FLAMINGO

European Seventh Framework Network of Excellence

`http://www.fp7-flamingo.eu/`

WP4 — Standardization

Deliverable D4.3 — Third Year Report on Standardization (Update)

University of Twente, The Netherlands (UT)
Institut National de Recherche en Informatique et Automatique, France (INRIA)
University of Zurich, Switzerland (UZH)
Jacobs University Bremen, Germany (JUB)
Universität der Bundeswehr München, Germany (UniBwM)
University Politecnicà de Catalunia, Spain (UPC)
iMinds, Belgium (iMinds)
University College London, United Kingdom (UCL)

Project funded by the European Union under the
Information and Communication Technologies FP7 Cooperation Programme
Grant Agreement number ICT-FP7 318488

Document Control

Title:	D4.3 — Third Year Report on Standardization (Update)
Type:	Public
Editor(s):	Jérôme François
E-mail:	jerome.francois@inria.fr
Doc ID:	D4.3
Authors:	Jürgen Schönwälder, Olivier Festor, Remi Badonnel, Filip De Turck, Marinos Charalambides, Mario Flores, Joan Serrat, Abdelkader Lahmadi, Rick Hofstede, Jeroen Famaey, Corinna Schmitt, Burkhard Stiller, Jérôme François

For more information, please contact:

Dr. Aiko Pras
Design and Analysis of Communication Systems
University of Twente
P.O. BOX 217
7500 AE Enschede
The Netherlands
Phone: +31-53-4893778
Fax: +31-53-4894524
E-mail: <a.pras@utwente.nl>

Legal Notices

Executive Summary

This document synthesizes the WP4 activities related to standardization, performed during the first three years of the FLAMINGO Network of Excellence.

In order to give a complete overview, the contributions of year 1, year 2 and year 3 are mentioned (separately per year).

The objective of WP4 is to advance the network and service management standardization and impact the relevant (de-jure and de-facto) working groups. For that purpose, FLAMINGO partners are actively contributing to the writing of Internet-Drafts and RFCs, to the co-chairing of IETF and IRTF working groups, and to the organization and participation to standardization meetings.

Within the IETF, WP4 has over Y1-3 contributed to a total of **17 Internet-Drafts** and **7 RFCs**. The partners have been involved in a total of **11 working groups**[1].

During the third year, WP4 has pursued the co-chairing of the NETMOD working group and contributed to the following topics:

- Configuration Management: FLAMINGO works on the evolution of the NETCONF framework in NETCONF and NETMOD working groups. The efforts are centered on a configuration model for NETCONF servers, a collection of YANG design patterns, in addition to the usage of NETCONF over TLS and a data model for SNMP configuration. During the third year, these contributions correspond to **2 revised Internet-Drafts**, **8 revisions** and **2 new RFCs** in Y3.
- Flow-based Monitoring: FLAMINGO specifies a set of location information elements for the IPFIX protocol. The specified elements support both geodetic and civic location data. In that context, an IPFIX probe and a IPFIX collector have already been developed by two FLAMINGO partners and successfully showed their interoperability. Initially targeting the IPFIX working group, the work was recentered in year two towards the NMRG. This process has continued. In addition, a work has been carried out to define IPFIX elements to carry out MIB objects. All together, this led to **2 revised Internet-Drafts** and **4 revisions** in Y3.
- Cloud and Service Delivery: FLAMINGO works on a management information base for virtual machines in the OPSAWG working group. It has also specified a common log format for the session initiation protocol (SIP) in the SIPCLF working group, and worked on experiments on HTTP adaptive streaming over interconnected content delivery networks in the CDNi working group. During the third year, the efforts have resulted in **1 revised Internet-Drafts**, **3 revisions** and **1 RFC** in Y3.
- Internet of Things: In the 6LOWPAN working group, FLAMINGO contributes to the definition of managed objects for IPv6 over Low-Power Wireless Personal Area Networks. In the CoRE/ACE working group, it also specifies a two-way authentication mechanism for these networks. In the Core WG, a RESTCONF adaptation for constrained environments has been proposed. In Coman/OPSAWG, it contributes to the problem specification and solutions for managing networks of constrained devices. During the third year, these contributions have led to **4 revised Internet-Drafts**, **9 revisions** and **2 RFCs** in Y3.

Compared to previous years, Y3 shows a continuation of previous stable activities with less participation to new Internet-Drafts but a clear target of **pursuing the standardization process of the initiated documents towards RFC publications** as highlighted bt the table below:

[1] When a topic is move to a new working group, it is not counted twiced but one only

Project year	RFC number	Title	Publication date
Y3	RFC 7666	Management Information Base for Virtual Machines Controlled by a Hypervisor	October 2015
Y3	RFC 7589	Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication	June 2015
Y3	RFC 7548	Management of Networks with Constrained Devices: Use Cases	May 2015
Y3	RFC 7547	Management of Networks with Constrained Devices: Problem Statement and Requirements	May 2015
Y3	RFC 7407	A YANG Data Model for SNMP Configuration	December 2014
Y2	RFC 7388	Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs)	October 2014
Y1	RFC 6991	Common YANG Data Types	July 2013

Within the IRTF, FLAMINGO has also been involved in pre-standardization activities during this first three years period. It has co-chaired the Network Management Research Group (NMRG) and co-organized a total of **9 meetings**. It has also participated to the ICNRG working group. During the third year, FLAMINGO has co-organized a series of **3 new NMRG meetings** focused on Autonomics for Network Management and presented documents in NMRG and ICNRG.

In addition, FLAMINGO has pursued its contributions to socio-economic standardization in the Study Group 13 of the ITU-T following the publication of the recommendation 'Y.3013 : Socio-economic Assessment of Future Networks by Tussle Analysis' in the second year. FLAMINGO's participation to this group has continued with the analysis of socio-economic consequence of end-users located-caches for social networks. A new activity starts within ITU-T by the **presentation to the Study Group 17 of a tutorial about tiny devices two-way authentication** developed by UZH in the FLAMINGO project. FLAMINGO is also working on the FiTSM standard family adopted by the Helix Nebula consortium. During the third year, it has contributed to FiTSM documents relative to samples, templates and practical guides. In addition, an audit of the Service Management System and a training framework have been realized.

Contents

1 Introduction

This work package is dedicated to standardization activities performed within the FLAMINGO Network of Excellence. Its primary goal is to create impact on relevant standardization groups (de-jure and de-facto) with the work carried out within FLAMINGO. For that purpose, the following objectives have been defined for this work package:

- To contribute to the writing of Internet-Drafts and RFCs,
- To chair IETF working groups,
- To organize IRTF-NMRG meetings,
- To contribute to other standardization fora.

In order to reach these different objectives, this work package is composed of the three following tasks (in accordance with the DoW document):

- Task T4.1: IETF standardization

  This task is focused on the integration of the community towards the Internet Engineering Task Force (IETF) to ensure high visibility and impact of the protocols and models developed by the FLAMINGO community. Its aim is to foster involvement of European researchers into the IETF. This is done by supporting the chairing of working groups and the (co-)authoring of contributions to the IETF and the standardization activities beyond.

- Task T4.2: IRTF pre-standardization

  The IRTF activities operate in a similar way than the IETF but the addressed challenges can have a more long term scope and allow for the investigation of a wide variety of approaches to a given problem. This task is, like for the IETF participation, to strongly encourage initiatives by its members in the IRTF, through the creation and animation of IRTF research groups, as well as the contributions to IRTF through Internet-Drafts and RFCs.

- Task T4.3: Standardization in other fora (such as socio-economics)

  In addition to the core IETF/IRTF activities, this task consists in evaluating on a case by case basis the opportunities to contribute to other fora that develop their own standardization efforts on network and service management. In particular, this includes socio-economic standardization initiatives performed at International Telecommunication Union Telecommunication Standardization Sector (ITU-T) on economic incentives of future networks within the Study Group 13. During year 3, this activity has been extended to SG17 (Security).

This document reports the WP4 activities undertaken during the first three years addressing ongoing short to mid-term standardization efforts. It is an update of Deliverables D4.1 and D4.2. To ease the review of the update, year three contributions are highlighted and for each activity, described in a dedicated section when appropriate.

After detailing the status with respect to the objectives in Section 2, the document has been structured in accordance with the three previously mentioned tasks. Section 3 discusses the efforts done with respect to the IETF standardization, Section 4 discusses the efforts done with respect to the IRTF pre-standardization and Section 5 discusses the standardization efforts in other fora. Section 6 and 7 summarize partner roles within these tasks and links with other research work packages. Section 8 highlights the most important FLAMINGO-based contributions to standards. Section 9 provides the conclusions.

2 Objectives

The following table[2] summarizes the status of WP4 with respect to the previously mentioned objectives, and shows that all of the objectives are in progress during the first three years of the project.

It is important to note that this deliverable updates Y2 contributions which were not possible to report in last year deliverable (D4.2) as they have not been published yet as of the time of writing. It concerns RFC7388 and 2 documents revisions in IPFIX and CORE).

Objective	Y1 status		Y2 status (delta)	Y3 status (delta)	Relevant tasks
To contribute to the writing of Internet-Drafts and RFCs	NETCONF	1 ID	2 new IDs, 3 revised IDs, 6 revisions	2 revised IDs, 8 revisions, 1 new RFC	T4.1, T4.2
	NETMOD	1 ID, 1 RFC	1 new ID, 1 revised ID, 6 revisions	1 new RFC	
	IPFIX	2 IDs	2 revised IDs, 3 revisions	2 revised IDs, 4 revisions	
	OPSAWG	1 ID	1 new ID, 1 revised ID, 1 revision	1 revised IDs, 3 revisions, 1 new RFC	
	CDNi	1 ID	-	-	
	6LOWPAN/6LO	2 IDS	1 revised ID, 4 revisions, 1 new RFC	-	
	ROLL	1 ID	-	-	
	COMAN/OPSAWG	2 IDS	2 revised IDs, 4 revisions	2 revised IDS, 4 revisions, 2 new RFCs	
	CoRE		1 revised ID, 1 revision	1 revised ID, 3 revisions	
	CoRE/ACE	1 ID, 1 revision	1 new ID, 1 revised ID, 2 revisions	1 revised ID, 2 revisions	
	Total	12 IDS, 1 RFC	5 new IDs, 12 revised IDs, 27 revisions, 1 new RFC	9 revised IDs, 25 revisions, 5 new RFCs	
To chair IETF Working Groups	Co-chairing of the IETF NETMOD Working Group		Co-chairing of the IETF NETMOD Working Group (continuation)	Co-chairing of the IETF NETMOD Working Group (continuation)	T4.1
To organize IRTF-NMRG meetings	Co-chairing of the IRTF NMRG research group		Co-chairing of the IRTF NMRG research group	Co-chairing of the IRTF NMRG research group	T4.2
	Co-organization of 3 NMRG meetings (29th, 30th, 31st NMRG meetings)		Co-organization of 3 new NMRG meetings (32th, 33th, 34th NMRG meetings)	Co-organization of 3 new NMRG meetings (35th, 36th, 37th NMRG meetings)	
To contribute to other standardization for a	ITU-T SG 13	Draft recommendation on socio-economic assessment	"Recommendation Y.3013: Socio-economic assessment of future networks by tussle analysis" published	Presentation on 'Tussles for edge network caching	T4.3
	ITU-T SG17			Tutorial presented on 'Two-way authentication for tiny devices	
	HELIX NEBULA (FITSM)	3 FitSM documents	2 new FiTSM documents (FiTSM-4, FiTSM-5)	2 revised FiTSM documents (FiTSM-4:2014, FiTSM-5:2014)	

In adherence to the S.M.A.R.T. (Specific, Measurable, Achievable, Relevant, Timely) objectives, FLAMINGO was mainly active in the following activities:

- **Contributions to Internet-Drafts and RFCs**. FLAMINGO has participated to 10 working groups, namely NETCONF, NETMOD, IPFIX, OPSAWG, SIPCLF, CDNi, 6LOWPAN/6LO, ROLL, COMAN, CoRA and CoRE/ACE. The milestones indicate at least 5 Internet-Drafts for T0+15 and at least 2 RFCs for T0+30. The contributions for the three years period consist of 25 contributions corresponding to 18 Internet-Drafts and 7 RFCs.
- **Chairing and organization of standardization meetings**. FLAMINGO has co-chaired the IETF NETMOD Working Group and the IRTF NMRG Research Group. The milestones indicate a first NMRG meeting for T0+9. FLAMINGO has (co-)organized a total of 9 NMRG meetings during the first three years period.

[2] An ID may be revised several times on a time period (indicated by the number of revisions). A new ID may also be a revised ID on a time period if it has been revised. Three new IDs (`draft-ietf-opsawg-vmm-mib`, `draft-ietf-netconf-server-model` and `draft-schmitt-ace-twowayauth-for-iot`) are the follow-up of previous IDs (respectively `draft-asai-vmm-mib`, `draft-kwatsen-netconf-server` and `draft-schmitt-two-way-authentication-for-iot`).

3 Task T4.1: IETF standardization

The integration of the community towards the Internet Engineering Task Force (IETF) is done through contributions to 10 working groups (NETCONF, NETMOD, IPFIX, OPSAWG, SIPCLF, CDNi, 6LOWPAN/6LO, ROLL, CORE/ACE and the COMAN informal group).

3.1 NETCONF

3.1.1 Context

The NETCONF working group has created the NETCONF protocol and currently maintains and extends the base protocol specifications. The NETCONF protocol was first published in 2006 as RFC 4741 [1] and a revised protocol specification was published in 2011 as RFC 6241 [2]. The protocol can run over a number of secure transports. The default secure transport defined in RFC 6242 [3] uses the SSH protocol. An alternate transport uses the TLS protocol. Other transports, namely the transport over SOAP and BEEP, have meanwhile been declared historic.

The NETCONF over TLS transport, originally published in 2009 in RFC 5539 [4], requires several updates:

- The framing should be aligned with the new framing used by the SSH transport.
- A configuration data model should be added to control how a user name is extracted from X.509 certificates. This data model should be aligned with the way this is done for the SNMP over (D)TLS transport.
- The transport should support a call home mechanism enabling NETCONF servers behind network address translators to initiate the connection establishment.

Within FLAMINGO, work on NETCONF is important for the interoperability lab maintained as part of WP4. Since NETCONF (and RESTCONF) and the associated data modeling language YANG have significant uptake in the industry, it seems important for the visibility of the FLAMINGO project to provide contributions to core specifications of this set of standards.

3.1.2 Contributions (year 1)

During the first year of the project, work on a revision of the TLS transport document was supported by the project, resulting in the submission of [5]. During the working group meeting at the Summer IETF meeting in Berlin, it was decided to change the way the current document approaches the call home problem. A next revision of the Internet Draft [6] contains the necessary changes. Another issue discussed was whether a common namespace for NETCONF configuration data models is useful and if so how to implement this given the IETF's process constraints. This topic likely will come up again since the policy objects that control when and how frequently a device behind a network address translator calls home should be shared between the TLS transport and a call home extension of the SSH transport.

3.1.3 Contributions (year 2)

The TLS transport document was updated in January 2014 [9] in order to move the NETCONF configuration data model into a separate document [10]. This server configuration model was revised a couple of times [11], [12], [13] in order to incorporate feedback from the working group. During the 90th IETF meeting in Toronto, it was decided to move the call-home mechanism of the TLS transport into a separate document. This leads to another revision of the TLS transport document that essentially removes the call-home related text [14].

During Spring 2014, the revised TLS transport of NETCONF was prototyped using the `libnc` NETCONF server implementation and the `ncclient` NETCONF client implementation and the results have been reported to the IETF working group. Note that both `libnc` and `ncclient` are part of the interoperability lab established as part of WP3 and `ncclient` is an open source package further described in the WP1 deliverables.

3.1.4 Contributions (year 3)

The work on the TLS transport specification of NETCONF has been finished in 2015. The final review process in the working group and the IETF and IESG led to a number of updates ([15], [16], [17],[18] that finally resulted in the publication of RFC 7589 [19].

The work on the server configuration model continued ([20], [21]). One of the remaining issues is the handling of keys. While the server configuration model proposes a way to manage the necessary security credentials, it seems desirable to have a more generic key chain data model. During the 93rd IETF meeting in Prague, it was discussed to contact authors of similar models and to check with the Security Area of the IETF whether work on a key chain model can be entertained in the Security Area. Integrating into a generic key chain model may delay the completion of the server configuration model.

Work on a variant of RESTCONF designed for constrained embedded devices with limited resources has taken place in the third year of the project ([22], [23], [24]). Being related to constrained devices, this work may become chartered in the CORE working group (see Section 3.10.1).

3.1.5 Future developments

The work on a REST protocol to access NETCONF datastores (RESTCONF) has been progressing in the NETCONF working group during the third year and it enjoys strong interest by the industry. It is possible that in the long run RESTCONF becomes more widely used than NETCONF because it integrates more easily into application development frameworks. The RESTCONF variant for embedded devices may become an IETF working group work item in the fourth year of the project. This work is linked to research in the FLAMINGO WP6 related to the management of devices on the Internet of Things.

3.2 NETMOD

3.2.1 Context

The NETMOD working group in the IETF has produced a data modeling language for the NETCONF protocol called YANG [25], published as RFC 6020 in 2010, and a core set of data types,

originally published in RFC 6021 [26]. The working group is now working on a core set of configuration data models that will form the basic building blocks for additional more specific configuration data models.

Since these data models will most likely be used as templates for future configuration data models, the working group is trying to develop clean models and as part of this exercise, certain questions not directly addressed by the NETCONF protocol specification or the YANG data model specification need to be addressed.

The NETMOD working group is also working on an update of the YANG data modeling language and associated documents such as the YANG guidelines for authors and reviewers.

3.2.2 Contributions (year 1)

Jacobs University is contributing to this IETF activity in a leadership role by providing one of the working group co-chairs and by actively contributing to the various documents. During the reporting period, a revision of the core set of data types has been progressed through the whole IETF publication cycle, from individual draft [27] through several working group drafts [28, 29, 30, 31] to the published specification RFC 6991 [32].

At a slower pace, work has progressed on the configuration data model for SNMP agents [33, 34]. While the configuration data model is essentially complete, it remains unclear whether the data model needs to be extended to cover also operational state. Work has progressed slower on these documents because the other working deliverables were given higher priority by the document editors.

The working group leadership required close collaboration with the different document authors during the reporting period. In particular, several working group documents were progressed through working group last call early 2013 and passed to the IESG with a request for publication. During the IETF reviews, issues were raised that could not be resolved without taking the documents back to the working group. In particular, concerns were raised that the relationship of configuration state to operational state is not always clear. By organizing several conference calls with key contributors, it was possible to find a solution by representing operational state in a separate subtree which is loosely coupled to the configuration subtree. This solution has meanwhile been incorporated into the various data models (except the SNMP configuration data model). Working group leadership activities also involved the preparation of the two face-to-face meetings at the IETF meetings in Orlando and Berlin plus the preparation of meeting minutes and reports.

3.2.3 Contributions (year 2)

The work on the SNMP configuration data model has been wrapped up by producing a number of revisions to deal with working group last call, IETF last call, and IESG review comments ([35], [36], [37], [38], [39], [40]). The IESG approved the publication of this work as Proposed Standard in September 2014.

The rechartering process of the NETMOD working group finished in April 2014. Since then, the working group is working on (i) the core YANG infrastructure (a revision of the YANG specification and the usage guidelines and a serialization of YANG defined instance data to JSON) and (ii) a number of YANG data models that do not fall into the charters of other IETF working groups. The chairs of the NETMOD working group decided to split the main responsibility along these two axes. Jacobs University Bremen is taking the lead for the work on the core YANG infrastructure. For

the YANG 1.1 revision, a process has been implemented where issues were collected in an initial phase. In the subsequent phase, the issues are decided to be in scope or out of scope and finally the third phase is addressing the details of the in scope issues. In order to be effective, regular virtual online meetings are used. In addition, a physical interim meeting was organized that took place in September in New York.

3.2.4 Contributions (year 3)

The YANG data modeling language has significant uptake in the industry. There are more than hundred YANG modules being worked on the IETF. Some open source projects such as OpenDaylight have produced several hundreds of YANG data models. Other standards developing organizations such as the IEEE or BBF are considering to adopt YANG for their data modeling work.

The maintenance of the YANG language definition and the production of the YANG 1.1 maintenance release of the language is thus a critical piece of work. During the third year of the FLAMINGO project, all issues in the YANG 1.1 issue tracker were closed, which involved some intense discussions around certain issues. Jacobs University has chaired several face-to-face meetings of the NETMOD working group as well as several virtual interim meetings of the NETMOD working group on YANG 1.1. The goal is to have the specification complete in October 2015.

The work on the SNMP configuration data models was finished with the publication of RFC 7388 [41].

3.2.5 Future developments

With the finalization of YANG 1.1, Jacobs University will step from its role as co-chair of the NETMOD working group.

3.3 IPFIX

3.3.1 Context

Android-based devices, including smartphones and tablets, are emerging and widely adopted by users because of their interesting capabilities. They evolved from simple telephony devices into sophisticated yet compact computing devices, connected to a wide spectrum of networks including Internet via Wi-Fi, GPRS/EDGE and 3G network access. In contrast to fixed devices, which usually have their physical location in a static manner, mobile devices have capabilities for determining and exposing their geographic location using several location systems. Besides that, the network traffic generated by these devices is increasing since they enable users to access and browse web sites, send emails, play on-line games and exchange information. It is projected that mobile traffic will grow ten times faster than fixed Internet traffic.

Analysis of the network behavior of applications running on a mobile device requires the collection of information about data leaving the device and where it is sent. Cisco's NetFlow and the more recent IPFIX are flow export technologies that have seen a rapid adoption and widespread integration in many campus, enterprise and backbone networks. Relating the location information of a device to NetFlow/IPFIX flows can be beneficial to many network management and measurement applications, including traffic profiling, anomaly detection and provider-independent measurements.

To be able to export and analyze mobile device characteristics (such as its location at the moment of certain network activity), the NetFlow/IPFIX protocols have to be extended. The flow exporter, flow collector and analysis application need to be aware of these extensions as well. This work has been divided between INRIA and University of Twente (UT). On the one hand, INRIA is responsible for developing a flow exporter tailored to Android devices. On the other hand, UT is responsible for the flow collector and analysis application.

3.3.2 Contributions (year 1)

Information Elements for IPFIX Metering Process Location INRIA and UT have authored and presented an IETF draft [42, 43] where they have defined a set of Information Elements for the IP Flow Information Export (IPFIX) protocol to include location information of any device (both fixed and mobile) that acts as an IPFIX Flow Exporter. The specified Information Elements support both geodetic and civic location data. Figure 1 depicts an example of an IPFIX record to export a geographic position defined using the latitude and the longitude GPS coordinates.

The draft has been initially presented during the IETF 87 meeting in Berlin within the IPFIX and NMRG working groups.

Duration	Dst IP Addr:Port	bps	Lat. (int)	Lat. (dec)	Lng. (int)	Lng. (dec)
318.039	173.194.40.129:443	71	48	6657094	6	1583253
317.787	152.81.144.14:53	1	48	6657094	6	1583253
77.221	173.252.100.27:443	266	48	6657094	6	1583253
317.366	152.81.144.14:53	1	48	6657094	6	1583253
317.187	98.137.200.255:80	13	48	6657094	6	1583253
315.919	152.81.144.14:53	1	48	6657094	6	1583253
75.090	188.125.73.190:80	72	48	6657094	6	1583253
326.120	152.81.144.14:53	1	48	6657451	6	1583478
145.667	173.252.100.29:443	153	48	6657451	6	1583478
312.646	152.81.144.14:53	1	48	6657451	6	1583478
312.546	193.51.224.165:443	57	48	6657451	6	1583478
312.480	152.81.144.14:53	1	48	6657451	6	1583478
953.086	74.125.132.95:443	138	48	6657451	6	1583478
370.779	74.125.132.101:443	35	48	6655431	6	1628925
370.806	172.20.2.10:53	1	48	6655431	6	1628925
368.348	74.125.132.101:443	67	48	6655431	6	1628925
81.586	74.125.195.95:443	240	48	6655431	6	1628925
339.782	152.81.144.14:53	1	48	6657451	6	1583478
79.297	173.252.100.27:443	1153	48	6657451	6	1583478
6671.083	10.103.80.171:47175	1	48	6652353	6	1614169
661.711	74.125.132.147:443	0	48	6652353	6	1614169
5636.372	1.1.1.1:67	1	48	6657451	6	1583478
306.969	193.51.224.148:443	49	48	6657451	6	1583478
306.850	184.73.193.117:443	35	48	6657451	6	1583478
427.759	173.194.34.34:443	1	48	6657451	6	1583478

Figure 1: Data record of a geographic 2D point location

Location-aware Mobile Flow exporter (INRIA) Using the set of information elements defined in this IETF draft, INRIA has developed Flowoid, a NetFlow/IPFIX exporter tailored to Android devices. The current version of the probe relies on two components:

- A native driver listens to the network traffic exchanged between the device and other hosts on a specific interface (3G cellular or Wi-Fi).
- A flow exporter written in Java that receives packet headers from the driver and constructs NetFlow/IPFIX records to be transmitted to a specific collector.

The exporter associates to each observed network flow a geolocation data containing the GPS coordinates of the device, among others. This information is exported together with the traditional fields defined in the NetFlow/IFPIX protocols: IP version, source and destination addresses, the number of exchanged bytes, the type of protocol, the number of exchanged packets, the source and destination ports and the duration of the flow. In addition, it contains 7 additional fields that denote the identifier of the device: the identifier of the localization method, a timestamp, the integer part of the latitude, the decimal part of the latitude, the integer part of the longitude and the decimal part of the longitude.

Flow collector (UT) The task of a flow collector is to receive and store flow data from a flow exporter. Since more data is exported than the NetFlow/IPFIX protocols supports by design (e.g. mobile device location), special support for location-aware flow data export needs to be added to the flow collector. UT has chosen to use the state-of-the-art flow collector NfSen/NfDump, both because of its wide deployment and its support for extensions. The location extension has already been developed and tested and is ready for deployment. Figure 1 corresponds to a set of NetFlow records exported using the INRIA flow exporter from an Android device and analyzed using the extended version of nfdump.

3.3.3 Contributions (year 2)

INRIA and UT have worked on the update of the draft [44] which has been presented at the IETF 90 in Toronto during the NMRG session. There it was decided to recenter the contribution towards the NMRG due to the closing of the IPFIX working group. This change also implies a significant rewriting of the draft emphasizing more the use cases than the information elements themselves. The update will be presented at the NMRG meeting in november 2014 and updated to be presented at the NMRG meeting right after at IETF 91.

INRIA did also deploy the probe on several devices of researchers and students (5 in total) leading to a bigger dataset. INRIA did also integrate the probe into a larger measurement framework under development in the MADYNES Team. This integration also led to some optimization of the framework to reduce traffic overhead concerning the exchange of probed data.

3.3.4 Contributions (year 3)

Inria and UT have presented a major revision of the draft in October 2014 [44]. It has been followed by several revisions [45, 46] based on collected feedback in order to pursue towards a RFC proposition. Those revisions have been introduced during the 35th and 36th IRTF NMRG meetings as the IPFIX working group has been closed.

The IPFIX protocol can benefit from being able to export objects defined in SNMP MIB modules. Jacobs University got asked to review a corresponding proposal to ensure the specification is correct from an SNMP point of view. This resulted in contributions to several revisions of the specification of MIB variable export for IPFIX ([47], [48], [49], [50]). While the IPFIX working group was closed down in 2015, this document may still be published as an Area Director sponsored document.

3.3.5 Future developments

Both INRIA and UT pursue their collaboration on the evolution of the underlying codes supporting the draft. Last received comments from the NMRG mailing list are related to privacy concerned introduced by embedded location information. Those issues will be covered in the next versions.

3.4 OPSAWG

3.4.1 Context

The OPSAWG working group of the IETF serves two main purposes. Firstly, it takes on maintenance work for protocols that do not have an active working group. Secondly, it takes on work that is of general importance for the operations and management area of the IETF but where chartering a new working group seems to be overkill. In the later case, it can of course happen that work taken on in OPSAWG evolves into something bigger that warrants its own working group (this has happened for example for the energy management work, which is now hosted by the EMAN working group). As such, the OPSAWG does not have a narrowly scoped charter but instead serves as a place to carry out maintenance and house keep work and develop new ideas or areas of work.

3.4.2 Contributions (year 1)

Today's cloud infrastructures rely heavily on virtualization technology in the data centers to provide elastic services. Several proposals were made in the past to create data center specific working groups in the IETF but only a very few narrowly scoped activities were officially chartered so far. One of the criteria for chartering decisions is always whether the IETF has the right expertise to carry out an activity.

The monitoring of virtual machine infrastructures is one such aspect where the IETF has significant know-how that can be leveraged. Two independent proposals of data models for monitoring and troubleshooting virtual machines surfaced in 2012 and were later merged into a joint proposal. During the reporting period, the joint proposal got revised several times to incorporate feedback received from discussions in the OPSAWG [51, 52, 53, 54]. Specific work items concern the development of a general state machine model for hypervisors and the definition of scalable mechanisms for notifications (e.g., a restart of a rack full of servers, each running a hypervisor, should not cause a flood of notifications due to the large number of state changes that occur almost simultaneously).

This work is done in collaboration with people affiliated with VMware, Huawei, and the University of Tokio. The goal is to develop a specification that replaces parts of VMware's proprietary data models but at the same time is easily implementable on top of abstractions such as `libvirt`, an open source C library that can be used to monitor and control a number of different hypervisors.

3.4.3 Contributions (year 2)

The data model for virtual machines was accepted as a WG deliverable in early 2014. This has led to the publication of [55] and [56]. One of the changes was to make the MIB module purely read-only, following the general guidance issues by the IESG on writable MIB modules. The MIB module has been reviewed by a number of people within the IETF and while some minor additions have been suggested, it seems the document is rather stable.

3.4.4 Contributions (year 3)

Several updates of the MIB model for virtual machines were produced during the third year of the FLAMINGO project ([57], [58], [59]). The document was published as Proposed Standard in October 2015 [60].

3.4.5 Future developments

With the publication of the MIB module for virtual machines, the work in the OPSAWG has concluded. It is not planned to undertake any other activities in the OPSAWG working group during the fourth year of the project.

3.5 SIPCLF

3.5.1 Context

The SIP Common Log Format (SIPCLF) working group was chartered at IETF to define a standard logging format for systems processing SIP messages. Well-known web servers such as Apache and web proxies like Squid support event logging using a common log format. The benefits induced by such a log format are twofold:

- The logs produced using these de facto standard formats are invaluable to system administrators for troubleshooting a server and to tool writers to craft tools that mine the log files and produce reports and trends.
- These log files can also be used to train anomaly detection systems and to feed events into a security event management system.

The Session Initiation Protocol (SIP), defined by RFC 3261 [61], provides to Internet endpoints a signaling support for discovering one another, and then establishing and managing real-time multimedia sessions, such as IP telephony calls. However, it does not have a common log format, and, as a result, each server supports a distinct log format that makes it unnecessarily complex to produce tools to do trend analysis and security detection.

3.5.2 Contributions (year 1)

While the work on SIPCLF was initiated already a couple of years ago, the final development of the standard did benefit from FLAMINGO support, enabling INRIA to pursue the necessary work to bring the draft to an RFC level and build a prototype implementation of the log framework. INRIA has contributed to RFC 6872 published in February 2013 [62]. As the work was not directly in the scope of FLAMINGO, it has not been counted as an additional RFC with respect to the WP objectives. This RFC describes a framework, including requirements and analysis of existing approaches, and specifies an information model for development of a SIP common log file format that can be used uniformly by user agents, proxies, registrars, and redirect servers as well as back-to-back user agents.

The work has therefore consisted in analyzing and discussing the limits of four alternative approaches: Call Detail Records, Packets Capture Tools (such as Wireshark and TCPdump), the Syslog protocol and the IP Flow Information Export (IPFIX) protocol.

This analysis has led to the definition of an information model that specifies a total of 19 mandatory fields for a SIPCLF record:

- Timestamp: date and time of the request or response represented as the number of seconds and milliseconds since the Unix epoch,
- Message type: an indicator of whether the SIP message is a request or a response,
- Directionality: an indicator of whether the SIP message is received by the SIP entity or sent by the SIP entity,
- Transport: the transport over which a SIP message is sent or received,
- Source-address: the IPv4 or IPv6 address of the sender of the SIP message,
- Source-port: the source port number of the sender of the SIP message,
- Destination-address: the IPv4 or IPv6 address of the recipient of the SIP message,
- Destination-port: the port number of the recipient of the SIP message,
- From and from tag: the From URI and the tag parameter of the From header,
- To and to tag: the To URI and the tag parameter of the To header,
- Callid, CSeq-Method, CSeq-Number: the call identifier, the method and number from the CSeq header,
- R-URI: the Request-URI, including any URI parameters,
- Status: the SIP response status code,
- Server-Txn: the transaction identifier associated with the server transaction,
- Client-Txn: the client transaction identification code.

This information model applies to all SIP entities and supports extensibility by providing the capability to log optional fields. Its applicability has been illustrated through four example scenarios including user agent registration, direct call between two users, single downstream branch call and forked call. As log files by their nature reveal the state of the entity producing them, security considerations such as disk encryption and physical access restriction to the machine storing the SIPCLF files have also been discussed.

Following RFC 6872 to which INRIA has contributed, RFC 6873 [63] has defined an indexed text file format for logging SIP messages received and sent by SIP clients, servers, and proxies that adheres to this information model. These two RFCs have successfully addressed the objectives of the SIPCLF activity and led to its conclusion in 2013.

3.6 CDNi

3.6.1 Context

The IETF Content Delivery Networks interconnection (CDNi) working group aims to standardize architectural concepts, interfaces and protocols that facilitate the collaboration of separately administered CDNs. This will enable the end-to-end delivery of content from content providers, through

multiple CDNs and ultimately end users. Specifically, the interconnection of large-scale global CDNs and local telco CDNs (e.g., deployed with an Internet Service Provider's (ISP) network) allows content to be delivered from much closer to the end user, significantly increasing Quality of Experience. Other advantages of CDNi include overload handling, increased resiliency, capability extension, and user mobility support.

3.6.2 Contributions (year 1)

A major topic of discussion within the CDNi working group, is the deployment of HTTP-based adaptive streaming (HAS) services on interconnected CDNs. In August 2012, a first version of a draft [64] was published that identified related problems and described how CDNi components could be adapted to better support this type of services.

iMinds contributed to the discussion of these issues by publishing an informational draft [65] in September 2012 that experimentally evaluated the delivery of content over interconnected CDNs using HAS. Results showed that the main culprit is the CDNi request routing function, which causes significant quality degradation in HAS services due to a potentially large number of HTTP request redirects. Based on these results, several alternative request routing schemes were proposed that are better suited for delivering HAS content. Based on feedback from CDNi working group members, and discussions on the CDNi mailing list, a new version [66] with extended results was published in January 2014.

The published iMinds documents have aided in the evaluation of the HAS-related issues exposed in the drafts on HAS over CDNi [64, 67]. This has lead to the publication of RFC 6983 [68] in July 2013. This RFC describes models for HAS-aware CDN interconnection.

The work was concluded in year one of FLAMINGO with the successful publication of RFC 6983 [68].

3.7 6LOWPAN / 6LO

3.7.1 Context

The 6LOWPAN working group of the IETF has developed specifications detailing how to run IPv6 over short distance radio links such IEEE 802.15.4 that differ from other wireless link technologies significantly since they are optimized for small power consumption and have significant limits in terms of supported frame sizes and data rates. The main technical specifications developed by the 6LOWPAN working group define a 6LoWPAN adaptation layer providing fragmentation / reassembly functions and header compression services. It also provides the necessary infrastructure to support mesh routing below the IPv6 layer.

3.7.2 Contributions (year 1)

Jacobs University developed a MIB module for a set of counters that provide basic information necessary for monitoring and troubleshooting the 6LoWPAN adaptation layer [69, 70]. The Case Diagram in Figure 2 shows how the counters are related to each other.

The counters have been integrated into the 6LoWPAN implementation of the Contiki operating system and the Contiki SNMP engine developed by Jacobs University (see also the open source section in deliverable D1.1) has been extended to support the proposed MIB module. The work has been presented to the IETF.

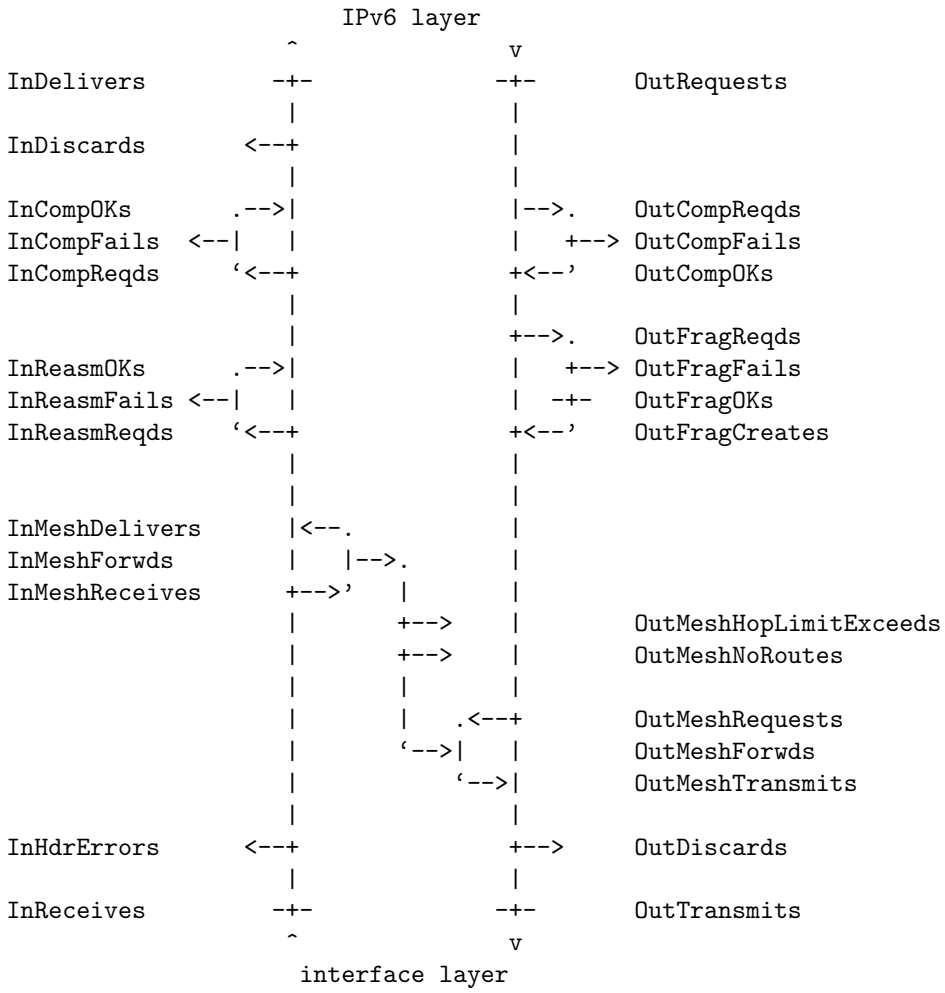

Figure 2: Case Diagram of the counters of the 6LoWPAN MIB

3.7.3 Contributions (year 2)

The 6LoWPAN working group was closed in 2013 and a new working group 6LO was formed to take over maintenance work of the 6LoWPAN specifications. The MIB module was revised and submitted to the new 6LO working group [71, 72] and finally accepted as working group document [73]. Several revisions were produced while going through the working group last call, IETF last call, and IESG review process [74, 75, 76]. The document was approved to be published as Proposed Standard by the IESG in August 2014.

The MIB module has been implemented as part of IoT management related research activities described in WP5 deliverables. This implementation was demonstrated during the “Low Power and Lossy Networks Plugfest”[3] that took place on Sunday before the 90th IETF meeting in Toronto.

3.7.4 Contributions (year 3)

The work on the 6LoWPAN MIB module concluded with the publication of RFC 7388 [41].

[3] https://bitbucket.org/6tisch/meetings/wiki/140720a_ietf90_toronto_plugfest

3.7.5 Future developments

It is not planned to undertake any other activities in the 6LO working group during the fourth year of the project.

3.8 ROLL

3.8.1 Context

The ROLL working group of the IETF has developed the RPL routing protocol. The RPL protocol establishes IPv6 routing trees, more precisely destination oriented directed acyclic graphs (DODAGs), rooted at a border router. The RPL protocol is essentially a distance-vector protocol and it can generate topologies optimized for different objective functions. The RPL protocol aims at providing an IP-layer routing solution for so called low-power and lossy networks.

3.8.2 Contributions (year 1)

Jacobs University has developed a MIB module providing objects for managing the RPL protocol [78]. It also provides management access to the Trickle parameters as they are used by RPL. The MIB module provide the information necessary to determine the routing topology established by RPL and it provides access to parameters that control the RPL exchanges. Finally, the MIB module contains a number of counters tracking things like RPL message processing errors or important state changes like the number of triggered local and global repairs.

The RPL-MIB module integrates well into the set of existing MIB modules, such as the IP-FORWARD-MIB and the IP-MIB. In particular, it is assumed that the IPv6 routing table is exposed via the inetCidrRouteTable defined in the IP-FORWARD-MIB and that the IPv6 prefixes used by DODAGs are exported via the ipAddressPrefixTable of the IP-MIB.

The RPL-MIB module has been prototyped using the RPL implementation that is part of the Contiki operating systems. The MIB module was implemented using the Contiki SNMP engine developed by Jacobs University (see also the open source section in deliverable D1.1).

3.8.3 Contributions (year 2)

The ROLL working group has been reluctant to take on this work. One reason is that some people are concerned that work on a MIB module can be read as an endorsement that RPL networks are to be managed by SNMP. Discussions of other ways to transport management information in constrained networks are ongoing and it seems that the ROLL working group at this point prefers to wait for these discussions to lead to more concrete results and recommendations. As a consequence, we did decide to not push this work further. Note that this work is related to research on attacks on RPL networks documented in deliverable D5.2.

3.9 COMAN / OPSAWG

3.9.1 Context

COMAN is an informal activity in the IETF to identify the requirements and possible solutions for the management of networks with constrained devices. Since constrained devices differ significantly

from other devices not only by their resource constraints but also their use cases, there is an ongoing debate about how such devices should be managed and what management of these devices really means. In order to focus these discussions, the COMAN activity was started with the goal to produce a problem statement.

3.9.2 Contributions (year 1)

Several informal meetings have been held at the last couple of IETF meetings in order to discuss and produce a problem statement document that discusses typical use cases and identifies requirements from them. Some of the discussions about the management protocols to be used in networks with constrained devices also took place in the COMAN meetings.

During the reporting period, Jacobs University has worked on the COMAN problem statement document [79]. The main body of this document describes twelve different use case scenarios. From these use cases, a large number of requirements have been derived that have been classified into eleven groups. The appendix provides pointers to activities in other standardization bodies and related research projects.

A detailed review of the document has been produced and submitted to the COMAN mailing list in April. Several of the comments are waiting for resolution. At the 87th IETF meeting in Berlin, it was suggested to split the current document into one that discusses the use cases and a second identifying requirements [80, 81]. It was also suggested that any protocol work, e.g., a specification on how to transport MIB data over CoAP, would likely belong into other existing working groups.

3.9.3 Contributions (year 2)

The COMAN drafts were accepted as working group documents by the OPSAWG in 2014. This resulted in a number of revisions in order to incorporate feedback from the working group and to fill in missing pieces, for details see [82, 83, 84, 85] and [86, 87, 88, 89]. In addition, we participated in a side meeting at the 90th IETF in Toronto where people gathered to discuss how to build a REST-based management protocol that can run over CoAP on constrained devices. In October 2014, the IETF also formed an IoT directorate which we joined. Note that this work is also related to a special session on Internet of Things management we organized as part of NOMS 2014 (see deliverable D3.3) and the collaborative research on Internet of Things related management aspects (see deliverable D5.2).

3.9.4 Contributions (year 3)

The COMAN drafts were progressed through the OPSAWG during the third year of the project ([90], [91], [92], [93]). The drafts were finally approved by the IESG and published as Informational RFC 7548 [94] and Informational RFC 7547 [95].

3.9.5 Future developments

The COMAN activity has concluded with the publication of RFC 7548 [94] and RFC 7547 [95].

3.10 CORE/ACE

3.10.1 Context

Standardization within FLAMINGO performed by UZH is addressed toward the IETF and the ITU-T in terms of two UZH investigations. The main topics arise from work performed in WP7 on 'Economic, Legal, and Regulative Constraints'.

In that context, the following example outlines the major set-up of respectively needed methodology and functionality:

Once a user wants to upload data into an online portal and this portal is publicly available, the upload is guided and constrained by multiple legal implications. In addition, all entities (stakeholders) involved have different incentives and, thus, tussles arise due to distinct optimization dimensions. Stakeholders (e.g., ISPs, network providers, cache owners, or portal owners and users themselves) sharing content are within the scope of major legal acts and bills, like access control, age limits, and validation schemes, and regulations, such as data privacy, maximum tariffs and rates, and caching schemes.

Therefore, the goal of the key UZH investigations is to explore, determine, and as far as possible standardize the following three aspects in case of the existence of user-generated data and content, which can be shared publicly:

1. Tussles and incentives of involved stakeholders.
2. Feasibility of caching from legal point of view.
3. Recommendations for secure data sharing.

The first goal is investigated under ITU-T and , thus, it is referred to Task 4.3 (see Section 5.2 for further information).

In order to address the second goal, UZH investigates legal implications of user-generated content combined with in-network caching, which are still unaccounted for and not fully explored. This situation leads to stakeholders, who have to deal with high legal risks. Implications can be categorized as copyright infringement, data-privacy violation, and profiling. Legal questions, which must be kept in mind and be answered, are the following ones:

- What content can be cached?
- How can cached data be used?
- Who can cache the data?
- Where can cached data be located/stored?
- How can cached data be used?
- Are the stakeholders trustworthy?

One option to deal with those questions is to regulate and secure the communication between the stakeholders. Therefore, the participating communication partners should perform a two-way authenticated handshake. As a consequence the legal uncertainties are reduced, because the

caching is only possible based on regulative requirements with appropriate security features (e.g. authentication, certificates, access tickets).

Note that such investigations are yet not part of a standardization process. However, there is the possibility to interact with regulators on those aspects, to ensure that major technical as well as operational facts are incorporated into new regulations.

3.10.2 Contributions (year 1)

The third goal is currently under standardization plans within the IETF. The first contribution in project year one was submitted to working group CoRE. CoRE itself deals with 'Constrained RESTful Environments'.

The research and respective standardization work focuses on security in such constraint environments, which is required due to the extremely fast growing connection of billions of devices to the Internet, especially labeled as the Internet-of-Things (IoT). Independent of dedicated device dimensions it is a fact that all data includes sensitive information (e.g., personal information, IDs, location information, or private knowledge). Thus, if data is streamed or cached, as it is the case within the context of FLAMINGO and its related management tasks, this problem of secure data sharing (while enabling certain levels of data privacy) must be faced.

Therefore, since April 2013 UZH started the investigations of the possibility to bring two-way authentication to constraint devices. For resource-full devices a DTLS solution was proposed and under construction is currently a solution using elliptic curve cryptography (ECC) for devices with less resources. UZH is in the process to specify hardware and message work flow requirements, which brings the relevant level of trust into the network for upcoming communications between any two stakeholders. Therefore, UZH deals with the following research and standardization aspects:

- DTLS-based two-way authentication handshake using unreliable UDP,
- Authentication of each stakeholder,
- Certificate Authority for creating certificates,
- Trusted Platform Module inclusion for building chain of trust,
- ECC-based two-way authentication handshake.

In turn, the work in FLAMINGO fills the gap of an application scenario for the standardization process of the aforementioned concept. These standardization efforts include, besides project-internal cooperation, a cooperation with the Information and Communication Technology (ICT) Centre of the CSIRO research institute in Brisbane, Australia.

3.10.3 Contributions (year 2)

Due to long discussions within CORE it was decided to build a new working group that should focus only on security issues for constraint environments. Thus, a new working group 'Authentication and Authorization for Constrained Environments' (ACE) had its BOF in March 2014 during the IETF 89 in London, U.K. and was approved in June 2014. All Internet drafts addressing the security topic were requested to shift and rename to working group ACE.

Based on the received feedback of the community during the meeting IETF 87 in Berlin in summer 2013 UZH improved the submitted draft [97] for IETF 88 in Vancouver, Canada in November 2013. The new version of the draft included a use-case description that is inspired by the aforementioned settings in Section 3.10.1 and the standardization approaches in ITU-T by University of Zurich. A subgroup was established dealing with authorization and authentication within the CORE working group, where the draft of UZH was grouped to. Together with other drafts a cooperation was build in order to work together on common drafts dealing with authorization and authentication topics, specifying terminology, roles, use-cases, and recommendations for mechanisms.

Due to participation in different IETF meetings in 2014 and received feedback the original Internet draft was updated several times resulting in [99] that already mirrors the renaming process and linkage to the new working group ACE. Furthermore, the content was generalized for different device classes and restructured looking on the following points:

- Terminology,
- High Level Design Requirements,
  - Implementation of A Standards Based Design,
  - Focus on Application Layer and End-to-End Security,
  - Support for UDP,
- End-to-End Security Using Two-way authentication,
  - Class 2 Devices or Higher: Handshake Description and Certificate creation,
  - Class 1 Devices (under construction),
- Architecture Description,
- Hardware Requirements,
  - Class 2 Hardware Requirements,
  - Class 1 Hardware Requirements,
- Security Considerations,
  - Class 2 Hardware Requirements,
  - Class 1 Hardware Requirements.

UZH was involved in different presentations during IETF meetings and in interim meetings of working group ACE.

3.10.4 Contributions (year 3)

University of Zurich continued with standardization within WG ACE by updating the Internet draft entitled ‘Two-way Authentication for IoT’ [100, 101]. Within year three the draft was updated twice including solution for two-way authentication for class 1 devices based on a modified Bellare-Canetti-Krawczyk (BCK) with pre-shared master key using elliptic curve cryptography (ECC) for performed public key cryptography (PKC). ECC, standardized in RFC 6090 itself offers efficient algorithms (ECDSA , ECIES, ECDH) for key generation, key exchange, encryption, decryption, and signatures. For message encryption an integrated encryption scheme (IES) is recommended to

harness the speed-advantage of symmetric encryption for large amount of data without drawback of a repeated key exchange for every transmission to avoid reusage of secrets.

The RESTCONF protocol adaptation for constrained devices has been presented in the CoRE working group ([22], [23], [24]).

3.10.5 Future developments

In order to continue the work delegates of University of Zurich will participate in the upcoming IETF meetings in 2015 and 2016. The goal is to fill pending sections of the current draft [101], present the work to the community, and work with the received feedback.

4 Task T4.2: IRTF pre-standardization

FLAMINGO is also actively participating to pre-standardization activities at the Internet Research Task Force (IRTF) through the NMRG and ICNRG research groups.

4.1 NMRG

4.1.1 Context

The IRTF Network Management Research Group (NMRG - http://irtf.org/nmrg) provides a forum to explore new technologies for the management of the Internet and the Future Internet.

In particular, the research group is working on solutions for problems that are not yet considered or well understood enough for engineering work within the IETF.

In that context, it aims at identifying and documenting requirements, surveying possible approaches, providing specifications for proposed solutions, and proving concepts with prototype implementations that can be tested in large-scale real-world environments.

4.1.2 Contributions (year 1)

During the first year, INRIA has co-chaired the Network Management Research Group (NMRG), and the following events have been organized:

- the **29th NMRG Meeting centered on ICN Management** which took place in Orlando, USA in March 2013 and included the following topics:
  - Management considerations for information-centric networks,
  - Firewalls for content-centric networks,
  - Autonomic and software-defined networks,
- the **30th NMRG Meeting centered on IPFIX/Netflow Approaches** which took place in Berlin, Germany in July 2013 and included the following topics:
  - NFQL: A tool for querying network flow-records,
  - Location-aware network monitoring using IPFIX/NetFlow,

  - An approach for correlating flow data,
  - IPFIX QoS measurement extensions,

- the **31st NMRG Meeting centered on Large-Scale Measurements** which took place in Zurich, Switzerland in October 2013. It was organized by JUB in co-location with the IEEE/IFIP International Conference on Network and Service Management (IEEE/IFIP CNSM'2013) and was focused on topics such as:
  - Novel metrics for measuring Internet performance,
  - Techniques to estimate quality of experience from raw measurements,
  - Novel data analysis techniques,
  - Interactive information visualization techniques,
  - Software and hardware tools,
  - Interfaces of measurement systems to network management systems.

4.1.3 Contributions (year 2)

During the second year, INRIA has co-chaired the Network Management Research Group (NMRG), and the following events have been organized:

- the **32nd NMRG Meeting centered on Autonomics for Network Management (Part I)** which took place in Vancouver, Canada in November 2013 and included the following topics:
  - Definition of autonomic networking terms,
  - Autonomic networking frameworks and architectures,
  - Network configuration negotiation problem statement,
  - Peer-to-peer detection of service level agreement violations,
  - Bootstrapping trust on a homenet,
- the **33rd NMRG Meeting centered on Autonomics for Network Management (Part II)** which took place in London, UK in March 2014 and included the following topics:
  - Definition of autonomic networking terms (continuation),
  - Proactive self-healing mechanisms for IP networks,
  - Gap analysis for autonomous networking,
- the **34th NMRG Meeting centered on Autonomics for Network Management (Part III)** which took place in Toronto, Canada in July 2014 and included the following topics:
  - Definition of autonomic networking terms (continuation),
  - Gap analysis for autonomous networking (continuation),
  - Lessons learned on using autonomics for network management,
  - Real world experiences on using autonomic principles in network management.

An important outcome of the NMRG work is the acceptance of the principles of Autonomic management within the IETF/IRTF community. A measurable element of this acceptance is the popularity of the BOF at IETF 90 on Autonomics which leads to a dedicated WG entitled ANIMA within the IETF.

4.1.4 Contributions (year 3)

As in the previous years, the goal of the NMRG workshop is to be a place where researchers, operators and manufacturers can exchange and discuss their experiences and ideas in the network management area. During the third year, INRIA has co-chaired the Network Management Research Group (NMRG), and the following events have been organized:

- the **35th NMRG Meeting centered on Autonomics for Network Management (Part IV)** which took place in Rio de Janeiro, Brazil in November 2014 co-located with CNSM, and included the following topics:
  - Definition of autonomic networking terms (continuation),
  - Autonomic Networking Use Case for Distributed Detection of SLA Violations,
  - Cloud-based data storage and management,
  - Location-aware network monitoring using IPFIX/NetFlow , (continuation),
  - Network Function Virtualization
- the **36th NMRG Meeting centered on Security** which took place in Ottawa, Canada in May 2015 co-located with IEEE/IFIP IM and included the following topics:
  - Attack detection,
  - Secure routing,
  - Privacy,
  - Definition of autonomic networking terms (continuation),
  - Autonomic Networking Use Case for Distributed Detection of SLA Violations (continuation),
  - Location-aware network monitoring using IPFIX/NetFlow (continuation)
- the **37th NMRG Meeting centered on flow-based network management** which took place in Prague, Czech Republic in July 2015 at the IETF 93. Flow-based approaches are used in various areas of network management today, such as link monitoring, accounting, and security. We organized previous workshops on this topic. This 6th edition has been extended to integrate more recent research activities about Software-Defined Networking with the following program:
  - TinyIPFIX for Efficient Data Transmission in Wireless Sensor Networks (Corinna Schmitt, UZH, Switzerland)
  - Hardware Accelerated L7 Monitoring at 100 Gbps
  - Interactive Monitoring, Visualization, and Configuration of OpenFlow?-Based SDN
  - Towards botnet detection: What botnet characteristics can be detected in real-life network environments by using flow data? (Christian Dietz, UniBW, Germany)
  - Flow data storage and retrieval utilizing big data approach
  - Characterizing the IPv6 security landscape by large-scale measurements (Luuk Hendriks, U. Twente, the Netherlands)
  - Automaton models applied for fingerprinting and network participants classification
  - Distributed Anomaly Detection Based on Flow Information
  - Challenges for flow-based management - implications of draft-unify-nfvrg-devops

  This time, three presentations were done by FLAMINGO partners as indicated in the above topic list with speaker's names and affiliation.

4.1.5 Future developments

FLAMINGO partners will pursue their pre-standardization efforts through the organization and the participation to new IRTF NMRG meetings.

4.2 ICNRG

4.2.1 Context

The IRTF Information-Centric Networking Research Group (ICNRG - http://irtf.org/icnrg), which was chartered in April 2012, provides a forum for the exchange and analysis of ICN research ideas and proposals. ICN is an approach to evolve the Internet infrastructure by introducing uniquely named data as a core Internet principle. Data becomes independent from location, application, storage, and means of transportation, enabling in-network caching and replication. Compared to current content distribution technologies, the expected benefits are improved efficiency, better scalability with respect to information/bandwidth demand and better robustness in challenging communication scenarios.

The main objective of the ICNRG is to couple ongoing ICN research with solutions that are relevant for evolving the Internet at large. The group focuses on three working documents:

- ICN Survey (survey of different approaches and techniques),
- ICN Research Challenges (ICN problem statement, main concepts and research challenges),
- ICN Baseline Scenarios (scenarios to enable performance comparisons between different approaches).

The activities of the group will be documented in Informational and Experimental RFCs.

4.2.2 Contributions (year 1)

University College London (UCL) has been following and contributing to the activities of the group. During the first year of FLAMINGO UCL participated in two ICNRG meetings in Stockholm and Berlin, in February and July of 2013, respectively, in a continuous effort for contributions and status updates to the working items of the group. More specifically, UCL contributed to the second document on research challenges[102] focusing on issues related to in-network caching. These include cache placement (on-path, off-path), content-to-cache distribution techniques and resource management, and routing of content requests. After the meeting in Berlin, UCL also worked on the dependencies between the different research challenges in a coordinated effort with other contributors.

4.2.3 Contributions (year 2)

In the second year of FLAMINGO UCL participated in two ICNRG meetings that took place in London and Paris (interim meeting), in March and September 2014, respectively. During the meetings UCL contributed to the group discussions on ICN issues related to video distribution, IoT and mobility, CCN/NDN implementation differences, and also to the status review of the working documents.

UCL continues to contribute to the second document on research challenges mainly focusing on issues related to cache-aware routing. During the review phase of the working documents, UCL received comments from other group members on its contributions and has also provided comments to the other two documents, which will be taken into account in the next version. In addition, UCL participated in the Dagstuhl seminar on Information-Centric Networking, which took place in July 2014 and was organized mainly by ICNRG members. During the seminar UCL presented ongoing work on in-network resource pooling and name-based replication for disaster management; there was a lot of discussion around these topics from the community.

UCL contributions related to in-network caching (e.g. cache-aware routing, content distribution) have been influenced by the joint research between iMinds and UCL on cache management, which is carried out in the context of WP6.

4.2.4 Contributions (year 3)

In the third year of FLAMINGO, UCL continued its contributions to the second document on ICN research challenges and integrated comments received from other members of the group. This document has now been submitted for becoming an Informational RFC. In addition, UCL contributed to a newly created document about using ICN in disaster scenarios[103]. Based on the feedback received from the group, the disaster management approach, which was presented during the previous reporting period, was revised accordingly and the text was integrated to this new document.

UCL also participated in a two-day ICNRG meeting that took place in Prague, Czech Republic, in July 2015. During the meeting, UCL presented on-going work for solving the congestion problem using information centric network principles, and about information resilience in disrupted information centric networks. The presentations received questions and constructive feedback that will influence the future extensions of this work. In addition, the document on ICN research challenges was discussed with other members of the group, who did not object to submit it for becoming an Informational RFC in its current state. UCL also participated in the discussions concerning the Internet of Things (IoT) and ICN. More specifically, an ICN architecture for IoT was discussed and how good an application environment IoT is for ICN.

UCL contributions related to in-network caching and information resilience have been influenced by the joint research activity between iMinds and UCL on cache management for telco operated content delivery, which is carried out in the context of WP6 (see D6.3).

4.2.5 Future developments

During the last year of FLAMINGO, UCL plans to follow upcoming ICNRG meetings and continue contributing to the working documents. Most importantly, UCL plans to address the comments that will be received on the second document that has been submitted for becoming an Informational RFC. In the immediate future, UCL will participate in the interim meeting, which will take place in San Francisco (in conjunction with the ICN'15 conference) and the meeting in Yokohama, Japan.

5 Task T4.3: Standardization in other fora

FLAMINGO is also interested in investigating new opportunities in other fora on a case by case basis. In particular, it has contributed to the FitSM family on federated IT service management,

part of the FedSM project and recently adopted by the Helix Nebula consortium, and to socio-economic standardization at the ITU-T within the Study Group 13 on economic incentives of future networks.

5.1 FiTSM

5.1.1 Context

The FitSM family of documents is produced by the FedSM project, an initiative co-funded by the European Commission Seventh framework Programme to improve service management in a selected set of federated ICT infrastructures and bring experience from this improvement to a broad community of federated communities. This standard is meant to be constituted of seven documents, namely from FitSM-0 to FitSM-6. UPC is a partner of the FedSM project and as such, it participates in its development.

FitSM, which stands for ”Federated information technology Service Management” is meant to become a lightweight standard family aimed at facilitating service management in federated IT service provision.

The main goals of the FitSM family are:

- Create a clear, minimal standard that allows for effective, defined service management,
- Offer a version of service management that can cope with federated environments, which often lack the hierarchy and formal agreements seen in other situations,
- Provide a baseline level of service management than can act to support management interoperability in federated environments where disparate or competing organisations must cooperate to manage services.

The FitSM family of documents is produced by the FedSM project, an initiative co-funded by the European Commission Seventh framework Programme to improve service management in a selected set of federated ICT infrastructures and bring experience from this improvement to a broad community of federated communities. UPC is a partner of the FedSM project and as such it participates in its development.

The FitSM family is composed of the following six documents:

- FitSM-0: Overview and vocabulary,
- FitSM-1: Standard requirements for lightweight service management in federated IT infrastructures,
- FitSM-2: Recommended activities for lightweight service management in federated IT infrastructures,
- FitSM-3: Recommended role model for lightweight service management in federated IT infrastructures,
- FitSM-4: Recommended documents and selected templates for lightweight service management in federated IT infrastructures,
- FitSM-5: Guidance on the application and implementation of lightweight service management in federated IT infrastructures.

5.1.2 Contributions (year 1)

UPC has participated in the creation of the currently available documents. In particular, UPC has contributed to the following documents.

Contribution to FitSM-0:2013 This document provides: a general overview of the FitSM family of standards for lightweight service management in federated IT infrastructures; and terms and definitions for use in the FitSM family of standards.

This document is applicable to all types of organizations (e.g. commercial enterprises, government agencies, non-profit organizations) who are part of or otherwise involved in a federation from which federated services are provided, regardless of type, size and the nature of the services delivered.

UPC has been involved in the adaptation of different terms from other source vocabularies to the FitSM problem domain.

This document is publicly available at http://www.fedsm.eu/sites/default/files/FitSM-0-2013.pdf

Contribution to FitSM-1:2013 This document sets out a very minimal set of requirements for ITSM. This is intended to be achievable but useful in a federated environment or other environment where traditional ITSM is difficult to introduce. It targets a lower level of ability than ISO/IEC 20000, but one compatible with this Standard and that can act as a first step to introducing more traditional ITSM.

In terms of scope, FitSM-1:2013 seeks to achieve or describe only a moderate level of ability in ITSM. It targets an overall ITSM maturity that can be said to be defined. This means that it must be defined and documented, with well understood roles and responsibilities. It does not target higher levels of maturity that would achieve heavily metricized and tightly managed or optimized situations. However, those reaching the limits of the scope set by FitSM would be very well placed to implement the more complex requirements listed in ISO/IEC 20000 and other traditional ITSM standards and approaches.

UPC has been contributing in the establishment and refinement of the requirements to be fulfilled in each of the fourteen management processes dealt within FitSM. This document is publicly available at `http://www.fedsm.eu/sites/default/files/FitSM-1-2013.pdf`

Contribution to FitSM-2:2013 This document sets out a set of goals for each IT service management process in the FitSM model. It also provides a set of activities which can be undertaken to meet the requirements set out in FitSM-1:2013. These activities are not intended to be exhaustive or the only activities that can be used to meet the requirements, but they give some of the guidance needed to address meeting the FitSM-1 requirements. UPC has contributed to derive activities from requirements in a a subset out of the fourteen service management processes considered in FitSM. This document is publicly available at http://www.fedsm.eu/sites/default/files/FitSM-2-2013.pdf.

5.1.3 Contributions (year 2)

Year two led to the drafting of the remaining documents of the FitSM family of standards. FitSM-3 consists of the recommended role model in federated environments. The FLAMINGO contribution to this document was minor, limited to a reviewer role. FitSM-4 is a set of templates that were

created to design the service management system. FLAMINGO's contribution to this specific effort is the template for SLAs. Complementing the definition of templates, a set of procedures were defined. They are part of the FitSM-5 document. Procedures are in general issued when defining a template seems too much rigid for the service providers. In this context we participated in the elaboration of the guidelines to identify services and to specify services. FitSM-6 is the final document of the FitSM family. FitSM-6 is a tool for service providers to "self-assess" their system management capabilities. The document is structured around the fourteen processes of the standard. For each process we only consider the three capability levels developed within the project, namely Ad-hoc, Repeatable and Defined, Then, for each process requirement we describe in text what has to be fulfilled to have the given capability level. UPC was also contributing to the definition of this document and in particular to the specification of the capability levels of the Configuration Management process and the Capacity Management process.

5.1.4 Contributions (year 3)

Year 3 has been concentrated in the production of new samples, templates and practical guides, thus augmenting the documents available in FitSM-4 and FitSM-5. The specific templates where we contributed were dictated by the needs of our client partners in the FedSM project and we proposed drafts that were conveniently discussed with such partners before were finally released. Among the samples UPC produced we can mention one for the Capacity Plan, the Availability Plan and the Continuity Plan. In others like the SLA Template, a sample of an SLA, a template of an OLA/UA, the sample for the OLA/UA and a sample for a corporate level SLA, UPC contributed reviewing the corresponding documents. Also an achievement of year 3 in that context was the realization of an audit of the Service Management System at each client site (three in total). In that activity, UPC contributed participating as co-auditor in the audit conducted at CSC/Cyfronet in Helsinki. Last but not least, another of our contributions has been in the domain of building the training framework of FitSM. That training framework consist of four course levels, namely Foundations, Advanced in Service Operation and Control (SOC), Advanced in Service Provision and Delivery (SPD) and Expert Level. Each is constituted by course slides and sets of questions for the exams and to be used during the training courses. In the reported year UPC contributing proposing new questionnaires and reviewing others from colleagues for the Advanced in SOC level course, the Advanced in SPD and the Expert Level as well.

5.1.5 Future developments

The FedSM project that coined the FitSM standard is ended. Nevertheless the exploitation rights and maintenance of the standard have been transferred to ITEMO, http://www.itemo.org, a non profit organization devoted to ITSM and to which UPC and others institutions participating in the creation of FitSM are members. From such a perspective we will continue monitoring the adoption of the standard and we will improve it in several aspects. At the moment of editing this deliverable several working groups in ITEMO have been created to drive the development. In particular, UPC is participating in the working groups aimed at producing and improving the documents of FitSM-4 and FitSM-5 and it is also contributing in the marketing group with the idea to promote its use in Spain through its participation in the Spanish itSMF of which a representative of UPC is already a member. In addition UPC leads the working group that will be devoted to control the translation of the standard from English to different languages. All these activities will our subject in the next year.

5.2 ITU-T SG13

As mentioned in Section 3.10 University of Zurich investigates Legal Implications in WP7, which influences the standardization approaches. The standardization approaches by University of Zurich aim on three mentioned goals, where the first goal is in the focus of standardization under ITU-T SG13 Q16. The upcoming subsection will characterize the approach in more details.

5.2.1 Context

UZH states that Future Network (FN) technology as investigated in the context of FLAMINGO has to undergo a systematic socio-economic assessment during (a) technology design and (b) technology standardization phases in order to anticipate the extent to which the FN technology is designed for tussle. This is important, since all major design goals and principles for Internet-related technology, services, and operations must be critically reviewed to ensure that the Internet continues to operate.

Therefore, UZH is highly active in standardization, which resulted in the framework of the SESERV project in the ITU-T recommendation Y.3001 on 'Future networks: Objectives and design goals', which contains the major contribution by UZH and AUEB on 'Economic Incentives' which highlights the need to consider 'economic and social aspects, such as economic incentives in designing and implementing the requirements, architecture, and protocol of FNs, in order to provide the various participants with a sustainable, competitive environment.'

5.2.2 Contributions (year 1)

The recent work in continuation of this general statement on tussles in Y.3001 started on October 10, 2011, under ITU-T's SG13 Q16 with the draft Recommendation Y.FNsocioeconomic entitled 'Economic Incentives of Future Networks'. Its main content addresses the first goal as follows. Tussle analysis determines the meta-methodology recommended for conducting a socio-economic assessment in the context of Future Networks (FN). When applying tussle analysis to FN technology, the following steps should be performed [104, 105]:

1. Identify all primary stakeholder roles and their characteristics for the functionality under investigation.
2. Identify tussles among identified stakeholders (e.g. impact of technology, circumvention of negative impacts).

In the ideal scenario of a tussle analysis, the outcome is an equilibrium where (a) all stakeholders of this functionality derive a payoff that is considered fair and (b) no stakeholder of another functionality, who was receiving a fair payoff before, gets an unfair payoff after this tussle equilibrium has been reached. If both conditions (a) and (b) hold then the analysis of this particular tussle is completed and the focus should be shifted on to the remaining tussles identified in step 2. In case, condition (a) is not met, a new iteration of the methodology must be performed. Here modified assumptions on the most probable policies adopted by unhappy stakeholders must be performed. Similarly, a new iteration must be performed for each spillover to other functionalities when (b) is not met. Ideally a new technology should lead to a stable outcome without spillovers to other functionalities. In case where no such improvement takes place, the technology designer should examine whether a change in the implementation details would lead to a better outcome [104, 105].

5.2.3 Contributions (year 2)

After several years of participation in ITU-T meetings, discussions within SG13 Q16, and updates of the draft recommendation Y.FNsocioeconomic it passed the consensus in SG13's Working Party 3 (WP3) and the consensus in ITU-T Study Group 13 (SG13) successfully in beginning of July 2014. The final printed Recommendation has been published unde the title entitled 'Y.3013 : Socio-economic Assessment of Future Networks by Tussle Analysis' [106]. The Recommendation Y.3013 is the first Swiss academic Recommendation within ITU-T. Based on this success UZH members were invited to the CS4 - Commission for Standardization by the Swiss Telecommunication Association (ASUT) in September 2014. Here the development process of the recommendation Y.3013 and the proposed Tussle Analysis were presented. The audience consisted of members from telecommunication area (e.g., Swisscom), industry (e.g., Microsoft), and academic field. Lots of discussion took place and they agreed that Tussle Analysis will be a helpful tool for market analysis in their business areas.

5.2.4 Contributions (year 3)

On April 24, 2015 UZH held a presentation on 'Tussles for Edge Network Caching' at the ITU Workshop on 'Future Trust and Knowledge Infrastructure'. In this talk the Tussle Analysis was applied to analyze and predict socio-economic consequences, when content from social networks is cached in end-users controlled nano data centers. The talk applied Tussle Analysis to identify the most important stakeholders for this technology, their interests, and conflicts between them. Since there were several security and trust experts in the audience, valuable feedback on the proposed solution and evaluation was received. Therefore, UZH's presentation not only ensured FLAMINGO's visibility in a world-wide established and influential standardization organization, it also provided the basis for the establishment of a valuable feedback for the project to further improve different technologies.

5.2.5 Future developments

Representatives of the University of Zurich will participate in upcoming meetings of ITU-T in 2016. UZH will look for new contribution areas and will continue activity within ITU-T's RevCom meetings. The need for consideration of socio-economic aspects is recognized by ITU-T but a suitable tool to address these aspects in the standardization process is missing. This gap became particularly visible in the discussions on UZHs contribution to ITU-T's RevCom meeting in 2014, which proposed to integrate tussle analysis into ITU-T's standardization process. This proposal was delayed, because tussle analysis is specified in Y.3013, which was still under development at that point. However, as Y.3013 is now published, also UZH's efforts within RevCom are planned to be resumed. Furthermore, UZH is getting habitually contacted be the ITU-T secretary to attend and contribute to different ITU events. Of course, these opportunities will also be embraced in the future to participate and enrich ITU-T events.

5.3 ITU-T SG17

Based on UZH's visit at ITU in November 2014 UZH was invited by the SG 17 chair Martin Euchner to present a tutorial on security research under the umbrella of the external liaison between SmartenIT and FLAMINGO.

5.3.1 Context

ITU-T Study Group 17 (SG17) coordinates security-related work across all ITU-T Study Groups. Often working in cooperation with other standards development organizations (SDOs) and various ICT industry consortia, SG17 deals with a broad range of standardization issues (e.g., cyber security, security management, security architectures, security of applications and services for the Internet-of-Things.

5.3.2 Contributions (year 3)

The tutorial entitled 'Two-way Authentication for Tiny Devices' was held on April 15, 2015 in front of SG 17 members (around 15 participants). The tutorial covers a brief overview about the research, the application area, developed solutions TinyDTLS and TinyTO, and lessons learned. The audience acknowledged these standard-based solutions, which allow for the support of a two-way authentication on constraint devices, like sensor nodes (e.g., TelosB or OPAL). The audience was pleased to learn that not only theoretical ideas were presented, but existing solutions and successfully running code. The following discussions raised the question of what can be a common definition for constraint devices. This seems to be a dedicated need for the ITU, since no formal definition is in place. Furthermore, the question on how to perform the key management and its standardization was asked. Potential solutions include creation and revocation mechanisms for any keys and specification on which algorithms should be used and can be performed by constraint devices. UZH is involved in discussions around this topic.

For external liaisons purposes the meeting was successful in order to continue standardization efforts under ITU in the SG 17 addressing security issues, especially Questions 5 and 11.

5.3.3 Future developments

UZH will participate in periodical meetings of SG17 and will attend online meetings in order to investigate how to continue with ITU-T activity in year four of FLAMINGO.

6 Partner role synthesis

The following table provides a synthesis of partner roles during the three years with respect to the three tasks defined for this work package on standardization. pre-standardization and T4.3 on other standardization fora).

Partner	T4.1 IETF Standardization	T4.2 IRTF Pre-Standardization	T4.3 Other Standardization Fora
UT	• Draft Editor (IPFIX)	• Participant (NMRG)	-
INRIA	• Draft / RFC Editor (IPFIX, SIPCLF)	• Co-Chair (NMRG), • Meeting Organizer (NMRG), • Participant (NMRG)	-
UZH	• Draft Editor (CoRE / ACE),	• Participant (NMRG)	• Draft Editor (ITU-T SG13) • Presenter (ITU-T SG13) • Tutorial presenter (ITU-T SG17)
JUB	• Co-Chair (NETMOD) • Draft / RFC Editor (NETCONF, NETMOD, OPSAWG, 6LOWPAN / 6LO, ROLL) • Participant (I2RS, LMAP) • Member (OPS Directorate, IoT Directorate, YANG Doctors, MIB Doctors)	• Meeting Organizer (NMRG) • Participant (NMRG)	-
UPC	-	-	• Editor (FiTSM)
iMinds	• Draft Editor (CDNi)	-	-
UCL	-	• Participant (ICNRG)	-

7 Links with research work packages

The following table provides a synthesis of links between the activities done in this work package on standardization and the three research work packages.

		WP5	WP6	WP7
T4.1 IETF Standardization	NETCONF	X	X	
	NETMOD	X	X	
	IPFIX	X	X	
	OPSAWG	X		
	SIPCLF	X		
	CDNi		X	
	6LOWPAN/6LO	X		
	ROLL	X	X	
	COMAN/OPSAWG	X	X	
	CoRE/ACE			X
	Core			X
T4.2 IRTF Pre-Standardization	NMRG	X	X	
	ICNRG		X	
T4.3 Other Standardization Fora	FITSM		X	
	ITU-T SG13			X
	ITU-T SG17			X

8 Top 5 contributions

The goal of this section is to identify the most important contributions to the standard (Top 5) which have been possible with the support of FLAMINGO. Contributions can take different forms such as producing a new standard by authoring or editing a document or animating a working or research group that will produce new standards. Both contributions are important to take into account.

Contributions to a standard is generally not limited to a single document as the realized work during the project on a specific topic may span multiple standards. Hence, the three first groups of contributions have firstly been identified by two other selected contributions

- Configuration management with activities related to NETCONF, YANG, and RESTCONF as well as the co-chairing of the NETMOD WG. The YANG data modeling language enjoys a significant uptake in the industry. This makes the co-chairing of the NETMOD WG a time consuming activity that can only be carried out through the support of the FLAMINGO project. This work is particularly linked to WP1 (open source nccclient) and WP3 (interoperability lab). More recently, adaptation of RESTCONF for embedded devices is closely related to WP6.
- IoT management and security related activities in COMAN/OPSAWG, ROLL and 6LOWPAN/6LO are related to research work in WP3 (special session on IoT management at NOMS 2014 reported in D3.3), WP5 (IoT management) and WP6 (security of RPL networks).
- The definition of location-aware flow measurement information elements is the outcome of joint work between UT and INRIA. This collaborative work was made possible by the support of the FLAMINGO project in WP6 (reported in D6.2) and has been presented in IETF IPFIX and IRTF NMRG.

- The *Socio-economic Assessment of Future Networks by Tussle Analysis* contribution would not have been possible without the work done in WP7 (reported in D7.3) and it reinforces the participation of UZH within ITU-T as highlighted by the expressed interest of other groups.
- By co-chairing the IRTF NMRG and by actively participating in NMRG meetings, we empowered people from this community to frequently meet together for exchanging ideas and starting new cooperations. Therefore, it is also one of the top 5 contributions since, being a Network of Excellence in network and service management, it was highly important that FLAMINGO partners are active and visible in the corresponding community. It is important to note that work from different WPs have been presented in NMRG espcially from WP5 (IPv6 measurement, DDoS monitoring, botnet detection) and WP6 (location-aware monitoring using IPFIX).

Since all these five contributions have different forms, no ranking between them can be provided.

9 Conclusions

Work package 4 aims at advancing the network and service management standardization and impact the relevant working groups. It is structured into three tasks: Task T4.1 on IETF standardization, Task T4.2 on IRTF pre-standardization and Task T4.3 on other standardization fora. During the three first years of the FLAMINGO project, these tasks have enabled to make progress on all the objectives of the work package, as follows:

- **Objective 1: to contribute to the writing of Internet-Drafts and RFCs**

  FLAMINGO partners have written 23 contributions relative to 18 Internet-Drafts and 7 RFCs. In particular, the efforts during Y3 have focused on:

  - 2 new RFCs on Configuration Management (NETCONF, NETMOD)
  - 1 new on Virtual Machines management (OPSAWG),
  - 2 new RFCS on Internet-of-Things (6LOWPAN/6LO, COMAN/OPSAWG),
  - 2 revised Internet-Drafts on Configuration Management (NETCONF),
  - 2 revised Internet-Drafts on Flow-based Monitoring (NMRG, IPFIX)
  - 1 revised Internet-Drafts on Virtual Machines management (OPSAWG),
  - 4 revised and 1 new Internet-Drafts on Internet-of-Things (COMAN/OPSAWG, CoRE/ACE, CoRE)

- **Objective 2: to chair IETF working groups**

  FLAMINGO has co-chaired the IETF NETMOD WG dedicated to the data modelling language (YANG) of the NETCONF network management protocol. It supports the ongoing deployment of YANG by developing a set of core YANG data models. During the third year, the efforts have mainly focused on the maintainance of YANG language definition by targeting a new release (v1.1) soon.

- **Objective 3: to organize IRTF-NMRG meetings**

  FLAMINGO has co-chaired the NMRG research group at the IRTF task force and (co-)organized a total of 9 meetings. A series of 3 new meetings took place during the third year:

  - 35th IRTF-NMRG meeting on Autonomics for Network Management (Part IV),
  - 36th IRTF-NMRG meeting on Security,
  - 37th IRTF-NMRG meeting on flow-based measurements (as a continuation of the series of Workshops on the Usage of Netflow/IPFIX in Network Management).

- **Objective 4: to contribute to other standardization fora**

  FLAMINGO has also continued its efforts in other fora during the third year:

  - FitSM family on federated IT service management adopted by the Helix Nebula consortium: new contributions have been done relatively to the FitSM-4 (selected templates) and FitSM-5 (guidance on the application) documents, the audit of the Service Management System and the training framework.
  - Socio-economic standardization at ITU-T within the study group 13 on economic incentives of future networks. During third year, a methodology applying tussle analysis has been designed for evaluating socio-economic consequences of end-users nano data centers.

- Security of constrained devices: a two-way authentication methods for tiny devices has been introduced to the ITU-T study group 17.

The general conclusion is that work package 4 is running well and made important contributions to the IETF and IRTF task forces during these first three years. Year 3 was particularity focused on revising previously proposed documents. Efforts and synergies should be maintained for the next period, in order to pursue the impact of FLAMINGO on the relevant standardization groups. It also consists in targeting newly created groups like IETF DOTS (DDoS Open Threat Signaling) and IRTF NMLRG (Network Machine Learning Research Group).

Abbreviations

6LO	IPv6 over Networks of Resource-constrained Nodes
6LOWPAN	IPv6 over Low power Wireless Personal Area Networks
ACE	Authentication and Authorization for Constrained Environments
AUEB	Athens University of Economics and Business
CDN	Content Delivery Networks
CDNi	Content Delivery Networks interconnection
CLF	Common Log Format
COMAN	Constrained Management
CoAP	Constrained Application Protocol
CoRE	Constrained RESTful Environments
DTLS	Datagram Transport Layer Security
ECDH	Elliptic Curve Diffie-Hellman
ECC	Elliptic Curve Cryptography
ECDSA	Elliptic Curve Digital Signature Algorithm
ECIES	Elliptic Curve Integrated Encryption System
EMAN	Energy Management
GPRS	General Packet Radio Service
GPS	Global Positioning System
ICN	Information-Centric Network
ICNRG	Information-Centric Networking Research Group
I-D	Internet-Draft
IESG	Internet Engineering Steering Group
IETF	Internet Engineering Task Force
IoT	Internet of Things
IRTF	Internet Research Task Force
IPFIX	Internet Protocol Flow Information Export
IPv4	Internet Protocol version 4
IPv6	Internet Protocol version 6
ITU	International Telecommunication Union

FiTSM	Federated information technology Service Management
FN	Future Networks
MIB	Management Information Base
NETCONF	Network Configuration Protocol
NETMOD	NETCONF Data Modelling Language
NMRG	Network Management Research Group
OPSAWG	Operations and Management Area Working Group
PKC	Public Key Cryptography
RFC	Request For Comments
REST	REpresentational State Transfer
RPL	IPv6 Routing Protocol for Low Power and Lossy Networks
ROLL	Routing Over Low Power and Lossy Networks
SESERV	Socio-Economics Service for European Research Projects
SMART	Specific, Measurable, Achievable, Relevant, Timely
SNMP	Simple Network Management Protocol
SG	Study Group
SIP	Session Initiation Protocol
SMI	Structure of Management Information
SSH	Secure Shell
TCP	Transmission Control Protocol
TLS	Transport Layer Security
UDP	User Datagram Protocol
VM	Virtual Machine
WG	Working Group
YANG	Yet Another Next Generation

References

[1] R. Enns. NETCONF Configuration Protocol. RFC 4741, Juniper Networks, December 2006.

[2] R. Enns, M. Bjorklund, J. Schönwälder, and A. Bierman. Network Configuration Protocol (NETCONF). RFC 6241, Juniper Networks, Tail-f Systems, Jacobs University, Brocade, June 2011.

[3] M. Wasserman. Using the NETCONF Protocol over Secure Shell (SSH). RFC 6242, Painless Security, June 2011.

[4] M. Badra. NETCONF over Transport Layer Security (TLS). RFC 5539, CNRS/LIMOS Laboratory, May 2009.

[5] M. Badra, A. Luchuk, and J. Schönwälder. Using the NETCONF Protocol over Transport Layer Security (TLS). Internet Draft <draft-ietf-netconf-rfc5539bis-03>, LIMOS Laboratory, SNMP Research, Jacobs University Bremen, May 2013.

[6] M. Badra, A. Luchuk, and J. Schönwälder. Using the NETCONF Protocol over Transport Layer Security (TLS). Internet Draft <draft-ietf-netconf-rfc5539bis-04>, LIMOS Laboratory, SNMP Research, Jacobs University Bremen, October 2013.

[7] K. Watsen J. Schönwälder. A YANG Data Model for NETCONF Server Configuration. Internet Draft <draft-kwatsen-netconf-server-00>, Juniper Networks, Jacobs University Bremen, January 2014.

[8] K. Watsen J. Schönwälder. A YANG Data Model for NETCONF Server Configuration. Internet Draft <draft-kwatsen-netconf-server-01>, Juniper Networks, Jacobs University Bremen, February 2014.

[9] M. Badra, A. Luchuk, and J. Schönwälder. Using the NETCONF Protocol over Transport Layer Security (TLS). Internet Draft <draft-ietf-netconf-rfc5539bis-05>, LIMOS Laboratory, SNMP Research, Jacobs University Bremen, January 2014.

[10] K. Watsen J. Schönwälder. NETCONF Server Configuration Model. Internet Draft <draft-ietf-netconf-server-model-00>, Juniper Networks, Jacobs University Bremen, May 2014.

[11] K. Watsen J. Schönwälder. NETCONF Server Configuration Model. Internet Draft <draft-ietf-netconf-server-model-01>, Juniper Networks, Jacobs University Bremen, June 2014.

[12] K. Watsen J. Schönwälder. NETCONF Server Configuration Model. Internet Draft <draft-ietf-netconf-server-model-02>, Juniper Networks, Jacobs University Bremen, September 2014.

[13] K. Watsen J. Schönwälder. NETCONF Server Configuration Model. Internet Draft <draft-ietf-netconf-server-model-03>, Juniper Networks, Jacobs University Bremen, September 2014.

[14] M. Badra, A. Luchuk, and J. Schönwälder. Using the NETCONF Protocol over Transport Layer Security (TLS). Internet Draft <draft-ietf-netconf-rfc5539bis-06>, LIMOS Laboratory, SNMP Research, Jacobs University Bremen, September 2014.

[15] M. Badra, A. Luchuk, and J. Schönwälder. Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication. Internet Draft <draft-ietf-netconf-rfc5539bis-07>, LIMOS Laboratory, SNMP Research, Jacobs University Bremen, December 2014.

[16] M. Badra, A. Luchuk, and J. Schönwälder. Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication. Internet Draft <draft-ietf-netconf-rfc5539bis-08>, LIMOS Laboratory, SNMP Research, Jacobs University Bremen, January 2015.

[17] M. Badra, A. Luchuk, and J. Schönwälder. Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication. Internet Draft <draft-ietf-netconf-rfc5539bis-09>, LIMOS Laboratory, SNMP Research, Jacobs University Bremen, February 2015.

[18] M. Badra, A. Luchuk, and J. Schönwälder. Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication. Internet Draft <draft-ietf-netconf-rfc5539bis-10>, LIMOS Laboratory, SNMP Research, Jacobs University Bremen, April 2015.

[19] M. Badra, A. Luchuk, and J. Schönwälder. Using the NETCONF Protocol over Transport Layer Security (TLS) with Mutual X.509 Authentication. RFC 7589, Zayed University, SNMP Research, Jacobs University, June 2015.

[20] K. Watsen J. Schönwälder. NETCONF and RESTCONF Server Configuration Model. Internet Draft <draft-ietf-netconf-server-model-05>, Juniper Networks, Jacobs University Bremen, December 2014.

[21] K. Watsen J. Schönwälder. NETCONF and RESTCONF Server Configuration Model. Internet Draft <draft-ietf-netconf-server-model-06>, Juniper Networks, Jacobs University Bremen, February 2015.

[22] P. van der Stok, B. Greevenbosch, A. Bierman, J. Schönwälder, and A. Sehgal. CoAP Management Interface. Internet Draft (work in progress) <draft-vanderstok-core-comi-06.txt>, Consultant, YumaWorks, Jacobs University, February 2015.

[23] P. van der Stok, A. Bierman, J. Schönwälder, and A. Sehgal. CoAP Management Interface. Internet Draft (work in progress) <draft-vanderstok-core-comi-07.txt>, Consultant, YumaWorks, Jacobs University, July 2015.

[24] P. van der Stok, A. Bierman, J. Schönwälder, and A. Sehgal. CoAP Management Interface. Internet Draft (work in progress) <draft-vanderstok-core-comi-08.txt>, Consultant, YumaWorks, Jacobs University, October 2015.

[25] M. Bjorklund. YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF). RFC 6020, Tail-f Systems, October 2010.

[26] J. Schönwälder. Common YANG Data Types. RFC 6021, Jacobs University, October 2010.

[27] J. Schönwälder. Common YANG Data Types. Internet Draft (work in progress) <draft-schoenw-netmod-rfc6021-bis-01.txt>, Jacobs University, December 2012.

[28] J. Schönwälder. Common YANG Data Types. Internet Draft (work in progress) <draft-ietf-netmod-rfc6021-bis-00.txt>, Jacobs University, February 2013.

[29] J. Schönwälder. Common YANG Data Types. Internet Draft (work in progress) <draft-ietf-netmod-rfc6021-bis-01.txt>, Jacobs University, March 2013.

[30] J. Schönwälder. Common YANG Data Types. Internet Draft (work in progress) <draft-ietf-netmod-rfc6021-bis-02.txt>, Jacobs University, May 2013.

[31] J. Schönwälder. Common YANG Data Types. Internet Draft (work in progress) <draft-ietf-netmod-rfc6021-bis-03.txt>, Jacobs University, May 2013.

[32] J. Schönwälder. Common YANG Data Types. RFC 6991, Jacobs University, July 2013.

[33] M. Björklund and J. Schönwälder. A YANG Data Model for SNMP Configuration. Internet Draft (work in progress) <draft-ietf-netmod-snmp-cfg-01.txt>, Tail-f Systems, Jacobs University, February 2013.

[34] M. Björklund and J. Schönwälder. A YANG Data Model for SNMP Configuration. Internet Draft (work in progress) <draft-ietf-netmod-snmp-cfg-02.txt>, Tail-f Systems, Jacobs University, April 2013.

[35] M. Björklund and J. Schönwälder. A YANG Data Model for SNMP Configuration. Internet Draft (work in progress) <draft-ietf-netmod-snmp-cfg-03.txt>, Tail-f Systems, Jacobs University, November 2013.

[36] M. Björklund and J. Schönwälder. A YANG Data Model for SNMP Configuration. Internet Draft (work in progress) <draft-ietf-netmod-snmp-cfg-04.txt>, Tail-f Systems, Jacobs University, February 2014.

[37] M. Björklund and J. Schönwälder. A YANG Data Model for SNMP Configuration. Internet Draft (work in progress) <draft-ietf-netmod-snmp-cfg-05.txt>, Tail-f Systems, Jacobs University, May 2014.

[38] M. Björklund and J. Schönwälder. A YANG Data Model for SNMP Configuration. Internet Draft (work in progress) <draft-ietf-netmod-snmp-cfg-06.txt>, Tail-f Systems, Jacobs University, July 2014.

[39] M. Björklund and J. Schönwälder. A YANG Data Model for SNMP Configuration. Internet Draft (work in progress) <draft-ietf-netmod-snmp-cfg-07.txt>, Tail-f Systems, Jacobs University, August 2014.

[40] M. Björklund and J. Schönwälder. A YANG Data Model for SNMP Configuration. Internet Draft (work in progress) <draft-ietf-netmod-snmp-cfg-08.txt>, Tail-f Systems, Jacobs University, September 2014.

[41] J. Schönwälder, A. Sehgal, T. Tsou, and C. Zhou. Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). RFC 7388, Jacobs University, Huawei, October 2014.

[42] O. Festor, A. Lahmadi, R. Hofstede, and A. Pras. Information Elements for IPFIX Metering Process Location. Internet Draft <draft-festor-ipfix-metering-process-location-00.txt>, INRIA, University of Twente, June 2013.

[43] O. Festor, A. Lahmadi, R. Hofstede, and A. Pras. Information Elements for IPFIX Metering Process Location. Internet Draft <draft-festor-ipfix-metering-process-location-01.txt>, INRIA, University of Twente, July 2013.

[44] O. Festor, A. Lahmadi, R. Hofstede, and A. Pras. Information Elements for IPFIX Metering Process Location. Internet Draft <draft-festor-ipfix-metering-process-location-02.txt>, INRIA, University of Twente, January 2014.

[45] O. Festor, A. Lahmadi, R. Hofstede, and A. Pras. Information Elements for IPFIX Metering Process Location. Internet Draft <draft-irtf-nmrg-location-ipfix-03.txt>, INRIA, University of Twente, April 2015.

[46] O. Festor, A. Lahmadi, R. Hofstede, and A. Pras. Information Elements for IPFIX Metering Process Location. Internet Draft <draft-irtf-nmrg-location-ipfix-04.txt>, INRIA, University of Twente, July 2015.

[47] P. Aitken, B. Claise, C. McDowall, and J. Schönwälder. Exporting MIB Variables using the IPFIX Protocol. Internet Draft <draft-ietf-ipfix-mib-variable-export-06>, Cisco Systems, Jacobs University, July 2014.

[48] P. Aitken, B. Claise, C. McDowall, and J. Schönwälder. Exporting MIB Variables using the IPFIX Protocol. Internet Draft <draft-ietf-ipfix-mib-variable-export-07>, Cisco Systems, Jacobs University, October 2014.

[49] P. Aitken, B. Claise, C. McDowall, and J. Schönwälder. Exporting MIB Variables using the IPFIX Protocol. Internet Draft <draft-ietf-ipfix-mib-variable-export-08>, Cisco Systems, Jacobs University, December 2014.

[50] P. Aitken, B. Claise, C. McDowall, and J. Schönwälder. Exporting MIB Variables using the IPFIX Protocol. Internet Draft <draft-ietf-ipfix-mib-variable-export-09>, Cisco Systems, Jacobs University, July 2015.

[51] H. Asai, M. MacFaden, J. Schönwälder, Y. Sekiya, K. Shima, T. Tsou, C. Zhou, and H. Esaki. Management Information Base for Virtual Machines Controlled by a Hypervisor. Internet-Draft (work in progress) <draft-asai-vmm-mib-02>, University of Tokyo, VmWare, Jacobs University, IIJ Innovation Institute, Huawei Technologies, February 2013.

[52] H. Asai, M. MacFaden, J. Schönwälder, Y. Sekiya, K. Shima, T. Tsou, C. Zhou, and H. Esaki. Management Information Base for Virtual Machines Controlled by a Hypervisor. Internet-Draft (work in progress) <draft-asai-vmm-mib-03>, University of Tokyo, VmWare, Jacobs University, IIJ Innovation Institute, Huawei Technologies, April 2013.

[53] H. Asai, M. MacFaden, J. Schönwälder, Y. Sekiya, K. Shima, T. Tsou, C. Zhou, and H. Esaki. Management Information Base for Virtual Machines Controlled by a Hypervisor. Internet-Draft (work in progress) <draft-asai-vmm-mib-04>, University of Tokyo, VmWare, Jacobs University, IIJ Innovation Institute, Huawei Technologies, July 2013.

[54] H. Asai, M. MacFaden, J. Schönwälder, Y. Sekiya, K. Shima, T. Tsou, C. Zhou, and H. Esaki. Management Information Base for Virtual Machines Controlled by a Hypervisor. Internet-Draft (work in progress) <draft-asai-vmm-mib-05>, University of Tokyo, VmWare, Jacobs University, IIJ Innovation Institute, Huawei Technologies, October 2013.

[55] H. Asai, M. MacFaden, J. Schönwälder, K. Shima, and T. Tsou. Management Information Base for Virtual Machines Controlled by a Hypervisor. Internet-Draft (work in progress) <draft-ietf-opsawg-vmm-mib-00>, University of Tokyo, VmWare, Jacobs University, IIJ Innovation Institute, Huawei Technologies, February 2014.

[56] H. Asai, M. MacFaden, J. Schönwälder, K. Shima, and T. Tsou. Management Information Base for Virtual Machines Controlled by a Hypervisor. Internet-Draft (work in progress) <draft-ietf-opsawg-vmm-mib-01>, University of Tokyo, VmWare, Jacobs University, IIJ Innovation Institute, Huawei Technologies, July 2014.

[57] H. Asai, M. MacFaden, J. Schönwälder, K. Shima, and T. Tsou. Management Information Base for Virtual Machines Controlled by a Hypervisor. Internet-Draft (work in progress) <draft-ietf-opsawg-vmm-mib-02>, University of Tokyo, VmWare, Jacobs University, IIJ Innovation Institute, Huawei Technologies, November 2014.

[58] H. Asai, M. MacFaden, J. Schönwälder, K. Shima, and T. Tsou. Management Information Base for Virtual Machines Controlled by a Hypervisor. Internet-Draft (work in progress) <draft-ietf-opsawg-vmm-mib-03>, University of Tokyo, VmWare, Jacobs University, IIJ Innovation Institute, Huawei Technologies, May 2015.

[59] H. Asai, M. MacFaden, J. Schönwälder, K. Shima, and T. Tsou. Management Information Base for Virtual Machines Controlled by a Hypervisor. Internet-Draft (work in progress) <draft-ietf-opsawg-vmm-mib-04>, University of Tokyo, VmWare, Jacobs University, IIJ Innovation Institute, Huawei Technologies, August 2015.

[60] H. Asai, M. McFaden, J. Schönwälder, K. Shima, and T. Tsou. Management Information Base for Virtual Machines Controlled by a Hypervisor. RFC 7666, Univ. of Tokyo, VMware Inc., Jacobs University, IIJ Innovation Institute Inc., Huawei Technologies (USA), October 2015.

[61] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler. SIP: Session Initiation Protocol. RFC 3261, Dynamicsoft, Columbia U., Ericsson, WorldCom, Neustar, ICIR, AT&T, June 2002.

[62] V. Gurbani, E. Burger, T. Anjali, H. Abdelnur, and O. Festor. The Common Log Format (CLF) for the Session Initiation Protocol (SIP): Framework and Information Model. RFC 6872, Alcatel Lucent Bell Labs, Georgetown University, Illinois Institute of Technology, INRIA, February 2013.

[63] G. Salgueiro, V. Gurbani, and A. B. Roach. Format for the Session Initiation Protocol (SIP) Common Log Format (CLF). RFC 6873, Cisco Systems, Alcatel Lucent Bell Labs, Mozilla, February 2013.

[64] R. van Brandenburg and O. van Deventer. Models for adaptive-streaming-aware CDN Interconnection. Internet Draft <draft-brandenburg-cdni-has-00.txt>, TNO, August 2012.

[65] J. Famaey and S. Latré. Experiments on HTTP Adaptive Streaming over interconnected Content Delivery Networks. Internet Draft <draft-famaey-cdni-has-experiments-00.txt>, Ghent University – IBBT, September 2012.

[66] J. Famaey and S. Latré. Experiments on HTTP Adaptive Streaming over interconnected Content Delivery Networks. Internet Draft <draft-famaey-cdni-has-experiments-01.txt>, Ghent University – iMinds, January 2013.

[67] R. van Brandenburg, O. van Deventer, F. Le Faucheur, and K. Leung. Models for adaptive-streaming-aware CDN Interconnection. Internet Draft <draft-brandenburg-cdni-has-05.txt>, TNO and Cisco Systems, April 2013.

[68] R. van Brandenburg, O. van Deventer, F. Le Faucheur, and K. Leung. Models for HTTP-Adaptive-Streaming-Aware Content Distribution Network Interconnection (CDNI). RFC 6983, TNO and Cisco Systems, July 2013.

[69] J. Schönwälder, A. Sehgal, T. Tsou, and C. Zhou. Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). Internet Draft <draft-schoenw-6lowpan-mib-02>, Jacobs University, Huawei Technologies, January 2013.

[70] J. Schönwälder, A. Sehgal, T. Tsou, and C. Zhou. Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). Internet Draft <draft-schoenw-6lowpan-mib-03>, Jacobs University, Huawei Technologies, February 2013.

[71] J. Schönwälder, A. Sehgal, T. Tsou, and C. Zhou. Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). Internet Draft <draft-schoenw-6lo-lowpan-mib-00>, Jacobs University, Huawei Technologies, October 2013.

[72] J. Schönwälder, A. Sehgal, T. Tsou, and C. Zhou. Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). Internet Draft <draft-schoenw-6lo-lowpan-mib-01>, Jacobs University, Huawei Technologies, November 2013.

[73] J. Schönwälder, A. Sehgal, T. Tsou, and C. Zhou. Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). Internet Draft <draft-ietf-6lo-lowpan-mib-00>, Jacobs University, Huawei Technologies, January 2014.

[74] J. Schönwälder, A. Sehgal, T. Tsou, and C. Zhou. Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). Internet Draft <draft-ietf-6lo-lowpan-mib-01>, Jacobs University, Huawei Technologies, April 2014.

[75] J. Schönwälder, A. Sehgal, T. Tsou, and C. Zhou. Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). Internet Draft <draft-ietf-6lo-lowpan-mib-02>, Jacobs University, Huawei Technologies, July 2014.

[76] J. Schönwälder, A. Sehgal, T. Tsou, and C. Zhou. Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). Internet Draft <draft-ietf-6lo-lowpan-mib-03>, Jacobs University, Huawei Technologies, August 2014.

[77] J. Schönwälder, A. Sehgal, T. Tsou, and C. Zhou. Definition of Managed Objects for IPv6 over Low-Power Wireless Personal Area Networks (6LoWPANs). Internet Draft <draft-ietf-6lo-lowpan-mib-04>, Jacobs University, Huawei Technologies, September 2014.

[78] K. Korte, A. Sehgal, J. Schönwälder, T. Tsou, and C. Zhou. Definition of Managed Objects for the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL). Internet Draft <draft-sehgal-roll-rpl-mib-06>, Jacobs University, Huawei Technologies, February 2013.

[79] M. Ersue, D. Romascanu, and J. Schönwälder. Management of Networks with Constrained Devices: Problem Statement, Use Cases and Requirements. Internet-Draft (work in progress) <draft-ersue-constrained-mgmt-03>, Nokia Siemens Networks, Avaya, Jacobs University Bremen, February 2013.

[80] M. Ersue, D. Romascanu, and J. Schönwälder. Management of Networks with Constrained Devices: Use Cases. Internet-Draft (work in progress) <draft-ersue-opsawg-coman-use-cases-00.txt>, Nokia Siemens Networks, Avaya, Jacobs University Bremen, October 2013.

[81] M. Ersue, D. Romascanu, and J. Schönwälder. Management of Networks with Constrained Devices: Problem Statement and Requirements. Internet-Draft (work in progress) <draft-ersue-opsawg-coman-probstate-reqs-00.txt>, Nokia Siemens Networks, Avaya, Jacobs University Bremen, October 2013.

[82] M. Ersue, D. Romascanu, and J. Schönwälder. Management of Networks with Constrained Devices: Use Cases. Internet-Draft (work in progress) <draft-ietf-opsawg-coman-use-cases-00.txt>, Nokia Siemens Networks, Avaya, Jacobs University Bremen, January 2014.

[83] M. Ersue, D. Romascanu, A. Sehgal, and J. Schönwälder. Management of Networks with Constrained Devices: Use Cases. Internet-Draft (work in progress) <draft-ietf-opsawg-coman-use-cases-01.txt>, Nokia Siemens Networks, Avaya, Jacobs University Bremen, February 2014.

[84] M. Ersue, D. Romascanu, A. Sehgal, and J. Schönwälder. Management of Networks with Constrained Devices: Use Cases. Internet-Draft (work in progress) <draft-ietf-opsawg-coman-use-cases-02.txt>, Nokia Networks, Avaya, Jacobs University Bremen, July 2014.

[85] M. Ersue, D. Romascanu, A. Sehgal, and J. Schönwälder. Management of Networks with Constrained Devices: Use Cases. Internet-Draft (work in progress) <draft-ietf-opsawg-coman-use-cases-03.txt>, Nokia Networks, Avaya, Jacobs University Bremen, October 2014.

[86] M. Ersue, D. Romascanu, and J. Schönwälder. Management of Networks with Constrained Devices: Problem Statement and Requirements. Internet-Draft (work in progress) <draft-ersue-opsawg-coman-probstate-reqs-00.txt>, Nokia Siemens Networks, Avaya, Jacobs University Bremen, January 2014.

[87] M. Ersue, D. Romascanu, and J. Schönwälder. Management of Networks with Constrained Devices: Problem Statement and Requirements. Internet-Draft (work in progress) <draft-ersue-opsawg-coman-probstate-reqs-01.txt>, Nokia Siemens Networks, Avaya, Jacobs University Bremen, February 2014.

[88] M. Ersue, D. Romascanu, and J. Schönwälder. Management of Networks with Constrained Devices: Problem Statement and Requirements. Internet-Draft (work in progress) <draft-ersue-opsawg-coman-probstate-reqs-02.txt>, Nokia Networks, Avaya, Jacobs University Bremen, July 2014.

[89] M. Ersue, D. Romascanu, and U. Herberg J. Schönwälder. Management of Networks with Constrained Devices: Problem Statement and Requirements. Internet-Draft (work in progress) <draft-ersue-opsawg-coman-probstate-reqs-03.txt>, Nokia Networks, Avaya, Jacobs University Bremen, Fujitsu Laboratories of America, October 2014.

[90] M. Ersue, D. Romascanu, A. Sehgal, and J. Schönwälder. Management of Networks with Constrained Devices: Use Cases. Internet-Draft (work in progress) <draft-ietf-opsawg-coman-use-cases-04.txt>, Nokia Networks, Avaya, Jacobs University Bremen, January 2015.

[91] M. Ersue, D. Romascanu, A. Sehgal, and J. Schönwälder. Management of Networks with Constrained Devices: Use Cases. Internet-Draft (work in progress) <draft-ietf-opsawg-coman-use-cases-05.txt>, Nokia Networks, Avaya, Jacobs University Bremen, March 2015.

[92] M. Ersue, D. Romascanu, and U. Herberg J. Schönwälder. Management of Networks with Constrained Devices: Problem Statement and Requirements. Internet-Draft (work in progress) <draft-ersue-opsawg-coman-probstate-reqs-04.txt>, Nokia Networks, Avaya, Jacobs University Bremen, January 2015.

[93] M. Ersue, D. Romascanu, and U. Herberg J. Schönwälder. Management of Networks with Constrained Devices: Problem Statement and Requirements. Internet-Draft (work in progress) <draft-ersue-opsawg-coman-probstate-reqs-05.txt>, Nokia Networks, Avaya, Jacobs University Bremen, March 2015.

[94] M. Ersue, D. Romascanu, J. Schönwälder, and A. Sehgal. Management of Networks with Constrained Devices: Use Cases. RFC 7548, Nokia Networks, Avaya, Jacobs University, May 2015.

[95] M. Ersue, D. Romascanu, J. Schönwälder, and U. Herberg. Management of Networks with Constrained Devices: Problem Statement and Requirements. RFC 7547, Nokia Networks, Avaya, Jacobs University, May 2015.

[96] C. Schmitt, B. Stiller, T. Kothmayr, and W. Hu. DTLS-based Security with two-way Authentication for IoT. Internet-Draft (work in progress) <draft-schmitt-two-way-authentication-for-iot-00>, IETF Internet Draft, Standards Track, CoRE, July 2013.

[97] C. Schmitt, B. Stiller, T. Kothmayr, and W. Hu. DTLS-based Security with two-way Authentication for IoT. Internet-Draft (work in progress) <draft-schmitt-two-way-authentication-for-iot-01>, IETF Internet Draft, Standards Track, CoRE, October 2013.

[98] C. Schmitt, B. Stiller, T. Kothmayr, and W. Hu. DTLS-based Security with two-way Authentication for IoT. Internet-Draft (work in progress) <draft-schmitt-two-way-authentication-for-iot-02>, IETF Internet Draft, Standards Track, CoRE, February 2014.

[99] C. Schmitt and B. Stiller. Two-way Authentication for IoT. Internet-Draft (work in progress) <draft-schmitt-ace-twowayauth-for-iot-00>, IETF Internet Draft, Standards Track, ACE, June 2014.

[100] C. Schmitt and B. Stiller. Two-way Authentication for IoT. Internet-Draft (work in progress) <draft-schmitt-ace-twowayauth-for-iot-01>, IETF Internet Draft, Standards Track, ACE, dec 2014.

[101] C. Schmitt and B. Stiller. Two-way Authentication for IoT. Internet-Draft (work in progress) <draft-schmitt-ace-twowayauth-for-iot-02>, IETF Internet Draft, Standards Track, ACE, June 2015.

[102] D. Kutscher, S. Eum, K. Pentikousis, I. Psaras, D. Corujo, D. Saucez, T. Schmidt, and M. Waehlisch. ICN Research Challenges. Internet-Draft <draft-kutscher-icnrg-challenges-02>, NEC, NICT, EICT, UCL, Universidade de Aveiro, INRIA, HAW HAmburg, FU Berlin, February 2014.

[103] J. Seedorf, M. Arumaithurai, A. Tagami, K. Ramakrishnan, and N. Blefari Melazzi. Using ICN in disaster scenarios. Internet-Draft <draft-seedorf-icn-disaster-03>, NEC, University of Goettingen, KDDI R&D Labs, Unviersity of California, University Tor Vergata, March 2015.

[104] M. Waldburger and T. Kurakova. How ITU can help develop future networks. *ITU News Magazine*, 2013(1):37–41, Jan. 2013.

[105] C. Kalogiros, C. Courcoubetis, G. D. Stamoulis, M. Boniface, E. T. Meyer, M. Waldburger, D. Field, and B. Stiller. An Approach to Investigating Socio-economic Tussles Arising from Building the Future Internet. In John Domingue et al., editor, *The Future Internet*, volume 6656 of *Lecture Notes in Computer Science (LNCS)*, 2011.

[106] ITU-T (contributors: M. Waldburger, P. Poullie, C. Schmitt, and B. Stiller). Y.3013 : Socio-economic Assessment of Future Networks by Tussle Analysis. Recommendation Y.3013, International Telecommunication Union, Geneva, August 2014.