Data security - Penetration testing

Data security of smart meters

With the installation of huge quantities of smart meters enabling various types of communication, the need for protection of all the data involved becomes crucial. Here not only the protection of data from the user to a head end system is important, but also the vulnerability of the smart meters themselves needs to be minimised. The question is: are modern smart meters protected sufficiently against possible attacks to alter data or to affect the measurement process? How can you be sure that those devices, installed in their millions, are fully safe, now and in the future?

In a number of countries local requirements on data protection and security are being developed. Some of the documents focus on particular aspects of the utility meters, others cover also the communication chain between meter and head end system. In order to standardise the different requirements the SM-CG (Smart Meters Coordination Group) Task Force on Privacy and Security together with ESMIG wrote a document "Minimum security requirements for AMI (Advanced Metering Infrastructure) components". This document, being published by CEN/CENELEC/ETSI, contains a set of generic minimum requirements that are valid for most of the European Member States.

MINIMUM SECURITY REQUIREMENTS

The document focuses on the technical aspects concerning the components and communication links of the AMI. The minimum requirements also serve as a basis to specify the security certification scheme for the AMI components. The SM-CG has investigated various approaches applied in Member States for security certification and concluded that it would be beneficial to have a common approach in order to support the European internal market. The specification of the security certification scheme is typically based on a set of security objectives which can easily be derived from the minimum requirements.

The document contains the following main requirements:

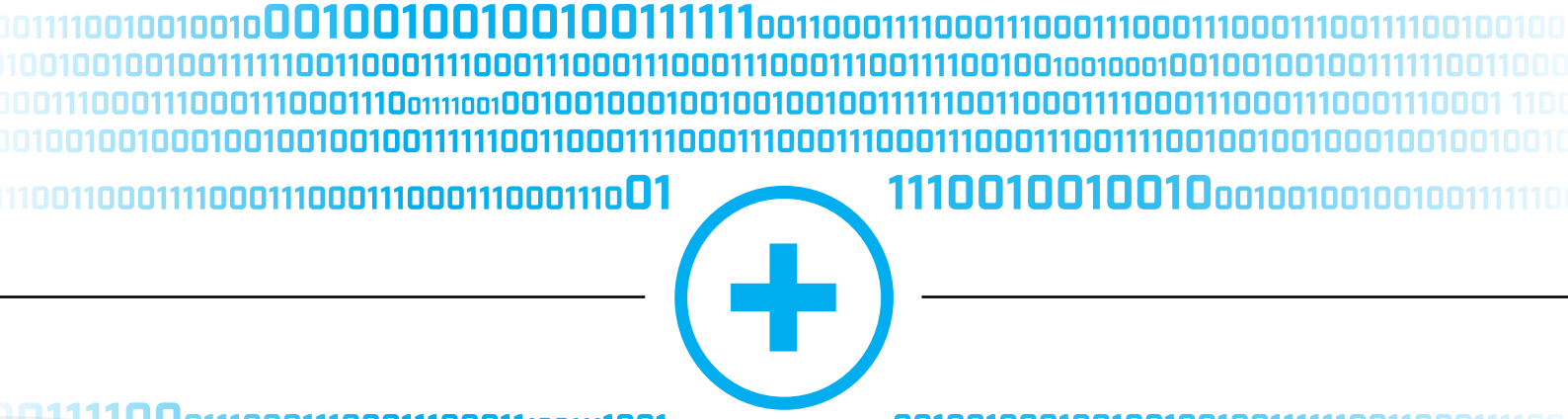
A. All AMI components SHALL provide a log of security events;
B. All data exchanges SHALL take place in a (end-to-end) secure manner;
C. Availability of the system (AMI components and communication network) SHALL be sufficient to perform the Use Cases the system has been designed for;
D. Crypto mechanism and key management SHALL be documented and be compliant with recognized/proven and approved open standards;
E. Every AMI component SHALL check the authorisation of any entity requesting access to it and grant or deny access based on the result of that check;
F. Data at rest SHALL be protected in all system components;
G. AMI components SHALL be upgradable to incorporate new (security) functionalities;
H. Functionalities in AMI components SHOULD be limited to the intended operational Use Cases and SHALL not be able to compromise security functions;
I. AMI components and the communications network SHALL be adequately protected against external disturbances and/or attacks and SHALL demonstrate resilience against attacks.

TESTING DATA SECURITY AT NMi

At NMi, smart meters and other AMI components can be examined in accordance with the CEN/CENELEC/ETSI document on the minimum requirements. The examination is performed while using a specific test environment, being developed in cooperation with the German company Exceeding Solutions. During the tests, the level of data protection of the meters under test is examined, by checking the meters with all the required tests. This includes penetration testing on all possible communication ports, a check of the event loggers as well as the applied crypto mechanism and so on. The results of the examination are presented in a report listing the outcome for each individual test.

INTERESTED?

If you are interested in the examination of smart meters and other AMI components, we are happy to answer all your questions. Please feel free to contact us at nmi@nmi.nl. On our website, you can find more information about our services.



TRUE VALUE

www.nmi.nl

T +31 (0) 88 636 23 32
E nmi@nmi.nl