Public version

Date
2018-01-22

Version
5.0

Author
Henrik Bengtsson
Robert Mohri
Jens Nordenberg
Jonas Nyfeldt
Anders Öhman
Martin Grubb

SDC Technical Communication Guidelines for VIOL 2

Table of Contents

1 Document Version History

A change to the version history requires an update of date and version in the page header.

The numbering format is Revision.Version, where Revision is an official document release and Version exceeding 0 is an internal work document. Please note that only if the document version has suffix 0 it is an official SDC version, e.g. 1.0, 2.0, 3.0, but NEITHER 0.1, 1.2 nor 1.10. The version suffix is initialized for each new revision level.

Version	Date	Description	Signature
5.0	18-01-22	VIOL 2 only disclaimer added. Waterstamp added Title modified Section 2.0 paragraph 1 modified	RoMo
4.0	17-08-31	Added reference to sftp with papiNet payload considerations in section 4.1 Added WMQ retention time section in 4.3 Added section 5.2.6 sftp using papiNet payload Added secion 4.1.1 Segmentation	MaGr RoMo
3.0	16-08-24	Reworked section 5.1.1 Character Encoding, removed binary transfer of XML over MQ messages as an option Updated section 5.2 Added section 5.2.2 Character Encoding Added section 5.2.4 Business Acknowledgement Added section 5.2.6 Miscellaneous Updated section 5.2.5 with the ID element Added reference [14] w3c UTF-8 Encoding specification	RoMo
2.0	16-05-23	Updated Table 1 Promoted network access/protocol combinations, section 4.1 FTP and SFTP, section 4.3 WMQ, section 5.1.3 Validation of Business Content, section 5.2.1 Global Party Identifiers and added section 5.3 StanForD2010	HeBe AnOh JeNo
1.0	14-06-11	Initial public version	JeNo

2 Introduction

This document describes general guidelines for the technical communication aspects of integration between SDC's customers (*consumer parties*, or just *consumers*) and SDC (*provider party*, or just *provider*), hereinafter collectively referred to as the *parties* for **VIOL 2.** A new guideline document will be authored for VIOL 3.

The terminology used in this document is described in more detail in reference [1] (all references are listed in chapter 6). Terms in Swedish are used as a complement to terms in English if it helps to explain an unfamiliar term in English. The Swedish terms are in these cases put within parentheses directly after the corresponding English term.

Available communication options provided by SDC are described at three levels, treated in more detail in the rest of this document:

- **Network Access**: Options on how to connect to SDC on the network level, for example VPN Partner Access.
- **Protocols**: Options on how to transfer data over the network, for example WMQ or SFTP.
- **Formats**: Options on formats used to interpret data transferred over a protocol, for example FUG_00NQ or papiNet DeliveryMessage.

To exchange information with SDC, a customer must pick a supported combination of communication options, at least one from each level. The combinations supported by SDC will vary depending on which integration service the customer is interested in consuming. For example, the integrations service FU (Följdrutinutgång) supports the following combinations (Network Access / Protocol / Format):

- VPN Partner Access / WMQ / FUG_00NQ
- VPN Partner Access / FTP / FUG_00NQ
- Web Access / FTP / FUG_00NQ[1]

[1] This combination is still supported but no longer promoted by SDC.

3 Network Access

This chapter describes current network access options when integrating with SDC.

SDC promotes two network access options to consume integration services: VPN Partner Access and Public Internet Access. These two options are described in more detail in the following two sections.

3.1 VPN Partner Access

The VPN partner access option is suitable for customers that exchange information with SDC on a continuous or frequent basis, typically using WMQ or FTP at the protocol level.

VPN partner access is ordered per customer via SDC's help desk. When ordering, please provide contact information to a technical contact person so that SDC can initiate a dialogue to establish the VPN tunnel.

When a VPN tunnel is established, all of the customers' users can consume both integration services and interactive services at SDC via the same VPN tunnel.

3.2 Public Internet Access

The public internet access option is always available to all customers for selected integration services, like external submitting of measurements from industries (extern insändning), using SFTP at the protocol level. Another example of an integration service provided over the public internet is external submitting of production data from harvesters and forwarders.

To be authorized to use an integration service over the public internet, the customer needs to be authenticated on the protocol level. A customer interested in an integration service provided via the public internet can contact SDC's help desk. When ordering, please provide contact information to a technical contact person so that SDC can initiate a dialogue to establish protocol access.

3.3 Other Network Access Options

SDC still supports three other network access options that are no longer promoted to consume integration services: DataNet, Modem and Web Access.

Please note that the web access option is still promoted to allow user client access to interactive services like VIOL.

4 Protocols

On top of the network access options described in chapter 3 a protocol is needed to transfer data between the involved parties.

The following network access/protocol combinations are currently promoted by SDC:

Protocol Options	Network Access Options	
	VPN Partner Access	Public Internet Access
FTP	Yes	No[2]
SFTP	No	Yes
HTTP	Yes	No
HTTPS	No	Yes
WMQ	Yes	No

Table 1: Promoted network access/protocol combinations

4.1 FTP and SFTP

If you are using papiNet as payload then please read section 5.2.6. The text belov applies to all other types of integration.

FTP and SFTP are two different file transfer protocols that allow customers to exchange files with SDC. The most important difference between the two is that SFTP secures the communication channel while FTP does not. This also explains why FTP is promoted over VPN Partner Access (that provides a secure communication channel) while SFTP is promoted over the public internet (that does not provide a secure communication channel) as described in Table 1.

A wide selection of FTP and SFTP clients, both free and commercial, are available making FTP/SFTP suitable options for small customers, see for example reference [2] and [3]. Large customers may also use FTP/SFTP, although WMQ, HTTP or HTTPS is recommended when supported by the integration service the customer is interested in consuming.

4.1.1 File name rules

SDC expects that file names have character encoding ISO-8859-1. The character encoding of textual file content is determined by some content internal mechanism, for example by an XML prolog as described in section 5.1.1.

Valid characters in file names sent to SDC are a-z, A-Z, 0-9, _ and -.

Two file name suffixes have, unless otherwise stated, special meaning at SDC: .gz and .ok.

A file name suffix of .gz means that the file is compressed using GZIP [4].

[2] FTP over public internet is not *promoted* by SDC although currently supported, for example when supporting SDC's application Sender that submits production data from harvesters and forwarders. The successor of Sender, Sender XC, uses SFTP instead of FTP.

A file name suffix of .ok means that a corresponding file without the .ok suffix is ready to be processed. A sending system should transfer a (typically empty) .ok file after sending a file. A receiving system should not process a file without a corresponding .ok file, as that might result in processing a partially written file. This does not apply when parties are sending production instructions to forest machines, in that case no .ok file needs to be sent in to start the transmission.

The two file name suffixes can be combined. For example, sending a file named x.gz followed by an (empty) file named x.gz.ok will allow the receiving system to process the compressed file x.gz when it is completely written.

4.2 HTTP and HTTPS

HTTP and the secure alternative HTTPS is a protocol allowing customers to exchange data with SDC using web services (REST or SOAP).

To be able to use these services the calling party needs to have a client key and a client secret that will be provided upon request.

4.3 WMQ

IBM® WebSphere® MQ (WMQ) is a product from IBM providing a proprietary messaging protocol to exchange messages via queues. WMQ has, over time, proven itself as a reliable and robust messaging channel with high availability. WMQ has a long tradition as the preferred integration protocol between SDC and large customers.

Customers have two options when using WMQ to integrate with SDC:

1. Use client connections to the SDC queue manager. Installing and using a WMQ client is free of charge. Using this option, messages are stored in queues at SDC and the customer is responsible for establishing a connection and retrieving messages.

2. Use server connections to the SDC queue manager. To use this option the customer must have its own queue manager. Installing and using a queue manager requires that a license is purchased. Using this option, messages are directly forwarded and stored in queues at the customer. Message forwarding is automatically reestablished after any queue manager downtime on either side.

   This is the preferred option if the customer has decided to invest in WMQ.

WMQ is best suited when transferring messages up to a size of a few megabytes. The maximum message size that SDC supports is 100 Mb, but some services might have other maximum message sizes. Streaming protocols like FTP, SFTP, HTTP or HTTPS are generally more appropriate for larger data transfers.

WMQ message retention time
SDC expects that integratiating parties continuously reads and empties their WMQ queues from messages. SDC will remove messages older than 14 days from outbound queues. Please

contact SDC if you have a situation that inhibits you from reading messages within the 14 day retention interval.

4.3.1 WMQ Headers

Message Segementation
SDC uses Webshere MQ:s option to segment large messages to multiple smaller messages during transition between queue managers. This is achieved by setting the MQ version 2 Header flag MQMF_SEGMENTATION_ALLOWED, this flag is set on all outgoing messages. For incoming messages this flag is not mandatory to be set. It can be used if the need occurs.

Se also section 5.1.1 regarding character encoding settings in WMQ header

5 Formats

This chapter describes general XML, StanForD2010 and papiNet interoperability guidelines when integrating with SDC. Over time this chapter is expected to also cover other major formats and standards for integrations with SDC.

5.1 XML

The XML standard [5] defines a general markup language that can be used in to exchange data in many communication scenarios. It is common that document standards are based on XML, using XML schemas to define formats to communicate documents with different purposes. Examples of such document standards are papiNet [7] and StanForD 2010 [10].

5.1.1 Character Encoding

It is important to get the character encoding right, otherwise data corruption might occur.

SDC currently supports the character encodings UTF-8 and ISO-8859-1 in XML documents depending on XML document standard and underlying system standards.

The recommended character encoding by W3C is UTF-8 [14]. SDC will henceforth only support UTF-8 for XML document exchange. If no character encoding is explicitly given, UTF-8 is assumed (see appendix F.1 in [5]).

UTF-8 introduces a slight overhead in file and message size compared to ISO-8859-1 when using Nordic characters but the interoperability aspect of UTF-8 outweighs that disadvantage.

An XML document's character encoding can, as described in appendix F in [5], be expressed in three ways:

- Externally, for example
  - Websphere MQ:s MQMD CodedCharSetId field.
  - HTTP:s header Content-Type property
- Internally by means of a Byte Order Mark (BOM).
- Internally by means of an XML prolog with an encoding declaration.

The following example describes how character encoding works:

```
<?xml version="1.0" encoding="UTF-8"?>
<A>ääö</A>

<?xml version="1.0" encoding="ISO-8859-1"?>
<A>ääö</A>
```

The binary representation (in hexadecimal) of the second row in the examples messages are:

```
UTF8:       3c 41 3e c3 a5 c3 a4 c3 b6 3c 2f 41 3e
ISO-8859-1: 3c 41 3e e5 e4 f6 3c 2f 41 3e
```

Note that the Swedish characters (å,ä and ö) are represented by two bytes in UTF-8.

XML message encoding in WMQ

When handling XML data in WMQ messages, SDC has decided to handle XML documents as character data (string). The encoding of the document must be stated in XML-prolog and WMQ header. No BOM is used when encoding XML documents with UTF-8

The following WMQ headers are expected to be set:

Header name	**Value**
MQMD Format	MQFMT_STRING
MQMD CodedCharSetId (CCSID or Code Page)	see code page value in table below
MQMD Encoding	MQENC_NATIVE

The CodedCharSetId values for the SDC supported character encodings:

Character Encoding Name (as defined in [6])	**WMQ CodedCharSetId** (IBM Code Page)
UTF-8	1208
ISO-8859-1	819

It is very important that the external and internal encoding definitions are accurate and reflect the contents of the XML message. I.e. the definitions in the XML prolog and the CSSID in the WMQ MQMD header must match each other and the actual encoding of the XML document.

An example of what happens when external and internal character encoding definitions mismatch follows. Consider a XML document written (we use the example document snippet from above) to a WMQ message using the UTF-8 character encoding according to its XML prolog but with the MQMD CodedCharSetID field of the WMQ messages set to 819. A consumer decoding the document from WMQ using the stated encoding of ISO-8859-1 would see the following, corrupted document. The corruption occurs when the six byte representation of the three characters “åäö” in UTF-8 is interpreted as six separate characters in ISO-8859-1:

```
<?xml version="1.0" encoding="UTF-8"?>
<A>Ã¥Ã¤Ã¶</A>
```

5.1.2 Schema Validation

All XML documents exchanged with SDC are required to be valid according to the documents’ XML schema.

A receiving party has, if not otherwise agreed, no obligation to process an invalid XML document. SDC will ignore invalid XML documents.

5.1.3 Validation of Business Content

The sender must verify the business content before issuing an e-document. It must not be assumed that a receiver validates business content. SDC will not validate all business content.

For example, the sender must before issuing a DeliveryMessage check that a referenced order is valid to be measured at place of measuring and PartyIdentifiers are correct.

5.1.4 Compatibility

Two XML documents are considered compatible when all documents that are valid according to XML schema version 1 are also valid according to XML schema version 2.

When exchanging XML documents with SDC, the parties must accept that the sending party at any time and without notice can choose to send any XML documents that are compatible with the XML schema version that originally was agreed by the parties. In practice this means that the receiving party must ignore unknown elements and attributes in XML documents.

5.2 papiNet®

As the papiNet standard is based on XML, all general interoperability guidelines specified in section 5.1 applies to all papiNet formats. Below are specific guidelines for exchanging papiNet documents with SDC.

5.2.1 Encoding

All exchange of papiNet documents with SDC will be encoded using UTF-8.

5.2.2 Global Party Identifier

When sending papiNet documents to SDC, the PartyIdentifier of the TransmissionReceiver and BusinessReceiver elements in the papiNet Envelope must be set to SDC's papiNetGlobalPartyIdentifier which is 1.3.6.1.4.1.29504. When SDC sends papiNet documents, the PartyIdentifier of the TransmissionSender and BusinessSender elements in the papiNet Envelope are set to 1.3.6.1.4.1.29504.

The papiNetGlobalPartyIdentifier pattern is 1.3.6.1.4.1.[private enterprise number].[enterprise location number]. A private enterprise number (PEN) for your organization can be obtained for free from IANA [9]. An example of an complete papiNetGlobalPartyIdentifier used by SDC is 1.3.6.1.4.1.29504.999.1, where 29504 is the PEN of SDC and 999.1 is an enterprise location number maintained by SDC used for tests.

5.2.3 Transaction History Number

Most papiNet document headers have an optional TransactionHistoryNumber element that indicates the order of the document being sent. When exchanging papiNet documents with SDC, TransactionHistoryNumber is **mandatory** except for the Business Acknowledgement document. If the sender fails to set the TransactionHistoryNumber of the document, the document will not be processed by SDC. When SDC sends out papiNet documents TransactionHistoryNumber will always be given.

Note that a non-contiguous number sequence is allowed (e.g. 1, 2, 3, 7, 12, …) as long as a newer version of a document always has a higher TransactionHistoryNumber than all previous editions of the same document. TransactionHistoryNumber sequences always starts with the number one or higher.

The TransactionHistoryNumber must be taken into account for situations where documents arrive out-of-order. The document with the highest TransactionHistoryNumber is used as the current. Documents with lower or equal TransactionHistoryNumber than the current document are discarded without any processing. An example of how a receiver should act in different situations is described in the following table:

Time	Document number	Transaction History Number	Document Status	Action taken by receiving part
1	123456	1	Original	Handle document
2	123456	2	Replaced	Handle document
3	987654	1	Original	Handle document
4	123456	5	Cancel	Handle document
5	987654	1	Replaced	Discard document
6	123456	3	Replaced	Discard document
7	987654	8	Replaced	Handle document

5.2.4 Business Acknowledgement

The papiNet document Business Acknowledgement is used to notify the sender of how a specific message (containing a papiNet document) was processed. The papiNet standard states the usage of Business Acknowledgement to be optional although strongly recommended. SDC:s papiNet document exchange uses the Business Acknowledgement for all papiNet documents, i.e. all transmissions must be acknowledged

In addition to be prepared for receiving Business Acknowledgement, the sender of the original message should have in place an error resolution process. This process should monitor errors received via the Business Acknowledgement, routing them to the correct organization for resolution. The monitoring process may also check for unacknowledged messages to increase the verification that all sent messages have been processed.

TransactionHistoryNumber is not used in the Business Acknowledgement document though the specification contains an optional TransactionHistoryNumber element. Consequently, Business Acknowledgements must not be resent or replaced.

The Business Acknowledgement's *Document* element is used to identify which document is acknowledged. The optional TransactionHistoryNumber element of the Document element is set for acknowledge of all papiNet documents with the exception of Shipment Status, which does not contain transaction history information.

Note that invalid papiNet documents may not be acknowledged by SDC. Validity is referred to that the message is parsable XML and it is valid according to its XML schema, see section 5.1.2

5.2.5 Envelope

When integrating with SDC a papiNet envelope is required. The actual format carrying the business information, e.g. a DeliveryMessage or ShipmentStatus, is wrapped in the

BusinessDocument element of the envelope. The papiNet envelope documentation includes a complete sample XML document with envelope.

The syntax and semantics of the papiNet envelope is fully described in [8]. However, a few important attributes and elements of the envelope are pointed out here:

- **DocumentNumber element:** The value of this element shall correspond to the document number in the header of the payload document.

- **DocumentHistoryNumber element:** This element, although optional according to the papiNet envelope XML schema, is mandatory when integrating with SDC. The value of this element should be equal to the value of the TransactionHistoryNumber element in the header of the payload document.

- **TestFlag attribute of the PayloadInfo element**: If "true" or "1" then this is a test transmission. If "false" or "0" then this transmission is for production use.

  This means that SDC will not use the information in production systems when receiving a document in a papiNet envelope with the TestFlag set to "true" or "1". Likewise, SDC expects the same behavior from the receiver when sending a document in a papiNet envelope with the TestFlag set to "true" or "1".

- **PartyIdentifier element**: When integrating with SDC the PartyIdentifier elements of the TransmissionSender, TransmissionReceiver, BusinessSender and BusinessReceiver shall have PartyIdentifierType "papiNetGlobalPartyIdentifier". How to obtain a papiNetGlobalPartyIdentifier is described in section 5.2.2.

- **ID element of the TransmissionInfo element:** The identity must be unique for the TransmissionSender and not reused. The ID used must not be reused regardless if it has been used with a TestFlag set to true or not. XPath to ID element: papiNetEnvelope/PayloadInfo/TransmissionInfo/ID.

5.2.6 SFTP file transfer using papiNet

When exchanging papiNet-documents using SFTP-protocol, SDC expect that the systems integrator honor the following guidelines:

Directories
When exchanging papiNet-documents with SDC, there are two main directories used;
- ./inbox is used when uploading documents **to** SDC
- ./utbox is used when downloading documents **from** SDC

./inbox and utbox has subdirectories for each type of papiNet document that the parties have agreed to exchange. The directory to use for each papiNet-integration will be presented in the integration contract.

File names
SDC expects the following naming convention to be used when exchanging papiNet-documents: d**ocumentname_[documenttype_]id.xml**

Document type is optional depending on the fact that some papiNet documents does not include documenttype. In that case document type should be omitted.

Document name, type and id can be found as values in any papiNet envelope. Use the following Xpaths to retreive the values

Attribute	Xpath
documentname	papiNetEnvelope/PayloadInfo/Document/@DocumentName
documenttype	papiNetEnvelope/PayloadInfo/Document/@DocumentType
id	papiNetEnvelope/PayloadInfo/TransmissionInfo/ID

The file extension is .xml since papiNet is XML based.
Filenames are stated in lower case

Examples:
measuringticket_measuringticket_234556-sdc-se.xml
measuringticket_455675-sdc-se.xml
loadtender_booking_456761-sdc-se.xml

When exchanging papiNet-documents, .OK-files are not used as described in section 4.1.

File retention time inbound (to SDC)
SDC removes papiNet-document files from the filestores inbox as soon as a successful reception from the sending party has occurred.

File retention time outbound (from SDC)
SDC expects that integrating parties polls the integration directories at least once a day. When downloading papiNet-documents from SDC. SDC expect parties to remove files from filestores utbox when a successful download has occurred.
SDC will remove files older than 14 days from the outbox directory.

5.2.7 Miscellaneous

Time information in a papiNet documents handled by SDC:s system VIOL 2 will have temporal resolution in seconds. Fractions of seconds in papiNet document sent to SDC will be discarded even though the XML time type allows fractions of seconds. For example: a time element <Time>09:30:47.2189+05:00</Time> (hh:mm:ss.ssss) will be truncated/interpreted and stored in VIOL 2 as 09:30:47 (hh:mm:ss)

Do not resend documents. If you have sent a papiNet document to SDC and you have not received the corresponding Business Acknowledgement do not resend the document. Contact SDC's help desk to resolve the issue.

5.3 StanForD2010

As the StanForD2010 standard is based on XML, all general interoperability guidelines specified in section 5.1 applies to all StanForD2010 formats.

5.3.1 Rules for production and quality reports to SDC

When sending production and quality reports to SDC all reports need to follow the rules defined for the specified report, Harvested production [11], Forwarded production [12] and Quality control [13].

5.3.2 Rules for communication with forest machines through SDC

When communicating with forest machines through SDC the following rules apply.

The sender may send all type of data to forest machines as long as the information is according to the StanForD2010 standard and one of the following conditions is met.

1. Addressed StanForD2010Envelope
    - The information is sent in a correct StanForD2010Envelope.
    - BusinessSender object needs to be specified describing the sender party for acknowledgement of the delivery
        i. If BusinessId is given this will be used for placing an acknowledgement file on the SFTP server, BusinessID shall be a valid SDCID (sdcgpx####) for the party
        ii. If email address is given this will be used for sending an acknowledgement of the distribution
    - One or more TransmissionInfo objects needs to be specified and identify a receiving forest machine. Each TransmissionInfo shall have TransmissionReceiver set and contain a valid SDCID (sdcgpx####) for the receiving forest machine
    - All attachment shall be placed inside the StanForD2010Envelope as EmbeddedDocument or EmbeddedAttachment
    - Binary attachment shall be Base64 encoded
2. Unaddressed StanForD2010Envelope
    - The information is sent in a correct StanForD2010Envelope.
    - BusinessSender object needs to be specified describing the sender party for acknowledgement of the delivery
        i. If BusinessID is given this will be used for placing an acknowledgement file on the SFTP server, BusinessID shall be a valid SDCID (sdcgpx####) for the party

ii. If email address is given this will be used for sending an acknowledgement of the distribution

- All attachment shall be placed inside the StanForD2010Envelope as EmbeddedDocument or EmbeddedAttachment

- Binary attachment shall be Base64 encoded

- The StanForD2010Envelope needs to contain at least one StanForD2010Message with messageCategory="pin". All EmbeddedDocument´s and EmbeddedAttachment´s will be routed to forest machines that has been working on the ProductUserId that is part of the embedded pin within the last two month.

3. Product Instruction (pin-file) (Only valid through SFTP)
   - The information is sent in a correct StanForD2010 pin file.

   - The pin file will be routed to forest machines that has been working on the ProductUserId that is part of the pin within the last two month.
   - An acknowledgement file will be placed on the SFTP server for the sending party

6 References

References:

1. Integration Terminology

2. Examples of FTP Client Software
   http://en.wikipedia.org/wiki/Comparison_of_FTP_client_software

3. Examples of SFTP Client Software:
   http://en.wikipedia.org/wiki/Category:SFTP_clients

4. GZIP file format specification
   http://www.ietf.org/rfc/rfc1952.txt

5. EXtensible Markup Language (XML) 1.0
   http://www.w3.org/TR/REC-xml/

6. IANA Character Sets
   http://www.iana.org/assignments/character-sets/character-sets.xhtml

7. papiNet
   http://www.papinet.org/

8. papiNet Envelope
   http://www.papinet.org/ → The Standard → Download Current Version →Envelope

9. IANA Private Enterprise Number – Application Form:
   http://pen.iana.org/pen/PenApplication.page

10. StanForD 2010
    http://www.skogforsk.se/en/About-skogforsk/Collaboration-groups/StanForD/StanForD-2010/

11. SDC rules for interpreting StanForD2010 harvester production data
    http://www.skogforsk.se/contentassets/1a68cdce4af1462ead048b7a5ef1cc06/sdc-regler-vid-tolkning-av-hpr_2015_12_29.pdf

12. SDC rules for interpreting StanForD2010 forwarder data
    http://www.skogforsk.se/contentassets/1a68cdce4af1462ead048b7a5ef1cc06/sdc-regler-vid-tolkning-av-fpr_2015_12_29.pdf

13. SDC rules for interpreting StanForD2010 harvesting quality control data
    http://www.skogforsk.se/contentassets/1a68cdce4af1462ead048b7a5ef1cc06/sdc-regler-vid-tolkning-av-hqc_2015_12_29.pdf

14. World Wide Web Consortium UTF-8 encoding specification
    http://www.w3.org/TR/encoding/

7 Legal Notice