Secure Vehicle Communications: Results and Challenges Ahead

Galileo, EGNOS and Security

Neil Warfield
Export Control and International Security Matters Specialist
GNSS Supervisory Authority

Neil.Warfield@gsa.europa.eu
www.gsa.europa.eu
Introduction - Overview

- European GNSS Review and Current Status
- Summary of the Recent Revisions to the Governance of EU GNSS
- Overview of the European GNSS Supervisory Authority (GSA)
- GNSS Security
- GNSS Applications in the Road Domain
- Galileo Open Service
  - Open Service Authentication
- EGNOS
  - EDAS for EGNOS
- Summary
European GNSS Review and Current Status

- European GNSS Review and Current Status
- Summary of the Recent Revisions to the Governance of EU GNSS
- Overview of the European GNSS Supervisory Authority (GSA)
- GNSS Security
- GNSS Applications in the Road Domain
- Galileo Open Service
  - Open Service Authentication
- EGNOS
  - EDAS for EGNOS
- Summary
European Radio Navigation Satellite System (RNSS) Milestones

December 1994: Resolution of European Transport Council

European contribution for a new GNSS

Agreement EC ESA EUROCONTROL

1994

1998

2009

1999

2002

2010

2012

2013

Definition

Development

IOV

IOC

FOC

GNSS-1

EGNOS

GALILEO

GNSS-2

OQR (2009)

FOC (2013)
Galileo

- GALILEO is to be the one and only independent European world wide global navigation satellite system.
- Galileo is expected to consist of up to 30 satellites and a network of ground stations.
- Provides superior coverage and accuracy compared with either GPS and Glonass.
- For certain services, Galileo includes a service guarantee, allowing for the expansion of GNSS services into safety of life critical areas.
- Galileo is designed to be fully interoperable with the American GPS system, allowing receivers to use both systems for increased accuracy and reliability.
Galileo System Overview

♦ Galileo System

- Satellites up to 30
- Control Centres up to 3
- Mission Uplinks up to 10 spread over up to 23 sites
  (Configuration to be confirmed)

- Sensor Stations 30-40 spread over up to 76 sites
  (Configuration to be confirmed)
<table>
<thead>
<tr>
<th>Service Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Open Access</td>
<td>Free air; Mass market; Simple positioning</td>
</tr>
<tr>
<td>Commercial</td>
<td>Encrypted; High accuracy; Guaranteed service</td>
</tr>
<tr>
<td>Safety of Life</td>
<td>Open Service + Integrity and Authentication of signal</td>
</tr>
<tr>
<td>Public Regulated</td>
<td>Encrypted; Integrity; Continuous availability</td>
</tr>
<tr>
<td>Search and Rescue</td>
<td>Near real-time; Precise; Return link feasible</td>
</tr>
</tbody>
</table>

EU Transport Council Approval: 09.12.2004
EGNOS is Europe’s first GNSS programme.

EGNOS provides augmentation signals for the GPS and GLONASS systems, re-transmitted by geostationary satellites and a network of ground stations. (Similar to the US WAAS augmentation system)

EGNOS provides:

- Correction data for the GPS and GLONASS systems throughout Europe, improving accuracy to the order of 1-3m.
- An integrity message to inform users of problems with GPS and GLONASS satellites in real time.
- An extremely accurate universal time signal.
<table>
<thead>
<tr>
<th>Transmission means</th>
<th>Open Service</th>
<th>Safety Of Life</th>
<th>Commercial Data Dissemination Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>RF signal (L1 frequency)</td>
<td>RF signal (L1 frequency)</td>
<td>Ground network</td>
<td></td>
</tr>
<tr>
<td>Reference</td>
<td>EGNOS MRD</td>
<td>EGNOS MRD</td>
<td>EGNOS MRD</td>
</tr>
<tr>
<td>Guarantee of Service</td>
<td>None</td>
<td>Guarantee of compliance to ICAO standards (certification)</td>
<td>Guarantee of compliance to SLA</td>
</tr>
<tr>
<td>Definition of the Service</td>
<td>SIS only</td>
<td>SIS + Guarantee of compliance to ICAO standards (certification)</td>
<td>EGNOS data + Guarantee of compliance to SLA</td>
</tr>
<tr>
<td>Typical user communities</td>
<td>Pedestrian, in-car navigation</td>
<td>Aviation, Maritime, railway, road (tolling), emergency services</td>
<td>Pedestrian, in-car navigation, research (e.g. atmospheric, tectonics), high-precision GNSS</td>
</tr>
</tbody>
</table>
Summary of the Recent Revisions to the Governance of EU GNSS

- European GNSS Review and Current Status
- **Summary of the Recent Revisions to the Governance of EU GNSS**
- Overview of the European GNSS Supervisory Authority (GSA)
- GNSS Security
- GNSS Applications in the Road Domain
- Galileo Open Service
  - Open Service Authentication
- EGNOS
  - EDAS for EGNOS
- Summary
Council Conclusions on launching the European Global Navigation Satellite System Programmes

♦ The Council, in its Resolution of 8 June 2007
  ➢ re-affirmed the value of Galileo, concluded stop the PPP concession negotiations, agreed in principle a re-profiling of the European GNSS programmes and recognised the need for additional public funding

♦ The Commission in its communication the European Parliament and the Council on 19 September 2007
  • “Progressing Galileo, re-profiling the European GNSS Programmes”
    – detailed alternative proposals for the financing
    – proposals for an implementation and procurement strategy by the public sector
    – concepts for the subsequent operation and exploitation phase of Galileo
    – proposals for a sound public sector management structure of the programme on the basis of a clear division of responsibilities between Commission, ESA, GSA, Member States and Council

♦ 2835th TRANSPORT, TELECOMMUNICATIONS AND ENERGY Council meeting Brussels, 29-30 November and 3 December 2007
3 main reasons for the PPP/Concession failure

♦ 1. GALILEO technical challenge
♦ 2. Risks transfer difficulties:
   ➢ Design Risk Transfer
     • Different entities in charge of design and deployment
     • IOV partial validation capabilities
     • Scalability problems
   ➢ Market Risk Transfer
     • Absence of market track record
     • Uncertainty on the forecast
     • GPS available for free
♦ 3. Industrial governance and workshare
Council Conclusions on launching the European Global Navigation Satellite System Programmes

♦ Political decision making and oversight
  ➢ The Council and the European Parliament
    • Budgetary Authority and ultimate political decision-making bodies for the programmes
  ➢ All Member States
    • Political oversight of the programmes

♦ Management and execution
  ➢ Commission
    • Fully responsible for the overall management of the programmes as the European GNSS Programme Manager
  ➢ Member States
    • Closely associated with the essential elements of the management of the programme, in particular the work programme and the programme implementation plan and associated financing
  ➢ GSA
    • Technical certification
    • Security accreditation
    • Market preparation and commercialisation of the system
    • Assists the Commission for all matters related the execution of the programmes
  ➢ ESA
    • Procurement agent for Galileo
    • subject the future agreement between the European Community, represented by the Commission, and the ESA
Overview of the European GNSS Supervisory Authority (GSA)

- European GNSS Review and Current Status
- Summary of the Recent Revisions to the Governance of EU GNSS
- Overview of the European GNSS Supervisory Authority (GSA)
- GNSS Security
- GNSS Applications in the Road Domain
- Galileo Open Service
  - Open Service Authentication
- EGNOS
  - EDAS for EGNOS
- Summary
An official European Union Regulatory Authority, the European GNSS Supervisory Authority (GSA) manages all public interests related to European GNSS programmes.

GSA strategic objectives include the achievement of a fully operational GALILEO system. This includes the laying of foundations for a fully sustainable and economically viable system.

Moreover, GSA's key stated objective is to make GALILEO not just a functioning system but also the world's leading satellite navigation system for civilian applications.
Missions of the Supervisory Authority

- 2(a) Conclude a concession contract for Galileo deployment and operating phases *
- 2(b) Manage and control the use of funds allocated
- 2(c) Manage the agreement with the EGNOS operator
- 2(f) Modernise and develop new generations of EU GNSS
- 2(h) Ensure that EU GNSS are duly certified (safety)
- 2(i) Enforce Joint Action 2004/552/CFSP (EU security)
- 2(j) Manage all aspects relating the system's safety and security

The key mission of the Authority is the management of public sector’s interest relating the European Galileo and EGNOS during the deployment and operational phases of the programme
Main tasks on security (1/2)

♦ General Security
  ➢ Provisions for the exchange, handling and storage of classified information
  ➢ Security Aspects Letter: security annexes of industrial contracts

♦ Security Accreditation
  ➢ GSA is the European GNSS security accreditation authority
    • initiate and monitor the implementation of security procedures and perform system security audits
  ➢ Security specifications of the system and its components
  ➢ Standards of security for information techniques
  ➢ Compliance of European GNSS signals/services with security requirements and standards

♦ Safety certification
  ➢ Support for issuing the relevant certificates and monitoring the respect of related standards and technical specifications
Main tasks on security (2/2)

♦ PRS
  ➢ Specifications and instructions for manufacturing PRS receivers
  ➢ Guidelines for the implementation of PRS management rules in the Member States
  ➢ Establishment of a GSA Security Centre for PRS management and EU GNSS security monitoring

♦ International Relations
  ➢ Export control
    • Compliance with international rules and agreements (Wassenaar, Missile Technology Control Regime, international agreements, …)
    • Establishment of a dedicated Galileo export control regime
  ➢ Support and coordination with the Council
    • Implementation of Joint Action 2004/552/CFSP
  ➢ Security policy issues in international agreements
  ➢ Frequency coordination
GNSS Security

- European GNSS Review and Current Status
- Summary of the Recent Revisions to the Governance of EU GNSS
- Overview of the European GNSS Supervisory Authority (GSA)
- GNSS Security
- GNSS Applications in the Road Domain
- Galileo Open Service
  - Open Service Authentication
- EGNOS
  - EDAS for EGNOS
- Summary
GNSS Security

♦ The Main Threats to European GNSS Systems

♦ 1. System Protection

♦ 2. Misuse

♦ 3. Commercial Security
System Protection

The design and deployment of the system needs to take into account a range of threats.

- Physical attacks
  - Against Space Assets
  - Against Ground Infrastructure

- System Failure
  - Deliberate / Accidental Action by System Administrators
  - Mechanical Failure

- Electronic Attack
  - Jamming
  - Spoofing
Misuse

EU GNSS are civil systems under civil control. They include, within Galileo, the Public Regulated Service (PRS) for use by public entities.

- PRS is encrypted
- Access only to approved public service users

Management of the access to PRS by approved users from all EU Member States.

- Key management
- Receiver misuse
- Service denial
GNSS Security

♦ Commercial Security

♦ Need to protect revenue streams from European GNSS
  ➢ Charges from access to the Galileo Commercial Service
  ➢ Expected use of the Open Service for Road Tolling applications

♦ The commercial threat will depend on the final uses of European GNSS
  ➢ ie Need to consider the risks involved
GNSS Applications in the Road Domain

- European GNSS Review and Current Status
- Summary of the Recent Revisions to the Governance of EU GNSS
- Overview of the European GNSS Supervisory Authority (GSA)
- GNSS Security
- **GNSS Applications in the Road Domain**
  - Galileo Open Service
    - Open Service Authentication
  - EGNOS
    - EDAS for EGNOS
- Summary
### Description of road applications (1/2)

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
<th>Benefit from EGNOS/Galileo</th>
</tr>
</thead>
</table>
| **ADAS**                     | Advanced Driver Assistance Systems  
It includes collision warning systems (e.g., lane change warning system) and vehicle control systems (e.g., Adaptive cruise control)                                                                 | Increased accuracy and improved positioning services like predictive cruise control, lane keeping and intersection support will be enhanced |
| **Emergency services**       | It covers the assistance to victims of road accidents as well as any other assistance which should be sorted out by the emergency services (police, firemen, ambulance…)                                           | Integrity and continuity will improve the services already provided today  
Enhanced navigation will reduce time to assistance from emergency services |
| **Fleet management**         | It is one of the main tool for the reduction of maintenance cost and improvement of services quality. It includes goods transport management, city logistics (matching process, itinerary calculation) & freight (logistic chain improvement) | Already available with GPS, EGNOS/Galileo will improve the system efficiency thanks to better positioning and timing information |
| **Infrastructure management**| It refers to network maintenance management by road administrations                                                                                                                                          | Better prediction of maintenance work required and type of pavement to plan, as the administration will know the exact number of vehicles on a section |
| **Law enforcement**          | It covers legal enforcement (mainly related to speed limits) and environmental enforcement (vehicles in use control, hazardous good control….)                                                                  | Positioning and velocity data will allow a permanent control of speed and a better tracking of hazardous goods transportation |

*Source: GIROADS project (D2220)*

Lausanne, 21 February 2008
## Description of road applications (2/2)

<table>
<thead>
<tr>
<th>Application</th>
<th>Description</th>
<th>Benefit from EGNOS/Galileo</th>
</tr>
</thead>
<tbody>
<tr>
<td>LBS / Navigation</td>
<td>Those systems provide route guidance and additional services like parking availability, location of points of interest, petrol station….</td>
<td>In-time update and increased accuracy will improve the services available (dynamic route guidance…)</td>
</tr>
<tr>
<td>Pay per use insurance</td>
<td>Increased competition encourages the creation of new and fairer insurance pricing. GNSS gives the opportunity to offer a price related to the exact mileage, driver’s behaviour, speed etc and offer the possibility of recovery after theft, accident reconstruction etc.</td>
<td>Galileo will offer the accuracy and integrity necessary to develop such services</td>
</tr>
<tr>
<td>Pay per use services</td>
<td>They regroup several services like pricing of on-street parking, taxi, car rental etc.</td>
<td>EGNOS/Galileo accuracy and integrity will reinforce the development of those services</td>
</tr>
<tr>
<td>Road tolling (Electronic fee collection)</td>
<td>It allows charging for the use of road infrastructure minimizing traffic disturbances, achieving a better social acceptance and reducing cost</td>
<td>Better accuracy and integrity will permit the development of GNSS tolling system, which are more flexible and eliminate expensive toll points…</td>
</tr>
<tr>
<td>Tracking and tracing</td>
<td>For livestock, food or hazardous goods it is important to track and guaranty the individual control from origin to destination and to react in case of problem</td>
<td>The use of GNSS will improve automatic vehicle location and increase efficiency. It will also guaranty continuous tracking</td>
</tr>
<tr>
<td>Traffic management</td>
<td>It refers to the management of freeway, road conditions for increased safety, non-recurring congestion, recurring congestion, public transport…</td>
<td>In-time update and continuity will allow a more efficient traffic management</td>
</tr>
</tbody>
</table>

*Source: GIROADS project (D2220)*
Road tolling is one key application to focus on

![Diagram](chart.png)

- **PUS H** emergency services
- **CORE** road tolling
- **PUL L** pay per use insurance
- **PUL L** fleet management
- **PUL L** tracking & tracing
- **PUL L** navigation

Legislation requirements

Appeal / Willingness to pay
Road tolling represents 12mln users and 19bln € revenues

### ASECAP network and traffic information (as of Jan ’07)

<table>
<thead>
<tr>
<th>Country</th>
<th>Network Companies</th>
<th>Kms</th>
<th>Traffic (daily average)</th>
<th>Payment means</th>
<th>Revenues (€ million)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td>Light vehicles</td>
<td>Toll stations</td>
<td>ETC</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Heavy vehicles</td>
<td>Toll lanes</td>
<td>ETC users</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>Total</td>
<td>ETC lanes</td>
<td></td>
</tr>
<tr>
<td>Austria</td>
<td>3</td>
<td>2,061,8</td>
<td>40.701</td>
<td>14</td>
<td>108</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.423</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>46.124</td>
<td>2</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14</td>
<td>108</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>307.458 (5)</td>
<td></td>
</tr>
<tr>
<td>Belgium</td>
<td>1</td>
<td>1,4</td>
<td>10.178</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.539</td>
<td>2</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>15.717</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>18</td>
<td>175</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5.261 (2)</td>
<td>546.000 (3)</td>
</tr>
<tr>
<td>Croatia</td>
<td>4</td>
<td>1,068,5</td>
<td>12.425</td>
<td>2</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.559</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13.984</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>18</td>
<td>175</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>5.324</td>
<td></td>
</tr>
<tr>
<td>Denmark</td>
<td>2</td>
<td>34,0</td>
<td>38.570</td>
<td>2</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4.780</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>43.350</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>345.000</td>
<td></td>
</tr>
<tr>
<td>France</td>
<td>16</td>
<td>8.330,5</td>
<td>22.381</td>
<td>482 (6)</td>
<td>4.301 (6)</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4.282</td>
<td>2</td>
<td>46</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>26.663</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.760.000</td>
<td></td>
</tr>
<tr>
<td>Germany</td>
<td>1</td>
<td>12.407,0</td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.784</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>546.000 (3)</td>
<td></td>
</tr>
<tr>
<td>Greece</td>
<td>1</td>
<td>916,5</td>
<td>7.514</td>
<td>18</td>
<td>175</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.017</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>8.531</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>14</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>72.000</td>
<td></td>
</tr>
<tr>
<td>Hungary</td>
<td>3</td>
<td>800,4</td>
<td>21.919</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>5.622</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>27.541</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Italy</td>
<td>23</td>
<td>5.649,4</td>
<td>31.281</td>
<td>464</td>
<td>3.779</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>9.952</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>41.233</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.992</td>
<td>5.300.000</td>
</tr>
<tr>
<td>NL</td>
<td>1</td>
<td>20,0</td>
<td>11.724</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.731</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>13.455</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Norway</td>
<td>37</td>
<td>669,8</td>
<td>436.869</td>
<td>85</td>
<td>290</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>42.458</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>479.327</td>
<td>1</td>
<td>14</td>
</tr>
<tr>
<td>Portugal</td>
<td>5</td>
<td>1.434,0</td>
<td>19.883</td>
<td>132</td>
<td>1.056</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>1.143</td>
<td>1</td>
<td>132</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>21.026</td>
<td>1</td>
<td>132</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>345</td>
<td>2.012.736</td>
</tr>
<tr>
<td>Serbia</td>
<td>1</td>
<td>603,0</td>
<td>-</td>
<td>37</td>
<td>146</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>-</td>
<td>31 (1)</td>
<td>500</td>
</tr>
<tr>
<td>Slovenia</td>
<td>1</td>
<td>455,0</td>
<td>19.307</td>
<td>26</td>
<td>181</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>4.412</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>23.719</td>
<td>1</td>
<td>18</td>
</tr>
<tr>
<td>Spain</td>
<td>31</td>
<td>3.099,6</td>
<td>21.015</td>
<td>212</td>
<td>2.157</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.316</td>
<td>1</td>
<td>212</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>24.331</td>
<td>1</td>
<td>212</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>1.364</td>
<td>762.740</td>
</tr>
<tr>
<td>UK</td>
<td>1</td>
<td>42,0</td>
<td>44.441</td>
<td>6</td>
<td>45</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>3.820</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>48.261</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Total</td>
<td>131</td>
<td>37.592,9</td>
<td>1.082</td>
<td>1.082</td>
<td>8.447</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td>11.707.886</td>
<td></td>
</tr>
</tbody>
</table>

Notes:
- Denmark: traffic in city ring included
- (1) 27 (manual + ETC) + 4 (ETC only)
- (2) Number of GNSS toll stations
- (3) Number of OBU subscribers
- (4) Number of video toll equipped
- (5) Number of video toll tickets sold
- (6) Provisional data

Source: ASECAP

Lausanne, 21 February 2008
Galileo Open Service

♦ European GNSS Review and Current Status
♦ Summary of the Recent Revisions to the Governance of EU GNSS
♦ Overview of the European GNSS Supervisory Authority (GSA)
♦ GNSS Security
♦ GNSS Applications in the Road Domain
♦ Galileo Open Service
  ➢ Open Service Authentication
♦ EGNOS
  ➢ EDAS for EGNOS
♦ Summary
Galileo Open Service

♦ The Open Service (OS) is the free to use mass market service available from Galileo
♦ It is the service of choice for mass market applications such as road user charging
♦ Since the OS will be used to levy a charge on users, there is a clear financial benefit to the user in disrupting the system
♦ There is therefore a threat to the system comes from the user (or at least occurs with their knowledge or consent) which is distinct from eg a terrorist attack
♦ We can assume that the user can not impact on the Space or Ground segments.
Threat from users

♦ User is only capable of changing the way their receiver perceives the signals provided by the system. Their goal is to disrupt the navigation solution.
  ➢ Preventing reception
    • Eg Break receiver antenna
    • Receiver clearly aware that no signal is being received
  ➢ Jamming
    • Eg Transmitting a sufficiently strong signal in the vicinity of the receiver
    • Receiver clearly aware that no signal is being received and, depending on jamming sophistication, it may be able to detect that the signal is jammed.
  ➢ Spoofing
    • Consists of providing the receiver with signals which appear genuine but which cause the receiver to compute a false position, record a false time etc
    • Authentication can make the generation of false signals very difficult

♦ However, to protect such a service security needs to focus on the system globally and not just focus on the user equipment.
Open Service (OS) Authentication

♦ Supporting the definition of OS Authentication

➢ The current Galileo core services definition and requirements documentation include an optional authentication capability applicable to the SoL service

➢ The inclusion of an OS authentication feature is considered a major revenue generator in terms of road tolling

➢ OS authentication could also be used for a wide variety of other uses:

   • **Multimodal transportation**: authenticating the handover of goods and/or containers from one provider (e.g. shipping company) to another provider (e.g., road transport company)

   • **Authenticated timestamp**: authenticate timestamp based on Galileo timing signal, for use in ecommerce, electronic transactions

   • **Maritime and fisheries**: to prove where you were and that you did not fish in someone else’s territorial waters

   • **Person tracking**: to keep away stalkers with a restraining order, tracking offenders on parole

   • **Monitoring resting times for truck drivers**
Authentication for the Open Service

- Considering the insufficient maturity of the authentication concept and requirements, and the considerable potential economic interest of this feature, the launch of a series of complementary studies was proposed.

- Therefore, the GSA has recently issued a CCN to the Galileo Advanced Concepts Program dealing with the better definition of OS authentication for road tolling.
  - Results are expected to be available mid 2008.
  - Depending on the study results there is still the possibility to introduce this feature in the FOC ITT.
Authentication of Open Service

Galileo Advanced Concepts Contract Change Notice Proposal (FP6)
- Authentication study extension
- 12/09/2007 (CCN), launch before EOY
- Finish by mid 2008

PVT authentication
- Task 6000
  - Detailed user requirements for the Road User Charging application
  - Requirements from the selected applications in the Maritime domain.
- Task 7000
  - Options for implementing authentication in the Galileo signals and navigation messages
  - Overview of opportunities to obtain an authenticated PVT in a multi-system, multi-sensor environment
- Task 8000
  - Implementation of schemes for obtaining the authenticated PVT that would satisfy the user requirements
  - Mainly be oriented on the Road User Charging application.
  - Recommendations to the Galileo Services, signals and the vehicle’s on-board unit
Existing Authentication in Galileo - Safety of Life Service

- The Safety of Life service is aimed at air / rail / maritime users where high accuracy and reliability are critical for the safety of life.

- The Safety of Life is an authenticated signal

- Receivers will be able to receive real time information of the reliability of the signal so that backup systems can be used in the event of signal degradation.
Safety of Life Authentication

- Safety of Life message includes an integrity table which contains integrity values for the message.
- An authentication word is computed from this table.
- This authentication word is then encrypted using a secret key.
- Receivers have their own key which they can use to decrypt the authentication word and thus validate the integrity table.

- The Safety of Life service is intended to be used in the Rail, Air and Maritime sectors when the reliability information is essential.
- Will only be available to selected users.
- Access rules to the safety of life service have yet to be finalised.
Safety of Life – The Threats

♦ The threat is different for the safety of life service.
  ➢ User is unlikely to tamper with their equipment
  ➢ Attacker is likely to be a third party
  ➢ Attacker is likely to attack the signal (jamming / spoofing etc)

♦ Primary aim of Safety of Life authentication is safety not security
  ➢ Ensuring that data is reliable
  ➢ Real time information on position quality
  ➢ Immediate notification in the case of system failure to allow for the employment of backup systems

♦ Open service authentication may follow a similar route to the safety of life service, depending on the main threats and main identified uses.
EGNOS

- European GNSS Review and Current Status
- Summary of the Recent Revisions to the Governance of EU GNSS
- Overview of the European GNSS Supervisory Authority (GSA)
- GNSS Security
- GNSS Applications in the Road Domain
- Galileo Open Service
  - Open Service Authentication
- EGNOS
  - EDAS for EGNOS
- Summary
Recall of EGNOS Services

<table>
<thead>
<tr>
<th></th>
<th>Open Service</th>
<th>Safety Of Life</th>
<th>CDDS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmission means</td>
<td>RF signal (L1 frequency)</td>
<td>RF signal (L1 frequency)</td>
<td>Ground network</td>
</tr>
<tr>
<td>Reference</td>
<td>EGNOS MRD</td>
<td>EGNOS MRD</td>
<td>EGNOS MRD</td>
</tr>
<tr>
<td>Guarantee of Service</td>
<td>None</td>
<td>Guarantee of compliance to ICAO standards (certification)</td>
<td>Guarantee of compliance to SLA</td>
</tr>
<tr>
<td>Definition of the Service</td>
<td>SIS only</td>
<td>SIS + Guarantee of compliance to ICAO standards (certification)</td>
<td>EGNOS data + Guarantee of compliance to SLA</td>
</tr>
<tr>
<td>Typical user communities</td>
<td>Pedestrian, in-car navigation</td>
<td>Aviation, Maritime, railway, road (tolling), emergency services</td>
<td>Pedestrian, in-car navigation, research (e.g. atmospheric, tectonics), high-precision GNSS</td>
</tr>
</tbody>
</table>
EGNOS Commercial Data Dissemination Service: An Introduction

- CDDS: Commercial Data Dissemination Service
- One of the 3 services of EGNOS (other two: Open Service, Safety-Of-Life Service)
- Provision of EGNOS data, in real time, via ground links
- Extends the EGNOS service to users that are not able to receive the EGNOS open service signal (eg urban users) or who require the service guarantee
- Access to this service is via EDAS – the EGNOS Data Server
What is involved?

- Connection to EDAS
- Use of EDAS client software for data access
- Data post-processing (value-added chain)
- Provision of services to end users

End users will not connect directly to EDAS.

- Service providers will connect to EDAS
- These service providers will then disseminate the EDAS data onwards, including any value added service that they provide
EDAS data types

- GPS data collected by all EGNOS Monitoring Stations (RIMS)
- EGNOS augmentation messages, also transmitted via the EGNOS Geostationary satellites (EGNOS SIS)
The Value Added Chain

EGNOS Data Server

Value-added service provider

EGNOS data (real-time)

User-specific information

End users
Phased approach:
- Phase 1: “beta-testing”
- Phase 2: commercial exploitation
CDDS phase 1 objectives

♦ Primary objectives:
  - To better understand the market for the EGNOS commercial service
  - To provide GSA with practical experience in the management of an operational European GNSS service
  - To support CDDS penetration within European Industry

♦ Other objectives:
  - To promote European GNSS
  - To observe EDAS performance
CDDS phase 1 principles

- EDAS data is provided free-of-charge
- GSA provides no guarantee/liability
- Phase 1 duration is 12 months minimum
- Users of EDAS data must provide feedback to GSA
Summary

- European GNSS Review and Current Status
- Summary of the Recent Revisions to the Governance of EU GNSS
- Overview of the European GNSS Supervisory Authority (GSA)
- GNSS Security
- GNSS Applications in the Road Domain
- Galileo Open Service
  - Open Service Authentication
- EGNOS
  - EDAS for EGNOS
- Summary
Any Questions?
Galileo Security Doctrine

Accidental or deliberate attack on Galileo

Protection of Galileo infrastructure and Protection of all services
- Ensure availability
- Ensure integrity

Prevention of misuse of services
- Control of service denial
- Control of legitimate use

Subversive and hostile use of Galileo services

Illegitimate use

References:
- « Interim security doctrine for the Galileo project » V2.0 18/10/2001
- « Galileo threats and vulnerabilities » V1.0 16/02/2001