sequential identifier of the local transaction, also used as primary key.
Direction	B	This data point designates the direction of the transaction for instance whether the NCP in its current role (either NCP-A or NCP-B) has issued the transaction "outbound" or received a transaction from another NCP "inbound".
HomeISO	E	This data point contains the ISO country code of the local NCP, such as "DK", "AT", or "FR".
HomeNCP_OID	A	This data point contains the OID of the local NCP that is used to establish the home community and for epSOS-internal addressing and localisation of the NCP.
HomeHCID	A	IHE home community I.D. of the local NCP.
HomeHost	A	This data field contains the fully-qualified host name of the local NCP.
HomeAddress	A	This data field contains the IP address of the local NCP.
SndISO	E	This data point contains the ISO country code of the sending NCP, such as "DK", "AT", or "FR".
SndNCP_OID	A	This data point contains the OID of the sending NCP.
SndHCID	A	IHE home community I.D. of the sending NCP.
SndAddress	A	This data field contains the IP address of the sending NCP.
SndHost	A	This data field contains the fully-qualified host name of the sending NCP.
SndMsgID	A	This data field contains a unique number that is explicitly identifying the concrete message that has been send. Please note: message I.D. are split in sent messages and received messages to enable the detection of messages that have been sent but never.
ReceivingISO	A	This data point contains the ISO country code of the receiving NCP, such as "DK", "AT", or "FR".
ReceivingNCP_OID	A	This data point contains the OID of the receiving NCP.
ReceivingHost	A	This data field contains the fully-qualified host name of the receiving NCP.
ReceivingAddr	A	This data field contains the IP address of the receiving NCP.
ReceivingMsgID	A	Contains a unique number that is explicitly identifying the concrete received message.
TransactionCounter	B	Total number of transaction processed by this NCP (not to be confused with the number of events, as events may require more than one transaction on order to be fulfilled).
HumanRequestor	A	Identifier of the HP who initiated the event, contains the name identifier as given in the Authentication Assertion that was issued for this HP (not necessarily human readable).
UserID	E	Human readable name of the HCP in the Subject-ID attribute of the HP Identity Assertion.
PoC	E	Point of Care that invoked the transaction. The PoC data point is containing the full PoC registration data as provided by the foreign NCP in country-B in a human readable form.
PoC_ID	A	Point of Care I.D. contains only the I.D. number of a foreign PoC as provided by the NCP-B.
AuthenticationLevel	B	This data point contains the authentication method, the foreign HP used to log-on to the epSOS system, such as username/password combination or a smart card with certificate.
RequestAction	B	The specific action that was contained and requested in the transaction.
ResponseAction	B	The response action caused by the reception of the request action.
ServiceType	B	Type of the service that was invoked by the transaction.
ServiceName	B	Name of the service that was invoked by the transaction.
StartTime	B	Time when the transaction was invoked. Please note: All NCP times are provided as POSIX time stamps that need to be converted to human readable time (RFC2822). As an example, a time value of "1318576240843" correlate to "GMT: Fri, 14 Oct 2011 07:10:40 GMT".
EndTime	B	Time when the transaction was transmitted and processed.
Duration	E	This data points reflects the time a given transaction took.
Void[0..9]		Extension slots for individual data extraction in the responsibility of the PN.

Table 1: Transactional Data Point Description

3.3. eADC Consumer Document Data Points

In addition to the transactional meta-data, any accessible node from a CDA document (for a complete list of nodes, see D3.9.1 Appendix B1) may also serve as data source for the eADC. The eADC in its default configuration already contains a set of exemplary data points:

1. patients country from: `cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:addr/cda:country`
2. patients birth date from: `cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:patient/cda:birthTime`

The data points extracted from the CDA are presented using four data columns for the end-users convenience, as illustrated in Table 2:

Column Heading	Description
Data Type	This field contains the source data type of the extracted data for enabling the end user to map the extracted data to its expected data type. For instance, for extracting the patient's Country of Affiliation (CoA), this information is contained in the CDA consumer document within the node: <code>cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:addr/cda:country</code> . The specific node, as contained in the CDA is also determining its data type (for instance a date, text or a number).
DataTypeName	This field contains a freely selectable name for the targeted data type.
DataValue	This field contains the "raw", e. g. untreated and unformatted, input data. This field has been added as a safeguard against display tools that interpret and manipulate the data based on guessing its actual data type. As an example, many different notations for a date are used within Europe and tools such as Excel are reformatting those terms according to the local configuration. This may disqualify data for further assessment, especially in cases where a raw date "03/01/1980" is read as "1 st of March 1980" in some countries but as "3 ^d of January 1980" in others.
ValueDisplay	This field contains a formatted display of the raw data.

Table 2: CDA Extraction Presentation

Figure 2 contains a data presentation of the eADC as anticipated for the Evaluation.

	A	B	C	D	E
1	Data Type	DataTypeName	DataValue	ValueDisplay	
2					
3	<code>cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:addr/cda:country</code>	Patients Country	CZ	CZ	
4	<code>cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:patient/cda:birthTime</code>	Patients Birthdate	19810101	01.01.1981	
5	<code>cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:addr/cda:country</code>	Patients Country	CZ	CZ	
6	<code>cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:patient/cda:birthTime</code>	Patients Birthdate	20010201	01.02.2001	
7	<code>cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:addr/cda:country</code>	Patients Country	AT	AT	
8	<code>cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:patient/cda:birthTime</code>	Patients Birthdate	19860331	31.03.1986	
9	<code>cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:addr/cda:country</code>	Patients Country	AT	AT	
10	<code>cda:ClinicalDocument/cda:recordTarget/cda:patientRole/cda:patient/cda:birthTime</code>	Patients Birthdate	19860331	31.03.1986	

Figure 2: Exemplary view of the extracted data