


	<h1 style="text-align: center;">Global System for Telematics</h1>
<h2 style="text-align: center;">Release</h2>	<h2 style="text-align: center;">DEL SEC 7.5: Technology Implementation Plan</h2>

<b>Author(s)</b>	Antonio Kung (Trialog)			
<b>Date</b>	<i>Contractual:</i>	28/02/2007	<i>Actual:</i>	15/12/2006
<b>SP Manager</b>	Antonio Kung Trialog Tel: 00 33 1 44 70 61 00 E-Mail: antonio.kung@trialog.com			
<b>IP Manager</b>	Peter Van der Perre ERTICO-ITS EUROPE Tel: +32 2 400 07 36 E-Mail: p.vanderperre@mail.ertico.com			

<b>Abstract</b>	Technology Implementation Plan (TIP).
<b>Keyword list</b>	GST, Exploitation.
<b>Nature of deliverable</b>	Report
<b>Deliverable Number</b>	DEL_SEC_7_5
<b>Version</b>	1.0
<b>Dissemination</b>	PP

<b>Project financially supported by</b>	
	European Union DG INFSO
Project number FP6-2002-IST-1-507033	

## Control sheet

<b>Version history</b>			
<b>Version number</b>	<b>Date</b>	<b>Main author</b>	<b>Summary of changes</b>
0.1	20.Aug.2006	Antonio Kung	Creation
0.3	13.Nov.2006	Antonio Kung	Additional Interviews
1.0	13.Nov.2006	Antonio Kung	Finalisation
<b>Approval</b>			
	<b>Name</b>	<b>Date</b>	
Prepared	Antonio Kung	6.Dec.2006	
Reviewed	GST SEC Partners	7.Dec.2006	
Authorized	Antonio Kung	8.Dec.2006	
<b>Circulation</b>			
	<b>Recipient</b>	<b>Date of submission</b>	
	Project partners	15.Dec.2006	
	European Commission	15.Dec.2006	

## Table of Contents

<b>CHAPTER 1 - INTRODUCTION.....</b>	<b>4</b>
<b>CHAPTER 2 - EXECUTIVE SUMMARY .....</b>	<b>5</b>
<b>CHAPTER 3 - OVERVIEW .....</b>	<b>6</b>
<b>Introduction.....</b>	<b>6</b>
3.1.1    SEC Scope .....	6
3.1.2    The SEC Sub-project Goals.....	7
3.1.3    High-level Architecture and Exploitation of Results.....	7
3.1.4    Overview of Expected Results.....	12
3.1.5    Approach to Dissemination and Use.....	12
3.1.6    Market Situation and Overview .....	13
3.1.7    Business Model Considerations.....	13
<b>CHAPTER 4 - DESCRIPTION OF DISSEMINATION PLAN.....</b>	<b>15</b>
<b>CHAPTER 5 - DESCRIPTION OF USE PLAN .....</b>	<b>16</b>
<b>Result No 1: Final Architecture and Interface Specifications (DEL_SEC_3_1).</b>	<b>16</b>
<b>Result No 2: Reference Implementation Components (DEL_SEC_3_2).....</b>	<b>16</b>
5.1.1    Description and Characterisation of Result .....	16
5.1.2    Market Characterisation.....	16
5.1.3    Approach, Timing and Estimated Effort for Use of Result .....	17
<b>Result No 3: Validation Results (DEL_SEC_6_2) .....</b>	<b>17</b>
5.1.4    Description and Characterisation of Result .....	17
5.1.5    Market Characterisation.....	17
5.1.6    Approach, Timing and Estimated Effort for Use of Result .....	18
<b>CHAPTER 6 - TRUST VALUE CHAIN ROADMAP.....</b>	<b>21</b>
<b>Deployment Stages on the Security Roadmap.....</b>	<b>21</b>
<b>Stage 1 – INITIAL .....</b>	<b>21</b>
<b>Stage 2 – ESTABLISHED .....</b>	<b>22</b>
<b>Stage 3 – FUTURE DEVELOPMENTS .....</b>	<b>22</b>
<b>CHAPTER 7 - INTERVIEWS.....</b>	<b>23</b>
<b>Interviewee 1: (Philippe Robin, Trialog) .....</b>	<b>23</b>

## Chapter 1 - INTRODUCTION

---

### Intended Audience

This document is primarily written for the members of the GST SEC SP. It will be circulated to members of the IPWP7MT, CT, CAG and SC for IP-level coordination purposes. The final version will be sent to the EC and GA.

### Organisation

This document consists of the following sections:

- Executive Summary
- Overview
- Description of Dissemination Plan
- Description of Use Plan
- Roadmap
- Interviews

### Typographic Conventions

The following typographic conventions are used in this document:

A word starting with a capital letter      Indicates a specific term explained by the appendix Terms and abbreviations

*Code Examples*

Code examples are printed in a courier font

*C:\Project\MyCode.c*

Filenames are represented in a courier italic font.

***Locales***

Words that have a specific meaning are printed in an italic bold font

[1]

Numbers in-between square brackets are references to publications mentioned in the appendix References.

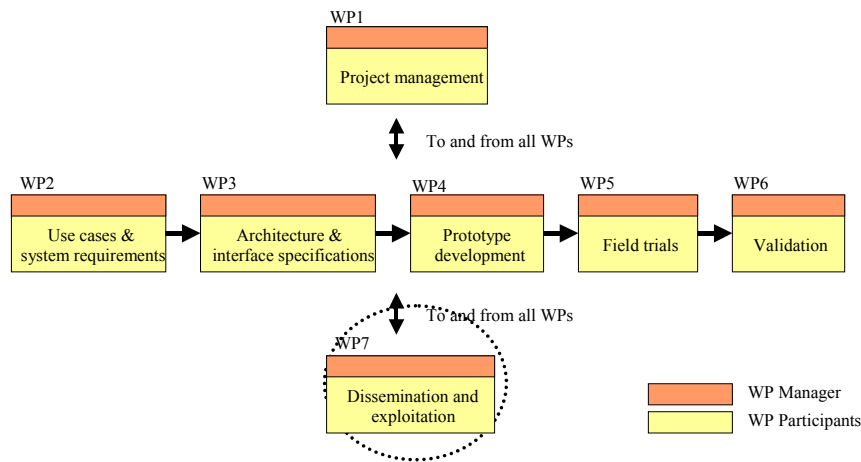
### Objectives

The objectives of this document are:

- To document the SP-level dissemination plan for GST SEC;
- To document the SP-level use plan for GST SEC.
- To suggest a roadmap.
- To provide some insight on exploitation managers view through interviews.

## Chapter 2 - EXECUTIVE SUMMARY

This document presents the Technology Implementation Plan (TIP) within Work Package 7 “Dissemination and Exploitation” for the GST project, at SEC SP-level (DEL\_SEC\_7\_5).



**Figure 1 - Sub-project Components**

The TIP is the final deliverable of WP7. It follows an earlier deliverable in the WP, the Communication Plan (DEL\_SEC\_7\_1) and the Dissemination and Use Plan (DUP, DEL\_SEC\_7\_4).

As such, it consist of five parts:

- An overview chapter
- A chapter on the dissemination plan
- A chapter on the use plan
- A chapter on roadmap
- A chapter on interviews

### Notes

*The SEC sub-project collaborates with 6 other sub-projects within GST, that represent different competence domains and may develop specifications on which the SEC sub-project relies. To understand the overall system in which SEC operates as well as possible links with other sub-projects, this document must be read together with the current version of the IP-level deliverable.*

## Chapter 3 - OVERVIEW

---

### Introduction

The SEC sub-project is part of the overall GST project, which is a shared-cost Integrated Project (IP) within the EU's 6<sup>th</sup> Framework R&D Programme running from 1<sup>st</sup> March 2004 to 1<sup>st</sup> March 2007.

The main objective of the GST project is to create and establish a common technical, operational and business framework for the Europe-wide deployment of open telematics platforms and services by implementing, testing and validating a common architecture and interface specifications at 7 trial sites across Europe seeking full interoperability.

Within GST, SEC is focussing on security aspects.

Dissemination activities play an important role within GST and SEC with the following overall objectives:

- To ensure an as wide as possible dissemination of the project results by identifying and reaching all interest groups with the dissemination,
- to establish a Forum where the projects results can be disseminated and discussed through Forum workshops,
- to organise and attend meetings to liaise with related projects and initiatives and
- to follow-up standardisation activities and submit standardisation proposals to the relevant bodies as an outcome of the project.

The objectives are being met via various dissemination activities linking all actors involved in the development and validation of the SEC modules. They include a. o.:

- Establishing a project website at project start <http://www.gstproject.org/sec>,
- preparing updated fact sheets and standard presentations during the project, representing the current state of the project progress,
- preparing a brochure and possibly CD-ROM at the end of the project to disseminate the final results of the project,
- making contributions to national and international magazines,
- participating in key events to inform stakeholders of progress made in the project.

The industrial actors involved in GST intend to widely deploy the GST solutions provided that GST achieves to meet the user needs and high-level system requirements identified in its user needs analysis and that it can reach industry consensus.

*The GST consortium believes that its results can help to transform the market for on-line services from a closed market based on proprietary approaches to an open one based on public standards. As such, the potential market for the GST solution is huge as we believe that all vehicle manufacturers could at one point in the future decide to factory-install GST-compliant terminals in their vehicles (according to ACEA, about 16 million new cars are sold in Europe every year). These will give access to a wide range of services that will continuously evolve and create a new market for service providers.*

### SEC Scope

Security addresses the following problems related to future security and trust infrastructures for Telematics:

- Security: The customer can expect that systems are resilient to attack, and that the confidentiality, integrity and availability of the system and its data are protected.
- Privacy: The customer is able to control data about themselves, and those using such data adhere to fair information principles.
- Reliability: The customer can depend on the product to fulfill its functions when required to do so.
- Adaptation to Vehicle Usage.
- Trust value chain and business Integrity

None of the above is true to date. When they are addressed in existing systems of today they are either adhoc/proprietary solutions or even solutions which are inherently flawed. These today systems are still deployed because (1) of the small scale of deployment, (2) because of the lack of awareness of the industry.

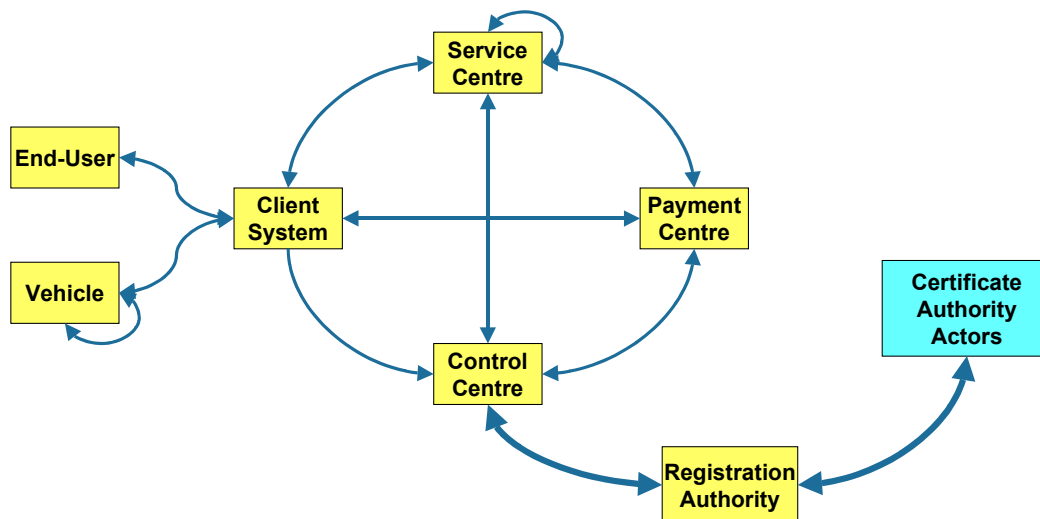
### ***The SEC Sub-project Goals***

The Security sub-project are the following :

- Define an architecture and provide security mechanisms for secure telematics applications.
  - functional point of view (applications, services, user devices)
  - infrastructure point of view (networks, platforms)
- Define roadmap for a trust value chain including certification requirements

### ***High-level Architecture and Exploitation of Results***

Figure 2 shows the GST high-level architecture as well as the visible impact in terms of security : an entity called registration authority is needed to interface with certificate authority stakeholders



**Figure 2 - Impact of SEC on GST High-level Architecture**

Figure 3 and Figure 4 shows a detailed version of the GST high-level architecture. In GST, all relationships between GST entities are called reference points (blue arrows).

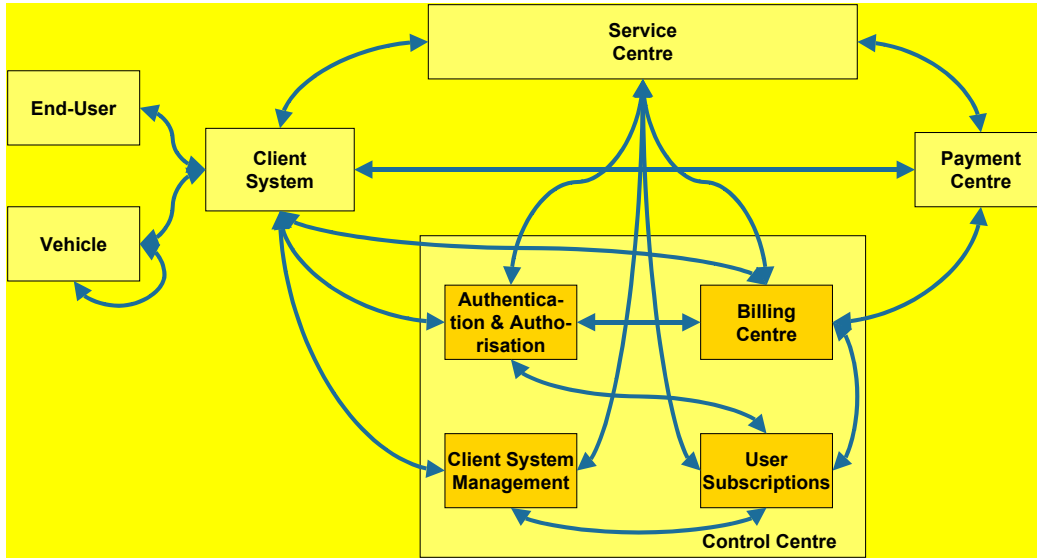


Figure 3 - Detailed GST High-level Architecture

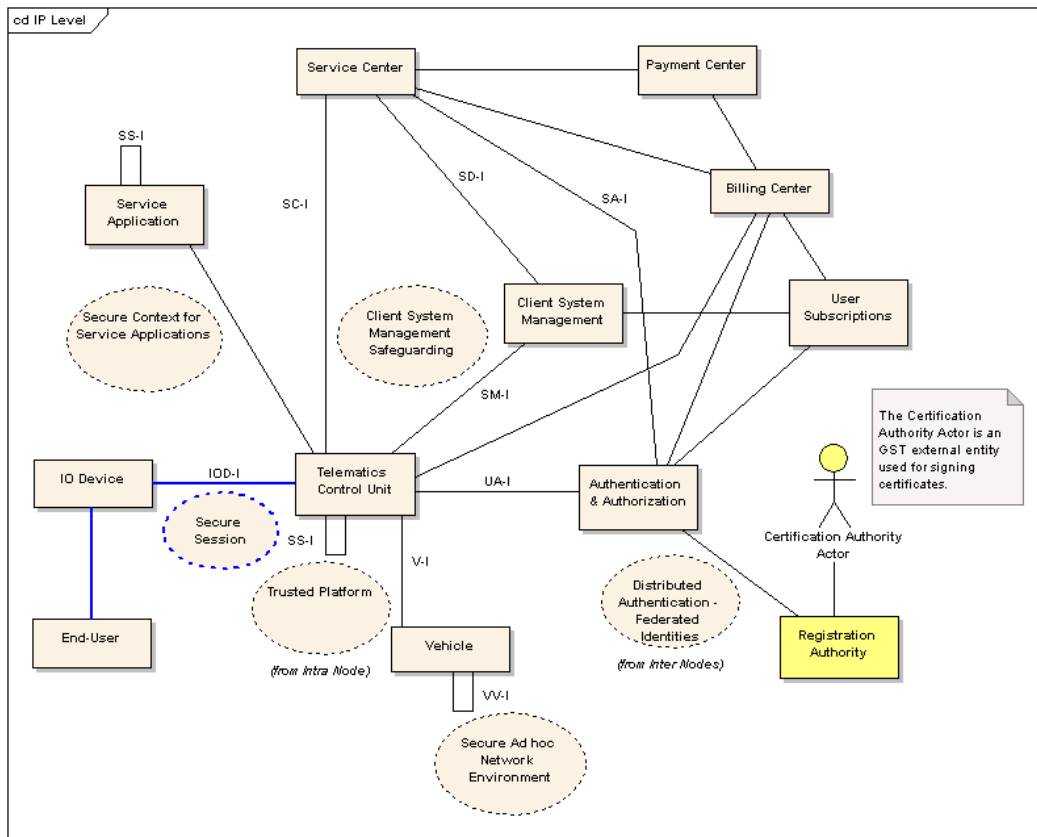
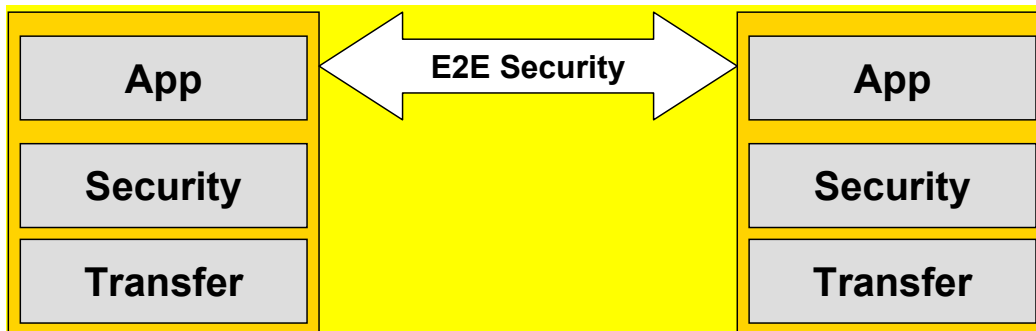


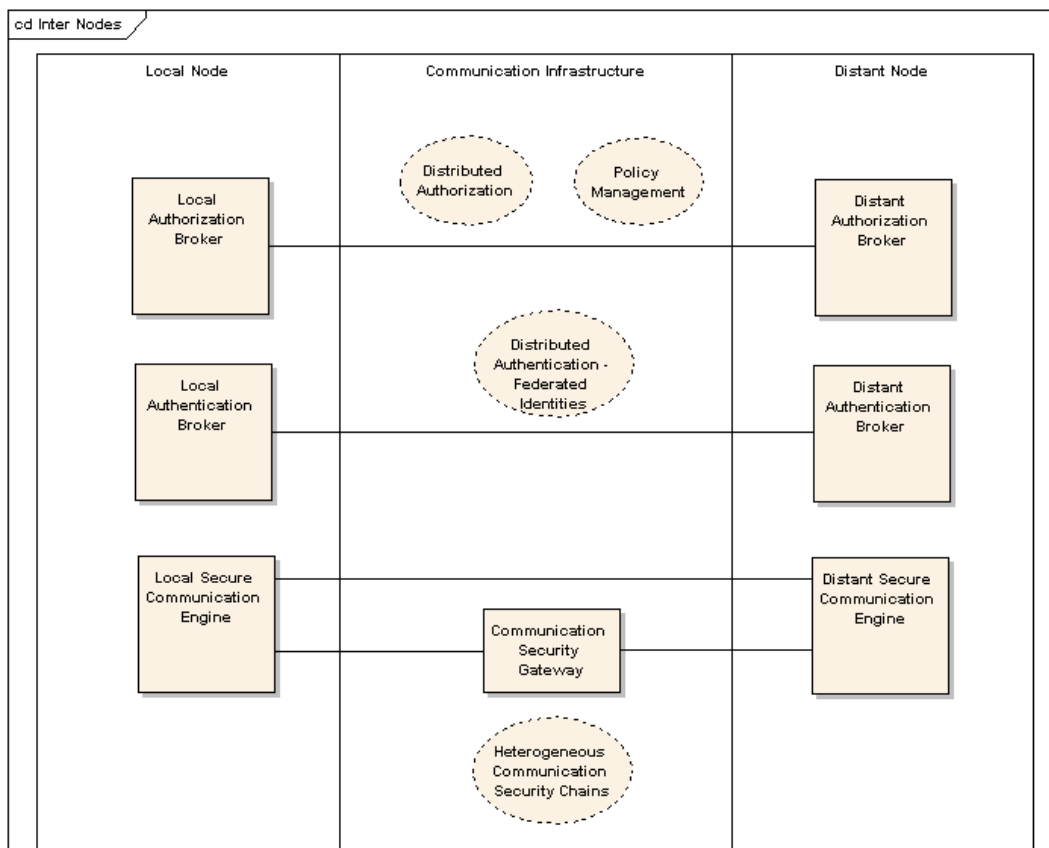
Figure 4 - Detailed GST High-level Architecture (IP Level Version)

In terms of architecture SEC is further focusing on

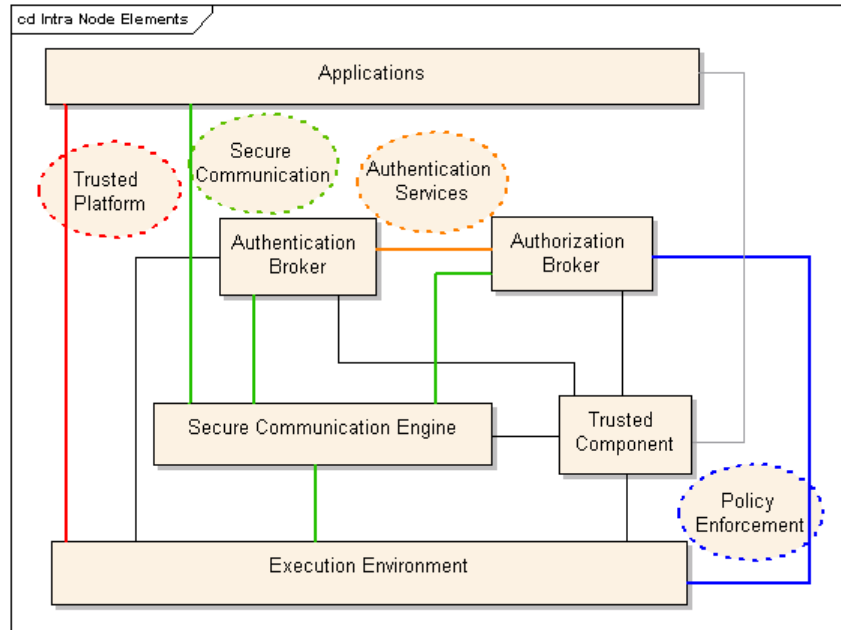
- a layered based security architecture (for communication at the level of references) as showed in Figure 5 (global representation) and in Figure 6 (SEC Architecture at the Internode level)
- the generic architecture at the node level as showed in Figure 7, as well as a decomposition of the trusted component entity in Figure 8



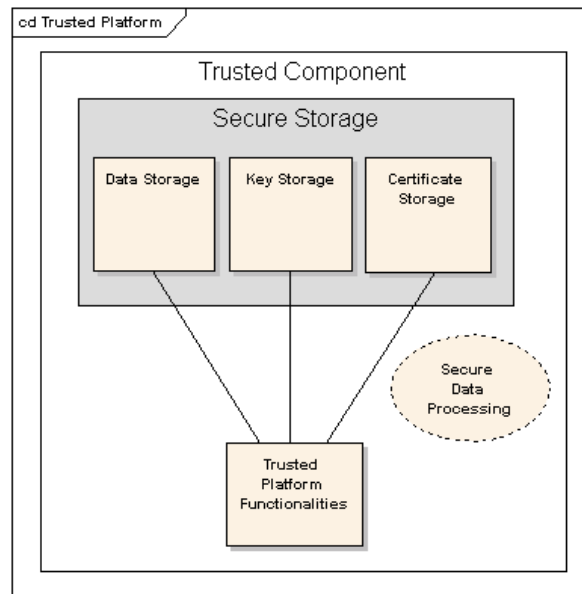
**Figure 5 - Layered-based Security Architecture**



**Figure 6 - Inter Nodes level**














**Figure 7 - Intra Node level**



**Figure 8 – Decomposition of the Trusted Component Entity**

Requirement identification work carried out in SEC led to the identification of a number of collaboration focus points in the architecture. They are showed in the table below, along with the partners in SEC which has an interest in the collaboration.

Collaboration	Partners
Authorization - distributed Authorization	 TECHNISCHE UNIVERSITÄT MÜNCHEN
Authorization - policy enforcement	
Authorization – policy management	 TECHNISCHE UNIVERSITÄT MÜNCHEN
Authentication - authentication services	
Authentication - federated identities	
Communication - secure communication	
Communication - heterogeneous chain	
Communication - adhoc network	 TECHNISCHE UNIVERSITÄT MÜNCHEN
Execution platform - client system management safeguarding	DAIMLERCHRYSLER
Execution platform - secure context for service applications	
Execution platform - secure data processing	
Execution platform - secure session	GST OS
Execution platform - trusted platform	

### Overview of Expected Results

The project will produce the following results:

	Result	Short description	Date
1	Final architecture and interface specifications (DEL_GST_3_2)	Overall architecture, specifications for interfaces between control centres and services resp. control centres and terminals a.o.	December 2006
2	Initial SEC Framework architecture and interface specifications (DEL_SEC_3_1)	SEC specific architecture <ul style="list-style-type: none"> <li>• Based on Trusted Components</li> <li>• Based on Middleware Approach</li> <li>• Support Trusted Domains</li> </ul>	July 2006
3	Reference Implementation (DEL_SEC_3_2)	Reference Implementation <ul style="list-style-type: none"> <li>• Client System Middleware Based on OSGi, with a trusted component</li> <li>• Control Centre/Service Centre Middleware</li> </ul>	October 2005
4	Validation Results (DEL_SEC_6_2)	Including trust value chain associated with a certificate authority hierarchy	December 2006

Table 1 - Overview of Results

### Approach to Dissemination and Use

The overall objectives for the dissemination and use task within SEC are formulated as follows:

- To establish effective mechanism for continuous communication and dissemination
- To follow-up standardisation activities and submit standardisation proposals to the relevant bodies as an outcome of the project
- To organise and attend meetings to liaison with related projects and initiatives
- To support the organisation of GST Forum events
- To help ensure that SEC results will be fully exploited.

The target groups of the SEC dissemination activity have been the following:

- Car manufacturers
- Service platform technology provider
- Middleware providers
- Terminal manufacturers.

The more detailed dissemination activities as part of WP7 of SEC are out as follows:

- Participate to the GST Forum consisting of both project participants and non-project participants. Invite vehicle manufacturers, service platform technology providers, middleware providers, terminal manufacturers, and others that could have an interest in the project and that could contribute to the findings.
- Set-up a project web site, which documents project objectives, activities and results. Keep the web site up-to-date. Provide a specific area for project participants only as a consortium-internal document archive.

- Participate to the GST three newsletters to inform a wider audience of the objectives, progress and results of the GST project: a first newsletter communicating the results of the GST user needs analysis, a second communicating the technical specifications development and finally the third newsletter informing about field trials and validation results.
- Participate to the preparation of a take-up brochure and CD-ROM at the end of the project to disseminate GST's final results and recommendations.
- Present SEC achievements regularly at national and international magazines, seminars and workshops (paper abstracts submitted to AAET2005, ITST 2005).
- Liaise actively with other security initiatives. In particular, at the level of IST, a liaison with other security projects has been created via the SecurIST transverse collaboration project (Trust and Security unit).
- Liaise actively with all relevant standardisation bodies and industry associations, such as: CEN, ETSI, ISO, Telematics Forum, AMI-C and MOST.
- Organise and attend meetings to liaise with related projects and initiatives.
- Create the necessary international co-operation.

The more detailed activities related to the use of results as part of WP7 of SEC are to develop a communication plan, a dissemination and use plan and a technology implementation plan seeking information on how the consortium seeks to use the achieved results.

### **Market Situation and Overview**

Security is a transversal consideration to telematics applications.

As stated in the IP level deliverable, *"the telematics deployment in Europe is currently characterised by a limited take-up of in-vehicle platforms, that are only partially based on public, open specifications and that therefore come across as rather closed systems. Bi-lateral agreements are made between specific service providers and terminal manufacturers implementing only a limited number of functions. In this situation, referred to earlier as second-generation telematics, the different stakeholders attempt to dominate the market with their specific approach creating in effect a fragmented market based on incompatible systems"*

The GST project in itself helping to overcome the difficulties that are behind this limited take-off. We would like to point out the following on the market :

- Because of the limited take-off of telematics applications, security has not been a priority until now, with adhoc solutions being deployed when needed.
- A prerequisite for massive deployment of telematics applications is the use of a suitable security architecture as well as a trust value chain as investigated in GST SEC
- In the mid term, opportunities to market GST SEC results will also depends on a roadmap from a small market with proprietary solutions to a big market with open solutions. This roadmap and the resulting prioritization of security exploitation results is still being shaped up in the project

### **Business Model Considerations**

In terms of potential business and business models, we foresee the following :

- Exploitation of intellectual property created in GST SEC in the course of demonstrating the security architecture defined in GST SEC (security middleware, trusted component wrappers, ...).
- Consulting activities in helping implement / modify code of practices related to security in the area.
- Activities related to the trust value chain (security evaluation, certification ...)

## Chapter 4 - DESCRIPTION OF DISSEMINATION PLAN

---

Please refer to an earlier deliverable in the WP, the Communication Plan (DEL\_SEC\_7\_1), that has been updated and extended in a new release of the deliverable rather than duplicating its content here.

The content of the (IP and SP-level) Communication Plans is as follows:

- Introduction
  - Intended audience
  - Organisation
  - Typographic conventions
  - Reference documents
  - Terminology
  - Purpose of document
  - Contractual references
  - Project purpose
- Executive summary
- Introduction and practical information
  - Project abstract
  - Organisation of communication activities in overall SP structure
  - Role and responsibilities of the Communication Manager
  - Approval procedures
  - Key personnel
- Communication strategy
  - Communication objectives
  - Communication sources
  - Project identity
  - Communication channels/media
  - Project stakeholders and communication channels
  - Highlights and deliverable planning
- Potential additional communication activities.

## Chapter 5 - DESCRIPTION OF USE PLAN

---

In this section, a first indication is given on how the GST SEC results are likely to be used.

### Result No 1: Final Architecture and Interface Specifications (DEL\_SEC\_3\_1)

In parallel to the GST deliverable on architecture and interface specifications (DEL\_GST\_3\_2)

In particular, SEC architecture further focuses on the following aspects :

- Use of trusted components and interfacing them
- Use of a middleware approach
- Support Trusted Domains

For the rest, refer to GST level deliverable.

### Result No 2: Reference Implementation Components (DEL\_SEC\_3\_2)

#### *Description and Characterisation of Result*

SEC reference implementation will include items/components which individually or combined will have exploitation potential. The current list that might be enriched or slightly modified depending on finalised priorities in GST include:

- Client System Middleware Based on OSGi, with a trusted component
- Control Centre/Service Centre Middleware
- Security part of Middleware
- Specific Wrappers to existing trusted components
- Specific Wrapper to existing systems (e.g. possibly Embedded Finread Component, Liberty alliance component,...)
- Possible modifications/contributions to initiatives (e.g. OSGi framework, OSGi bundles)

#### *Market Characterisation*

GST SEC addresses a derived market in the value chain, the OEM market that will allow some stakeholders to deploy infrastructures with security features. More precisely :

- Client System Middleware Based on OSGi, with a trusted component would be useful to OEM companies manufacturing client systems (i.e. telematics control units).
- Control Centre/Service Centre Middleware would be useful to platform integrators.

- Security part of Middleware would be useful to client system and service platform integrators
- Specific Wrappers to existing trusted components would be useful to client system and service platform integrators
- Specific Wrapper to existing systems (e.g. possibly Embedded Finread Component, Liberty alliance component,...) would be useful to client system and service platform integrators
- Possible modifications/contributions to initiatives (e.g. OSGi framework, OSGi bundles) would be useful to technology providers

### ***Approach, Timing and Estimated Effort for Use of Result***

The approach is as follows

- Car manufacturer to promote, standardise and recommend results from project
- Technology partners to promote, standardise exploit the results
- Academic partners to promote, standardise, and use the results in other research work

The timing is related to the telematics deployment timing.

The associated effort for use of the results is the following

- Product quality iteration and possibly standardisation driven modification for technology partners
- Academic partners to reuse results right away

### **Result No 3: Validation Results (DEL\_SEC\_6\_2)**

A major results from validation effort will be a consolidated definition of a trust value chain as described below.

#### ***Description and Characterisation of Result***

The result is a code of practice. This means that the following can be exploited in the future :

- Evaluation and certification consulting and tools
- Evaluation and certification activities

#### ***Market Characterisation***

The need for a trust value chain is very important in particular in the automotive industry where liability issues are crucial. The automotive supply value chain involves a very demanding business relationships with suppliers as they are liable for huge compensation related to detected defects. This also means that separation of roles, concerns and responsibilities in the value chain must be crystal clear. The cost of recalling vehicles upon defects is so high that the cause of such defects must be absolutely be identified so that the car manufacturer can share or transfer liability to other stakeholders in the value chain (i.e. the supplier that provided the component with a defect).

In order to limit the occurrence of such defects, validation approaches might be defined and required. Conformance/Evaluation/Certification mechanisms could be put in place.

As of today the automotive industry has no real experience on the trust value chain that should be associated with the deployment of a telematics infrastructure such as the one GST is assuming.

We foresee an iterative process whereby GST SEC results on the trust value chain definition will be the starting point.

***Approach, Timing and Estimated Effort for Use of Result***

The approach is to publish the trust value chain definition, and to provide feedback on its use at a limited scale (simulation, prototyping) at the GST level.

The timing for trust value chain adoption depends on the telematics deployment roadmap.

The trust value chain definition result is readily usable as the first step of a dynamic process.

Items (about the results)	Actual current quantity <sup>a</sup>	Estimated (or future) quantity <sup>b</sup>
Time to application / market (in months from the end of the research project)	12-36 months	
Number of (public or private) entities potentially involved in the implementation of the result :	GST consortium (ADSE, ALLIANZ, AVE, BMW, BOSCH, DAIMLERCHRYSLER, EBU, ERTICO, FIAT CRF, FORD, FRANCE TELECOM, GATESPACE, GEWI, ISMB, KREIS OFFENBACH, KU LEUVEN, MIZAR, MOTOROLA, NAVTECH, OPEL, ORANGE, PENDRAGON, PMI, PROSYST, PTV, Q-FREE, RENAULT, RSA, SES GLOBAL, SIEMENS VDO, SNRA, SUSSEX POLICE, TDF, TUM, TELCORDIA, TELEATLAS , TELECOM ITALIA, TELEMATICS CLUSTER, TELMACON, TNO, TRIALOG, TRUSTED LOGIC, T-SYSTEMS, TUV, VIALIS, VIKTORIA INSTITUTE, VOLVO, WIRELESS CAR.)	All car makers All tier 1 terminal makers All service providers All middleware providers All control centre operators
of which : number of SMEs :	15 (AVE, ERTICO, GEWI, KREIS OFFENBACH, MIZAR, PENDRAGON, PMI, PROSYST, PTV, Q-FREE, TELEMATICS CLUSTER, TELMACON, TRIALOG, TRUSTED LOGIC, WIRELESS CAR)	?
of which : number of entities in third countries (outside EU) :	?	?

Targeted user audience: # of reachable people	100 (Forum members)	?
# of S&T publications (referenced publications only)	-	-
# of publications addressing general public (e.g. CD-ROMs, WEB sites)	5-1 <sup>o</sup>	?
# of publications addressing decision takers / public authorities / etc.	1 (White Paper)	1 (White Paper)
Visibility for the general public	No	Yes (London World Congress)

<sup>a</sup> Actual current quantity = the number of items already achieved to date.

<sup>b</sup> Estimated quantity = estimation of the quantity of the corresponding item or the number of items that you foresee to achieve within the next 3 years.

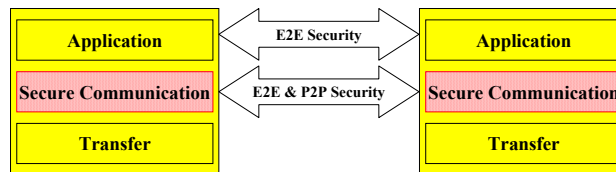
**Table 2 - Overview of Use Elements**

## Chapter 6 - TRUST VALUE CHAIN ROADMAP

### Deployment Stages on the Security Roadmap

Adding security functionality in a GST system means additional costs and complexity with no immediate benefits for system operators and end-users, at least in the first deployments. Yet, as the open market for telematics facilitated by the GST architecture will grow, it will face an increasing level of threats from malevolent individuals and organisations attracted by its very open and pervasive nature. Strong security will thus be required to protect the valuable assets of stakeholders. To establish the necessary security mechanisms as an afterthought in such mature systems is not a viable solution as it will trigger greater costs and expose stakeholders to potential security flaws.

The solution to this dilemma involves an initial architecture design that takes security into account and allows the staged deployment of security in the system following a defined roadmap. GST Security is defining such an infrastructure for secure telematics applications, both from the user and the technology point of view, to allow progressive integration, in a timely and cost-effective manner, of state-of-the-art security technologies and processes that respond to the rising level of threats while protecting the privacy rights of the end-users.



**Figure 9 – Layered Security Architecture**

With this approach, the same standard interfaces to security services are kept for services applications, with a staged introduction of more powerful security mechanisms in the infrastructure according to current market needs and available security technology.

Three different stages have been thus defined, from initial stage of first deployments, through established stage where the open telematics market is widely distributed, to future development stage that consider possible evolutions of initially defined system. For the first two stages, the general situation of the market, the implication on security and the trust value chain are considered. The third stage lists possible evolutions that may occur independently from one another.

The impact of each of these stages on actual security components for GST infrastructure are detailed in the corresponding implementation guides (see Annex C).

### Stage 1 – INITIAL

General market situation:

- Control centres operated by OEMs manage a limited number of client systems.
- Service applications in the client systems are statically installed under direct OEM control

Implications on security:

- Simple or even implicit authentication schemes for users, vehicles and applications.

- Integration of different control centres is still limited.
- OEM specific Public Key Infrastructure (PKI) and identity procurement.

Trust value chain is centred on the OEM operating their dedicated control centres, and controlling the details of both software and services.

## Stage 2 – ESTABLISHED

General market situation:

- Control centres operated by OEMs (and telecom operators, for mobile client systems) with large customer bases.
- Rich offer of telematics services across multiple control centres.

Implications on security:

- Control centre operators rely on stronger end-user authentication technologies and securely manage dynamically-loaded service applications.
- Secured access to services from multiple client systems is simplified via enhanced identity federation schemes.
- Improvement of secure execution levels in client systems with security modules and (possibly) a high-security execution space (for critical applications).
- Agreement within a circle of trust of Public Key Infrastructure (PKI) and identity procurement.

OEMs are still at the centre of the trust value chain, but with progressive involvement of other actors like security technology providers and federated service centres. This creates a need for security certification to establish the respective responsibilities of the actors:

- Conformance testing exists for security plug-ins at standardised interfaces.
- Security certification exists for security modules (FIPS140-2) and possibly for secure execution spaces and critical applications (“Common Criteria”).

## Stage 3 – FUTURE DEVELOPMENTS

A list of potential system and security evolutions that may occur at a later stage is now detailed:

- Control centres operated by third parties with full interoperability of client systems across multiple control centres.
- Standardisation of end-user authentication tokens across the industry.
- Management of multiple, simultaneous users on a single client system.
- Integration of service applications with very strong security constraints.
- Higher integration of circle of trust management schemes with convergence of management and security policies of control centre operators.
- Industry-wide factorisation of Public Key Infrastructure (PKI) and identity procurement leading to a Pan European PKI.

## Chapter 7 - INTERVIEWS

---

### Interviewee 1: (Philippe Robin, Trialog)

#### ***Background***

Philippe Robin is responsible for automotive activities in Trialog. He has 25 years experience, and he is involved in automotive subsystems since 1987. He has considerable experience and insight both at the technical and market level.

#### ***What tangible benefits will this technology bring?***

Security is a transversal feature which is needed for future mainstream telematics application. I simply view this as a prerequisite. No infrastructure, no application can become mainstream if appropriate technology features for security are not available.

#### ***What is the current market situation for this technology?***

Security technology is a growing market in general. I believe that any internet based application or even any communicating appliance will sooner or later include security related technologies. Consider for instance the TCG (Trusted Computing Group) technology which is now deployed by millions already in laptops.

Now in telematics applications, and in eSafety applications in general, I can see that the advent of car to car communication infrastructure will even increase the need for security.

#### ***How do you believe this market segment will evolve in the future?***

There are two stumbling blocks that I can think of that makes it difficult to this market segment to go quickly. On the one side, automotive OEMs cope with a very critical business implying liability (and recall problems). Consequently they are very conservative in making deployment decisions. On the other side, the market segment we are dealing with will involve different stakeholders (such as network operators, service providers) which are not used to work and make business together. This market still has to learn on how to create a value chain.

Consequently, I believe a roadmap including progressive steps for deployment is the only way. I think I can agree with the SEC roadmap.

#### ***What is the specific contribution of the SP to this evolution?***

I believe SEC is a pioneering initiative in that it has created European-wide awareness on security issues both on service-oriented internet-based infrastructure and on telematics platforms architecture (what GST calls the client system). Some of the principles defined in SEC will have a profound impact on the implementation of future such systems.

At a development level, GST has decided to go for Java and OSGi based technology, for which SEC proof of concept implementations of security features can be very good starting point to this market evolution.

***Is this technology going to fly on its own or does it need to be supported by other products or measures to become a commercial success?***

Security is a prerequisite, but it will not make the market. The advent of a service provider market will create the market for security. It also requires agreement on standards. So measures will have to be taken to promote such standards.

I also want to stress that many of SEC technologies could be exploited in different area. In particular, the principles for secure communication have already been proposed to other application area such as home connectivity.

## **Interviewee 2: (Dr. Albert Held, DaimlerChrysler AG)**

### ***Background***

Dr. Albert Held works with DaimlerChrysler Research since 1990. Besides his special experience in the assessment of new and disruptive technologies, the focus of his work is in the area of IT security.

### ***What tangible benefits will this technology bring?***

Security is more a prerequisite than a (additional) feature. So the benefits will be: trust in the system.

### ***What is the current market situation for this technology?***

At the time being, I do not see a big market for telematics security, simply because of the lack of widespread telematics applications.

### ***How do you believe this market segment will evolve in the future?***

As there will be no security per se, the security market segment is bound to the telematics functions market. Once telematics applications become widespread, security will follow (see situation in the mobile communications industry).

In the past, the automotive industry tried to push telematics services without notably success. But with more and more IT components in the cars and improved connectivity to the infrastructure, the vehicle will become more “interesting” for other (non-automotive) service providers. I believe, it is merely a matter of time until this will happen.

### ***What is the specific contribution of the SP to this evolution?***

It is an enabling technology, which allows for reliable (in terms of security) services. By this, SEC helps to build up trust in GST based services. This removes one big obstacle for customer acceptance.

***Is this technology going to fly on its own or does it need to be supported by other products or measures to become a commercial success?***

As already mentioned in 1.1.2 security is a prerequisite, so it will never fly on its own. On the other hand, being an enabling technology the SEC approach can also be deployed in other – non automotive - service scenarios. Terms and Abbreviations

DG INFSO	Directorate-General Information Society
EC	European Commission
FP6	Framework Programme 6
GA	General Assembly
IP	Integrated Project
IPM	Integrated Project Management
IPWPM	Integrated Project Work Package Manager (eg IPWP3M)
IPWPMT	Integrated Project Work Package Managers Team (eg IPWP3MT)
OCT	On-line Collaboration Tool
QP	Quality Plan
SC	Steering Committee
SP	Sub-Project
TS	Test Site
WP	Work Package

## Appendix A - REFERENCES

- [1] DEL\_SEC\_7\_1 GST\_Communication\_Plan
- [2] DEL\_SEC\_7\_4 GST\_Dissemination\_and\_Use\_Plan

## Appendix B - IMPLEMENTATION GUIDES

Implementation guides are available for following security components:

Type of Component	Component	Partner	Licence type
Secure Communication Engine	Stand alone version	KUL	MPL-GPL-LGPL triple license
Secure Communication Engine	Integrated with GST-OS security manager	KUL	MPL-GPL-LGPL triple license
Security Module	Security Module Hardware and Software	KUL	MPL-GPL-LGPL triple license
Entity Authentication	Authentication Retriever	TRIALOG	BSD
Distributed authentication	Single Sign-on	TUM	MPL-GPL-LGPL triple license
Distributed authentication	User Token Access	KUL	MPL-GPL-LGPL triple license
Local PDP	Permission based Policy Decision Point	TRIALOG	BSD
Distributed PDP	EFGD Masked User Authorization	TUM	MPL-GPL-LGPL triple license
Certificate Management	Certificate Management	DC	Not open source, but code available inside the project
Registration/Certification authority	Simple Open CA	DC	Not open source, but code available inside the project

It is also worth mentioning that specific test site have also implemented or integrated security technology complying with GST architecture

Type of Component	Description	SP/TS
Secure Execution Space	TRE	S-PAY
Local PDP	Subscribed Services Access	Munich Test site
Distributed Authentication	Integrated SSO	Munich Test site
Assertion Authority	Commercial Assertion Authority	Munich Test site
Registration/Certification authority	Commercial Registration and Certificate authority	Munich Test site

## Appendix C - OVERVIEW OF DISSEMINATION ACTIVITIES UNDERTAKEN SO FAR

*Conferences and/or workshops attended by the project*

Date	Title	Number of persons attended + other information
7-8 September 2004	GST Forum Requirement Workshop	whole group
12-14 Oct 2004	OSGi World Congress, Barcelona	2 persons from SEC (A.Kung and D.de Cock) made a presentation of GST SEC
6 <sup>th</sup> December 2004	Security Issues in Mobile and Wireless Heterogeneous Networks, Brussels	
18 <sup>th</sup> January 2005	SecurIST workshop	presentation of GST SEC
19 April 2005	2 <sup>nd</sup> SecurIST workshop	participation to task force initiative
7-8 June 2005	GST Forum Architecture Workshop	whole group
27-29 June 2005	ITST 2005, Brest	1 person representing SEC paper authors
29 November 2005	ESCAR 2005. Presentation by KU Leuven, "Security Architecture for Automotive Push and Pull"	Danny deCock (KUL), Antonio Kung (Trialog), Tim Leinmuller (DC). About 70 persons.
30 November 2005	ESCAR 2005. Presentation by DaimlerChrysler and Trialog, "Security in eSafety Projects"	Danny deCock (KUL), Antonio Kung (Trialog), Tim Leinmuller (DC). About 70 persons. The presentation raised significant interest.

*Articles published, press coverage, development web sites etc.*

Date and Type	Details
12-14 Oct 2004, paper & presentation	OSGi world congress 2004 in Barcelona
18 <sup>th</sup> January 2005, presentation	SecurIST workshop
27-29 June 2005, paper & presentation	ITST 2005, Brest
January 2006 issue of, International Journal of Electronics and Communications	"Federation Solutions for Inter- and Intradomain Security in Next-Generation Mobile Service Platforms" by H.J Voegel (BMW), B.Weyl (BMW) and S.Eichler (TUM)



+ regular updates of web site	
-------------------------------	--