

Meeting Notes

IAG – File Transfer Rulebook Working Group

Inaugural meeting, March 8th 2007 – Final Version

Attendees:

Dharmesh Sethi - Citigroup

Andreas Hoefler - Deutsche Bank

Serge Logelain - Clearstream representing Deutsche Boerse

Gaël David - BNP2S

Marc Winkler – LCH.Clearnet

Steve Feldstein - Morgan Stanley

Luc Castan - Euroclear

Martin Stolz - ISSA

Aki Tarri – NCSD

Alex Kech - SMPG

Andrew Muir, Frank Versmessen, Kris Ketels, Philippe Cornette, Bruno Lacroix of SWIFT

Objective:

The objective of this meeting was stated as to determine the Scope, Content Headings and Production Plan for a generic File Transfer Rulebook.

Scope and Contents:

The scope, as defined in the strawman rulebook circulated prior to the meeting by FV, was broadly agreed. Several points of principle, which need to be captured as part of its scope, were agreed:

File Construction:

- The Rulebook should permit any content in a file transmission (ie not just ISO messages – pdf's, FIX messages, images etc will also be valid content)
- Within a given file transmission, there will be limits to the types of content permitted. Specifically:

- one transmission may contain multiple pdfs, or multiple ISO15022/ISO20022 messages but not mixtures of the two;
- Single transmissions may contain multiple messages of a single standards family (e.g. ISO15022), or of multiple standards families (e.g. ISO15022, ISO20022, FIX) – but not of mixed formats (ie binary objects may not be mixed with text messages).
- Within a given file transmission, only one version of a content type would be allowed (ie current* versions of ISO15022 messages or future* versions, not both)
 - * a proposal as to the clear definition of these terms will be circulated by SWIFT
- File Transfer operational rules need to be specified about:
 - Delivery notification and error reporting (at the message and file level)
 - What kind of delivery notification is part of the rulebook, and how is this distinguished from network-level processing?
 - How are DN's and acknowledgements affected in store-and-forward mode as distinct from real-time delivery mode, and what effect do these differences have on the rulebook?
 - “Possible Duplicate” notification at the file level
 - What are the rules about Possible Duplicate markers where, for example, messages do not have PD markers defined in themselves?
 - Non-Repudiation and PKI certification
 - What accommodation for non-repudiation needs to be made in the rulebook? There are differences in law between countries as to the requirements for non-repudiation – how will these be catered for?
 - Specific attributes of file and/or message headers need to be included to include non-repudiation and PKI – what models are used (example cited by Citigroup is AS2), and how can these be represented generically?

File Transfer Operations:

The sense of the meeting was that several items in the strawman were more implementation-specific, and therefore not in the rulebook scope:

- Handling of intermittent communications failures
- Monitoring of transfer progress
- Concurrent transfer handling
- Archival

This needs verification – the group agreed that file transfer operations was a topic which needed considerable work – and that another workshop will be needed in order to cover it.

The key question is how much detail this rulebook needs to contain. For example – if this rulebook is to specify the detailed implementation of Public Key Infrastructure and Non-Repudiation to be used, it implies that all firms will standardise on a single technical implementation. Clearly, this would enable interoperability – but the costs of migration would be potentially prohibitive.

It is proposed that this rulebook should be file-transfer-platform-independent. It should contain enough information in the header definitions to enable any application to identify and process the payload in a standardised way – and to require that transmissions are signed end-to-end, and that non-repudiation is activated as required under the jurisdiction of the sender and/or receiver - but not be prescriptive about the method by which this is achieved.

Content:

Considerable progress was made on the definition of file and message metadata, which will form the bulk of the next version of the rulebook draft. Lists of file and message header attributes were proposed (see below), and SWIFT will work these into the next version of the draft rulebook with proposed definitions/values, along with the inventory of established principles.

File Header information

Header Attribute	Format	Description
Sender ID	BIC	
Receiver ID	BIC	
Sender File Reference		
Related File Reference		
Date/Time of file creation		
Session/Cycle number		
Sequence number		
Service ID		
Priority		
Number of messages in file		
Mode (ie test or live)		
Content Standard Family		
Content Standard Version		
Item Delimiter Value		
Content Expiration Date/Time		
Character set ID		

Compression Algorithm ID		
Possible Duplicate Indicator		
Delivery Notification Required		
Security Context		
Sending Application Name		
Target Application Name		
Non-Repudiation Flag		
PKI Certificate		

Message Header information

Header Attribute	Format	Description
Sender ID	BIC	
Receiver ID	BIC	
Sender Message Reference		
Related Message Reference		
Message Type		
Message Version		
Message Priority		
Delivery Notification Required		
Non-Repudiation Flag		
PKI Certificate		

File and Message Header Syntax is to be discussed;

- Should the header attributes be represented in a fixed syntax, or should they be in the same syntax as the content?

Next Steps:

SWIFT will draft a version of the rulebook according to the contents of the meeting summarised above. The draft should include a proposal from SWIFT (Philippe and Kris) on how to handle the file transfer operations questions about PKI and non-repudiation.

A schedule will be circulated showing a publication and meeting schedule designed to complete the rulebook in time for the SSC in June – I propose:

Next draft issued: 21 March

(Document scope, principles, Detailed File and Message Header information and definitions, and a proposal for handling PKI and non-repudiation questions)

Conference call to review: 23 March

Rework and reissue: 2 April

Workshop on File Transfer operations (inc PKI and non-rep) and outstanding questions:
18-19 April

Rework and reissue: 30 April

(This should be a near-final rulebook, containing all rules derived from the workshop and illustrative examples)

Conference call to review: 2 May

Rework and reissue (final): 14 May

Signoff conference call 17 May

IAG – File Transfer Rulebook Working Group

Discussion Point – Issue G1

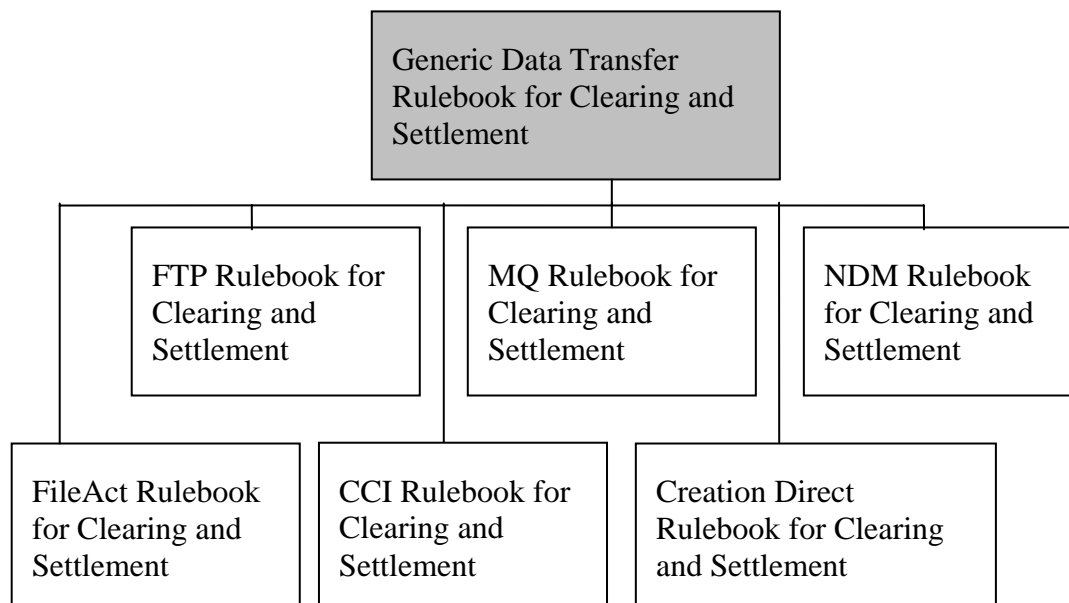
Structure of Rulebook - Generic versus Service-specific rules, and a framework that captures both?

The objective of the harmonisation program which is underway across all EU securities markets is to promote higher efficiency levels throughout the securities processing chain. At one extreme, within the context of the Rulebook under discussion here, it is possible to conceptualise a single file transfer regime, where all operational, technical and legal frameworks are themselves standardised, and to which all existing file transfer systems would be forced to migrate.

Practically, this is regarded as an impossible target. There will be many different file transfer systems in use for the foreseeable future – simply because the costs and risks of a widespread migration will seem so high as to outweigh the benefits. Likewise, the file transfer systems in widespread use today have their own operational characteristics, some of which are tightly bound to their design or contractual structure. Accordingly, the Rulebook being designed needs to be sufficiently flexible to accommodate a variety of different implementations; or sufficiently demanding as to force a wholesale program of change to a vast array of entirely satisfactory systems.

There is undoubtedly a benefit to a higher level of standardisation than is currently prevalent. But – it is also impractical to propose a solution that would force a very expensive change program, or risk being ignored for being too cumbersome.

Accordingly, it is proposed that we define a two-tier rulebook structure, where the generic rules to be used which can apply across all file transfer infrastructures are defined in a single, solution-neutral rulebook (defining the “what”), and a lower-level rulebook, one for each “approved” file transfer infrastructure, which defines the operational and technical implementation characteristics (ie the “how”), thus:



Generic Rulebook contents would thus be:

Approved File Transfer Infrastructures and Rulebook sources

Header Definitions:

- Business Metadata (ie description of business content in the payload)
- Structural Definitions (ie payload structure and batching rules)
- Security and Technical (ie information necessary to drive security/technical operations)
- Workflow (ie definition of business and/or application response requirements processes)

Content Rules

- Permissible mix of content
- Permissible types of content

Operation Rules

- Acknowledgement and Delivery Notification
- Content or Payload-Related Error Handling

Infrastructure-Specific Rulebook contents would include:

- PKI Terms and Conditions
- Non-Repudiation Terms and Conditions
- Technical Operations (ie Protocol)
- Service Levels (Availability, Reliability, Resilience)

Non-Proliferation of Rulebooks

It is further proposed that the number of approved file transfer infrastructures is controlled. In part, this is to prevent further proliferation of proprietary systems and rulebooks – but it is also to encourage industry participants to replace some of the less common infrastructures with more standardised solutions.

Those infrastructures identified at our meeting that are in widespread use today, are:

- FTP
- IBM MQ Series
- HTTPS
- SWIFTNet FileAct
- Euroclear CCI
- Clearstream Creation Direct
- Connect Direct NDM.

IAG – File Transfer Rulebook Working Group

Discussion Point – Issue G2

PKI and Non-Repudiation – what can a generic rulebook cover?

Non-repudiation is the capability to unambiguously resolve conflicts among two users of a messaging infrastructure about the exchange of a message or file at some point in the past. It can apply to both the generation by the sender and the response from the receiver. The duration of the non-repudiation capability depends on local requirements as specified by relevant national and community legislatures, regulators and conventions.

In the context of PKI, non-repudiation typically relies on PKI-signatures applied to messages and files and also covering the time of the transaction. It has to take into account the validity of the PKI certificate of the signer at the time of the transaction. In particular, it must establish that this certificate was not repudiated by then.

An infrastructure can support non-repudiation in several ways:

- Senders and receivers are given the means to store PKI-signed messages and files, as well as all certificates and repudiation information needed to subsequently re-verify that the signature was valid at the time of the transaction. The repudiation information can take the form of the certificate revocation list in effect by the time of the transaction.
- Senders and receivers are given the means to store signed messages and files, and the infrastructure provides services to re-verify that the signature was valid at the time of the transaction, including vis-a-vis the repudiation information.
- The infrastructure acts as a trusted third party, accepted by all participants, to keep a copy of all messages and files in transit. In case of conflict, the presence of the message or file in the records of the infrastructure is accepted by all as proof that the transaction happened.

PKI, and Non-Repudiation, is in many cases non-interoperable between networks. In the case that the infrastructure itself acts as a trusted third party, both PKI and non-repudiation is tightly bound to the service itself, and is both technically and contractually insulated from other infrastructures.

Accordingly, it is recommended that whilst the generic rulebook may refer to PKI and Non-Repudiation elements as part of generic header requirements, guidance as to the specific implementation of both PKI and Non-Repudiation is left to the individual infrastructure rulebooks as proposed in discussion point relating to issue G1.

IAG – File Transfer Rulebook Working Group

Discussion Point – Issue G3

Consolidation of generic rulebook attributes across all "harmonisation" domains; an explanation of the Header Attributes section of the proposed Rulebook Elements

The concept of harmonisation of processes extends throughout the range of processes supported by SWIFT, and beyond. To ensure that the Rulebook includes sufficient extensibility to encompass the known requirements of the various harmonisation initiatives underway, inputs have been sought from the following sources:

- SEPA (Single Euro Payments Area)
- UN/CEFACT
- ebXML
- Application Headers from existing SWIFT services

In the spreadsheet entitled "IAG Rulebook Elements", header attributes from these sources have been added to the original list of attributes identified by the IAG Rulebook Working Group. Thereafter, they were themselves consolidated into a single list, in order to avoid duplication.

In addition, we have tried to assign names to each attribute, and to propose a cardinality indicator (in the format x..y, where x is the minimum number of times the attribute should appear in a header and y is the maximum).

We have also mapped each header attribute to its application, so that readers can see what the "Giovannini profile" header attributes would be, as distinct from those for other solutions on which we are working (ie SEPA, SEPA with Netting, Customer-to-Bank and SWIFT Corporate (SCORE) domains).