Velonetic™

Powered by DXC Technology | IUA | Lloyd's

Write Back Functional Specification

Part E: The DRI Repository Download Service

Version: 2.0

Issue Date: 26 November 2015

Part G: CONTENTS

1 DRI: Repository Upload message interactions 4

1.1 Service Overview 4

1.2 Validation of Associated Data 4

1.3 Identification of Parties 4

1.4 Document Responses 5

1.5 Access Control List 5

1.6 Associate Document with Slip or Claim File 6

1.7 Creation and Update of UMR and UCR containers 6

1.8 Notification Lists 7

1.8.1 Summary 7

1.8.2 Detailed processing rules 7

1.8.3 Error handling 7

1.9 Document Metadata 8

1.10 Identification of Documents 9

1.11 Message Data Definition 11

1.11.1 Upload Request Message 11

1.11.2 Upload Response Message 11

1.12 Operational Behaviours 12

1.12.1 SOAP Faults and Post Rs Validation 13

1.12.2 DRI Repository Message Validation 14

1.12.3 Timeout & Retry 15

1.12.4 Message Persistence 15

1.13 DRI: Repository Upload Non-Functional Requirements 15

1.13.1 Security 15

1.13.2 Service Availability 15

1.13.3 Service Response Times 16

1.13.4 Performance and Maximum Load 16

1.13.5 Service Support and Maintenance 16

1.13.6 Invoking the Service 16
2 Document Control 18
2.1 Document Information 18
2.2 Revision History 18
2.3 PARCI 18

Part G: APPENDICES

Appendix G1: Validation 22
Appendix G2: ACL Approach for DRI Upload for Carriers 24

1 DRI: REPOSITORY UPLOAD MESSAGE INTERACTIONS

This section describes the interface which will be offered by central systems for a DRI Repository Upload service. This covers the data required to call the service together with the data returned in the response message.

1.1 Service Overview

Central systems will expose a service that will allow Carriers to individually upload a claim document to a specific claim folder (only if they are a participant on the claim) on the IMR. Carriers will be able to specify the access control list for organisations that can access the document once uploaded on the IMR.

All documents submitted via the Document Upload service must be associated with a UMR or UMR and UCR. When a message is received with a UMR alone (without a UCR) the document will be placed in the UMR container of the IMR. When a UMR and UCR are provided, the document will be placed in the claim related documents container in the IMR. The Sender will always be stored with the document.

The sender will generate an Upload Rq message containing document(s) and the data that references and describes each document.

Central systems will receive, validate and if the incoming message is found to be valid, process the upload request message. On completion of processing, an upload response message will be returned to the Carrier to confirm successful process completion.

1.2 Validation of Associated Data

The data associated with a document will be validated to ensure that all required data fields are populated and then that the populated data is appropriate in relation to a set of pre-defined rules. There will also be validation to ensure that all documents are referenced allowing them to be associated with a UMR or UMR and UCR.

1.3 Identification of Parties

Many of the elements within the DRI message and associated metadata include party ID. Many of these may validly include parties who are not identified by the Lloyd's, Institute of London

Underwriters or London Insurance and Reinsurance Market Association code lists. The agency responsible for the code set from which each party's code is taken must be identified by a valid value from the ACORD Responsible Agency code list (3055).

Only Lloyd's, Institute of London Underwriters or London Insurance and Reinsurance Market Association codes can be used in the DRI message sender or receiver Party Aggregates.

For codes identified by any other parties, for example within the referred objects aggregate, the Party Id will not be validated or used to give access to documents in the repository, but they will be stored and passed on in any outbound messages.

Note: Xchanging allow the DUNS code of the message sender to be quoted in the SOAP message.

A completed Party Aggregate example is shown below.

- Lloyd's example

```
<Party>
    <PartyId>urn:lloyds:5555</PartyId>
    <PartyRole>Insurer</PartyRole>
    <PartyName>InsurerName</PartyName>
</Party>
```

The ACORD DRI messaging framework will be adopted, including message management, message construct and data definitions.

1.4 Document Responses

Following successful validation the document is stored in the repository and an Upload Rs is sent to the sender confirming receipt of the document. The asynchronous response is not sent out until the document has been loaded to the IMR. If validation fails, an error response will be sent to the sender.

1.5 Access Control List

The UMR and UCR provided in the DRI message will be used to allocate documents to UMR or UCR containers. The market associated with the UMR or UCR in premium or claim systems will provide the default access list to containers and documents. Users with change rights may change the default access list for claims and individual documents (e.g. where a conflict of interest applies).

In addition, Access Control Lists can be provided within the DRI *RepositoryUpload* request to govern access to documents. Only London Market Broker and Carrier codes may be

included in the access lists (please refer to Appendix G2 “ACL Approach for DRI Upload for Carriers” for more detail on the ACL scenarios). XIS and/or XCS will also be given access as service provider or claims agreement party, in which case, the DUNS code (for XIS) is allowed.

1.6 Associate Document with Slip or Claim File

If a document is received with a business reference (UMR or UMR and UCR) that is already held in the repository, the document will be stored in the related container. If the UMR alone is supplied, the document will be stored in the UMR related container. When a UMR and UCR are supplied, the document will be stored in the claim related container. If a UMR, UCR and TR are supplied with the document, the document will be stored in the claim related container and will be automatically associated with the TR. If a TR is received with a UMR alone, it will not be stored with the document.

1.7 Creation and Update of UMR and UCR containers

When the first document quoting the UMR is received, the UMR repository container will be created. Subsequent documents quoting the same UMR will be loaded into the existing container.

UCR documents are always expected to be associated with a CLASS claim and may optionally be associated with a specific transaction.

When a UCR-related document is passed to the repository and there is no matching UMR or UCR container in the repository, a container will be created for the UCR and, if necessary the UMR. Claim documents will be stored within the repository awaiting structured data (from CLASS) to associate the document with. When a subsequent CLASS claim message is received (within 24 hours or subsequently) any documents with a matching UCR reference will be made available in the UCR container.

If a claim document is passed to the repository with a UMR, UCR and TR and a CLASS message with the TR has not been received, the TR will be added to the UCR container in the repository and the document associated with it. Documents received subsequently that quote the same UCR and TR will be placed in the UCR container and associated with the TR.

1.8 Notification Lists

1.8.1 Summary

A Notification list may be received from another repository in an Upload Rq message. An Upload Rq or Notify Rq will be generated for each party in the Notification list that is registered with Xchanging to receive messages. Only London Market Broker and Carrier codes may be included in notification lists.

There is no check that the Parties identified in the Notification List are included in the access list for that document in the repository or in the same inbound message.

A Party that has been notified of a document in a Notify Rq may send a Download Rq to retrieve the document.

1.8.2 Detailed processing rules

A Notification list may be sent for each document in a message.

The Notification list in an inbound message will be processed before the document is loaded to the repository.

If a receiving Party listed in a Notification List uses Upload to receive documents an Upload Rq message will be transmitted containing the document. If the receiving Party uses Notify and Download to receive documents the Notify Rq will be transmitted which may be followed, if the organisation wishes, by a Download Rq for the document.

If the document cannot be loaded to the repository (e.g. having failed validation) or the Party subsequently requesting Download is not in the Access Control List for the document, the Download Rs will include an Error response and the document will not be downloaded.

Any information contained in the inward message, including an ACL, will be included in the outward message. The Access List associated with the document in the market repository will not be included in the outward message.

1.8.3 Error handling

XAG will ensure that the message conforms to the ACORD DRI standard and return any errors in a response with an error indicator.

If one or more of the Parties on the list does not have a registration on XAG the message will not be rejected but outward messages will not be sent to those parties. Therefore, there are

no error conditions associated with the notification list after the ACORD schema validation has been passed.

1.9 Document Metadata

Additional data relating to the document may be sent in the Referred Objects Elements of the DRI Upload Rq. The full list of additional metadata elements to be displayed, edited, or searched on in the IMR is shown below. Any other metadata received with a document will also be stored and included on any outgoing message containing that document.

The following elements of the Referred Objects have specific purpose for DRI messages sent to the Market Repository:

- <*Contract*> <*BrokerReference*> must contain the Unique Market Reference (UMR). This is mandatory for all documents.
- • <*Claim*> <*BrokerReference*> must contain the Unique Claim Reference (UCR). This is mandatory for all claims documents.
- • <*ClaimEntry*> <*BrokerReference*> must contain the Transaction Reference (TR). This is optional.

The UMR, UCR and TR must each have a minimum length of 6 characters and a maximum length of 17 characters.

The first character must be 'B' and characters 2 – 5 must be a valid Lloyd's broker number.

Characters 6-17 are alphanumeric and must not include embedded spaces.

The following elements of the Referred Objects will be stored in the Market Repository as indexed data and will be available for use as search criteria with a DRI Search Request.

Referred Objects Data Elements
Insurer Party (Id or Name)
Broker Party (Id or Name)
Cedent (Id or Name)
Reinsurer (Id or Name)
Insured (Id or Name)
Unique Market Reference (Broker Contract Reference)

Referred Objects Data Elements
Cedent Contract Reference
Reinsurer Contract Reference
Insurer Contract Reference
Insured Contract Reference
Contract Period Start Date
Contract Period End Date
Year of Account (Underwriting Year)
Class of Business (JV Class of Business)
Unique Claim Reference (Broker Claim Reference)
Transaction Reference (Broker Claim Entry Reference)

1.10 Identification of Documents

Extract from the ACORD DRI Reference Guide v 1.2.0:

"A document is uniquely identified with one of two exclusive methods:

1) A globally unique <*DocumentId*>; or

2) An Owner's repository reference <*DocumentReference*>, optionally augmented by a document version number <*DocumentVersion*>.

When <*DocumentVersion*> is provided in addition to <*DocumentReference*>, it is considered part of the unique identifier. It will be used consistently for referencing this document. Note that <*DocumentVersion*> can be given with <*DocumentId*> as well, but then it is not part of the unique identifier."

The <*DocumentId*> provided for the document received in a DRI message will be stored in the repository alongside any internal identifier for that document. It will be supplied in the outgoing Search response in the relevant Document identifier data elements.

Central Systems Additional Document Identifiers

The current implementation of the IMR has meant that the standard ACORD Document Identifiers are not sufficient to uniquely identify a document on the repository. To facilitate document download, Xchanging introduced an additional Token ID element rlc:ServiceProviderContactDescription to outbound document information.

The data elements which enable unique identification of documents in the request message are shown below:

```
<DocumentItem>
    <Document>
        <DocumentID>SomeDocumentID</DocumentID>
        <DocumentReference>SomeDocReference</DocumentReference>
        <DocumentVersion>01</DocumentVersion>
    </Document>
</DocumentItem>
```

1.11 Message Data Definition

1.11.1 Upload Request Message

Please refer to the Data Dictionary embedded in the ECF –WriteBack – DRI Services – Interface Specification for the Upload Request Message structure, multiplicity and business usage.

1.11.2 Upload Response Message

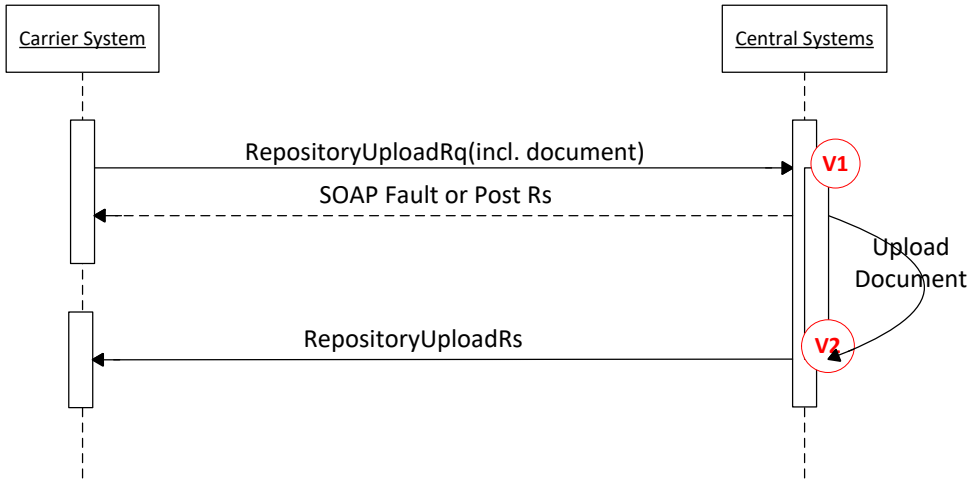
Please refer to the Data Dictionary embedded in the ECF –WriteBack – DRI Services – Interface Specification for the Upload Response Message structure, multiplicity and business usage.

1.12 Operational Behaviours

The service will exhibit the following operational behaviors:

- Request Successful
- Request Failed – SOAP failure or Negative Post Rs
- Request Failed – DRI Repository Upload Rejected

The diagram below illustrates the DRI Repository Upload main success path. Note: the diagram does not show the HTTP handshake.



- The Carrier User submits an Upload Request to Central Systems with a document attached and associated document metadata for the Central System to upload to the central repository (IMR).

  Validations

  (V1) Initial Checks

- The gateway receives the request and performs SOAP level validation at point V1 on the diagram before sending a synchronous response back to the Carrier System. The SOAP validation performed will be in line with the current DRI implementation. The validation is included in Appendix G1 below.

  SOAP Failure or Negative Post Rs

  If the Upload Request fails SOAP level validation at the gateway, the Carrier will receive a synchronous SOAP failure response / negative Post Rs notifying them of the failure and the process will terminate here.

  Positive Post Rs

If the Upload Request passes SOAP level validation at the gateway, the Carrier will receive a synchronous positive Post Rs response notifying them of the success and the request will continue to be processed. The gateway will then pass on the message to the Central System (IMR) in an asynchronous manner to apply business level validation at point V2 on the diagram above and explained below.

(V2): Business Message Checks

The business level validation carried out by the system at this point is specified in Appendix G1 below.

DRI Message Validation: Rejected

- If the business level validation on the message fails, then the Upload Response back to the Carrier will have an Acknowledgement Status of 'rejected' and will notify them that the upload of the document to the IMR has been terminated.

DRI Message Validation: Success

- If the business level validation on the message passes, then the Upload Response back to the Carrier will have an Acknowledgement Status of 'acknowledged' and will provide a confirmation receipt (only once the document and metadata is uploaded successfully to the IMR) of its successful upload.

1.12.1 SOAP Faults and Post Rs Validation

Technical errors e.g. SOAP fault handling will be in line with the existing DRI implementation. These will be fully confirmed in the phase two ACORD design phase.

1.12.2 DRI Repository Message Validation

A DRI Repository Upload response must be issued for each valid, accepted DRI Repository Upload request message. Each response message includes a response aggregate which informs the recipient of the processing status of the request message. The response aggregate will indicate that the request has been completed or that the request was not completed (and the reason).

Field Name	Definition
Message ID	The unique ID of the message being responded to.
Acknowledgement level	Code which indicates the level of acknowledgement provided in a response. Only two values from the RLC code table A43 are accepted: - "translation_validation": the response is given at a stage where the message is checked for syntax, unwrapping etc. before being validated according business rules - "application_validation": the response is given after message validation and processing by the application
Acknowledgement status	Code which indicates the status of the acknowledgment given within a response. - "acknowledged" : message successfully processed -- "rejected": message rejected - not processed at all
Error indicator	An error code from the A44 Codelist, identifying the type of error
Error description	Either Error Indicator or Response Description must be present if response status is not “acknowledged”

In the event of a DRI request validation error, the response message will be completed as follows:

Acknowledgement Level: “translation_validation” or ‘application_validation’ whichever is appropriate.

Acknowledgement Status:	will be **set to 'rejected'**
Error Indicator:	Will be set to the appropriate value in the ACORD A44 code set.

1.12.3 Timeout & Retry

It is expected that 98% of requests will have a response within 1 hour as per the SLA below. However any responses not acknowledged within 24 hours should be considered lost. Carriers could consider setting the timeout and retry handling to 24 hours in line with this if they choose to.

1.12.4 Message Persistence

Sent DRI Repository Upload messages will be persisted within central systems and retained for a period of 45 days (existing standard but to be confirmed in full NFS).

1.13 DRI: Repository Upload Non-Functional Requirements

This section sets out our initial understanding of the Non Functional Requirements as they relate to DRI and is based largely on the non-functional requirements established in the existing DRI services. More detailed analysis on the non-functional requirements will be contained in a separate Write Back Non Functional Requirements document. Any findings articulated in the Write Back Non Functional Requirements document will extend and supersede the Non Functional Requirements documented in this section.

1.13.1 Security

The service will only succeed if the Carrier is registered for the XAG service and has the appropriate security certificates and digital certificates in place to handle the encrypted message.

1.13.2 Service Availability

DRI Repository events are triggered by XAG which has a service availability of 24/7 though scheduled and unscheduled downtime may be required from time to time.

1.13.3 Service Response Times

1.13.3.1 Message Transmission from XAG

A synchronous receipt must be issued from Xchanging's ACORD gateway within 1 service minute of receipt of a DRI submission. Recommended practice suggests repeat requests should not be submitted until a synchronous response is received or a timeout threshold is exceeded.

DRI Repository Upload Response messages will be transmitted within a period of 1 core service hour of the Upload Request being received within central systems.

1.13.3.2 Message Response from Carriers System

DRI Repository Upload Response acknowledgment messages will be transmitted by Carrier systems within a period (to be defined in a separate NFR document) of the Upload Response being issued by central systems.

1.13.4 Performance and Maximum Load

1.13.4.1 Message and Document Size

The document upload IMR validation limits any particular document within a message to be no larger than 20MB. Central systems will not impose limits on message size, i.e. the cumulative size of documents within a message can exceed 20MB.

1.13.4.2 Anticipated Volumes

The anticipated volumes are to be defined in a separate NFR document.

1.13.5 Service Support and Maintenance

The XAG gateway is available 24/7, but service support will only be available during core business hours which are 7am-7pm UK time, Monday to Friday excluding public and bank holidays.

1.13.6 Invoking the Service

Xchanging will provide a separate Production URL and outbound Xchanging public security certificates for the DRI Upload Service per Carrier. The Carrier must provide their own inbound public security certificates to Xchanging. The URL will only succeed for those Carrier lines/stamps that have been registered and on-boarded for this service.

From time to time Xchanging will provide separate URLs for lower environments e.g. MAT to carry out testing but the outbound Xchanging public security certificates will be the same across all environments.

2 DOCUMENT CONTROL

2.1 Document Information

Prepared by:	Clarissa Montecillo
Project Manager:	Patrick Bergin
Programme Manager:	John Philips

2.2 Revision History

Version	Date	Author	Description
0.4.1	02/10/2014	Clarissa Montecillo	Initial Draft issued.
0.4.2	14/10/2014	Parminder Kaur	Updated with the review comments received from Paul T and other minor updates.
1.0	14/11/2014	Kajal Bhardwa	Final signed off version
1.1	15/09/2015	Kajal Bhardwa	Updates in line with Write Back (Phase 1) functionality to be implemented in September 2015
2.0	26/11/2015	Sonal Quadros	Incorporated comments received from the market team

2.3 PARCI

The following roles relate to the most recent version of this document as listed in the Revision History above.

PARCI	Project Role	Name	Signature	Date
Producer	Business Analyst	Parminder Kaur		

PARCI	Project Role	Name	Signature	Date
Approver	Business Requestor	Write Back Working Group (London Market Carrier community)		
Reviewer	Project Manager	Pat Bergin		
	Solution Architect	Vikas Acharya		
	Technical Consultant	Nitin Jain		
	Sponsoring Architect	Chris Hendry		
	Principal Architect	Rob Jillings, John Ticehurst		
	System Manager	David Burnett		
	Test Manager	Simon Taylor		
	Offshore Tech Project Mgr	Sonia Thakur		
	Technical Architect	Mark Fillier		
Consulted	Business Architect	Victoria Jandrell		

PARCI	Project Role	Name	Signature	Date
Informed	Configuration Manager	Robin Winfield		
	Enterprise Architecture Mgr	Kiwi Wilkinson		
	Design Team Manager	Stuart Plummer		
	Enterprise Apps Architect	Praveen Nagpal		
	Enterprise Info Architect	David Lee		
	Enterprise Infrastructure Architect	Aaron Goodship		
	Application Lead	Ross Daines		
	Technical Project Manager	Tarun Narang		
	PMO	Rubina Chaudhry		

Part G: Appendices

Appendix G1: Validation

SOAP Validation

Validation	Description	Error Message
Is the sender or owner valid?	The sender PartyId & PartyRoleCd (Broker, ServiceProvider etc) must be registered with Xchanging for the message type (Upload, Download, Search etc.) that they are sending in.	Either the Owner or the Sender is not a valid trading partner *Note:* Error message is not sent to the originator in this case, please contact Xchanging's support team in case the messages are not getting processed.
Is business message valid?	The business message was not well formed XML	SOAP Fault
Was SOAP body signed with valid key?	All incoming DRI messages have ACORD minimal security applied which means that they must have been signed with a valid certificate. The public version of this certificate needs to be registered on each gateway.	Signature validation failed
Is the business MsgId in the valid format?	The MsgId is not a valid GUID in the business message	The MsgId is not a valid GUID

Business Validation

Validation	Description	Error Message
Is the component UUID unique?	Each DRI message must have a unique MsgId	Duplicate component UUID
Does the organisation have access to the UMR/UCR?	Requester does not have access to the UMR/UCR	Validation errors
Do Soap and business message document counts match?	The amount of attachments that the SOAP message and DRI message refer to must be the same.	no data found for document<document id/reference>
Sender (Insurer/Reinsurer) should have access to UCR.	Sender of the DRI Upload request should have access to the Claim to which document should be uploaded	Invalid Insurer! You can only upload documents for the groups to which you belong.
Incorrect ACL supplied in the upload request	The ACL applied to a document should be a subset of the ACL of the UCR. If a party appears on the document ACL who is not on the UCR ACL, the Upload Request will be rejected with an appropriate error code and the Carrier will be required to resubmit the document with an amended ACL.	Invalid ACL Provided (<ACL_DETAILS>)!
More than one document sent in the upload request	Carriers are required to send only one document per document upload request.	Invalid Submission! Only single document upload request with ACL is allowed.

Appendix G2: ACL Approach for DRI Upload for Carriers

Purpose of this paper

There is a requirement for Carriers to specify an Access Control List (ACL) when uploading a document to the IMR via DRI Upload. This paper provides an overview of the main business scenarios to be supported and the proposed approach to accommodate these scenarios for validation by the Write Back business working group.

Business scenarios

The main business scenarios to be supported are:

- Allow a Carrier to supply an ACL in order to deny access to the Broker to a specific document (e.g. where the document is in respect of Coverage)
- Allow a Carrier to supply an ACL in order to restrict access to other parties on the claim to a specific document (e.g. where a document is only intended for participants within the same bureau on a cross-market claim)

Approach

- Only a party who is on the ACL of a UCR will be able to upload a document via DRI to that folder. Any senders of a DRI Upload request who are not on the ACL of the UCR in question will receive a rejection.
- Where a document can be viewed by all participants on a claim (Carriers and Brokers) no ACL should be supplied.
- Where a document can be viewed only by selected participants on a claim, the ACL should explicitly state which participants on a claim can view the document. Please note:
    - Any parties (excluding the sender) that do not appear explicitly on the ACL will not have access to the document.
    - The ACL applied to a document should be a subset of the ACL of the UCR. If a party appears on the document ACL who is not on the UCR ACL, the Upload Request will be rejected with an appropriate error code and the Carrier will be required to resubmit the document with an amended ACL.

- There will be no change to the ACL approach for Brokers implemented during the IMR Security Model project. Where a Broker specifies an ACL and a UCR is present in the Upload request, the ACL is ignored.
- Carriers will have an option to 'remove' a party who is on the ACL of the UCR from the document ACL. For example, in order to prevent a broker viewing a document relating to coverage, Carriers will send an ACL with PartyId = Broker Code, Party Role Code = Broker and AccessRightCd = REMOVE. This will prevent the Broker from viewing the document but allow all Carriers (including Carriers from different bureaus in a cross-market scenario) to view the document.