EUROPEAN COMMISSION

Community Research

SEVENTH FRAMEWORK PROGRAMME

Specific Targeted REsearch Project

PRISM

PRISM Project Presentation

Project acronym: PRISM
Project full title: Privacy-Aware secure Monitoring
Contract No.: 215350
Project Document Number: IST-2007-215350-WP1.1-D1.1-R1
Project Document Date: 31/03/2008
Workpackage Contributing to the Project Document: WP1.1
Deliverable Type and Security: Public
Author(s): Sathya Rao,Telscom

Abstract:

This deliverable will provide the information about the project objectives, project activities, expected results and dissemination plan. The information provided is targeted to persons at large interested in privacy-aware secure monitoring activities applied to future Internet. The document also facilitates information dissemination to general public on the European Commission funded project activities.

Keyword list: PRISM, IST-2007-215350, Project presentation

History

Version	Date	Description, Author(s), Reviser(s)
0.1	03/03/2008	Document creation, Sathya Rao
0.2	05/03/2008	Revision, Sathya Rao
1.0	21/03/2008	Final editing, Sathya Rao

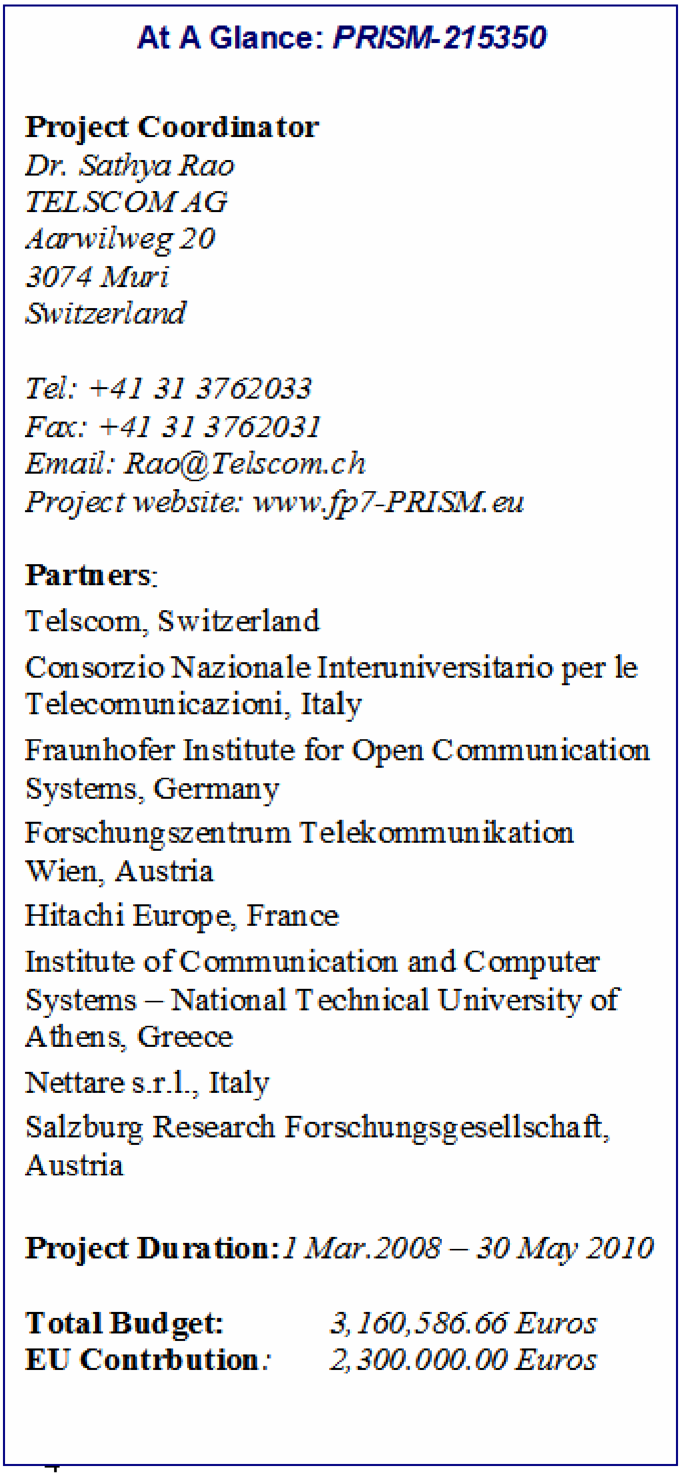
Table of Contents

1. Project Summary

Traffic monitoring has always been recognised as a feature of paramount importance for all sorts of networks, from very small access networks to world-wide operator domains. On one side, traffic monitoring is a fundamental method to acquire essential information for the operation and management of real networks and for Service Level Agreement validation. On the other side, traffic monitoring is needed to guarantee the security of the network infrastructure and its users. In fact, continuous traffic monitoring often feeds Intrusion / Anomaly Detection Systems (IDS/ADS) which trigger alarms and set up countermeasures in reaction to events such as network intrusions, denial-of-service attacks, worm infections and similar incidents. Network monitoring could also become a threat to users' privacy by keeping individual communications under surveillance.

To enhance the level of data protection in the community, the Commission has identified a set of actions aimed at promoting the widespread development of Privacy Enhancement Technologies (PET), also with the aim to foster consumers’ trust in on-line services. The PRISM project will demonstrate the operation of a traffic monitoring architecture whose technical design guarantees privacy preservation. Our challenge is to break, with specific reference to network monitoring, the commonly accepted dichotomy between privacy and utility that underlies most of the applications and services devised to operate on personal or user-related data. The goal of our project is to investigate how it is possible to preserve the customers’ privacy, by avoiding disclosure of raw captured data even inside the controller domain itself, while preserving the possibility of running monitoring applications, including the possibility to detect and react to attacks and trace back abuses (thus improving public security). The PRISM technology aims at being fully legally compliant with data privacy protection regulation on one side, and to the security legislation on the other side.

The PRISM project proposes to develop a two-tier privacy-compliant integrated monitoring architecture.



At A Glance: *PRISM-215350*

Project Coordinator
Dr. Sathya Rao
TELSCOM AG
Aarwilweg 20
3074 Muri
Switzerland

Tel: +41 31 3762033
Fax: +41 31 3762031
Email: Rao@Telscom.ch
Project website: www.fp7-PRISM.eu

Partners:

Telscom, Switzerland

Consorzio Nazionale Interuniversitario per le Telecomunicazioni, Italy

Fraunhofer Institute for Open Communication Systems, Germany

Forschungszentrum Telekommunikation Wien, Austria

Hitachi Europe, France

Institute of Communication and Computer Systems – National Technical University of Athens, Greece

Nettare s.r.l., Italy

Salzburg Research Forschungsgesellschaft, Austria

Project Duration: *1 Mar.2008 – 30 May 2010*

Total Budget:	*3,160,586.66 Euros*
EU Contrbution:	*2,300.000.00 Euros*

A first (front-end) tier of data protection mechanisms will be directly enforced at the traffic probe device, thereby guaranteeing that the data delivered to the controller will be already privacy-protected.

A second (back-end) tier will enforce access procedures to the collected data and will orchestrate the operation of reversing, when strictly needed, the data protection mechanisms set forth by the first tier. Furthermore, it will make available security features, such as the correct level of security on the management and storage platforms, as well as will support procedures devised to anonymise and export data traces to third party users and external monitoring applications.

Monitoring applications will be suitably adapted to operate on data protected traces and/or through the mediation of the back-end middleware, without losing in effectiveness and the ability to react and defend against mis-behaving users and attackers.

2. Main objectives:

PRISM aims at devising a privacy-preserving network monitoring system with guaranteed enforcement of data protection legislation. This will be accomplished by pursuing privacy-compliant technologies and solutions which are conveniently summarised in the following objectives.

- **Design of a two-tier monitoring architecture with data protection reversion bound to third-party cooperation.** The proposed architecture will devise three components. A **front-end** tier will enforce data protection primitives on the captured data prior to its delivery to the relevant data controller. A **back-end** tier running at the data controller site will safely store, manage and coordinate access to and processing of the collected data. A third entity referred to as **privacy-preserving controller** will cryptographically control the front-end data protection mechanisms to prevent unnecessary data disclosure within the controller domain itself.
- **Extension and promotion of standard-based data export protocols**. The project will design, develop, and demonstrate extended versions of the IETF IPFIX (IP Flow Information eXport) protocol and information model, capable of describing, handling and managing protected data, and ii) promote through IETF standardisation privacy-protective data exporting. The extended version of IPFIX will be employed in the considered architecture for both front-end to back-end communication as well as for data export from the back-end.
- **“Blind” intrusion detection.** The final objective is to adapt signature-based intrusion detection mechanisms to “blindly” operate over anonymised traces with encrypted payload.
- **Design of monitoring application friendly data protection mechanisms** – PRISM will design data protection mechanisms capable of preserving properties of the packet header information fields and of the events associated to the packet to be used by monitoring applications for their operation.
- **High performance front-end implementation** – An high performing front-end implementation based on special-purpose HW devices will be developed, to target accurate packet capture and related processing at link speed without loss. Leveraging hardware parallelism, the front-end will further support high performance / lightweight versions of the envisioned data protection algorithms and will integrate an IPFIX protocol stack version specifically redesigned and optimised for this purpose.

- **Secure and high-performing back-end implementation** – To increase its exploitability, the back-end will be designed to retain a secure and privacy-preserving operation even when deployed as a stand-alone component. It will be implemented as a distributed storage system to address both performance and security. Advanced database encryption technologies with multi-key decryption facilities will be employed.
- **Design of a privacy-aware back-end middleware** –Innovative privacy-centric role-based access control middleware tailored for network monitoring infra-structures will be designed. The middleware will incorporate a formal and machine-readable representation of policy rules that originate from a semantic description of the monitoring application operation and purpose, of the data types, of the entities and subjects involved, and of the privacy legislation provisions.
- **Regulatory compliancy** – The middleware policies will ensure that the processing of data gathered through monitoring will be carried out in line with the set of rules and limitations provided by data protection legislation. The ability to revert the front-end data protection mechanisms will ensure enforceability of legislation aimed at guaranteeing security.
- **Innovative approaches to privacy-respectful monitoring application design** – The project will address the challenge of out-sourcing monitoring applications without privacy concerns. The availability of customisable data processing functionalities embedded in the back-end allows an external monitoring application to use these internal processing primitives as intermediaries for accessing the data. This new approach will be tested by adapting selected monitoring applications.
- **Integrated trial** – The privacy-protective monitoring technologies developed in the project will be integrated and evaluated in a complete trial, involving all the system architecture components.

3. Work plan

The Goal of the PRISM project is to devise network monitoring technologies and architectures, which guarantee enforcement of data protection legislation. This will be accomplished through the specification, design, implementation and validation of a two-tiered network monitoring system The project is planned for the duration of 27 months. After each 6 months, a major project milestone has been set as control point, where decisions for the upcoming project phase will be made.

The overall work plan of PRISM is structured into 4 technical work-package groups, including a work-package group for project management and dissemination, standardisation and exploitation activities.

These WPGs are further subdivided into ten work-packages:

- **WPG 1** - Two WPs, namely, **WP1.1 project management** and **WP1.2 Dissemination and exploitation**, are dedicated to support the project as a whole, and maximise the effectiveness of its development, impact and exploitation of the project achievements on the standardisation bodies and on the scientific and technical community.
- **WPG 2** – It aims at supporting the specification and assessment activities dedicated to design the PRISM architecture and its components. Three workpackages are deinfed: **WP2.1 System requirements and Scenarios**, **WP2.2 System architecture specification** and **WP2.3 regulatory performance and security assessment**.

WP2.1 will produce system requirements by first analysing the regulatory framework and identifying usage scenarios.

WP2.2 tackles the challenging goal of precisely specifying the detailed architecture of each protocol and data model involved and of each system component and their interfaces. Moreover, it addresses the issue of how to map and properly integrate the data protection mechanisms and the adapted monitoring applications into the privacy-preserving monitoring infrastructure set forth.

WP2.3 is devised to assess both individual system components as well as the system operation as a whole in terms of capability to accomplish the performance and security requirements identified in WP2.1. It will assess the compliancy of the designed system with respect to applicable regulatory provisions, and verify the effectiveness of the designed system in integrating regulatory provisions into its technical operation.

- **WPG 3 –** It comprises two tightly intertwined WPs aimed at challenging the specific scientific and technical issues that privacy-preserving network monitoring raises. **WP3.1 data protection algorithm** is dedicated to investigate the most appropriate data protection mechanisms for monitoring application friendliness. **WP3.2 monitoring applications and their adaptation** is dedicated to challenge the re-design of monitoring applications and their deployment in the different involved domains (data controller, public community, third party out-sourcing) to comply with privacy-preservation requirements and to operate on protected data and/or through the mediation of the back-end privacy-preserving middleware.
- **WPG 4 –**The work package group 4 is to implement and validate the operation of the designed privacy-preserving network monitoring architecture and testing its characterizing data protection algorithms and adapted monitoring applications in the selected scenario. Three WPs are defined: **WP4.1 front-end tier implementation**, **WP4.2 back-end tier implementation** and **WP4.3 Integration and Trial**.

3.1 PRISM system architecture

As shown in Figure 1, the PRISM architecture involves the following four basic technical actors:

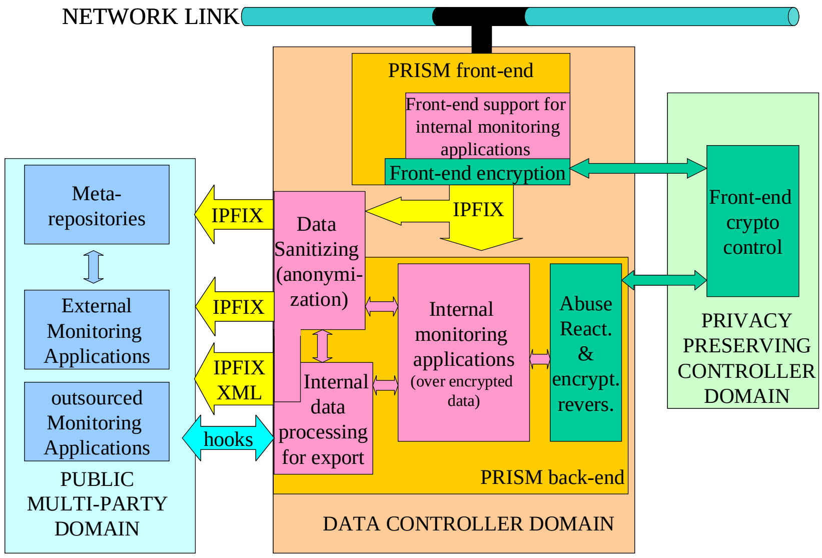

NETWORK LINK
PRISM front-end
Front-end support for internal monitoring applications
Front-end encryption
Meta-repositories
External Monitoring Applications
outsourced Monitoring Applications
PUBLIC MULTI-PARTY DOMAIN
IPFIX
IPFIX
IPFIX XML
hooks
IPFIX
Data Sanitizing (anonymi-zation)
Internal data processing for export
Internal monitoring applications (over encrypted data)
Abuse React. & encrypt. revers.
PRISM back-end
DATA CONTROLLER DOMAIN
Front-end crypto control
PRIVACY PRESERVING CONTROLLER DOMAIN

Figure 1: PRISM System architecture

- **PRISM Front-end –** This component is meant to be a “Black-Box” traffic probe, “cryptographically controlled” by an entity, in the figure referred to as third-party privacy-preserving controller, i.e. administratively different from the one that operates the back-end system. The PRISM front-end is devised to capture data on the network link(s), protect them according to suitably designed data protection mechanisms whose secrets are provided by the Privacy-Preserving Controller, and deliver them to the back-end system through standard-based data export protocols, IPFIX being the technology of choice.
- **Privacy-Preserving Controller –** This entity accomplishes the task of providing and maintaining the crypto secrets, which are used by the data protection mechanisms enforced on the front-end. It is very important to remark that such an entity is not meant, in general, to be able to access the actual captured data. In fact, as clearly highlighted in the figure, protected data are never directly conveyed to the privacy-preserving controller, but are collected in the PRISM back-end. Nevertheless, having it provided with the data protection secrets (or, in most generality, part of them), it will remain able to contribute to revert the data protection measures set forth on the data whenever this need will emerge.
- **PRISM back-end –** This part of the system, which coincides with the traditional data controller role, is in charge of collecting, storing and processing the front-end protected data traces. Monitoring applications running on the back-end will operate on encrypted traces, and when strictly necessary (e.g., when abuses and anomalies are detected and reactions are deemed necessary) and/or mandated by regulatory provisions (e.g., when inspection of retained data is deemed necessary by public authorities), it will interoperate with the privacy preserving controller to selectively (i.e., on the minimal subset of data necessary to perform the considered operation) revert the data protection mechanisms set forth at the front-end. Again, it is important to emphasise that the back-end will, in normal operation, not have access to the crypto secrets used for data protection on the front-end
- **Public Domain –** Finally, collected data traces and/or derived statistics will be further sanitised through robust anonymisation mechanisms. These will allow disclosure of data traces and/or related derived information to the public community, to meta-repositories, and to externally operated monitoring applications. Again, standard-based data export protocols and data representation languages will be exploited for such disclosure.

4. Project structure and work package relationship

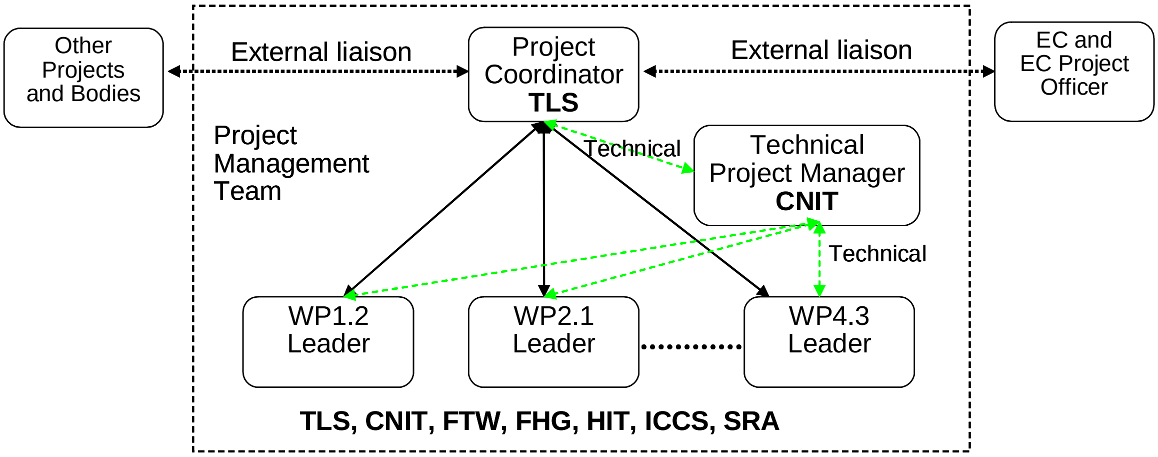
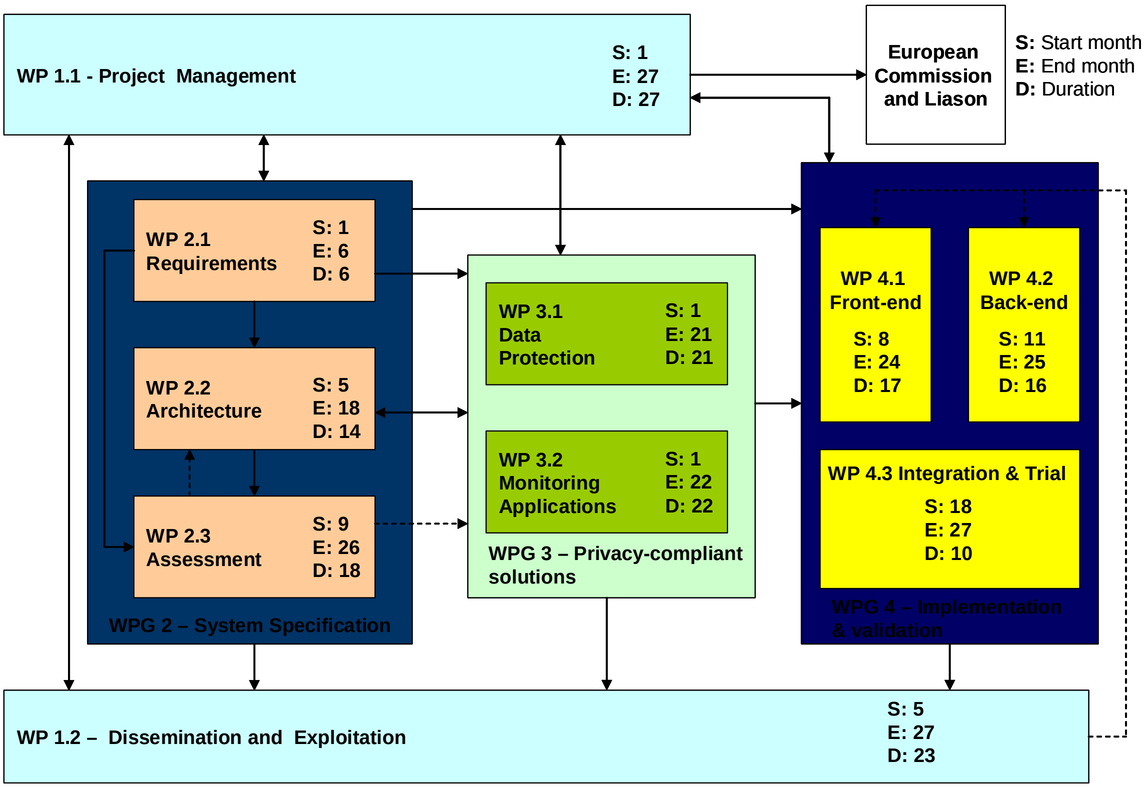


Figure 2: Project management structure

The work-package relationship and dependencies are highlighted in the figure 3.



Note: Solid lines indicate direct input from a WP (or WPG) to another. Dashed line indicate the feedback from a WP (or a WPG) to another. Obviously, WPs in WPG1 have/receive direct impact on/from all other WPs.

Figure 3: Work-package relationship

5. Project time plan

		Project Months & phases																										
		phase 1				phase 2									phase 3									phase 4				
		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27
WPG1 - Project Overall Support																												
WP1.1	Project Management	D	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	D
WP1.2	Dissemination & Exploitation					🟩	🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	D	D
WPG2 - System Specification																												
WP2.1	System Requirements and Scenarios	🟩	🟩	🟩	D	🟩	D																					
WP2.2	System Architecture Specification					🟩	🟩	🟩	🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	🟩	D									
WP2.3	Regulatory, Performance and Security Assessment									🟩	🟩	🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	D	
WPG3 - Privacy-compliant solution specification																												
WP3.1	Data Protection Algorithms	🟩	🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	D						
WP3.2	Monitoring Applications and their Adaptation	🟩	🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	D					
WPG4 - Implementation and validation																												
WP4.1	Front-end Tier Implementation								🟩	🟩	🟩	🟩	🟩	🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	D			
WP4.2	Back-end Tier Implementation											🟩	🟩	🟩	🟩	🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	🟩	D		
WP4.3	Integration and Trial																		🟩	🟩	D	🟩	🟩	🟩	🟩	🟩	🟩	D

Letters “D” on the Gantt diagram indicate the production of a deliverable. In terms of timing, our project has been planned into four phases.

- **Phase 1 (months 1-4)** – goal of this phase is to provide a solid knowledge base, shared by all project participants, upon which further actions will leverage on. To this purpose, the two WPG3 work packages will provide at month 4 a detailed and up-to-date assessment of the state of the art in their respective activity areas and the possible applicability of prior work to the PRISM scenario. WP2.1 will further produce a thorough analysis of the regulatory provisions in the legal areas that are likely to impact the design of a monitoring infrastructure.
- **Phase 2 (months 5-13)** – This phase is aimed at providing a first comprehensive draft of the system architecture specification, and of the technical issues and solutions emerging to integrate the WP3.1 data protection mechanisms and to adapt the WP3.2 monitoring applications. Phase 2 will initiate the start of the early implementation work.
- **Phase 3 (months 14-22)** – This phase is aimed at consolidating and transforming into a complete working solution the specification and early implementation work carried out in the previous phase. The third phase will produce a finalised architecture specification subjected to a thorough performance, security and regulatory assessment. The goal of phase 3 is to deliver an almost completed implementation of the front-end and back-end system components, as well as the related communication and exporting protocols.
- **Phase 4 (months 23-27)** –The integration of the system components, applications and algorithms and converge to a field-trial demonstration of the project achievements is addressed in this phase.

6. Project deliverables

Most of the project deliverables are defined as public deliverables to facilitate larger level of co-operation with exchange of ideas and documents.

Del. no.	Deliverable name	WP no.	Nature	Dissemi-nation level	date (project month)
D1.1.1	Project Presentation	WP1.1	R	PU	1
D1.1.2	Project Handbook	WP1.1	R	RE	3
D2.1.1	Assessment of the legal and regulatory framework	WP2.1	R	PU	4
D3.1.1	State of the art on data protection algorithms for monitoring systems	WP3.1	R	PU	4
D3.2.1	State of the art on monitoring applications	WP3.2	R	PU	4
D2.1.2	Scenarios and System Requirements	WP2.1	R	PU	6
D1.2.1	Initial Dissemination and Exploitation Plan	WP1.2	R	PP	8
D2.2.1	High-Level System architecture specification	WP2.2	R	PU	10
D3.1.2	Preliminary data protection algorithms specification and analysis	WP3.1	R	PU	11
D3.2.2	Preliminary monitoring applications specification and analysis	WP3.2	R	PU	12
D1.1.3	Intermediate Project Reports	WP1.1	R	PU	13,7,19,25
D2.3.1	Preliminary performance and regulatory assessment	WP2.3	R	PU	13
D4.1.1	Design and first prototype of the front-end device	WP4.1	P	RE	15
D4.2.1	Design and first prototype of back-end components	WP4.2	P	RE	17
D1.2.2	Intermediate Dissemination and Exploitation Plan	WP1.2	R	PP	17
D2.2.2	Detailed System architecture specification	WP2.2	R	PU	18
D4.3.1	Integration and Trials Plan	WP4.3	R	RE	20
D2.3.2	System assessment	WP2.3	R	RE	20
D3.1.3	Final data protection algorithms specification and analysis	WP3.1	R	PU	21
D3.2.3	Final monitoring applications specification and analysis	WP3.2	R	PU	22
D4.1.2	Front-end prototype	WP4.1	P	RE	24
D4.2.2	Back-end tier implementation	WP4.2	P	RE	25
D1.2.3	Final Dissemination and Exploitation Plan	WP1.2	R	PP	26
D2.3.3	Final performance and regulatory assessment	WP2.3	R	PU	26
D1.1.4	Final Project Report	WP1.1	R	PU	27
D1.2.4	Report on Raising Public Participation and Awareness	WP1.2	R	PU	27
D4.3.2	Trial	WP4.3	D	PU	27

7. Dissemination plan

The dissemination plan addresses the security and privacy community and the network monitoring community and players. With the involvement of a legal partner, the project will bridge the technical and R&D community with the regulators and public bodies, to foster a technical vision of data protection regulation. The following tools and methods will be part of using and disseminating knowledge activity.

- **Website**: the project web-site www.fp7-prism.eu will be set up for the on-line dissemination of project activities, public deliverables and news related to the project areas. The site will be linked to multiple other sites so that search engines can lead to the project website, to new comers. The site will be kept up to date with continuous updates with the results of the project.
- **Concertation process and Liaison: participation to ICT events**: the project will participate in ICT concertation process and appropriate cluster to disseminate the information among the projects of this cluster. The project will also develop liaison with ICT projects so that project results can be discussed to influence other European activities and receive feedbacks from them.
- **Publications**: the project will participate in conferences and events with contributions from the project to the events addressing ‘security and privacy’ and ‘network monitoring’ issues. The goal is to fertilise a transversal transfer of knowledge from these two typically distinct communities.
- **Scientific journals**: the project will publish the results in the scientific journal, for maximum impact of the project results on the scientific community.
- **Raising public participation and awareness:** To address non-technical community, different Channels that will be used include newsletters, press release, on-line services, etc. In raising public participation and awareness, the project is significantly facilitated by the topic: privacy issues are of likely interest for the citizen regardless of her/his technical background.
- **Interaction with regulation authorities**: The project will contact regulation authorities and other legal entities in order to convey them information on how data protection regulation might be significantly enhanced through the adoption of technical views and metrics.
- **Dissemination activities specifically targeted towards the industry**: The planned standardization contributions planned in the project will be targeted to accomplish industry-targeted dissemination initiatives.

7.1 Standardisation activities

The design of the privacy-compliant measurement components, the requirements for integration into the overall network architecture, the compliance to existing regulations, as well as the knowledge from implementing and evaluating the components provide valuable input to the mentioned standardisation groups. Project results on privacy compliant monitoring and data export is likely to impact the IP Flow Information Export (IPFIX) and Packet Sampling (PSAMP) standardisation groups at the IETF. Both groups are concerned with defining flexible means to export flow-based metering information from routers or other traffic measurement devices. Experiences with the metrics and measurement methods used will be likely contributed to IETF/IPPM and ETSI/STQ.

The IPFIX and PSAMP standards, as well as most IETF and ETSI standards, are closely monitored by the project; once privacy aware solutions will be available in measurement components (e.g. in routers or network probes) on the market, the output from this project can be commercialised by European enterprises without delay. There would be benefit for network equipment vendors due to new differentiating product features.

Within ETSI, a project partner (Hitachi) is already ETSI rapporteur for the Guide on performance metrics and measurement methods. Second, another working group which envisions the participation of a project partner (Hitachi, again) is ‘Legal interception’. Since this group is currently defining the interface between storage systems and the government when data has to be provided, it is a perfect target for the PRISM back-end interface specifications.

8. Expected results and exploitation potential

PRISM is a proof-of-concept project that ultimately aims at showing the technical feasibility of “blind” traffic monitoring, i.e. operate over protected data meanwhile not impairing the network monitoring process effectiveness and the capability, when needed (for legal or technical reasons) to revert the data protection mechanisms set forth. This is achieved by a system architecture that comprises two system tiers (front-end and back-end) plus an additional control component referred to as privacy-preserving controller invoked by data protection reversion procedures.

PRISM also aims at developing privacy-preserving technologies and solutions that may be independently exploited as system enhancements. The next two sections are dedicated to first discuss the exploitation of the individual PRISM technologies, and then discuss the possible exploitation directions for the whole PRISM architectural concepts.

The IPFIX extensions, at both protocol and information model levels that will emerge from the project activities are expected to be of significant interest for a multiplicity of network equipment vendors. Once standardised, these extensions will be integrated in the IPFIX evolving standard.

The PRISM front-end can be also independently exploited as a traffic-probing device, regardless of the data protection mechanisms implemented, because of modular design planned (enable/disable functionality).

The back-end tier will be designed to provide a complete set of solutions which do not strictly require the front-end tier data protection operation. The operators may leverage the back-end role-based access control technology to improve their control and management of the access and processing procedures over data gathered in raw form. The back-end middleware will provide privacy-aware access control and query logging capabilities which are deemed to increase the level of protection of the data collected over the back-end storage, and are expected to provide an effective solution even in the presence of native raw data traces. The distributed storage solutions and the relevant encryption procedures are also enhancements that may be exploited on a stand-alone basis.

The Privacy-Preserving Controller can be deployed as a privacy authority or a data protection officer, administratively external to the operator domain (i.e. the data controller) that can become an important exploitation opportunity.