Network of Excellence

D4.2 Part I:
Report on the Cutting-Edge Activities, Alignment and Integration with Relevant European and International Activities and Release of the Research Roadmap
**Abstract**

This deliverable reports on the activities carried out within the NESSoS consortium in order to achieve integration with other communities that work also on the area of secure service engineering.

We have also made an analysis of the research collaborations that have been done and are planned to happen within the NESSoS consortium, including associate partners.

The deliverable also points out at the NaLAB constituency and the activities that have been done together with them.

**Keyword list**

Future Internet, Software and Service Engineering, Security, Integration activities, events, Roadmap
# Document History

<table>
<thead>
<tr>
<th>Version</th>
<th>Type of change</th>
<th>Author(s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>V0.1</td>
<td>Table of Contents</td>
<td>Carmen Fernandez</td>
</tr>
<tr>
<td>V0.2</td>
<td>Section 3</td>
<td>Carmen Fernandez</td>
</tr>
<tr>
<td>V0.3</td>
<td>Section 2</td>
<td>Carmen Fernandez, Francisco Moyano, Javier Lopez</td>
</tr>
<tr>
<td>V0.4</td>
<td>Update of Section 2 and section 3, Section 1</td>
<td>Carmen Fernandez, Francisco Moyano, Fabio Martinelli</td>
</tr>
<tr>
<td>V0.5</td>
<td>Section 4, List of figures and tables, update of Section 2, Section 5</td>
<td>Carmen Fernandez, Francisco Moyano</td>
</tr>
<tr>
<td>V0.6</td>
<td>Updates of Sections 1, 2,3 and 4</td>
<td>Carmen Fernandez, Javier Lopez, Francisco Moyano</td>
</tr>
<tr>
<td>V0.7</td>
<td>Comments by Fabio Martinelli addressed</td>
<td>Carmen Fernandez, Javier Lopez, Francisco Moyano</td>
</tr>
<tr>
<td>V0.8</td>
<td>Comments by Maritta Heisel, Kristian Beckers and Wouter Joosen addressed</td>
<td>Carmen Fernandez, Javier Lopez, Francisco Moyano</td>
</tr>
<tr>
<td>V3.0</td>
<td>Approved by reviewers</td>
<td>Carmen Fernandez, Javier Lopez, Francisco Moyano</td>
</tr>
</tbody>
</table>
Table of Contents

TABLE OF CONTENTS ........................................................................................................... 3
LIST OF FIGURES .................................................................................................................. 5
LIST OF TABLES .................................................................................................................... 5
LIST OF ACRONYMS .............................................................................................................. 6
EXECUTIVE SUMMARY ......................................................................................................... 7
1 INTRODUCTION ..................................................................................................................... 8
2 JOINT RESEARCH ACTIVITIES ....................................................................................... 10
  2.1 Collaborations within NESSoS Consortium ................................................................. 10
  2.2 Collaborations with Associate Partners ....................................................................... 20
3 NESSoS ACTIVITIES FOR ACHIEVING INTEGRATION .............................................. 22
  3.1 NESSoS Meetings .......................................................................................................... 22
  3.2 Flagship Event: ESSoS Conference .............................................................................. 22
  3.3 Participation in Activities with Other Communities ..................................................... 23
  3.4 Other Events .................................................................................................................. 34
  3.5 Education and Training Activities .............................................................................. 39
  3.6 Roadmapping Activities ............................................................................................. 39
4 REPORT ON THE NALAB ACTIVITIES ........................................................................ 41
5 CONCLUSION ...................................................................................................................... 43
REFERENCES ......................................................................................................................... 44
List of Figures
Figure 1 Joint research collaborations................................................................. 18
Figure 2 Joint Publications ..................................................................................... 19
Figure 3 Joint Organization of Events ...................................................................... 20
Figure 4 Topics addressed by NESSoS ................................................................... 33
Figure 5 Quantification of Approached Topics .......................................................... 34

List of Tables
Table 1-CNР Collaborations .................................................................................... 11
Table 2-ATOS Collaborations .................................................................................. 12
Table 3-ETH Collaborations .................................................................................... 13
Table 4-IMDEA Collaborations ................................................................................ 13
Table 5-INRIA Collaborations ................................................................................. 14
Table 6-KUL Collaborations .................................................................................... 14
Table 7-LMU Collaborations ................................................................................... 15
Table 8-SIEMENS Collaborations ........................................................................... 15
Table 9-SINTEF Collaborations .............................................................................. 16
Table 10-UDE Collaborations .................................................................................. 16
Table 11-UMA Collaborations .................................................................................. 17
Table 12-UNITN Collaborations .............................................................................. 17
## List of Acronyms

<table>
<thead>
<tr>
<th>Acronym</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>ETP</td>
<td>European Technology Platform</td>
</tr>
<tr>
<td>FI</td>
<td>Future Internet</td>
</tr>
<tr>
<td>ICT</td>
<td>Information and Communication Technologies</td>
</tr>
<tr>
<td>IT</td>
<td>Information Technology</td>
</tr>
<tr>
<td>SDLC</td>
<td>Service Development Life Cycle</td>
</tr>
</tbody>
</table>
Executive Summary

This deliverable is divided into two parts, being the first part the current document. The second part is the second version of the NESSoS roadmap that is presented as a separate document due to its extension.

The current document describes the activities carried out by the members of the NESSoS consortium in order to achieve the integration of the NESSoS community with other relevant communities in the area of secure service engineering. We also show the research activities and collaborations that are taking place within the consortium, including associated partners.
1 Introduction

The ultimate goal of NESSoS is to build a long-lasting research community in the area of secure service engineering that brings together all the practitioners in this area and other close related areas. In this sense, one essential step towards the creation of this community is the identification of relevant research gaps and the alignment of activities with other research communities that makes possible the integration of research agendas in secure service engineering.

NESSoS consortium consists of partners, who are well known and make relevant research contributions in the area of secure service engineering. Nonetheless, the fragmentation of the communities is a fact and, thus, some significant effort is required towards the reduction of the fragmentation of the communities involved.

During the first year of NESSoS, the consortium started the integration at an internal level. As a result, different collaborations were started and are still taking place among the partners. This trend also has continued during the second year, including this time the associated partners. In more detail, we can classify the collaborations into joint research collaborations, publications, Ph.D. supervision, and organization of events.

Beyond the collaboration among NESSoS core and associated partners, the NoE has been involved in a series of events together with other communities, mainly European. The main objective has been to show in these events the NESSoS research and integration efforts towards the reduction of the fragmentation in the area of secure service engineering. Additionally, NESSoS has been present in other congresses and conferences where we have been able to identify existing gaps with some other communities at the international level.

It must be pointed out that an important step for setting the layout for an integrated future research is the development of a roadmap that proposes the research lines that should be proactively considered by the community. For this reason, the NESSoS consortium has elaborated a roadmap as part of those integration activities. It is presented as a separated document, due to space restrictions of the current document.

Actually, the structure of the deliverable is as follows. In first place, Section 2 presents the research collaborations that are being carried out within the NESSoS partners, including associated partners. As we have already mentioned we have classified these collaborations into joint research (JR), that in some cases has led or is leading to Joint publications (JP), Joint Project Proposal (JPP), Joint organization of events (JOE) and Joint PhD supervision (JPhD). The analysis that we have carried out on the existing collaborations tells us that all the NESSoS partners are collaborating with at least four other partners.

Then, in Section 3 we show a description of all the activities that NESSoS has participated in as a way to reduce fragmentation. We list the events that the NESSoS consortium has organized together with other communities or events where we have participated by presenting NESSoS results. Considering as a reference the set of research topics identified as relevant for the NESSoS community, we have subsequently analysed which of the related communities we have approached in a closer way, and for which ones we need to make a stronger effort in the near future. We also consider the events we have attended in order to identify topics addressed by other communities to which we could approach for the future.
In Section 4 we report on the Network and Liaison Advisory Board (NaLAB). Firstly, we report on the constituency of the members of the NaLAB and their main research interests. Secondly we report on the initial activities we have performed together with them. Finally, Section 5 concludes the deliverable and outlines the future work.
2 Joint Research Activities

As it was mentioned in [D4.1_I], we have followed an onion strategy for the integration of the activities of the NESSoS community. The inner layer of the onion corresponds to the concentration on the activities that are carried out within NESSoS partners, and the following layer corresponds with the integration with associated partners. In this section, we will review the results of those integration strategies. Further details up to M18 can be found in [ID12.3]. We have classified these results into the following categories:

- Research collaborations. This includes joint research carried out within NESSoS and more advanced research giving as a result joint publications and supervision of PhD students
- Joint project proposals
- Organization of events

Section 2.1 describes the integration activities within the NESSoS consortium, whereas Section 2.2 include those activities performed with associated partners.

2.1 Collaborations within NESSoS Consortium

The main research results achieved by the NESSoS consortium are reflected in the number of publications, but obviously they are not the only ones. The consortium achieved a total number of 172 publications, from where 21 were joint publications. In the following, we will describe the peer-to-peer collaborations taking place at the moment among NESSoS partners.

Joint research and publications

- Trust and Contract management → INRIA
- Testing XACML security policies → INRIA
- Quantitative analysis of security (SESAMO project) → Research starting with SIEMENS
- Secure service composition and several joint publications related to this → UMA
- Services and trust management. Investigating the possibility of starting a new joint research line → UMA

Joint Project Proposals

- Project proposal on risk management → ATOS
- FET proposal together → ATOS and UNITN
- Project proposal on risk management → SINTEF
- Project proposal at EIT ICT Labs -> ENG/SAP/TU/e (associated and IAB partners)
**Joint organization of events**

- Clustering activities in the ambit of the EFFECT+ project (where CNR manages the service&cloud cluster) \(\rightarrow\) ATOS
- Organization of events such as the NESSoS industry seminar as well as NESSoS special session at FIA Poznan (together with other EU projects) \(\rightarrow\) ATOS
- FOSAD/NESSoS school for 2011 and 2012 \(\rightarrow\) UMA, IMDEA and CNR cooperate in the definition of the scientific program as part of the FOSAD Steering Committee;
- In the ambit of the EU CSP Forum 2012, CNR was a catalyst to activate a cluster workshop with other projects as ANIKETOS, ASSERT4SOA (managed by Ernesto Damiani, associate partner of NESSoS) and FI-ware where \(\rightarrow\) UMA is the NESSoS representative
- Organization of the ERCIM STM 2012 in Pisa during ESORICS 2012 \(\rightarrow\) UMA, as the head of the STM Working Group.
- Organization of the workshop MDSec \(\rightarrow\) ATOS, LMU, INRIA

We summarize the joint activities of CNR in Table 1 by using the following terminology that, from now on, will be also used for the tables of the other partners:

- **JR** means that joint research is being carried out
- **JP** If the research produced joint publications
- **JPP** means joint project proposal
- **JOE** will stand for joint organization of events
- **JPhD** for joint PhD supervision

<table>
<thead>
<tr>
<th></th>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATOS</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>INRIA</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KUL</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LMU</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SIEMENS</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SINTEF</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UMA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UNITN</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

*Table 1-CNR Collaborations*

Black checkmarks indicate two by two collaborations, whereas non-black checkmarks indicate that three or more partners have carried out the same collaboration. For example, in Table 1, CNR has collaborated with ATOS in a Joint Project Proposal, but it has also collaborated with ATOS and UNITN in another Joint Project Proposal. Likewise, CNR has collaborated with ATOS, INRIA and LMU in the Joint Organization of an Event.
ATOS

Joint research and publications
- Collaboration on research carried out under WP7 that led to a publication → INRIA
- Ongoing triple collaboration that has led to joint publications and still will do in the future on model-driven security and business workflows → ETH, IMDEA
- Evaluation of methodologies against scenarios in WP11. In particular linking CORAS → SIEMENS
- Joint PhD supervision → IMDEA
- Comparison of tools for WP2 → LMU
- Linking CORAS to PRRS → SINTEF

Joint Project Proposals
- See CNR’s collaborations on joint project proposals

Joint organization of events
- Organization of the workshop MDSec → CNR, LMU and INRIA
- See CNR’s collaborations on events organization
- End-Customer for e-Rise → UNITN

<table>
<thead>
<tr>
<th></th>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNR</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>ETH</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>IMDEA</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>INRIA</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>LMU</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SIEMENS</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SINTEF</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>UNITN</td>
<td></td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

Table 2-ATOS Collaborations

ETH

Joint research and publications
- Ongoing triple collaboration that has led to joint publications and still will do in the future on model-driven security and business workflows → ATOS, IMDEA
- Algorithmic verification of protocols and services → INRIA
- Integration of UWE and ActionGUI → IMDEA, LMU
### IMDEA

**Joint research and publications**

- Ongoing triple collaboration that has led to joint publications and still will do in the future on model-driven security and business workflows \(\rightarrow\) ATOS, ETH
- Joint PhD supervision \(\rightarrow\) ATOS
- Information flow and verification techniques \(\rightarrow\) KUL
- Integration of UWE and ActionGUI \(\rightarrow\) LMU, ETH
- Model-driven security \(\rightarrow\) LMU
- Model-driven security and information flows. An analysis of the dynamic access control rules for a clinical e-Health scenario, concerning the privacy of e-Health Records and an automatic analysis of the amount of information leaked in side channels for caches (publications) \(\rightarrow\) SIEMENS

### INRIA

**Joint research and publications**

- See CNR, ATOS and ETH collaborations
- A requirements-based approach to runtime reconfiguration of security policies \(\rightarrow\) KUL
- Trust architectures and implementation of models by using Kevoree (INRIA’s tool) \(\rightarrow\) UMA

**Joint project proposal**

- The project has been accepted in call 9 of FP7 and is called DIVERSIFY \(\rightarrow\) SINTEF
Joint organization of events

- Organization of the workshop MDSec at MODELS → CNR, LMU and ATOS

<table>
<thead>
<tr>
<th></th>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNR</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>ATOS</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ETH</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>KUL</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>LMU</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>SINTEF</td>
<td></td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>UMA</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 5-INRIA Collaborations

---

**KUL**

Joint research and publications

- Information flow and verification techniques → IMDEA
- A requirements-based approach to runtime reconfiguration of security policies → INRIA
- Activity in other projects → SINTEF
- Security patterns → UDE
- Dynamic reconfiguration and policy enforcement and metrics and empirical evaluation → UNITN

<table>
<thead>
<tr>
<th></th>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>IMDEA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>INRIA</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SINTEF</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>UDE</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNITN</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Table 6-KUL Collaborations

---

**LMU**

Joint research and publications

- See ATOS, ETH, IMDEA collaborations tables
- Extension of the UWE navigation model Modeling e-Health scenarios with UWE → SIEMENS
• Connections of SDE and CBK → UDE

**Joint events organization**
• Doctoral symposium at ESSoS 2012 → SIEMENS
• MDSec workshop at Models 2012 → CNR, ATOS, INRIA

<table>
<thead>
<tr>
<th></th>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>ATOS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>CNR</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ETH</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>IMDEA</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INRIA</td>
<td>✓</td>
<td></td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEMENS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
<tr>
<td>UDE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td></td>
</tr>
</tbody>
</table>

*Table 7-LMU Collaborations*

---

**SIEMENS**

**Joint research and publications**
• See previous collaborations of other partners (CNR, ATOS, IMDEA, LMU)
• Work on e-Health scenarios → SINTEF
• Work on privacy location services for Wireless Sensor Networks to be applied to the smart grid scenario → UMA
• Applications of trust to web services → UMA

**Joint events organization**
• Doctoral symposium at ESSoS 2012 → LMU
• Organization of ISARCS, a workshop of CompArch → UMA

<table>
<thead>
<tr>
<th></th>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNR</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>ATOS</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>IMDEA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>LMU</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>SINTEF</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UMA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>

*Table 8-SIEMENS Collaborations*
**SINTEF**

<table>
<thead>
<tr>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNR</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>ATOS</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>INRIA</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
<tr>
<td>KUL</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>SIEMENS</td>
<td>✓</td>
<td></td>
<td></td>
<td>✓</td>
</tr>
<tr>
<td>UMA</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNITN</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table 9-SINTEF Collaborations*

**UDE**

**Joint research and publications**
- See KUL and LMU collaborations
- Ongoing work on specification of trust requirements for cloud → UMA
- Requirements conflicts analysis → UNITN

<table>
<thead>
<tr>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>KUL</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>LMU</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UMA</td>
<td>✓</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>UNITN</td>
<td>✓</td>
<td>✓</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

*Table 10-UDE Collaborations*

**UMA**

**Joint research and publications**
- See collaborations for CNR, INRIA, SIEMENS and UDE
- Trust-based threats identification. Paper submitted to ESSoS 2013 → UNITN

**Joint events organization**
- See joint events organizations for CNR and SIEMENS

<table>
<thead>
<tr>
<th>JR</th>
<th>JP</th>
<th>JPP</th>
<th>JOE</th>
<th>JPhD</th>
</tr>
</thead>
<tbody>
<tr>
<td>CNR</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>INRIA</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
<tr>
<td>UDE</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
<td>✓</td>
</tr>
</tbody>
</table>
Joint research and publications

- See previous collaborations

Joint events organization

- See ATOS collaboration details

By observing the tables we can see that all the partners in NESSoS collaborate with a good number of others, where previously this did not happen. We can observe that most of the aforementioned collaborations include joint research, and just after it, joint publications. This is normal, as much of this research will eventually produce publications.

Also, it is worth pointing out that more than a half of the partners have been involved in at least one joint project proposal together with another partner. Obviously, the degree of collaboration in this activity is lower than the one in joint research, as the opportunities to carry it out depend on the available calls where our new ideas could fit.

Seven partners have joined efforts in the organization of at least one event. On the joint PhD supervision side, there have been four partners collaborating in this activity. We are aware that joint PhD theses supervision is a key performance indicator of the research carried out within the project. Therefore, one goal for the next period report will be to foster this activity.

The summary of all the collaborations can be checked in the following figures. Figure 1 shows the research collaborations that are happening within NESSoS. It shows that all the vertices are connected with at least three edges connecting to other partners, which means that all the partners are doing some research work within NESSoS with other partners. Figure 2 depicts the joint publications and Figure 3 the joint organization of events.
Figure 1 Joint research collaborations
Figure 2 Joint Publications
2.2 Collaborations with Associate Partners

CNR

- Paola Inverardi (and her group), University of l'Aquila
  - Definition of an approach for analysis and monitoring of dependability and security in dynamic system connection
  - Proposal for joint projects
  - Joint papers
- Yves le Traon, University of Luxemburg
  - Definition of methodologies for automating Test Generation based on Access Control Policies specifications.
  - Joint papers
- Matthias Buechler (Technische Universität München Institute of Informatics, Alexander Pretschner group)
  - Comparison and possible integration of methodologies for Security Testing of Web Applications with approaches based on access control policies
  - Joint papers
**SIEMENS**

- Joint publications

**KUL**

- SAP (work inspired by SIEMENS): web security

**SINTEF**

- Alexander Pretschner is guest scientist in the Norwegian part of the DIAMONDS project which is led by SINTEF

On the other hand, the NESSoS associated partners participated into several NESSoS activities, in particular, events organization:

- Sandro Etalle organized ESSoS 2012; He is serving in the Scientific Committee of the FOSAD school
- Jan Jürjens is program co-chair of ESSoS 2013, He has been also a NESSoS speaker at FOSAD 2012 school
- Alexander Pretschner is the general chair of ESSoS 2014, He was invited speaker at the NESSoS workshop in Usage control organized during the NESSoS meeting at ETH Zurich in June 2012
- Ernesto Damiani (University of Milan) co-organized the NESSoS sponsored Workshop on Web Service Security Contracts at EU CSP Forum
3 NESSoS Activities for Achieving Integration

The integration of research agendas requires the alignment of activities with other communities working on similar areas, or in some cases in areas where we believe NESSoS research topics can be beneficial to the whole research community.

This section presents a detailed description of the activities that have been carried out by NESSoS partners in order to expand the secure service engineering community. It is organized as follows. Section 3.1 addresses the meetings where NESSoS partners discuss about the evolution of the project. The NeSSoS flagship event, namely the ESSoS conference, is presented in Section 1.1. Then, in Section 3.3, we provide insight into the collaboration activities that have been performed with external communities. Section 3.4 discusses other relevant events where NESSoS, although more passively, has had presence. Section 1.1 describes activities targeting at education and training purposes, whereas Section 3.6 summarizes one of the most important expected outputs from NESSoS: the roadmap, which is fully available in [D4.2_partII].

3.1 NESSoS Meetings

NESSoS meetings are assumed to be a main tool for cooperation with other activities. We summarize some of them here, and later we give more details. Indeed, in October 2011 we organized a review rehearsal meeting in Poznan, collocated with Future Internet Assembly (FIA) and the first NESSoS industry/research seminar. Then, last February, NESSoS plenary meeting in Eindhoven was collocated with the ESSoS (International Symposium on Engineering Secure Software and Systems) conference (as usual), our flagship event. Also, NESSoS plenary meeting in June was collocated with ICSE (International Conference on Software Engineering), the main conference in Software Engineering worldwide. Moreover, in September, the NESSoS plenary meeting in Pisa was collocated with the ESORICS (European Symposium on Research in Computer Security) conference, the main event in Europe in Computer Security. This strategy has allowed other communities to eventually know us (as NESSoS community), what definitely has been a main achievement of this second year.

The NESSoS events are also open to participation from associate partners. In this sense, Sandro Etalle (Technical University of Eindhoven) and Yves Le Traon (University of Luxembourg) attended the aforementioned NESSoS meeting in Pisa. They presented their research interests that nicely fit the NESSoS topics:

- Software testing
- Model-driven security
- Security modelling and design

Additionally, Erik Poll (Radboud University Nijmegen) attended the Eindhoven Plenary meeting of NESSoS (collocated with ESSoS’12) hosted by Sandro Etalle.

3.2 Flagship Event: ESSoS Conference

The International Symposium on Engineering Secure Software and Systems celebrated in 2012 its fourth edition. This event has been set as the NESSoS flagship event as the topics of
the symposium clearly considered most of the research topics that are being addressed by the consortium.

The development of secure software and services is a challenging issue that is becoming a core ingredient in today’s systems. The complexity of modern systems and the huge variety of available software technologies make essential the consideration of engineering techniques that could improve the security properties of those systems and applications. This task, however, is far from being straightforward and would greatly benefit from drawing the attention from the academia. Surprisingly, very few conferences are devoted to these issues.

Hence the idea of this symposium, the goal of which is to bring together researchers and industrial parties to advance in the area of secure software engineering. As the interests of the ESSoS community and NESSoS are strongly linked, NESSoS is one of the sponsors of the event and collaborates with organization, as some NESSoS partners are part of the steering committee of the conference. This year’s event was held in Eindhoven (Netherlands) in the premises of TUe (Technical University of Eindhoven), one of NESSoS associated partners. The programme included two days of research papers, where three NESSoS papers were presented. Besides the specific programme based on reviewed papers, this year a Doctoral Symposium was organized by NESSoS (SIEMENS and LMU) in order to give PhD students in the area the opportunity to present their ongoing research works, share opinions and obtain feedback. The programme of the doctoral symposium included nine presentations of PhD theses that are being carried out under the umbrella of NESSoS. It is worth noticing that the editions of ESSoS’13 and ESSoS’14 are already under organization. This basically shows as the main event we were planning to establish is up and running.

3.3 Participation in Activities with Other Communities

Next, we are describing the NESSoS activities carried out together with other communities. These activities were usually in the framework of major events where we considered NESSoS could enrich the proposed agendas by including the view of NESSoS on secure service engineering. The major events where these activities took place are the following:

- Future Internet Assembly week.
- BIC project meetings.
- Cyber Security and Privacy (CSP) forum.
- Schloss Dagstuhl venue.
- ESORICS and its collocated workshops.
- Italian technological platform in homeland security.
- Model-Driven Security workshop

Subsequent sub-sections give insight into the activities performed within the scope of each of the aforementioned events.
3.3.1 Activities organized during the FIA Week

The Future Internet Assembly (FIA) is a collaboration initiative among projects that have seen the need for Europe to collaborate, strengthen and integrate the European activities towards a Future Internet that help Europe maintain competitiveness.

The FIA currently includes projects that are part of Challenge 1 of the ICT FP7. The research areas of these projects are:

- The network of the future
- Cloud Computing, Internet of Services and Advanced Software Engineering
- Internet-connected objects
- Trustworthy ICT
- Networked Media and Search Systems
- Socio-economic considerations for the Future Internet
- Application domains for the Future Internet
- Future Internet Research and Experimentation (FIRE)

As part of their activities the assembly organizes meetings where interested parties meet and discuss their research points of view in the area of Future Internet.

Integration with NESSoS. Being Future Internet the main scenario of application of NESSoS, it seems reasonable for the project to approach this community and to organize events together. In particular, NESSoS organized two events during the FIA week in Poznan in October 2011 clearly orientated to pursue integration with this community. NESSoS organized a session where the objective was to discuss about how we can build trustworthy Future Internet services, being this, the main research goal of NESSoS. The other event was the first industry seminar, which is being described below and in [D14.3].

FIA also organized another event in June 2012 on roadmapping activities and NESSoS presented there their research roadmap on secure service engineering.

3.3.1.1 Session: Building a Trust Framework for Future Internet Services and Infrastructures

The session was organized by several EU projects or initiatives being NESSoS one of the organizers. The session focused on how the concept of trust should be approached addressing three different dimensions:

- Network-centric trust
- Component-centric trust
- User-centric trust

Aljosa Pasic (ATOS) presented the NESSoS approach in these terms, based on the devising of mechanisms to validate or manage assumptions relating to architectural design and engineering for secure services; design and run-time validation; simulations; prediction of the security status of a system, etc.
3.3.1.2 First NESSoS Industry Seminar on Secure Service Engineering (as a workshop of ServiceWave 2011)

The ServiceWave 2011 conference was collocated with the FIA week in Poznan. This conference is part of a series organized by academia and industry parties, and its organizers include the ETP platform and the S-Cube NoE, which are dedicated to software and services. Besides this, other ETPs are involved in the organization of this conference.

Being an interesting event for service and software community, NESSoS approached it and organized its first industry seminar as part of the conference. The topic of the workshop was on secure service engineering but from the industrial point of view. Thus, we invited Gary McGraw as invited speaker, who is a member of our IAB. Other industry and academic contributors offered their points of view on the topic.

3.3.1.3 FIA Roadmapping Session

In June 2012 FIA organized the FIA roadmapping session. One of the objectives of FIA is to produce a roadmap on Future Internet that serves as an input for the Horizon 2020 programme. The production of a roadmap in the area of secure service engineering is also one of the main objectives of NESSoS, therefore this event served as a way to obtain feedback from the FIA community to the NESSoS roadmap and the other way around.

The NESSoS roadmap was presented there obtaining very valuable comments from the audience, which was composed mainly of those who have contributed to the FIA roadmap from industry, academia and stakeholders. A main comment was on how we are going to approach the raise of user security awareness. This topic seems to be highly considered and very convenient for achieving a successful deployment of FI scenarios.

3.3.2 BIC Project Meetings

The Building International Cooperation (BIC) for Trustworthy ICT is a EU-funded project coordinated action that intents to promote research programmes in the area of Trustworthy ICT with new emergent countries such as Brazil, India and South Africa. In order to achieve their goals, the project organizes different events for bringing together researchers of all the aforementioned countries and European researchers. One of these events is the BIC Annual Forum. As a first step of the realization of this forum, topics of interests in the area of trust and security were identified to be included in the agenda.

**Integration with NESSoS.** In its effort of integrating research agendas NESSoS attended several BIC meetings in order to learn how the integration can be done outside Europe. Several topics of interest to NESSoS partners were discussed in these meetings. Privacy and, especially, trust, were widely covered as context-dependent areas, where location and other factors determine the way they must be ensured. In order to make security easily accessible by different users’ profiles, security management was identified a crucial issue to address. Also, assurance and risk and cost-awareness along the SDLC were considered primary areas of research that need further insight.

Next, we describe NESSoS participation in these events.
### 3.3.2.1 First BIC Annual forum

The first BIC Annual Forum was held in Brussels on the 29th of November 2011. The event consisted of several panels where the possibilities for international cooperation in the area of Trustworthy ICT were analysed. In particular, NESSoS, represented by Fabio Martinelli, contributed to the panel on “Human oriented approaches to security, privacy and trust and how international cooperation can provide mutual benefits”. Following this event, several research items came up for the agenda on international cooperation. We highlighted the following ones:

- Multidisciplinary international cooperation through the creation of international cooperation or working groups. Security management was identified as a key point as it should be accessible for all kind of users.
- Privacy issues should be dealt with in an international level taking into account that different locations could mean different preferences on privacy.
- Secure software-services development. In this point, NESSoS was the main contributor and the NESSoS research topics were shown to the audience, concentrating on the aspects of assurance and risk and cost-aware of the SDLC.
- International approaches to trust. Similarly, as in the case of privacy, trust issues should be taking into account the context where trust is going to be used.

### 3.3.2.2 BIC Working Groups Meeting

During the WG1, Human oriented/citizen approaches for trust, privacy and security, meeting several presentations were given. These presentations were divided into different sessions following the topics dealt with during the panel held at the BIC annual forum. This time the approach that NESSoS presented deepened on the role of trust management in secure software services (Fabio Martinelli). Other relevant presentations considered data and privacy protection, user centricity or social computing and the influence of security in it.

### 3.3.3 Cyber Security & Privacy EU Forum (CSP)

The Cyber Security and Privacy EU forum is a conference organized by the EU funded project Effectsplus and the former Trust and Security Unit. This conference was held in Berlin (Germany) on 24-25th of April 2012. Fabio Martinelli (CNR) was among the organizers of the event.

The main purpose for the creation of this forum was to bring together all the parties involved in research in the area of security and privacy from different sectors such as academia, industry or policy makers. This forum gave them the opportunity to exchange impressions and ideas about the state of research in privacy and security nowadays and about the main gaps to be solved in the future.

The event was organized in different slots each of them dealing with different topics in the area of security and privacy:

- Demos session. One of them organized by Trust in digital Life, where experimental results developed under its umbrella were presented; and the other one organized by the BonFire project devoted to present the ExSec experiment.
- Posters. Some EU projects exhibit their posters as well as other institutions, showing their research areas.
- Workshops organized by some projects or initiatives.
- Two tutorials, one of them organized by NESSoS (more details on it will follow).
- Cluster workshops. Effectsplus identified several clusters, which organized different workshops for the CSP forum. The projects participating in these clusters participated also as panellists of them by presenting the views of the projects they represent with respect to the topic of the project. Thus, NESSoS, together with other projects in the Services and Cloud cluster organized the workshop on Web Service Security Contracts.
- Invited talks by three keynote speakers from different sectors, including the European Commission.

**Integration with NESSoS.** As the event was devoted to security and privacy these areas were horizontal along the event. Very similar is the case of trust, which is very related to privacy and security issues. However, there were some other more specific topics that deserved several discussions. For example, assurance and service composition were considered relevant issues, especially in SOA infrastructures where services and applications are made up of smaller, composable services. Lastly, risk management and its application along the whole SDLC were discussed as well.

In the following we will describe some of the sessions, which topics overlap with the topics of NESSoS, or are directly NESSoS events.

### 3.3.3.1 Workshop on Web Service Security Contracts

The aim of this workshop was to bring together different views from relevant EU projects and standardization bodies in the area of Assurance Level Agreement (ALA) for SOA. The project was organized by the EU projects ASSERT4SOA, Effectsplus, FIWare, NESSoS and ANIKETOS.

The speakers of the workshop presented how their respective projects tackled the problem of assurance by design and assurance by contract. All the panellists agreed that there is the need to work towards a common notion of ALA that will include models and languages for determining assurance of services implemented by a SOA infrastructure.

As a result of this workshop, all the projects involved and some attendees from the audience agreed on working together towards standardization in this area. NESSoS will participate in this standardization attempt, as assurance is one of the main topics of research of NESSoS. In a lower extent, but still present in this workshop the area of Secure Service Composition was also considered as this topic is constantly present on web services. The first step towards it has been taken and some effort is already being dedicated to this.
3.3.3.2 Tutorial workshop: Analysing risk in practice: the CORAS approach to model-driven analysis

This tutorial was organized and presented by SINTEF. The main purpose of this tutorial was to introduce CORAS, a model-driven risk analysis methodology. Risk analysis has been considered by the NESSoS consortium as one of the main transversal topics for research, therefore the topic of this tutorial clearly covers one of the major interests of NESSoS. In this case, the audience of this tutorial learned about the Project and the approach that we are taking concerning risk analysis.

3.3.3.3 The GINI Concept of the INDI Ecosystem: Self-created, self-managed, self-controlled identity services.

The purpose of this workshop was to present the GINI Support Action. The main objective of this support action is to analyse a Personalized Identity Management (PIM) ecosystem in which individuals can manage their own digital identities and control the exchange of their identity information. Even though the topic of Identity Management is not a proper topic of the NESSoS short-term, it has been identified by the consortium as a relevant topic to be considered in the near future. Therefore, from the NESSoS project we are very interested in knowing the state of the art in the area as well as what the community dedicated to this topic foresee as relevant lines of research on it.

3.3.4 Schloss Dagstuhl

The Schloss Dagstuhl-Leibniz Center for Informatics is one of the most popular venues for computer scientists to meet. It fosters the exchange of knowledge among practitioners, young researchers and very-well known senior researchers.

The way this is achieved is by the organization of seminars and workshops, with the objective of promoting research topics that will be of interest for the research community. One the organized events was “All Meets Formal Software Development”, where NESSoS partners were also involved.

There are several bodies and boards for the activities of these events. One of these boards is the Industrial Curatory Board. SIEMENS, and more specifically, Jorge Cuellar, is part of this board. As part of the board, he attended the meetings they organized.

Integration with NESSoS. The events and seminars organized at Dagstuhl are very-well known by their excellence and quality. It is therefore a key community to approach by NESSoS. Clearly, the event held on formal methods intersects with the interests of NESSoS, and even more, when the focus is on industry. Most of the times, industry players find it difficult to implement formal methods approaches that will enormously benefit them, but in contrast it is hard for them to assess the costs and risks to do it. Other events organized by NESSoS partners have already been planned at Dagstuhl; in particular the Seminar on Quantitative Security Analysis, organized by Boris Koepf (IMDEA) is on one of the emerging topics where NESSoS community is interested in.
3.3.5 ESORICS and co-located Workshops

The aim of the European Symposium of Research in Computer Security (ESORICS) is to progress in the research of computer security by establishing a European forum for bringing together researchers in this area, by promoting the exchange of ideas with system developers and by encouraging links with researchers in related areas.

The ESORICS community progressively organises the event in a series of European countries. The symposium is confirmed as the leading European research event in computer security.

The 17th edition of ESORICS was held in Pisa from 10th to 14th of September 2012 hosted by CNR, and sponsored by NESSoS. Besides the main conference, there were several co-located workshops and a NESSoS plenary meeting was also organized at the same time of the event.

Being this event a computer security one, most of the topics covered in it were of interest for NESSoS. In particular, the ESORICS programme included a NESSoS paper, which is a joint paper between SIEMENS and UMA.

Additionally, and as a way to make the computer security community aware about the work being carried out by the project, a booth dedicated to the NESSoS tool workbench was at the ESORICS conference to provide information about it. Someone from LMU was available to explain participants in ESORICS what the NESSoS tool workbench provides in order to include and promote their tools. To support this promotion, a specific brochure for this tool was designed [D12.4] and distributed among the audience of ESORICS.

It is also relevant to mention that this edition of the ESORICS conference has been the one that received the highest number of submissions (250) and for the first time, parallel sessions were established for this conference to accommodate 50 accepted papers.

Integration with NESSoS. In addition to the dissemination activity regarding the tool workbench, several topics of interest for NESSoS partners were widely discussed during the time ESORICS took place. During the last day of the conference and the two days when the workshops took place, a NESSoS plenary meeting was held. In particular, NESSoS organized a workshop on Quantitative Aspects of Security and Assurance (QASA). This workshop included an invited talk by Boris Köpf from IMDEA, a panel organized by CNR and ATOS and some papers showing the NESSoS advances in the area. Furthermore, two of the topics of interest for NESSoS were widely covered in the ESORICS workshops, namely trust and privacy. The former constituted the primary concern in the Security and Trust Management workshop, whereas the latter was discussed in the Data Privacy Management workshop.

3.3.5.1 ESORICS Workshops

Five workshops were co-located with ESORICS, all of them in the security area. However, three out these five workshops had NESSoS involvement or were created with the purpose of integrating it with the NESSoS community.
**International Workshop on Quantitative Aspects in Security Assurance (QASA)**

The International Workshop on Quantitative Aspects in Security Assurance served as a vehicle to bring together researchers in the area of security assurance and the NESSoS consortium. In order to achieve this, QASA was organized as part of the NESSoS meeting and consisted of reviewed papers as well as NESSoS presentations, including an invited talk for the vent, where the audience could learn about the NESSoS approach to quantitative aspects in security assurance.

NESSoS sponsored the QASA workshop together with the SESAMO project. The programme included a panel on “Quantitative Aspects of Security”. The panel included some experts mainly from the industry area including NESSoS partners such as ATOS and SIEMENS; representatives from the SESAMO; VTT (Finland), as well as academic contributions from the Centre for Software Reliability at the CITY University of London and KUL.

**Security and Trust Management (STM)**

The Security and Trust Management is a working group of ERCIM that organizes every year a workshop that aims at bringing together contributions and attendance from academia and industry in the area of security and trust management. This year’s event was organized together with ESORICS in order to specifically improve interaction between both communities. Pierangela Samarati, member of the NESSoS NaLAB is the chair of this working group, and additionally this year was also the PC Co-chair of the workshop that the working group organizes.

Obviously, the same opportunity was present for the NESSoS community and several research papers produced under the umbrella of NESSoS were presented at STM. Besides this close relationship, the programme of the event also included many interesting research topics in the area of security that clearly overlap with the research objectives of NESSoS.

The workshop usually includes a business meeting of the working group where members present to the STM community their work in the area. This year UMA has presented to this community the NESSoS roadmap. The idea was to raise awareness about the elaboration of the roadmap in the area of secure software engineering. We were interested in obtaining feedback and opinions from all the communities, in particular from the STM community. We took advantage of this opportunity and asked for their feedback to those who attended this meeting.

**Data Privacy Management (DPM)**

The 7th DPM International Workshop on Data Privacy Management was also co-located as one of the workshops of ESORICS. As an involvement of NESSoS in this event, Javier Lopez (UMA) co-organized it. Even though privacy is not one of the key topics of research in the NESSoS DoW, it has been identified as a very important topic of research for the future. Therefore, the sessions of this workshop resulted very interesting for the project members who attended them.

These sessions covered a wide range of problems and challenges in the privacy area, including anonymous authentication and location privacy; specification, verification and enforcement of privacy policies, especially in the web context; and mechanisms to ensure citizens’ privacy under certain circumstances, such as during police work.
3.3.6 Second annual day of the Italian technological platform in homeland security (SERIT)

SERIT technological platform, coordinated by F. Martinelli - CNR and C. Leone - Finmeccanica, representing more than 250 partners, was formally approved in 2011 by the Italian Ministry of Education, University and Research (MIUR) as the Italian Technology Platform that deals with issues related to security in the country. It plays the role of aggregator. Its capabilities lay (in particular, industrial) on security, in order to analyse the prospects of national security in the medium and long term, in reference to European and global background. They also aim at defining the requirements needed for research, to draw supply and demand in technological market.

During this year, the SERIT main activity has been to develop an agenda of research and innovation in security for Italy. In few words, a strategic roadmap that can direct the priority areas for future research on security that responds to needs that emerged in the region and, at the same time, in line with the perspectives of research in Europe.

NESSoS sponsored the second edition of the annual meeting Italian Platform for Security, SERIT, at the CNR’s Headquarters in Rome1. NESSoS also contributed to reshape the research agenda (in Italian), by focusing on cybersecurity issues, rather than generic ICT issues for security. The SERIT research agenda has been thus integrated with NESSoS topics.

Integration with NESSoS. The objective of the SERIT platform is to design a research roadmap, which is a shared objective with NESSoS. Thus, as we pointed out above both research roadmaps share topics and therefore, each of them benefit from the other.

3.3.7 Model-Driven Security Workshop

The ACM/IEEE 15th International Conference on Model Driven Engineering Languages & Systems (MODELS 2012) is held this year in Innsbruck (Austria). The conference is the 15th of a series starting back in 1998. Along these years the conference has become one of the most well known and relevant in the area of model-based software and systems engineering, covering all the aspects of modelling from languages and methods to tools and applications.

The conference consisted, as usual, of a main program where reviewed papers are presented and keynote speakers gave specialized talks. Also, satellite events were held. In particular the program included fifteen workshops and twelve tutorials covering different aspects of model-driven engineering.

Integration with NESSoS. It seems that security for the model-driven paradigm has not been widely covered by MODELS so far. It is in this particular aspect where some members of NESSoS tried to fill the lack of security by organizing the workshop on Model-Driven Security (MDSec). LMU, ATOS and INRIA were part of the organization team. The main idea for holding it was to make the model-driven engineering community aware of how security should be included and considered at the very early stages of the SDLC, being this one of the main research objectives of the NESSoS project. The programme included different tracks about

1 http://www.piattaformaserit.it/?cat=37
secure architectures; secure development, access control and cryptography. In particular, two NESSoS papers were presented in this event showing the advances achieved in the area of Model-driven access control by the project as well as one joint paper (CNR-UMA) in the area of secure service composition.

3.3.8 Analysis of the Performed Activities and its Relevance to the NESSoS Community

The goal of this section is to analyse the activities performed under the lens of its relevance to the NESSoS community. For this purpose, research areas of interest for NESSoS are first identified. Then, we identify the research areas covered by the aforementioned activities and check whether they are aligned with NESSoS research areas.

Figure 4 shows a topics diagram where the main research areas addressed by the NESSoS community are identified. An earlier version of this diagram was sketched last year, which has been improved in two ways. First, the overall shape has been changed in order to improve legibility and to reflect the topics from three different angles:

- Service development lifecycle topics: distributed around the purple pentagon, they represent the research areas directly related to the different phases of the service lifecycle.
- Enabling technologies: the research areas around the smaller rectangle represent technologies and mechanisms that, at a higher level of abstraction, leverage services security.
- Properties: the topics around the bigger rectangle identify higher-level properties that must be considered prior to deploying service-based applications.

The second change introduced is the addition of a new topic that the community considered to be important enough to deserve its own slot in the picture: Quantitative Aspects of Security. Further details on this figure and the topics represented in them can be found in [D4.2-II].

From the aforementioned activities we can observe that there are some areas where our participation has been higher and other areas where we should focus on more for future events. Figure 5 depicts a bar diagram that makes explicit the topics more widely covered during the previous activities. As we can observe, the most addressed topic is trust. This is normal as this topic was discussed in several activities, including ESORICS conference (as part of the STM workshop), one of the FIA Week sessions or the one of the BIC project meetings. Privacy has also been widely discussed, as shown by its relevance in ESORICS, where a workshop was devoted to this area, and it was a primary concern also in the Cyber Security and Privacy forum.

The two main transversal topics of NESSoS research, risk and cost-awareness and assurance, have also been targeted in events like CSP tutorials and workshops, the First BIC Annual Forum and ESORICS.

Finally, there are several topics that, although to a shorter extent, have been discussed, such as Identity Management or Quantitative Aspects of Security.

Even though we have approached many of the NESSoS relevant areas of research, it is important to point out some gaps that can be identified if we map the topics in Figure 5 to those in Figure 4. From the analysis of the events we have been involved in, we observe that there are
several topics that have remained untouched, concretely, compliance, user security awareness, autonomic security, security requirements and runtime verification and enforcement. This calls for a joint NESSoS effort in the following year in order to approach the communities that deal with these topics and fill the existing gaps. However, this does not mean NESSoS partners are not actively working on them. NESSoS publications showed the opposite.

Figure 4 Topics addressed by NESSoS
3.4 Other Events

In this section we are going to report on the events that we did not directly participate or organize but we have attended as part of the audience. These events allowed us to find out more about the research trends in the corresponding areas as well to identify those of interest where we can contribute to by having a more active participation.

3.4.1 The European Identity and Cloud Conference (EIC)

The European Identity and Cloud Conference (EIC) is an event where enterprise technologists meet in order to shape and learn about the market in several areas such as Identity and Risk Management, and Cloud Computing. The last edition of the event was held in Munich, from 18th to 20th April, and was organized in several blocks and sessions where a huge amount of topics were reviewed.

Among all of them assurance is one of the central topics that is of interest for the NESSoS research community. In EIC, assurance is analysed in the context of cloud computing by trying to answer several questions such as how a cloud can be audited and which mechanisms can be put in place for cloud computing, which is challenging due to its shared resourcing, multi-tenancy and geo-location features. In the NESSoS roadmap [D4.2_partII] we consider that cloud computing is an emerging scenario application for the FI where the proposed research topics should be validated. Thus, in EIC we observed that at least assurance is already considered and aligned with our proposal of research.

The topic of risk and cost-awareness is horizontal to the Service Development Life Cycle. According to EIC contributions and outputs, the main challenge of this topic is setting the focus and understanding the priority on actions in order to mitigate risks at the businesses level. This level is of particular interest for NESSoS, being one of the goals to achieve (goal G4 in
as business risks and IT risks become more aligned in service-based applications and systems.

Participants at EIC also emphasized the need for coding following standardized application security infrastructures in order to minimize risks and future code-level vulnerabilities. This event also included a session where mechanisms towards user awareness were discussed. Concretely, the focus was on how to allow users to hold control as well as to manage who is able to verify its identity and by means of which procedures.

Finally, EIC dealt with the triad trust, privacy and identity in the cloud context. First, talks were devoted to discuss how identity and privacy could be protected in this environment. Trust frameworks were proposed to leverage open identities and to protect privacy of these identities. Privacy and electronic identity challenges from 2012 and beyond were also discussed.

3.4.2 International Conference on Software Testing, Verification and Validation (ICST)

The IEEE ICST conference aims at all the areas related to software quality, and seeks to address the problems that arise when dealing with software verification and validation. Last edition of the event was held in Montreal (Canada), from the 17th to the 21st of April and comprised a set of workshops, panel discussions, poster sessions and a PhD symposium.

As the name and scope of the conference imply, software testing and, in general, late assurance form the core of the topics presented, which represent a relevant, horizontal area of research within NESSoS.

The main conclusions we can draw from this event is that techniques such as search-based testing can enhance assurance during the last phases of the development lifecycle. Also, automatic testing becomes a necessity as complexity of service-based applications increase, something that is a fact in FI scenarios.

3.4.3 International Conference on Software Engineering (ICSE)

ICSE provides a forum for educators, practitioners and researchers to present latest results and innovations in the field of software engineering. Last edition was held from the 2nd to the 9th of June in Zurich (Switzerland), and, in addition to the main conference, it comprised workshops, co-located events, tutorials and symposiums. Additionally, during the last edition in 2012 a NESSoS plenary meeting was co-located with this conference.

The main conference was split into several tracks, dealing with different aspects of software engineering, ranging from software architecture to software evolution. Late assurance was a relevant topic in this conference, which is especially relevant for the NESSoS community. In this regard, several sessions were devoted to software testing and debugging procedures. A variety of mechanisms were identified as enablers for holistic late assurance, including formal verification, regression testing and tests automation.

Another topic that stood out from the rest was secure programming. The topic was covered by several talks that described mechanisms to detect and predict bugs and defects in code, whereas other talks explicitly addressed best practices and recommendations for safe coding.
A conclusion to draw from this event is that even when late assurance techniques are in place, the quality of service-based applications is greatly influenced and improved by using programming standards of high quality.

### 3.4.4 Formal Methods Seminar at Dagstuhl

A particular community that we have approached in Dagstuhl is the Formal Methods community. One of the members of NESSoS attended the seminar “All meets Formal Software Development”. The objective of this seminar was to bring together researchers, and users of formal methods from industry and research in order to find commonalities and gaps to be filled. Industries usually face problems when trying to adopt formal methods. This problem is also known to the NESSoS partners and some of them contribute towards this within the consortium and particularly for this specific seminar. This is the case of SIEMENS who presented in this seminar the vision of NESSoS regarding how to include the use of formal methods from the very beginning of the software engineering design and not only for verification phases.

Several areas that fall into the formal methods, such as machine learning, automated reasoning, proof planning and theory development, were elicited as useful in order to enhance the processes underlying assurance and runtime verification and enforcement.

### 3.4.5 IEEE Computer Security Foundations Symposium

This conference, created originally as a workshop in the late eighties, provides a forum for researches interested in computer security, especially in the areas of formal models and techniques for verifying security. Last edition was held in Cambridge, MA (USA), from 25th to 27th of June.

If we look at this event under the NESSoS lens, one of the main topics considered is assurance. A corpus of techniques were identified as very relevant in order to enhance assurance and runtime verification and enforcement all along the lifecycle. These techniques include model checking, cryptographic verification, information-flow security and attack discovery.

User security awareness was also part of the event. Research on this area should consider mechanisms to improve usability in authentication mechanisms by means of visual preferences.

### 3.4.6 Principles of Security and Trust (POST)

This new conference of the federated event ETAPS (European Joint Conferences on Theory And Practice of Software), has been recently created though the contribution of several existing communities/workshops such as Formal Aspects in Security and Trust (FAST - initially co-promoted by Fabio Martinelli (CNR) and Theo Dimitrakos (BT)). Fabio Martinelli is currently in the Steering Committee of this conference, and in the one of ETAPS as POST representative. WP9 leader David Basin has been nominated program co-chair for 2013.

Even though the conference is new, it targets excellence regarding research topics on security and trust. As part of them, security assurance has been included in the programme of the event and it is expected to be part of the key topics to be included in the future call for papers. More specifically, 2012’s programme included several papers that considered verification techniques for enforceable policies or verification of security protocols, topics that
fall very much into algorithmic protocol verification, which is considered within the NESSoS research agenda.

3.4.7 Information Security Solutions Europe (ISSE)

ISSE is a Europe’s independent and interdisciplinary security conference that was founded in 1999 as an initiative of the European Commission Directorate General Information Society. The conference provides a forum for educating and informing ICT security professionals and policy makers in a wide variety of security-related topics.

The last edition was held in Prague (Czech-Republic) in a two days programme from November 22nd to 23rd. The conference deals with many of the topics that fall into the security area and more specifically, concerning the area of risk management in the Strategic Industry Solutions session.

A slot was reserved to deal with security management, concretely, on how to counter threats with network behaviour analysis. Also, within the Security Management session, a method to manage risks in value chains was discussed.

Trust is another topic covered by NESSoS that had a representation in ISSE through the special interest track session, where the talk “Trust in Digital Life” was given. Trust was also reviewed in the context of clouds with several trust considerations in these scenarios.

User security awareness was also present in the sessions of ISSE, which is also relevant to the NESSoS community. This session included a campaign developed by the German Federal Administration to increase the information security awareness, as well as studies on the psychological and mental obstacles in awareness campaigns.

Finally, identity management had a strong representation in this event, taken into account from different views, including its legal aspects and its application to e-government applications. From a more technical perspective, a talk reflected how to build identity as a service and how to manage identity in mobile environments, an approach that could be useful for certain NESSoS scenarios, such as patient monitoring.

3.4.8 Component-based Software Engineering and Software Architecture (CompArch)

CompArch is a federated conference that targets the areas of component-based and service-oriented engineering and architecture. Las edition of this event was held in Bertinoro, from 25th to 28th June, and comprised the following events:

• CBSE (15th International ACM SigSoft Symposium on Component-Based Software Engineering): this conference brings together researchers and practitioners with the goal of analysing component-based software engineering form different perspectives.

• QoSA (8th International ACM SigSoft Conference on the Quality of Software Architectures): the aim of this conference is to analyse and describe the quality aspects of software architectures, such as reliability, security or performance.

• ISARCS (3rd International ACM SigSoft Symposium on Architecting Critical Systems): the main topics of this area include how to achieve robust, dependable and secure systems even if this requires accepting some level of service degradation. This edition was organized by Jorge Cuellar (SIEMENS) and Javier Lopez (UMA), who acted as PC co-chairs.
• WCOP (17th International Doctoral Symposium on Components and Architecture): component-based software engineering, architecture and software quality are the main concerns for this doctoral symposium, where young researchers present their more recent results.

• ROSS (Workshop on Reusing Open-Source Components): this workshop aims to study the issues related to reuse of open-source components from technical, process, organizational, legal, and business perspectives.

The topics covered in CompArch are of paramount importance for NESSoS, as they deal with software engineering, which is the core area upon which NESSoS builds its research. CompArch reviews most of the software and service development lifecycle phases, although the highest emphasis is placed on design and architecture. In this area, the focus is often on formalisms to model architectures, evaluation of architectures, and methodologies that support the inclusion of quality attributes at this early stage.

It is however noticeable that security is not a primary concern for the software engineering community, which has been traditionally focusing on the inclusion of other non-functional requirements such as performance. Regardless this fact, NESSoS can greatly benefit from approaching this event (and the software engineering community behind it) as software engineering tools and techniques along the SDLC may yield the foundations onto which to build security. As an example, misuse and abuse case models are basically extensions of traditional use cases models. Another example includes security stereotypes in design models and security annotations in programming environments, which are extensions of traditional design models and programming languages, respectively. In this regard, events like ISARCS are very interesting, as they allow bringing closer the software engineering and security communities.

3.4.9 The European association for e-identity and security (EEMA)

This event is a two days forum where industry, business and administrations can discuss about different areas in the digital identity arena. Last edition was held in Biel (Switzerland), from 27th to 28th March, and comprised TDL (Trust in Digital Life) consortium workshops, where a research and innovation agenda for trustworthy ICT was introduced.

Given that this event targets identity management, this is the main topic where NESSoS intersects the event. However, other topics of interest, especially within the scope of TDL, are also covered by the NESSoS community.

How to achieve effective security management scenarios with multiple stakeholders, which constitutes a major challenge, was discussed in this event.

Trust was analysed in the context of e-Health scenarios and also under the lens of trusted reputation systems. Privacy was also considered in the context of Internet voting mechanisms and mobility scenarios.

EEMA also organized together with OASIS and Microsoft, among other partners, the European Identity Management Conference (EIMC). It constituted a forum to discuss about security in today’s personal, business and government processes, taking e-identity as the core enabler of them.
3.5 Education and Training Activities

- **e-RISE event 2012**: the Training and Application week of e-RISE 2012 challenge took place at the University of Trento from May 7th to 11th. Forty-two participants were involved: twenty seven participants were professionals with a minimum of five years of working experience in the field of Auditing in Information Systems attending an MBA at Dauphine University in Paris. Fifteen participants were MSc Students in Computer Science from Trento with a background in Security Engineering and Information Systems.

  Five research groups have been invited to join the challenge and to give a tutorial to the participants about their methods on security requirements elicitation and risk analysis. The methods were CORAS from SINTEF, LINDUNN from Katholieke Universiteit Leuven, SECURE TROPOS from University of East London, SREP from University of Castilla-la Mancha, and SECURITY ARGUMENTATION from Open University.

  Moreover, two industrial partners: Siemens and Atos have participated by providing two case studies about the management of electronic health care records and the smart grid systems.

  The Training phase started on May 8th when participants have attended tutorials by method designers about the method they are going to use for the analysis of the scenario. On May 9th and 10th participants have been introduced to the case studies. The face-to-face Application phase lasted two days, May 10th and 11th, where the participants divided in groups have applied the security engineering methods on the two case studies.

  The preliminary feedbacks of the participants have been collected through questionnaires and short presentations given by the groups in the afternoon of May 11th.

  The second phase of eRISE 2012 took place at Dauphine University in Paris from June 14th to June 15th.

- **FOSAD summer school**: Fabio Martinelli (CNR) has been appointed as new chair of the FOSAD Steering Committee.

- **Future joint ANIKETOS/NESSoS/IFIPTM summer school**: we are organizing a spring school to be held in Malaga together with the IFIPTM 2013 spring school, where Fabio Martinelli will be the chair of the school. This will be a good opportunity for NESSoS to approach the IFIPTM community and organize and event together. The project ANIKETOS will be also part in the organization.

3.6 Roadmapping Activities

  One of the pillars for the integration of agendas is the design of a roadmap in the area of Secure service Engineering. During the first year of the NESSoS project, the partners developed a roadmap [D4.1_II] that included the main topics that they consider for research in the mid-long term period.

  The roadmap starts with the premise that there are two major changes driving the evolution of ICT: the shift towards a service-based ICT and the tightening between the virtual and physical world. From these assumptions, and considering that this evolution is to be
steadily increasing during the following ten years, NESSoS partners develop a view on the research areas that should be of crucial concern under these conditions.

These research areas are organized into crossing research themes and enabling methodologies and technologies. The former describe research topics that are horizontal to the service development lifecycle, whereas the latter discusses, on the one hand, a set of research topics that addresses security at every stage of the SDLC, and on the other hand, research areas that ensure certain properties required for achieving trusted, secure service-based applications.

The crossing research themes include risk and cost-awareness and assurance. Developers must consider these areas in every phase of the SDLC in order to ensure that risk and cost remain stable and controllable all along the project duration, and in order to be able to verify that trust and security properties are being held in every phase as the project moves forward.

Enabling technologies and methodologies include those research areas involved in every phase of the software development lifecycle, from security requirements engineering to runtime verification and enforcement. Given the aforementioned vision of a service-based ICT, service composition and adaptation becomes a SDLC phase of paramount importance.

There are other enabling technologies that may be considered on top of the previous ones, which are motivated by the increasing complexity of ICT and the goal of which is to smoothly pave the adoption of FI by users and developers. Examples of these areas are users security awareness and security management.

Finally, there are general properties that must be ensured in order to guarantee the success of the 2020 vision, and they result from the increase of interoperability, heterogeneity and privacy concerns. These properties are compliance, trust, privacy and identity protection.

The second version of the roadmap elaborates on the same topics that we identified as relevant in the first version by considering their advance on the state of the art as well as our advances as a consequence of the research results achieved within NESSoS. In this second version, the vision and opinions of the associated partners and the IAB have also been taken into account.

In addition, these major changes, other improvements have been carried out. In order to provide the context onto which the roadmap ideas are to be realized, a new section describing two FI scenarios has been added. Another section has been created to make the goals of the document explicit as well as the gaps that must be overcome to achieve them, providing a more solid justification of the research areas identified. Finally, for the sake of higher legibility, the document has been partially restructured.

The complete roadmap can be found in a separate document [D4.2_II].
4 Report on the NaLAB Activities

As described in the NESSoS DoW, the Network and Liaison Advisory Board (NaLAB) consists of a set of experienced researchers that play a significant role in the scientific community. The main objective for the constituency of this lab is to act as a bridge with international research communities for fostering cooperation with other communities. In order to achieve this objective we invited for this task two very well-known researchers in the different pillar areas of NESSoS, mainly from outside Europe.

The chair of the NaLAB is Javier Lopez from UMA. The members of the NESSoS NaLAB are listed below:

**Ron van der Meyden** is a professor at the School of Computer Science and Engineering at the University of South Wales in Sydney (Australia). His research is mainly concentrated in formal methods. More specifically in theory for computer security, logic of knowledge and belief, temporal logic or theory of distributed systems. He is editor of several journals and member of the program committee of many important conferences in his area of research. He is also author of many papers.

**Moti Yung** is a research scientist working at Google Inc. He is also Adjunct Professor of Computer Science at the Columbia University (US). Before joining Google he was technical director at RSA Labs, Vice-president and chief scientist at CertCo and researcher at IBM. He belongs to the Security, Cryptography and Privacy area of research at Google. He is very active participating in the organization of events in the area of security and is authoring many papers in the area.

**Martin Abadi** is Principal Researcher at Microsoft Corporation, and Professor at the University of California at Santa Cruz (US). His main research interests are in the areas of security, programming languages and systems and specification and verification. He is very well known for his work on the formal specification of authentication protocols (BAN logic) and from there his efforts have concentrated in the formal specification and reasoning of security properties.

**Pierangela Samarati** is a Professor at the Computer Science Department of the Università degli Studi di Milano (Italy). Her main research interests are access control policies, models and systems, data security and privacy, information system security, and information protection in general. On these topics she has published more than 200 peer-reviewed articles in international journals, conference proceedings, and book chapters. She is chair and coordinator of several working groups and technical committees as well as member of the program committee of many conferences and workshops in the area of privacy.

As we mentioned above he members of the NaLAB are very active and well-known researchers in their respective areas. In particular, they are involved in some areas that are of interest for the NESSoS community such as security in general, formal methods or privacy. More specifically, the areas of assurance, security support in programming environments, quantitative security, run-time verification and enforcement, users security awareness and security management as well as privacy, trust or identity management are research topics that
are specifically the main interests of the NaLAB members. We believed it was of paramount importance that the industry players were represented in this board, as it is reflected by the inclusion of Martin Abadi and Moti Yung working at Microsoft and Google research respectively.

Activities

- Moti Yung organized together with CNR ESORICS’12. He was program co-chair of this event.
- Pierangela Samarati also took part of ESORICS’12 as program co-chair of STM’12, one of the workshops of the conference.
- Pierangela Samarati was an invited speaker at the IEEE CRISIS conference (sponsored by NESSoS).
- Pierangela Samarati was invited speaker at the FOSAD School.
- Martin Abadi is serving in the FOSAD school scientific committee and gave a talk at the FOSAD school in 2012.
5 Conclusion

Achieving an integrated corpus of knowledge on secure service engineering requires drastically reducing the divergence between different research communities that have been traditionally working in different directions.

This deliverable reports on the activities that have been carried out in order to reduce this divergence. The strategy has been developed in two fronts in parallel: on the one hand, joint research activities have been performed in order to reduce the fragmentation and to foster cooperation within the NESSoS consortium. On the other hand, several activities have been carried for building bridges and connections with other communities.

Regarding the joint research activities, we have classified them into joint research, joint publications, joint organization of events, joint project proposals and joint Ph.D. supervision. It is worth remarking that all the NESSoS partners have collaborated or are collaborating with at least five other NESSoS partners and that the ongoing collaborations will in most cases produce joint research publications. Also, collaborations are taking place with associate partners.

As for the activities for external integration, we have divided them in several groups. In the case of the participation with other communities, we have performed an analysis, contrasting the approached research areas with those of interest for the NESSoS partners. We can draw two conclusions from this analysis: the first one is that we have made an important effort towards covering different, heterogeneous research areas; the second conclusion is that we need to increase this effort in order to approach several topics that have remained untouched or poorly covered.

We have reported on the constituency of the NaLAB, providing a description of its members and the activities that they have carried out as members of the NaLAB.

Regarding the future, there are two main courses of action. First, we intend to continue participating in events related to the NESSoS research topics, in order to bring together the research communities involved in the different areas of research that NESSoS considers. In this direction, we are already committed to participate in some events such as a panel for presenting NESSoS research on the 6th International Conference on Computers, Privacy and Data Protection (CPDP). Furthermore, ESSoS will be organized again in February 2013 as the NESSoS flagship event, together with the ESSoS doctoral symposium, among others.

Second, but strongly related to the previous one, we are aware of the need to put the emphasis on those research areas that have been poorly covered this year. Therefore, the selection of events where NESSoS is to be present will be partially driven by this fact.
References

[D4.1_II] Engineering Secure Future Internet Services: A Research Manifesto and Agenda from the NESSoS Community
[D4.2_II] Engineering Secure Future Internet Services: A Research Manifesto and Agenda from the NESSoS Community. An Updated Version
[ID12.3] Official Launch of the Virtual Community Network
[D14.3] Report on First Industry Research Seminar