Grant Agreement Number: **248113/O70**

Project acronym: **IoTSec**

Project full title:

Security in IoT for Smart Grids

D 0.1
Collaborative Knowledge Platform

Due delivery date: M03

Actual delivery date: M03

Organization name of lead participant for this deliverable:

UiO

Dissemination level		
PU	Public	**X**
RE	Restricted to a group specified by the consortium	
CO	Confidential, only for members of the consortium	

Deliverable number:	D 0.1
Deliverable responsible:	UiO
Work package:	WP0
Editor(s):	Josef Noll

Author(s)	
Name	**Organisation**
Josef Noll	UiO

Document Revision History			
Version	**Date**	**Modifications Introduced**	
		Modification Reason	**Modified by**
V01	01.01.2016	Final version	Josef Noll
V02	20.09.2016	Extensions with list of Thesis, Presentations and Publications	Josef Noll

1 ABSTRACT

The IoTSec - Security in IoT for Smart Grids initiative was established in 2015 to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. The Research Project received funding from the Research Council of Norway (RCN) to contribute to a safe information society.

IoTSec addresses the basic needs for a reliable and efficient, uninterrupted power network with dynamic configuration and security properties. It addresses in addition the needs of businesses and end users of additional IoT services by exploring use cases for value-added services with the intent to design the building blocks for future services that consider the necessary security and privacy preconditions of successfully deployed large-scale services. IoTSec will apply the research in the envisaged Security Centre for Smart Grids, co-located with the Norwegian Centre of Excellence (NCE Smart).

This document describes the collaboration platform http://IoTSec.no. The collaboration platform is based on a Semantic Media Wiki engine, extended with project administration tools. Content is structured automatically, using semantic queries. Thus, information is automatically updated.

The collaboration platform is accompanied with a document repository for administrative and confidential information.

2 EXECUTIVE SUMMARY

The IoTSec - Security in IoT for Smart Grids initiative was established in 2015 to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. The Research Project received funding from the Research Council of Norway (RCN) to contribute to a safe information society.

IoTSec addresses the basic needs for a reliable and efficient, uninterrupted power network with dynamic configuration and security properties. It addresses in addition the needs of businesses and end users of additional IoT services by exploring use cases for value-added services with the intent to design the building blocks for future services that consider the necessary security and privacy preconditions of successfully deployed large-scale services. IoTSec will apply the research in the envisaged Security Centre for Smart Grids, co-located with the Norwegian Centre of Excellence (NCE Smart).

Since the start of the project, the initiative has grown from 11 founding partners to more than 20 partners, including the leading academia institutions in Norway, strong industry partners, and international collaborators.

This document describes the collaboration platform http://IoTSec.no. The collaboration platform is based on a Semantic Media Wiki engine, extended with project administration tools. Content is structured automatically, using semantic queries. Thus, information is automatically updated. A substantial change as compared to conventional platforms is the adoption of the open-world-principle, suggesting that “everything is open unless specified confidential”. This open-world-principle ensures that security knowledge is spread to a much broader way in IoTSec, as compared to other projects.

Specific functionality of the platform includes:

- Action Item handling, keeping track of the action items agreed in the meetings,
- Invitations and minutes of meetings and phone conferences,
- Contact information of participants and partners,
- Structure and content of workpackages (WPs) and tasks, and
- Presentations from workshops and conferences.

The collaboration platform is accompanied with a document repository for administrative and confidential information.

I. TABLE OF CONTENTS

II. TABLE OF FIGURES AND TABLES

3 INTRODUCTION

The IoTSec - Security in IoT for Smart Grids initiative was established in 2015 to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. The Research Project received funding from the Research Council of Norway (RCN) to contribute to a safe information society.

IoTSec addresses the basic needs for a reliable and efficient, uninterrupted power network with dynamic configuration and security properties. It addresses in addition the needs of businesses and end users of additional IoT services by exploring use cases for value-added services with the intent to design the building blocks for future services that consider the necessary security and privacy preconditions of successfully deployed large-scale services. IoTSec will apply the research in the envisaged Security Centre for Smart Grids, co-located with the Norwegian Centre of Excellence (NCE Smart).

Our aim is to contribute to a secure and privacy-aware ecosystem for the Internet of Things. We invite national and international partners for collaborations in the IoTSec initiative. The initiative has collected leading partners from Academia and Industry, to

- increase the knowledge on security and privacy related to IoT,
- provide security- and privacy-aware models, methods and services,
- translate academic developments into industrial applicability, and
- contribute to innovative services from IoT- and big-data collected in a privacy-aware manner.

We have created the knowledge base on security and privacy and keep extending the knowledge through our collaboration platform IoTSec.no. In addition, we collaborate through

- Regular phone conferences for the core team, every month,
- Topic-related workshops addressing aspects like measurable security, clustering of big data, about every 2nd month,
- Collaborative documents addressing achievements in the initiatives,
- Regular face-to-face meetings about every 3rd month, including a short industrial session focussing on "industrial requirements", and
- Workshops at national and international conferences.

This document describes the knowledge platform, and the functionality related to it. The challenge of each collaborative project is two create physical and virtual meeting places for collaboration, as well as an efficient handling of information and documentation in a platform.

Starting from the discussions during the kick-off meeting, we saw the need for different types of requirements:

- An efficient handling of deliverables, answering “where to find the latest version of that file”
- A collaborative tool for handling all “up to date” information, avoiding email spamming an the search for “latest information”.
- Functional requirements like
- single sign on
- user management
- data export

Based on these requirements, the project decides to select two platforms:

- **Semantic Media Wiki for collaboration**: Wiki software is the state-of-the-art collaboration software and used in a number of international projects. It supports day-to-day work through a useable interface. Special focus in IoTSec was to on the semantic extensions, allowing machine-readable information and information exchange through the platform. The Semantic Wiki is available at http://IoTSec.no.

- **IoTSec Web page:** In IoTSec we considered an own-standing platform for the Web page, but concluded that an integrated Web was preferable. An "own-standing platform" for the publication of information and news provides a good "look and feel". Such a functionality is not a core functionality of wiki implementations. However, an own-standing platform would have required to maintain two platforms, each of them having a different set of instructions. Thus, we concluded that an integrated Web Page in the Wiki would be sufficient for this type of a Research Project. The Web page is available at http://IoTSec.no.
- **Document Repository for a secure document exchange:** The document repository uses the state-of-the-art owncloud[1] software for document storage of all relevant documents, such as administrative details, the consortium agreement, and all deliverables. The document repository is hosted by UNIK and available at http://owncloud.unik.no. While owncloud supports a clean structure for documents storage and secure access to these documents, it does not support an easy-to-use collaboration. This is the reason for having introduced a wiki-based collaboration.

This document was created as v01 in month M3, describing the semantic functionality, and extended in M12 with actual information regarding meetings, action items, and topics of e.g. master thesis.

[1] Owncloud is a cloud instantiation on a local server, providing functionalities such like automatic sync, access control, web access and secured exchange. Software is maintained by http://owncloud.org

4 COLLABORATION PLATFORM IOTSEC.NO

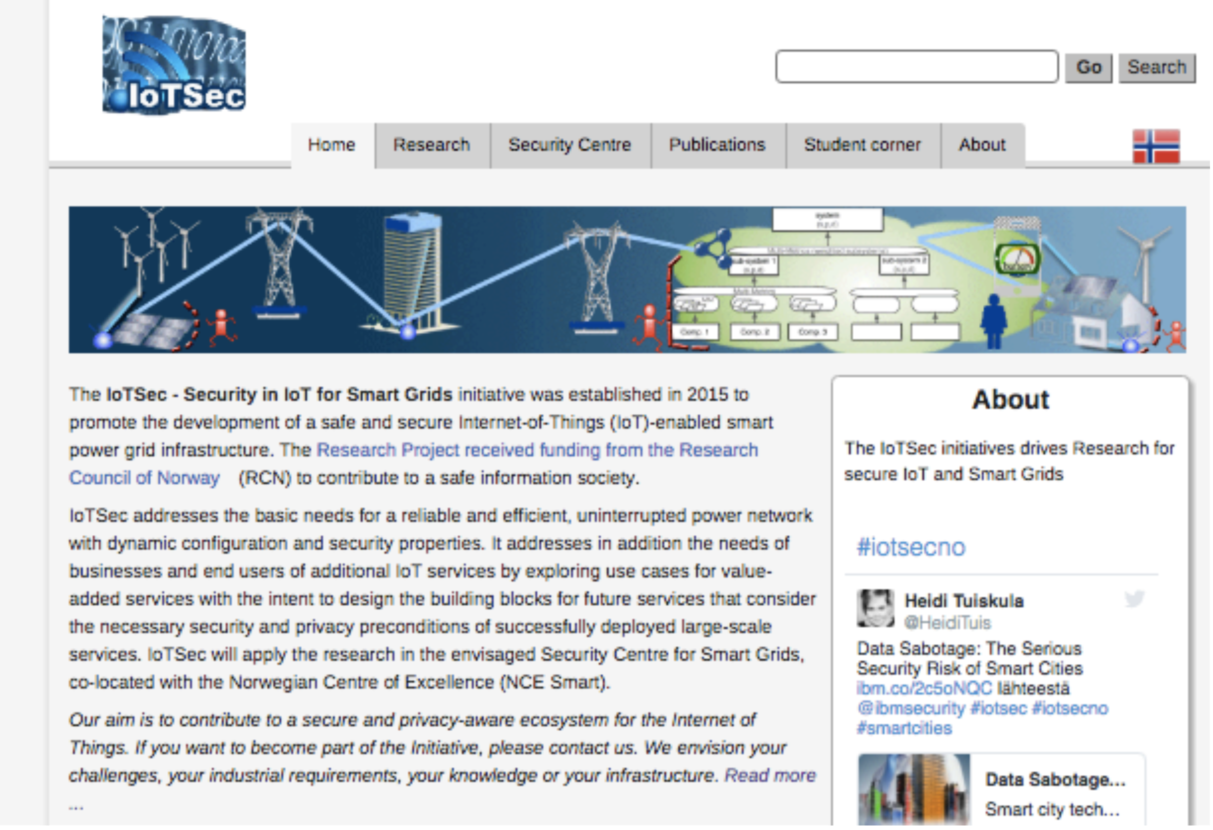
Wiki software is the state-of-the-art collaboration software and used in a number of international projects. It supports day-to-day work through a useable interface.

Special focus in IoTSec was to on the semantic extensions, allowing machine-readable information and information exchange through the platform. As of now, the platform is used for information exchange, but has the interfaces in place to connect to IoT systems.

This vision of sensor input for business processes is "a long way ahead", and will not be implemented in the IoTSec project. However, the selection of a semantic MediaWiki platform introduces functionality to handle the specific challenges for projects. These functionalities are further described in the next sections.

4.1 Functionality overview

The IoTSec collaboration platform is based on a Semantic Wiki implementation and is available at http://IoTSec.no. Figure 1 shows the entry page for the IoTSec wiki.



The **IoTSec - Security in IoT for Smart Grids** initiative was established in 2015 to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. The Research Project received funding from the Research Council of Norway (RCN) to contribute to a safe information society.

IoTSec addresses the basic needs for a reliable and efficient, uninterrupted power network with dynamic configuration and security properties. It addresses in addition the needs of businesses and end users of additional IoT services by exploring use cases for value-added services with the intent to design the building blocks for future services that consider the necessary security and privacy preconditions of successfully deployed large-scale services. IoTSec will apply the research in the envisaged Security Centre for Smart Grids, co-located with the Norwegian Centre of Excellence (NCE Smart).

Our aim is to contribute to a secure and privacy-aware ecosystem for the Internet of Things. If you want to become part of the Initiative, please contact us. We envision your challenges, your industrial requirements, your knowledge or your infrastructure. Read more ...

About

The IoTSec initiatives drives Research for secure IoT and Smart Grids

#iotsecno

Heidi Tuiskula
@HeidiTuis

Data Sabotage: The Serious Security Risk of Smart Cities ibm.co/2c5oNQC lähteestä @ibmsecurity #iotsec #iotsecno #smartcities

Data Sabotage...
Smart city tech...

Figure 1 - Welcome page for the IoTSec wiki, providing a quick overview on activities

The core platform was originally developed for the SHIELD projects[2]. Having demonstrated the functionality towards project partners, the platform has been adopted for IoTSec as a collaboration platform. Specific functionality of the platform includes:

- Action Item handling, keeping track of the action items agreed in the meetings,

[2] The SHIELD methodology for measurable security was developed through JU Artemis projects pSHIELD (http://pSHIELD.unik.no) and nSHIELD (http://nSHIELD.unik.no), creating pilot as well as domain specific applications of measurable security.

- Invitations and minutes of meetings and phone conferences,
- Contact information of participants and partners,
- Structure and content of workpackages (WPs) and tasks, and
- Presentations from workshops and conferences.

The platform uses form templates for creating inputs, such that these semantic informations can be used to in automated page generations, avoiding the input for manual creation of pages. Figure 2 provides the footer of the collaboration platform, indicating the semantic templates under the "Forms" entries.

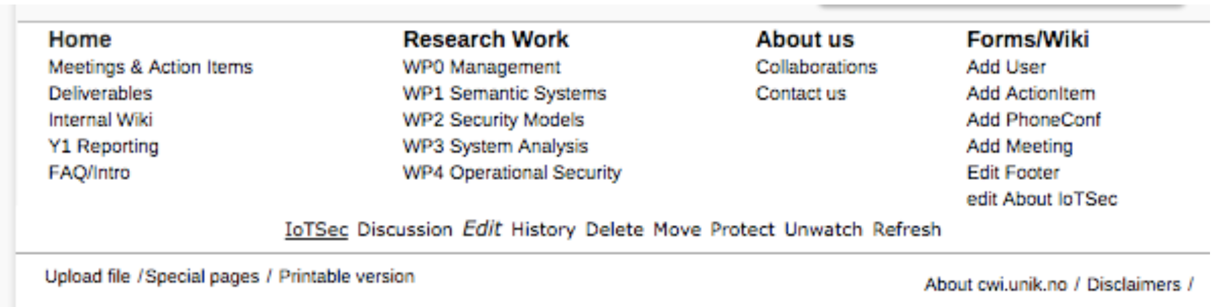


Figure 2 – Footer of the IoTSec collaboration platform

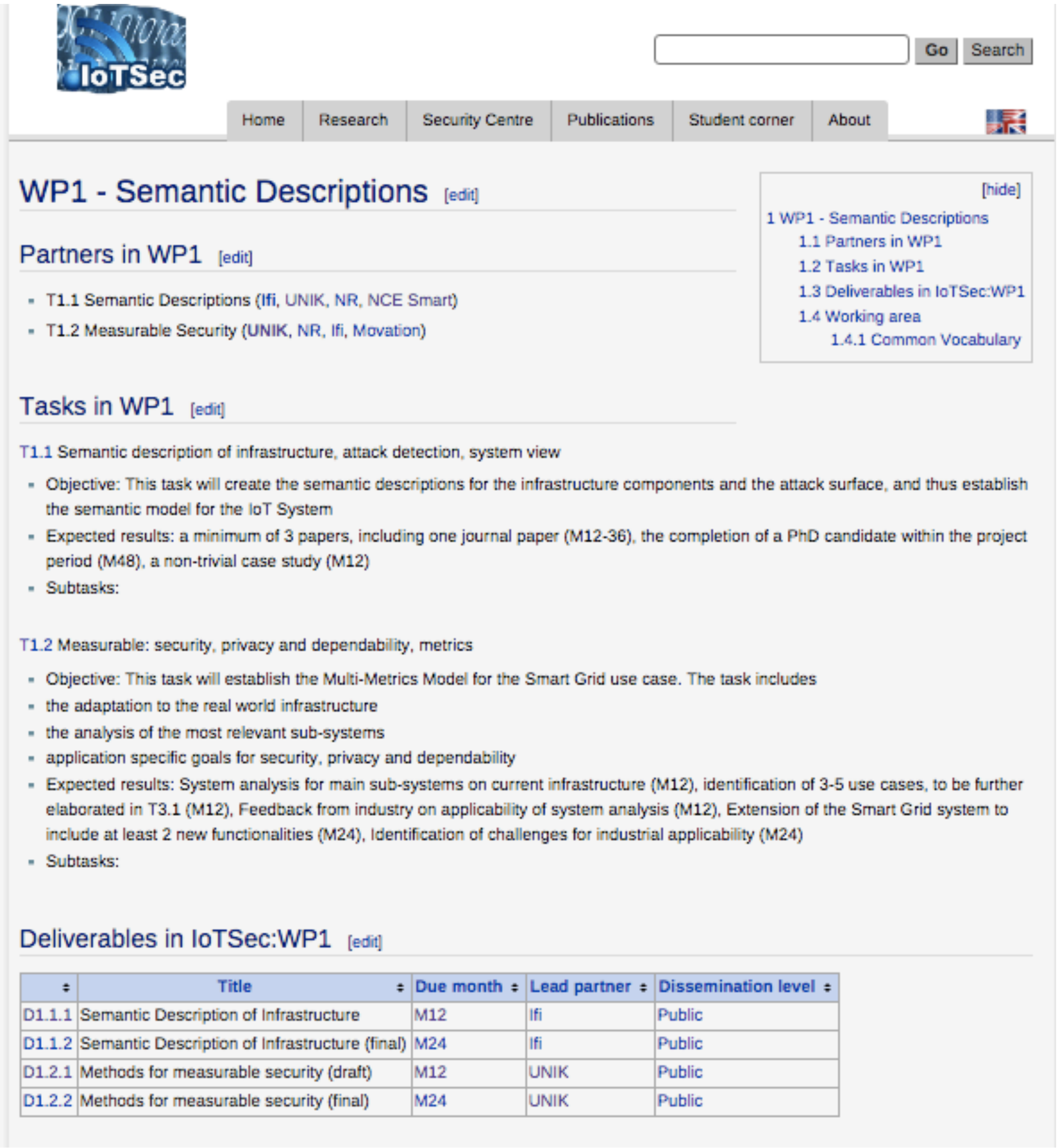
A substantial change as compared to conventional platforms is the adoption of the open-world-principle, suggesting that "everything is open unless specified confidential". This open-world-principle ensures that security knowledge is spread to a much broader way in IoTSec, as compared to other projects.

4.2 Semantic search for automated pages

Traditional Web pages are hand-made, and require manual input for any relevant updates. Advanced Web tools use dynamic content, which is configured through manually described page settings.

IoTSec introduces a Semantic MediaWiki, allowing the on the fly generation of pages based on the semantic queries and the input being provided through forms and templates. Two examples of such forms are provided here, further details can be obtained directly from the wiki: http://IoTSec.no.

Figure 3 shows an implementation of WP1, providing both the list of deliverables, the contributors and tasks of this workpackage. A traditional web or wiki would have needed duplication of information, while our IoTSec Wiki uses semantic queries based on the ask functionality.



WP1 - Semantic Descriptions [edit]

Partners in WP1 [edit]

- T1.1 Semantic Descriptions (Ifi, UNIK, NR, NCE Smart)
- T1.2 Measurable Security (UNIK, NR, Ifi, Movation)

Tasks in WP1 [edit]

T1.1 Semantic description of infrastructure, attack detection, system view

- Objective: This task will create the semantic descriptions for the infrastructure components and the attack surface, and thus establish the semantic model for the IoT System
- Expected results: a minimum of 3 papers, including one journal paper (M12-36), the completion of a PhD candidate within the project period (M48), a non-trivial case study (M12)
- Subtasks:

T1.2 Measurable: security, privacy and dependability, metrics

- Objective: This task will establish the Multi-Metrics Model for the Smart Grid use case. The task includes
- the adaptation to the real world infrastructure
- the analysis of the most relevant sub-systems
- application specific goals for security, privacy and dependability
- Expected results: System analysis for main sub-systems on current infrastructure (M12), identification of 3-5 use cases, to be further elaborated in T3.1 (M12), Feedback from industry on applicability of system analysis (M12), Extension of the Smart Grid system to include at least 2 new functionalities (M24), Identification of challenges for industrial applicability (M24)
- Subtasks:

Deliverables in IoTSec:WP1 [edit]

⇕	Title ⇕	Due month ⇕	Lead partner ⇕	Dissemination level ⇕
D1.1.1	Semantic Description of Infrastructure	M12	Ifi	Public
D1.1.2	Semantic Description of Infrastructure (final)	M24	Ifi	Public
D1.2.1	Methods for measurable security (draft)	M12	UNIK	Public
D1.2.2	Methods for measurable security (final)	M24	UNIK	Public

Figure 3 - Workpackage description containing Deliverables, Contributors (Partners) and Tasks

Using these functionality, our implementation uses the following commands to establish WP1:

```
={{PAGENAME}} - Semantic Descriptions =
==Partners in {{PAGENAME}}==
{{#ask: [[Workpackage::{{FULLPAGENAME}}]] [[Partner::+]]| ?Page Title |?Lead partner | ?Partner | format=template | template=Partner_listing
}}

== Tasks in {{PAGENAME}} ==
{{#ask:[[Workpackage::{{FULLPAGENAME}}]] [[Category:Task]]| ?Title= | ?Objective |?has result |?has subtask | format=template | template=Task_listing}}

==Deliverables in {{FULLPAGENAME}} ==
{{#ask:  [[Workpackage::{{FULLPAGENAME}}]] [[Deliverable::+]]
| ?Title
| ?Due month
| ?Lead partner
| ?Dissemination level
}}
```

The first part of the codes establishes the workpackage specific description, while the second part starting contains three “ask” statements, which provide the list of partners, list of tasks and the list of deliverables in this workpackage.

The same mechanism is used to establish the responsibility of each partner. This description is identical for all partners, thus the set-up of the complete collaboration platform is made extremely easy. Once developed, the content of each partner info page is identical.

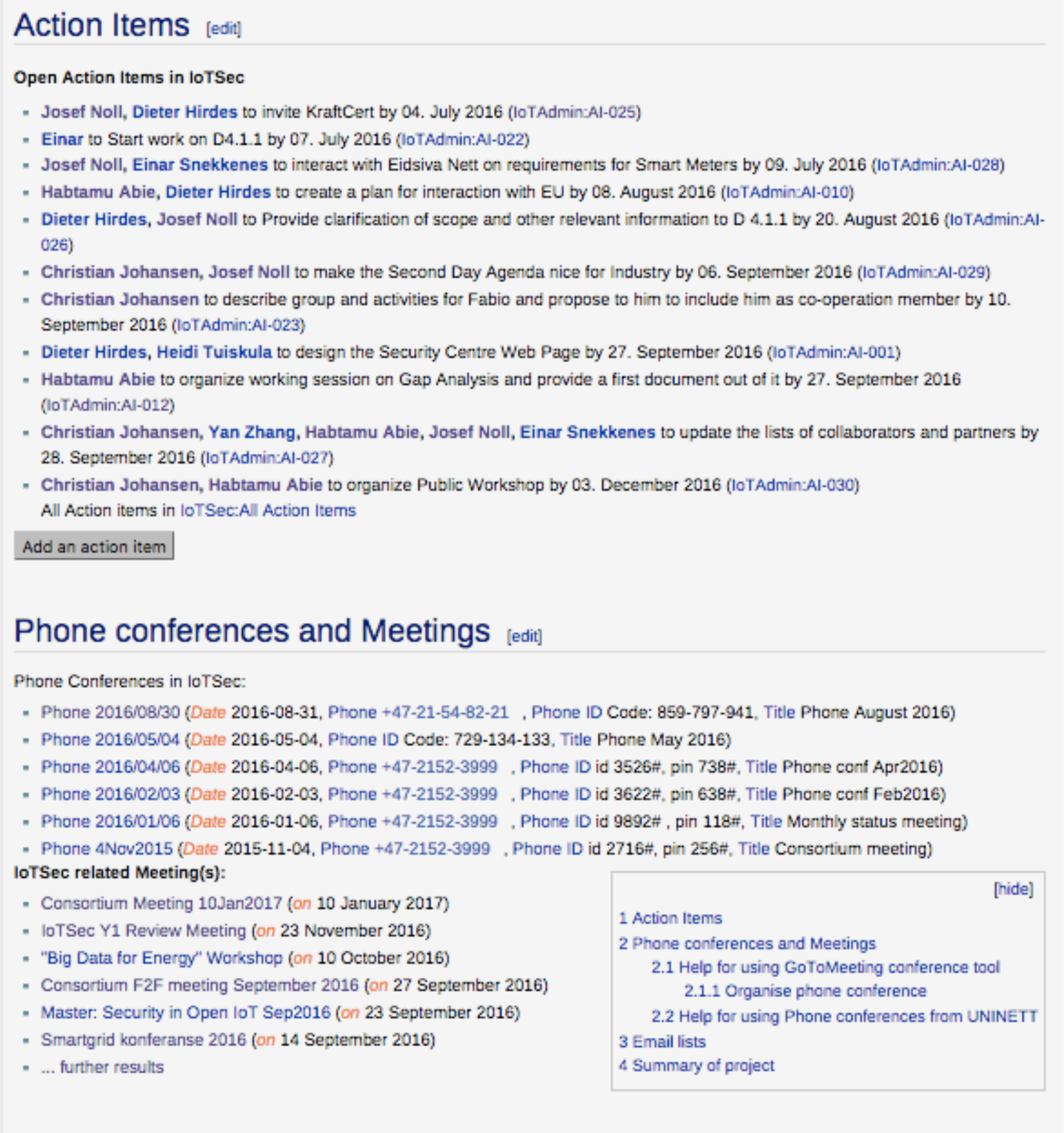
Semantic technologies opens for export of information towards other platforms and systems. it further allows the import of information, a functionality which will be further investigated to realise the vision of importing sensors into business processes.

4.3 List of Forms and Templates

As indicated in the previous section, the IoTSec collaboration platform uses standardised input mechanisms based on semantic templates. These forms were established allowing the following tasks:

- 1. ActionItem
- 2. AddTask
- 3. AddUser
- 4. Deliverable
- 5. Meeting
- 6. NewTask
- 7. PhoneConf
- 8. UserRegistration
- 9. Workpackage

An example is provided for meetings and conferences.



Open Action Items in IoTSec

- Josef Noll, Dieter Hirdes to invite KraftCert by 04. July 2016 (IoTAdmin:AI-025)
- Einar to Start work on D4.1.1 by 07. July 2016 (IoTAdmin:AI-022)
- Josef Noll, Einar Snekkenes to interact with Eidsiva Nett on requirements for Smart Meters by 09. July 2016 (IoTAdmin:AI-028)
- Habtamu Abie, Dieter Hirdes to create a plan for interaction with EU by 08. August 2016 (IoTAdmin:AI-010)
- Dieter Hirdes, Josef Noll to Provide clarification of scope and other relevant information to D 4.1.1 by 20. August 2016 (IoTAdmin:AI-026)
- Christian Johansen, Josef Noll to make the Second Day Agenda nice for Industry by 06. September 2016 (IoTAdmin:AI-029)
- Christian Johansen to describe group and activities for Fabio and propose to him to include him as co-operation member by 10. September 2016 (IoTAdmin:AI-023)
- Dieter Hirdes, Heidi Tuiskula to design the Security Centre Web Page by 27. September 2016 (IoTAdmin:AI-001)
- Habtamu Abie to organize working session on Gap Analysis and provide a first document out of it by 27. September 2016 (IoTAdmin:AI-012)
- Christian Johansen, Yan Zhang, Habtamu Abie, Josef Noll, Einar Snekkenes to update the lists of collaborators and partners by 28. September 2016 (IoTAdmin:AI-027)
- Christian Johansen, Habtamu Abie to organize Public Workshop by 03. December 2016 (IoTAdmin:AI-030)
  All Action items in IoTSec:All Action Items

Phone Conferences in IoTSec:

- Phone 2016/08/30 (Date 2016-08-31, Phone +47-21-54-82-21 , Phone ID Code: 859-797-941, Title Phone August 2016)
- Phone 2016/05/04 (Date 2016-05-04, Phone ID Code: 729-134-133, Title Phone May 2016)
- Phone 2016/04/06 (Date 2016-04-06, Phone +47-2152-3999 , Phone ID id 3526#, pin 738#, Title Phone conf Apr2016)
- Phone 2016/02/03 (Date 2016-02-03, Phone +47-2152-3999 , Phone ID id 3622#, pin 638#, Title Phone conf Feb2016)
- Phone 2016/01/06 (Date 2016-01-06, Phone +47-2152-3999 , Phone ID id 9892# , pin 118#, Title Monthly status meeting)
- Phone 4Nov2015 (Date 2015-11-04, Phone +47-2152-3999 , Phone ID id 2716#, pin 256#, Title Consortium meeting)

IoTSec related Meeting(s):

- Consortium Meeting 10Jan2017 (on 10 January 2017)
- IoTSec Y1 Review Meeting (on 23 November 2016)
- "Big Data for Energy" Workshop (on 10 October 2016)
- Consortium F2F meeting September 2016 (on 27 September 2016)
- Master: Security in Open IoT Sep2016 (on 23 September 2016)
- Smartgrid konferanse 2016 (on 14 September 2016)
- ... further results

Figure 4 - List of Action Items and (phone) conferences

Figure 4 shows the list of Action Items and meetings, both phone conferences and physical meetings. As previously, the functionality is achieved through two semantic queries, here presented for the meetings:

```
= Phone conferences and Meetings =
{{#ask: [[Category:Phone_IoTSec]] <!--- [[Phone::+]] --->
| sort=Date
| ?Date#ISO
| ?Phone
| ?Phone_ID
| ?Title
| limit=8
| format=ul
| order=desc
| intro=Phone Conferences in IoTSec:
}}
{{TOCright}}

<!-- Meetings -->
{{#ask: [[Project::IoTSec]] [[Category:Meeting]]| ?Date=on  | format=ul |sort=Date | sep=',
|order=desc
| limit=6
| intro='''IoTSec related Meeting(s):'''&#10;
}}
```

The semantic functionality ensures the quality of the information, as information is only added once, and then shown in all relates queries.

4.4 Student corner and Publications

The collaboration platform has two specific areas related to the research, the student corner and the publication site.

4.4.1 Student corner with Master Topics

The corner lists topics for master thesis work, showing also the supervisors of the suggested topics. Examples of open thesis are:

- Multi Metrics Based Framework (Supervisor(s): Josef Noll, Seraj Fayyad)
- Evaluation of the Component`s Interconnection Impact on the System Security (Supervisor(s): Josef Noll, Seraj Fayyad)
- Privacy labels for IoT consumer products (Supervisor(s): Josef Noll, Hanne Brostrøm)
- Building an Attack Simulator on the Electric Grid Infrastructure (Supervisor(s): György Kálmán, Josef Noll)
- Semantic Modeling of a Smart Home Infrastructure (Supervisor(s): Josef Noll, Christian Johansen)
- Risk Assessment tool analysis for Industrial Automation and Control Systems (Supervisor(s): Mohammad Mushfiqur Rahman Chowdhury, Judith Rossebø, Josef Noll)
- Prosumers for the future smart electricity grid (Supervisor(s): Josef Noll)
- Measurable Security for Sensor Communication in the Internet of Things (Supervisor(s): Josef Noll, Mohammad Mushfiqur Rahman Chowdhury)

The page contains also a button, to allow the creation of new Thesis topics. What is missing is the automatic presentation of these theses on the Master Thesis pages of UiO, NTNU and UiA.

Ongoing theses are listed, showing the student executing the thesis:

- Smart Meter Security Analysis (Editor: Mehdi Noroozi)
- Security challenges of open low-capacity wifi access (Editor: Naji Ahmed Kadah)
- The human aspect in Smart grids (from Security and Privacy point of view) (Editor: Linn Eirin Paulsen)
- Pervasive computing in smart electricity grid (Editor: Kaniz Fatema Tuly)

Thus, the student corner is the entry point for students to look for thesis work, and for academic supervisors to identify research topics. The page will be extended by links to the PhD project pages of the PhD-students.

4.4.2 IoTSec Publications

IoTSec publications are listed on the publications page http://IoTSec.no/publications, presenting presentations, newspaper articles and scientific publications.

4.4.2.1 *Presentations*

The list of presentations contain presentations given at certain events, e.g. the Smartgrid conference, and the “Norsk informasjonssikkerhetsforum”.

1. J. Noll, "Security and privacy-aware ecosystem for the Internet of Things in Smartgrids", Smartgrid conference, 13-14Sep2016, Fornebu, [1]
2. J. Noll, "Measurable Security and Privacy for the Internet of Things", Nemko's compliance & market access seminar, 13-15June2016, Oslo
3. O. Owe, "A framework for reasoning about object-oriented concurrent systems", SINTEF seminar Dec 15 2015, Oslo
4. J. Noll, "IoTSec - Security in IoT for Smart Grids", Norsk informasjonssikkerhetsforum (ISF), Møte, Nov 2015
5. J. Noll, "Sikkerhetsutfordringer i fremtidens Smartgrid", Partnerseminaret NCE Smart Energy Markets, Nov 2015
6. J. Noll, and D. Hirdes, "Nasjonalt senter for sikkerhet i SmartGrid", Resultater fra Arbeidsgruppe, Partnerseminaret NCE Smart Energy Markets, Nov 2015
7. J. Noll, "Measurable Security as Driver for the Internet of Things Ecosystem", e-Innovation Seminar, University of Montenegro, 4.-6.Nov2015
8. H. Abie, "IoTSec - Security in IoT for Smart Grids", AF Security Seminar, Oct 2015, Oslo
9. H.Tuiskula, "IoTSec - Security in Internet-of-Things for Smart Grids", Poster in ACSAC Conference, Dec 2015, Los Angeles

4.4.2.2 *Other publications*

Other publications include e.g. newspaper interviews and related public information, e.g.

1. Interview "Knut Johansen" on future of Energy Companies
2. *further reading* Massedød i Strømbransjen (E24) *(in Norwegian)*

4.4.2.3 *Scientific Publications*

The scientific publications in conferences and journals are listed thereafter:

1. R. Bubel , F. Damiani, R. Haehnle, E.B. Johnsen, O. Owe, I. Schaefer, I.C. Yu: Proof Repositories for Compositional Verification of Evolving Software Systems: Managing Change When Proving Software Correct. In Proof Repositories for Software Verification In-the-Large, LNCS Transactions on Foundations for Mastering Change (FOMAC) (27 pages), 2016, To appear.
2. Olaf Owe: Verifiable Programming of Object-Oriented and Distributed Systems. In Luigia Petre and Emil Sekerinski (eds.) From Action System to Distributed Systems: The Refinement Approach CRC Press Taylor & Francis, pp. 61–80, 2016
3. Olaf Owe: Reasoning about Inheritance and Unrestricted Reuse in Object-Oriented Concurrent Systems, iFM'16 Iceland, in Lecture Notes in Computer Science 9681, Springer, pages 210-225, June 2016.
4. Aman, W.; Snekkenes, E. EDAS: An Evaluation Prototype for Autonomic Event-Driven Adaptive Security in the Internet of Things. Future Internet 2015, 7, 225-256.

In conclusion, the collaboration platform platform includes semantic forms for the day-to-day management of the IoTSec initiative, acts as a knowledge base related to IoT Security, and an entry point for students and scientific partners.

5 CONCLUSIONS

The IoTSec - Security in IoT for Smart Grids initiative was established in 2015 to promote the development of a safe and secure Internet-of-Things (IoT)-enabled smart power grid infrastructure. IoTSec addresses the basic needs for a reliable and efficient, uninterrupted power network with dynamic configuration and security properties. It addresses in addition the needs of businesses and end users of additional IoT services by exploring use cases for value-added services with the intent to design the building blocks for future services that consider the necessary security and privacy preconditions of successfully deployed large-scale services.

This document describes the collaboration platform http://IoTSec.no. The collaboration platform is based on a Semantic Media Wiki engine, extended with project administration tools. Content is structured automatically, using semantic queries. Thus, information is automatically updated. A substantial change as compared to conventional platforms is the adoption of the open-world-principle, suggesting that "everything is open unless specified confidential". This open-world-principle ensures that security knowledge is spread to a much broader way in IoTSec, as compared to other projects.

Specific functionality of the platform includes:

- Action Item handling, keeping track of the action items agreed in the meetings,
- Invitations and minutes of meetings and phone conferences,
- Contact information of participants and partners,
- Structure and content of workpackages (WPs) and tasks, and
- Presentations from workshops and conferences.

The collaboration platform platform includes semantic forms for the day-to-day management of the IoTSec initiative, acts as a knowledge base related to IoT Security, and an entry point for students and scientific partners. Envisaged extensions include a better presentation of the topics for Master thesis, the participants and the partners of the IoTSec initiative. Extensions towards semantic functionalities include the quarterly reporting from partners, as well as a semantic map of security functionalities.