**Annex 4**

**"Smart Meter Security"**

1. **Foreword**

The aim of this annex is to provide a list of security requirements regarding design and implementation so as to prevent and limit possible security issues concerning Smart Meters in relation to the relevant regulations.

1. **Security requirements**

The security requirements outlined in this document aim to address the main vulnerabilities of the Smart Meter system that could be used to create disruptions, alter normal intended operations and/or leak information.

The **security** **requirements** are listed below:

|  |  |
| --- | --- |
| **No.** | **Security requirements** |
| **1** | The device must be configured so that only the system administrator can create new roles or assign privileges. |
| 2 | The device supplied must include security measures to prevent the parameters of the device from being controlled or changed without proper user authentication. |
| **3** | The device or software supplied enabling profiling and the assignment of privileges must include security measures preventing the user from controlling or changing the device parameters, unless envisaged. This requirement must be verified by means of Penetration Testing conducted by a qualified third party. |
| **4** | The device supplied must include security measures for managing user access and authorisation (role-based access control model), as well as user sessions. In addition, the Supplier must provide Italgas with the results of Penetration Test activities carried out by a qualified Third Party to demonstrate compliance with this requirement. |
| **5** | The device supplied must allow use of authorised communication channels only:   * DLMS Protocol * The use of wi-fi connections via hotspots is not permitted * The use of "ad hoc" (static) wi-fi connections must include a time of use, an activation button and an inactivity timeout (maximum 1 minute). The wi-fi network must use a WPA2 protocol with a minimum key length of 16 characters (at least 1 upper case, at least 1 lower case, at least 1 special character, at least 1 number) * The use of "ad hoc" (static) Bluetooth connections must include a time of use, an activation button and an inactivity timeout (maximum 1 minute). |
| **6** | The device must allow firmware upgrades exclusively via the Italgas network, remotely and, if not possible, locally, and by an Italgas user. |
| **7** | The Supplier must provide mechanisms on the device to verify the integrity and authenticity of the firmware (e.g. digital signature mechanisms using the root of trust on the device). |
| **8** | The Supplier must digitally sign, via an authorised and recognised CA, the firmware of the device. The signature must be sent to Italgas for verification before distribution. The installation of firmware the same as or older than the version on the device must not be permitted. |
| **9** | The Supplier must disable debug interfaces (RS232, JTAG, UART, etc.) after the devices have been correctly configured in production and in the field. |

Please fill-in the attached excel file.



1. **Right of the Client**

Italgas reserves the right to carry out security audits also by means of Vulnerability Assessment, Penetration Test, Software Static and Dynamic Analysis, or by verifying the security level of the firmware against attempts at reverse engineering.