GRIDPOCKET

Expérience projets H2020

Filip GLUSZAK, CEO

Paris 20 juin 2019

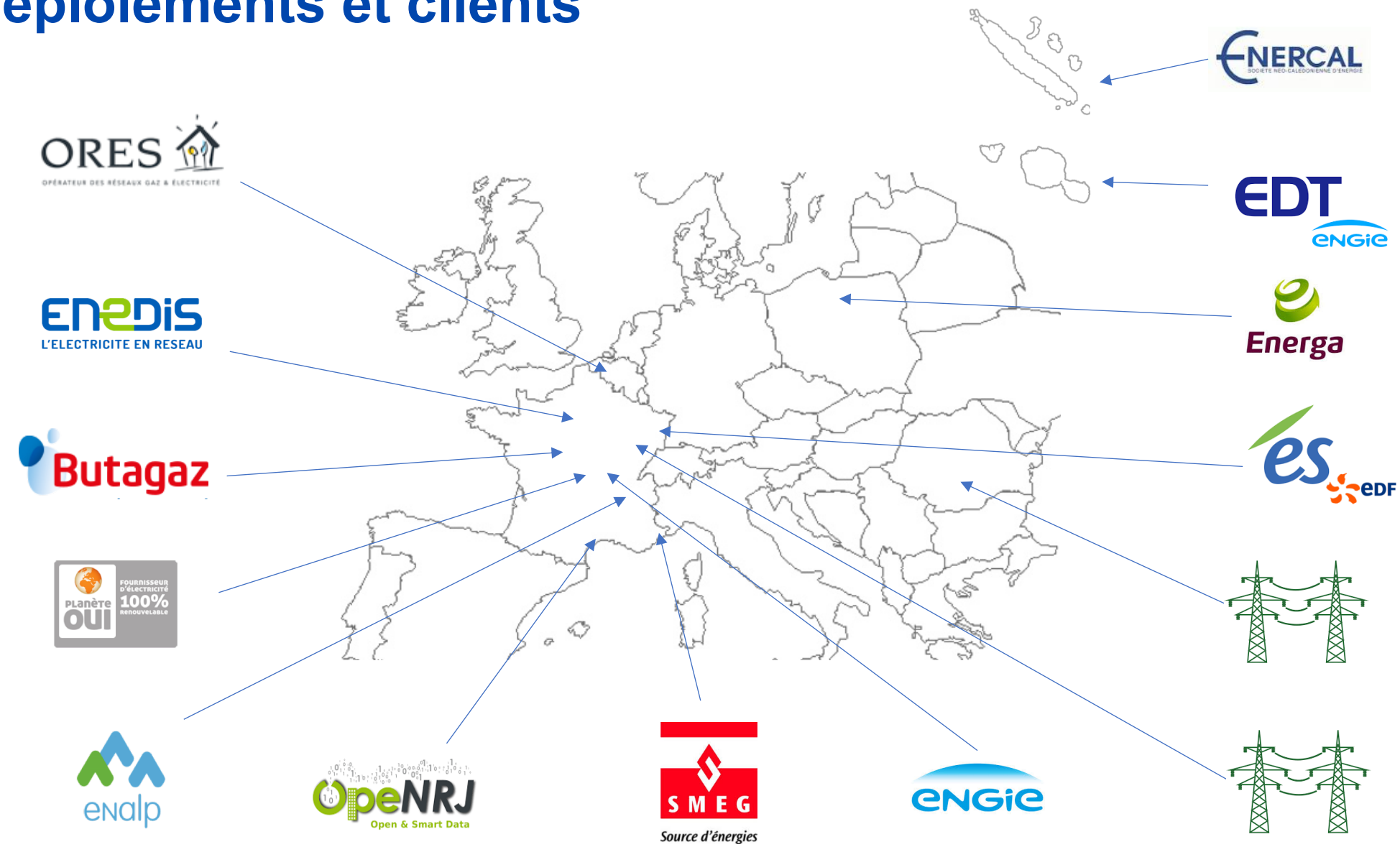
Plate-forme marque blanche de services clients pour utilities avec l'électricité, gaz, eau, chaleur

PME Innovante, 25 personnes, siège à Sophia-Antipolis, bureau en Pologne

- Smart metering and energy efficiency B2C & B2B
- Artificial Intelligence, revenue generation for utilities
- CXP, behavioural engagement and gamification
- Demand response and auto-consumption
- Electric car, smart home and renewable energy

GRIDPOCKET

Déploiements et clients



GRIDPOCKET

Activités recherche

DEFeND – Security and GDPR

C3ISP – Infrastructures security

DR BOB – Demand response

SMESEC – Infrastructures security

Emilie – Energy efficiency and gamification

GreenFeed – EV Energy Management System

IOStack – Big data

OpeNRJ – Open data platform

GridTeams – Gamification

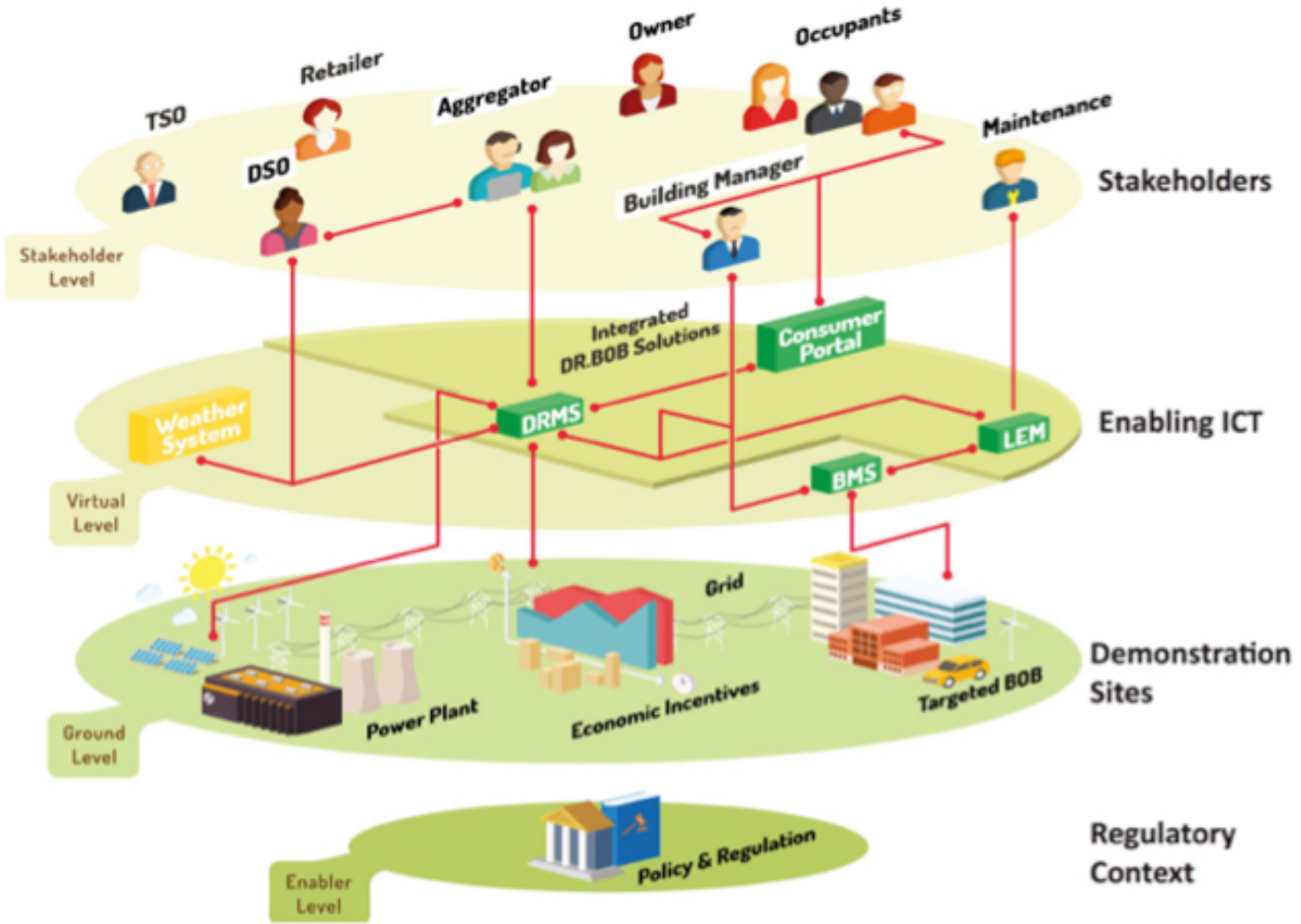
SME Innovation Instrument Phase I - Efficiency

BigFoot – Big data

DR-BOB

Effacement à l'échelle de groups de bâtiments

Demand Response for Blocks of Buildings



UK Pilot Site: Teesside University

French Pilot Site: Anglet business park

Italian Pilot Site: Fondazione Poliambulanza Hospital

Romanian Pilot Site: Technical University of Cluj-Napoca

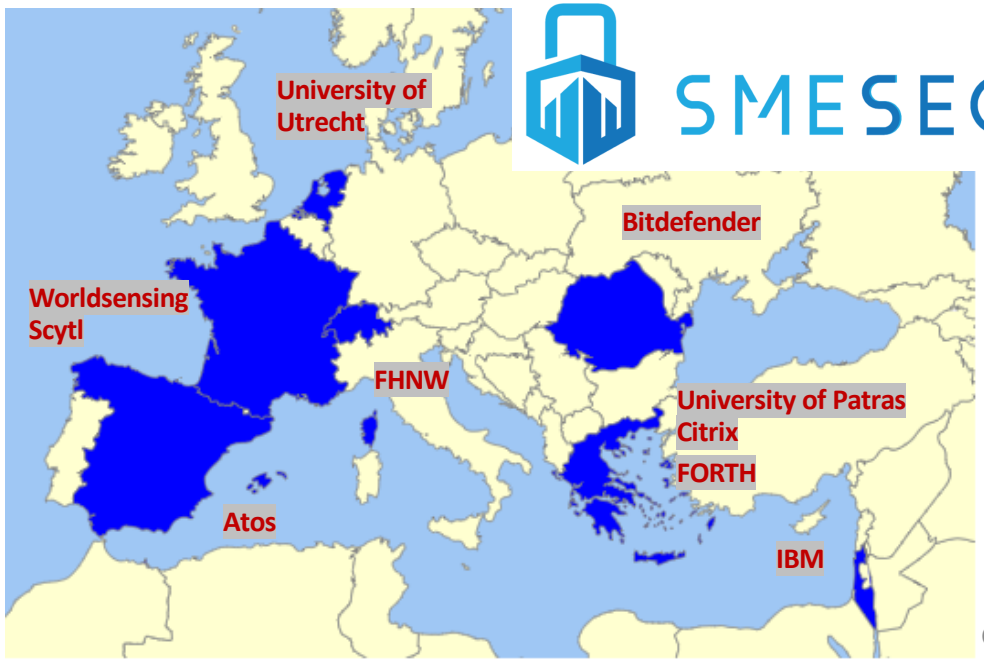
GridPocket's contribution: Consumer Portal for Demand Response

4 pilots

Cybersecurity for Small and Medium-Sized Enterprises

SMESEC : Lightweight framework for cybersecurity. 13 protection components and 4 pilots (E-vote, Smart Vity, IoT, Smart Grid)

GridPocket : Specification, integration and validation of the framework in Smart Grid Pilot

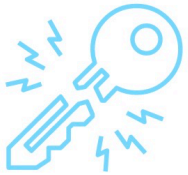


Distributed Denial of Service (DDoS)

An attacker controls many computers that overload a server. Impact: the server is slow or shuts down completely.

Using Known Vulnerable Components

An attacker scans a system for well-known vulnerabilities of legacy components. Impact: arbitrary code may be executed.



Broken Access Control

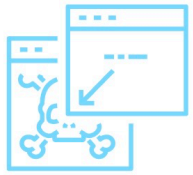
An attacker obtains passwords or sessions. Impact: access to only one or a few accounts may compromise a system.

Security Misconfiguration

An attacker accesses default accounts, unused pages, or unprotected files. Impact: unauthorized access to data or functionality.

Injection

An attacker sends hostile data to an interpreter (SQL, LDAP, etc.). Impact: data loss, corruption, or disclosure.



Cross Site Scripting (XSS)

An attacker lets another user execute malicious code, e.g. with a fishing mail. Impact: stolen credentials, sessions, or

Sensitive Data Exposure

An attacker steals keys or data, e.g. because the data or keys were not sufficiently encrypted. Impact: compromised data.

Garbage Data

An attacker enters or sends irrelevant or objectionable content ("Spam"). Impact: burden for filtering the relevant data.

Internal Threats (Malicious Insiders)

Privileged users, third-parties, and terminated employees may inadvertently or maliciously use data for personal gain,

GRIDPOCKET

GRIDPOCKET

GridPocket SAS
300 route des Crêtes
06560 Sophia-Antipolis
France

+33 (0) 9 510 68 802
contact@gridpocket.com

www.gridpocket.com

7