SealedGRID

Project ID: 777996
Funded under: H2020-EU.1.3.3. - Stimulating innovation by means of cross-fertilisation of knowledge

Scalable, trustEd, and interoperAble pLatform for sEcureD smart GRID

From 2018-01-01 to 2021-12-31, ongoing project

Project details

<table>
<thead>
<tr>
<th>Total cost:</th>
<th>Topic(s):</th>
</tr>
</thead>
<tbody>
<tr>
<td>EUR 1 080 000</td>
<td>MSCA-RISE-2017 - Research and Innovation Staff Exchange</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>EU contribution:</th>
<th>Call for proposal:</th>
</tr>
</thead>
<tbody>
<tr>
<td>EUR 1 080 000</td>
<td>H2020-MSCA-RISE-2017 See other projects for this call</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Coordinated in:</th>
<th>Funding scheme:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Greece</td>
<td>MSCA-RISE - Marie Skłodowska-Curie Research and Innovation Staff Exchange (RISE)</td>
</tr>
</tbody>
</table>

Objective

The rapid evolution of ICT has revealed the potential for centrally monitoring, controlling, and optimising the power grid. In this context, a more intelligent, responsive, and efficient, system has been devised, known as the Smart Grid (SG). As explained in the EU Third Energy Package the SG will support a dynamic two-way information exchange between utility companies and their customers, contributing towards a smart and sustainable energy management in Europe and the establishment of a wiser energy consumption mentality. However, besides the benefits of such an endeavour, the power grid will be exposed to security threats inherited from the ICT sector, while privacy issues and new vulnerabilities, related to the specific characteristics of the SG infrastructure, will emerge. The problem is assessed as crucial, if we consider that a potential attack to the SG may lead to cascading failures, ranging from destruction of other interconnected critical infrastructures to loss of human lives. Thus, the development of a security platform tailored to the SG is required, that i) can efficiently manage the plethora of SG nodes, ii) deal with potential malicious hardware or software modifications due to the physical access of the customers to the SG nodes, and iii) operate over heterogeneous systems. Considering all the above, SealedGRID aims at bringing together experts from industry and academia from cross-sectorial research areas having complementary background with the long-term goal to design, analyse, and implement a scalable, highly trusted and interoperable SG security platform. The platform will combine, for the very first time, technologies like Blockchain, Distributed Hash Tables, Trusted Execution Environments, and OpenID Connect, while for its realization the SealedGRID consortium is committed to a fully-integrated and multi-disciplinary secondment programme combined with a set of networking, dissemination, and exploitation activities.

Related information
Coordinator

UNIVERSITY OF PIRAEUS RESEARCH CENTER
GR. LAMPRAKI 122
185 32 PIRAEUS
Greece

EU contribution: EUR 270 000

Activity type: Higher or Secondary Education Establishments
Contact the organisation

Participants

UNIVERSIDAD DE MALAGA
AVDA CERVANTES, NUM. 2
29016 MALAGA
Spain

EU contribution: EUR 270 000

Activity type: Higher or Secondary Education Establishments
Contact the organisation

BEIA CONSULT INTERNATIONAL SRL
STREET POIANA NARCISELOR 12 1ST FLOOR APARTMENT 3 SECTOR 1
010158 BUCURESTI
Romania

EU contribution: EUR 270 000

Activity type: Private for-profit entities (excluding Higher or Secondary Education Establishments)
Contact the organisation

NEUROSOFT SOFTWARE PRODUCTIONS SA
466 HRAKLEIOU AV N HRAKLEION
141 22 ATHENS
Greece

EU contribution: EUR 270 000

Activity type: Private for-profit entities (excluding Higher or Secondary Education Establishments)
Contact the organisation

Last updated on 2018-01-24
Retrieved on 2019-08-14

© European Union, 2019