Certification of EGNSS Timing Receivers and Services

Roland Bauernfeind

03.11.2016

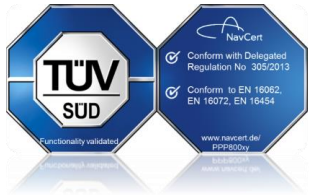
International Timing & Sync Forum 2016,
Time for a Smart Future

NavCert

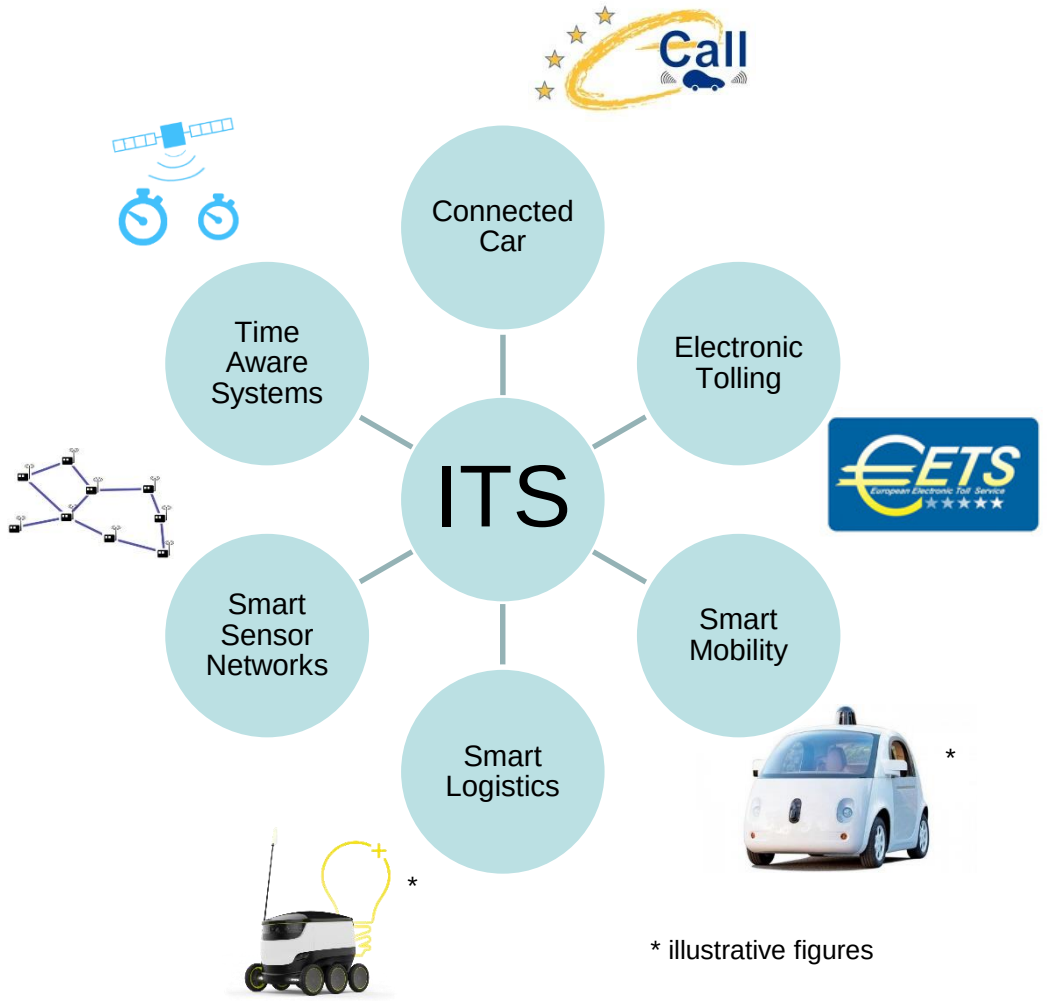
NavCert, “the GNSS-Certifier for ITS”

- 2006 founded as joint venture between TÜV SÜD and OECON
- 2012 became 100%-subsidiary of OECON group
- Office in Munich and Braunschweig

- ISO 17025 accredited Laboratory for GNSS Equipment and Applications
- Notified Body (NB2603) for the European Electronic Toll Service (EETS)
- Certification based on cooperation with TÜV SÜD, certification mark:



- Current R&D-Projects:
  - GNSS: FOSTER ITS, **Robust EGNSS Timing Services**
  - eCall: I_HeERO, EMYNOS



* illustrative figures

Robust EGNSS Timing Services Project

- **Netherlands Aerospace Centre (NLR)**
  Consortium lead
- **Finnish Geospatial Research Institute (FGI)**
  Concept development, testing environment
- **Dutch Metrology Institute (VSL)**
  synchronisation service, business case
- **VTT MIKES Metrology**
  synchronisation service, testing, timing receivers, business case
- **NavCert GmbH**
  Standardisation and Certification
  - Development of standardization roadmap
  - Definition of possible certification schemes based on analysis of stakeholder's opinions

➢ Funding: European Commission – DG GROW

Content

- Overview
  - EGNSS Services (specific Timing Service)
  - Certification Needs
- Certification Entity
  - Qualified by Legal Entity
  - Accredited by Authority
- Specifications and Standards
  - Roadmap
- Summary and Conclusions

Overview - Services

- GNSS time determination capabilities within current portfolio of services
  - Galileo
    - Open Service (OS)
    - Commercial Service – High Accuracy (CS-HA)
    - Commercial Service – Authentication (CS-Auth)
    - Public Regulated Service (PRS)
  - EGNOS
    - Open Service (OS)
    - Safety of Life (SoL) Service
- Performance requirements only for UTC time reference scale, not for the user receiver time solution

- Establishing a specific **Galileo and EGNOS Timing Service (TS)** with associated performance requirements
  - Todays accuracy is more than sufficient for the majority of the current timing applications
  - Focus on providing **robustness and trust**
    - Standardization of reference receiver signal processing, incl. Receiver Autonomous Integrity Monitoring (RAIM)
    - Leveraging Galileo Authentication Features
    - Definition of Certification Schemes

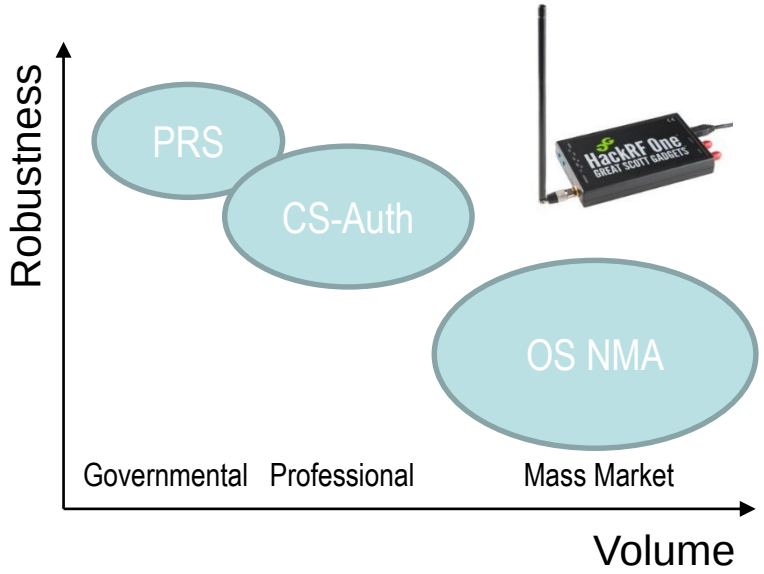
Overview - EGNOS

- Current EGNOS V2 augments the GPS L1 Coarse/Acquisition (C/A) civilian signal
- EGNOS V3 is the second generation of the EGNOS System
  - EGNOS V3 will provide Dual-Frequency (L1/L5) Multi-Constellation (GPS/Galileo) augmentation
  - EGNOS V3 Phases C/D ~2017-2024 (ESA Tender from 06/06/2016)
- Ongoing studies to include also safety critical applications in the maritime and rail sector

- **EGNOS Safety of Life (SoL) Service Certification**
  - EGNOS operator certified as Air Navigation Service Provider (ANSP)
    - Certification requirements baseline - Single European Sky Regulatory package
    - ICAO Standards and Recommended Practices (SARPS) Annex10 Volume I (Radio Navigation Aids)
  - EGNOS Safety of Life Receiver certified according ETSO-C145c/C146c
    - RTCA document DO-229D, Minimum Operational Performance Standards for Global Positioning System/Wide Area Augmentation System Airborne Equipment

Overview - Galileo Authentication

- **Authentication to counter spoofing threats**, the malicious manipulation of navigation signals in order to control position and time estimate of a targeted GNSS receiver
  - Galileo OS **Navigation Message Authentication (NMA)**
    - Authentication at Data Level
    - Enables attack detection (allows ranging under attack)
  - Galileo CS-Auth and Galileo PRS **Spreading Code Encryption (SCE)**
    - Authentication at Signal Level
    - Ranging only with valid keys
      (attacker does not know the PRN chips)



- **Security Certification**, e.g. Digital Tachograph – External GNSS Facility
  - EU Parliament and Council Regulation (EU) No 165/2014 on tachographs in road transport
  - Common Criteria for Information Technology Security Evaluation, ISO/IEC 15408
  - EC DG JRC – IPSC develops Protection Profile (PP), an independent set of security requirements
  - Certification Scheme is provided by the Evaluation Authority, e.g. German Federal Office for Information Security

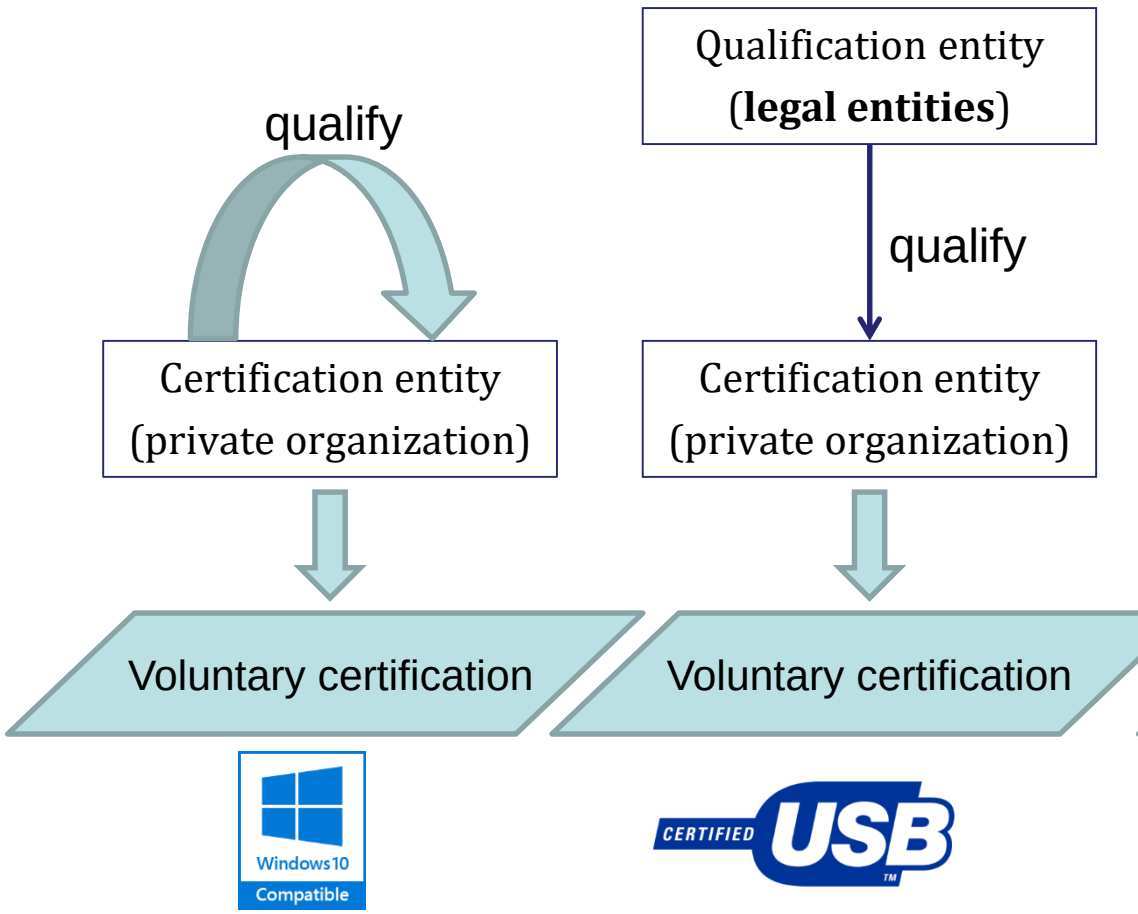
Certification Needs - Timing

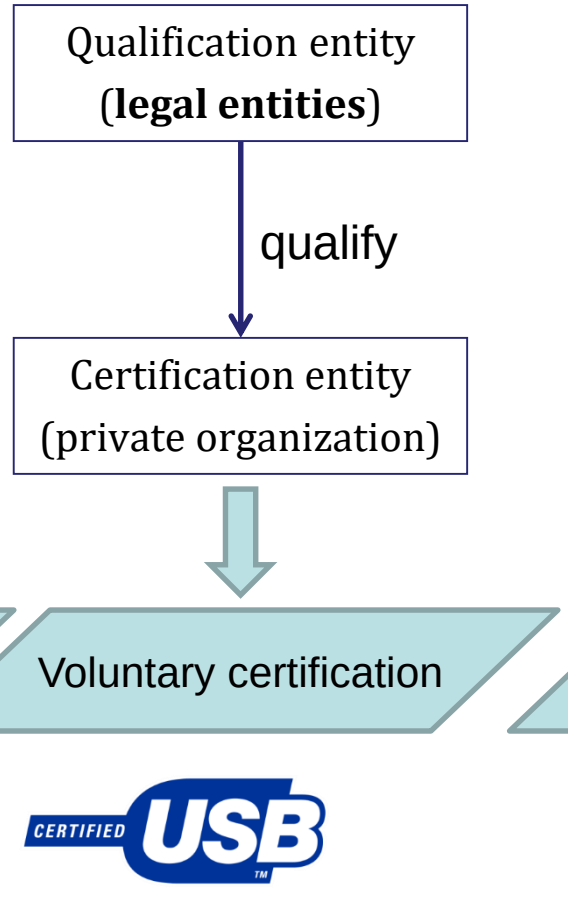
- Certification to support applications within critical infrastructure
  - Performance, Conformance, Security
    - **Receiver processing** against which the system (Galileo/EGNOS) can **ensure the specified performance**
    - **Alternative to common criteria security certification** needed

- Example of alternative certification scheme – company alliance:
  - Fast Identity Online (FIDO) ; “simpler stronger authentication”
    - Specifications and Certification scheme developed by FIDO Alliance
    - Initially conformance specifications, now developing also security specifications
    - Self-validation, to validate that the implementation conforms to the FIDO specifications
    - Documentation is submitted as a request for certification
    - “FIDO® Certified” mark and logo trademark usage is optional (based on license agreement)

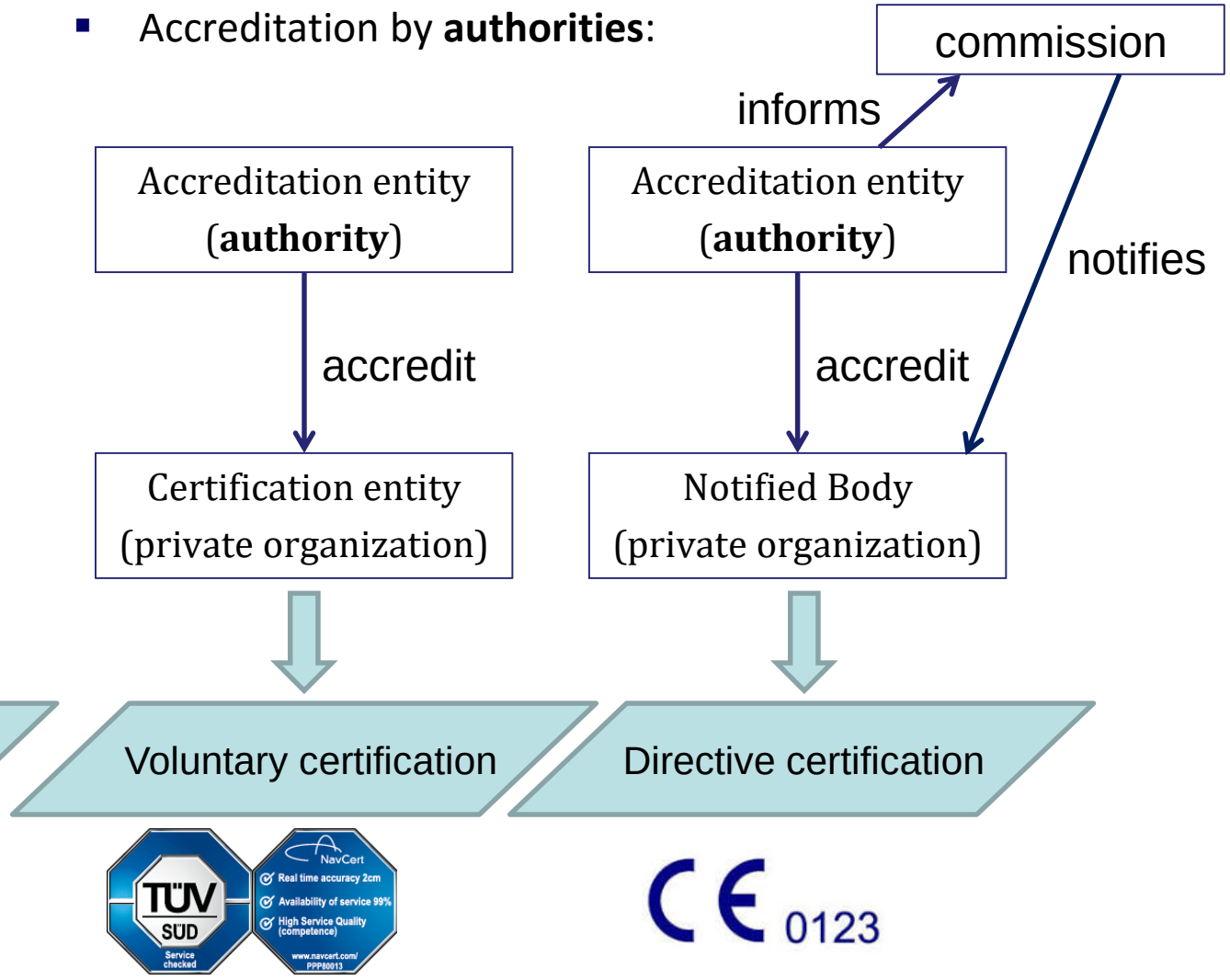
Certification Entity

- Qualification by **legal entities**:



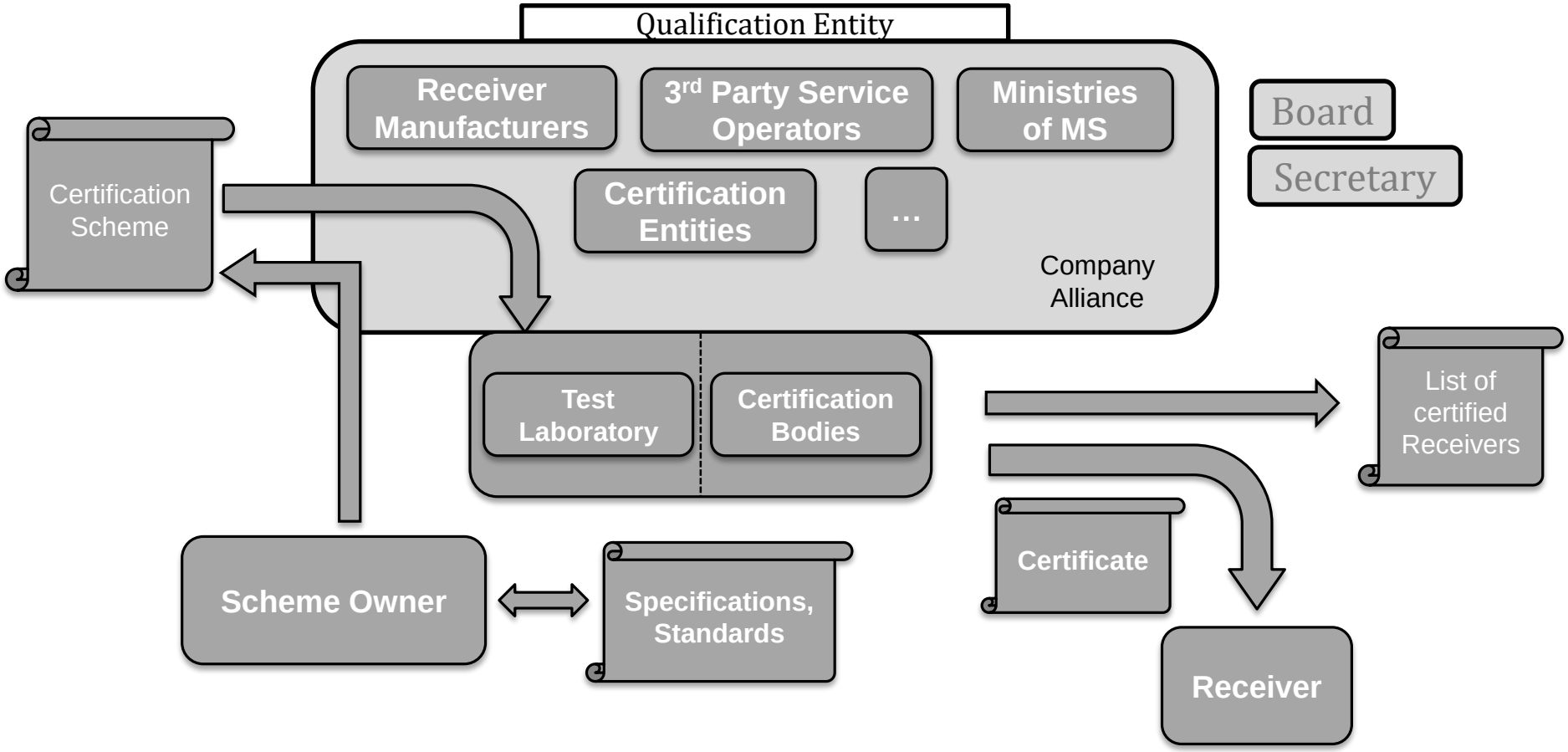


- Accreditation by **authorities**:



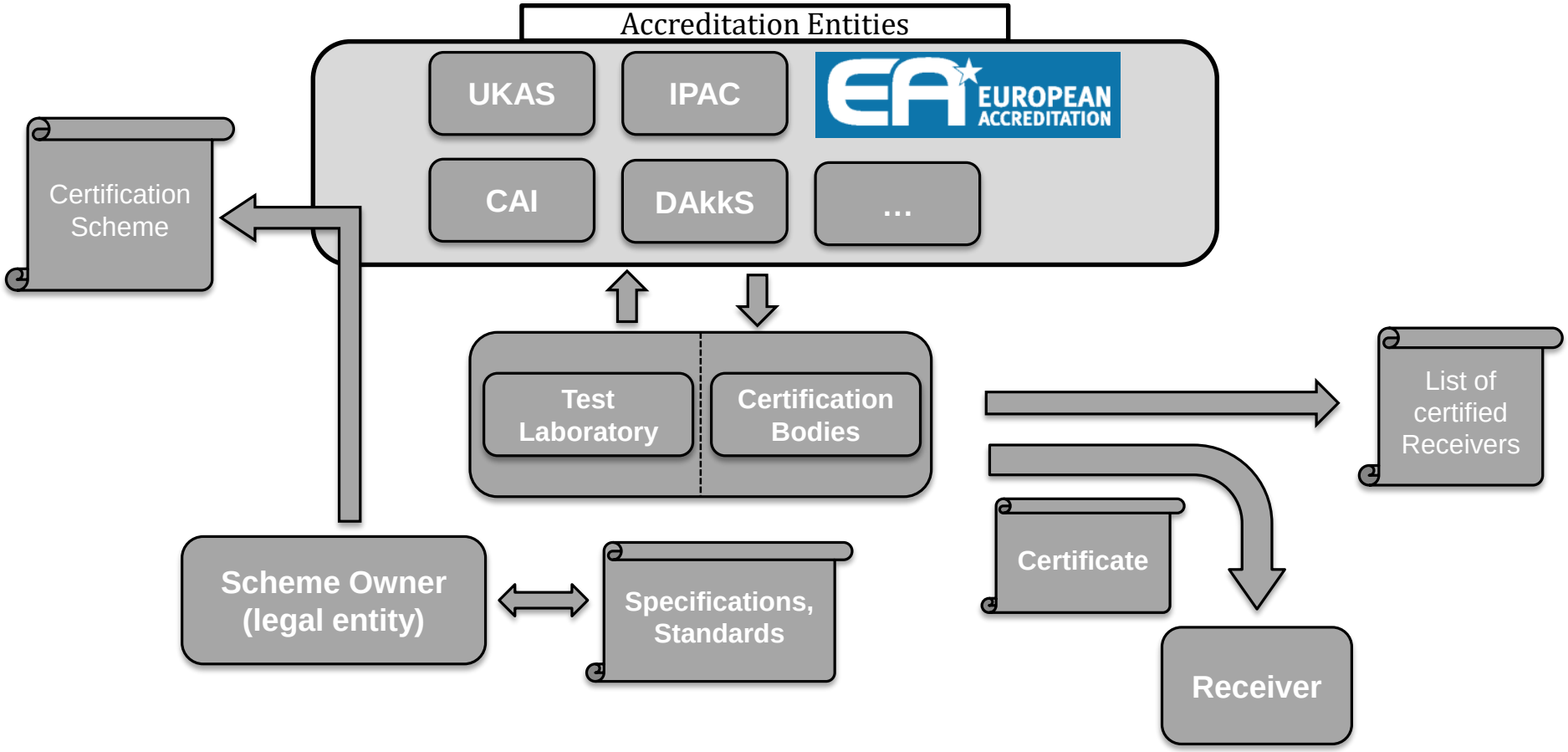
Qualified Certification Entity by Legal Organizations

- Typical association of stakeholders defines from scratch own processes, procedures and legal framework :



Accredited Certification Entity by Authorities

- European agency EA consisting of national accreditation bodies with agreed processes, procedures in an existing legal framework :



Certification Entity

- Comparison of both alternatives
  - Qualification Entity
    - Starting from scratch with freedom of action
    - Complexity in setting up processes, voting rights, membership
    - More flexible and independent solution
    - Company alliance can also develop the specifications
  - Accreditation Entity
    - Well-established, and accepted international organization structures
    - Existing, defined, official processes
    - Use of Accreditation Body is implemented and well known in every member states
    - Time-dependency for accreditation on internal authority processes

Specifications and Standards

- Certification scheme based on Specifications / Standards
  - Issued by Company Alliance or Standards Developing Organization
  - Deliverables differentiate in respect on their degree of openness, consensus and formal approval process

- Timing related Specifications/Standards by organizations
  - GNSS Time Transfer (e.g. CGGTTS-Version 2E)
  - Time-stamping services (e.g. ISO/IEC 18014)
  - Clock Characteristics (e.g. ITU-T G.8272)
  - Precise Time Protocol Profiles (e.g. IEEE C37.238)
  - Performance Standards (e.g. ETSI TS 103 246)

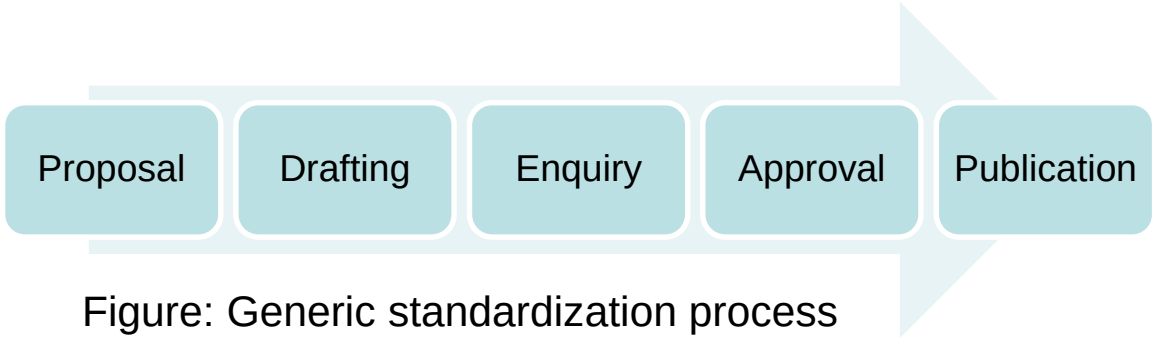


Figure: Generic standardization process

Specifications and Standards

- Work Item Proposal to initiate an Standards project requires
  - Support, e.g. ETSI at least four companies (members)
  - Funding

- Example: Standardization initiated by European Commission Mandates
  - ETSI Technical Committee (TC) Satellite Earth Stations and Systems (SES) / Satellite Communications and Navigation (SCN)
    - Technical Specification (TS) 103 246: GNSS based location systems
    - European Standard (EN) 303 413; GNSS receivers; … ; Harmonized Standard covering the essential requirements of article 3.2 of the Directive 2014/53/EU
  - CENELEC Technical Committee (TC) 5 / Working Group (WG) 1
    - European Standard (EN) 16803: Space - Use of GNSS-based positioning for road Intelligent Transport Systems (ITS)

Summary and Conclusions

- Definition of Galileo Timing Service and EGNOS Timing Service to reflect the needs for timing users and the performance and limitations of the systems.
- Standardization of reference receiver processing for the assurance of specified service performance
- Certification to provide trust

- Standardization (IPR-based) and Certification (registered certification mark) can enable new business models based on licensing

➢ stakeholder's opinions, pros and cons, on possible certification of timing service, timing receiver or timing applications is very welcome (Looking for volunteers)

NavCert GmbH
Tal 26
80331 München

roland.bauernfeind@navcert.de
www.navcert.com

NavCert