CONSEIL INTERNATIONAL DES GRANDS RESEAUX ELECTRIQUES
INTERNATIONAL COUNCIL ON LARGE ELECTRIC SYSTEMS

STUDY COMMITTEE D2
INFORMATION SYSTEMS AND TELECOMMUNICATION

http: //d2.cigre.org
/

2017 Colloquium
September 20 to 22, 2017
Moscow – RUSSIA

Preferential Subject N°- PS2: Resilience to cyber threats of information and telecommunication systems in the power industry

« MADES (Market Data Exchange Standard): Create a secure and reliable communication platform for European electricity market »

Antony ENG and Patrick BOURDON
RTE
FRANCE
Antony.eng@rte-france.com

Capability of the power industry to resist to cyber threats is becoming a growing concern for all parties. Indeed, TSOs, PXs, and market operators are exchanging an increasing amount of data related to market, network, and operations. The exchanges are speeding up and the period within which these information need to be exchanged and tackled is shorten every day, mainly because parties are trying to maximize and optimize the use of their infrastructure (by dealing more and more with short term process for example).

All these data are thus becoming more and more critical and traditional communication protocols (such as E-mail, SFTP, SCP, …) may not be sufficient anymore. That's why parties are trying to agree on a shared, secure and reliable way to exchange information. Such a communication platform should offer all security commitments (guarantee on the sender and receiver authentication and on the payload) and it needs also to offer good performance, to be relatively easy to deploy and to be scalable.

In order to fit all these requirements, European TSOs worked on the MADES initiative (**MA**rket **D**ata **E**xchange **S**tandard): the idea is to create a communication platform which allows single, common, harmonized and secure exchange of messages between TSOs and European Electricity Market Participants. This solution also reduces the cost of building different IT platforms to exchange data with all the parties involved.

This paper will therefore cover:

- Detailed description of MADES and focus on the used security layers.
- Presentation of a MADES implementation: Energy Communication Platform software, and examples of deployments within Europe.
- Limitation of MADES v1.1 and current improvement work done in ENTSO-E (main modification is the integration of AMQP v1.0 in MADES v2.0 for highly improving the performance of the solution).

The aim of this paper is to present the MADES initiative and to share the advantage of having a unified and secured communication platform. The paper will focus on the main security principles:

- Confidentiality - Any message shall be readable only by the recipient.
- Authentication - The sender and the receiver of any message shall be unambiguously identified.
- Non-repudiation of the messages – it shall be possible to unambiguously prove that the sender sent the message and that the recipient received it.
- Non-alteration of the messages - the content of a message is not altered during the delivery process (integrity).
- Encryption - All communication routes shall be encrypted.