




Interoperable Trust Assurance Infrastructure

Legal, Social and Economical constraint specification first version

Type (distribution level)	Public
Contractual date of Delivery	28/02/2013
Actual date of delivery	28/02/2013
Deliverable number	D2.5.1
Deliverable name	Legal, Social and Economical constraint specification first version
Version	V 1.00
Number of pages	51
WP/Task related to the document	WP2/T2.5
WP/Task responsible	INDRA
Author(s)	Jaime Arrazola, Leyre Merle, Antonio Skarmeta, Fernando Pereñíguez, Jose Santa, Crisan de los Santos.
Partner(s) Contributing	INDRA, UMU, SCYTL
Document ID 	INTER-TRUST-T2.5-INDRA-DELV-D2.5.1-LegalSocEconReq-First-V1.00.doc

Abstract

This document aims to collect and combine all the legal, social and economic requirements and constraints as related to the Inter-Trust project objectives (Interoperable security and trust policies for the evolving needs of the IT world). Special focus is paid to the interests of the main industrial actors, electronic voting and traffic and transport co-operative services but other interests are incorporated in this document.

Executive Summary

This document, D2.5.1 on Legal, Social and Economical Requirements Specification - First Version, aims to provide a comprehensive view of those requirements that, while still very relevant to the successful implementation of the Inter-Trust Framework, run a risk of assuming a more secondary role in the product planning and design stage. Deliverable D2.5.1 is thus a necessary document that makes up part of D2.1.1 and that provides the supplement needed to prioritize the requirements gathered for that deliverable.

A detailed description of the scenarios addressed by the Inter-Trust project can be found as part of deliverable D2.1.1 which may aid in understanding the origins of the legal, social and economical requirements described here. This document, however, should not need much detailed knowledge of the particulars of the scenarios as the requirements elicited in this document were gathered assuming a generic outlook on the services, trying to account for industry-wide issues that arise due to lax security and privacy in their services. In fact, it is recommended that document D2.2.1 on Gap and Standards Analysis be used in conjunction with this document to provide a comprehensive approach to the relevant industry practices and limitations (V2X and eVoting) which gave rise to the legal, social and economic requirements.

The next step in the requirements elicitation process will be the specification of the overall framework architecture, for which feedback from the legal social and economic considerations gathered within this document will be used. Furthermore, as the project develops and takes shape, functionalities are expanded or reduced and new previously undetected constraints emerge, this document will be regularly updated until the final definition of the framework.

Table of Contents

1	INTRODUCTION.....	6
1.1	SCOPE OF THE DOCUMENT	6
1.2	APPLICABLE AND REFERENCE DOCUMENTS	6
1.3	REVISION HISTORY	6
1.4	LIST OF ABBREVIATIONS	7
2	PREFACE.....	8
3	LEGAL REQUIREMENTS.....	10
3.1	NATIONAL LAW CONSIDERATIONS.....	10
3.2	DOES THE SYSTEM FALL UNDER THE JURISDICTION OF ANY LAW OR DIRECTIVE?	11
3.2.1	<i>Legal-Specific Template Content Description</i>	<i>11</i>
3.2.2	<i>Requirements</i>	<i>11</i>
3.3	ARE THERE ANY STANDARDS WHICH THE SYSTEM MUST COMPLY WITH?	16
3.3.1	<i>Standards-Specific Template Content Description</i>	<i>16</i>
3.3.2	<i>Requirements</i>	<i>17</i>
3.4	IMPACT.....	28
3.4.1	<i>Types of Impacts.....</i>	<i>28</i>
3.4.2	<i>Impact of Requirements</i>	<i>29</i>
4	SOCIAL REQUIREMENTS	32
4.1	SOCIETY AND SECURITY	32
4.1.1	<i>Consumer Attitudes towards Cybersecurity (European Focus).....</i>	<i>32</i>
4.1.2	<i>Internet Security Breach Example: Bad Practice</i>	<i>33</i>
4.1.3	<i>Internet Security Breach Example: Good (not Best) Practice</i>	<i>34</i>
4.1.4	<i>Interacting with White Hat Hackers</i>	<i>36</i>
4.2	WHAT REQUIREMENTS/CONSTRAINTS DOES SOCIETY IMPOSE?	37
4.2.1	<i>Social-Specific Template Content Description</i>	<i>37</i>
4.2.2	<i>Requirements</i>	<i>37</i>
4.3	IMPACT.....	41
4.3.1	<i>Types of Impact</i>	<i>41</i>

4.3.2	<i>Impact of Requirements</i>	42
5	ECONOMIC FEASIBILITY REQUIREMENTS	43
5.1	BACKGROUND AND LIMITATIONS ON ECONOMIC REQUIREMENTS.....	43
5.2	WHAT ARE THE REQUIRED ECONOMIC CONSIDERATIONS?	45
5.2.1	<i>Economic-Specific Template Content Description</i>	45
5.2.2	<i>Requirements</i>	45
5.3	IMPACT.....	47
5.3.1	<i>Types of Impact</i>	47
5.3.2	<i>Impact of Requirements</i>	47
6	SUMMARY AND CONCLUSIONS	48
7	REFERENCES	49
ANNEX.A	BASIC REQUIREMENT FORM GUIDE	51

1 Introduction

1.1 Scope of the document

The requirements of the INTER-TRUST framework are elicited from various sources:

- User needs (User Pull) included in the deliverable D2.1.x *Requirements Specification*.
- State-of-the-Art (Technology Push) included in the deliverable D2.2.x *Gap and standards analysis*.
- Market needs and gaps (Market Pull) included in the deliverable D2.4.x *Market analysis*
- Socio-economical constraints included in the deliverable D2.5.x *Legal, social and economical constraint*.

These four deliverables provide a complete view of the Inter-Trust requirements. Inter-Trusts adopts an incremental approach, all the deliverables will be issues in two versions: initial, with the requirements defined in the first project cycle, and final, with the definitive, full scope, elicited requirements.

This document clearly identifies all the legal, social and economic constraints in the electronic voting and V2x/ITS scenarios which may have a significant impact on the Inter-Trust project. Further similar considerations within related industries are also covered to a lesser extent.

1.2 Applicable and reference documents

This document refers to the following documents:

-None thus far.

1.3 Revision History

Version	Date	Author	Description
0.1	13/12/2012	Jaime Arrazola	Initial document draft
0.2	02/01/2013	Antonio Skarmeta, Jose Santa, Fernando Pereñiguez	Contribution from UMU
0.3	25/01/2013	Crisan de los Santos	Contribution from ScytI
0.9	07/02/2013	Jaime Arrazola, Leyre Merle	Addition of executive summary, relevant EU Directives and initial collection of social and economic requirements.
0.95	22/02/2013	Jaime Arrazola,	Modified document with modifications

		Leyre Merle	highlighted in the 1 st round of reviews.
--	--	-------------	--

1.4 List of Abbreviations

Abbreviation	Full Name
ITS	Intelligent Transport Systems
V2I	Vehicle to Infrastructure
V2V	Vehicle to Vehicle
V2x/ITS	Vehicle to Vehicle and Vehicle to Infrastructure
NDA	Non-Disclosure Agreement
CAM	Co-operative Awareness Message
DENM	Decentralized Environmental Notification Message
IPR	Intellectual Property Rights
DoS	Denial of Service
CALM	Communications Access for Land Mobiles

2 Preface

The purpose of this task, T2.5-Legal, Social and Economic Requirements and Constraints, is to gather all of the soft requirements needed for the formalization of the Inter-Trust framework. The requirements described in this document are made up of different types, including constraints, minimum or maximum design or operating values, measures to take after certain events, etc. Because the requirements gathered within this document do not always naturally arise during the design or production cycle of a product or service it is essential to address them separately in as concise a manner as possible. In fact, a lack of a thorough compilation of all possible factors that could have an effect on the service or product often results in grievous consequences at the very latest stages of development, or even after deployment. To find that a requirement of the type addressed within this document has not been included until a late stage in development could signify a catastrophic failure for the project.

In order to guarantee that the objectives of this task are met, the requirements are divided into three broad categories that should include all aspects not directly addressed during design and development of a system: these are legal, social and economic requirements. In order to gather each specific requirement, reflections and conclusions will be drawn from a range of studies and other informative material (such as reports of security breaches made public, stock valuations of companies following a security breach, etc). Due to the many factors that make up a breach of security and the wide scope of this document, no relevant studies exist that address the specific issues giving rise to the Inter-Trust requirements. Therefore, this document will ask the use case providers, with their experience in deploying highly critical services, to gather the necessary research material in order to cover any and all issues of relevance to Inter-Trust with regard to legal, social and economic aspects. From the research material, generic conclusions will be drawn that could be applied regardless of the industry they are implemented on. These conclusions will be made available as an easy to use reference to anyone wishing to use the Inter-Trust framework. An individual requirement template for all legal, social and economic requirements will also be made available so as to facilitate the future dissemination of the project's results.

Following the generic study, a selection of specific requirements relevant to both the Inter-Trust objectives and the specific use case services will be developed to be used directly in the design of the Inter-Trust tools and eventual demonstrators. These individual requirements are based on a template included in Annex A of this deliverable. Due to the different natures of each of the three categories of requirements mentioned here, the template is only a representation of the common areas shared by all requirements. The template on Annex A also serves to explain how each field in the template has been filled out and as a helpful guide to understand how the requirements are gathered throughout the document. The actual individual requirements, however, have fields in excess of those found in the template, individual for each of the categories, which are explained in sections 3.2.1, 4.2.1 and 5.2.1 of this document. These sections of the document, designed to help in the understanding of the requirement as well as to provide instructions on how to fill the requirements template for anyone making use of the Inter-Trust framework, also include suggestions on how to fill the Fit Criterion field in each requirement. It is worth noting that the choice of an appropriate Fit Criterion for each requirement is essential to maintaining the relevance of said requirement.

In order to gather the legal requirements a distinction was made between the more strict requirements that originating from a national law or EU directive, and the standards-based requirements. A total of 10 legal requirements and 21 standards requirements have been specified as a result. For cohesion with the requirement elicitation process used throughout the principal document, D2.1.1: the UI-REF methodology, the 10 legal requirements that result from laws and directives are considered of mandatory priority. In contrast, the 21 standards requirements are of desirable priority but do not constitute strict priority requirements.

Social requirement gathering is particularly difficult to approach due to both the lack of readily available quantifiable data and the fact that even when data is obtained it is often an extrapolated estimate based on studies with an inappropriate sample size. As such, this document has approached the task of eliciting 7 social requirements in the form of a best-practices approach to security, based on the well documented social response to the latest and most relevant security breaches. It should be taken into account that compliance with these 7 requirements will only show benefits in the case of a security breach and that without these the results of a breach will yield much greater losses, possibly even dooming the commercial success of an otherwise successful product. Thus it can be assumed that the social requirements gathered are of a desirable or even optional priority, but that a minimum number of the requirements should be maintained nonetheless maintained.

It is generally assumed that before undertaking the launch or development of a product, its economic feasibility has been taken into account and that this step should have taken place before the launch of the product. Thus the purpose of gathering economic requirements is to both assess the possible financial cost of an attack and measure this cost against those financial characteristics of the project that enable a successful commercialization of the product or service. However, this does not mean that the economic circumstances and environment surrounding the product will remain constant throughout its lifetime. The economic and financial conditions (which are assumed feasible prior to the launch of Inter-Trust) will be tracked to make sure they are maintained or improved and that mitigating actions can be taken should any change occur. The economical requirements gathered for this document take the most rigorous, measurable and impartial approach that was found feasible for this task, but may still lack well defined numerical bounds.

3 Legal Requirements

The pervasiveness of a system of law under which all human actions take place is a basic and irrefutable assumption in modern society. While, on occasion, these may be broken either accidentally or deliberately, this kind of action is entirely unsustainable in the long-term and of highly reproachable nature. As such, it is necessary to conduct a comprehensive study of all the legal barriers a system could possibly face in order to comply with the law so as to avoid later delays, lawsuits and legal fees, as well as a deterioration of the public image of the project and those involved. The legal requirements gathering will lead the project to comply with all relevant national and EU laws and directives in order to guarantee the successful execution of Inter-Trust and its later marketability.

3.1 National Law Considerations

As part of this deliverable, legal requirements are largely obtained from European Union Directives. While this provides a very comprehensive look at the state of law regarding security and privacy issues or relevant to the basic functioning of the services being proposed (without which the service could not legally exist), it is not perfectly complete. The fact that the EU has, over the last two decades, worked hard to enact legislation that guarantees the rights, safety and wellbeing of its citizens in an increasingly online world, has turned EU countries into the best safeguarded (from a legal point of view) in terms of minimum online security and privacy requirements. This is, overall, a good base point for a legal framework since by using EU Directives a method of abiding to the most restrictive law possible may be followed. In order to achieve a complete set of relevant requirements, national law considerations in the countries that the use case demonstrators take place will be incorporated into this document as the demonstrators are defined and implemented. This approach will generally guarantee that if the legal requirements labelled in this document are followed, legal compliance in countries even outside the EU can also be generally assumed.

While it lies somewhat beyond the scope of this document, there is a real need to analyze the national legal frameworks of the countries where the services are to be developed. This is both within the EU (as a directive may be implemented in a range of different ways in each country of the EU, some being even more restrictive in their legislation than the EU Directive) and globally. There are even some cases where the emphasis to protect the privacy of Europe's citizens makes EU law completely inappropriate for export to other countries. Most notably amongst these countries are China, Russia and Israel, where the use of encryption in any form of electronic communication is highly regulated and not freely allowed for public use. Furthermore, even the export of any technology that uses or enables the use of encryption is regulated by the exporting country, as encryption technologies are considered by many nations (including a large part of the EU) a dual-use technology, with both civilian and military applications. As such it is strongly recommended that any future deployment of the Inter-Trust framework or components pay special attention to the legislations of the exporting and importing countries since it would be impossible for the Inter-Trust framework to accommodate all legal frameworks regarding security and privacy.

3.2 Does the system fall under the jurisdiction of any law or directive?

3.2.1 Legal-Specific Template Content Description

A statement specifying the legal requirements for this system; includes copyright issues, NDAs, pending or foreseeable legislation as well as any new changes to licences, permits or authorisation processes needed. In the case of very similar and non-conflicting requirements (such as different implementations of the same EU directive), the most restrictive legal requirement should be used to avoid redundancies. Include country of origin where the requirement was raised, as well as a list of all other EU countries known to include the requirement if known.

Law, Regulation or Directive

Include the formal name of the law, regulation or directive in this field. If the requirement arises as a result of a national law, the name of the law as written in the original text (presumably in the country's official language) should be included here to facilitate searching for the relevant documents. In the case of EU laws, directives and regulations include only the English name.

Fit Criterion Suggestions

This is to be assessed by validating that the product does not (and will not) break any laws. If possible it should be supported by previous relevant cases brought before national or EU courts

3.2.2 Requirements

Requirement #: 5101		Use Case: V2I, V2V, e-Voting	
Description: Compliance with EU Charter of Fundamental Rights			
Law, Regulation or Directive: EU Charter of Fundamental Rights (12/2000)			
Fit Criterion: <ul style="list-style-type: none">• Verification that the products and services covered by Inter-Trust comply with the charter of fundamental rights. In particular Article 7 – Respect of Privacy and Family Life, and Article 8 – Protection of Personal Data, of said document merit particular importance.			
Dependencies: N/A		Conflicts: N/A	
Revision History			
Created on: 18/12/2012		Created by: Jaime Arrazola (INDRA)	
Revised on:	Revised by:	Revision changes:	

Requirement #: 5102	Use Case: V2I, V2V
Description: Compliance with Directive 2010/40/EU	

Law, Regulation or Directive: Directive 2010/40/EU of the European Parliament and of the Council of 7 July 2010 on the framework for the deployment of Intelligent Transport Systems in the field of road transport and for interfaces with other modes of transport		
Fit Criterion: <ul style="list-style-type: none"> Article 2. Priority areas – Where area II, on Continuity of Traffic and Freight Management ITS Services, and area IV, Linking the Vehicle with the Transport Infrastructure, highlight the relevance of this law to both the V2I and V2V services. Article 10. Rules on privacy, security and re-use of information – Where clauses 1-4 of the article define the extent to which a vehicular service or network must protect against misuse of personal data, maintain privacy and respect the provisions on consent to the processing of personal data. Clause 5 is relevant only to services making use of data from public institutions. 		
Dependencies: 5103, 5105		Conflicts: N/A
Revision History		
Created on: 02/01/2013		Created by: José Santa (UMU)
Revised on:	Revised by:	Revision changes:

Requirement #: 5103		Use Case: V2I, V2V, eVoting
Description: Compliance with Directive 2002/58/EC		
Law, Regulation or Directive: Directive 2002/58/EC - concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications)		
Fit Criterion: <ul style="list-style-type: none"> Article 4 on Security, Article 5 on Confidentiality and Article 9 on Location data are of particular attention and should be strictly followed. Articles 5, 6 and 9 of this directive are derogated by Article 5 of Directive 2006/24/EC and special attention should be paid to follow the recommendations on Article 3 of Directive 2006/24/EC regarding a possible conflict between the two directives. An amendment to this Directive was passed in the form of Directive 2009/136/EC. This directive has thus far only been put to law in member states in a way affects only network operators and not networked service providers. Since the V2I and V2V use cases carry a component of network operation as part of the service, it is strongly recommended that the amendment be enforced at least in those use cases. 		

Dependencies: N/A		Conflicts: 5106
Revision History		
Created on: 07/02/2013		Created by: Jaime Arrazola
Revised on:	Revised by:	Revision changes:

Requirement #: 5104		Use Case: V2I, V2V, eVoting
Description: Compliance with Directive 96/9/EC		
Law, Regulation or Directive: Directive 96/9/EC – on the legal protection of databases		
Fit Criterion: <ul style="list-style-type: none"> Careful monitoring of the data that is input to the database shall be enacted to assess its ownership. Special attention to the differences between copyright and <i>sui generis</i> right should be paid. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 07/02/2013		Created by: Jaime Arrazola
Revised on:	Revised by:	Revision changes:

Requirement #: 5105		Use Case: V2I, V2V, eVoting
Description: Compliance with Directive 95/46/EC		
Law, Regulation or Directive: Directive 95/46/EC – on the protection of individuals with regard to processing of personal data and the free movement of such data		
Fit Criterion: <ul style="list-style-type: none"> Adherence to Sections II (on criteria for legitimate data processing), IV (on information to be given to the data subject) and V (on the data subjects right to access to the data) of the directive should be a critical requirement of any database regardless of national jurisdiction. 		
Dependencies: N/A		Conflicts: 5010
Revision History		

Created on: 07/02/2013		Created by: Jaime Arrazola
Revised on:	Revised by:	Revision changes:

Requirement #: 5106		Use Case: V2I, V2V, eVoting
Description: Compliance with Directive 2006/24/EC		
Law, Regulation or Directive: Directive 2006/24/EC – on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC		
Fit Criterion: <ul style="list-style-type: none"> • Compliance with this directive, as well as those other directives dependent on this directive • Article 5 causes a possible conflict with Directive 2002/58/EC and should be addressed by prioritizing Directive 2006/24/EC according to Article 3 in this Directive. • Article 7 can only be enforced without prejudice to Directives 2002/58/EC and 95/46/EC 		
Dependencies: 5103, 5105		Conflicts: 5103
Revision History		
Created on: 07/02/2013		Created by: Jaime Arrazola
Revised on:	Revised by:	Revision changes:

Requirement #: 5107		Use Case: V2I, V2V
Description: Compliance with Directive 97/7/EC		
Law, Regulation or Directive: Directive 97/7/EC – on the protection of consumers in respect of distance contracts		
Fit Criterion: <ul style="list-style-type: none"> • Compliance with this directive is not mandatory, as it is only valid in some (but not all) the possible market scenarios for the use cases. However, the Inter-Trust platform should allow for electronic commercial contracts between service suppliers and their clients in a secure manner. 		
Dependencies: 5108		Conflicts: N/A
Revision History		

Created on: 07/02/2013		Created by: Jaime Arrazola
Revised on:	Revised by:	Revision changes:

Requirement #: 5108		Use Case: V2I, V2V
Description: Compliance with Directive 93/13/EC		
Law, Regulation or Directive: Directive 93/13/EC – on unfair terms in consumer contracts.		
Fit Criterion: <ul style="list-style-type: none"> • If a contract needs to come into effect between the service provider and consumer, this directive shall be strictly enforced. Otherwise this requirement does not need to be followed. 		
Dependencies: 5107		Conflicts: N/A
Revision History		
Created on: 07/02/2013		Created by: Jaime Arrazola
Revised on:	Revised by:	Revision changes:

Requirement #: 5109		Use Case: V2I, V2V, eVoting
Description: Respect of Intellectual Property Rights		
Law, Regulation or Directive: Directive 2004/48/EC – on the enforcement of intellectual property rights		
Fit Criterion: <ul style="list-style-type: none"> • The entirety of the text is of very high relevance to the successful implementation of the Inter-Trust services. • Section 6, on damages and legal costs, is of particular relevance to the economic requirements as it details the different mechanisms by which damages are legally awarded in IPR cases ruled by EU laws and directives. • Section 7, on publicity measures, is of some importance to the social requirements as it concerns a high-impact social result of an IPR breach. 		
Dependencies: N/A		Conflicts: N/A
Revision History		

Created on: 07/02/2013		Created by: Jaime Arrazola
Revised on:	Revised by:	Revision changes:

Requirement #: 5110		Use Case: V2I, V2V, eVoting
Description: Compliance with EC Regulation 45/2001		
Law, Regulation or Directive: Regulation EC 45/2001 - on the protection of individuals with regard to processing of personal data by the EU institutions and bodies and on the free movement of such data.		
Fit Criterion: <ul style="list-style-type: none"> • This regulation should be followed and strictly enforced when dealing with data from European institutions (whether as provider or receiver of data) or when no national implementation of Directive 95/46/EC exists. In all other cases the national implementation of Directive 95/46/EC should be followed. • There is considerable overlap/interaction between Regulation 45/2001 and Directives 95/46/EC and 2002/58/EC, and care should be taken to apply the correct legal framework. If necessary, the European Data Protection Supervisor (EDPS) can provide clarification on this. 		
Dependencies: 5103, 5105		Conflicts: 5105
Revision History		
Created on: 07/02/2013		Created by: Jaime Arrazola
Revised on:	Revised by:	Revision changes:

3.3 Are there any standards which the system must comply with?

3.3.1 Standards-Specific Template Content Description

Content

Requirements under this category will provide a statement specifying the standards that should be adhered to by each part of the project. In this category, “legal standards” such as those that would result as consequence of an official Recommendation from the Council of Europe/Committee of Ministers are also included. It is worth noting that these legal standards include provisions that are already gathered in the national legal framework of most European countries, and the purpose of the standard is to guarantee a shared framework across the EU rather than to label the specific laws of each country. Unlike a technical standard, adherence to legal standards is compulsory.

Fit Criterion Suggestions

In order to assess the requirement, verification with standard-keeping body or relevant expert (when evaluating confidential issues) should be carried out. If there are any industry or specialized watchdogs these should also be included as part of the requirement.

3.3.2 Requirements

Requirement #: 5111		Use Case: V2V, V2I	
Description: Adherence to ETSI ITS Standard EN 302 665			
Standard: Intelligent Transport Systems (ITS); Communications Architecture		Issuing Body: ETSI Watchdog: N/A	
Fit Criterion: <ul style="list-style-type: none">• The communication architecture envisaged in the project must follow the guidelines presented in this standard.			
Dependencies: N/A		Conflicts: N/A	
Revision History			
Created on: 20/12/2012		Created by: Jaime Arrazola (INDRA)	
Revised on: 02/01/2013	Revised by: José Santa	Revision Changes: Concrete standard labelling	

Requirement #: 5112	Use Case: V2V, V2I
Description: Adherence to ETSI ITS Standard TS 102 637-2	
Standard: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Part 2: Specification of Cooperative Awareness Basic Services	Issuing Body: ETSI Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none">Co-operative Awareness Messages must be compliant with ETSI specifications.	
Dependencies: N/A	Conflicts: N/A
Revision History	
Created on: 02/01/2013	Created by: José Santa

Revised on:	Revised by:	Revision changes:
--------------------	--------------------	--------------------------

Requirement #: 5113		Use Case: V2V, V2I
Description: Adherence to ETSI ITS Standard TS 302 636-6-1		
Standard: Intelligent Transport Systems (ITS); Vehicular Communications; GeoNetworking; Part 6: Internet Integration; Sub-part 1: Transmission of IPv6 Packets over GeoNetworking Protocols		Issuing Body: ETSI Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> The GeoNetworking implementation used to set-up ITS project scenarios must be compliant with this standard. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 02/01/2013		Created by: José Santa
Revised on:	Revised by:	Revision changes:

Requirement #: 5114		Use Case: V2V, V2I
Description: Adherence to ETSI ITS Standard TR 102 638		
Standard: Intelligent Transport Systems (ITS); Vehicular Communications; Basic Set of Applications; Definitions		Issuing Body: ETSI Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> The Inter-Trust security architecture must be applicable to the Basic Set of Applications (BSA) defined in this ETSI ITS standard. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 02/01/2013		Created by: Fernando Pereñíguez
Revised on:	Revised by:	Revision changes:

Requirement #: 5115		Use Case: V2V, V2I	
Description: Adherence to ETSI ITS Standard TR 102 893			
Standard: Intelligent Transport Systems (ITS); Security; Threat, Vulnerability and Risk Analysis (TVRA)		Issuing Body: ETSI Watchdog: N/A	
Fit Criterion: <ul style="list-style-type: none">• The designed Inter-Trust architecture must be able to deal with the security threats identified in this standard for ITS application services using both V2V and V2I communications.			
Dependencies: N/A		Conflicts: N/A	
Revision History			
Created on: 02/01/2013		Created by: Fernando Pereñíguez	
Revised on:	Revised by:	Revision changes:	

Requirement #: 5116		Use Case: V2V, V2I	
Description: Adherence to ETSI ITS Standard TS 102 731			
Standard: Intelligent Transport Systems (ITS); Security; Security Services and Architecture		Issuing Body: ETSI Watchdog: N/A	
Fit Criterion: <ul style="list-style-type: none">• The Inter-Trust security framework must provide mechanisms specified in this standard intended to provide secure and privacy-preserving communications in ITS environments.			
Dependencies: N/A		Conflicts: N/A	
Revision History			
Created on: 02/01/2013		Created by: José Santa	
Revised on:	Revised by:	Revision changes:	

Requirement #: 5117		Use Case: V2V, V2I	
----------------------------	--	---------------------------	--

Description: Adherence to ETSI ITS Standard TS 102 940		
Standard: Intelligent Transport Systems (ITS); Security; ITS communications security architecture and security management		Issuing Body: ETSI Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> The Inter-Trust security framework must consider the security guidelines described in this standard to create the communications architecture. 		
Dependencies: 5118, 5119, 5120		Conflicts: N/A
Revision History		
Created on: 02/01/2013		Created by: José Santa
Revised on:	Revised by:	Revision changes:

Requirement #: 5118		Use Case: V2V, V2I
Description: Adherence to ETSI ITS Standard TS 102 941		
Standard: Intelligent Transport Systems (ITS); Security; Trust and Privacy Management		Issuing Body: ETSI Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> Scenarios in ITS within the project must consider the basic trust and privacy management services defined in this standard, totally or partially. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 02/01/2013		Created by: José Santa
Revised on:	Revised by:	Revised on:

Requirement #: 5119		Use Case: V2V, V2I
Description: Adherence to ETSI ITS Standard TS 102 942		
Standard: Intelligent Transport Systems (ITS);		Issuing Body: ETSI

Security; Access Control		Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> Scenarios in ITS within the project must consider the basic access control services defined in this standard, totally or partially. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 02/01/2013		Created by: José Santa
Revised on:	Revised by:	Revision changes:

Requirement #: 5120		Use Case: V2V, V2I
Description: Adherence to ETSI ITS Standard TS 102 943		
Standard: Intelligent Transport Systems (ITS); Security; Confidentiality services		Issuing Body: ETSI Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> Scenarios in ITS within the project must consider the basic confidentiality services defined in this standard, totally or partially. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 02/01/2013		Created by: José Santa
Revised on:	Revised by:	Revision changes:

Requirement #: 5121		Use Case: V2V, V2I
Description: Adherence to ISO ITS Standard ISO 21210		
Standard: Intelligent Transport Systems – Communications access for land mobiles (CALM) – IPv6 Networking		Issuing Body: ISO Watchdog: N/A
Fit Criterion:		

<ul style="list-style-type: none"> Project scenarios in ITS will use IPv6 following this recommendations. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 02/01/2013		Created by: José Santa
Revised on:	Revised by:	Revision changes:

Requirement #: 5122		Use Case: V2V, V2I
Description: Adherence to ISO ITS Standard ISO 16788		
Standard: Intelligent transport systems -- Communications access for land mobiles - IPv6 Networking Security		Issuing Body: ISO Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> IPv6 security considerations specified in this document must be considered in ITS scenarios. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 02/01/2013		Created by: José Santa
Revised on:	Revised by:	Revision changes:

Requirement #: 5123		Use Case: eVoting
Description: Adherence to Principles recommendations to Universal suffrage		
Standard: Recommendation Rec(2004)11 on "legal, operational and technical standards for e-voting"		Issuing Body: Council of Europe Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> The voter interface of an e-voting system shall be understandable and easily usable. Possible registration requirements for e-voting shall not pose an impediment to the voter participating in e-voting. E-voting systems shall be designed, as far as it is practicable, to maximize the opportunities 		

that such systems can provide for persons with disabilities.		
<ul style="list-style-type: none"> • Unless channels of remote e-voting are universally accessible, they shall be only an additional and optional means of voting. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 16/01/2013		Created by: Crisan de los Santos
Revised on:	Revised by:	Revision changes:

Requirement #: 5124		Use Case: eVoting
Description: Adherence to Principles recommendations to Equal suffrage		
Standard: Recommendation Rec(2004)11 on “legal, operational and technical standards for e-voting”		Issuing Body: Council of Europe Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> • In relation to any election or referendum, a voter shall be prevented from inserting more than one ballot into the electronic ballot box. A voter shall be authorized to vote only if it has been established that his/her ballot has not yet been inserted into the ballot box. • The e-voting system shall prevent any voter from casting a vote by more than one voting channel. • Every vote deposited in an electronic ballot box shall be counted, and each vote cast in the election or referendum shall be counted only once. • Where electronic and non-electronic voting channels are used in the same election or referendum, there shall be a secure and reliable method to aggregate all votes and to calculate the correct result. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 16/01/2013		Created by: Crisan de los Santos
Revised on:	Revised by:	Revision changes:

Requirement #: 5125	Use Case: eVoting
----------------------------	--------------------------

Description: Adherence to Principles recommendations to Free suffrage		
Standard: Recommendation Rec(2004)11 on “legal, operational and technical standards for e-voting”		Issuing Body: Council of Europe Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> • The organization of e-voting shall secure the free formation and expression of the voter's opinion and, where required, the personal exercise of the right to vote. • The way in which voters are guided through the e-voting process shall be such as to prevent their voting precipitately or without reflection. • Voters shall be able to alter their choice at any point in the e-voting process before casting their vote, or to break off the procedure, without their previous choices being recorded or made available to any other person. • The e-voting system shall not permit any manipulative influence to be exercised over the voter during the voting. • The e-voting system shall provide the voter with a means of participating in an election or referendum without the voter exercising a preference for any of the voting options, for example, by casting a blank vote. • The e-voting system shall indicate clearly to the voter when the vote has been cast successfully and when the whole voting procedure has been completed. • The e-voting system shall prevent the changing of a vote once that vote has been cast. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 16/01/2013		Created by: Crisan de los Santos
Revised on:	Revised by:	Revision changes:

Requirement #: 5126		Use Case: eVoting
Description: Adherence to Principles recommendations to Secret suffrage		
Standard: Recommendation Rec(2004)11 on “legal, operational and technical standards for e-voting”		Issuing Body: Council of Europe Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> • E-voting shall be organized in such a way as to exclude at any stage of the voting procedure 		

<p>and, in particular, at voter authentication, anything that would endanger the secrecy of the vote.</p> <ul style="list-style-type: none"> • The e-voting system shall guarantee that votes in the electronic ballot box and votes being counted are, and will remain, anonymous, and that it is not possible to reconstruct a link between the vote and the voter. • The e-voting system shall be so designed that the expected number of votes in any electronic ballot box will not allow the result to be linked to individual voters. • Measures shall be taken to ensure that the information needed during electronic processing cannot be used to breach the secrecy of the vote. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 16/01/2013		Created by: Crisan de los Santos
Revised on:	Revised by:	Revision changes:

Requirement #: 5127		Use Case: eVoting
Description: Adherence to Principles recommendations to Transparency		
Standard: Recommendation Rec(2004)11 on “legal, operational and technical standards for e-voting”		Issuing Body: Council of Europe Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> • Member states shall take steps to ensure that voters understand and have confidence in the e-voting system in use. • Information on the functioning of an e-voting system shall be made publicly available. • Voters shall be provided with an opportunity to practice any new method of e-voting before, and separately from, the moment of casting an electronic vote. • Any observers, to the extent permitted by law, shall be able to be present to observe and comment on the e-elections, including the establishing of the results. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 16/01/2013		Created by: Crisan de los Santos
Revised on:	Revised by:	Revision changes:

Requirement #: 5128		Use Case: eVoting	
Description: Adherence to Principles recommendations to Verifiability and accountability			
Standard: Recommendation Rec(2004)11 on “legal, operational and technical standards for e-voting”		Issuing Body: Council of Europe Watchdog: N/A	
Fit Criterion: <ul style="list-style-type: none">• The components of the e-voting system shall be disclosed, at least to the competent electoral authorities, as required for verification and certification purposes.• Before any e-voting system is introduced, and at appropriate intervals thereafter, and in particular after any changes are made to the system, an independent body, appointed by the electoral authorities, shall verify that the e-voting system is working correctly and that all the necessary security measures have been taken.• There shall be the possibility for a recount. Other features of the e-voting system that may influence the correctness of the results shall be verifiable.• The e-voting system shall not prevent the partial or complete re-run of an election or a referendum.			
Dependencies: N/A		Conflicts: N/A	
Revision History			
Created on: 16/01/2013		Created by: Crisan de los Santos	
Revised on:	Revised by:	Revision changes:	

Requirement #: 5129	Use Case: eVoting
Description: Adherence to Principles recommendations to Reliability and security	
Standard: Recommendation Rec(2004)11 on “legal, operational and technical standards for e-voting”	Issuing Body: Council of Europe Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none">• The member state's authorities shall ensure the reliability and security of the e-voting system.• All possible steps shall be taken to avoid the possibility of fraud or unauthorized intervention affecting the system during the whole voting process.	

<ul style="list-style-type: none"> • The e-voting system shall contain measures to preserve the availability of its services during the e-voting process. It shall resist, in particular, malfunction, breakdowns or denial of service attacks. • Before any e-election or e-referendum takes place, the competent electoral authority shall satisfy itself that the e-voting system is genuine and operates correctly. • Only persons appointed by the electoral authority shall have access to the central infrastructure, the servers and the election data. There shall be clear rules established for such appointments. Critical technical activities shall be carried out by teams of at least two people. The composition of the teams shall be regularly changed. As far as possible, such activities shall be carried out outside election periods. • While an electronic ballot box is open, any authorized intervention affecting the system shall be carried out by teams of at least two people, be the subject of a report, be monitored by representatives of the competent electoral authority and any election observers. • The e-voting system shall maintain the availability and integrity of the votes. It shall also maintain the confidentiality of the votes and keep them sealed until the counting process. If stored or communicated outside controlled environments, the votes shall be encrypted. • Votes and voter information shall remain sealed as long as the data is held in a manner where they can be associated. Authentication information shall be separated from the voter's decision at a pre-defined stage in the e-election or e-referendum. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 16/01/2013		Created by: Crisan de los Santos
Revised on:	Revised by:	Revision changes:

Requirement #: 5130		Use Case: V2V, V2I, eVoting
Description: Adherence to ISO/IEC Standard 27002:2005		
Standard: Information Technology – Security Techniques – Code of Practice for Information Security Management		Issuing Body: ISO Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> • Information security management considerations specified in this document must be considered and the code of conduct shall be followed where possible. • A risk or cost/benefit analysis will be carried out whenever this standard is disregarded. 		

Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 07/02/2013		Created by: Jaime Arrazola
Revised on:	Revised by:	Revision changes:

Requirement #: 5131		Use Case: V2V, V2I, eVoting
Description: Adherence to ISO/IEC Standard 27035:2011		
Standard: Information Technology – Security Techniques –Information Security Incident Management		Issuing Body: ISO Watchdog: N/A
Fit Criterion: <ul style="list-style-type: none"> Information security incident management procedures specified in this document should be followed in the event of a security breach. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 07/02/2013		Created by: Jaime Arrazola
Revised on:	Revised by:	Revision changes:

3.4 Impact

3.4.1 Types of Impacts

The impact associated with the legal and standards requirements in this document is seldom a positive one. Rather, the possible impact is almost always negative due to non-compliance with the requisites, which should be a large enough incentive to encourage abiding by them. Non-compliance to standards will not draw the large number of possible penalties that can be imposed through non-compliance to legal requirements, but it can still have consequences that affect the business context of a particular service or product.

Awards, Damages and Fines

As a result of breaking any of the legal requirements elicited in this document, the defendant may be forced to pay compensation to the wronged party or the state. Damages tend to be awarded as a result of a lawsuit between two private parties, whereas fines are awarded between a private party and the local, regional or national government. There is, in particular, a large difference in the

monetary amount dispensed for each on average. Fines normally have pre-set limits for each punishable offence which tend to be in the tens to hundreds of thousands of Euros (or equivalent). These fines have risen to the millions of Euros for security breaches in the case of financial institutions. There is no clear precedent in EU law for awarding damages to affected users due to a security breach. This is largely attributed to the expense of civil lawsuits (compared to the expected returns) and the low potential for a class action suit. As a consequence, these cases have largely been kept out of EU courts. In contrast, in the US for example, class action suits have seen awards rise to the millions of dollars since as early as 2008.

Injunctions or Suspensions of Service

An injunction, in the context of this document, is the result of legal action taken and is awarded against the party found to be infringing on other entities' rightfully held intellectual property. It requires the infringer to refrain from doing specific actions, namely the commercialization or distribution of any product or service that uses the infringing material. An injunction on an existing product or service is the harshest punishment that a company can suffer, and judges and juries alike prefer to award damages before an injunction as the latter benefits nobody and tends to negatively affect the competitiveness of the market. Particularly within the Inter-Trust context, security issues that would lead to Intellectual Property litigation are regarded as highly unlikely.

Loss of Reputation

Any security breach has a strong likelihood of quickly being made public by the mass media and internet due to growing public interest in the field. This kind of news is never seen in a positive light and thus it is reasonable to assume that any security breach will result in a loss of reputation, at a minimum among the affected users/clients, and possibly from a much wider market segment if details are published by the mass media. Public relations efforts can curtail the negative effects of such an event, as will a prompt and professional response to the crisis. However, while some mitigation strategies exist, to entirely eliminate the loss of reputation following a security breach is impossible.

Market Access and Competitiveness

Standards do not impact on a company's actions in the same way that laws do. Since compliance to standards is voluntary, disregarding them would probably arouse much milder consequences. However, this does not mean that ignoring a standard would be without impact on a product. Most of the time, this impact can be assessed in terms of market access and competitiveness. A standard's ability to unify certain industries, products or services by enlarging those markets tends to lead to lower costs, greater sales and overall enhanced competitiveness. Occasionally, legislation will force a certain standard on a range of products -as is the case with antennas that emit in the regulated sections of the spectrum. Therefore, legislation-enforced requisites should be treated as mandatory legal requirements, and not standards-based ones.

3.4.2 Impact of Requirements

Requirement Number	Impact
5101	The Charter of Fundamental Rights is the blueprint used to define the laws

	governing the right to privacy of individuals, as well as their personal data. It is expected to have a great indirect impact on Inter-Trust results since the directives that determine the right to privacy of Europeans are in a revision and update period, with upcoming modifications based on this Charter that should last through 2014.
5102	This requirement has a small impact since most of the relevant text within the directive that acts as source of the requirement refers to issues better addressed by requirements 5103 and 5105. The greatest contribution of this requirement is on the encouragement of the use of anonymous data in ITS applications.
5103	This requirement has one of the greatest impacts within the legal requirements, together with requirement 5105, and is of extremely important relevance to Inter-Trust. It details the minimum level of security needed to guarantee the privacy of a user and his/her personal data from a functional point of view (where specific implementation is governed either by national legislation or by the specific industry interests), thus creating a security baseline for Inter-Trust (in conjunction with requirement 5105).
5104	Requirement 5104 has a moderate impact on the project but is likely to affect all industries that would make use of the Inter-Trust framework. It provides details regarding the rights and rights-holders of the information stored in databases in electronic services. Of particular impact are the provisions that detail when <i>sui generis</i> right is awarded to database owners and the extent to which this is granted so that this right can be secured accordingly.
5105	Together with requirement 5103, this requirement has the largest impact here. Where req 5103 deals with the functional minimum security that must be guaranteed to preserve privacy, req 5105 deals with access requirements to electronic data and legitimate uses of said data. This requirement, in essence, poses a limit on the information that can be obtained from a user, as well as how said information can be obtained and processed. Due to the essential necessity to obtain personal information from users and to process this information within Inter-Trust, this requirement is key for certain industries (ITS and eVoting prominently amongst these).
5106	This requirement has a minor to moderate impact on Inter-Trust and is highly dependent on the nature of the service. If the service includes any publicly available network operation or communications service, such as an Internet Service Provider might, the impact will be moderate as the entire directive is likely to apply and form part of the security needs of the service (it is not a high impact since the directive is not very restrictive and aimed primarily at facilitating the audit process). For all other services the impact is minimal, as only a few of the articles of the directive need to be applied. These are minor amendments to pre-existing req 5103 and affect security only slightly.
5107	The impact of this requirement is dependent on the nature of the service deployed as part of Inter-Trust, with no relevance unless it is a billable service with an electronic contract and of only minor relevance otherwise. This requirement is relevant to Inter-Trust to outline the kind of information that needs to be securely exchanged between the contracting parties.
5108	This requirement only has a minor relevance for Inter-Trust as it deals mostly with unfair contract terms. The only implication of relevance to security is that no article or clause in a contract may attempt to subvert the basic rights to security and privacy all European citizens should have.

5109	Although Intellectual Property Rights are not directly related to security or privacy, they are still relevant to Inter-Trust and can have a considerable impact. There is a range of mechanisms that makes IPR important within the project, from the fact that Intellectual Property data is extremely valuable and requires strong security, to the issues that can arise when a third party's Intellectual Property data is being used, stored or transferred by a service.
5110	For those services where information is exchanged to or from a European institution this requirement has the same high impact as req 5105 as it replaces some of the relevant text of that requirement with often more stringent measures. Otherwise this is not a requirement and thus has no impact.
5111, 5112, 5113, 5114	These 4 requirements share the same impact as they form the basis of the standard that the ITS services (V2V and V2I) have to follow. They have a moderate impact within ITS-based Inter-Trust services (with no impact outside ITS) since following the standard will greatly increase the competitiveness of the product or service, due both to the price reduction of commercial, off-the-shelf components, and to the increased market available for the product/service as a result of interoperability with other services/infrastructure/vehicles. It is worth mentioning that this standard is not the only ITS standard in widespread circulation and that ISO's CALM standard requirements could replace the current ETSI standards as both teams have been working in close liaison[1] to guarantee interoperable standards.
5115, 5116, 5117, 5118, 5119, 5120	These 6 requirements represent the security-specific standards and threat analysis procedures that are part of ETSI's group of ITS standards. They have a high impact on Inter-Trust's objectives as they represent a state of the art view on the minimum security requirements of ITS applications. ETSI's standard has furthermore approached security in a highly interoperable way, at least between the full ranges of current and predicted ITS services, further increasing the impact these requirements can have within Inter-Trust.
5121, 5122	Although the bulk of Inter-Trust will abide by ETSI's ITS standard, the more technical implementation of IPv6 will be done according to ISO's standards for IPv6 networking and IPv6 security. Impact is expected to be moderate to minor for the Inter-Trust objectives as these standards cover a relatively small niche of the system's security - that of the security embedded within IPv6.
5123, 5124, 5125 5126, 5127, 5128, 5129	While not originating from a formal standards body, European Recommendation Rec(2004)11 is a recent attempt at developing a standard for eVoting practices within Europe. Unlike most standards, however, this recommendation is based on the constitutional provisions for a fair and free election in democratic countries and has more to do with operating and design principles, without much technical description. For this reason the impact should be considered moderate or high for the 7 requirements as, despite being a non-binding recommendation, non-compliance could effectively lead to a conflict with a democratic nation's laws.
5130, 5131	The security techniques addressed in these 2 requirements complement the technical specifications of security requirements expressed above by providing a code of conduct and incident management protocol. These have a moderate impact and tie in hand in hand with the social requirements, as the main goal of these is to reduce the blowback that might follow from security reach.

4 Social Requirements

Acceptance of a product does not rely exclusively on its compliance with the law. In order for a system or product to have any measure of success it must both be socially accepted by at least a fraction of the population, and not be outright rejected by society at large. Thus it is necessary to gather social requirements originating from the perspective of both perceived acceptance and (perceived) rejection. The level of acceptance is relatively quantifiable and will be addressed in the market analysis with regard to the market size. This section of the requirements will address the aspects leading to social rejection of the product. It is worth noting that due to their very nature, these requirements are rather vague and prone to large error margins, even those that originate from carefully executed studies, polls and interviews.

4.1 Society and Security

Beyond the inherent difficulties of assessing any social requirement, in the field of security and privacy there is the added problem of a lack of technical knowledge[2][3][4][5] by the bulk of internet users regarding their security options. This implies that perceived security (by society) does not need to necessarily relate to the real security of a system as users may be unaware of their security options and think they are less secure than they are. Alternatively it is not rare for internet users to subvert pre-existing security mechanisms in order to make it easier to use a program or application, sometimes leaving users less secure than they think they are. This has led to the existence of a gap between society's reaction to security and privacy flaws and the scope and seriousness of an attack. It is also worth noting that society can react not just to a security or privacy breach, but also to changes in the security or privacy policy of a service, as happened with the photo-sharing service, Instagram in December 2012. In order to introduce the social requirements for the Inter-Trust project it is necessary to first give a good description of society's reactions to security and privacy as these have a large effect on the relevance of each social security requirement.

4.1.1 Consumer Attitudes towards Cybersecurity (European Focus)

A study released in July 2012, commissioned by the European Commission[6] gave a very comprehensive insight into the perception of Europeans regarding cybersecurity. Although the study makes clear that there are noticeable differences among demographics and countries, it also highlights some trends that are unrelated to these factors. In this regard the largest gaps existed between the NSM12 and EU15 countries, between young and elder internet users, and between people of different educational levels or occupation. The most noticeable differences arose between people with different views of their proficiency in the use of Internet. For instance, people who believed that they were well informed about Internet security risks also tended to show greater confidence in the use of Internet services, although this was not always the case. It is worth noting that there are marked differences between wealthier and poorer countries[7], but at least in Europe, there is a clear natural trend towards homogenization where less wealthy members gradually move towards the same levels of use and confidence as wealthier members of the EU. This trend toward homogenization is more prominent within Europe than outside, largely due to the fact that the socio-political and legislative frameworks are very similar throughout all EU27 countries. These trends contrast sharply against those of countries that heavily regulate the internet.

In Europe, a leader in terms of internet use, 71% of all EU citizens use the internet; furthermore, 53% of citizens use the Internet on a daily basis. Of all citizens that use the internet in the EU, 29% do not feel confident enough to use banking or online shopping services, a number that is steadily reducing. The study [6] also evidences a clear correlation between internet use and confidence in the use of internet services. There also exists a consistent trend relating how concerned users are with their use of the internet with how informed and confident they feel to be concerning Internet use. Indicating also that as users become better informed and confident, they also become more concerned. This conclusion reflects the idea that uninformed users, while likely to be insecure about their use of internet, do not need to be necessarily concerned about it. This follows from the assumption that those users that are uninformed about security measures are also uninformed about the consequences of a breach in security. Likewise, informed users are aware of the very serious consequences of poor cybersecurity (which increases how concerned they are) but probably know how to identify the more serious threats well enough to use the internet with relative confidence. It is also likely that those users that are more concerned about using the internet also dedicated more time and effort into becoming better informed, eventually growing more confident in the use of the internet.

Of those citizens that use the internet, the largest security concern is the misuse of personal data, with 40% of EU citizens [6] stating this as their highest concern. Thus, 89% of EU citizens would avoid disclosing personal information online and 77% believe their personal information is not kept secure by websites, with 66% thinking this even of internet services deployed by public authorities. These statistics arise despite the fact that identity theft is the least common type of criminal activity experienced by EU citizens with only 8% of citizens ever affected¹. From this data it is possible to extract a very relevant social consideration: that the misuse of personal information has an increased impact (within European society) compared to any other type of attack. In contrast, 38% of all Europeans received a fraudulent email but only 48% of Europeans are very or fairly concerned by this fact (8% of citizens were affected by a personal data misuse but 51% were very or fairly concerned by this). In consequence, any security breach that could result in loss or misuse of personal data should be considered of utmost importance within Inter-Trust.

4.1.2 Internet Security Breach Example: Bad Practice

Cybercrime has risen from a mild annoyance to a full blown issue of near epidemic proportions over the last 5 years and it seems that not even some of the largest and most important players in the net are immune to this. In fact some of the greatest blunders with the most noticeable social repercussions have originated at some of the largest IT companies worldwide. As a result, an increasing number of experts are beginning to voice their concern that the current paradigm of perfectly secure internet services is rapidly disappearing and that all internet services should assume breaches will take place, with much greater efforts directed at mitigating any damage these might cause as well as improving the venues of communication between the company and the affected users. These facts, although not directly backed by data (it is nearly impossible to obtain data on how often companies are successfully attacked and completely impossible to obtain data on how often hackers try and do not succeed) seem to reflect a “best practices” approach that has been shown to

¹ Identity theft is the only form of misuse of personal data that is covered in the study.

be capable to placate public anger following a breach in security with a resulting harm to the legitimate users of the service.

During an otherwise unremarkable afternoon on April 19th 2011, Sony's PlayStation Network systems in San Diego, California experienced an unscheduled reboot on some of their machines; after further investigation it became apparent that someone had broken into the system. Throughout the following night and day the extent of the breach was found to be greater than imagined and eventually, as the security breach failed to be brought under control quickly, all of Sony's PlayStation Network servers were taken down, resulting in a worldwide service blackout that affected about 77 Million users. It was not until April 26th that Sony announced that troves of personal user data, including credit card data, had likely been stolen, and declares this as the reason for taking down the service, having provided no service and no convincing explanations for nearly a week, and public outcry fuelled by an avalanche of rumours resulted in a large number of initiatives against the company. One day later Sony's shares dropped 2%, followed by a 4.5% drop the following day. Eventually, the issue grew completely out of Sony's control and several countries political representatives demanded an official answer from Sony, most notably the US Congress' House of Representatives.

It is worth noting that the exact causes of the breach have not yet been discovered or divulged, that legal action was taken against Sony but that outside the UK no other regulatory agency or judiciary has found blame in Sony's actions. This is important because it shows that users are not as worried about the causes or details of a security breach as they are about the effects of it, and in this respect Sony failed to mitigate the fears of their users by persistently delaying or hiding information that directly affected them. Eventually the backlash from this event resulted in even greater losses for Sony as it was forced to hand out free games to almost all of the PlayStation Network users in order to re-populate their service a month after the initial incident, when the service finally was restored. Seeing how the services that were taken down were offered for free and the users suffered no monetary loss as a result of the downtime, the act of giving away free products was largely interpreted as a redeeming gesture due to the data loss and not as a form of compensation for the service loss (although compensation was given to users of certain paid subscription services that had been also taken down). Overall it is generally believed that Sony elicited not just a much more vitriolic reaction from the public, but also exposure to a wider range of litigating actions against itself due to the poor communication and customer support during the initial weeks after the attack. This also forced Sony to give out very expensive compensation (in the form of free games to all affected) for the totality of their users to restore its public reputation.

4.1.3 Internet Security Breach Example: Good (not Best) Practice

Not all are horror stories within the world of internet security. While a company has yet to experience a security breach without some form of social backlash, some have incorporated steps and procedures to greatly minimize its effect. This is the case of the LinkedIn security breach that took place in early June 2011, barely more than a year after the Sony hack. In this scenario, however, the response of society was much milder, despite the fact that the information stolen was potentially more harmful than in the Sony incident. Furthermore, unlike Sony, LinkedIn was made aware of the security breach at the same time as the rest of the world when, on June 6th, 6.5 million hashed passwords were released on an unauthorised website (although no mention to LinkedIn was made at the time).

The encrypted passwords that were posted did not include the personal data from the users needed to render the password useful, such as an associated email or username. Regardless of intent and the damage those passwords would cause if decrypted, within the first couple of hours over 200,000 passwords had been decrypted and published in clear-text. If the original poster would have had access to the original emails or usernames, each one of those 200,000 cracked passwords would have allowed the hacker to access the full personal profile of each one of the LinkedIn members, whose profiles are known for the accuracy of the data, unlike other social networks. LinkedIn made an initial public statement saying that it was aware of the leakage and that it was investigating whether the passwords really did belong to members of their service. It was not until June 9th that the company made their next statement, much like Sony, leaving the general public in the dark for almost 3 days.

While it seemed that thus far both attacks and their responses were very similar, it is the actions that LinkedIn took during the first 3 days that truly distinguished both cases apart. Despite not making any public statement for those 3 initial days, this did not mean LinkedIn wasn't visibly mitigating the damage. In fact, before the night of the 7th of June, LinkedIn had forcibly disabled every one of the 6.5 Million passwords, notified all affected users and implemented and directed the users to a secure password recovery, essentially eliminating the threat to the vast majority of affected users and restoring faith amongst those affected. Meanwhile, as with all security breaches, criticism about the security came through, in this case mainly aimed at the fact that while the passwords had been hashed, they had not been salted, a step considered common practice in modern encryption. It is worth noting that in this hack, as well as in the Sony hack, little or no attention had been paid to the vulnerability that enabled access, but rather to the inherent security, or lack thereof, of the stolen data. Yet this criticism did not last long, as on June 9th LinkedIn issued a blog post from one of its Directors where LinkedIn effectively:

- Acknowledged the fact that an attack had taken place and accepted its full scope of it.
- Explained the actions that had taken place during the 6th and 7th to guarantee that no damage was done to the affected users, and highlighting that, although the world may have been learning of the details now, those affected were already aware and protected.
- Highlighted the password hashing/salting issue and explained that this should prevent any future theft of this kind, as well as protecting current users.
- Included the names and short CV of those responsible for the security systems and the fix deployed.

LinkedIn estimated that the resulting costs for this breach amounted to \$1 Million in damage control and \$2-3 Million more² in future enhancements to their security as part of a program to improve the security of the social network across all its services. This compares to the \$171 Million [8] Sony claimed was lost as a result of the hack, no further figures having been given detailing any future spending on more secure systems. Both companies have a similar number of users, both intrusions

² LinkedIn Data Breach Costs More than £1M <http://www.computerweekly.com/news/2240160962/LinkedIn-data-breach-costs-more-than-1m>

were of a similar nature, with highly sensitive information stolen, and both companies managed to largely avoid the leaked data from causing direct harm to their users. Yet the never-explained delays, the reluctance to address any detail or responsible person, and the fact that no information was given as to how they fixed the problem, left millions of users irate at Sony. In the end, both LinkedIn and Sony had to implement large PR and outreach campaigns to placate angry users. But due to the diligence, transparency and speed of these efforts in LinkedIn's case, the company was able to reduce the costs of such an event to a small fraction of those incurred by Sony, highlighting a very clear competitive advantage that results from knowing how to inform society and a product or service's user base about a security solution, particularly when things go wrong.

4.1.4 Interacting with White Hat Hackers

While the word hacker has attained a nefarious reputation, it is worth noting that some of the most prominent security experts consider themselves to be hackers, albeit often differentiated by the name "white hat" hacker. Although an extremely varied range of people falls under this moniker, from industry experts to hobbyists, the collective shares a common ethos: to actively subvert existing security measures with the purpose of improving the very security of the systems they disrupt. Where white hat hackers differ wildly from each other is in how, once a security flaw has been detected, they go about bringing the change in security needed to stop the flaw they uncovered.

There is no denying that having a white hat hacker break into a company's secure infrastructure or service is almost always a better alternative than finding out about the security breach through a malicious attack. However white hat hackers often respond to different interests than those of the company affected and these interests can put them at odds with the owners of the systems they broke into. Most commonly a white hat hacker will inform the affected company in private about the security risk and work with the company to fix the issue as soon as possible. At times however, either due to economic inability or outright reluctance to implement the sometimes extremely stringent security measures on the part of the affected company, a white hat hacker might try to force a push for better security by "going public" with details of the breach he/she discovered. Although very rarely, a few hackers have been known to go public without first contacting the affected company. However, because the motivation for this course of action is almost always to embarrass or otherwise cause harm to the company affected, even among the white hat hacker community this method is looked down upon and its practitioners, although self-titled white hat hackers, are rarely integrated within the white hat hacker community. For these reasons, this latter kind of attack will not be considered the actions of a white hat hacker within this document, but those of a malicious hacker.

It should be mentioned that 100% of malware toolkits³ (the most widely used software for security breaching, found pervasively throughout the internet) found available today used logic exploits made available from white hat disclosures. In fact, malicious hackers actively search through white hat forums as they prefer white hat code due to its reliability and ease of use. This has serious implications, particularly for a company that is willing to alienate the white hat community rather than fix the security of their systems, as it is almost certain that these exploits will very quickly reach the hands of malicious hackers. For this reason a careful balance needs to exist between companies

³ The Exploit Intelligence Project v2 <http://vimeo.com/31548167>

and the white hat community. It is generally advisable to attempt to work with the white hat community as the benefits from a close and understanding relationship between both sides help fulfil the white hat community's goals while the affected company essentially gets the free services of some of the best security analysts in the world. It should also be noted that companies that take legal action against white hat hackers almost always win in court, as their actions are not defended by any country's legal framework (breaking into a secure system is a crime regardless of motive or gains). The downside to this course of action is that the white hat community is unlikely to ever contact a company that sues white hat hackers, yet that does not mean that the security holes they might find will not be disclosed more discreetly next time. This eliminates a possible early warning venue while doing nothing to improve the security of the company's systems. Ultimately, white hat hackers are an individualistic sort and a company can find their presence to be as likely to be beneficial as harmful, thus a case by case evaluation should be carried out with each contact with a white hat hacker.

4.2 What requirements/constraints does society impose?

4.2.1 Social-Specific Template Content Description

These requirements should address any factors that would make it unacceptable due to any social, political or cultural issues that could arise including issues related to the use of the system by minorities or other vulnerable users.

Social Group/s Affected:

If there is any clearly identifiable social group or groups that are affected by the requirement they should be included in this section.

Expected Impact

A description of the possible impact that will result from non-compliance with the requirement should be included. Figures are encouraged when known (although this is rarely the case as there is very little accurate data on social implications of security).

Fit Criterion Suggestions

A social impact analysis/evaluation should be used to assess these requirements, possibly a small poll could also be conducted during evaluation.

4.2.2 Requirements

Requirement #: 5201	Use Case: V2I, V2V, eVoting
Description: Limitations on informed consent from consumers.	
Social Group/s Affected: Consumers of V2V/V2I products and services.	
Expected Impact: Lack of transparency can lead to product rejection or backlash. Realization by consumers of this fact at a late stage in the product development lifecycle can lead to a failed or	

cancelled product that will greatly increase development cost overrun.		
Fit Criterion: <ul style="list-style-type: none"> European Data Protection Supervisor (EDPS) evaluation or inquiry results. 		
Dependencies:		Conflicts:
Revision History		
Created on: 18/12/2012		Created by: Jaime Arrazola (INDRA)
Revised on:	Revised by:	Revision changes:

Requirement #: 5202		Use Case: V2I, V2V, eVoting
Description: Establishment of a threat hierarchy in terms of notification urgency		
Social Group/s Affected: All		
Expected Impact: Following this requirement will enable an appropriate public response to any attack, minimizing the risk of over-worrying users by omitting certain attacks such as non-data stealing malware infections or short-duration DoS attacks, while maximizing consumer confidence with prompt and extended notifications in the case of a theft of private personal data or hijack of the service.		
Fit Criterion: <ul style="list-style-type: none"> Validate threat hierarchy against known user reactions to different attacks. 		
Dependencies: N/A		Conflicts: N/A
Revision History		
Created on: 13/02/13		Created by: Jaime Arrazola
Revised on:	Revised by:	Revision changes:

Requirement #: 5203		Use Case: V2I, V2V, eVoting
Description: Case-by-case analysis on notification to individuals		
Social Group/s Affected: Exclusively those users directly affected by a security or privacy breach.		
Expected Impact: Notifying individuals with customized instructions to aid in solving any client-side issue (in the broadest terms) that a security or privacy breach may trigger, is necessary to mitigate		

public anger. Users who have been unaffected or who cannot do anything regarding the effects of the breach should not be contacted individually, which will avoid undue mistrust and user frustration.

Fit Criterion:

- If any actions are needed from a user after a security breach, the user is notified as quickly as possible with a mechanism in place to detect when users have taken said actions (such as checking when a user has changed their password after a mandatory password check to verify compliance).
- Users who will not notice or suffer any harm as a result of a security breach are only notified when a public disclosure is made.

Note: This case must acknowledge that some private information could humiliate or embarrass a user as a form of possible harm to the user. These users in particular should be warned as early as possible before a public announcement is made.

Dependencies: N/A

Conflicts: N/A

Revision History

Created on: 13/02/13

Created by: Jaime Arrazola

Revised on:

Revised by:

Revision changes:

Requirement #: 5204

Use Case: V2I, V2V, eVoting

Description: Establish visibly and publicly a competent high-ranking employee to lead restoration efforts.

Social Group/s Affected: All

Expected Impact: Users will feel more confident that real work is being done behind the scenes by assigning a person responsible for this task.

Fit Criterion:

- Within 24 hours of detection of a security breach there should be a specialized appointee for this role of senior management / directing level.
- The name of this responsible shall be included within the first public announcement.

Dependencies: N/A

Conflicts: N/A

Revision History

Created on: 13/02/13

Created by: Jaime Arrazola

Revised on:	Revised by:	Revision changes:
--------------------	--------------------	--------------------------

Requirement #: 5205	Use Case: V2I, V2V, eVoting
Description: Development of an internal protocol to deal with interactions with white hat hackers.	
Social Group/s Affected: company, white hat hackers, gray hat hackers	
Expected Impact: Useful contacts established between the company and white hat community while giving security officers the ability to discern between white and gray hat hackers.	
Fit Criterion: <ul style="list-style-type: none"> • Successful interaction with white hat hackers leads to security holes found and patched in time. • Appropriate and prompt action (litigation or otherwise) taken against gray hat hackers. 	
Dependencies: N/A	Conflicts: N/A
Revision History	
Created on: 13/02/13	Created by: Jaime Arrazola
Revised on:	Revised by:
Revision changes:	

Requirement #: 5206	Use Case: V2I, V2V, eVoting
Description: Notification of breach to relevant authorities	
Social Group/s Affected: company, national or international cybercrime fighting units.	
Expected Impact: Better chances at successful detection and possible arrest of the attacking party as well as the creation of a strong disincentive towards another attack on the company's system. Note: in some countries notification to authorities is a compulsory action following any breach in security or theft of personal data. As such this requirement could be a fully mandatory legal requirement as well. Local and national laws should be verified to decide the importance of this requirement.	
Fit Criterion: <ul style="list-style-type: none"> • Authorities contacted after an attack and involved in the forensic activities. 	
Dependencies: N/A	Conflicts: N/A

Revision History		
Created on: 13/02/13		Created by: Jaime Arrazola
Revised on:	Revised by:	Revision changes:

4.3 Impact

4.3.1 Types of Impact

Social impacts with regard to security tend to be extremely costly and of an unexpected nature. This impact within the world of cybersecurity is often negative and implies losses for the company or individual affected, often as a result of the publication of a security breach. On the other hand, engaging society to increase profits or sales is generally achieved through advertisement, which has proven effective in a wide range of industries. However, the value of advertising security characteristics or better security solutions does not seem to have such a clearly positive effect, particularly for companies that do not develop or market their own security solution, but instead integrate a solution from other security providers. Within Inter-Trust, the security requirements are intended to minimize the negative effects of a security breach while engaging with users to better explain the benefits of a security upgrade. The impact the effects may have is detailed below.

Social Discontent as a Trigger for Legal Reform

Legal frameworks in most democratic countries can be thought of as the collective conscience of the voting population, and innumerable social concerns get addressed by the law as they become more prominent. In this sense it is worth to highlight the beneficial impact of identifying and respecting widespread social perceptions as it can sometimes foreshadow future changes to the law in the medium/short term.

Loss/Gain of Customer Base

A gain or loss of customer base is easily the most recurring impact resulting from any type of security publicity of a product (negative or positive). The magnitude of this impact is directly related to how publicised an event is their frequency of occurrence and their nature. Events can be positive (such as adding a security label to a service or product) or negative (such as a publicized breach of security). While research on the former shows non-existent⁴ or small [10] benefits, research has consistently shown that a negative event causes a considerable customer loss [9]. It is very important to acknowledge that this effect tends to tarnish the entire brand involved and normally has an impact across the range of products or services endorsed or owned by a brand, and not only on the product or service whose security has been breached.

⁴ Security Seal vs No Security Seal Site Test: <http://www.proimpact7.com/ecommerce-blog/security-seal-vs-no-security-seal-site-test/>

4.3.2 Impact of Requirements

Requirement Number	Impact
5201	Informed consent can be hard to achieve for some products since undue or overly negative warnings may give rise to suspicion on the part of the user. However the impact of using an adequate level of informed consent as part of a security solution is moderate to high. This is due to the fact that everyone using the product will come across this warning on first use and is thereby given the opportunity to determine the initial level of trust that will be granted to the product/service. Furthermore, the impact of foregoing this requirement is not only very negative, as it can both make the user confused or distrustful and lead to legal action against the product or service provider.
5202	In order to compose an adequate response to the public following a security breach it is essential to have a well-defined action plan in place. This requirement is the basis of such an action plan and therefore has a high impact on the social requirements of the project.
5203	A large number of security breaches can result in personal information from users/clients being acquired by the attackers. In these cases it may be necessary to engage the affected users individually to help them reduce the effects of a breach. The impact of this measure can be great, such as when personal banking information is stolen, but is highly dependent on the nature of the attack, and notifying individual users about, for example a DoS attack, could even have a small negative impact.
5204	Appointing a specific individual or group within a company to dedicate him/herself full time to handle a security breach is one of the simplest measures, and with the largest impact, that a company may take. The impact of this decision is further enhanced by publicising the name of the responsible person or group and creating venues of direct communication between this person or group and the top clients. This impact is also related to the position of this individual within the company, with the largest effect achieved by naming a Security Director or CISO for this role.
5205	The impact of this requirement is often minor. White hat hackers most regularly interact with security providers and not all that often with those that integrate security solutions within their products. Contact with white hat hackers is not foreseen as a likely result of using Inter-Trust.
5206	Depending on the country the service is based on, this requirement could have a huge impact as it may be compulsory by law.

5 Economic Feasibility Requirements

Economic feasibility is the measure of the cost effectiveness of an information system solution. Information systems are often viewed as capital investments for most businesses, and, as such, should be subjected to the same type of investment analyses as other capital investments. This section will analyse and take into account Economic Feasibility Requirements. However, these requirements have a relevant impact and will be therefore further analysed and taken into account in the Exploitation Plan (D6.1.2). Financial analyses such as return on investment (ROI), rate of return, cost/benefit, payback period, and the time value of money are utilized when considering information system development projects. Further considerations that could have a direct impact on the economic feasibility also need to be taken into account.

5.1 Background and Limitations on Economic Requirements

Although security and privacy in every ICT-related service are closely related to economic factors, it is not easy to estimate the economic benefit that the implementation of this type of policies adds to the service, as an investment in security does not usually lead directly to profits.

However, while it is difficult to evaluate the economical revenue from an improvement in security, as users are not aware if it works properly, a lack in privacy and security has an important and negative economic as well as social impact, as explained before. The most noticeable economic impacts resulting from an attack on the privacy or security of a system are:

- A system failure resulting from a security breach, generating direct economical losses to the company. Business interruption may include lost revenue and loss of productivity during the disruption.
- Cost due to restoring a system to its original, pre-attack state.
- Loss of reputation or damage to a firm's brand: attacks on privacy and security damage the image of the company, losing clients' trust and losing actual or potential users, with its consequent economical impact.
- In some cases, attacks on security may provide the hacker access to the products' source code. It is then possible to copy the code or use it without paying the license.
- Attacks on privacy, related to personal data and specially credit cards, may generate large losses to the users.
- Attacks or lack of privacy can be penalized by the law, forcing companies to pay a fine.

Attacks produce many kinds of costs, some of which cannot be quantified easily, as there are no standard methods for measuring the costs/benefit of security and privacy attacks. Without accurate cost data, it is difficult for organizations to assess the risks they face, make rational decisions about how much to spend on information security, or evaluate the effectiveness of security efforts. This section presents some noticeable examples of financial losses and general studies based on the analysis of a significant number of companies affected by this kind of attacks, in order to give the reader a general idea of the economic risks those attacks involve.

Sony's case, as explained in the previous section, is one of the most remarkable examples of a successful cybernetic attack of the last decade, and its financial consequences should be mentioned in this section (although it has been briefly covered in the previous section). It affected more than 100 million users, from whom personal information was stolen, and a range of Sony's online services

were out of commission for weeks. According to a Sony financial report [12], the attacks suffered by the company in 2011 have had the following economical impact:

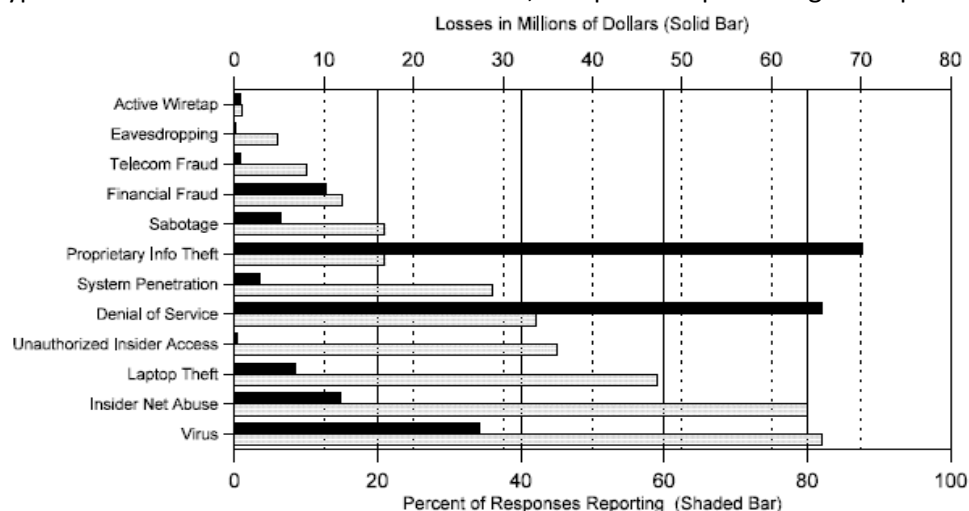
- United Kingdom Government imposed a \$395,000 fine to Sony.
- Damages were valued at more than 170 million dollars (not taking into account financial penalties awarded in each country as exemplified above).
- Sony offered its affected users an insurance coverage of up to a million dollars per customer in case they suffered information theft involving economic losses for them.

Several investigations have been carried out in order to measure the costs/benefits of investing in security and privacy. A CRS report for the US Congress [11] tried to estimate total worldwide losses attributable to virus and worm attacks and to hostile digital acts in general, and will be considered as a reference.

- First, the study found, using the entire set of observations, that firm value was negatively affected by Internet security breaches. Firms affected by the attack experienced an average 2.1% decline in value, relative to unaffected firms.
- Conclusions draw average losses due to different types of attacks:

Type of attack	Average loss in stock value	
	First / Second day	Third day
Simple web site defacing	2%	Rebounded to 1.1%
DoS	2.9%	Declined to 3.6%
Theft of credit card information	0.5%	Declined to 1.5%
Theft of other customer information	9.3%	Declined to 15%.

However, the study also shows that the most frequently reported attacks are not the ones that cause the greatest losses. A more detailed evaluation could be observed in the chart below [11]. It shows different types of attacks and its losses in dollar terms, compared to percentage of reported attacks.



5.2 What are the required economic considerations?

5.2.1 Economic-Specific Template Content Description

In order to guarantee economic feasibility it is necessary to assess the economic constraints that enable the successful marketability of the product. These constraints, expressed as requirements within this document, aim to evaluate the conditions under which a product ceases to be a worthwhile investment and poses limits on the success of the project. These requirements also represent the features of the market that need to be closely monitored or evaluated as they can impose an economic impact on the project. The nature of these latter issues makes them highly unquantifiable until the solution is placed on the marketplace, but the conditions that would trigger a substantial economic impact need to be clearly identified beforehand.

Constraints

The limits mentioned in this requirement address minimums or maximums on the economic feasibility which will thereafter be evaluated by the Fit Criterion. As such, a limit could be that the return on investment yields positive results after X years, or that the rate of return does not become negative at any stage in the first 5 years of the product's life.

Fit Criterion Suggestions

Each type of requirement will have its own quantifiable approach in order to evaluate the limits suggested, such as a predictive cost/benefit analysis to evaluate the return on investment, or an analysis of the internal and external rates of return to evaluate the limits on the payback period. These approaches will be taken into account in the Exploitation Plan, D6.2.1. An economical study is not expected here as this will make part of the evaluation of the project at a later stage. The criteria used to evaluate the more unquantifiable requirements are the conditions that would lead to the monitored effects resulting in a noticeable economic impact, such as government involvement in a non-competitive public/private marketplace or a loss of relations between cooperating partners.

5.2.2 Requirements

Requirement #: 5301	Use Case: V2I, V2V, e-voting
Description: Expensive solutions will not make it to the market	
Constraint: N/A	
Fit Criterion: <ul style="list-style-type: none"> Efficient solutions keep economic aspects in mind. The implementation of policies such as those that will be proposed in Inter-trust should cover all the needs of the services, but these should not raise the cost significantly in order to maintain a competitive advantage. 	
Dependencies: N/A	Conflicts: N/A
Revision History	

Created on: 14/02/2013		Created by: Leyre Merle
Revised on:	Revised by:	Revision changes:

Requirement #: 5302	Use Case: V2I, V2V, eVoting
Description: Risks must be identified and prioritized attending to its likelihood and economic impact.	
Constraint: Suppression of risks with a high likelihood and high economic impact. Mitigation of both risks with high likelihood and medium economic impact, and risks with medium likelihood and high economic impact.	
Fit Criterion: <ul style="list-style-type: none"> • It is too costly to protect against every threat, so it is necessary to rank risks in order to prioritize countermeasures and invest in the most harmful ones. Need to estimate the probability for specific intrusions and their consequences and costs. Trade-off towards the corresponding costs for protection. • All the attacks whose occurrence considered of medium to high likelihood should have an estimated cost analysis per x users. 	
Dependencies: N/A	Conflicts: N/A

Revision History		
Created on: 14/02/2013		Created by: Leyre Merle
Revised on:	Revised by:	Revision changes:

Requirement #: 5303	Use Case: V2I, V2V, eVoting
Description: Information collected will not be used to benefit any party other than those explicitly involved in the operation of the service.	
Constraint: N/A	
Fit Criterion: <ul style="list-style-type: none"> • Careful isolation of service databases must be maintained so that data obtained as part of this service does not end up being marketed for another solution or sold or otherwise delivered to a third party. 	
Dependencies: N/A	Conflicts: N/A

Revision History		
Created on: 14/02/2013		Created by: Leyre Merle
Revised on:	Revised by:	Revision changes:

5.3 Impact

5.3.1 Types of Impact

The impact that results from the implementation of the Inter-Trust economical requirements is expected to be relatively high, since without basic economic feasibility it would be wasteful to sell a product or service. Despite the very important impact, unlike legal or social events, this is only manifested in one way, through monetary losses to the owner of the product/service.

Monetary/Financial Losses

The high importance of this type of impact must not be underestimated as it is often tied in to the basic success of the service or product. Estimates of the basic mechanisms that can incur a monetary loss or gain due to security issues are largely covered in previous sections. However, all these factors can lead to a product or service that no longer generates a profit, virtually guaranteeing its failure. In the Inter-Trust context, profitability is assumed if the solution's cost plus the cost of a security incident is less than the cost of an identical security incident. The main impact of this economic requirement is guaranteeing that this condition holds.

5.3.2 Impact of Requirements

Requirement Number	Impact
5301	One of the basic requirements for economic feasibility is that the cost of the security solution does not exceed that which would be gained without it. Thus this requisite has a high impact and will also determine a minimum point at which the Inter-Trust solution is feasible. Furthermore, it will give a good indication of the profitability of the solution as it is scaled.
5302	In order to focus on the most effective solution there is a need to identify the risk that each security event has, and to estimate the cost of this attack. This should have a considerable impact, as not only will it highlight the most likely security events and assess the effects of each one, but also allow for an action strategy that takes this into account and can enforce the appropriate measures to mitigate damage based on expected costs. This will allow each service to enact the least costly solution, highlighting the value of the Inter-Trust framework.
5303	Although some legal frameworks allow for the sharing of customer data to other parties, within Inter-Trust this is seen as causing greater harm (in terms of a negative public response) than the profits it can bring. This requirement has little impact on Inter-Trust except in countries where this requirement is enforced by law.

6 Summary and Conclusions

The security industry is rapidly evolving as the world becomes increasingly connected and pervasive threats from all over the world become a commonplace characteristic of the internet. Furthermore, the current legal framework surrounding cybersecurity is seen by many as antiquated and inappropriate for the modern security paradigms that do not abide by borders or national jurisdictions and where anonymity is a de facto state for most attackers. Recent scandals in the tech industry, where the privacy of users was seriously compromised, have also generated a great user interest in cybersecurity as well as a further legislative push. It is therefore assumed as likely that the requirements within this document will change throughout the duration of Inter-Trust, as the legal and social requirements are expected to change in the following years (and in turn this will modify the costs related to the economical requirements). In order to track these expected changes, the requirements have been designed to accommodate for easy editing and a revision tracker is included so that this document may act as both a reflection of the most up-to-date legal, social and economic considerations, as well as a log of the changes that have been experienced in these fields.

This first deliverable resulting from Task 2.5 – Legal, Social and Economic Requirements and Constraints, has gathered an initial but comprehensive set of requirements. Within them are all the relevant legal boundaries, particularly those of the V2V, V2I and eVoting use case scenarios, a set of social best practices designed to best deal with any social response to a security incident, and a collection of economic indicators that are essential to evaluate any security system from a financial point of view. Together with the functional and non-functional design requirements gathered in Task 2.1 – Hierarchical Requirements Engineering, the elicitation of requirements has been gathered for the Inter-Trust project and will be updated accordingly. This document has also been written to act as an example and guide of the specific requirement elicitation process that those using the Inter-Trust framework in the future should carry out.

7 References

- [1] K. Brannon, W. Weigel. “*Establishment of Category A liaison between ISO/TC 204 and ETSI TC ITS*”. Official email correspondence. 20th May 2008.
- [2] A. M. McDonald, R. W. Reeder, P. G. Kelley, L. F. Cranor. “*A Comparative Study of Online Privacy Policies and Formats*”. Lecture Notes on Computer Science, Springer.
- [3] P.G. Leon, B. Ur, R. Balebako, L. F. Cranor, R. Shay, and Y. Wang. “*Why Johnny Can’t Opt Out: A Usability Evaluation of Tools to Limit Online Behavioral Advertising*”. Carnegie Mellon University CyLab Technical Report. October 31st 2011.
- [4] Kaspersky Labs. “*Digital Consumer Online Trends and Risks*”. Russia 2012.
- [5] S. Sheng, M. Holbrook, P. Kumaraguru, L. Cranor, J. Downs. “*Who Falls for Phish? A Demographic Analysis of Phishing Susceptibility and Effectiveness of Interventions*”. China 2010.
- [6] TNS Opinion & Social at the request of the European Commission, Directorate-General Home Affairs. “*Special Eurobarometer 390*”. Wave EB77.2. July 2012.
- [7] J. A. Chaula, L. Yngström, and S. Kowalski. “*Security Metrics Evaluation of Information Systems Security*”. Department of Computer and System Sciences, Stockholm University. Forum 100, 164 40 Kista, Sweden.
- [8] M. Hachman. “*Playstation Hack to Cost Sony \$171M; Quake costs much higher*”. PC Mag. May 23rd 2011. Retrieved from <http://www.pcmag.com/article2/0,2817,2385790,00.asp>
- [9] Ponemon Institute. White paper on “*2011 Cost of Data Breach Study: United States*”. March 2012. Retrieved from
- [10] McAfee. “*McAfee Secure Website Certification Leads to Increased Sales*”. Data Sheet 2012. 2821 Mission College Boulevard Santa Clara, CA 95054.
- [11] B. Cashell, W. D. Jackson, M. Jickling, and B. Webel. “*The Economic Impact of Cyber Attacks*”. Congressional Research Service Report for Congress (USA), Order Code RL32331, 1st April 2004.
- [12] Sony. “*Consolidated Financial Report for the Fiscal Year Ended March 31st, 2011*”. In Sony News and Information, No.11-060E, 1-7-1 Konan, Minato-ku, Tokyo 108-0075 Japan.
- [13] I. Hargreaves. “*Digital Oportunity – A Review of Intellectual Property and Growth*”. May 2011. United Kingdom.
- [14] E. Yu, P. Giorgini, N. Maiden, J. Mylopoulos. “*Social Modeling for Requirements Engineering*”. October 2010. MIT Press.
- [15] S. Viller, I. Sommerville. “*Social Analysis in the Requirements Engineering Process: From Ethnography to Method*”. Proceedings of the 4th IEEE International Symposium on Requirements Engineering, p.6-13, June 07-11, 1999.

- [16] SeVeCom. “VANETs Security Requirements, Final Version, Deliverable 1.1”. 2006. Retrieved from <http://www.sevecom.org>.
- [17] SeVeCom. “Secure Vehicular Communications: Security Architecture and Mechanisms for V2V/V2I, Deliverable 2.1”, 2007-2008. Retrieved from <http://www.sevecom.org>.
- [18] PRESERVE. “Security Requirements of Vehicle Security Architecture, Deliverable 1.1”. June 2011. Retrieved from <http://www.preserve-project.eu>.
- [19] Cisco Systems. White Paper on “Recovery after a breach in Network Security”. 2001. Retrieved from http://www.cisco.com/warp/public/cc/so/neso/sqso/roi3_wp.pdf.
- [20] E. Q. Freeman, B. Beeson. Lockton White Paper titled “Exposed in Europe”. 2011. Retrieved from http://www.lockton.com/Resource_/InsightPublication/1980/Exposed%20in%20Europe%20to%20post.pdf.
- [21] Ponemon Institute. White paper on “2012 Confidential Documents at Risk Study”. July 2012. Retrieved from <http://info.watchdox.com/Ponemon.html>.
- [22] Ponemon Institute. White paper on “2013 State of the Endpoint”. December 2012. Retrieved from http://www.ponemon.org/local/upload/file/2013%20State%20of%20Endpoint%20Security%20WP_FINAL4.pdf.
- [23] Watchdox. White paper on “Top 5 Reasons Why Security Fails”. 2012. Retrieved from <https://www.watchdox.com/doc?a=ov&c=a8Lv2BHadtq2Y.spyKiCfcA&eov=t>.

Annex.A Basic Requirement Form Guide

Below is a basic template of the requirement form with all the generic elements that can be found throughout all forms in the legal, social and economic requirement gathering. Brief descriptions of the content expected in each section are included in red.

Requirement #: Unique requirement identifier, to follow agreed upon numbering convention.		Use Case: Include the use case or use cases to which this requirement applies to.
Description: Brief description of requirement.		
Fit Criterion: This area is to be filled with the conditions that need to be monitored in order to guarantee compliance with the requirement. These conditions are of a wide and varied nature, even for requirements within the same category. As such, suggestions on how to complete this section are included just before each set of individual requirements (Sections 3.2.1, 4.2.1 and 5.2.1) <ul style="list-style-type: none"> • 		
Dependencies: Include any other requirements that have a dependency on this requirement. Use the requirement number.		Conflicts: Include any other requirements that impose a conflict on this requirement. Use the requirement number.
Revision History Blank		
Created on: Date the requirement was created.		Created by: Name of person that created it.
Revised on: Date of revision	Revised by: Named of the person who made the revision.	Revision changes: Description and rationale for changes to be included here.

The Requirement # value is compiled as followed:

- 51XX – Legal requirements
- 52XX – Social requirements
- 53XX – Economic requirements

With the XX values ranging from 01 to 99 and assigned in the order they are added to this document.