Matthias Schreitl

GALILEO DIENSTE & IMPLEMENTIERUNGSSCHRITTE

Signals2Trust Webinar, 16.6.2020

GALILEO PROGRAMM

- **In-Orbit Validation**

4 Satelliten in 2011/2012 gestartet, reduziertes Bodensegment

erste Satelliten mit allen Funktionen für den Vollbetrieb 2014 gestartet

- **Initial Services**: seit 2016

Satelliten (14+4) und Bodensegment sind einsatzfähig
reduzierte Signalverfügbarkeit (Satellitenkonstellation noch nicht vollständig)

jetzt

- **Full Operational Capability**

vollständige Satellitenkonstellation → weltweite Abdeckung

GALILEO SATELLITEN: STATUS

Navigation (22 in service)
Search and Rescue (24 in service)

- 26 satellites in orbit
- 2 in testing (NAV P/L only)
- 1 spare
- 1 unavailable
- 2 no SAR (by design)

GSAT 104 (NAVANT failure)
GSAT 204 (spare, SAR operational)
GSAT 201/202 (not yet in service)

Quelle: ESA

GALILEO SATELLITEN: AUSBLICK

- **12 weitere Satelliten in Produktion**

paarweise ab 2021 gestartet

baugleich mit bisherigen FOC Satelliten (1. Generation)

- **transition satellites**

Übergang von Satelliten der 1. Generation zur 2. Generation

Einführung neuer Technologien

zur Zeit: Dialog mit Industrie zur technischen Ausgestaltung

- **Galileo 2. Generation**

neue Ausstattung auf den Satelliten

neue Services & Signale

GALILEO DIENSTE (SERVICES)

- **Open Service (OS)**
  offenes Signal, weltweiter Dienst zur Positionierung und Zeitsynchronisation, gratis nutzbar
  wird in Zukunft auch die Open Service Navigation Message Authentication (OSNMA) beinhalten

  heutige Präsentation

- **High Accuracy Service (HAS):** gratis Dienst in Ergänzung zum Open Service
  liefert zusätzliche, hochgenaue Daten und bietet damit eine verbesserte Positionierung (Genauigkeit von 20cm)

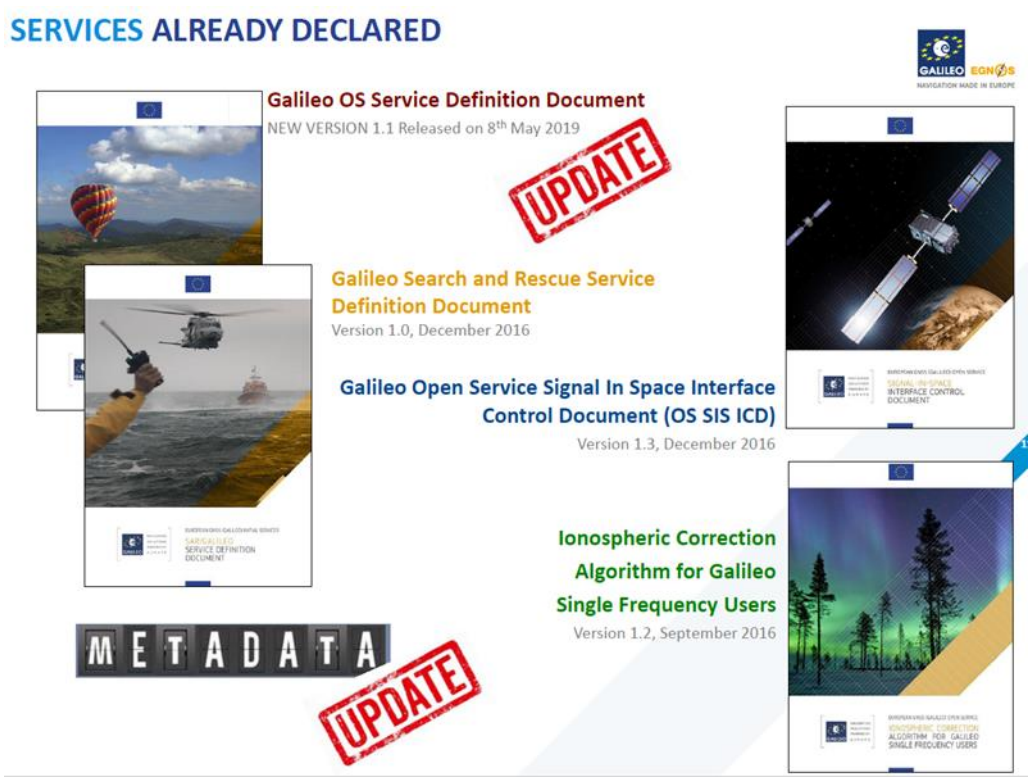
- **Commercial Authentication Service (CAS):** ergänzend zum Open Service,
  bietet Authentifizierungsfunktionen für die Nutzer

  heutige Präsentation

- **Public Regulated Service (PRS)**
  eingeschränkter Zugang: nur für authorisierte Nutzer mit Bedarf an hoher Kontinuität

- **Search and Rescue Service (SAR)**:
  Europas Beitrag zu COSPAS-SARSAT, einem internationalen satellite-basierten Such- und Rettungsdienst zur Erfassung und Lokalisierung von Notrufsignalen

GALILEO DIENSTE: STATUS & AUSBLICK



Quelle: Galileo Service Center

- Referenzdokumente für **bestehende Dienste**: Galileo Service Centers
  https://www.gsc-europa.eu/electronic-library/programme-reference-documents

- **neue Dienste**

– SAR Return Link Service: demnächst verfügbar

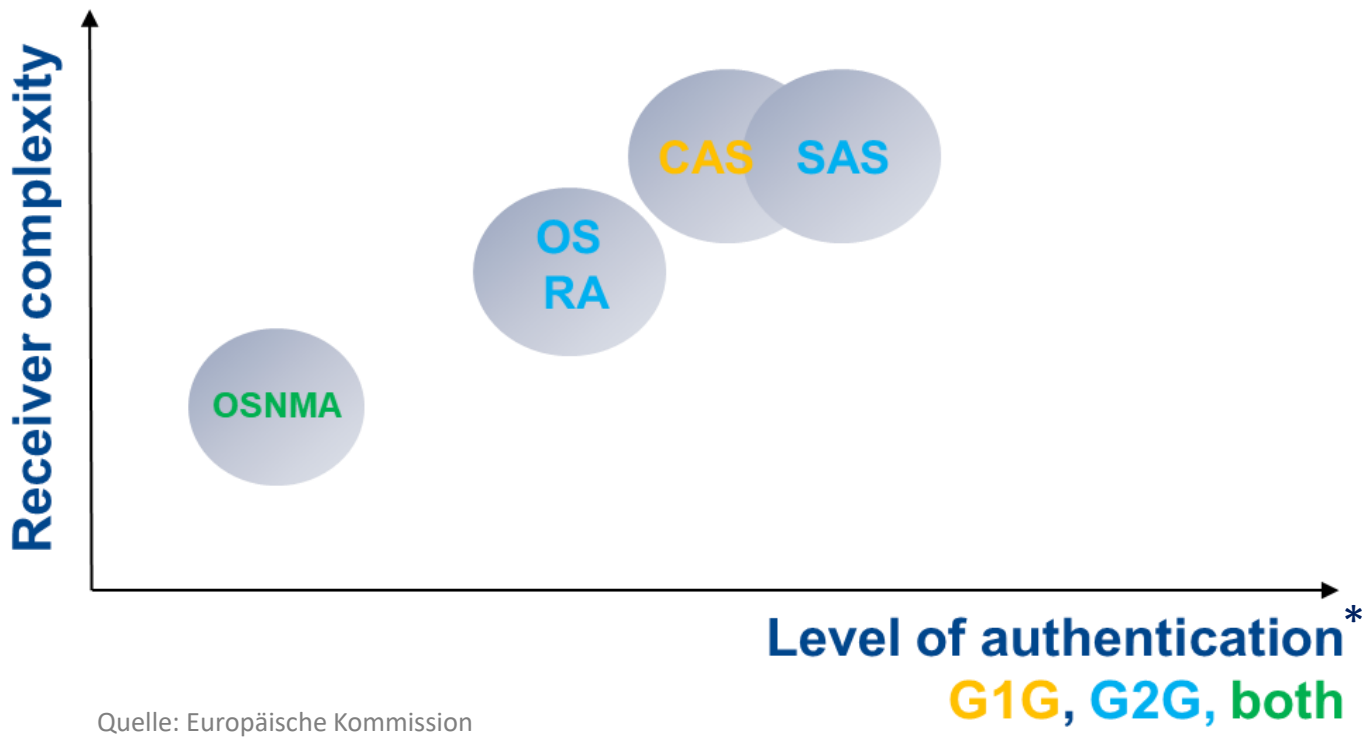
– Open Service Navigation Message Authentication: interne Tests gefolgt von Demonstrationsphase: 2020/2021

– High Accuracy Service: graduelle Einführung ab 2020/2021

– Commercial Authentication Service

– Emergency Warning Service

GALILEO DIENSTE ZUR AUTHENTIFIZIERUNG



Quelle: Europäische Kommission

OSNMA: Open Service Navigation Message Authentication

OSRA: Open Service Ranging Authentication

CAS: Commercial Authentication Service

SAS: Signal Authentication Service

G1G…Galileo 1. Generation

G2G…Galileo 2. Generation

* Robustheit gegenüber spoofing

AUTHENTICATION SERVICE FEATURES

Service	Gen.	Signal	Receiver Requirements	Level of Protection
OSNMA	G1G	E1	Public cryptographic keys Loose time synchronization	Data authentication
OSNMA	G2G	E1, E5	Public cryptographic keys Loose time synchronization	Data authentication
OSRA	G2G	E1, E5	Public cryptographic keys Loose time synchronization Signal Storage and post-processing	Range authentication (periodic, delayed)
CAS	G1G	E6	Public cryptographic keys Partial ground assistance (1) or Decryption module (2)	Range authentication (1: periodic, delayed; 2: real time)
SAS	G2G	E6	Partial ground assistance (1) or security module (2)	Range authentication (1: periodic, delayed; 2: real time)

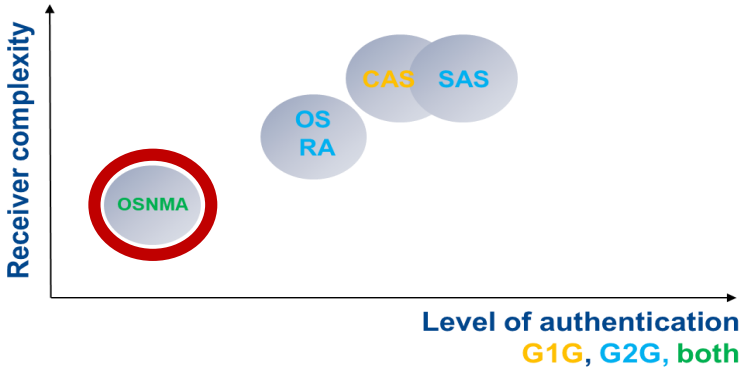
Open Service Navigation Message Authentication

OSNMA

1. Generation

- Authentifizierung der I/NAV Navigationsdaten
- verzögerte Übertragung der kryptographischen Information
- Rückwärtskompatibilität

- grobe Synchronisation mit Referenzzeit erforderlich
- ranging signal nicht authentifiziert



2. Generation

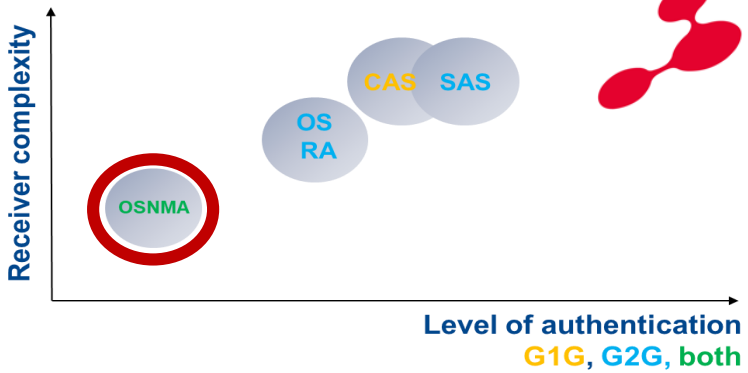
- zusätzliche authentifizierte Information (z.B. ARAIM ISM, EWS, neue G2G Daten)
- bessere Performance (time to first authenticated fix)
- zusätzliche Signalkomponenten zu E1B

ARAIM: Advanced Receiver Autonomous Integrity Monitoring
ISM: integrity support message
EWS: Emergency Warning Service

Open Service Navigation Message Authentication

OSNMA

Implementierungsschritte (1. Generation)



Internal Test Signal → **Public Observation** → **Service**

- intern: ESA & GSA
- Robustheitstests
- Auswahl der Signal Konfiguration

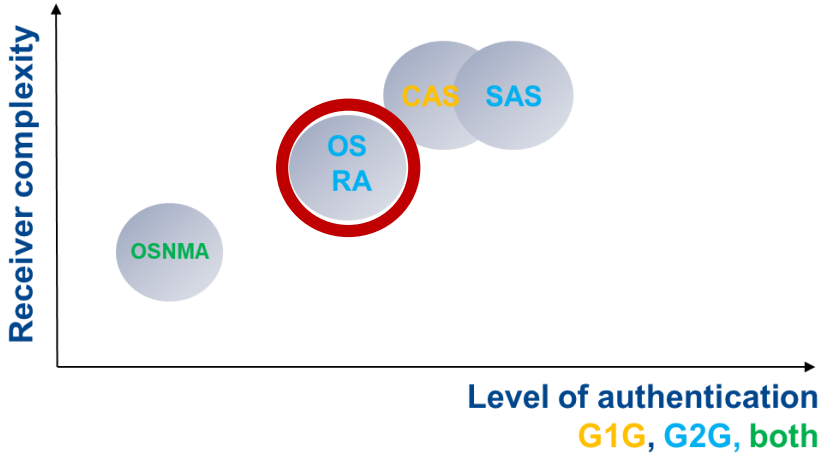
- öffentliche Signal Demonstration (mehrere Monate)
- Unterstützung für Nutzer

- initial service capability
- Service Updates

Open Service Ranging Authentication

OSRA

- Wasserzeichen auf Teilen des OS Signals
- verzögerte Verifikation der Signalauthentizität
- Robustheit gegenüber Attacken auf das ranging signal

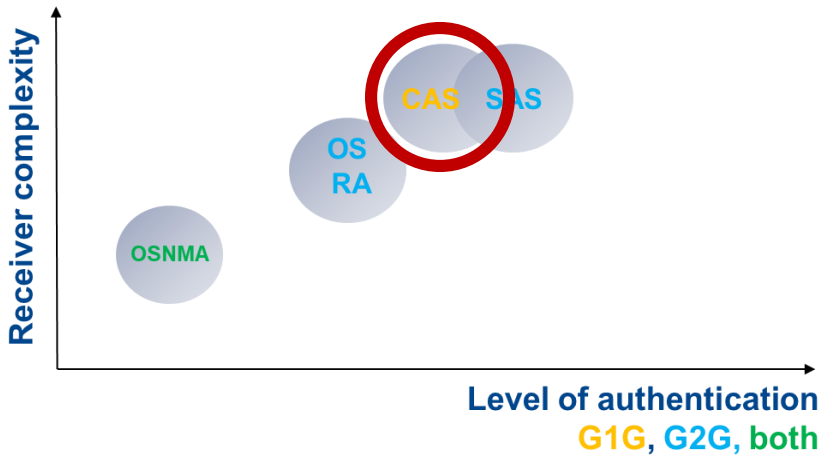


OSRA	**G2G**	**E1, E5**	**Public cryptographic keys Loose time synchronization Signal Storage and post-processing**	**Range authentication (periodic, delayed)**

Commercial Authentication Service

CAS

- Verschlüsselung des E6C Signals
- Details des Service und Zeitplan noch unter Konsolidierung
  1. assisted CAS: Signalauthentifizierung mittels OSNMA,
     Autonomie für Stunden/Tage,
     dann Update erforderlich
  2. stand-alone CAS: Receiver mit symmetrischer, geheimer Verschlüsselung

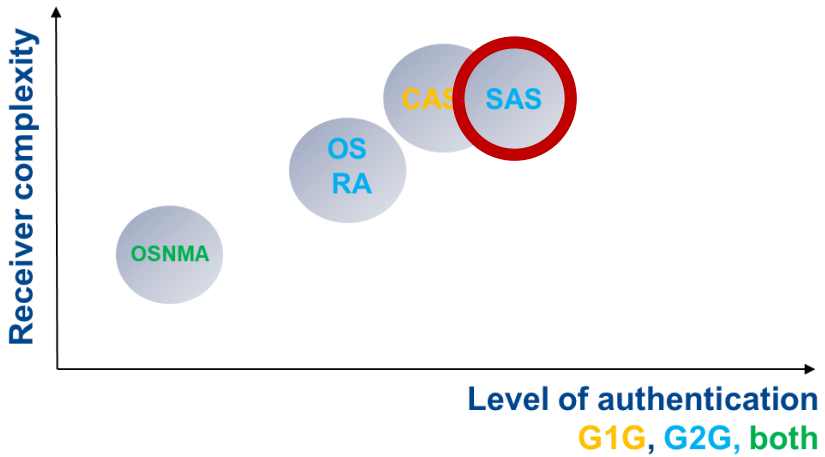


CAS	**G1G**	E6	Public cryptographic keys Partial ground assistance (1) or Decryption module (2)	Range authentication (1: periodic, delayed; 2: real time)
SAS	**G2G**	E6	Partial ground assistance (1) or security module (2)	Range authentication (1: periodic, delayed; 2: real time)

Signal Authentication Service

SAS

- G2G Weiterentwicklung von CAS
- gleiche Funktionalität, aber bessere Performance
- Details werden in der aktuellen Definitionsphase von G2G festgelegt



CAS	**G1G**	E6	Public cryptographic keys Partial ground assistance (1) or Decryption module (2)	Range authentication (1: periodic, delayed; 2: real time)
SAS	**G2G**	E6	Partial ground assistance (1) or security module (2)	Range authentication (1: periodic, delayed; 2: real time)

KOMPLEMENTARITÄT DER DIENSTE

- G1G: Nutzeranforderung (anti-spoofing) vs. minimaler Eingriff ins bestehende System
  → Daten-Authentifizierung mittels OSNMA
  → Signal-Authentifizierung in E6 (wird bereits für verschlüsselte Signale genutzt)
- G2G: mehr Flexibilität durch Neudesign

  → ranging authentification, die keine geheimen, kryptographischen Komponenten im Empfänger erfordert

  → voll autonom, aber „assisted users“ werden berücksichtigt

  → ranging authentification features in allen Frequenzbändern:
  E1 und E5 (OSRA) + E6 (SAS)

  → Daten Authentifizierung: Rückwärtskompatibilität zu OSNMA,
  aber bessere Performance und größere Menge an authentifizierten Daten

Galileo Prize Austria

galileo-masters.eu/austria

Partners

organised by FFG

supported by Federal Ministry Republic of Austria Climate Action, Environment, Energy, Mobility, Innovation and Technology; Science Park The High Tech Incubator Graz; esa business incubation centre Austria

The Austrian Research Promotion Agency (FFG) implements Austria's aerospace policy and connects enterprises, research institutions and researchers with aerospace stakeholders worldwide. Together with strong partners, FFG is scouting for innovative business ideas in order to turn them into high-flyers. No matter if the valley is deep and the mountain high, Austria and the satellite navigation industry are joining forces to promote space-based innovation.

Prizes

powered by

- EUR 6,500 cash prize for the winner, EUR 1,000 for 1st runner-up, EUR 500 for 2nd runner-up
- Technical and business support by experts from the space domain
- Mentoring programme with experts from science and business
- Evaluation and development of the winner's business model
- Fast-tracked access to ESA BIC Austria 2-year programme offered for a period of two months at the ESA BIC in Graz (additional EUR 50,000 if eligible)
- The winner will benefit from a free trip to the Awards Ceremony 2020 (max. budget EUR 1,000)
- Extra EUR 10,000 Cash Prize if your concept gets selected as Galileo Masters 2020 Overall Winner
- Chance to win one of six tailored Galileo Incubation prizes worth up to EUR 62,000 each