ECM DOCUMENT 2

-

EFET STANDARDS 1.0

CENTRAL MATCHING AND P2P AUTHENTICATION PROCESS

VERSION 1.14

CREATED BY EFET IT TF – BUSINESS WORKGROUP

Revision History

Version	Date	Changes	Author of changes
Version 1.2		Created by EFET IT TF – Business workgroup	
Version 1.2.2	16/7/2002	Amended to reflect new vision as proposed by Electrabel & Transmeta.	
Version 1.4	18/7/2002	Extensively reviewed & approved by EFET IT TF – Business Workgroup during 18/7 Brussels Workshop	EFET IT TF – Business Workgroup
Version 1.5	12/8/2002	Amended to include comments by Mike Conroy (Schlumberger Sema) • Add key field concept in standard • Replace affirmation with authentication • Replace bi-lateral with peer-to-peer • Replace ECMS with ECM • Minor syntax and grammar and other corrections • Proposal for match, authentication and rejection messages	Kris Bouckaert (Transmeta)
Version 1.6	19/8/2002	• Minor corrections • Changes in data structure of authentication and matching messages.	Kris Bouckaert (Transmeta)
Version 1.7	21/8/2002	• Correction of delivery point and country of origin description	Sophie van der Haegen (Electrabel)
Version 1.9	26/8/2002	• Specify scope limited to UK & continental power fixed price • Confirmation message type: Add energy account, remove country of origin, rename market, quantity and unit	Sophie van der Haegen (Electrabel)
Version 1.10	12/9/2002	Changes after meeting on 5/9/2002 in Amsterdam and 11/9/2002 conference call • Remove “total value” field • Change the fields “Memo” and “Trade Reference” to informational • Match message only contains	Kris Bouckaert (Transmeta)

		content of other party's confirmation • Authentication contains no confirmation content • Align document names	
Version 1.11	25/9/2002	Changes after meeting on 20/9/2002 in Brussels • Change the names of some of th fields • Add a cancellation message • Add an acknowledgement message	Kris Bouckaert
Version 1.12	30/9/2002	• Add two additional fields for England and Wales, after input of John Lowther • Align message structure to Brussels 3/10/02 meeting decisions	Kris Bouckaert
Version 1.13	7/10/2002	• Align with document 5 • Copyright notice	Sophie van der Haegen (Electrabel)
Version 1.14	9/10/2002	• Replace EXIS application box with EFET box	

Copyright notice

Copyright © EFET 2002. All Rights Reserved.

This document and translations of it may be copied and furnished to others, and derivative works that comment on or otherwise explain it or assist in its implementation may be prepared, copied, published and distributed, in whole or in part, without restriction of any kind, provided that the above copyright notice and this paragraph are included on all such copies and derivative works. However, this document itself may not be modified in any way, such as by removing the copyright notice or references to EFET except as required to translate it into languages other than English.

The limited permissions granted above are perpetual and will not be revoked by EFET or its successors.

This document and the information contained herein is provided on an "as is" basis.

EFET DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

I. INTRO 6

II. DOCUMENTS 7

III. BACKGROUND INFORMATION 8

III.1. CURRENT CONFIRMATION PROCESS 8
III.2. ISSUES LINKED TO CURRENT PROCESS 9
III.3. CENTRAL MATCHING SERVICE 10

IV. SCOPE 11

V. EFET COMPLIANT ECM PROCESSES 12

V.1. PEER-TO-PEER AUTHENTICATION PROCESS 14
V.2. CONFIRMATION MATCHING PROCESS TROUGH A CENTRAL SERVICE PROVIDER 16
V.3. USE OF ACKNOWLEDGEMENT AND REJECTION DOCUMENTS 18
V.4. LEGAL AND CONFIDENTIALITY ISSUES 19

VI. DOCUMENT TYPES & ATTRIBUTES 20

VI.1. CONFIRMATION DOCUMENT 20
VI.2. AUTHENTICATION DOCUMENT 23
VI.2.1. CONFIRMATION MATCHING TROUGH A CENTRAL SERVICE PROVIDER 23
VI.2.2. PEER-TO-PEER AUTHENTICATION 23
VI.3. CANCELLATION DOCUMENT 27
VI.4. REJECTION DOCUMENT 28
VI.5. ACKNOWLEDGEMENT DOCUMENT 30

I. INTRO

Goal of the current project is to find **a common solution for the automation of the transmission, reception, matching and processing of electronic trade confirmations**.

Considering the existence and emergence of Central Matching Service providers offering confirmation matching services for standard trades but also the huge diversity in confirmation processes, the EFET IT TF came to the conclusion that no single service will ever process all confirmations between all involved parties.

EFET's first mission is to define a common language and process for all confirmations. The "EFET electronic confirmation standard" resulting from this project should thus enable parties to confirm trades either through a central service or via a peer-to-peer connection both for standard and more complex structured trades.

The EFET organization itself will provide a central EFET directory service and will ensure maintenance of the standard with the publication of new codes etc…

II. DOCUMENTS

All EFET definitions related to the electronic confirmation process are listed in the **EFET ECM doc1 - Lexicon**.

The current confirmation process, future electronic confirmation process, possible scenarios and legal issues will be described in the **EFET ECM doc2 - EFET Standards 1.0 - Central Matching and P2P Authentication Process.**

To encourage emerging Central Matching Service providers to conform with this "EFET Electronic Confirmation and/or Matching Standard" and meet certain business requirements expressed by EFET industry participants, the **EFET ECM doc3 - Recommendations for Central Matching Service** will describe the business requirements for a Central Matching Service.

The EFET IT TF - Business Workgroup, will validate these first three documents.

Code conventions and best practices for the technical implementation of ECM and other EFET compliant interfaces will be described in **EFET ECM doc4 - EFET Standards 1.0 - Core Components & Coding Scheme.**

This last document is to be generated by the EFET IT TF - Business Workgroup with basic EFET codes proposals and then revised and completed by the EFET IT TF – technical workgroup.

The exact definition of the EFET ECM interface will be described in **EFET ECM doc5 - EFET Standards 1.0 - ECM Interface Definition.**

This last document is to be validated by the EFET IT TF - Technical Workgroup.

Finally, for members wanting to automate peer-to-peer process, the business and technical requirements of the EFET box (ECM module) will be described in **EFET ECM doc6 - Recommendations for EFET box.** This document could be used for tendering for the development of the EFET box.

This last document is to be generated by the EFET IT TF - Business Workgroup with the business requirements and then revised and completed with additional technical requirements by the EFET IT TF – technical workgroup.

III. BACKGROUND INFORMATION

III.1. CURRENT CONFIRMATION PROCESS

The current trade matching processes are generally paper based requiring both parties to produce documents that summarise the transaction. These documents are passed between each party to confirm that the transaction details are accurate and valid.

The main steps in the process are:

1. A transaction is agreed between two parties and details of the transactions are entered into each party's trade management system
2. An internal check (usually manual) is normally undertaken by each party to ensure that the transaction details have been accurately entered into the trade management system
3. A trade confirmation document is then generated by the trade management system. The trade confirmation document is checked for accuracy. The trade confirmation might also be signed by the originator (normally the seller) as an accurate summary of the trade details and then faxed or digitally sent to the recipient party (normally the buyer) for that transaction
4. The recipient party then checks the trade confirmation. (A number of trade management systems will generate a confirmation independently of the fact that the party is the buyer or the seller. The buyer will often use their version of the confirmation to check the details of the seller's confirmation). If the recipient party agrees with the details of the transaction, they might sign the trade confirmation to confirm that the details are accurate and valid.
5. The recipient party's signed document might then be faxed back to the originator of the confirmation. This is then a paper affirmation or authentication.
6. Each party will enter information into their trade management system to indicate that the transaction has been authenticated.
7. The paper work associated with the trade data capture and trade confirmations will, at an appropriate point in time, be archived and retained for a number of years (depending upon local procedures and laws)
8. In the event that the transaction details are not agreed as accurate (or the seller has not raised a confirmation):
    - The party finding the mistake first will contact the other party (normally verbally) to indicate the details that are not agreed (or in the case where the seller did not send a confirmation the buyer will contact the seller to indicate that the confirmation has not been received)
    - After investigations the transactions details are agreed
    - Steps 1 to 8 are repeated such that an accurate and confirmed transaction is recorded in each party's trade management system.

Many variations of this process exist. Depending on the agreements (Master Agreements like EFET2.1 or industry accepted terms and conditions like NBP97) that exist between the two parties, both the buyer and the seller will send a confirmation or only seller will send a confirmation and the buyer will affirm or authenticate:

- One of the parties (logically the seller) has to send the trade confirmation to the other party. The buyer will then check this confirmation against its own record of the trade. If consistent he will consider the trade confirmed. He might or might not send back by fax an authentication (signed acknowledgement authenticating the confirmation). Certain parties require an authentication of their confirmation to be sent back and will systematically expect one, others will not.
- Both parties send each other the trade confirmation and each will check for itself the validity of the received party's confirmation against its own trade data. If consistent the trade is then considered "confirmed". Even in this case one of both parties might still send back an authentication of the received confirmation.
- In the case where a trade is concluded by mediation of an intermediary (either on an e-OTC platform or a voice broker), the intermediary sends a broker "confirmation" of the transaction to both the buyer and the seller. It is also customary for a trader to check at the end of the day by phone, the trades concluded via a certain broker. Some e-OTC platforms either list the executed trades or immediately after execution send an email to the trader with the trade details.

Some industry participants refer in the confirmation to an existing Master Agreement in place between both parties. In case no Master is in place, the confirmation might contain certain legal language to ensure legal enforceability of the trade.

The content of the confirmations will also typically vary according to the product (gas, power, oil), the delivery point, Master Agreement and the legal framework.

In case of a dispute, the transaction tapes or the transaction log of an e-OTC platform will always prevail on the written documents (confirmations) irrespective if they are matched or authenticated. Of course, it goes without saying, that if the confirmations match or the confirmation of the seller is authenticated by the buyer, it would highly unlikely for the traders to revert successfully to the transaction tapes and the trade would stand as confirmed.

Important Note: Currently, no unique trade reference for a trading transaction exists between the parties (as is customarily the case for example for the purchase of airline tickets). Each party defines its own unique TradeID.

III.2. ISSUES LINKED TO CURRENT PROCESS

Major issues with the current process are:

- Cost and operational risk linked to manual processing of confirmations
- Archiving cost of paperwork
- Neither the process itself nor the material terms of the trade are standard, introducing complexity in the confirmation matching process and trade follow up

- Risk linked to delay in identifications of trade data capture errors and inconsistencies between parties
- Traders are not certain of their trading positions until the first day of delivery

III.3. CENTRAL MATCHING SERVICE

A huge improvement to the manual process is the introduction of one or different Central Matching Services.

If both parties are registered to the same Central Matching Service provider and the corresponding trade type is supported by the matching service, both parties will simply send their trade confirmations to a central service provider who will try to match them and return a matching result. Either a match was found, or a probable match has been found or no party confirmation was received before timeout.

In the event a match is found, the both parties will consider their trade confirmed and will store the (reference to) matching result. Note that the matching result can contain warnings to signal differences in non-material attributes of both confirmations.

In the event that no match is found after a certain time period (time-out), the central service will return the confirmation as unmatched. Each party is then responsible for the analysis of the unmatched confirmations and to contact the other party to resolve the problem. As soon as the reasons for the mismatch have been detected and corrected, each party will resend a "corrected" confirmation to the Central Matching Service for a second matching attempt. In case the reason of the mismatch is due to a fundamental incapability of the Central Matching Service to match the trade, the trade will be confirmed outside the system.

For any Central Matching Service to operate efficiently, both confirmations need to refer to the same existing Master Agreement between the parties.

We can conclude that no Central Matching Service provider will in the near future be able to match all trades, as you can't expect every party to register to the same service provider nor any service to support all possible trade types. Therefore, there will always be the need for peer-to-peer electronic confirmation capability.

IV. SCOPE

The aim of the EFET IT TF is to define a "standard electronic confirmation process" and thus provide a framework enabling parties to:

- Replace the manual transfer of information with the electronic transmission of standard confirmation data between two parties (on a peer-to-peer basis)
- Allow transfer of information to a central service provider for the automatic matching of trades between the parties registered as users of that service
- Facilitate the reporting and capture within their trade management systems of electronic data related to the trade confirmation process (be it through a peer-to-peer or central service confirmation)

The EFET ECM standard will thus have to support both peer-to-peer confirmation data exchange and use of a central service.

Important Note:

The definition of an electronic trade confirmation framework does NOT imply that the current manual process of comparing a trade confirmation received against the own trade data will be fully automated!

It does mean that receiving and sending the trade confirmation will be carried out in an electronic and standardised way (thus facilitating the manual reconciliation task). It is up to each member to decide whether he wants to subscribe to a central service provider or whether he wants to confirm through a peer-to-peer connection and possibly build its own matching logic (cfr. EFET box). In the last case, the result of this matching, if positive, will not be sent to the other party as being a match result (only valid if sent by an approved central service provider) but as being an authentication of the received confirmation.

The exchange of information between a central service user and a party not subscribed to this Central Matching Service, will be carried out through a peer-to-peer connection without the intervention of the central service provider.

This implies that even if a company is subscribed to a Central Matching Service, it might want to build its own confirmation reconciliation logic to handle trades with parties that are not subscribed to that central service.

V. EFET COMPLIANT ECM PROCESSES

EFET will here describe what workflow will be defined as a standard EFET compliant ECM process. For this purpose the actors and their systems are considered to be "black boxes". EFET has restricted itself to defining the interface requirements for the incoming and outgoing messages.

The actors of this ECM process:

- A central directory & standardisation service, run by EFET on its website, will keep track of the capability of each EFET member to send and receive EFET compliant electronic confirmations through peer-to-peer connections as well as the registration of the EFET members to the different Central Matching Service providers.
- A number of Central Matching Service providers who will receive trade confirmations as input and return matching results (e.g. ICE and Logica).
- An inbox at each and every party, being a central repository for incoming document.
- Possibly in the future a number of electronic brokerage platforms who will either send their OTC confirmation data to a Central Matching Service provider and/or to the parties directly…

Typical scenarios implying the exchange of data between these actors (excluding the brokerage platforms for this first phase) are:

- the exchange of data peer-to-peer between parties
- the exchange of data via a Central Matching Service provider since both parties are registered to the same Central Matching Service provider

If both parties are NOT registered to the same Central Matching Service, a confirmation can only be carried out via a peer-to-peer connection between the parties (refer to the diagram in figure1).

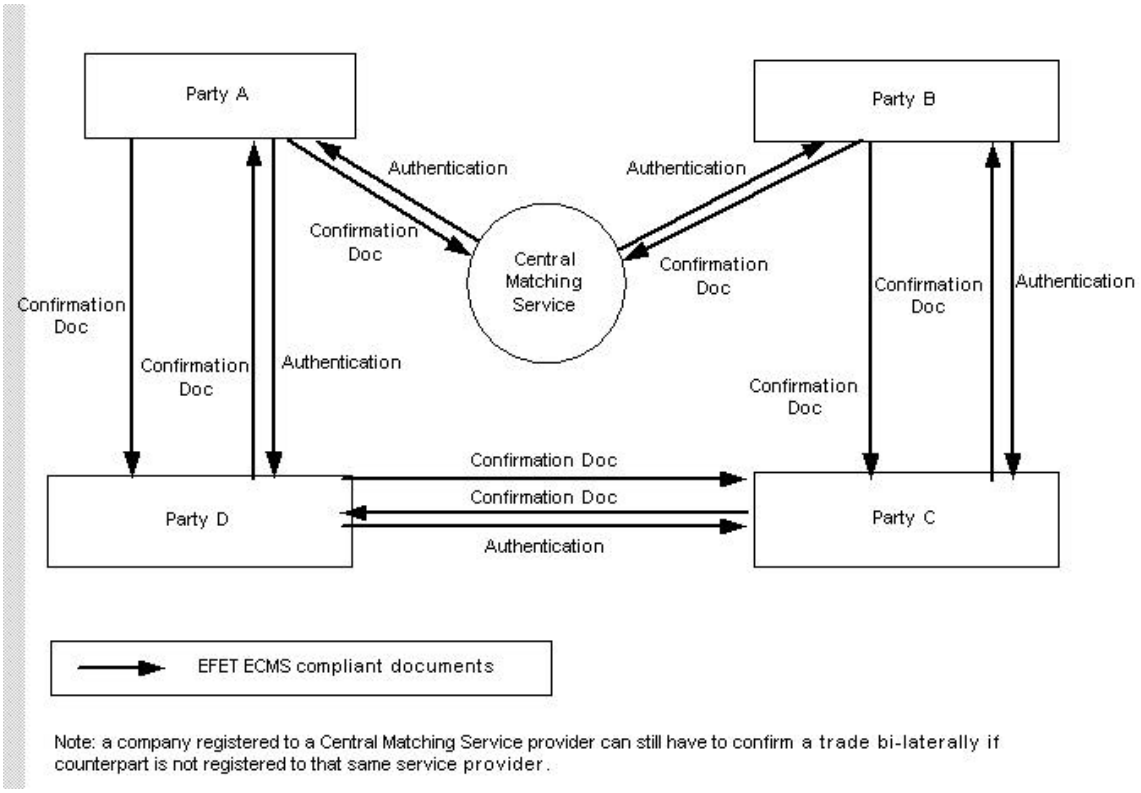

Figure 1. Electronic Confirmation Process: Peer-to-Peer Authentication Process and Confirmation Matching through a Central Matching Service Provider

V.1. PEER-TO-PEER AUTHENTICATION PROCESS

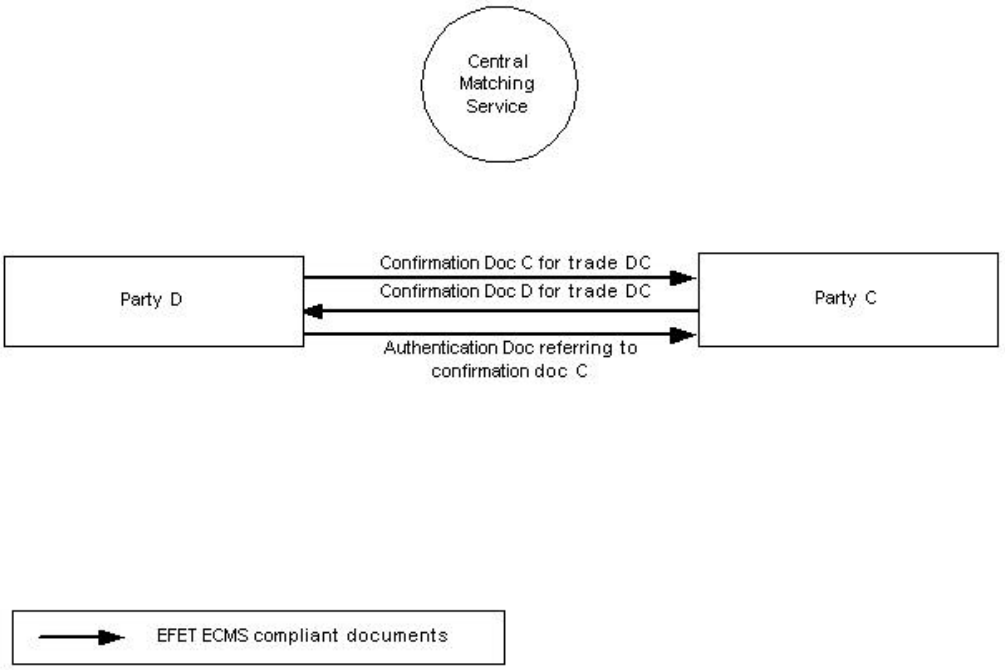

Figure 2. Peer-to-Peer Authentication Process

The process is quite similar (in fact quasi identical) to the current fax exchange flow, with the exception that both the buyer and the seller shall send each other a trade confirmation and one of the parties shall send back an authentication.

Assuming B is the one who has to send back the authentication message, we get following exchange of data between both actors:

- A sends a **confirmation message** to B
- B sends an **acknowledgment message** back to A to acknowledge that he has correctly received the confirmation message of A
- B sends a confirmation message to A
- A sends an **acknowledgment message** back to B to acknowledge that he has correctly received the confirmation message of B
- A might but B definitively will check the received confirmation against their own trade data or confirmation (**INTERNAL automatic or manual** reconciliation process)
- Scenario 1: both confirmations are coherent
    - Scenario 1a:
        - B sends back the countersigned confirmation (=**authentication message**)

        - A sends an **acknowledgement message** to acknowledge that he has correctly received the authentication message. A now considers his trade to be reconciled
    - Scenario 1b:
        - B does not send back any message
        - A will call up B to require the transmission of the authentication
        - Scenario 1a
- Scenario 2: both confirmations do not contain the same material terms
    - A and B contact each other to settle the dispute.
    - Scenario 2a: They resolve the dispute
        - Either A or B sends the amended **trade confirmation message** to the other
        - scenario 1
    - Scenario 2b: They cannot resolve the dispute
        - The dispute is escalated (listen to tapes, notification of desk manager, arbitration,..)

Additional rules as defined by EFET:

- The party responsible for the transmission of the authentication might depend on the arrangements in the Master Agreement in place between both parties. EFET best practices: **the BUYER sends back the authentication**.
- EFET requires both parties to send their confirmation message before end of business day of the trade date (8pm CET).
- An authentication message sent by one of the two parties and related to the confirmation of the other party, shall mean that this party agrees on all key fields of the corresponding other party confirmation document. A party will thus check the Key fields of a confirmation before replying with an authentication document on that confirmation.
- A party can always send an amended version of a previously sent trade confirmation, using the same tradeID and an augmented version number. The amended trade confirmation will overrule the previously sent trade confirmation if it has not been matched yet in the system of the receiver.
  Once a trade confirmation has been matched, it can not be changed anymore.
- If a party wants to cancel a trade confirmation document, they can either do that by sending a **cancellation document** or by calling the other party.
  The cancellation document will only cancel the trade confirmation if it has not been matched yet in the system of the receiver. Once a trade confirmation has been matched, it can not be cancelled anymore.

V.2. CONFIRMATION MATCHING PROCESS TROUGH A CENTRAL SERVICE PROVIDER

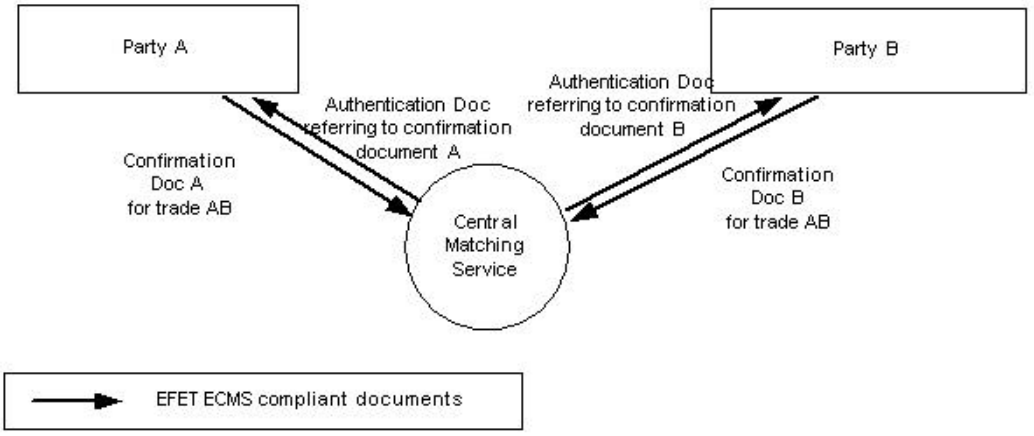

Figure 3. Confirmation Matching through a Central Matching Service Provider

In case both parties of a trade are registered to the same Central Matching Service Provider, they will both send their trade confirmations to this Central Matching Service Provider who will in return report a matching result.

This result basically can be a match or a time out. The matching result to a given party shall contain the other party's trade confirmation content.

Important Note:

Some Central Matching Service providers might foresee additional functionality, such as the availability of online reports with information about possible or probable matches etc… made available through a user interface (e.g. web browser or client) or downloadable structured files (XML or other).

The description of this information is consciously kept out of the scope of the EFET Electronic Confirmation Interface standard as it can not be expected to be exactly the same for all central service providers.

Recommendations towards Central Service Providers on what EFET members expect to be the matching logic, on minimum requirements on reporting, user interfaces and service level agreements will be described in ***EFET ECM doc3 - Recommendations for Central Matching Service.***

Assuming both A and B are subscribed to Central Matching Service Provider X, we get following exchange of data between actors:

- A sends its **trade confirmation document** to the central service provider X
- X sends back an **acknowledgement document** to A
- Scenario 1: B sends its **trade confirmation document** to the central service provider X
- X sends back an **acknowledgement document** to B
    - Scenario 1A: X matches both trade confirmations
        - X sends a trade confirmation match document **(=authentication document)** to A
        - X sends a trade confirmation match document **(=authentication document)** to B
        - A considers the trade matched
        - B considers the trade matched
    - Scenario 1B: X can not match both documents because of inconsistencies
        - One of the parties, suspicious about his confirmation remaining unmatched, contacts the other to settle the issue
        - One or both parties will re-send their "corrected" **trade confirmation document** to X
        - Back to scenario 1A
- Scenario 2: B fails to send its trade confirmation document to the Central Matching Service X
    - X can not match A's confirmation and it remains in status unmatched
    - A suspicious about his confirmation remaining unmatched, contacts B to settle the issue
    - B will send its **trade confirmation document** to X
    - Back to scenario 1A

EFET has defined following additional rules:

- Both buyer and seller shall send their confirmation documents before end of business day of the trade date (8pm CET).
- The matching process itself should be carried out as soon as possible after the reception of the document.
- **Only key fields** will be taken into account in the matching process. An authentication document sent by a Central Matching Service provider shall mean that the key fields of the confirmations to which the document refers are identical. The key fields of two confirmations will thus have to be identical for the Central Matching Service to report a match on those two confirmations.
- Participants have to have a **Master Agreement** in place with each other, referring the actual commodities as being treated by a Central Matching Service.

- Time out shall occur three business days after the reception of a document. A **delivery point based holiday calendar** shall be used for calculation of business days.
- A party can always send an amended version of a previously sent trade confirmation, using the same document ID and an augmented version number. The amended trade confirmation will overrule the previously sent trade confirmation if it has not been matched yet in the system of the Central Matching Service. Once a trade confirmation has been matched, it can not be changed anymore.
- If a party wants to cancel a trade confirmation document, they can either do that by sending a **cancellation document** or by using the Graphical User Interface to access the system of the Central Matching Service.
  The cancellation document will only cancel the trade confirmation if it has not been matched yet in the system of the receiver. Once a trade confirmation has been matched, it can not be cancelled anymore.

Note: The internal processing of a trade confirmation match (=authentication document) received from a central service provider will be very similar if not identical to the processing of a counter party trade confirmation signature (=authentication document) in the peer-to-peer scenario.

V.3. USE OF ACKNOWLEDGEMENT AND REJECTION DOCUMENTS

When a trading party has sent a document to another party, either another trading party or a Central Matching Service, he will expect a document back which will inform him of the status of his document in the system of the receiver.

This is required after the sending of one of the following documents:

- Trade confirmation document (P2P and central)
- Authentication document (only P2P)
- Cancellation document (P2P and central)

The document sent back will be:

- **An acknowledgement document**, when the received document has been validated successfully, and could be processed by the receiving system.
- **A rejection document**, when the received document could not be understood or could not be validated successfully, or when the received document could not be processed successfully by the receiving system. A reason code will point out the reason for which the received document was rejected.

Successful processing of a document means the following:

- **Trade confirmation document**:
  First, it will be checked if there is already a confirmation with this Document ID in the system. This indicates if this is a new confirmation or an update of a previously received confirmation.
  - New confirmation: A new confirmation document is successfully processed when it could be placed in the matching queue.
  - Update of confirmation: The version of the update needs to be higher than the current active version in the system. As well, the current active version cannot already have the status of matched or timed-out in the system of the receiver. An update of a confirmation is successfully processed when the update could be carried out, and the updated version could be placed in the matching queue.
- **Authentication document**:
  The authentication refers to a trade of the receiving party, which still has a status of "awaiting authentication" in the trade system of the receiver.
- **Cancellation document:**
  The cancellation document needs to refer to an existing trade confirmation in the system of the receiver. As well, the referenced trade cannot already have the status of matched or timed-out in the system of the receiver. A cancellation of a confirmation is successfully processed when the cancellation could be carried out, i.e. the referenced trade has been taken out of the matching queue and has received the status "cancelled" I the receiving system.

Note that the rejection document will also be used to indicate a time-out of a trade confirmation to the originator of the confirmation. In this case, the rejection document is not sent out as a response to a received document, the sending is triggered by an internal event in the system.

V.4. LEGAL AND CONFIDENTIALITY ISSUES

For the legal validity of the electronic documents, EFET refers to the Master Agreement in place between participants for the legal issues. The Master Agreement will typically describe the legal specifications of electronic transactions.

Similarly the Master Agreement should contain a confidentiality clause applying to the trade confirmation data sent over to counter parties.

VI. DOCUMENT TYPES & ATTRIBUTES

Important Note

"RELEASE 1.0" of the EFET ECM framework focuses on physical fixed-price power forward contracts for delivery in UK and Continental Europe. Later releases will take floating priced, options, gas, and more complex structured trades into account.

The business document types identified so far are thus:

- Trade Confirmation Document
- Cancellation Document
- Trade Confirmation Authentication Document
- Rejection Document (both for invalid documents and timed-out trade confirmations)
- Acknowledgement Document

There are three types of fields:

- Mandatory: The field has to be filled in
- Conditional: The field has to be filled in if applicable
- Optional: The field doesn't have to be filled in

Generic data to be contained in all document types will typically be Sender ID, Receiver ID, Sender Role, Receiver Role, Time Stamp etc…

VI.1. CONFIRMATION DOCUMENT

The concept of "Key & Information Fields"

The EFET ECM standards shall include the definition of Key Fields. The introduction of the concept of key and informational fields will define the "meaning and scope" of an authentication or match result document.

In the case of the use of Central Matching Service provider, a match document sent by a Central Matching Service provider shall mean that the key fields of the confirmations to which the match document refers are identical. The key fields of two confirmations will thus have to be identical for the Central Matching Service to report a match on those two confirmations.

In the case of exchange of confirmations through a peer-to-peer connection, an authentication document sent by one of the two parties and related to the confirmation of the other party, shall mean that this party agrees on all key fields of the other party's confirmation document. A party will thus check the Key fields of a confirmation before replying with an authentication document on that confirmation.

Name	**Mandatory / Optional / Conditional**	**Key / Information**	**Description**
Document Header			
Document ID	Mandatory	Information	Unique reference as generated by the trade capture system of the sender.
Document Version	Conditional	Information	Version number is entered when present trade confirmation is an amendment to a previously sent one.
Sender ID	Mandatory	Information	Unique identifier for party who sends the document and as such confirms a trade.
Receiver ID	Mandatory	Information	Unique identifier for party who receives this trade confirmation document.
Receiver Role	Mandatory	Information	Either "central matching service provider" or a "trader" (=principal).
Trade Details			
Trade Type	Mandatory	Key	E.g. fixed physical, index physical, swap, call option…
Commodity	Mandatory	Key	E.g. Active Power, gas …
Market	Mandatory	Key	The market of delivery of the underlying commodity. Usually country, but can be different in the U.K., e.g. "England & Wales", "Scotland", …
Delivery Point	Mandatory	Key	Location of delivery (Hub)
Buyer	Mandatory	Key	Unique identifier for buyer
Seller	Mandatory	Key	Unique identifier for seller
Load Type	Mandatory	Key	E.g. peak, base, off peak…
Agreement	Mandatory	Key	Master Agreement under which trade has been executed.
Capacity Unit	Mandatory	Key	Unit in which capacity is expressed
Currency	Mandatory	Key	Currency in which price is expressed
Total Volume	Mandatory	Key	Total volume delivered over total delivery period expressed in capacity unit*hour. Basically capacity*number of hours of delivery.
Trade Date	Mandatory	Key	Date on which trade has been executed
Broker	Conditional	Key	Broker platform on which the trade has been executed.

			Only relevant for a broker trade.
Buyer Energy Account	Conditional	Key	Consumption or production account, only to be specified for England and Wales.
Seller Energy Account	Conditional	Key	Consumption or production account, only to be specified for England and Wales.
Notification Agent	Conditional	Key	Party responsible for notifying the transaction to the Energy Contract Volume Aggregation Agent (ECVAA) for England and Wales. Mandatory for this market.
Transmission charges	Conditional	Key	Indicates how transmission charges are allocated. The requirements are either Schedule 5 on or Schedule 5 off. This only applies to the England and Wales market, but is mandatory for this market.
Trade Time	Optional	Information	Time on which trade has been executed
Trader Name	Optional	Information	Name of trader having executed trade in originator company.
Comment	Conditional	Information	General free text field
TIME INTERVAL QUANTITIES (1-N)			
Delivery Start Date & Time	Mandatory	Key	Start date and time of delivery period
Delivery End Date & Time	Mandatory	Key	End date and time of delivery period
Contract capacity	Mandatory	Key	Contract capacity in capacity unit
Price	Mandatory	Key	Price per capacity unit*hour

Table 1: Data model for trade confirmation document.

VI.2. AUTHENTICATION DOCUMENT

VI.2.1. CONFIRMATION MATCHING TROUGH A CENTRAL SERVICE PROVIDER

An authentication document sent by a central matching service provider, means that **the Central Matching Service provider certifies that the primary and secondary KEY fields of the confirmation document referred to match those of a counter party confirmation document**.

See also figure 4 on next page.

The document should contain at least the following information:

- Unique Document Identifier (unique for the Central Matching Service Provider)
- REFERENCE party Confirmation identifier and version number
- COUNTERPARTY party Confirmation identifier and version number
- Information fields from COUNTERPARTY Confirmation[1]

VI.2.2. PEER-TO-PEER AUTHENTICATION[2]

An authentication document sent by a counterparty, means that **the counterparty agrees with ALL KEY fields of the confirmation document referred to**.

An authentication document sent by one of the two parties always relates to the (previously sent) confirmation of the counter party. It therefore means that this party agrees on all key fields of the other party's confirmation document. A party will thus check if he agrees on all Key fields of the other party confirmation before replying with an authentication document.

See figure 5 on next page.

The document should contain at least the following information:

- Unique Document Identifier (unique for the Sender)
- REFERENCE party Confirmation identifier and version number
- COUNTERPARTY party Confirmation identifier and version number
- Information fields from COUNTERPARTY Confirmation[3]

---

[1] If a service provider is not able to deliver an authentication message, which includes the other party's confirmation information fields, this might be temporarily accepted.

[2] Note that the authentication message is almost the same message as the match message from a technical point of view. However, they are both part of a different business scenario.

[3] On one hand, if the receiver of the authentication message received the other party confirmation prior to the authentication, the receiver needs the unique document identifier to find back the other party confirmation and make the link between both documents.

Document Header		
Document ID	Mandatory	Unique for the sender for this type of message.
Sender ID	Mandatory	Unique identifier identifying the Party who sends this document and thus 1) certifies that a counterparty confirmation has been received matching the reference confirmation, in the case of a matching through a central matching service or 2) authenticates the reference confirmation, in the case of peer-to-peer communication.
Sender Role	Mandatory	Either a central matching service provider or a "trader" (=principal).
Receiver ID	Mandatory	Unique identifier of the party who receives this message, and who has previously sent the trade confirmation message that now is authenticated.
Reference Confirmation Document Identifier		
Reference Document ID	Mandatory	Referencing your confirmation tradeID on which an authentication is reported.
Reference Document Version	Mandatory	Referencing the version number of the confirmation on which an authentication is reported.
Counterparty Trade Details		
CounterParty ID	Mandatory	Unique identifier for party who sends the document and as such confirms a trade.
Counterparty Document ID	Mandatory	Referencing the confirmation of the other party and to which your confirmation matches.
Counterparty Version	Mandatory	Referencing the confirmation of the other party and to which your confirmation matches.
Trade Time	Optional	Time on which trade has been executed according to the counterparty.
Counterparty Comment	Optional	Comments from counterparty trade confirmation document.
Counterparty Trader Name	Optional	Name of counterparty trader having executed trade.

Table 2: Data model for authentication document.

On the other hand, if he did not receive the other party confirmation document prior to the authentication or if he discarded it, he needs within the authentication document, the information fields of the other party confirmation for later reference.

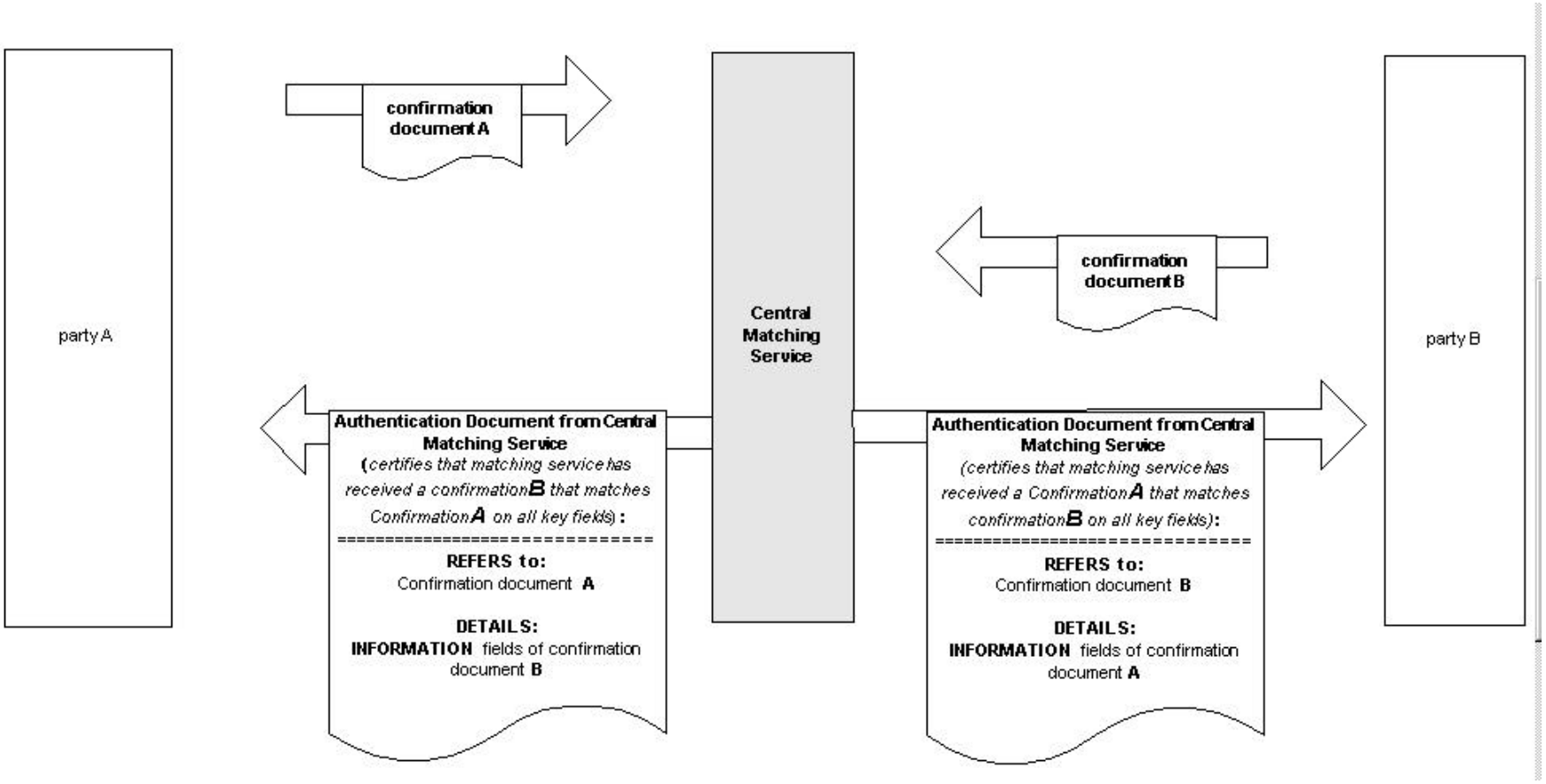

Figure 4 - Content of authentication document in case of matching through a central matching service provider

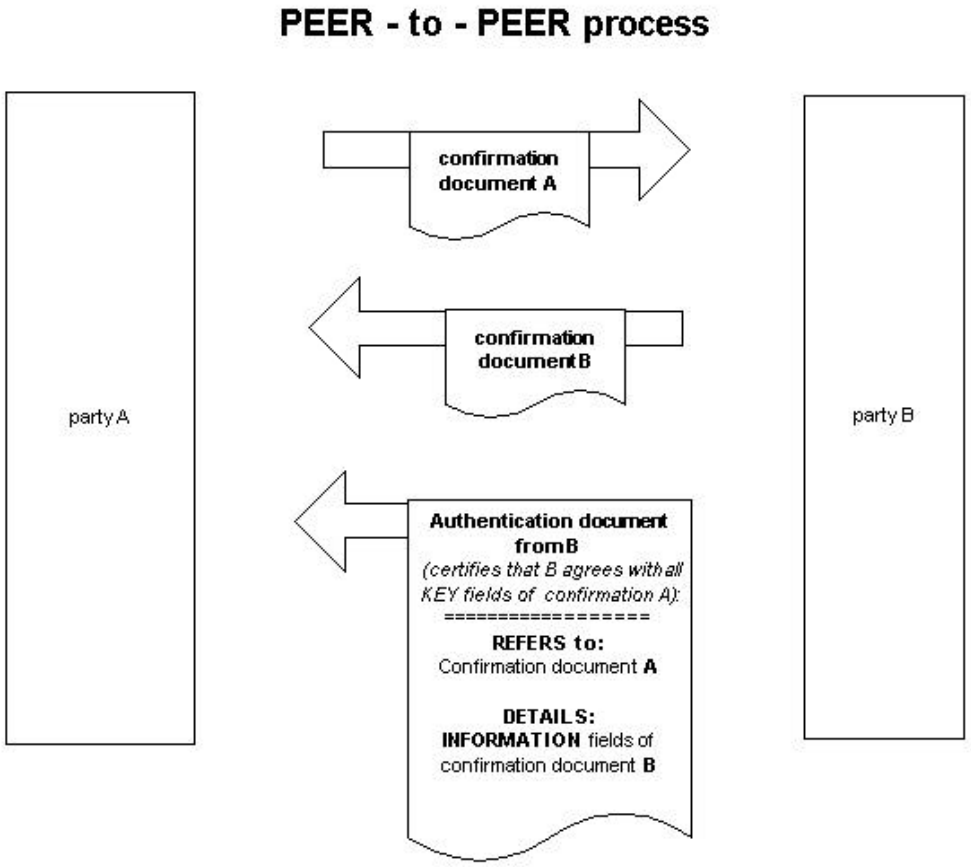

Figure 5 – Content of authentication document in case of P2P

VI.3. CANCELLATION DOCUMENT

A Cancellation Document always refers to a trade confirmation document and is used to inform the receiver of the sender's desire to remove the trade confirmation document from their system.

A Cancellation Document should therefore contain at least the following information:

- The sender ID
- The Document ID and version of the trade confirmation that needs to be cancelled

Document Header		
Document ID	Mandatory	Unique for the sender for this type of message.
Sender ID	Mandatory	Unique identifier of the party who sends this message.
Receiver ID	Mandatory	Unique identifier of the party who receives this message, and who has previously sent the trade confirmation message that needs to be cancelled.
Referenced Document Identifier		
Reference Document ID	Mandatory	Referencing your confirmation document ID that you want to cancel.
Reference Document Version	Mandatory	Referencing the confirmation version that you want to cancel.

Table 3: Data model for cancellation document.

Important note: Because of the fact that the cancellation document has a very similar structure to the authentication document, they will be combined into one document in the technical implementation (Document 5). A document type will distinguish which of the two documents is meant.

VI.4. REJECTION DOCUMENT

A rejection messages can be used to:

- Report a time-out of a trade confirmation to the owner of that trade confirmation
- Report to the sender of a trade confirmation, authentication or cancellation document that the document sent was invalid because of:
    - Invalid XML message structure,
    - Invalid codes etc….
- Report to the sender of a trade confirmation, authentication or cancellation document that the document sent could not be processed correctly because:
    - The cancellation/authentication sent referred to a confirmation document that was not found
    - The confirmation sent had the same document ID as another confirmation previously received and already processed etc…

A Rejection document should contain at least the following information:

- Receiver, i.e. the sender of the rejected message
- Document Type of the rejected message (Deal confirmation, Authentication or Cancellation)
- Unique Identifier of message that is rejected
- Version number of the document that is rejected (Note that only deal confirmation have version numbers.)
- Reason for Rejection

Document Header		
Document ID	Mandatory	Unique for the sender for this type of message.
Sender ID	Mandatory	Unique identifier of the party who sends this message.
Receiver ID	Mandatory	Unique identifier of the party who will receive this rejection document, and who has sent the document that is being rejected.
REFERENCE Document Identifier		
Reference Document ID	Mandatory	The ID of the document that is being rejected.
Reference Document Version	Conditional	Only in the case of the rejection of a trade confirmation document for a reason other than time-out. Referencing the document version of the confirmation that was rejected.
Reference Document Type	Mandatory	The document type of the document that is being rejected/acknowledged
REASON (0…N)		
Error Code	Mandatory	Code giving the reason for rejection: • Invalid format • Time-out • Trade confirmation already matched • …
Error Text	Optional	Text describing the reason for rejection

Table 4: Data model for rejection document.

VI.5. ACKNOWLEDGEMENT DOCUMENT

An acknowledgement document is to be used to report that a document has been well received and processed correctly:

- A confirmation document is in the "matching" queue (see documents 3 and/or 6)
- The confirmation update document (a version number different from zero) has correctly replaced the formerly received confirmation document in the "matching" queue.
- A cancellation document has led to the removal of a confirmation document from the "matching" queue.

Thus no acknowledgement is to be sent after reception of an acknowledgement or a rejection document!!

An acknowledgement document should contain at least the following information:

- Receiver Party ID, i.e. the sender of the message that is being acknowledged
- Document Type of the rejected document
  (Trade confirmation, Authentication or Cancellation)
- Unique Identifier of the document that is acknowledged
- Version number of the document that is acknowledged
  (Note that only trade confirmation have version numbers)

REFERENCE Document Identifier		
Receiver ID	Mandatory	Unique identifier of the party who will receive this acknowledgement document, and who has sent the document that is being acknowledged.
Reference Document Type	Mandatory	The document type of the document that is being acknowledged.
Reference Document ID	Mandatory	The ID of the document that is being acknowledged.
Reference Document Version	Conditional	Only in the case of the acknowledgement of a confirmation document. Referencing the document version of the confirmation that was acknowledged.

Table 5: Data model for acknowledgement document.

Important note: Because of the fact that the acknowledgement message has a very similar structure as the rejection message, they will be combined into one message in the technical implementation (Document 5). A message type will distinguish which of two messages is used.