1.1.1 WP 8: Security, Privacy, Trust

Once the deadline for contributions is long passed this document was ported to the draft version of the 3rd Yearly report that will be kept in word format for now on.

The snapshot was taken on March, 26 and this document is closed for edition now.

If you need a copy the current 3rd Report or need to ask for changes, please contact Telefónica adding these 3 people to the loop:

- miguel.carrillopacheco@telefonica.com
- javier.depedrosanchez@telefonica.com
- santiago.martinezgarcia@telefonica.com

1. Progress towards objectives and details for each task

WP Objectives:

The main goal of this WP8 is to develop and provide a security ecosystem which comprises a set of core as well as optional generic enablers for creation, delivery, and usage of security solutions and services for the Future Internet. Overall WP8 aims at delivering operational and actionable security enablers to other Chapters and Use Case Projects and thus throughout the whole FI-PPP programme.

The main objectives of this Work Package are:

· Design and delivery of an advanced security monitoring system that covers the whole spectrum from acquisition of events up to display, going through analysis but also going beyond thanks to an assisted decision support in case of cyber attacks. This is mainly the scope of Task 8.1 “Security Monitoring”.

· Design and delivery of Core Generic Enabler components that will provide baseline identity and access management as well as privacy and trust. This is the scope of Task 8.2 “General Security Enablers”.

· Dynamic invocation and composition of security services to answer related security needs while dealing with constraints which may apply (e.g. regulatory). This component will result from work performed in Task 8.3 “Context-based security and compliance”.

· Optional Generic Security Services supporting description and provisioning of such services and their instantiation to address current and future requests from Usage Areas. This work will be performed in Task 8.4 “Optional Generic Security Services”.

WP Tasks and Interrelations:

WP8 is led by Thales (TS) and consists of four tasks: Task 8.1 “Security Monitoring” led by Thales (TS); Task 8.2 “General Security Enablers” led by NSN; Task 8.3 “Context-based security and compliance” led by ATOS; Task 8.4 “Optional Generic Security Services” led by SAP.

Security in scope of WP8 is a cross-cutting concern for other WPs: WP3- Application and Service Ecosystem, WP4- Cloud Hosting, WP5-IoT Services Enablement, WP7- Interface to Network and Devices, WP9-Development Community and Tools and WP-13-Advanced Middleware and Web based User Interfaces). As such WP8 interacts with them on the basis of its GEs Security offering.

Overall WP approach

The approach in WP8 is to align each of the tasks on the shared milestones, follow their development on a regular basis (taking necessary steps when appropriate) and let the task leaders organize the work at team level to deliver. This while controlling and assisting at WP8 level. Also important in the WP8 approach is to share information. Especially information provided at consortium level through Technical Coordination and it is important to keep WP8 aligned to other Technical WPs & WP2 but also other WPs (WP9, WP10, WP11, WP12). Last but not least the approach in WP8 is also to team and cross-fertilize at WP, Task and GE level with other WPs and/or Use Case Projects.

Main Progress in the period:

The main progress made during this period in the WP are:

M25-M30:

- Delivery of the Security GEs as per Technical Roadmap for Release 2 (12 GEs delivered!)
- Deployment of the Security GEs V2 on FI-WARE Testbed (support provided to the testbed team)
- Advertisement of the GEs V2 on FI-WARE Catalog
- Improved version of Security Chapter wiki for GEs V2,
- Training (webinars) and coaching on Security GEs V2
- Improved version of Security Chapter Backlog
- Further collaboration with Use Case Projects Phase II (e.g.FI-CONTENT 2, FI-SPACE and FI-STAR) through Security GEs V2 released.
- Further collaboration and support to other WPs (e.g. Chapter’s contributions).

M31->End (i.e. M36 for NSN, SAP, IBM, DT & INRIA who decided to close their work on M36 and M44 for Thales, Atos and FT who decided to continue the work on activities as per project extension)

- Delivery of Chapter Contribution to Technical Roadmap for R3 (D2.4.3)
- Delivery of Security GEs Open Specifications and Open APIs for R3
- Delivery of Security GEs for R3 (10 GEs delivered!) including software release, manuals and unit testing plan
- Deployment of the Security GEs V3 on FI-WARE Testbed (support provided to the testbed team)
- Deployment of the Security GEs V3 whenever applicable on FI-LAB
- Advertisement of the GEs V3 on FI-WARE Catalog
- Improved version of Security Chapter wiki for GEs V3,
- Improved version of the GEs as a whole through a number of cross-check/cross-review of the manuals and software. Overall a number of activities were conducted on the continued GEs ranging from development (with focus on open source) to packaging.
- Training and coaching on Security GEs V3
- Further improvement of Security Chapter Backlog
- Further collaboration with Use Case Projects on Security GEs R3. Finalization of work engaged with Phase II Projects and engagement with Phase III Projects (so called accelerator projects).
- Further collaboration and support to other WPs (e.g. Chapter's contributions).

WP8 has delivered as planned this while coping with (also adapting to) the changes introduced through Coordination Team. Overall, the milestones for the 3rd year have been met despite some delays.

1.1.1.1 *Task 8.1: Security Monitoring*

Task Objectives:

The objective of this task 8.1 is to deliver a security monitoring solution according to the Future Internet requirements identified, with the following functionalities: security events correlation, risk analysis, visualization and probably most importantly a comprehensive decision support system that helps in the selection of adequate countermeasures.

Task Activities during the period:

The breakdown of the contribution, results, deviation and proposed corrective action of each partner in this task 8.1 are:

- **05-THA:**

Contribution and results:

TS :

- Overall coordination of the Task 8.1 and Security Monitoring

GE development.

- Delivery of Security Monitoring GE V2 as per Technical Roadmap for R2 (i.e. delivery of SecMon GE V2 SW + manuals, also update of the wikis). Further enhancements of MulVal Attack Paths, Scored Attack paths
- Preparation and delivery webinars were the Security Monitoring GE functionalities were presented also shown in action through live demos.
- Update of Security Monitoring GE entry FI-WARE Catalogue with features. Support and maintenance of the VMs where Thales features were installed (i.e. MulVAL Attack Web Application Paths, Scored Attack Paths, Web Application Remediation).
- Upload of content on Wikis & Forge
- Update of Architecture of the Security Monitoring GE for R3. Security Monitoring GE service suite.
- Security Monitoring GE services namely Attack Path Computation & Attack Paths Scoring have been further developed (new features as per R3) also improved from a usability perspective.
- Creation and management of Task force between Security and Cloud aiming to get installed and deployed SecMon GE at platform/instance level (Testbed).
- Support to the integration of features developed by other partners when ready (i.e.SIEM/ATOS, Visualization/TRT-UK, …)
- Continuous improvement of Security Chapter backlog management (one Backlog per GE and review organized helping in this process).
- Production of new/updated training and eLearning material for Security Monitoring GE V3
- Deployment of the Security Monitoring GE V3 on the FI-WARE Testbed (support provided to the Testbed team)
- Support provided to the team with regard to deployment of the Security GEs on FI-LAB (when applicable – e.g; not applicable to GE not delivered in SaaS mode)

TCS :

- Security Monitoring GE Remediation service has been further developed. Overall work has been focused on a system help supporting the decision maker in his/her selection of countermeasures when an attack is detected (focus is here on mitigation of cyber-attacks and reduction of the risk level). It has been delivered in release 2.3 and deployed on the FIWARE Testbed V2 and further developed (especially from a

usability perspective) in V3. It has finally been deployed on Testbed V3 as one of the service of Seurity Monitoring GE.

· Production of training (eLearning) material for Security Monitoring GE remediation service

TRT-UK:

· Visualisation support for SIEM feature of Security Monitoring GE added to previous visualisations for attack graphs and scored attack paths and made available in Release 2.3.

· Visualisation support was added for IDMEF and event timelines in Release 3.

· Supporting FI-LAB documentation (Installation & Admin Guide, Unit Tests and User & Programming Manual) produced and approved. Contributed to the FI-WARE Security Monitoring Catalogue entry.

· e-Learning material produced. Contribution on Digital Forensics for Evidence created for FI-WARE State of the Art Analysis – Emerging Technologies deliverable

Deviation and proposed corrective action:

Delivery of Botnet Tracking feature from Orange arrived very late and was rejected since incomplete also not conformant to the set quidelines. Decision was taken not to wait any longer and deliver R3 without that feature. Also to leave a chance to Orange to deliver it afterwards as add-ons. Unfortunately this didn't happen. See below justification provided by Orange.

- **07-FT:**

Contribution and results:

o Development of Botnet Tracking feature for R3. Worked has focused on trying to make adaptations of Botnet tracking asset to deliver the functionalities planned in R3 (focus on R3.3). Unfortunately and despite the adaptations made by Orange the results in terms of performance were poor and against real exploitation of the results as initially planned As such decision was taken by Orange not to deliver the Botnet Tracking in R3.

Deviation and proposed corrective action:

o In view of the poor performance of Botnet Tracking system despite adaptations put in place, decision was taken (by Orange) not to submit in R3 since not leading to exploitation of results as initially expected.

- **14-ATOS:**

Contribution and results:

o Finalization of the implementation, testing and bug fixes of the Service Level SIEM component of the Security Monitoring GE

- Support to the integration of the Visualization/TRT-UK tool and MulVALAttackPath/Thales tool to the Service Level SIEM.
- Finalization of the documentation about the usage, installation and testing plan of the ServiceLevelSIEM component: User and Programmers Guide, Installation and Administration Guide, Unit Testing Plan and Report.
- Updated the Open Specs and the Open APIs. Updated content on Wikis & Forge. Contribution to the FI-WARE Security Monitoring Catalogue entry.
- Deployment of the Service Level SIEM component on the FIWARE Testbed
- Creation of recipes for the automatic installation of the ServiceLevelSIEM
- Creation of training material and eLearning platform courses about the ServiceLevelSIEM
- Satisfied all the requirements to include the ATOS implementation of the Service Level SIEM to FILAB.

Deviation and proposed corrective action:

Neither deviation nor proposed corrective action of this partner in this task.

- **22-INRIA:**

Contribution and results:

- Update and consolidation of vulnerability assessment and IoT fuzzer work and their respective documentation (guides, description and testing report).

Deviation and proposed corrective action:

- None

1.1.1.2 *Task 8.2: Generic Security Enablers*

Task Objectives:

The main objective of this task 8.2 is to work on Identity and Access Management (IAM), Privacy and Trust Framework meeting the requirements of FI-WARE. As such focus is here on covering the requirements shared by the Use Case projects related to IAM, Privacy and Trust.

Task Activities during the period:

The breakdown of the contribution, results, deviation and proposed corrective action of each partner in this task 8.2 are:

- 02-SAP:
  - The third release of the Data Handling GE was delivered on time (documentation and software). Knowing that SAP is leaving the project M36 everything was achieved with end of March 2014. A performance study of the Data Handling GE was presented as a research paper at the CLOSER

conference in April.

o The third release of the Data Handling incorporated a new Encryption feature. This encryption feature offers the possibility to Encrypt/Decrypt data using the Identity/Attribute Based encryption schema. This modern encryption mechanisms has the advantage to get rid of the limitations of the traditional PKI mechanisms by providing a semantic meaning (identity) to the public key.

o In parallel SAP team worked on the integration of the Data Handling GE into a common Demo together with NSN and IBM. This common Demo shows how easy we can combine and compose security GE in order to achieve innovative security use cases. SAP was in charge of implementing a privacy aware file store web application protected by the Data Handling GE, connected to the NSN Identity management system and the Anonymous credential service offered by the Privacy GE from IBM. The goal is to proof that we can securely share data with different users and preserving their anonymity at the same time.

o The Open Source release of the Data Handling GE also called PPL Engine is officially adopted by two FP7 EU projects that are A4Cloud and Co Co Cloud.

- **04-IBM-CH:**

Contribution and results:

o Delivered an implementation of the Privacy GE as software library that can perform credential issuance, token generation, and token verification.

o Delivered the Open Specifications (including RESTful API) of the Privacy GE.

o Delivered the Installation and Administration manual of the Privacy GE.

o Delivered the User and Programmer manual of the Privacy GE.

o Delivered the Unit Testing Plan of the Privacy GE.

o Installed our Privacy GE software library in the FI-WARE Testbed, so as to show that all unit tests are running successfully.

o Extended the Identity Selection GUI widgets such that they can handle basic issuance scenarios.

o Extended the Identity Selection GUI widgets such that they can handle advanced issuance scenarios.

o Created and FI-Ware Catalog entry for our Privacy GE.

o Cleanup, restructuring, and regular update of tickets in Backlog Tracker in FI-Ware Forge to report on FI-Ware tasks.

o Started requirement analysis and initial design of technical architecture for common demo that involves the features of the Privacy GE

(IBM), the Identity Management GE (NSN), and the Data Handling GE (SAP).

o Attended multiple standardization events to advance standardization of privacy-enhancing technologies for international driver's licenses. A detailed list of attended events and contributions is reported separately in the standardization deliverable D11.4.

o Prepared and held a Privacy GE Webinar on Privacy-Preserving Authentication on Thursday, July 18, 2013 at 04:00 PM CEST.

o Compiled, edited, and uploaded a recording of the Webinar to the FI-WARE Forge.

o Specified the RESTful web service API for credential revocation to add support for the revocation of issued attribute-based credentials via RESTful web service methods.

o Specified the RESTful web service API for token inspection to add support for the inspection of tokens via RESTful web service methods.

o Updated the Installation and Administration Guide to be ready for the final release (R3.3).

o Extended the Unit Testing Plan and Report with additional test cases to be ready for the final release (R3.3)

o Updated the Open Specs and the Open APIs to be ready for the final release (R3.3).

o Delivered the Privacy GE as software for the final release 3.3 in the FI-WARE forge.

o Regular update of tickets in Backlog Tracker in FI-Ware Forge to report on FI-Ware tasks.

o Reworking the tickets in the Backlog Tracker in FI-Ware Forge and their associated Wiki pages to achive 0 issues in the 1900 tests in Manuel's tracker review

o Organization and coordination of the security chapter's Open Specs Release 3 (R3) peer review of the Apps chapter's Generic Enablers.

o Performed the peer review of the Open Specs R3 for the App chapter's Marketplace GE, Mediator GE, and Revenue Settlement and Sharing System GE.

o Worked in the reviews received for our Privacy GE Architecture, Open Specs, and Open APIs.

o Updated the technical roadmap for the Privacy GE.

Standardization:

o Continued to drive the standardization of privacy technologies in electronic driver licenses.

o Continued to drive the established privacy task force to advance the standardization of identity documents.

o Created (serveral versions of) a requirements document based

on the use cases for the future driving license, with a focus on privacy.

o Created a comprehensive use case document based on use cases for the future driving license, with a focus on privacy.

o Progressed the requirements document, discussed the related concepts, created awareness within and outside of the WG 10 on driving licenses, as well as worked on the related technologies.

o Created awareness for the privacy requirements within and outside of the WG 10 on driving licenses.

o Setup of and contributions to a Joint Study Period related to a generic standard on Privacy-ABCs in SC27 Working Groups 5 and 2.

o Made contributions related to PrivacyABCs to NP ISO/IEC 19268 called "ICC protocols and services ensuring privacy".

Standardization Event Participation:

o Attended the ISO/IEC JTC 1/SC 17 plenary meeting to present our initiative and discuss relations to a new privacy effort of ISO/IEC JTC 1/SC 17/WG 4 on chip cards. [Singapore, 10/2013].

o Attended meeting with the Swiss mirror group of ISO/IEC JTC1 SC 27 to trigger discussions related to a Joint Study Period on Privacy-ABCs in WG5 and WG2 of ISO/IEC JTC1 SC 27. [Winterthur, 01/2014].

o Proposed to standardize privacy-preserving attribute based credential technology for chip cards in the new Working Group (WG) 4 effort of Subcommittee (SC) 17. [London, 01/2014].

o Attended the ISO/IEC 18013, ISO/IEC SC 17/WG 10/TF 13 meeting to progress use case and requirements documents related to privacy in the future electronic driving license. [Costa Rica, 02/2014].

o Proposed consideration of privacy-preserving attribute credentials for identity management to ISO/IEC SC 27 working groups. [Hong Kong, 04/2014].

Dissemination:

o Michael Osborne gave a talk on "Privacy and the future driving license" at the Connect-ID conference in Washington, DC, USA on March 19, 2014.

o Michael Osborne gave a talk on "Privacy and Data Protection in FI-WARE" at the 1st European Conference on Future Internet (ECFI) in Brussels, Belgium on April 2, 2014.

o Dieter Sommer gave a talk on "Privacy-enhanced Authentication" at an ISO/IEC Meeting in London, UK on January 30, 2014.

o Dieter Sommer gave a talk on "Privacy-enhanced Attribute Credentials" at an ISO/IEC Meeting in Hong Kong on April 8, 2014.

Deviation and proposed corrective action:

No deviation and thus no corrective action.

- **05-THALES:**

Contribution and results:

TS:

- Release 2.3.3 (may 2013): implementation of new features: PDP attribute finder for DT IdM GE, XACML RBAC Profile
- Collaboration with UPM to demo Access Control (AC) GE
- Collaboration/integration on FISPACE Use case
- Fixing webinars/presentations/courses for the FIWARE e-learning website
- Release R3 of AC GE:
  - Update manuals: Install guide, user guide, Unit test plan report
  - Update specs: OpenSpec, API spec, etc.
  - Update catalogue entry
  - Preparation/process to move image for R3 to FILAB (testbed cockpit, etc.)
  - Release 3.1 -> Implementation of new feature: PEP extension for getting attributes from IdM GE API
  - Release 3.2 -> Implementation of new features: PDP attribute finder for NSN IdM GE, XACML Multiple Resource Profile…
  - Release 3.3 -> Implementation of new feature: Accounting (integration with Security Monitoring)
- Support on the global instance of Access Control GE
  - Providing access to people willing to test it,
  - Version upgrades
  - Reboots after testbed maintenances
- Fixing backlog dashboards from Telefonica (fixing trackers, links between features/stories, the wiki links, etc.)
- FIWARE bootcamp :
  - Preparing presentation for all bootcamps with UPM on How to add access control to your application (september-october 2014)
  - Delivering the presentation to Berlin bootcamp meeting in October 2014

Deviation and proposed corrective action:

- Neither deviation nor proposed corrective action of this partner in this task.

- **11-DT:**

Contribution and results:

- Enhancement of the REST API through new features.
- finishing the API documentation with all features of the GCP API
- finishing the Java library, which supports Java programmers regarding user management
- first features to use the GCP in new knowledge domains.
- full documentation with programming examples on how GCP can be integrated into a Web project
- support of project partners
- since Q1 the product “Internet Business Suite”, which is based on GCP, is on the marked

Deviation and proposed corrective action:

- none.

- **33-NSNG1:**

Contribution and results:

- The Identity Management Generic Enabler was improved in its back-end functionalities. There was no impact on the existing API.
- According to the feedback and requirements coming from the Use Case projects enhancements to the GE have been provided. Here mainly for FI-Space and FI-Content2.
- Implementation of the System for Cross-domain Identity Management (SCIM) in the DigitalSelf GEi in order to communicate with the Access Control GE.
- Implementation of a tool including a GUI for managing employees and roles for organisations within the DigitalSelf GEi.
- Making available the source code and description of a small example how to setup an own service which uses the OAuth capabilities of the DigitalSelf.
- Provisioning of example source code how to use OpenIDConnect together with the DigitalSelf GEi.
- Development and test of extended privacy functionality (verification service) of the One-IDM and common demo with Privacy GE (IBM) and Access Control GEi (SAP). Common demo and related description is available.
- Development and test of One-IDM extensions for a common demo with Privacy GE, concerning issuance and use of privacy-enhancing credentials.
- Design and implementation of a tool including a GUI for users to manage their registration in DigitalSelf by their own.
- DigitalSelf requires web application operators and their applications to be registered properly. A web based tool was implemented to allow them to do these steps in a convenient manner.

- Preparation and provision of e-learning material
- Maintenance of backlog and WIKI content.

- Joint demo between IdM GE (NSN), Privacy GE (IBM) and Data Handling GE (SAP). Successful presentation of this joint demo at the Trust in Digital Life conference in Vienna.

Deviation and proposed corrective action:

- Neither deviation nor proposed corrective action of this partner in this task.

1.1.1.3 *Task 8.3: Context-based security and compliance*

Task Objectives:

The main objective of this task 8.3 is to support the dynamic invocation and composition of security services by providing the following key contributions:

· An extended service description language taking security requirements and properties into consideration (USDL-SEC)

· A set of required runtime components (Registry, Discovery, Brokerage, Composition, Invocation, Monitoring)

· A set of required context connectors to compliance frameworks

· Framework for binding of requirements and constraints

· Framework for observable deployment of optional security enablers

· Framework for context-based reconfiguration of deployed optional security enablers

This task is structured into three main lines of work:

· Design and describe abstract security and compliance solutions (in terms of requirements, security properties and service description);

· Provide the framework for selection and deployment of reconfigurable solutions (this would include the engine, the brokering service, repository/inventory, amongst others); and finally,

· Specification of monitoring aspects of the solution (in terms of context-based rules to monitor the correct execution of the deployed optional security enabler, contractual terms, compliance-based metrics, etc.).

Task Activities during the period:

The breakdown of the **contribution, results, deviation and proposed corrective action** of each partner in this task 8.3 are:

- **02-SAP:**

  Contribution and results:

  - SAP continued the development of USDL-SEC in cooperation with USDL development team. In particular, the work on USDL Editor for the USDL-SEC part continued, for bug fixing and for design of new upcoming features that could be included in future releases.
  - For steering the evolution of USDL-SEC, contacts have been developed with the FP7 OPTET project that is planning to reuse USDL and USDL-SEC for describing the offerings of a software marketplace concept using Linked Data principles.

- **14-ATOS:**

  Contribution and results:

  - Finalization of implementation, testing and bug fixes of the PRRS implementation of the Context-based Security&Compliance GE
  - Finalization of the documentation about the usage, installation and testing plan of the Context-based Security&Compliance GE: User and Programmers Guide, Installation and Administration Guide, Unit Testing Plan and Report.
  - Updated the Open Specs and the Open APIs. Updated content on Wikis & Forge. Contribution to the FIWARE Context-based Security & Compliance GE Catalogue entry.
  - Deployment of the Context-based Security & Compliance GE on the FI-WARE Testbed
  - Creation of recipes for the automatic installation of the Context-based Security&Compliance GE
  - Creation of training material and eLearning platform courses about the Context-based Security&Compliance GE
  - Satisfied all the requirements to include the ATOS implementation of the Context-based Security & Compliance GE to FILAB.

  Deviation and proposed corrective action:

Neither deviation nor proposed corrective action of this partner in this task

1.1.1.4 *Task 8.4: Optional Generic Security Services*

This task is concerned with the description and provisioning of optional generic security services. Such optional security services are potentially applicable across a number of usage areas, however, unlike generic enablers, it is not expected that all usage areas will make use of any particular one. As such, the objective of task 8.4 will be to support the instantiation of optional security services that have the potential to contribute to generic enablers in future requests from usage areas.

In summary, the key objectives of this task are:

- To provide descriptions and specifications of optional generic security services

· To describe mechanisms for the deployment of optional generic security services
· To provide tools and techniques for the deployment of new security technologies as optional generic security services as these become available.

The breakdown of the **contribution, results, deviation and proposed corrective action** of each partner in this task 8.4 are:

- **02-SAP:**

Contribution and results:

- SAP team in T8.4 has been working on DB Anonymizer (DBA), releasing a new dataset anonymization functionality as requested by the FINESCE UC project. A paper to the Cyber Security Forum 2014 on FINESCE PoC was developped. Contacts with non-FI-PPP have also to be reported: with Spanish and Brasilian companies interested in evaluating DBA. Specific feedback and assistance was provided per email, and contacts are still ongoing.
- Open Specification and API, reference implementation and software documentation were released in due time, testbed and fi-lab deployment as well. Source code for Release 3.3 was released and Catalogue details were updated accordingly.
- New feature for DBA released and documented
- Open Specification, API, reference implementation and all documentation released
- Testbed, FI-LAB and Catalogue information updated and released.

Deviation and proposed corrective action:
Neither deviation nor proposed corrective action of this partner in this task.

- **05-THALES:**

Contribution and results:

- [TRTUK] Multi-Broker version of Content Based Security GE developed and integrated with the Access Control GE. Made available in Release 2.3. Integration of CBS OGE with Identity Management (GCP) GE released in Release 3.2. Supporting FI-LAB documentation (Installation & Admin Guide, Unit Tests and User & Programming Manual) produced and approved. Recipe produced to aid installation on FI-LAB testbed. FI-WARE Catalogue entry created. Webinars held to introduce Use Case projects to the GE. e-Learning material produced.
- [TCS] Delivery of Secure Storage Service Optional GE as software and not service. Update of all the manuals accordingly and Wiki.

Deviation and proposed corrective action:

- SSS GE [TCS] initially planned for R1 and then R2 was finally delivered the way expected at R3. Rejected since initially delivered as a Service it took more time than expected to get it delivered as software product.

- **22-INRIA:**

Contribution and results:

- Update and consolidation of Android flow monitoring work, Malware detection Service and their dedicated documentation (guides,

description and testing report).
Deviation and proposed corrective action:
o None.

2. Significant results

<List here the biggest achievements from the WP during this period>

- All milestones were met.
- All deliverables due were delivered
- No major deviation
- 10 Security GEs delivered in R3 where made available on testbed V3 (in coordination with WP10) and advertised on FI-WARE Catalog
- Additional cross-chapter collaboration through creation of dedicated task forces (e.g. task on IDM between Sec & Cloud, task force on SecMon GE deployment between Sec/Cloud and Testbed)
- New demos of Security GEs have been developed/shown (i.e. joint demo of IdM GE/NSN, DH GE/SAP and Privacy GE/IBM but also the demo of Security Monitoring deployed on a FI-WARE instance).
- Further training and coaching on FI-PPP Projects team
- Strengthening of the collaboration with XIFI Project and projects willing to make use or contribute to FI-WARE (e.g. OPTET, …)
- Active dissemination of results within and outside FI-PPP (e.g. AAL Community, EIT ICT Labs through FI-PPP Liaison projects, TDW, …)
- Numerous actions conducted on Standardization, Market Analysis, Exploitation, Communication etc. , leading to a number of inputs being contributed to other WPs in charge of those aspects (namely WP11 and WP12).

3. Deviations from Annex I and impact on other tasks, available resources and planning (if applicable)

<Add here any deviations in terms of expected achievements, planned scope, or schedule and state whether these deviations have affected other tasks, the overall project planning, or the planned use of resources>

The main deviation in WP8 for the period was:

- The Botnet Tracking system feature of ORANGE which couldn't be integrated to Security Monitoring since delivered too late, incomplete and not conformant to the guidelines. Overall this caused Security Monitoring GE to be delivered for R3 without that feature.

Nevertheless it as limited impact since Botnet Tracking system feature was an add-on feature and not part of the core features of Security Monitoring GE.

4. Reasoning for failing to achieve critical objectives and/or not being on schedule (if applicable)

All critical objectives were achieved while adapting to the changes introduced in the project.

5. Use of resources

Note: The following info below is expected to be included as part of section 2.3.8 Use of resources for Project Management (WP1) of the periodic report by Javier de Pedro (TID). Figures below are being updated by Javier with the info corresponding to current period.

General valuation of the effort and status of the WP have to be updated by the WPL below (XXX).

Planning of effort in WP8:

This WP has a weighted rate by month of the linear distribution of total effort per partner as follows:

M1-M9: 50 % of its linear distribution in 36 months

M10-M33: 100 % of its linear distribution in 36 months

M34-M36: 50 % of its linear distribution in 36 months

M37-M44: Extension of the project: Each partner has provided their own planning.

As result of the amendments, planning has could be changed due to its recalculation based in the new effort per partner in the DoW.

Follow-up of effort in WP8:

The following table depicts the planned resources vs. real resources (in PMs) for WP8:

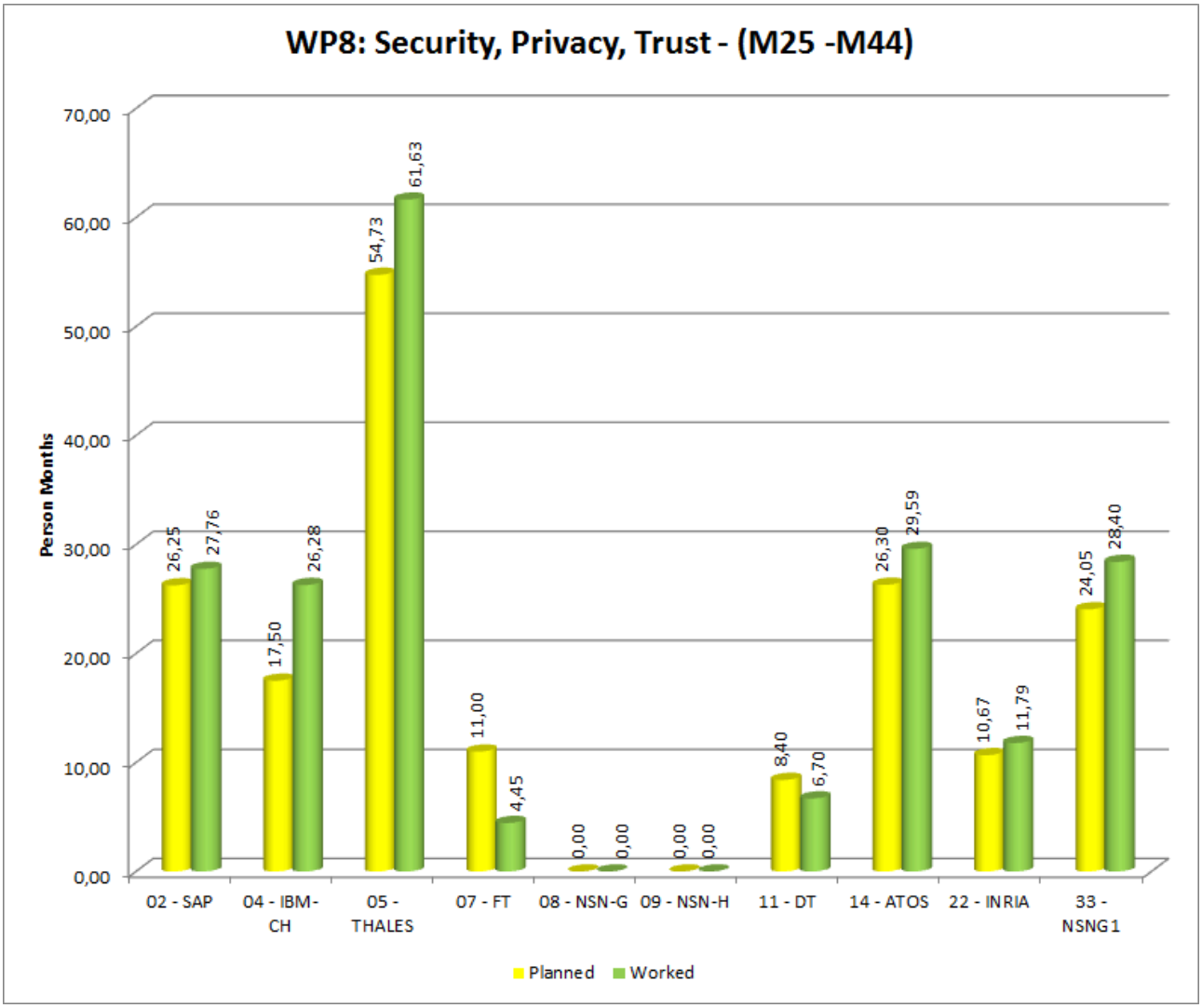
WP8	Y1	Y2	Y3	Y1	Y1+Y2	Y1+Y2+Y3
DoW: 490	**M1-M12**	**M13-M24**	**M25-M44**	**M1-M12**	**M1-M24**	**M1-M44**
Planned	125	194	179	125	319	498

Worked	109	187	197	109	296	493

Note: Worked cell contains the accumulative declared effort.

In general, the consumption of resources in this WP8 is overall close to what was initially planned.

The following image depicts the planned resources vs. real resources (in PMs) during period M25-M44 in WP8 by partner:



Explanations of significant deviations (±10%) are explained in the “Explanation of the use of the resources -> “Effort per partner” section.

Note: The above reference (explanations) is currently managed by the consortium in the following shared document:

https://docs.google.com/document/d/1NoS4-7DjKbAlPc98c3lHCMgHkoNk3G7VSiNTDMkoQ_c/edit

In summary, the status of this WP8 is overall as planned with some partners consuming a bit more compensating by partners consuming a bit less. This with major overconsumption of resources from IBM-CH and major under consumption of resources from Orange. This for the reasons exposed below:

ATOS: All the process followed to fulfil and satisfy the requirement to go to FILAB took more time than planned, because ATOS had some difficulties with the recipes. In particular for the Service Level SIEM due to the nature of its dependencies, which were not compatible with the Operating Systems available through the FIWARE Cloud Portal. Thus the entire process was delayed and an alternative solution had to be found with the migration to one of the available Operating System from the source code of the open source software OSSIM, required by the Service Leve SIEM. This migration was not planned initially because at that moment there were no restrictions defined. This task was very time consuming.

SAP consumed effort in WP8 for the reference period was slightly bigger than expected, essentially for the reason that a number of resources have integrated the team in order to carry out the development, testing and documentation activities, but their profile was of a different seniority than what expected at the time of writing the DOW. Therefore, considering also the effort required to cope with the high quality of internal FI-WARE processes for documenting, testing and deploying our GEs and a certain physiological turnover in the mentioned additional resources, the consumed effort slightly increased with respect to the forecast, despite our initiatives to keep the two values aligned.

IBM-CH has higher effort compared to what was planned for the reporting period in order to deliver the total work load that was committed to in the description of work, and also to utilize the total available funding from the European Commission. Also, the increased work effort was necessary to finalize the common demonstrator that was requested by our work package leader to show successfull integration between multiple Generic Enables of the Security chapter.

Orange has far less effort than expected since Botnet Tracking system asset couldn't be delivered as expected due to poor performance and as a consequence a number of activities (e.g. integration or documentation) didn't occur or at some point were stopped.

6. Corrective actions proposed (if applicable)

The main proposed corrective actions in WP8 were:

.

- NSN ending the project as stated in the DoW and the legal documents by end of M36. Thales (TS) volunteered to continue until M44 and took over T8.2 lead.
- SAP ending the project as stated in the DoW and the legal documents by end of M36. Thales (TRT-UK) volunteered to continue until M44 and took over T8.2 lead.
- Deliver R3 deliverables without input from Orange (since rejected as incomplete nor

conformant to the guidelines) This was done in concertation and with agreement of Project coordinator that added a note at delivery time.