ACER
Agency for the Cooperation of Energy Regulators

# Draft RMM requirements

*Annamaria Marchi and Tomaž Zaplotnik*

**Roundtable meeting on REMIT implementation with associations of energy market participants**

**Ljubljana, 21-22 May 2014**

ACER
Agency for the Cooperation of Energy Regulators

# Outline

- Draft Implementing Acts
- Overview of registration Process
- ACER assessment of compliance
- Technical description of registration process
- Technical description of reporting process

# Draft REMIT Implementing Acts

## Article 11
## Technical and organisational requirements and responsibility for reporting data

*In order to ensure efficient, effective and safe exchange and handling of information the Agency shall after consulting reporting parties develop technical and organisational requirements for submitting data.*

*The requirements shall foresee mechanisms:*

*a) to ensure the security, confidentiality and completeness of information,*
*b) to identify and correct errors in data reports,*
*c) to authenticate the source of information,*
*d) to ensure business continuity.*

*The Agency shall assess whether reporting parties comply with the requirements. Reporting parties who comply with the requirements shall be registered by the Agency. Entities listed under the first subparagraph of Article 6(5) shall not be subject to requirements under this Article.*

# Who shall register?

Any entity reporting trade and / or fundamental data to ACER:

- Market participants
- Organised market places
- ENTSOs
- TSOs
- LSOs
- SSOs
- Third parties reporting on behalf of the above entities
- Trade repositories?
- Approved reporting mechanisms?

However, Article 6(10) draft Implementing Acts:
*In relation to the reporting of information referred to in this article, the Agency shall, after consulting the reporting parties concerned, define electronic formats for the submission of information […]*

# Overview of registration process

| | |
|---|---|
| IDENTIFICATION | • MPs - CEREMP<br>• Others – online identification form (similar to Sec. 1 &2 of MPs form)<br>• ACER verifies identity and issues credentials |
| TECHNICAL SPECS | • Login with ACER's credentials<br>• Online signature of NDA<br>• Download technical specs |
| DECLARATION | • Declaration of fulfilment of requirements on security and timely transmission, input validation, output content, format & validation<br>• Undertaking to comply with other requirements |
| TESTING | • Reporting of data using test environment<br>• Successful reporting of a certain % of transactions per data type |
| REGISTRATION | • Credentials for access to production environment issued<br>• Registration process completed<br>• Reporting of data to production environment |

# Registration - Declaration that requirements are met / 1

**SECURE TRANSMISSION**

- Mechanism to ensure secure transmission of information to ACER, including:
  - Non- repudiation
  - Minimise risk of data corruption, unauthorised access and leakages during transmission

**TIMELY TRANSMISSION**

- Mechanism to ensure transmission within the deadlines indicated in IAs
- Business continuity mechanisms to ensure timely transmission in case of incidents

**VALIDATION OF INPUT**

- Guarantee certainty of:
  - Source of information created or collected by the RRM
  - Proper authorisation of person submitting info on behalf of MP
- No significant risk of corruption in input process
- Check transactions reports for completeness, identify omissions and obvious errors, request and / or initiate re-transmission of any such erroneous or missing reports

# Registration - Declaration that requirements are met / 2

**OUTPUT FORMAT**

- Ability to report data in format defined by ACER
- Commitment to adapt the reporting processes as required by ACER (e.g. format updates, data quality improvement, etc.)

**OUTPUT CONTENT**

- The report must contain information prescribed in the Implementing Acts

**OUTPUT VALIDATION**

- Possibility for MPs to receive information on what data was reported and on the outcome of the reporting process.

# Registration - Undertakings

**DISRUPTION**

- Undertaking to inform ACER without delay if operations are disrupted
- Undertaking to provide ACER within 5 working days with a report on the reasons for disruption and actions taken to prevent future incidents
- Ability to demonstrate that no information was unreported or lost

**SECURITY BREACH**

- Undertaking to immediately notify ACER of the breach
- Undertaking to provide ACER within 5 working days with a report on the reasons for security breach and actions taken to prevent future incidents

**CONTACT PERSONS**

- Provide ACER with names and contact details of staff in charge of assisting ACER with its regulatory responsibilities
- Undertaking to timely update such contact details

# Assessment of compliance

**RESPONSE TO ACER REQUEST**

- Undertaking to timely reply to ACER's requests for clarification concerning application and / or operation of the RRM
- Undertaking to provide information / evidence ACER may request concerning application and / or operation of the RRM

**ONGOING COMPLIANCE**

- Undertaking to meet requirements at all time
- Periodic renewal of registration OR
- Annual report to be provided on request

Supported by external audit report based on ACER's audit plan

ACER may consult regulators and/or competent authorities that may be able to provide any clarification concerning the application / operation of the RRM and take into account any information which it considers appropriate to assess compliance with the requirements

# Technical description of the registration process

1. The registration will be entirely electronic and done online.

2. First part of the registration process (Identification) will be done using CEREMP (for MPs) or Reporting Entity Registration Tool (for other reporting entities).

3. A user account will have to be created with ACER before any registration information can be submitted.

4. The user account form will have to be filled in with information about the user, the company on whose behalf he/she is acting and the details for further communication (e.g. valid email address).

5. After successful creation of the user account the reporting entity identification form will have to be filled in with information about the potential RRM. For MPs CEREMP information will be used and for other reporting entities a form similar to Sections 1 & 2 of CEREMP Registration form will be used.

# Technical description of the registration process

6. After identification of reporting entity is complete and ACER approves the submitted information as valid, the email will be sent to the contact for communication with the instructions on how to proceed with the registration. Credentials will be provided to access ARIS User Registration System.

7. When the person responsible for reporting (RRM Account Administrator) logs on to ARIS User Registration System the following information will have to be provided:

   - information necessary to identify the user (e.g. name, surname, company, email);
   - information necessary to create the account (e.g. username, password);
   - digital certificate issued to the user;
   - written application to register as RRM signed by a legal representative;
   - written authorisation to the user that he acts on behalf of the RRM (e.g. as an employee) signed by a legal representative.

# Technical description of the registration process

8. After the RRM Account Administrator submits all the necessary information and the Agency approves that the information is complete and accurate the new RRM System Account will be created. Both the contact for communication and the RRM Account Administrator will be notified via email.

9. When the RRM Account Administrator logs on with the RRM System Account the following information will have to be provided:

   - information about which interfaces will be used by the RRM
   - information about the type of data that will reported by the RRM
   - information about the scope of the reporting (e.g. own behalf vs. other's behalf, estimated data volume that will be reported)
   - information about testing (e.g. time slot, duration, test certificates and keys)
   - information about the start of reporting
   - information about how the RRM can fulfil the technical and organisation requirements for data submission (a declaration)

# Technical description of the registration process

10. The user logged on with an RRM System account will be able to access all the technical documentation about data submission (subject to NDA).

11. When the RRM successfully completes the testing of data submission process within the ARIS testing environment and when the Agency approves that the provided information is complete and accurate, the registration of the RRM is accepted. The notification email is sent to contact for communication and RRM Account Administrator.

12. The last remaining step is related to creation of RRM credentials for accessing the ARIS production environment. Accounts for particular interfaces will have to be created and production certificates and keys will have to be provided. Only after this step the RRM registration process will be considered as completed.

# Technical description of the reporting process

Prerequisites for reporting:

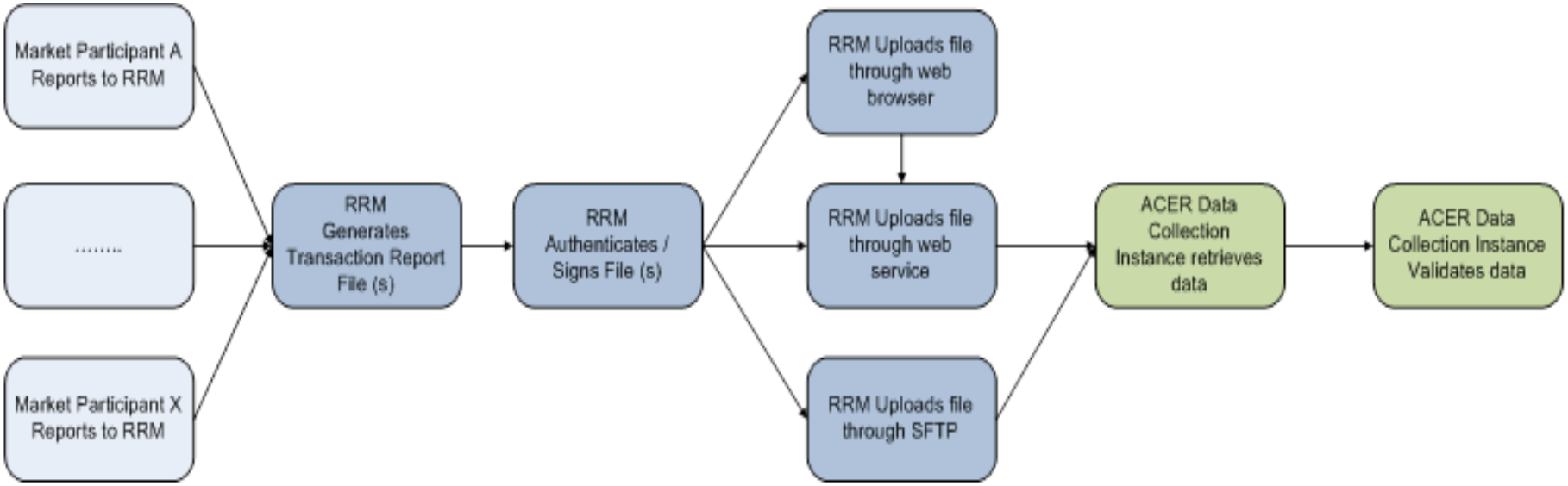
- Registration finalised
- Certificates issued/obtained
- PGP keys generated and signed by ACER
- Accounts/credentials created
- Interfaces in place
- Testing completed
- Data available

# Technical description of the reporting process

## Inbound data flow:

At least 1 file shall be submitted by the RRM containing the transactions being reported. If a RRM has no transactions to report, then no submission is required; however, a submission with no entries is also accepted.

The RRM can submit multiple transaction report files. Each file must be identified in sequence and submitted sequentially by the RRM.

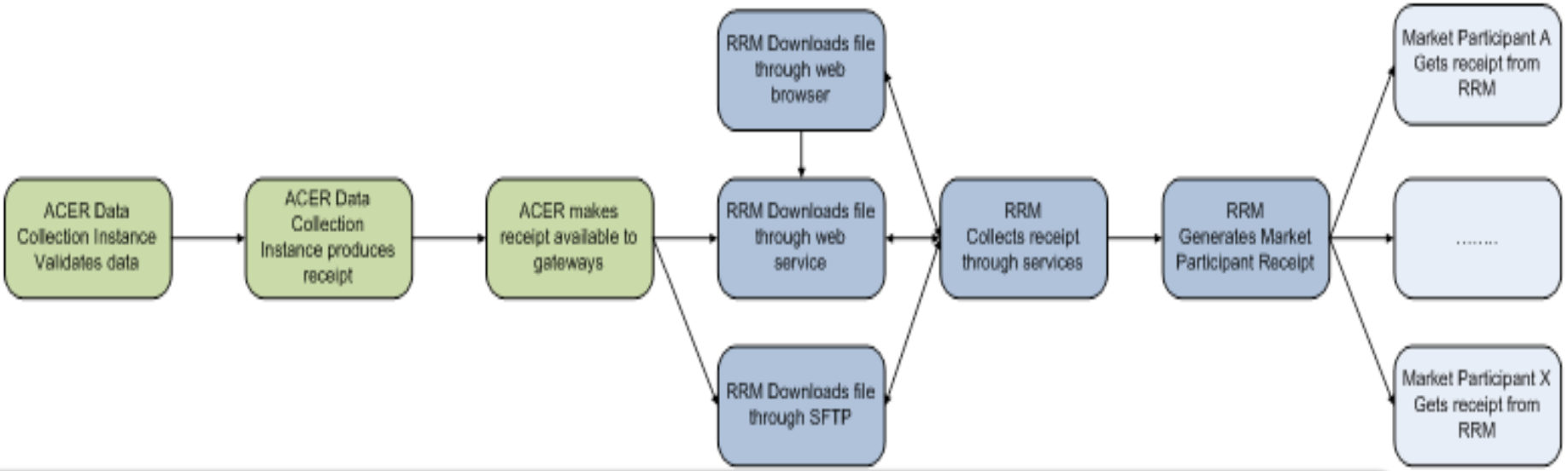


# Technical description of the reporting process

## Outbound data flow:

ACER shall produce a receipt for each report file submitted by a reporting RRM.

Receipts will be issued to confirm acceptance/rejection of the submitted file as well as every particular logical record (e.g. transaction, order) within the file.



# Main principles

Secure Data Submission - Through each of the defined interfaces, the reporting RRMs are guaranteed security through international standards for secure communication over the internet, either through a secure web service or through secure shell data transfer.

Flexible Data Submission – ACER accepts that each RRM may support different standard technologies for submission of data and has therefore attempted to consider the most standard platforms for data submission only to reduce overhead of defining and implementing any new protocols for data submission.

Quality Data Submission – The number of transactions and the variety of data that is available means that a data quality assurance consideration must be included in the definition. ACER have defined a strongly typed interface that can be easily validated against standard formats by the reporting RRMs and by ACER.

# Main principles

Valid Data Submission – upon receipt of data from RRMs, ACER shall validate the technical and functional quality of the data and identify to RRMs any items submitted that do not conform to the standards and specifications laid out.

Minimal Changes – ACER makes considerations that any changes to the interface, either technically or functionally, may cause additional cost to the RRM or market participants. The use of industry standard interfaces and the use of a flexible data format means that participants RRM will not be as affected by possible changes to the system and also that the number of required changes following implementation will be minimal.

# Interfaces

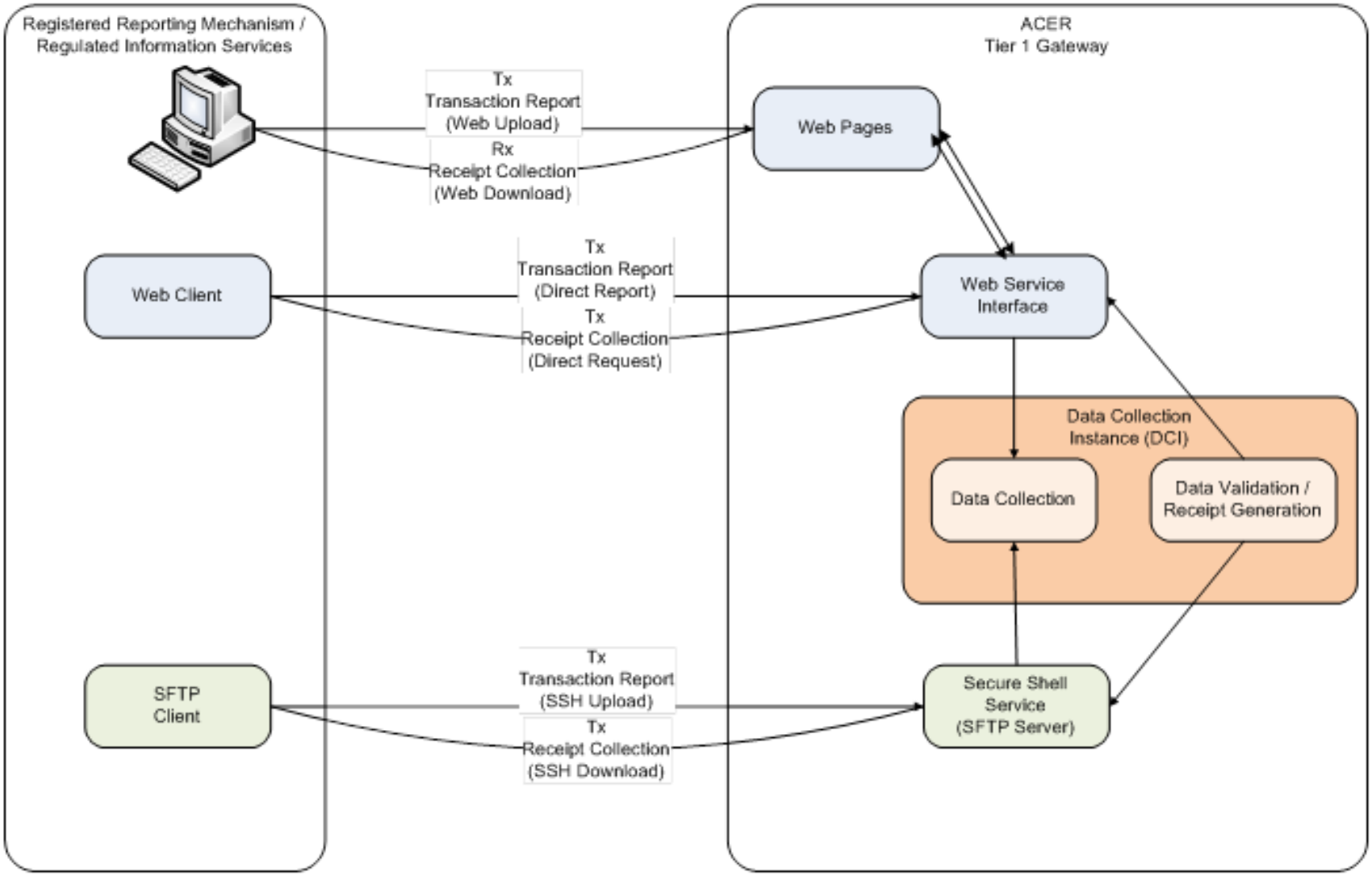
RRMs shall be able to provide transaction reports to ACER through the following interfaces:

- Static file upload via SFTP using SSH authentication
- Automated file upload via secure web services
- Interactive user uploads through the RRM reporting web interface

RRMs shall be able to access receipts for reported transactions to ACER through the following interfaces:

- Static file download via SFTP using SSH authentication
- Automated file download via secure web services
- Interactive user download / viewing through the RRM reporting web interface

# Interfaces


Registered Reporting Mechanism / Regulated Information Services
ACER Tier 1 Gateway
Tx Transaction Report (Web Upload)
Rx Receipt Collection (Web Download)
Web Pages
Web Client
Tx Transaction Report (Direct Report)
Tx Receipt Collection (Direct Request)
Web Service Interface
Data Collection Instance (DCI)
Data Collection
Data Validation / Receipt Generation
SFTP Client
Tx Transaction Report (SSH Upload)
Tx Receipt Collection (SSH Download)
Secure Shell Service (SFTP Server)

# Data validation

| | File / Record / Event Uniqueness | Completeness | Accuracy | Consistency / Integrity | Participant Identification | Comment |
|---|---|---|---|---|---|---|
| **File Naming Convention Validation** | X | | | X | | Every filename is unique. Sequential numbering is the simplest solution. |
| **Signature & Encryption Validation** | | | | X | X | |
| **Schema Compliance** | | X | | X | | |
| **Data Duplication Checks** | X | | | X | | Duplicated data coming from the same reporting entity. |
| **Double Reporting Validation Check** | X | | X | X | | Duplicated data coming from different reporting entities. Some duplication may be allowed. |
| **Participant Identifier Validation** | | | | X | X | *A* says the trade was with *B*, *B* says the trade was with *C* or doesn't say anything. |

# Data validation

| | File / Record / Event Uniqueness | Completeness | Accuracy | Consistency / Integrity | Participant Identification | Comment |
|---|---|---|---|---|---|---|
| **Correcting or Updating an Existing Transaction Validation** | X | X | X | X | | Lifecycle events including modify and cancel events. |
| **Dates and Times Validation** | | X | X | X | | Many different validation rules, some also simple and basic (e.g. trading in the future) |
| **Product Code Type Validation** | | X | X | X | | Mainly for standard trades. |
| **Field Integrity Compliance** | | X | X | X | | E.g. physically settled contract without a delivery profile |
| **Organised Market Sequencing Data Compliance** | X | X | X | X | | Data from organised markets is crucial and they have means to quickly correct errors. |

X – unconditional rejection if validation fails, X – conditional rejection if validation fails

# Data integrity

- On Agency side the RRM's electronic signature of the submitted file will guarantee that it is always possible to verify the integrity of the reported data and the source of the data, provided that the submitted file and public PGP key of the reporting entity are kept. Validity of the digital signature can be checked anytime.

- On RRM side the Agency's electronic signature of the receipt issued for a submitted file will guarantee that it is always possible to verify the integrity of the reported data, provided that the original file, the receipt and the public PGP key of the Agency are kept. The integrity of the reported data can be checked by calculating a hash value of the original file and comparing this value to the hash value in the receipt after validating the electronic signature of the receipt. If the values match the integrity of the reported data is confirmed.

# Non-repudiation

- On Agency side the RRM's electronic signature of the submitted file will ensure that the origin of the report can be ascertained. The Agency's electronic signature of the receipt will ensure that the origin of the receipt can be ascertained, including acknowledgement of what was actually received (with the use of file hash). Submitted file, the receipt and the public PGP key of the RRM will be kept by the Agency.

- On RRM side the Agency's electronic signature of the receipt will ensure that the origin of the receipt can be ascertained, including acknowledgement of what was actually received (with the use of H1 hash). The submitted file and the receipt should be kept by the RRM. The RRM should also keep the original unencrypted and unsigned XML file to be able to prove what was submitted independently, without the assistance of the Agency. By keeping the original unencrypted and unsigned XML file, the submitted file, the receipt and the public PGP key of the Agency, the RRM can always prove what data was submitted to the Agency and what was the final outcome of the reporting process (e.g. acceptance, rejection, etc.).

# Non-repudiation & reconciliation

- On Market Participant side the only way to achieve non-repudiation independently, without the assistance of the Agency or the RRM, is to require from the RRM the copy of the receipt issued by the Agency and referring only to information reported for that particular Market Participant. The Agency's electronic signature of the receipt will ensure that the origin of the receipt can be ascertained, including acknowledgement of what was actually submitted on behalf of the Market Participant (with the use of hash for each logical record). By keeping the receipt and the public PGP key of the Agency, the Market Participant can always verify that the integrity of the data submitted by the RRM has been preserved and that the Agency received and processed the data.

# Non-repudiation & reconciliation

- Market Participant can calculate the hash values of the logical records in his own database and compare them with the hash values in the receipt. It is assumed that every Market Participant maintains a full database of reportable information as it is a responsibility of a Market Participant to know which actions (e.g. trading, etc.) result in creation of reportable information. By comparing the calculated hash values of logical records in his own database with the hash values included in the receipt (for each particular record) the Market Participant can ascertain which records were reported and what was the outcome of the reporting process (e.g. acceptance, rejection) for every particular record.

# Data retention and handling

- ACER shall only maintain data received from RRM and receipts provided in return to RRM for a maximum of 45 days.

- After 45 days, all files within the inbound or outbound directories for a RRM will be purged that are older than the 45 days. This means that any file which has been received more than 45 days ago will be removed from the system.

- ACER will keep all transaction reports provided by RRM internally within the ACER system for a period of 5 years for full traceability of transaction reporting, however, these reports will no longer be accessible to the RRM through the defined interfaces.

- If a RRM has not collected a transaction report receipt prior to the date of purging of the receipt file, a request can be made to ACER to retrieve the receipt file from the archives. It is believed that sufficient time within the 45 days has been given for all reporting parties to retrieve their transaction report receipts during this time.

ACER
Agency for the Cooperation of Energy Regulators

# Providing feedback

Please provide comments to

Remit.roundtable@acer.europa.eu

by end of May

ACER
Agency for the Cooperation of Energy Regulators

# Thank you for your attention!

**www.acer.europa.eu**