

DATA PROTECTION IMPACT ASSESSMENT

Smart Grid and Smart Metering Systems

Ewa Piatkowska

ewa.piatkowska@ait.ac.at

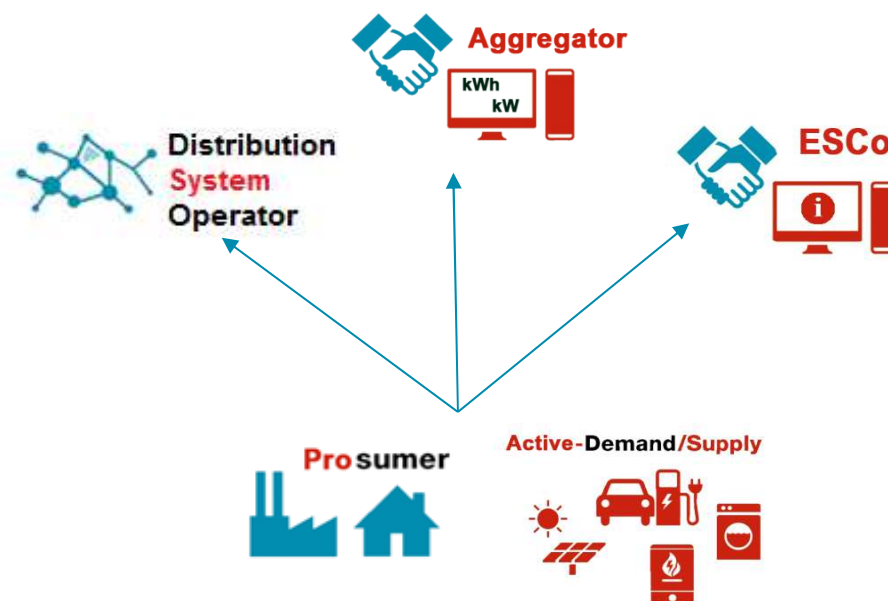
Centre for Digital Safety and Security

AIT Austrian Institute of Technology



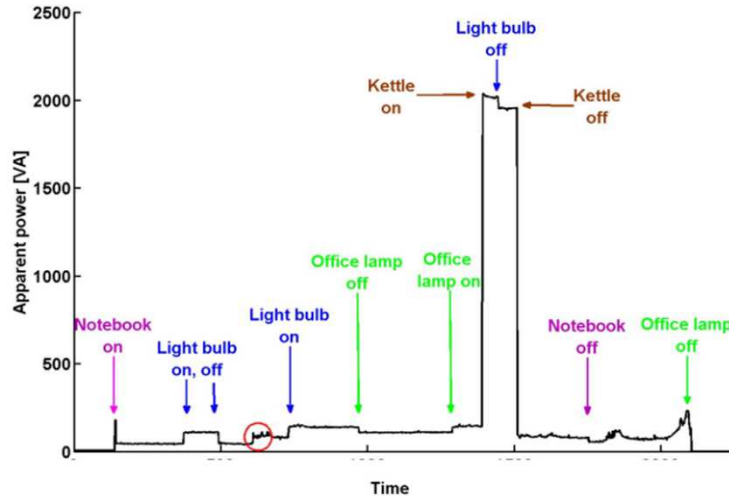
PRIVACY AND SMART GRID

- Large quantities of sensing data collected, processed and retained by smart grid stakeholders
- **Demand response** and flexibility services require high frequency data readings for profiling and forecasting
- Applications for energy consumption **monitoring** and **analysis**



PRIVACY AND SMART GRID

Smart Grid data reveal **personal details** about one's behaviour at home



M. Weiss, A. Helfenstein, F. Mattern and T. Staake, "Leveraging smart meter data to recognize home appliances," *2012 IEEE International Conference on Pervasive Computing and Communications*, Lugano, 2012, pp. 190-197.

Smart Hacking For Privacy : What TV shows you watch ?

Monday, January 09, 2012 Mohit Kumar

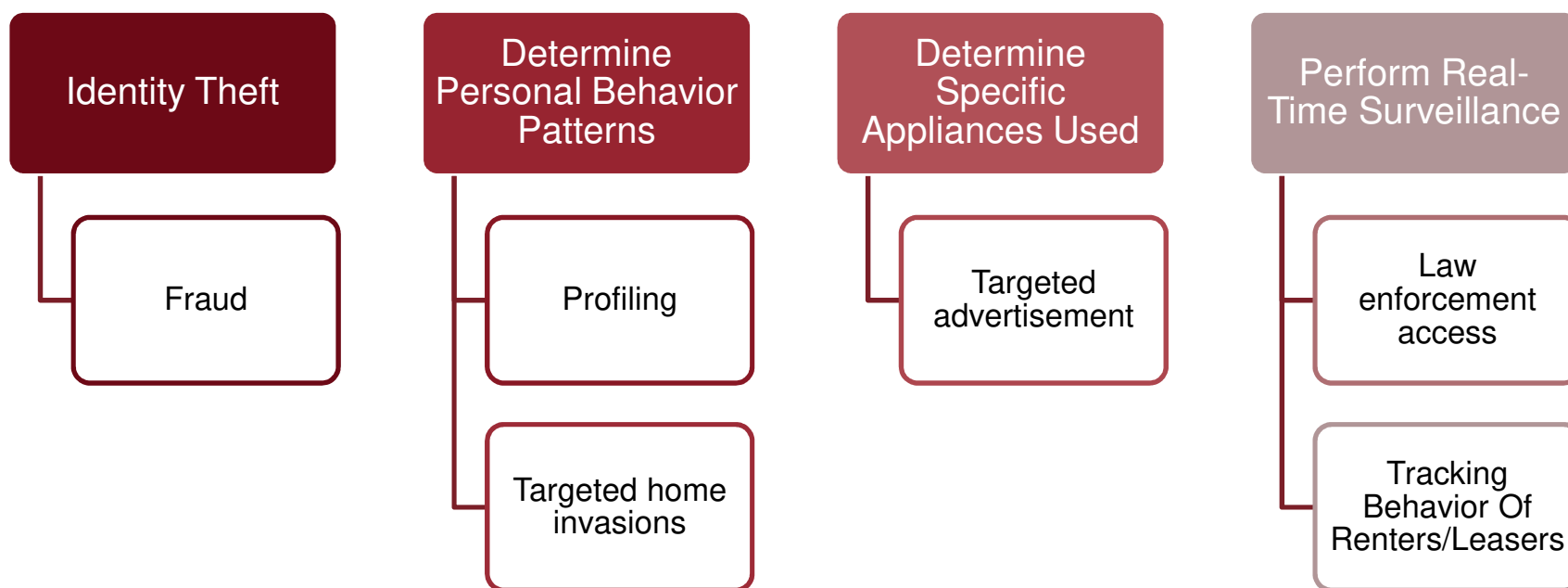
G+ 11

14 1 0 222

Smart Hacking For Privacy : What TV shows you watch ?



POTENTIAL RISKS



GENERAL DATA PROTECTION REGULATION (GDPR)

- In April 2016, the **General Data Protection Regulation (GDPR)** was adopted by the Council of the European Union and European Parliament, replacing Directive 95/46/EC
- The regulation ensures that personal data can be gathered under strict conditions, with data subject consent and only for legitimate purposes
- It is mandated that new services that collect or process personal data are subjected to a **Data Protection Impact Assessment (DPIA)**
- GDPR provisions will be directly applicable in all Member States from **25 May 2018**

DATA PROTECTION IMPACT ASSESSMENT (DPIA)

- Examples of EU generic frameworks:
 - Germany: *Standard Data Protection Model*, V.1.0, 2016.
 - Spain: *Guía para una Evaluación de Impacto en la Protección de Datos Personales* (EIPD), Agencia española de protección de datos (AGPD), 2014.
 - France: *Privacy Impact Assessment* (PIA), Commission nationale de l'informatique et des libertés (CNIL), 2015.
 - UK: *Conducting privacy impact assessments code of practice*, Information Commissioner's Office (ICO), 2014.
- Examples of EU sector-specific frameworks:
 - *Privacy and Data Protection Impact Assessment Framework for RFID Applications*, 2011.
 - ***Data Protection Impact Assessment Template for Smart Grid and Smart Metering Systems***, 2014.

DATA PROTECTION IMPACT ASSESSMENT (DPIA) TEMPLATE

- Template proposed by Smart Grid Task Force 2012-14, Expert Group 2, in consultation with Article 29 Working Party
- **Risk driven** approach to privacy impact assessment
- Considered as complementary or included in **a risk management process**

Smart Grid Task Force 2012-14

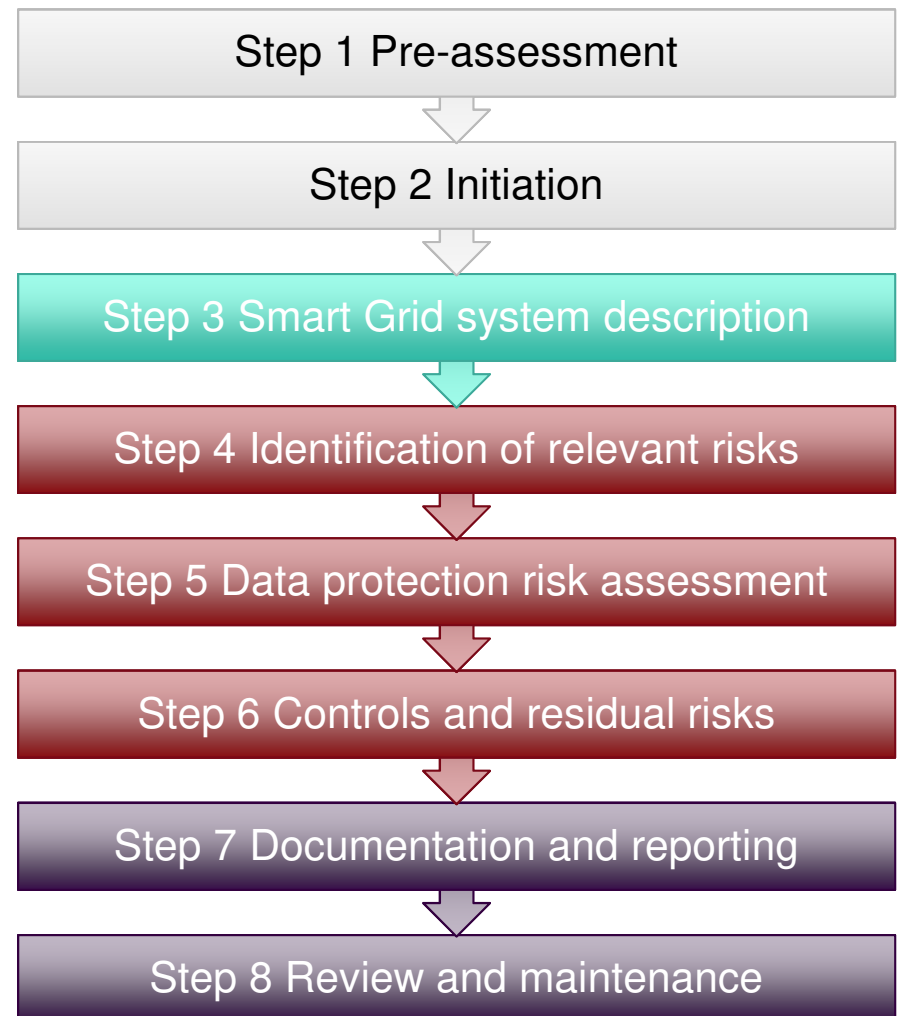
Expert Group 2: Regulatory Recommendations
for Privacy, Data Protection and Cyber-Security
in the Smart Grid Environment

Data Protection Impact Assessment
Template for Smart Grid and Smart
Metering systems

18.03.2014

DATA PROTECTION IMPACT ASSESSMENT PROCESS

- **What data** is being collected and how is it processed?
- **What are the risks** to rights and freedom of data subjects?
- What are the **measures**, privacy targets and controls **to ensure privacy**?



TOOL SUPPORTING IMPLEMENTATION OF DPIA

Direct support for
distributed team
working

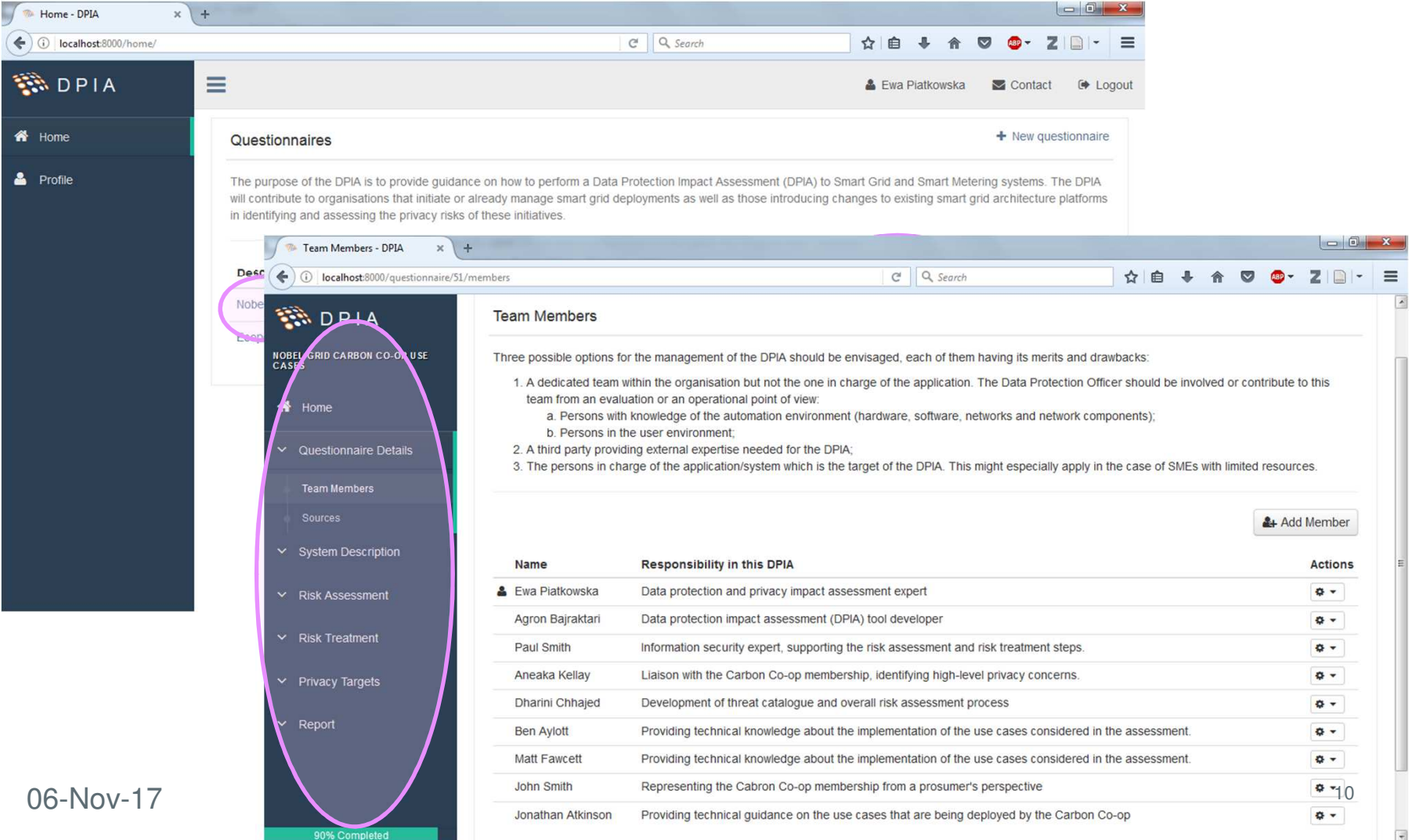
Guidance about how
to implement each
step embedded
directly in the tool

Hints about the
nature of the
required input
(catalogues, tooltips)

Pre-selected
relevant content to
support analyses

The automatic
generation of
documentation

TOOL SUPPORTING DPIA IMPLEMENTATION



Home - DPIA

localhost:8000/home/

DPIA

Home Profile

Questionnaires + New questionnaire

The purpose of the DPIA is to provide guidance on how to perform a Data Protection Impact Assessment (DPIA) to Smart Grid and Smart Metering systems. The DPIA will contribute to organisations that initiate or already manage smart grid deployments as well as those introducing changes to existing smart grid architecture platforms in identifying and assessing the privacy risks of these initiatives.

Team Members - DPIA

localhost:8000/questionnaire/51/members

Team Members

Three possible options for the management of the DPIA should be envisaged, each of them having its merits and drawbacks:

1. A dedicated team within the organisation but not the one in charge of the application. The Data Protection Officer should be involved or contribute to this team from an evaluation or an operational point of view:
 - a. Persons with knowledge of the automation environment (hardware, software, networks and network components);
 - b. Persons in the user environment;
2. A third party providing external expertise needed for the DPIA;
3. The persons in charge of the application/system which is the target of the DPIA. This might especially apply in the case of SMEs with limited resources.

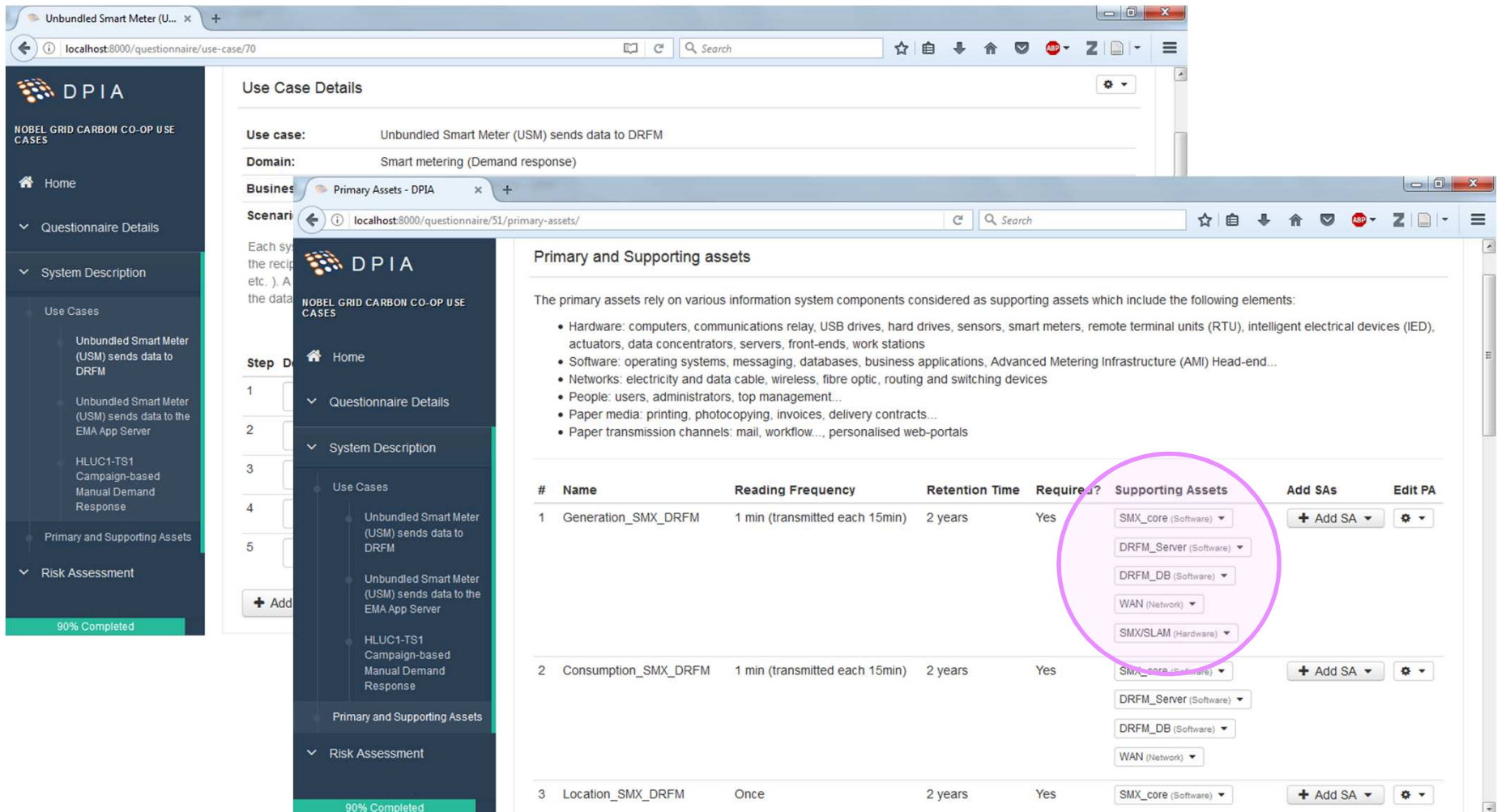
Team Members Table:

Name	Responsibility in this DPIA	Actions
Ewa Piatkowska	Data protection and privacy impact assessment expert	⚙️
Agron Bajraktari	Data protection impact assessment (DPIA) tool developer	⚙️
Paul Smith	Information security expert, supporting the risk assessment and risk treatment steps.	⚙️
Aneaka Kellay	Liaison with the Carbon Co-op membership, identifying high-level privacy concerns.	⚙️
Dharini Chhajed	Development of threat catalogue and overall risk assessment process	⚙️
Ben Aylott	Providing technical knowledge about the implementation of the use cases considered in the assessment.	⚙️
Matt Fawcett	Providing technical knowledge about the implementation of the use cases considered in the assessment.	⚙️
John Smith	Representing the Carbon Co-op membership from a prosumer's perspective	⚙️
Jonathan Atkinson	Providing technical guidance on the use cases that are being deployed by the Carbon Co-op	⚙️

90% Completed

06-Nov-17

SYSTEM DESCRIPTION



The screenshot displays two overlapping browser windows from the DPIA (Data Protection Impact Assessment) system. The top window shows the 'Use Case Details' for 'Unbundled Smart Meter (USM) sends data to DRFM' under the domain 'Smart metering (Demand response)'. The bottom window shows the 'Primary and Supporting assets' section, which lists three use cases and their associated supporting assets.

Use Case Details:

- Use case:** Unbundled Smart Meter (USM) sends data to DRFM
- Domain:** Smart metering (Demand response)


Primary and Supporting assets:

The primary assets rely on various information system components considered as supporting assets which include the following elements:

- Hardware: computers, communications relay, USB drives, hard drives, sensors, smart meters, remote terminal units (RTU), intelligent electrical devices (IED), actuators, data concentrators, servers, front-ends, work stations
- Software: operating systems, messaging, databases, business applications, Advanced Metering Infrastructure (AMI) Head-end...
- Networks: electricity and data cable, wireless, fibre optic, routing and switching devices
- People: users, administrators, top management...
- Paper media: printing, photocopying, invoices, delivery contracts...
- Paper transmission channels: mail, workflow..., personalised web-portals

#	Name	Reading Frequency	Retention Time	Required?	Supporting Assets	Add SAs	Edit PA
1	Generation_SMX_DRFM	1 min (transmitted each 15min)	2 years	Yes	SMX_core (Software) DRFM_Server (Software) DRFM_DB (Software) WAN (Network) SMX/SLAM (Hardware)	+ Add SA	⚙
2	Consumption_SMX_DRFM	1 min (transmitted each 15min)	2 years	Yes	SMX_core (Software) DRFM_Server (Software) DRFM_DB (Software) WAN (Network)	+ Add SA	⚙
3	Location_SMX_DRFM	Once	2 years	Yes	SMX_core (Software)	+ Add SA	⚙

LIKELIHOOD ASSESSMENT



DPiA
 NOBEL GRID CARBON CO-OP USE CASES

Home
 Questionnaire Details
 System Description
 Risk Assessment
 Threat Identification
 Likelihood Assessment
 Impact Assessment
 Risk Treatment
 Privacy Targets
 Report

90% Completed

Threat identification

The aim of this step is to establish, for the system which is under the scope of this assessment, a detailed and prioritized list of all threats related to the primary and supporting assets of processing operations identified in the previous step that would trigger different risks.


DPiA
 NOBEL GRID CARBON CO-OP USE CASES

Home
 Questionnaire Details
 System Description
 Risk Assessment
 Threat Identification
 Likelihood Assessment
 Impact Assessment
 Risk Treatment
 Privacy Targets
 Report

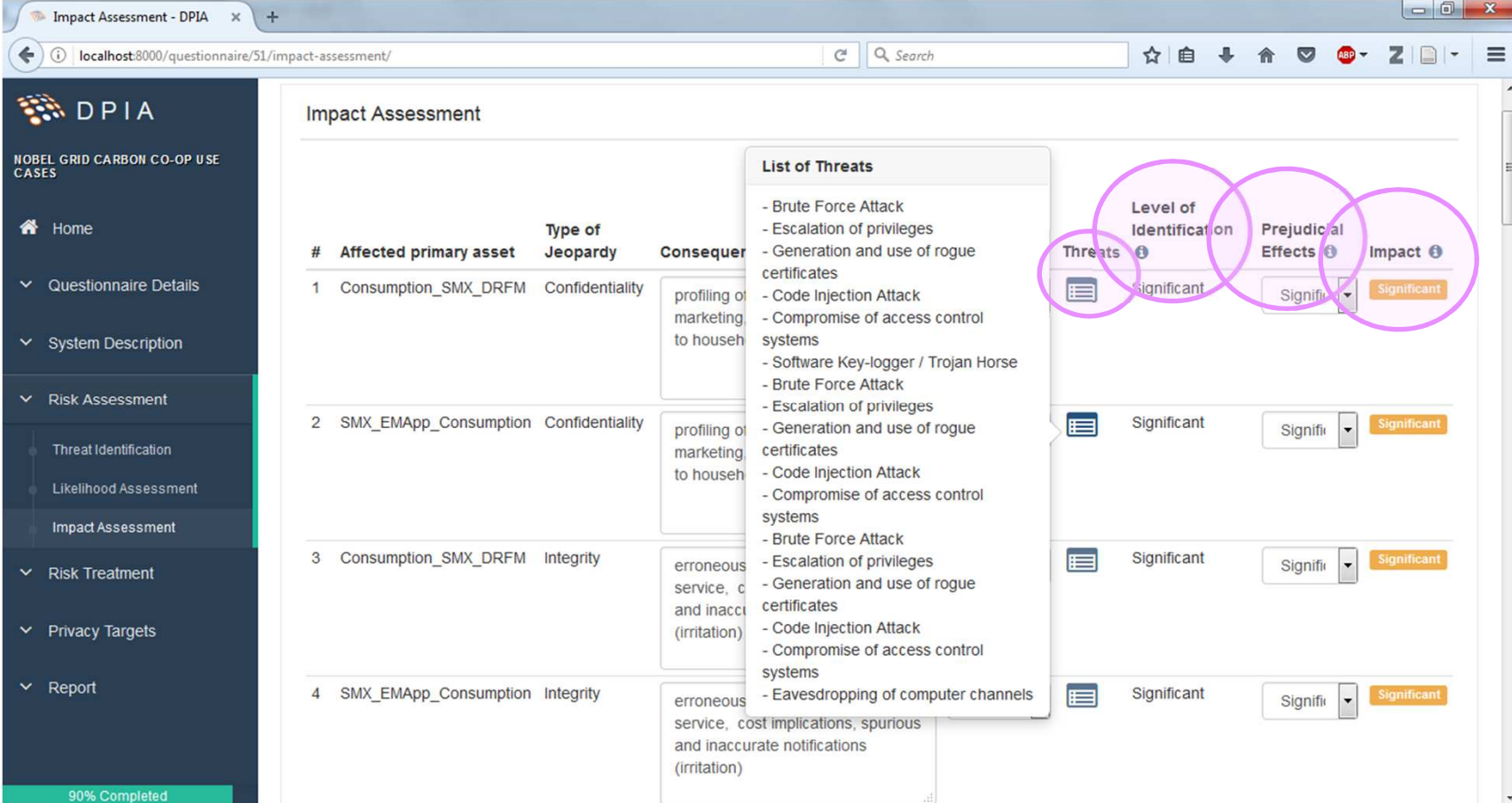
90% Completed

Likelihood Assessment

#	Affected Supporting Asset	Threat	Level of vulnerability	Risk source capability	Likelihood
1	SMX_core	Denial of service	Maximum	Maximum	Maximum
2	SMX_core	Brute Force Attack	Maximum	Maximum	Maximum
3	SMX_core	Escalation of privileges	Maximum	Maximum	Maximum
4	SMX_EMA_App	Denial of service	Maximum	Maximum	Maximum
5	SMX_EMA_App	Brute Force Attack	Maximum	Maximum	Maximum
6	SMX_EMA_App	Escalation of privileges	Maximum	Maximum	Maximum
7	DRFM_Server	Denial of service	Maximum	Maximum	Maximum
8	DRFM_Server	Brute Force Attack	Maximum	Maximum	Maximum
9	DRFM_DB	Denial of service	Maximum	Maximum	Maximum
10	DRFM_DB	Brute Force Attack	Maximum	Maximum	Maximum

06-Nov-17

IMPACT ASSESSMENT



Impact Assessment - DPIA

NOBEL GRID CARBON CO-OP USE CASES

Home

Questionnaire Details

System Description

Risk Assessment

Threat Identification

Likelihood Assessment

Impact Assessment

Risk Treatment

Privacy Targets

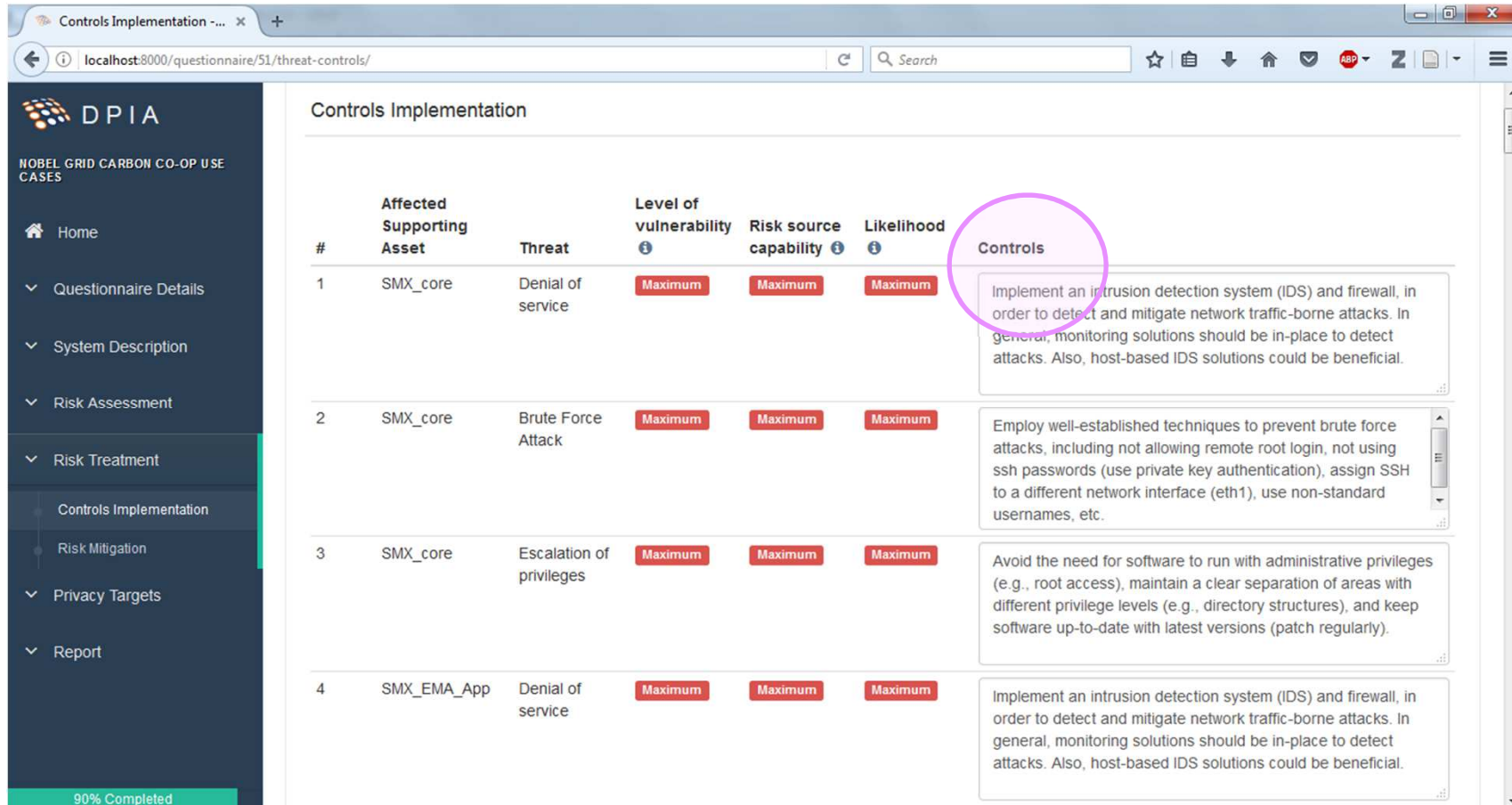
Report

90% Completed

Impact Assessment

#	Affected primary asset	Type of Jeopardy	Consequences	Threats	Level of Identification	Prejudicial Effects	Impact
1	Consumption_SMX_DRFM	Confidentiality	profiling of marketing to household	<ul style="list-style-type: none"> - Brute Force Attack - Escalation of privileges - Generation and use of rogue certificates - Code Injection Attack - Compromise of access control systems - Software Key-logger / Trojan Horse 	Significant	Significant	Significant
2	SMX_EMAApp_Consumption	Confidentiality	profiling of marketing to household	<ul style="list-style-type: none"> - Brute Force Attack - Escalation of privileges - Generation and use of rogue certificates - Code Injection Attack - Compromise of access control systems 	Significant	Significant	Significant
3	Consumption_SMX_DRFM	Integrity	erroneous service, cost and inaccurate notifications (irritation)	<ul style="list-style-type: none"> - Brute Force Attack - Escalation of privileges - Generation and use of rogue certificates - Code Injection Attack - Compromise of access control systems 	Significant	Significant	Significant
4	SMX_EMAApp_Consumption	Integrity	erroneous service, cost implications, spurious and inaccurate notifications (irritation)	<ul style="list-style-type: none"> - Brute Force Attack - Escalation of privileges - Generation and use of rogue certificates - Code Injection Attack - Compromise of access control systems - Eavesdropping of computer channels 	Significant	Significant	Significant

RISK TREATMENT



The screenshot shows a web application titled "DP IA" with a sidebar menu. The main content area is titled "Controls Implementation" and displays a table with four rows of risk treatments. The "Controls" column is highlighted with a purple circle.

#	Affected Supporting Asset	Threat	Level of vulnerability	Risk source capability	Likelihood	Controls
1	SMX_core	Denial of service	Maximum	Maximum	Maximum	Implement an intrusion detection system (IDS) and firewall, in order to detect and mitigate network traffic-borne attacks. In general, monitoring solutions should be in-place to detect attacks. Also, host-based IDS solutions could be beneficial.
2	SMX_core	Brute Force Attack	Maximum	Maximum	Maximum	Employ well-established techniques to prevent brute force attacks, including not allowing remote root login, not using ssh passwords (use private key authentication), assign SSH to a different network interface (eth1), use non-standard usernames, etc.
3	SMX_core	Escalation of privileges	Maximum	Maximum	Maximum	Avoid the need for software to run with administrative privileges (e.g., root access), maintain a clear separation of areas with different privilege levels (e.g., directory structures), and keep software up-to-date with latest versions (patch regularly).
4	SMX_EMA_App	Denial of service	Maximum	Maximum	Maximum	Implement an intrusion detection system (IDS) and firewall, in order to detect and mitigate network traffic-borne attacks. In general, monitoring solutions should be in-place to detect attacks. Also, host-based IDS solutions could be beneficial.

90% Completed

DPIA WORKSHOPS

- We have conducted a series of DPIA workshops to evaluate the usability of both: the DPIA process, and the tool supporting it.



- NOBEL GRID
 - Green Energy Max – shifting energy consumption to time when green energy is at its most
 - Price-based demand response



- RASSA
 - Energy Portal for monitoring household appliances and energy consumption



LESSONS LEARNED

- The DPIA process **is not linear**, some additional methods could be used for brainstorming and extracting the information from the DPIA team
- **Definition of the privacy risk** has proved to be confusing. The privacy risk is a sum of likelihood of a threat to the supporting assets (system infrastructure) and impact of primary asset (personal data) being compromised.
- Limited guidelines on the assessment method; no **domain-specific examples** of possible impacts and their place on the 4-level scale.
- Risks should be considered **not only per each primary asset**, but also **combination (subsets) of assets**.
- **Customer's versus Operator's perspective** → shall the number of affected customers should be taken into account in DPIA?

CONCLUSIONS

- Tool provides user-friendly interface and makes the implementation of the DPIA **more straightforward**, and therefore **requiring less effort**.
- The DPIA template for smart grid and smart metering systems is being revised and we are expecting a new version any time now.
- Standards and more detailed guidelines on the **security controls** and technologies to ensure the compliance with data protection regulation are required.

THANK YOU!

Ewa Piatkowska

ewa.piatkowska@ait.ac.at

