TACOT

TRUSTED MULTI APPLICATION RECEIVER FOR TRUCKS

FDC

ACTIA®

Continental

intellic
Intelligent Solutions for Transport Logistics

Stoneridge

CORTE

SQUARIS
CONSULTANTS

certSIGN
Secure your on-line transactions

Probayes
Mastering Uncertainty

KEYNECTIS

Agenda

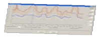
- Brief overview of FDC
- Introduction to TACOT:
  - Satellite Navigation and Security issues
  - GEODatage
- Presentation of TACOT

Few words about FDC…

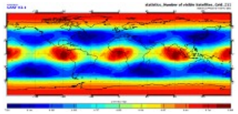
- Created in 1989
- Independent research, and engineering firm
- Main fields of Expertise:
  - Positioning, Timing, GNSS (GPS, Galileo, EGNOS, GLONASS…)
  - IT Communications
  - Security and Defence
  - GMES
- Development Target
  - Trusted multi-sensors positioning/timing systems

Experience in GNSS

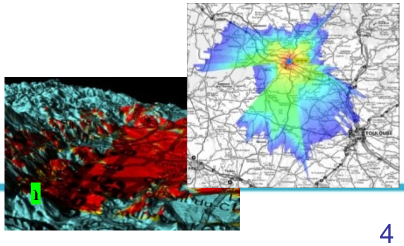
- Military GPS since 1989
  - French MoD, NATO
  - In cooperation with US DoD and NSA



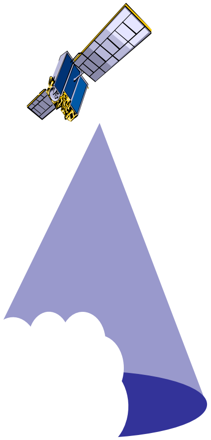
- Civil GNSS since 1993
  - 85 European projects (40 led by FDC) for EC support and R&D
  - Eurocontrol, CNES, Fr MoT…



- Promoter of Security for civil GNSS systems since 1997
  - Galileo System Security Board, Galileo PRS,
  - Cryptography, Authentication, Threats and Vulnerabilities



Satellite Navigation



Trendy and cheap …

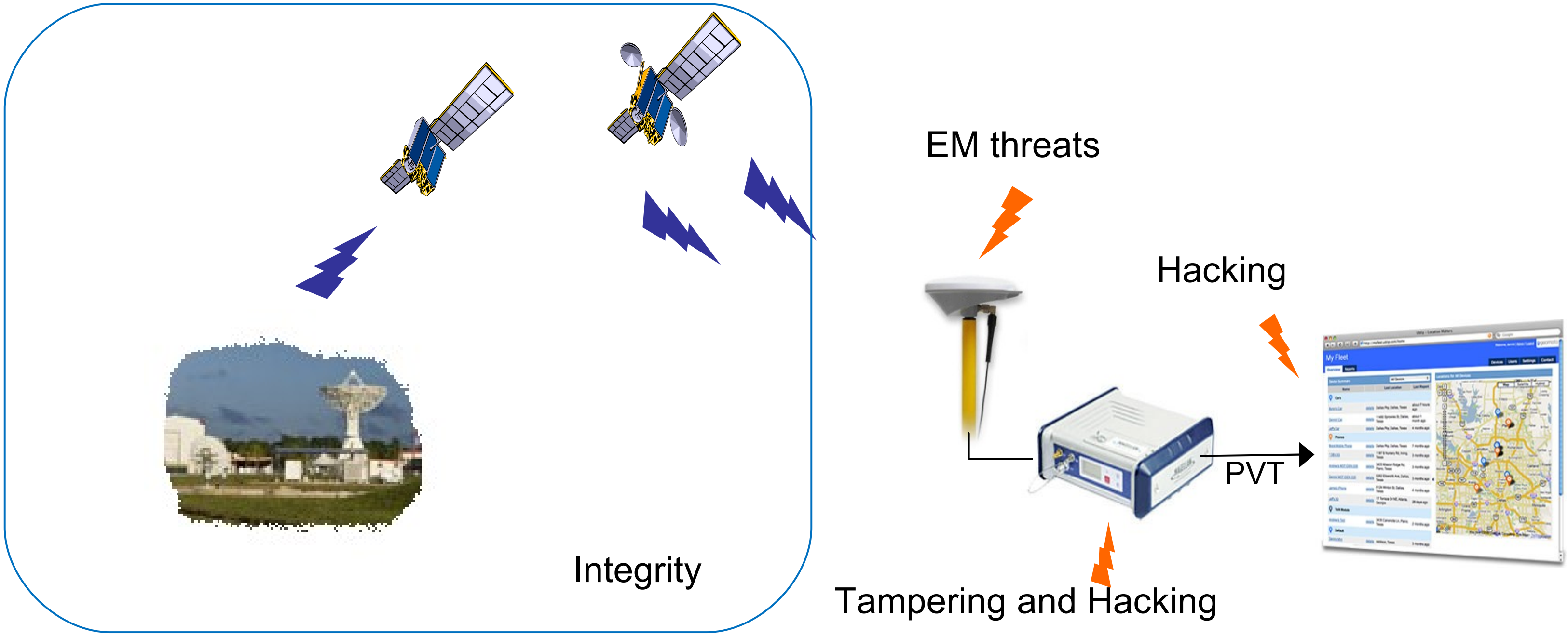
… But vulnerable

Need for **Reliability** and therefore **Securitv**

•www.spy-craft.co.uk

Source: http://www.youtube.com/watch?v=ShRPXkpW1mM

GNSS Threats



Integrity

EM threats

Hacking

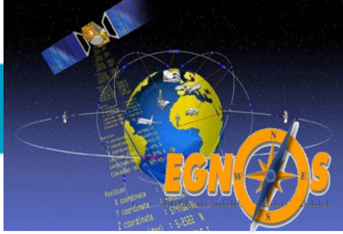
PVT

Tampering and Hacking

Examples of Trusted PVT Applications

- Time stamping
- Bank transactions
- Synchronization of electricity networks
- Maritime surveillance
- Monitoring of Police and Civil Security services
- VIP, Prisoner, kids monitoring
- Monitoring of disabled people
- Law enforcement
- Customs
- Common Agricultural Politics monitoring
- IPR protection
- Legal document and records
- Auction
- Electronic Tolling
- PAYD Insurance
- Car Parking
- Ecall
- Dangerous or high value goods monitoring

First step: GEODatage



- Objectives
  - To provide a trusted and autonomous Time Stamping Authority

    Time Stamps are used to prove the existence of certain data before a certain time without the possibility that the owner can backdate the timestamps

  - To ensure a legal recognition of the delivered Time Stamp Tokens
  - A solution affordable to every one
  - The provision of location information in the Tokens

- Sponsors
  - French Ministry of Economy
  - Important self-financing
  - Technical review by French Space Agency

Targeted Applications

- A wide range of applications…
  - Laboratory notebooks
  - Proofs for patent registration
  - Administrative documents
  - Emails (e.g. with acknowledgement of receipt)
  - Court records
  - Notarial deeds
  - Leisure applications

2,929,922

No 2,929,922

THE UNITED STATES OF AMERICA

TO ALL TO WHOM THESE PRESENTS SHALL COME:

Whereas Arthur L. Schawlow, of Madison, New Jersey, and Charles H. Townes, of New York, N. Y., assignors to Bell Telephone Laboratories, Incorporated, of New York, N. Y., a corporation of New York,

[illegible] Commissioner of Patents [illegible]

Whereas [illegible]

[illegible] Letters Patent [illegible]

Bell Telephone Laboratories, Incorporated, its successors [illegible]

[illegible] SEVENTEEN [illegible]

[illegible]

In testimony whereof I have hereunto set my hand and caused the seal of the Patent Office to be affixed at the City of Washington this twenty-second day of March, in the year of our Lord one thousand nine hundred and sixty, and of the Independence of the United States of America the one hundred and eighty-fourth.

Robert C. Watson

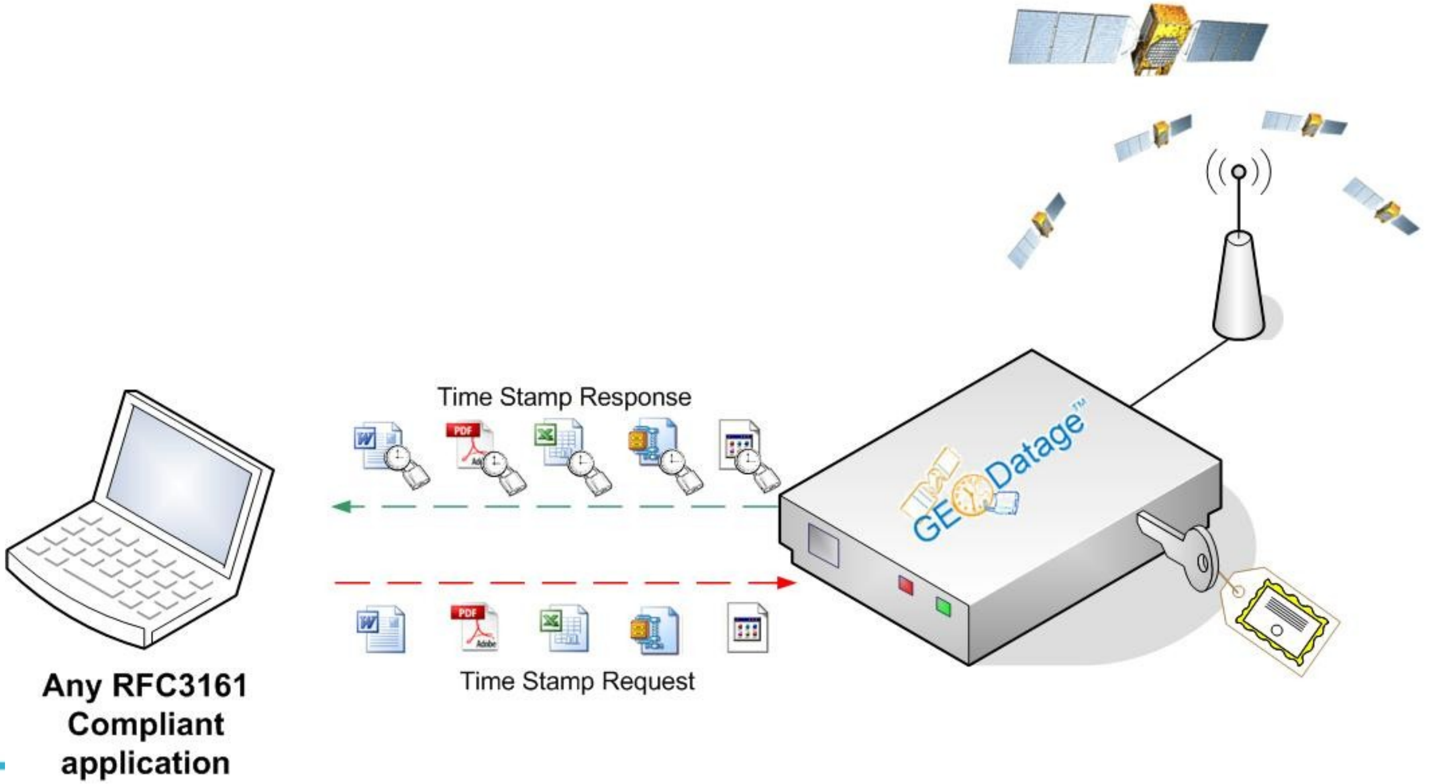
Our solution …

- Is based on the EGNOS Network Time bringing:
  - Real time and accurate access to UTC(OP)
  - Integrity of the delivered time
- Uses certified smartcard technology and implements a set of countermeasures to detect GNSS spoofing attacks and to ensure timestamp non repudiation
- Is developed according internationally recognized standards:
  - RFC3161: Internet X.509 PKI Time-Stamp Protocol (TSP)
  - PKCS : Public Key Cryptographic Standards

Secured, Trusted and Certified

- Certified product
  - Product under evaluation by ANSSI (French Network and Information Security Agency)

ANSSI | Agence nationale de la sécurité des systèmes d'information



2nd Step

- Galileo enabled

- New version under design
  - Additional countermeasures
  - Performance improvement

- **GEODatage** paved the way for the **TACOT** Project

TACOT

- Project objectives:
  - To demonstrate feasibility & boost penetration of European GNSS in road transport through the vector of digital tachographs,
  - To anticipate the amendment of 3821/85 regulation on recording equipment in road transport: recording of location data & enhanced security.

- EC FP7, Galileo 3rd call 3
- Total budget: 2.7 M€
- Start : January 2012
- Duration: 24 months
- Project led by FDC

SEVENTH FRAMEWORK
PROGRAMME

Genesis

- Market and industry interest
  - PVT function into tachographs multiplies numbers of applications/services (fleet management, PAYD,…),
  - Open huge new market opportunities at least for tachometer manufacturers.
- Community interest:
  - Digital tachographs are onboard 95% of trucks
    - Rapid penetration of EU GNSS (EGNOS/Galileo) into trucks
    - EU GNSS will become the basis for many other applications
    - Potential propagation to any other road vehicles
    - Industry will be ready for the update of the 3821/85 regulation which may include tracing/tracking features
- Tachometer is a secured device
  - Enforce the security of the PVT function
  - Propose a Protection Profile for PVT function

TACOT consortium 1/2

- The whole European Tachograph Industry:

ACTIA® Continental INTELLIC Intelligent Solutions for Transport Logistics Stoneridge

- Expert in Trusted GNSS: FDC

- Expert in Sensor fusion: Probayes Mastering Uncertainty

- Expert in Fleet management: ACTIA® (It)

- Experts in Security certSIGN. Secure your on-line transactions KEYNECTIS

TACOT consortium 2/2

- Users representative and institutions:

  Confederation of Organisations in Road Transport Enforcement

  & Advisory group including:

  –*European Automobile Manufacturers' Association:*

  –*International Road Transport Union:*

  –*European Traffic Police Network:*

- Legal / regulatory aspects:
- Business & exploitation plans, dissemination:

Rationale for using EU GNSS

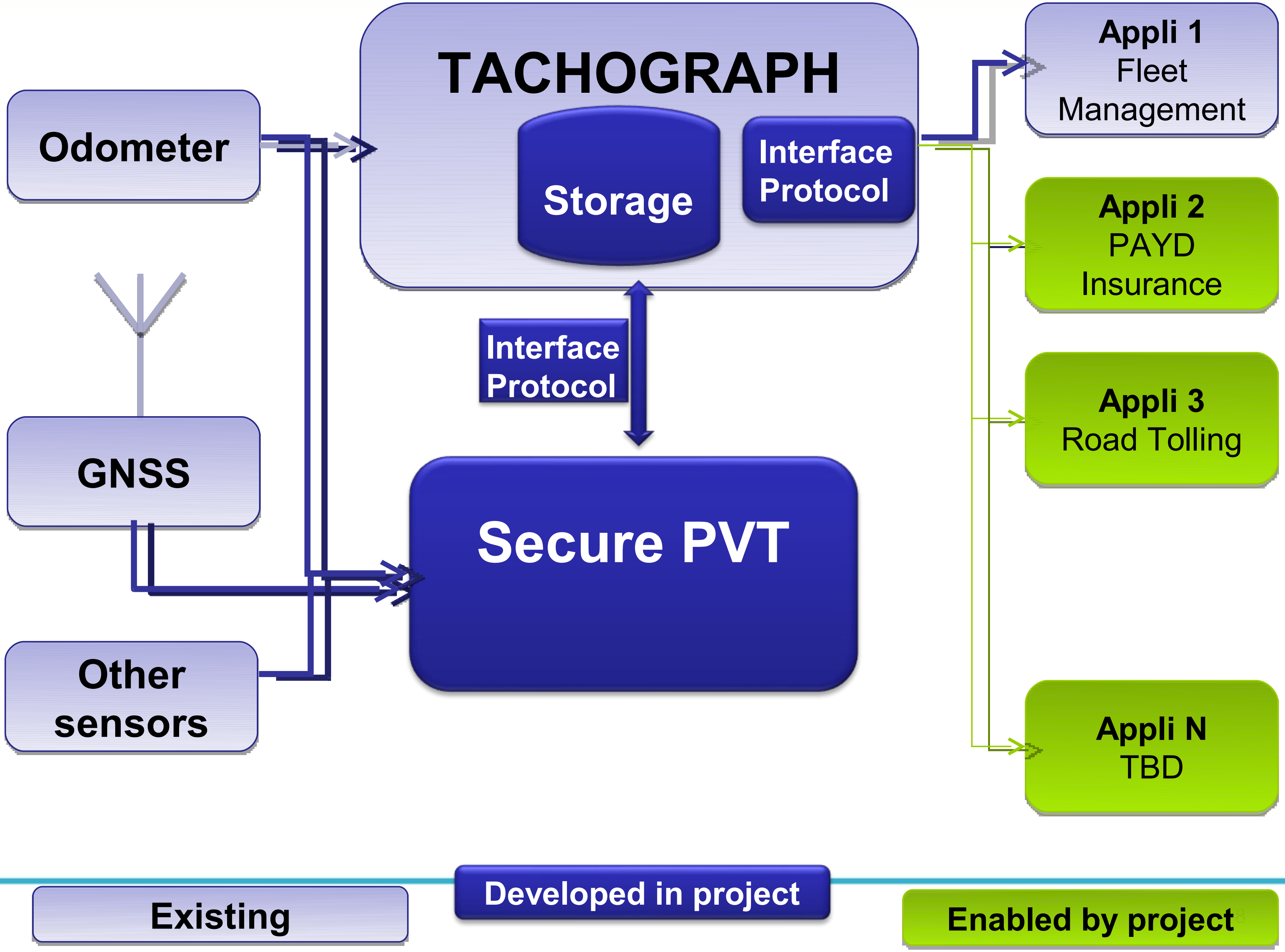
- Economic
  - The addition of PVT to the digital tachograph enables the development of applications deemed attractive by the industry.
  - GNSS allows PVT information at low cost.

- Legal
  - EGNOS provides UTC(OP) time, a legal time scale in Europe.
  - A trusted PVT is a necessary enabler for liability critical / legally binding applications

- Technical
  - EGNOS provides an increased accuracy,
  - EGNOS integrity provides an upper boundary to the position errors (reliability)

- Access to an authenticated SIS, hence to trusted pseudoranges
  - Easier computation of a trusted PVT
  - Relaxed specifications for the “other sensors”

Scope of project



TACHOGRAPH

Storage

Interface Protocol

Odometer

GNSS

Other sensors

Interface Protocol

Secure PVT

Appli 1 Fleet Management

Appli 2 PAYD Insurance

Appli 3 Road Tolling

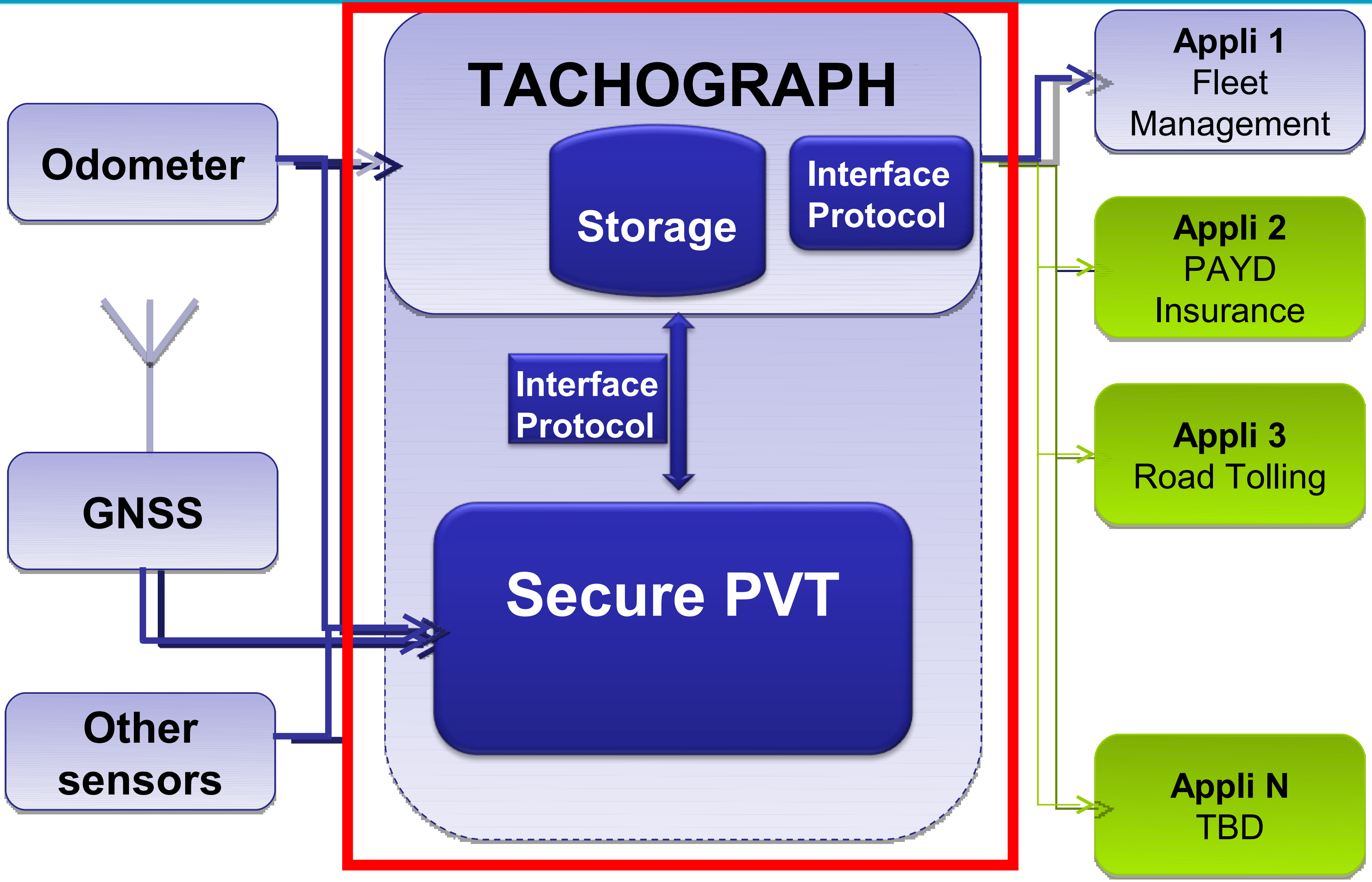
Appli N TBD

Existing

Developed in project

Enabled by project

Augmented Tachograph functional perimeter

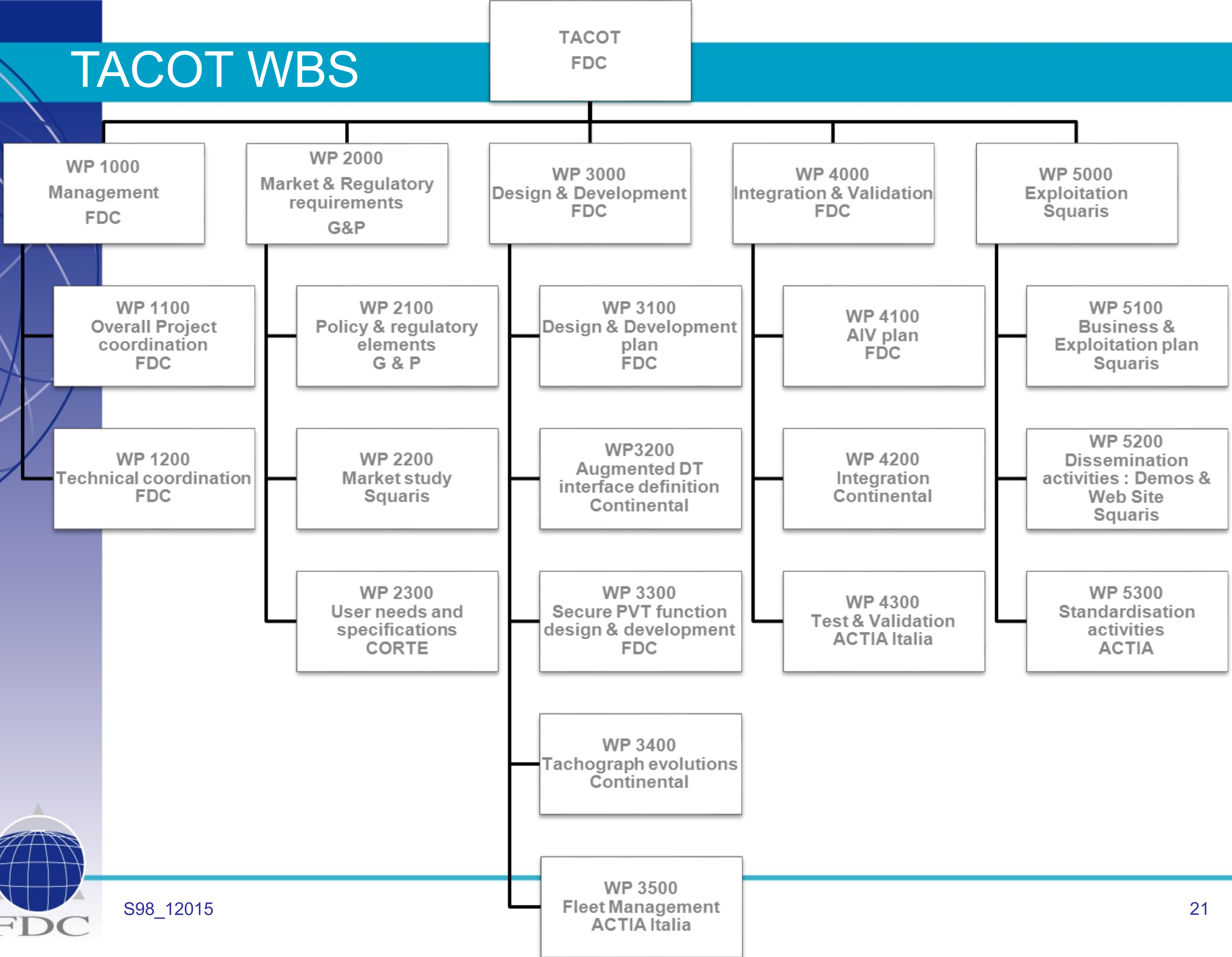


Prototype augmented tachograph

Project outputs

- PVT Augmented **Prototype Tachograph**
- Demonstration of 1 real time application enabled by secure GNSS positions addition (Fleet management)
- “PVT Augmented Tachograph” **Interface Control Document** (including GNSS & Applications interfaces)
- Draft standard derived from above
- Secure GNSS function specifications and **Protection Profile**

TACOT WBS



TACOT
FDC

WP 1000
Management
FDC

WP 1100
Overall Project coordination
FDC

WP 1200
Technical coordination
FDC

WP 2000
Market & Regulatory requirements
G&P

WP 2100
Policy & regulatory elements
G & P

WP 2200
Market study
Squaris

WP 2300
User needs and specifications
CORTE

WP 3000
Design & Development
FDC

WP 3100
Design & Development plan
FDC

WP3200
Augmented DT interface definition
Continental

WP 3300
Secure PVT function design & development
FDC

WP 3400
Tachograph evolutions
Continental

WP 3500
Fleet Management
ACTIA Italia

WP 4000
Integration & Validation
FDC

WP 4100
AIV plan
FDC

WP 4200
Integration
Continental

WP 4300
Test & Validation
ACTIA Italia

WP 5000
Exploitation
Squaris

WP 5100
Business & Exploitation plan
Squaris

WP 5200
Dissemination activities : Demos & Web Site
Squaris

WP 5300
Standardisation activities
ACTIA

Innovation

- PVT security will rely on multi-sensors:
  - EU GNSS (EGNOS & Galileo), GPS and GLONASS
  - Truck onboard sensors (odometers, secure clock,…),
  - Other sensors (time sources, accelero...)
- Our solution will use secure certified technologies and an innovative sensor fusion approach based on Bayesian to detect GNSS spoofing attacks
- Bayesian techniques are field proven e.g.:
  - Fraud detection for banking electronic transaction
  - Threat identification and detection in aerial defense
- This technique :
  - Reduces the sensors fusion complexity,
  - Matches security constraints,
  - Stays at affordable cost

FDC’s way forward

- FDC works together with the CNES to the definition of a cryptographic authentication mechanism for the future release of EGNOS,
- FDC worked with the EC to the definition of the cryptographic authentication mechanism of the Galileo Commercial Service,
- FDC is involved in the definition and the development of the Galileo PRS service,
- Further Transport Applications R&D, e.g. Electronic Tolling, Ecall and Transport of dangerous goods.

Thank you for your attention

www.fdc.eu

pascal.campagne@fdc.eu
alexandre.allien@fdc.eu