



**Personal Energy Administration Kiosk application:**  
an ICT-ecosystem for Energy Savings  
through Behavioural Change, Flexible Tariffs and Fun  
**Contract No 695945**

## **Deliverable D7.3:** **Privacy and Security Advisory Board** **System Specification Approval Letter**

## Motivation

Cyber Security is a topic of highest priority in PEAKapp. The project consortium itself includes dedicated specialists on this topic, being involved in large-scale research activities with respect to cyber security of smart grids and smart metering (e.g. EI-JKU is partner of the SPARKS<sup>1</sup> project). To have institutionalised supervision of the project's activities to ensure cyber security of the ICT-to-Human ecosystem, the project established a Privacy and Security Advisory Board (PSAB). The PSAB is led by Alberto Stefanini, acknowledged contributor to the *European Union Agency for Network and Information Security* (ENISA) report<sup>2</sup> on "Smart Grids Task Force Deliverable: Proposal for a list of security measures for smart grids" and his CV is found in the Appendix of this Deliverable.

In addition to Cyber Security, PEAKapp collects fine-grained electricity consumption data and includes functionalities allowing consumers to post specific data on platforms like Facebook, and therefore requires careful supervision of legal experts and privacy specialists. In PEAKapp, the consortium members together with the Privacy and Security Advisory Board agreed on the set of graphs and figures that can be posted by users. Furthermore, the user has the ability to deactivate Facebook posting altogether.

The analysis of privacy related and legal aspects was organized by Dr. Kathrin de Bruyn, project manager and WP leader of a significant number of national and European projects (e.g. she is leader of the legal and social acceptance WP in the FP 7 SPARKS - <https://project-sparks.eu>, and key legal expert in the Austrian national project RASSA - <http://www.ait.ac.at/themen/smart-grid-security/rassa/>) on the issue of smart metering and smart grid data protection.

The subsequent Letter was issued by the PSAB to PEAKapp and confirms careful consideration of the above mentioned issues.

---

<sup>1</sup> The research project SPARKS (Smart Grid Protection Against Cyber Attacks, FP7 grant number 608224)

<sup>2</sup> Find the report e.g. on <http://tinyurl.com/lhokdjg>.

## Privacy and Security Advisory Board System Specification Approval Letter

The research and innovation project PEAKapp aims at the development and testing of a software system dedicated to household customers to trigger lasting energy savings through behavioural change and continuous engagement, to enable increased consumption of clean and low-priced electricity from the spot market for household customers, to connect them to social networks, and to motivate them through serious gaming.

The PEAKapp system comprises a backend engine installed on the servers of electricity companies (retailers or DSOs) that collects and processes the electricity load profiles of households and a smart phone app displaying certain aggregates thereof to the user. The functionalities available to the app user are described in the public Deliverables 1.2 (Documentation of functionalities – system specification) and 1.4 (Documentation of functionalities – Serious Game specification), and can both be downloaded from <http://www.peakapp.eu/public-deliverables/>.

Considering household-specific data is collected and processed by the PEAKapp system, careful consideration of privacy and data security is paramount. The Privacy and Security Advisory Board has therefore scrutinized the procedures foreseen to ensure cyber security (task responsibility: Alberto Stefanini) for both, the hosting utilities and the households using PEAKapp. It was identified that the foreseen measures and procedures represent the state-of-the-art.

Additionally, the Privacy and Security Advisory Board has taken care that the information provided to households about the privacy related ramifications of participating in the field tests, and the consent forms for collecting their formal approval, represent the respective state-of-the-art (task responsibility: Kathrin de Bruyn).

To conclude, the Privacy and Security Advisory Board has no objections against providing PEAKapp to households.

Alberto Stefanini	Dr. Kathrin de Bruyn Senior Legal Expert Energieinstitut an der Johannes Kepler Universität Linz
-------------------	---

## Privacy and Security Advisory Board System Specification Approval Letter

The research and innovation project PEAKapp aims at the development and testing of a software system dedicated to household customers to trigger lasting energy savings through behavioural change and continuous engagement, to enable increased consumption of clean and low-priced electricity from the spot market for household customers, to connect them to social networks, and to motivate them through serious gaming.

The PEAKapp system comprises a backend engine installed on the servers of electricity companies (retailers or DSOs) that collects and processes the electricity load profiles of households and a smart phone app displaying certain aggregates thereof to the user. The functionalities available to the app user are described in the public Deliverables 1.2 (Documentation of functionalities – system specification) and 1.4 (Documentation of functionalities – Serious Game specification), and can both be downloaded from <http://www.peakapp.eu/public-deliverables/>.

Considering household-specific data is collected and processed by the PEAKapp system, careful consideration of privacy and data security is paramount. The Privacy and Security Advisory Board has therefore scrutinized the procedures foreseen to ensure cyber security (task responsibility: Alberto Stefanini) for both, the hosting utilities and the households using PEAKapp. It was identified that the foreseen measures and procedures represent the state-of-the-art.

Additionally, the Privacy and Security Advisory Board has taken care that the information provided to households about the privacy-related ramifications of participating in the field tests, and the consent forms for collecting their formal approval, represent the respective state-of-the-art (task responsibility: Kathrin de Bruyn).

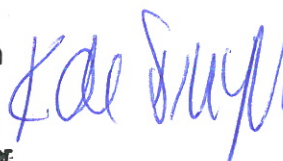
To conclude, the Privacy and Security Advisory Board has no objections against providing PEAKapp to households.

Alberto Stefanini



Dr. Kathrin de Bruyn

Senior Legal Expert  
Energieinstitut an der  
Johannes Kepler Universität Linz



## ANNEX 1: Curriculum Vitae of Alberto Stefanini



### Europass Curriculum Vitae



### Personal information

First name(s) / Surname(s) **First name(s) Surname(s) Alberto STEFANINI**

Address(es) **Via Tagliamento, 4 43036 Fidenza Italy**

Telephone(s) **+39.0524.84097** Mobile: **+39.3473640214**

Fax(es)

E-mail **alberto\_stefanini@virgilio.it**

Nationality **Italian**

Date of birth **May 12, 1949**

Gender **male**

### Work experience

- Consultant (since 2008)
- Contract Agent with the Joint Research Centre of the European Commission – Institute for Protection and Security (2004-2008)
- National Detached Expert, JRC (2004)
- Manager, Electrical System research, CESI (2000-03)
- Manager, Relations with R&D funding Institutions, Enel (1997-2000)
- Marketing manager, Energy products, CISE (1995-96)
- Section Leader, Artificial Intelligence, CISE (1983-1994)

Dates **See above**

Occupation or position held **Consultant (present – 2008). Since Oct 2012 partner of Novareckon knowledge brokers ([www.novareckon.it](http://www.novareckon.it)), a company to develop entrepreneurial and social ideas through best findings from European applied research, multidisciplinary knowledge systems and an international consulting network.**

Main activities and responsibilities	Since Jan. 2009 Alberto Stefanini retired as a full time employee, but keeps operating as an industry consultant. His clients include the EC DG Research, the Joint Research Centre of the EC, the It. National Research Council and Politecnico di Torino. His range of activities includes: <ul style="list-style-type: none"> <li>studies on smart grids, critical infrastructures protection, process control security and related standards, advanced automation, language technologies and their socio-economic impact</li> <li>dissemination, training and awareness activities on the above subjects</li> <li>preparation of project proposals on the above subjects under various funding schemes, included Horizon</li> </ul>																																		
Name and address of employer	-																																		
Type of business or sector	Energy automation																																		
<b>Education and training</b>	Master, Electronic Engineering (1974) Master, Classical Letters (2017)																																		
Dates	See above																																		
Title of qualification awarded	Laurea in Electronic Engineering																																		
Principal subjects/occupational skills covered	Computer Science, Communications, Automation, Engineering disciplines																																		
Name and type of organisation providing education and training	University of Bologna																																		
Level in national or international classification	Master (remove if not relevant, see instructions)																																		
<b>Personal skills and competences</b>																																			
Mother tongue(s)	<b>Specify mother tongue</b> (if relevant add other mother tongue(s), see instructions) Italian																																		
Other language(s)																																			
Self-assessment																																			
<i>European level (*)</i>																																			
<b>Language</b>	<table border="1"> <thead> <tr> <th rowspan="2"></th> <th colspan="2">Understanding</th> <th colspan="2">Speaking</th> <th rowspan="2">Writing</th> </tr> <tr> <th>Listening</th> <th>Reading</th> <th>Spoken interaction</th> <th>Spoken production</th> </tr> </thead> <tbody> <tr> <td>English</td> <td>good</td> <td>good</td> <td>good</td> <td>good</td> <td>good</td> </tr> <tr> <td>French</td> <td>average</td> <td>good</td> <td>average</td> <td>average</td> <td>good</td> </tr> <tr> <td>Spanish</td> <td>average</td> <td>good</td> <td>average</td> <td>average</td> <td>average</td> </tr> <tr> <td>Latin</td> <td>good</td> <td>good</td> <td>(usually) does not apply</td> <td>does not apply</td> <td>average</td> </tr> </tbody> </table>		Understanding		Speaking		Writing	Listening	Reading	Spoken interaction	Spoken production	English	good	good	good	good	good	French	average	good	average	average	good	Spanish	average	good	average	average	average	Latin	good	good	(usually) does not apply	does not apply	average
	Understanding		Speaking		Writing																														
	Listening	Reading	Spoken interaction	Spoken production																															
English	good	good	good	good	good																														
French	average	good	average	average	good																														
Spanish	average	good	average	average	average																														
Latin	good	good	(usually) does not apply	does not apply	average																														
	<i>(*) <a href="#">Common European Framework of Reference for Languages</a></i>																																		

Organisational skills and competences	<p>As a consultant he has recently set up a number of EU projects on matters regarding threat identification and prevention, formal methods, impact and harmonization of cyber security standards and security research with the CIPS EU programme and Horizon 2020. He has recently organized the final Conference of the project ESSENCE in Brussels, October 2014. Previously he worked as a contract Agent and as a National Detached Expert (2004) with the Joint Research Centre of the European Commission – Institute for Protection and Security of the Citizen until Nov. 2008. He organised the international workshop <i>The future of ICT for power systems: emerging security challenges</i>, Brussels, Feb. 2005. Until Sept. 2004, he was an assistant to CESI research director, held the job title of Scientific Manager, and was in charge of diffusion and take-up of research results. Until March 2003, he was responsible for research on the electrical system development. Very active with the framework programme since the seventies, he organized or contributed to organize some thirty EU projects on matters ranging from industrial diagnostics to power unit efficiency, man-machine interfacing, decision support, intelligent training and the life cycle of industrial automation.</p>
Technical skills and competences	<p>His recent activities include ESSENCE, a project to evaluate costs and benefits of applying emerging security standards to the European power grid controls systems, TIDES, a project to point out, assess and rank potential threats to critical infrastructures and to identify action plans to reduce the relevant risks, and FM BIASED, a project to evaluate the business impact of formal methods on application to security relevant devices. These projects were partly funded by the CIPS EU programme. At JRC, he was involved in a range of activities including: cyber security assessment of SCADA &amp; on-line process control systems, dissemination of relevant best practice, participation to standardisation efforts in this area, coordination of research activities EU wide on critical infrastructures and related subjects, modelling of antagonist threats to critical infrastructures with game theory and multi-agent systems. Over 2008, he made a study on the importance of Public-Private partnership to foster awareness of cyber security threats. In 2007, he was a major contributor to the launch of ESCoRTS, a European network for the Security of Control and Real-Time Systems. ESCoRTS is a joint endeavour of process control equipment manufacturers and process companies, under the lead of CEN, the European Committee for Standardisation. The project was funded by the FP7 security programme. Since Jan 2005 until March 2008, he was managing strategies &amp; dissemination in GRID, a EU Coordination Action on ICT vulnerabilities of Power Systems. In 2004 he worked as a national expert on detachment at JRC-IPSC where he performed a study on electric system vulnerabilities, based on analysis of recent blackouts.</p> <p>Until March 2003, he was responsible at CESI for research on the electrical system development: this included projects to enhance electricity transport capacity, to enforce electrical system security in the open market, and to introduce innovative monitoring and control equipment, for a total portfolio in excess of Euro 30 Mio. Previously, he co-ordinated participation of Enel Research in the European framework programme, and was actively involved in the launch of about 20 R&amp;D projects on diverse subjects, including management of technical and organisational knowledge, power generation monitoring and control, emission containment, electrical system security and control, final uses of electricity and intelligent metering. In 1998-99 he also liaised with US research on critical infrastructures, and coordinated energy technology transfer projects with Latin America and Mediterranean countries. He was very active with the European framework programme, and contributed to launch several European R&amp;D projects on industrial application of knowledge-based systems. In 1983-94 he established and led an Artificial Intelligence research group at CISE, focusing on the application of AI techniques to industrial problems. He started and led several European R&amp;D projects on knowledge-based support in process operation, engineering, learning, man-machine systems. In 1989-93 he was also involved in research programmes on Industrial Diagnostics and Artificial Intelligence Systems, sponsored by the Italian national Research Council, CNR. From 1976 to 1983 he worked with CISE, Telettra and as an independent consultant, mostly on the development of advanced process control and diagnostic equipment. He developed microprocessor based systems in the early years and was a designer of telecom equipment.</p>



---

Computer skills and competences	Professional experience in Artificial Intelligence applications (1983-94)
Driving licence	Italian driving licence



Additional information (Selected Publications)

*Elena Ragazzi and Alberto Stefanini (2015). Are security standards for electricity infrastructure a good choice for Europe? Evidence on cost and benefits from two case studies. To appear on IEEE Security & Privacy.*

*Bompard E., Napoli R., Russo A., Xue F., Masera M., Stefanini A. (2007). Analysis of malicious threats to infrastructures: a conceptual approach based on multi-agent systems. In: First annual IFIP working group 11.10 - International conference on critical infrastructure protection. New Hampshire, USA, Mar 19-21, 2007.*

*N. Hadjsaid, J. Rognon, R. Caire, A. Stefanini, M. Masera, N. Flataboe, G. Doorman, A. Morch, G. Kjolle, G. Oddbjorn, G. Dondossola, P. Friessem, M. Stoewer, G. Deconinck, G. Ruzzante (2007). ICT Vulnerabilities of Power Systems: A Roadmap for Future Research Office for Official Publications of the European Communities (Publ.), Luxembourg - ISBN 978-92-79-07138-6 (2007) - JRC42207*

*Bompard E., Gao C., Napoli R., Russo A., Masera M. and A. Stefanini (2007). The Analysis of Malicious Threats To Power Systems: a Conceptual Approach Based On Game Theory DNS - Dependability of Networked Systems Conference, June 2007.*

*Gardner R. M and A. Stefanini, Criticality and vulnerability of power system controls: the R&D needs. ECN, the European CIIP Newsletter, February-March 2007*

*Stefanini, A. (2006). Electric System Vulnerabilities: Lessons from Recent Blackouts and the Role of ICT. Technical EUR report EUR 21551 EN, March 2006.*

*Stefanini, A. (2006). The Future of ICT for Power Systems: Emerging Security Challenges. Technical EUR report, EUR 21740 EN, March 2006.*

*Stefanini, A. and E. Ciapessoni (2001). La Vulnerabilità del Sistema Elettrico come Infrastruttura Interdipendente. AEI - Rivista Ufficiale dell'Associazione Elettrotecnica Italiana, n. 88, Nov. 2001.*

*Stefanini A., Bertin, A., and F. Buciol, (1998). Towards industrial application of Intelligent Training Systems. Expert Systems, February 1998, Vol. 15, No. 1*

*Guida, G. and A. Stefanini, eds. (1992) Industrial Applications of Knowledge-Based Diagnosis. Elsevier. Amsterdam (1992).*

*Leitch, R. and A. Stefanini (1989). Task Dependent Tools for Intelligent Automation. International Journal of Artificial Intelligence in Engineering. 4 (1989), pp. 126-143.*

*Gallanti, M., Roncato, M., Stefanini, A. and G. Torielli (1989). A Diagnostic Algorithm based on Models at Different Level of Abstraction. 11th International Joint Conference on Artificial Intelligence, Detroit, August 1989.*

*R. R. Leitch and A. Stefanini (1989). Task Dependent Tools for Intelligence Automation, in Artificial Intelligence in Engineering, pp. 126 - 143, 1989.*

*Gallanti, M., Gilardoni, L., Guida, G. and A. Stefanini (1987). Exploiting Physical and Design Knowledge in the Diagnosis of Complex Industrial Systems. Advances in Artificial Intelligence-II, pp. 481-495. Elsevier Science Publishers B. V., 1987.*

*Gallanti, M., Guida, G., Spampinato, L., and A. Stefanini (1985). Representing Procedural Knowledge in Expert Systems: an Application to Process Control. 9th Int. Joint Conference on Artificial Intelligence, Los Angeles, Aug. 1985.*

---

## ANNEX 2: Curriculum Vitae of Kathrin de Bruyn

### Dr. Kathrin de Bruyn



#### Personal

**Vorname/Nachname** Kathrin de Bruyn  
**Telefon** +43-732/2468-5668  
**Fax** +43-732/2468-5651  
**E-Mail** [deBruyn@energieinstitut-linz.at](mailto:deBruyn@energieinstitut-linz.at)  
**Büro:** HF 325 Campus der JKU Linz

#### Education

---

09/2009-07/2011 Doktoratsstudium der Rechtswissenschaften, Johannes Kepler Universität Linz  
01/2009-04/2009 Fachanwaltslehrgang für Verwaltungsrecht bei der Deutschen Anwalt Akademie  
09/2006-06/2009 Rechtsreferendariat, Landgericht Düsseldorf  
10/2000-02/2006 Studium der Rechtswissenschaften, Ruhr-Universität Bochum

#### Positions

---

Seit 05/2014 Nebenberufliche Lektorin an der FH Wieselburg  
Seit 06/2011 Wissenschaftliche Mitarbeiterin der Abteilung Energierecht am Energieinstitut an der Johannes Kepler Universität Linz

#### Publications

---

##### Presentations (Selection):

*EnInnov 2012, 12. Symposium Energieinnovation der TU Graz, 16. Februar 2012, Vortrag: Rechtliche Darstellung der Power-to-Gas-Technologie in Österreich und Deutschland*

*Fachtagung "Aktuelle Fragen des Energierechts" an der Johannes Kepler Universität Linz, 04. Dezember 2012, Vortrag: Smart Grids – Rechtliche Aspekte von intelligenten Stromnetzen in Österreich*

*IEWT 2013, 8. Internationale Energiewirtschaftstagung an der TU Wien, 14. Februar 2013, Vortrag: Smart Grids in Österreich aus rechtlicher Sicht*

*EnInnov 2014, 13. Symposium Energieinnovation der TU Graz, 14. Februar 2014, Vortrag: Sara Fritz / Kathrin de Bruyn, Welche Auswirkungen hat eine gebäudeübergreifende Betrachtung von Solarthermie auf deren Wirtschaftlichkeit?*

*Fachtagung „Aktuelle Fragen des Energierechts“ an der Johannes Kepler Universität Linz, 01. Oktober 2015, Vortrag: Kathrin de Bruyn / Michael Schmidthaler, Forschungsprojekte zu Versorgungssicherheit und Blackouts*

#### **Contributions in Books and Journals (Selection):**

de Bruyn, Kathrin / Markl, Beatrice, Rechtliche Darstellung der Power-to-Gas-Technologie in Österreich und Deutschland, Kurzfassungsband zur EnInnov 2012, 12. Symposium Energieinnovation der TU Graz, 15.-17.02.2012, Graz

de Bruyn, Kathrin / Markl, Beatrice, Rechtsrahmen für Power-to-Gas fehlt, UmweltJournal 6/2012, S. 9

de Bruyn, Kathrin / Markl, Beatrice, Ausgewählte rechtliche Aspekte von Smart Grids in Österreich, in: Steinmüller, Horst / Hauer, Andreas / Schneider, Friedrich (Hrsg.), Energiewirtschaft Jahrbuch 2012, Neuer Wissenschaftlicher Verlag NWV, Wien / Graz 2012, S. 49-72

de Bruyn, Kathrin / Markl, Beatrice, Smart Grids in Österreich aus rechtlicher Sicht, Kurzfassungsband zur IEWT 2013, 8. Internationale Energiewirtschaftstagung an der TU Wien, 13.-15.02.2013, Wien

de Bruyn, Kathrin, Ökostromförderung und Territorialitätsprinzip: Keine Pflicht zur Förderung von in einem anderen Mitgliedstaat erzeugtem Ökostrom, ZTR 1/2015, S. 29-44

de Bruyn, Kathrin, Smart Metering und Strafrecht, in: Steinmüller, Horst / Hauer, Andreas / Schneider, Friedrich (Hrsg.), Energiewirtschaft Jahrbuch 2015, Neuer Wissenschaftlicher Verlag NWV, Wien / Graz 2015, S. 33-56

de Bruyn, Kathrin, Strafrechtliche Aspekte im intelligenten Stromnetz, in: Göllner, Johannes / Langer, Lucie / Tischlinger, Matthias, Smart Grid Security Guidance (SG)<sup>2</sup>, Schriftenreihe der Landesverteidigungsakademie, Wien 2016