Signals2Trust?

Webinar zur Verlässlichkeit und Robustheit von satellitenbasierten Positions- und Zeitdaten

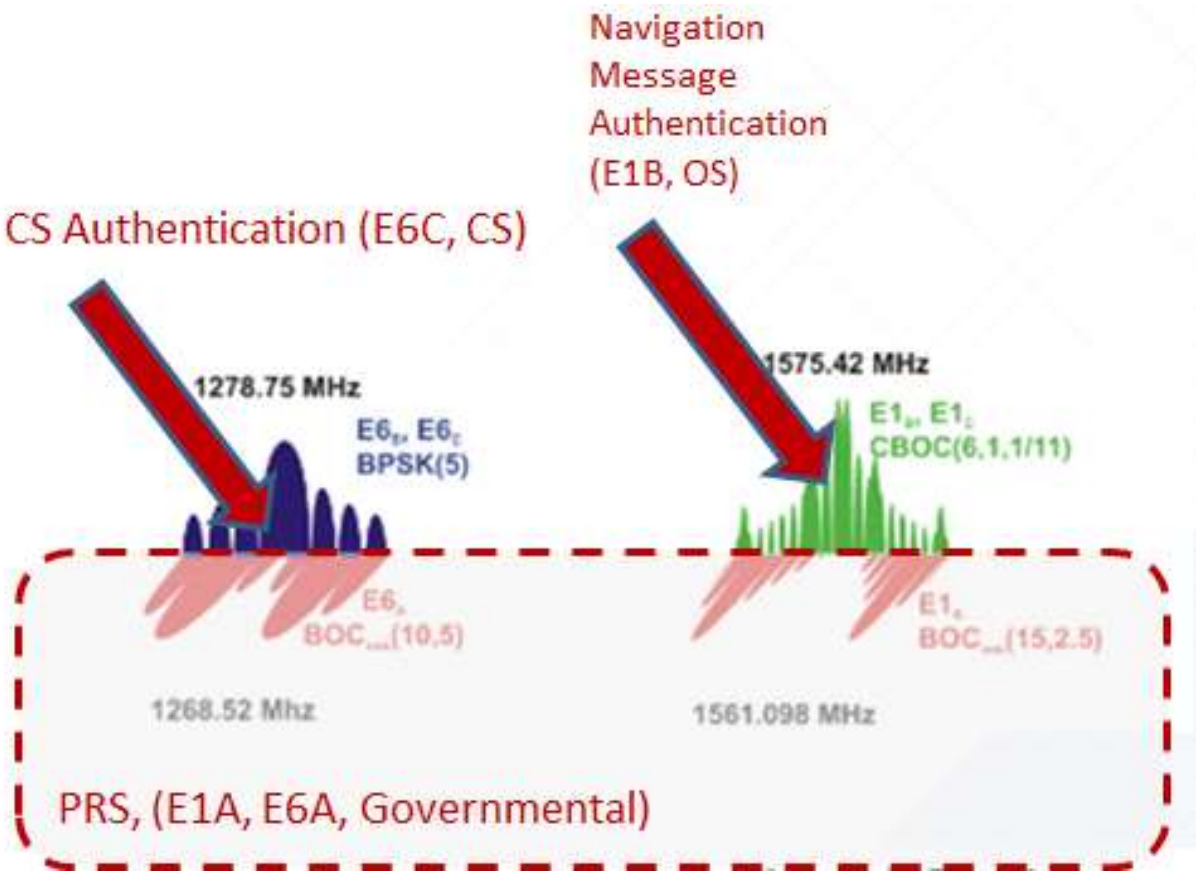
Dienstag, 16. Juni 2020, 10-12 Uhr

Robert Weber
Department Geodäsie und Geoinformation
FB Höhere Geodäsie
TU-Wien

Galileo Authentication Services
(G1G Satellitengeneration)

- OSNMA (Open Service Navigation Message Authentication)
- CAS (Commercial Service Authentication)
- PRS (Public Regulated Service)

Galileo Authentication Services



Quelle: Galileo Authentication – A Programme and Police Perspective,
I. Fernandez-Hernandez et al. , 69. Astr. Congress Bremen , 2018

Galileo Authentication Services

Galileo OS –NMA Tesla	Galileo CAS Nav + Spreading Codes	GPS Nav + spreading codes Chimera	Galileo PRS Governmental
E1-B	E6-C (E6-B,E1-B)	L1C	E1-A, E6-A
I/NAV	I/NAV, TOW	C/NAV , TOW	
open	encrypted		encrypted
needs: E1 receiver	needs E1,E6 receiver	needs L1C receiver	needs special receiver
Tests 2020	2023/24 ?	2023/24 ?	

Optionen - Authentifizierung

- Authentifizierung der Navigationsnachricht (NMA)
  oder
  Authentifizierung der Spreading Codes (Ranging Signale)
  oder
  beides

- Optionen : symmetric versus asymmetric key techniques
  symmetric -> mit secret key (geheim) wird Message vom Satelliten verschlüsselt und vom User dekodiert (Geheimhaltung?)
  asymmetric -> secret key wird aufgeteilt in private key (geheim, Systembetreiber) und public key (User)

- **Galileo ->** ‚TESLA chain' verwendet eine Mischung
  asymmetric/symmetric für OS-NMA
  TESLA=Timed Efficient Streamed Loss-Tolerant Authentication

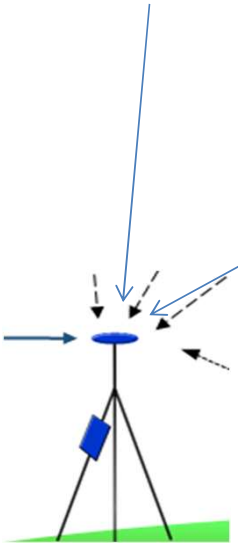
- **GPS** -> ‚Chimera' verwendet
  asymmetric für C/Nav Authentifizierung
- und voraussichtlich symmetric für Spreading Codes

Galileo OS-NMA Approach (TESLA)

key 0 = seed key
key N = root key
key i = f (key 0)
key N = f (key 0)

MAC mit Hilfe von key i generiert;
MAC = f(key i) +f(I/NAV);
Satelliten senden I/NAV und MAC

key i wird zeitverzögert nachgesendet
key i = f(key0)



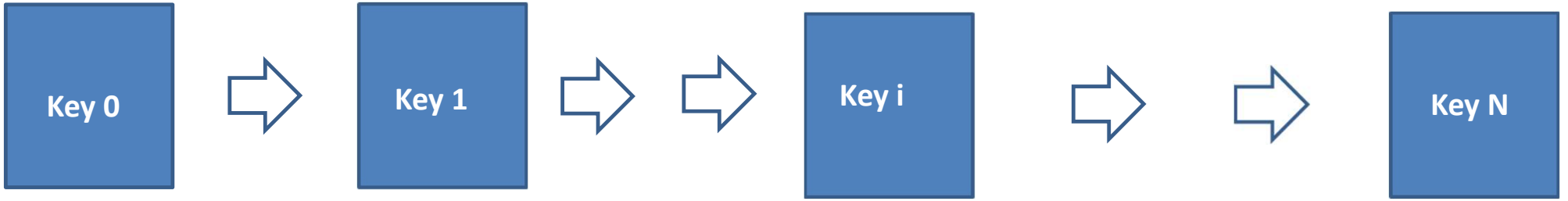
1. Receiver prüft ob key i Teil der TESLA Kette
2. Nutze key i um zu prüfen ob Nav.Message und MAC von selber Quelle

I/NAV = E1 Navigation Message

MAC = Message Authentication Code

TESLA=Timed Efficient Streamed Loss-Tolerant Authentication

Chain of Keys (Schlüssel)
One way function f



Seed key geheim, System

Root key, muss Receiver bekannt sein

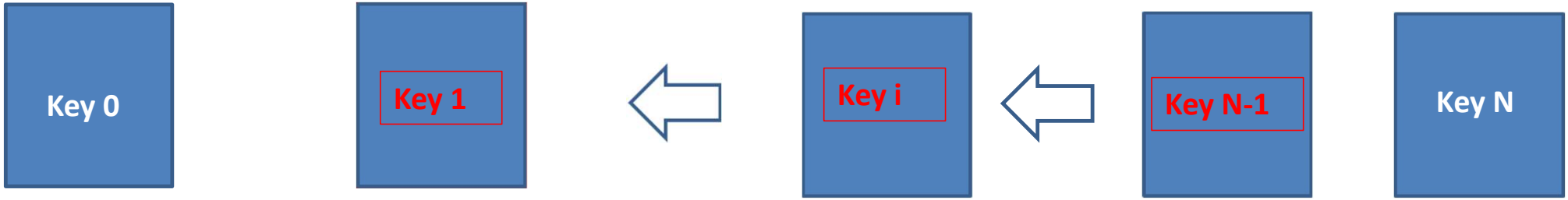
$$\text{Key } 1 = f^{1}(\text{key } 0),\ \text{Key } i = f^{i}(\text{key } 0),\ \text{Key } N = f^{N}(\text{key } 0)$$

Jeder Schlüssel der Kette K_i wird aus dem vorhergehenden Schlüssel K_{i-1} mittels der Funktion f erzeugt $K_{i+1} = f(K_i)$. Die Funktion f ist leicht zu berechnen,

aber faktisch nicht invertierbar.

Der Nutzer kann also nicht auf den Schlüssel K_{i-1} schließen.

Zeitliche Nutzung der Schlüssel durch Galileo



Seed key geheim, System

Root key, muss Receiver bekannt sein

Die Satelliten verwenden die Schlüssel in der Reihenfolge beginnend mit K_{n-1} bis hin zum Schlüssel K_1.

Dem Nutzerreceiver muss der Root Key K_n vorab über terrestrische Netze bekannt sein

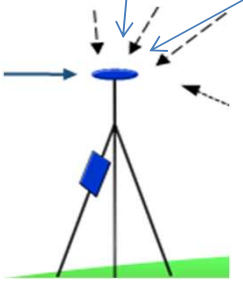
Galileo OS-NMA Approach (TESLA)

key 0 = seed key
key N = root key
key i = f (key 0)
key N = f (key 0)

MAC generiert mit Hilfe von key i;
MAC = f(key i) +f(I/NAV);
Satelliten senden I/NAV und MAC

key i wird zeitverzögert nachgesendet
key i = f(key0)

1. Receiver prüft ob key i Teil der TESLA Kette
2. Nutze key i um zu prüfen ob Nav.Message und MAC von selber Quelle



I/NAV = E1 Navigation Message

MAC = Message Authentication Code

TESLA=Timed Efficient Streamed Loss-Tolerant Authentication

Prozessfolge

- Satellit generiert mittels key i und I/NAV einen MAC
- Satellit sendet I/NAV und MAC
- **Empfänger speichert I/NAV und MAC**
- Satellit sendet **zeitverzögert** key i
- Receiver authentifiziert key i mit Funktion f und root key N
- Receiver generiert mittels key i, I/NAV und Funktion f den MAC
- Wenn korrekt -> I/NAV = authentifiziert

- **Prozess startet im Satelliten mit key i-1**

Vorausetzungen:
Satellit und Receiver müssen grob zeitsynchronisiert sein.
Zeitverzögerung der Schlüsselaussendung um zumindest die Signallaufzeit
um Spoofing zu verhindern.

Probleme: gleicher key oder unterschiedliche keys bei verschiedenen Satelliten;
gleichzeitig abgesendete Signale kommen zu unterschiedlichen Zeiten im Receiver an;

OS-NMA (Zusammenfassung)

- Authentifizierung der Navigationsnachricht
  I/Nav auf Signal E1b
- OS NMA liefert nur Information, dass Broadcast Message korrekt ist; PVT ist nicht gesichert da range measurements manipuliert sein können
- PVT Authentication gelingt nur über Authentication der Ranging Signale
  (E6 Authentifizierung)

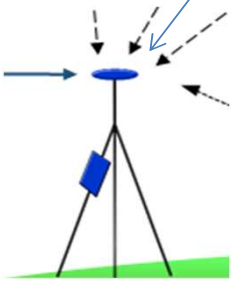
Chimera Prinzip (GPS)

Chips Message Robust Authentication

Satelliten senden C/NAV und key 1;
Key 1 = f(C/NAV)
Key 1=private

Range Signals werden mit CHIMERA ebenfalls codiert

Nutze key 2 um zu prüfen ob Navigation Message und key 1 aus der selben Quelle stammen



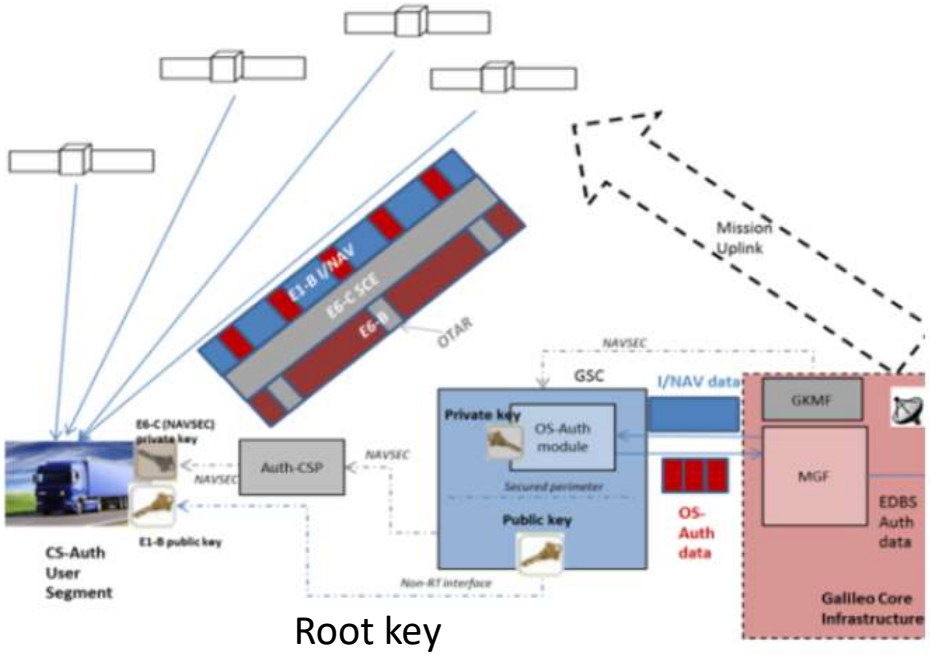
Key 2 wird über Terrestrische Netze übertragen;
Key 2 =public key

Schlüssel (keys) werden zeitverzögert über Satellit oder , Public Key Infrastructure‘ versendet

Commercial Authentication Service

- (wahrscheinlich) kostenpflichtiger Authentication Service
- Verschlüsselt auch Ranging Information (spreading codes)
- E6C Pilot Signal wird mit Schlüssel kodiert
- Schlüssel ist jedem CAS Empfänger bekannt (Sicherheit?)
- E6B freier Datenkanal, liefert neben HAS auch
  Daten zum ‚Over the air re-keying' und Bias (DCB) Daten
  zum Positionieren mittel E6 und I/NAV Navigationsinfo
- I/NAV Authenticated mittels OS-NMA

Galileo Authentication Service Architecture



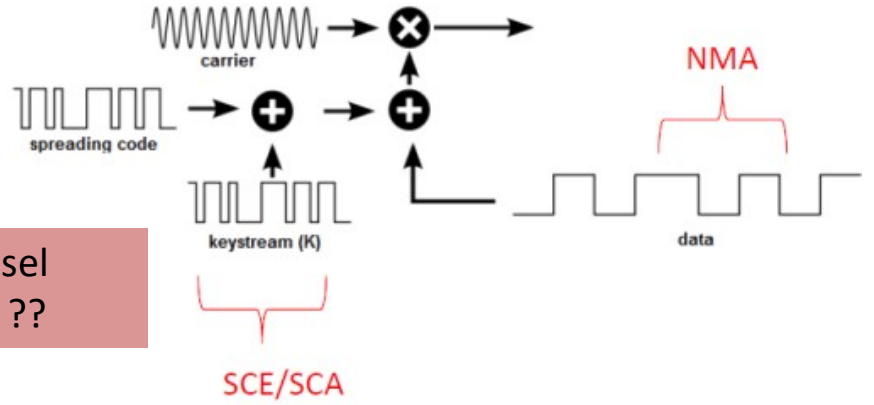
Root key

	CS authentication	
	Specifications common to OS and CS: Authentication of geolocation information	**Specifications related to CS: Authentication through encrypted codes**
General specifications	Provision of authentication data for OS geolocation information contained in the signals	Signal authentication through encrypted codes contained in the signal itself.
Components of the signals used	E1, component E1-B for the authentication data for OS geolocation information	E6, component E6-B for the access data to the encrypted codes and component E6-C (pilot)
User segment specifications	Data authentication via encryption (asymmetrical protocol and public cryptographic key)	Signal authentication via encryption (private cryptographic key)
Geographical coverage	Global	Global

Übersicht der Unterschiede zwischen OS-NMA und dem Galileo CAS (Commercial Authentication Service)

Quelle: Galileo Authentication – A Programme and Police Perspective, I. Fernandez-Hernandez et al. , 69. Astr. Congress Bremen , 2018

Schlüssel
Sicher ??



E6-C pilot Verschlüsselung

Commercial Service Authentication Service CAS

‚Assisted' versus ‚Stand-Alone'

- Summary of information concerning the technical architecture status
  - Updated CAS architecture
  - OSNMA updates/improvements anticipated and documented in ICD 1.1

- The main update concerns the proposal of an Assisted CAS conceived to loose receiver requirements in order to ease CAS adoption

No key storage by the user receiver means no anti tampering requirements which have high cost

Raw data storage requires a specific receiver capability already available in some receivers on the market. Additional cost is low

Characteristic	A - CAS	S - CAS
GNSS receiver type	Dual frequency (E1 E6)	Dual frequency (E1 E6)
Need of raw GNSS data storage at receiver side	Yes	No
Navigation signals decryption by GNSS receiver	No	Yes
Need of a network connection	Occasionally (e.g. once every week)	No. Only in case of recovery from system compromise
Authenticated PVT (real time)	Delayed	Real time
Authenticated PVT (update)	Available with given periodicity	At least once per second
Anti-tampering characteristic for receiver	Not needed: the receiver does not store any secret key	Required. Specific solutions from service providers can be put in place to relax this requirement.
Service provider needed	Depends on service provision scheme	Required for user management and key protection*

* A distinction exists between the service providers and the key distributor(s) which provides secret keys

Summary/General Update

- **OSNMA**:
  - ICD and guidelines under review.
  - OSNMA part of new Smart Tachograph regulation (2021, spec and SIS needed before)
  - Public Test Phase starting Q2/2021
  - Service Opening 2022/2023
- **CAS:**
  - A-CAS Assisted Authentication (Internet Support)- without fee?
  - S-CAS Stand Alone Comm. Authentication (Close to Real-Time)
- **PRS**
- Higher Level of Robustness
- Regulated User Groups