

# NET2GRID

# Security Statement

## Table of contents

- Introduction
- Table of contents
- Introduction
- User Security
- SmartCloud Security
- Platform Security

## Introduction

NET2GRID is serious about the concerns of users considering security and privacy. This is the reason we strive to store our users' data in the most secure manner and separate the storage of personal data and metering data.

This document is intended to provide the readers with a transparent view of our security infrastructure and creating a peace of mind about the security of their data.

## User security

NET2GRID employs several technologies for internet and networking security in the process of communicating with users and the storage of users' data.

- User are obligated to sign-in with a user name and a password. The password is stored encrypted and can not be read or decrypted by NET2GRID employees.
- The secure section of the web site, like myNET2GRID, the forum and the SmartApp communication, are encrypted using SSL (Secure Sockets Layer).
- There is a strict separation between personal data and the data that is sent by the SmartBridge into the SmartCloud. This means that metering data and personal data is stored on different servers and in other databases.

## SmartCloud Security

- The NET2GRID servers that establish our SmartCloud are located in Europe in several secure data centers. These data centers are in physically secured buildings with a strict security policy to rule out unauthorized physical or logical access to the servers. The buildings are manned and guarded 24/7.
- All server rooms are only accessible with valid key cards and all access to server rooms is logged. The individual server racks are secured with locks and logical access controls.
- The data centers are equipped with fully redundant IP-connections and several independent connections with internet service providers.
- Each server has redundant internal and external power supplies.

## Platform security

- All our servers are secured by firewalls. Only ports 53 (DNS), 80 (HTTP) and 443 (HTTPS) are open.
- Intrusion detection systems are active to prevent unauthorized access to the servers.
- We use monitoring software to intensively monitor the stability and health of the platform.
- All operating and application systems have the latest security updates installed.
- Our platform applications are code in PHP5 and are running on MySQL, Apache and CentOS Linux.
- The software development is done using a stable framework and clear coding standards.