GPS and Galileo Signal Authentication Using Quasi-Zenith Satellite System (QZSS) Signal

United Nations/Finland Workshop on
the Applications of Global Navigation Satellite Systems

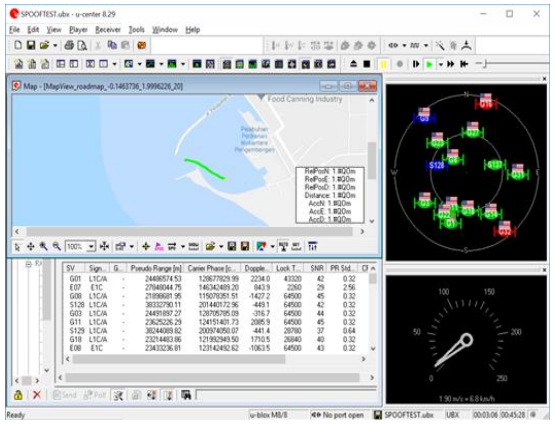
Dinesh MANANDHAR, Associate Professor (Project)

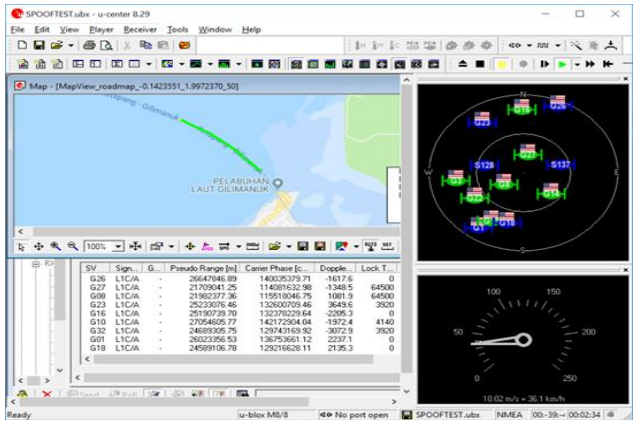
Center for Spatial Information Science, The University of Tokyo

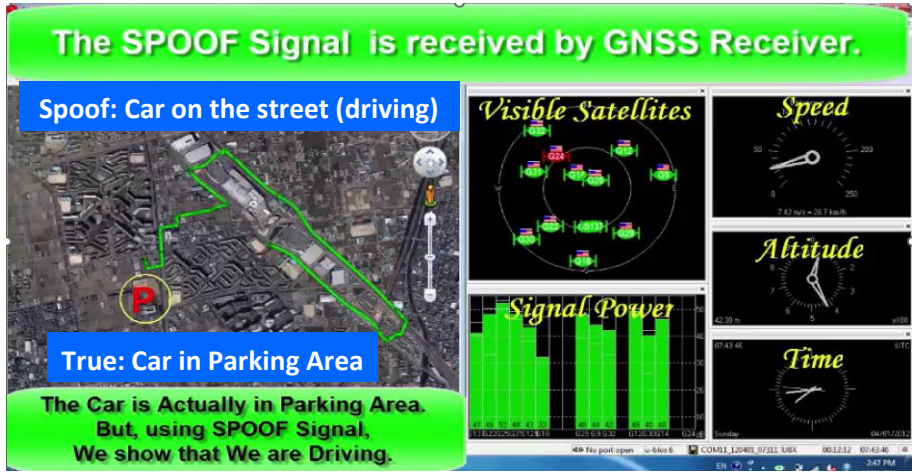
dinesh@csis.u-tokyo.ac.jp

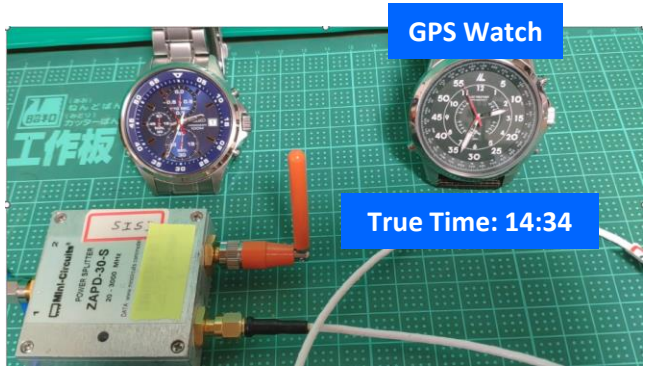
Spoofing Problems

GNSS devices can be spoofed
A low-cost SDR device can be used to transmit GNSS signals









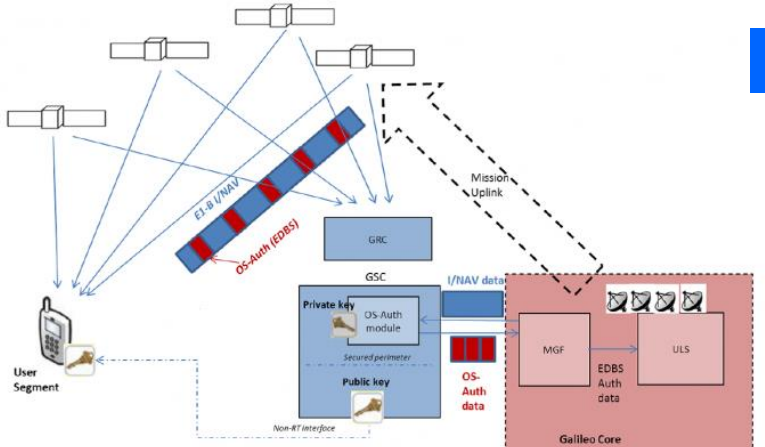
How to Detect / Protect Spoofing Attacks?

Hardware Level	RF Level	Signal Monitoring	Signal Encryption	Navigation Message Authentication
➢ Multi Antenna ➢ Direction of Arrival	➢ AGC Monitoring ➢ RF Fingerprint	➢ P-Code Reference ➢ RAIM or ARAIM ➢ Signal Sanity Check ➢ Multi-Correlator	➢ PRN Code Encryption ➢ NAV Message Encryption	➢ Broadcast Digital Signature of NAV Message
➢ Impact on Receiver Hardware	➢ FW/SW Modification ➢ Little Impact on Hardware	➢ FW/SW Modification		
			➢ No PVT Solution until Decryption	➢ PVT Solution available even if Authentication is not performed
		➢ Fully Backward Compatible		➢ Fully Backward Compatible
		➢ Possible to Implement on Existing Signals		➢ Possible to Implement on Existing Signals
➢ Spoofing attacks may be identified but difficult to verify ➢ Authentication is not possible			➢ Spoofing attacks can be detected and verified ➢ Authentication is possible	

Current Status on Signal Authentication

Galileo OS NMA

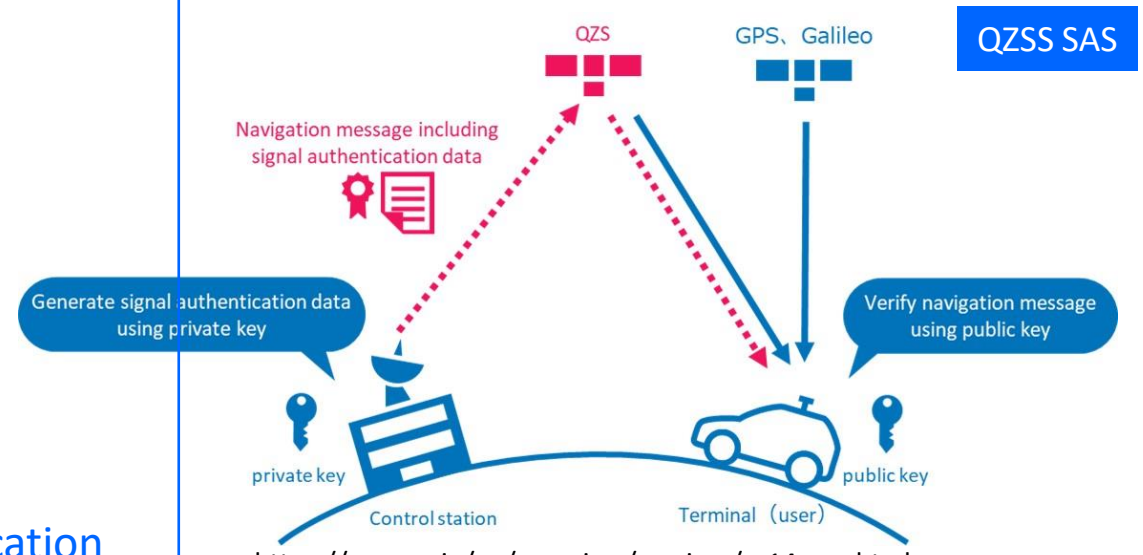
- Authentication of OS E1b (I/NAV)
- Navigation Data Authentication
- Based on NMA using TESLA



https://gssc.esa.int/navipedia/index.php/Galileo_Open_Service_Navigation_Message_Authentication

QZSS SAS (Signal Authentication Service)

- Authentication of
  - QZSS L1C/A/B (LNAV)
  - QZSS L1C (CNAV-2)
  - QZSS L5 (CNAV)
  - GPS L1C/A (LNAV)
  - GPS L1C (CNAV-2)
  - GPS L5 (CNAV)
  - Galileo E1b (I/NAV)
  - Galileo E5a (F/NAV)
- Navigation Data Authentication
- Based on NMA, Digital Signature Verification



https://qzss.go.jp/en/overview/services/sv14_sas.html

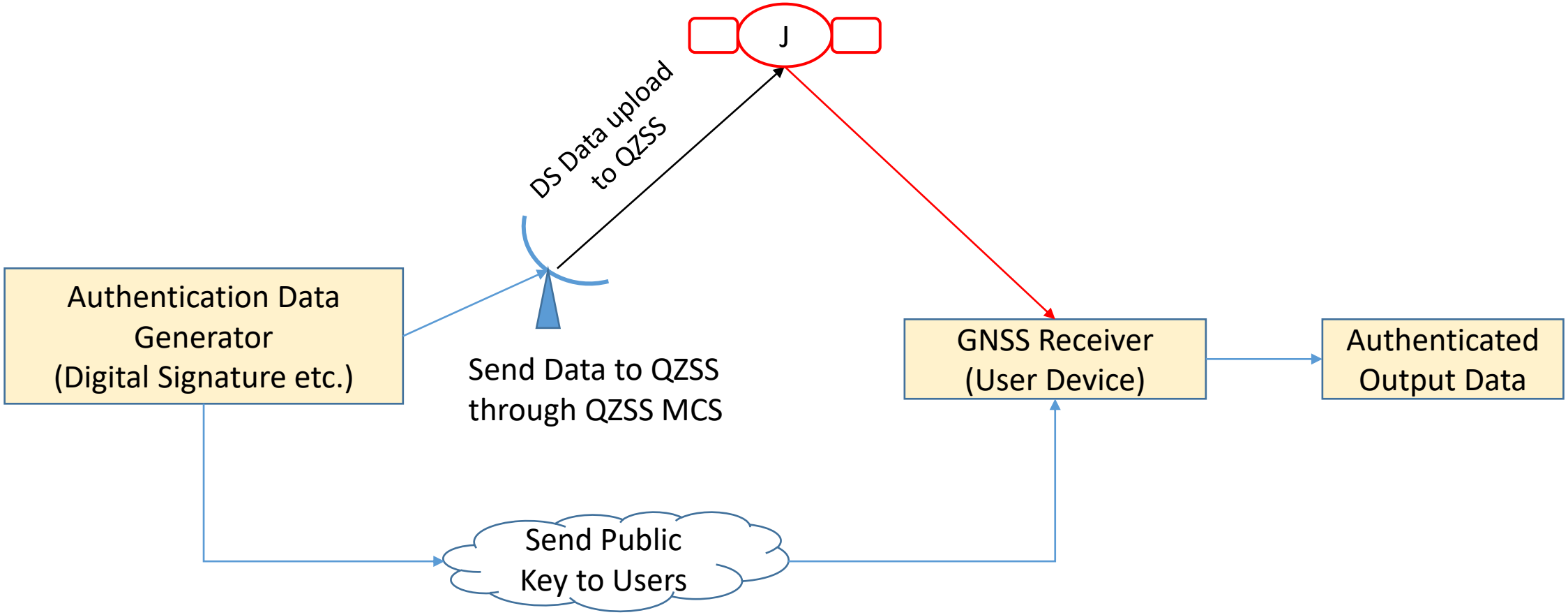
QZSS Signal Authentication Service (QZSS-SAS)

- QZSS authenticates QZSS using QZSS Navigation Messages (LNAV, CNAV, CNAV-2)
- QZSS authenticates both GPS and Galileo using QZSS L6E Message

Signal used for Authentication	Signals to be Authenticated			Remarks
QZSS LNAV, CNAV, CNAV-2	QZSS LNAV, CNAV, CNAV-2	NA	NA	Self-Authentication
QZSS L6E	NA	GPS LNAV, CNAV, CNAV-2	NA	Cross-Authentication
	NA	NA	Galileo I/NAV, F/NAV	

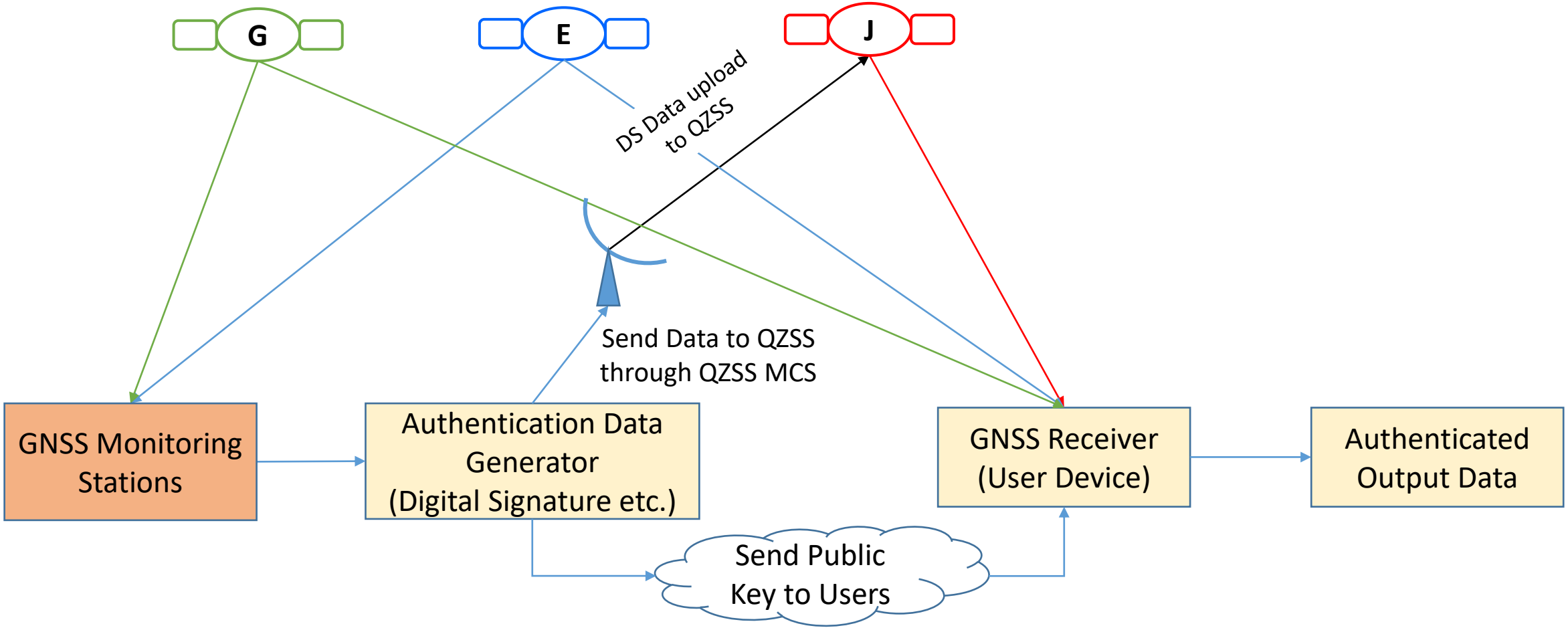
QZSS Signal Authentication by QZSS

- NMA (Navigation Message Authentication) based Signal Authentication.
- Broadcast Digital Signature of QZSS Navigation Message using one of the Navigation Messages of the Signal.

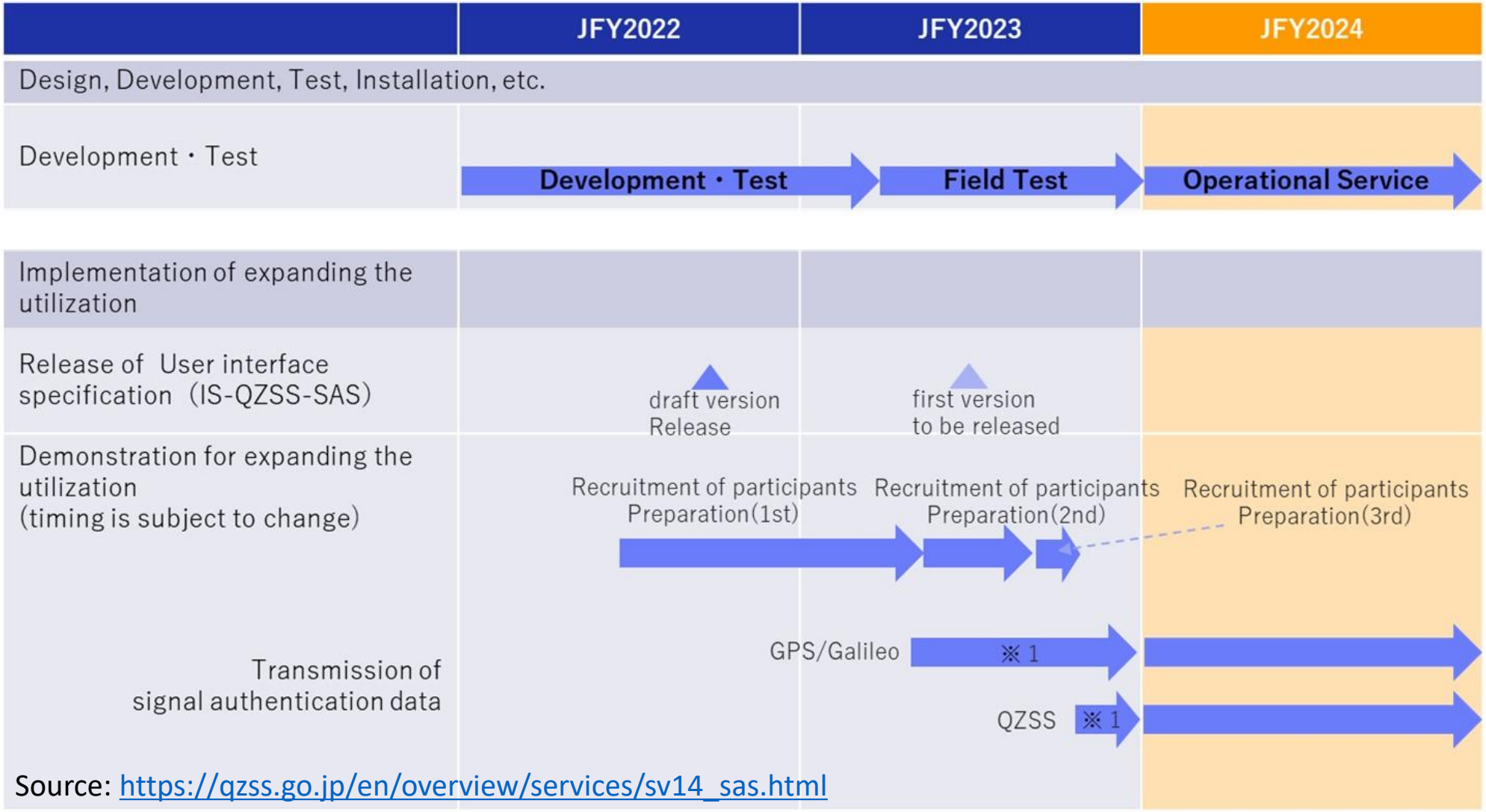


GPS and Galileo Signal Authentication by QZSS

- NMA (Navigation Message Authentication) based Signal Authentication.
- Broadcast Digital Signature of GPS and Galileo Navigation Message using QZSS L6E Signal.



QZSS SAS Schedule



Source: https://qzss.go.jp/en/overview/services/sv14_sas.html

QZSS SAS IS Document

Refer QZSS SIS IS document for technical details on QZSS signal authentication

https://qzss.go.jp/en/technical/ps-is-qzss/ps-is-qzss.html

	Performance Standard (PDF)	Interface Specification (PDF)	Service Performance Evaluation
Satellite Positioning, Navigation and Timing Service	PS-QZSS-003 (Mar.17, 2022 / 1.1MB)(*)	IS-QZSS-PNT-004 (Jan. 25, 2021 / 2.3MB)	Satellite Positioning, Navigation and Timing Service
		IS-QZSS-PNT-005 (Oct. 24, 2022 / 3.9MB)(**)	
Sub-meter Level Augmentation Service (SLAS)		IS-QZSS-L1S-005 (Feb. 3, 2023 / 1.0MB)	Sub-meter Level Augmentation Service (SLAS)
Centimeter Level Augmentation Service (CLAS)		IS-QZSS-L6-005 (Sep. 21, 2021 / 1.4MB)	Centimeter Level Augmentation Service (CLAS)
Satellite Report for Disaster and Crisis Management (DC Report)		IS-QZSS-DCR-010 (Jan. 24, 2022 / 4.5MB)	-
Positioning Technology Verification Service		IS-QZSS-TV-003 (Dec. 27, 2019 / 0.9MB)	-
MADOCA-PPP		IS-QZSS-MDC-001 (Feb. 28, 2022 / 3.3MB)	MADOCA-PPP
Signal Authentication Service	-	IS-QZSS-SAS-001_Draft-002 (Jan. 24, 2023 / 2.7MB)	-

Quasi-Zenith Satellite System

Interface Specification

Signal Authentication Service

(IS-QZSS-SAS-001)

Draft-002

(January 24 2023)

Cabinet Office

3 Signal Authentication Services

QZSS provides signal authentication services for QZSS L1C/A, L1C/B, L1C and L5 signals. It is done by transmitting Navigation Message Authentication (NMA) data embedded into the navigation messages of the respective QZSS signals. A NMA data is a portion of digital signature computed from the navigation message of a signal that has to be authenticated. For example, if QZSS L1C/A signal has to be authenticated, sub-frames 1, 2 and 3 of L1C/A signal are used to compute a digital signature. This digital signature is then reformatted to insert in Sub-frame 5. The satellite broadcasts this signal with NMA data in sub-frame 5. Table 3-1 shows the list of QZSS signals that is used to authenticate the respective QZSS signals. QZSS L1C/A signal is used to authenticate L1C/A signal. Similarly, L1C signal is used to authenticate L1C signal and L5 signal is used to authenticate L5 signal.

QZSS also provides signal authentication services for GPS L1C/A, L1C, L5 signals and Galileo E1b and E5a signals. It is done by transmitting NMA data embedded into the navigation messages of QZSS L6E signal to authenticate GPS and GALILEO signals. Table 3-2 shows the list of GPS and Galileo signals that is authenticated by using QZSS L6E signal.

Table 3-1: QZSS signals that will be used to authenticate respective QZSS navigation messages

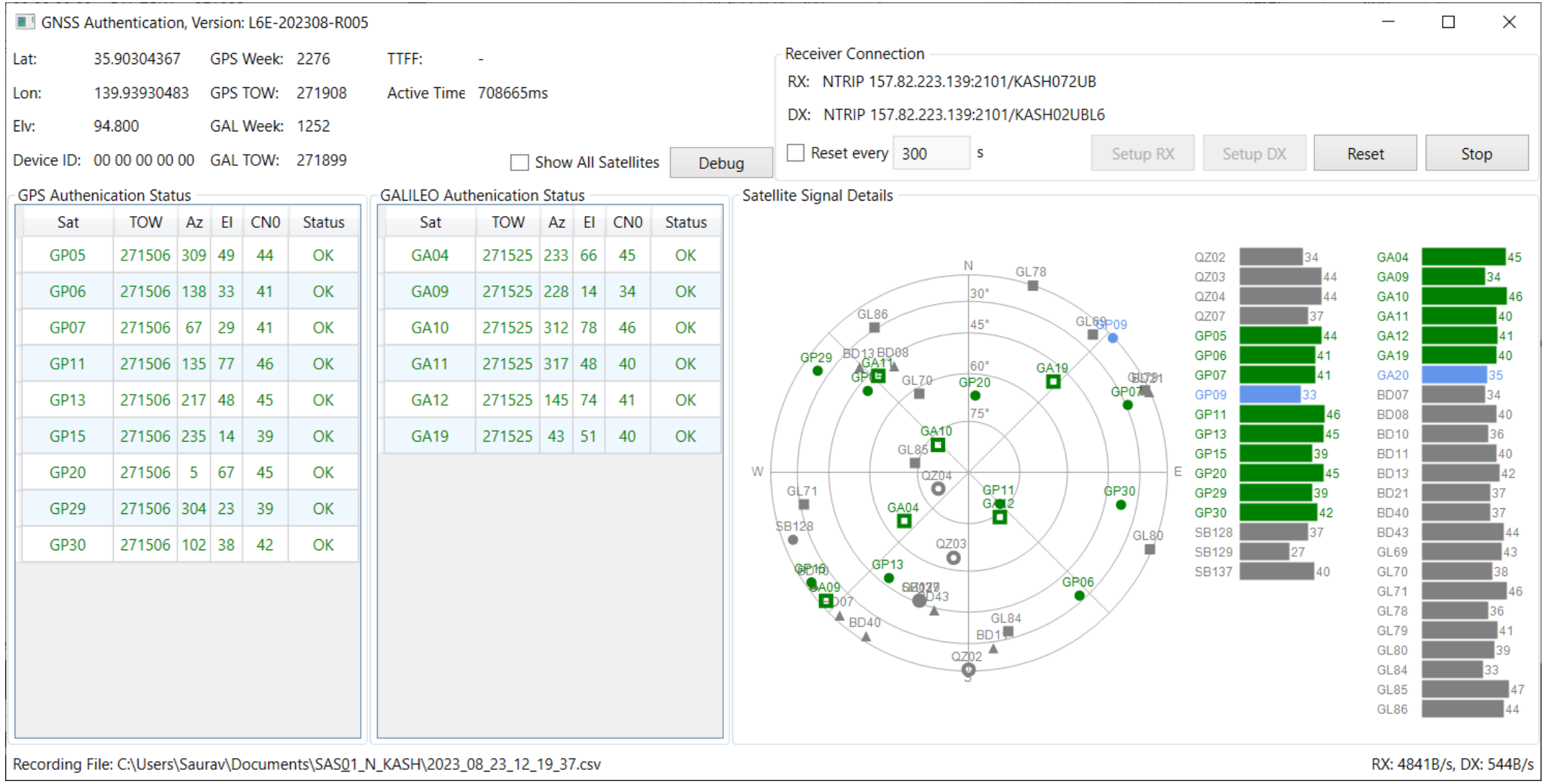
SV ID	QZSS Signals with QZSS Navigation Message Authentication				Satellite Orbit Type	Comments
	PRN ID	Signal	Signal	Signal	Orbit	
QZS01	193	L1C/A	L1C	L5	QZO	Eligible if operational
QZS02	194	L1C/A	L1C	L5	QZO	
QZS04	195	L1C/A	L1C	L5	QZO	
QZS1R	196	L1C/A	L1C	L5	QZO	Switching from L1C/A to L1C/B in the future
	203	L1C/B	-	-		
QZS05	197	L1C/A	L1C	L5	QZO	Switching from L1C/A to L1C/B in the future
	204	L1C/B	-	-		
QZS03	199	L1C/A	L1C	L5	GEO	
QZS06	200	L1C/A	L1C	L5	GEO	Switching from L1C/A to L1C/B in the future
	205	L1C/B	-	-		
QZS07	201	L1C/A	L1C	L5	(Q)GEO	Switching from L1C/A to L1C/B in the future
	206	L1C/B	-	-		

Table 3-2: QZSS signal that will be used to authenticate GPS and Galileo navigation messages

SV ID	QZSS L6E Signal with GPS and Galileo Navigation Message Authentication			Satellite Orbit Type	Comments
	PRN ID	Signal	GNSS Navigation Message	Orbit	
QZS01	203	-	-	QZO	
QZS02	204	L6E	GPS LNAV GPS CNAV GPS CNAV2 Galileo I/NAV Galileo F/NAV	QZO	
QZS04	205	L6E		QZO	
QZS1R	206	L6E		QZO	
QZS05	207	L6E		QZO	
QZS03	209	L6E		QGEO	
QZS06	210	L6E		QGEO	
QZS07	211	L6E		QGEO	

5

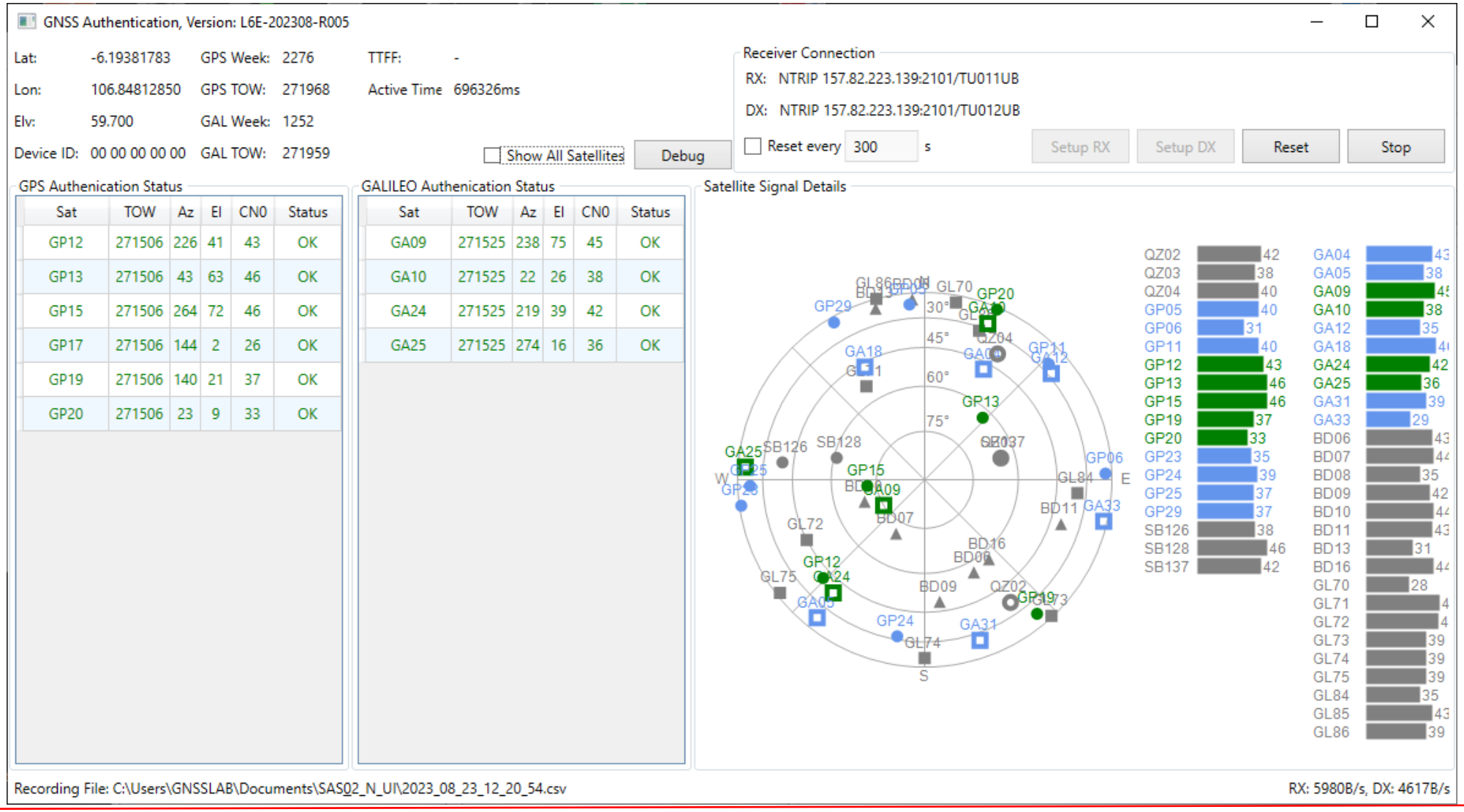
QZSS Signal Authentication of GPS and Galileo: Tokyo Test Results



Sat	TOW	Az	El	CN0	Status
GP05	271506	309	49	44	OK
GP06	271506	138	33	41	OK
GP07	271506	67	29	41	OK
GP11	271506	135	77	46	OK
GP13	271506	217	48	45	OK
GP15	271506	235	14	39	OK
GP20	271506	5	67	45	OK
GP29	271506	304	23	39	OK
GP30	271506	102	38	42	OK

Sat	TOW	Az	El	CN0	Status
GA04	271525	233	66	45	OK
GA09	271525	228	14	34	OK
GA10	271525	312	78	46	OK
GA11	271525	317	48	40	OK
GA12	271525	145	74	41	OK
GA19	271525	43	51	40	OK

QZSS Signal Authentication of GPS and Galileo: Jakarta Test Results



QZSS Signal Authentication of GPS and Galileo: Kathmandu Test Results

GNSS Authentication, Version: L6E-202308-R005

Lat: 27.69258420 GPS Week: 2276 TTFF: -
Lon: 85.33936920 GPS TOW: 271920 Active Time 696773ms
Elv: 1278.842 GAL Week: 1252
Device ID: 00 00 00 00 00 GAL TOW: 271915

Show All Satellites | Debug

Receiver Connection
RX: NTRIP cors.aviyaan.com:2101/KTM1UB
DX: NTRIP cors.aviyaan.com:2101/KTM1L6
Reset every 300 s | Setup RX | Setup DX | Reset | Stop

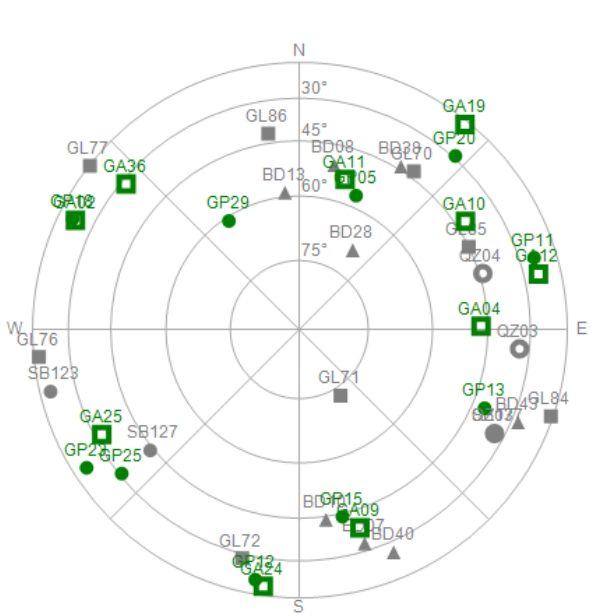
GPS Authenication Status

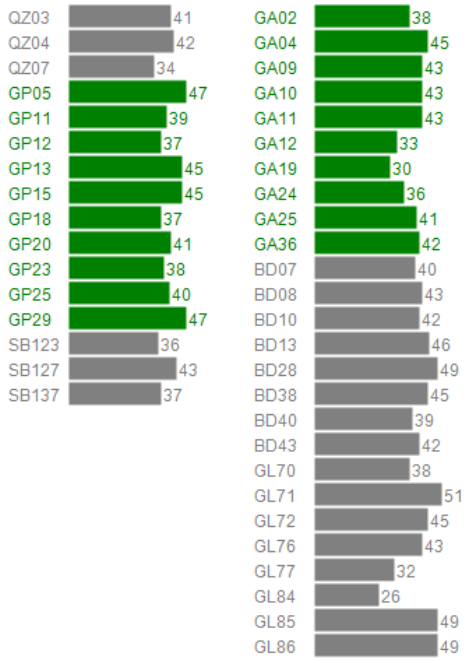
Sat	TOW	Az	El	CN0	Status
GP05	271506	23	57	47	OK
GP11	271506	73	23	38	OK
GP12	271506	190	18	37	OK
GP13	271506	113	41	45	OK
GP15	271506	167	44	45	OK
GP18	271506	296	19	37	OK
GP20	271506	42	29	41	OK
GP23	271506	237	18	38	OK
GP25	271506	231	31	40	OK
GP29	271506	327	61	47	OK

GALILEO Authenication Status

Sat	TOW	Az	El	CN0	Status
GA02	271525	296	21	38	OK
GA04	271525	89	47	45	OK
GA09	271525	163	39	43	OK
GA10	271525	57	42	43	OK
GA11	271525	17	54	43	OK
GA12	271525	77	23	33	OK
GA19	271525	39	9	30	OK
GA24	271525	188	14	36	OK
GA25	271525	242	33	41	OK
GA36	271525	310	32	42	OK

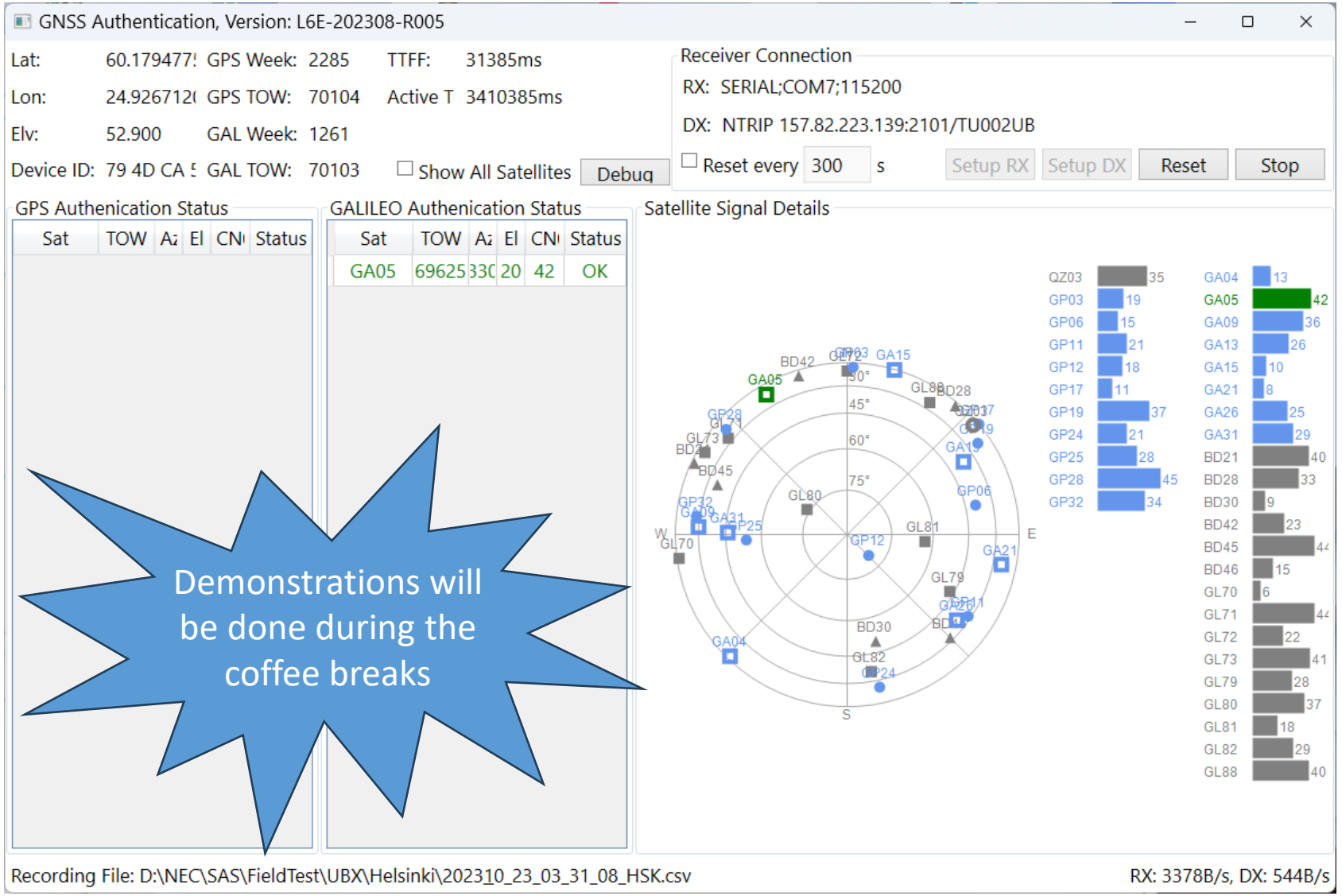
Satellite Signal Details





Recording File: C:\Users\Saurav\Documents\SAS01_N_KATH\2023_08_23_12_19_58.csv
RX: 6997B/s, DX: 544B/s

QZSS Signal Authentication of GPS and Galileo: Helsinki Test Results

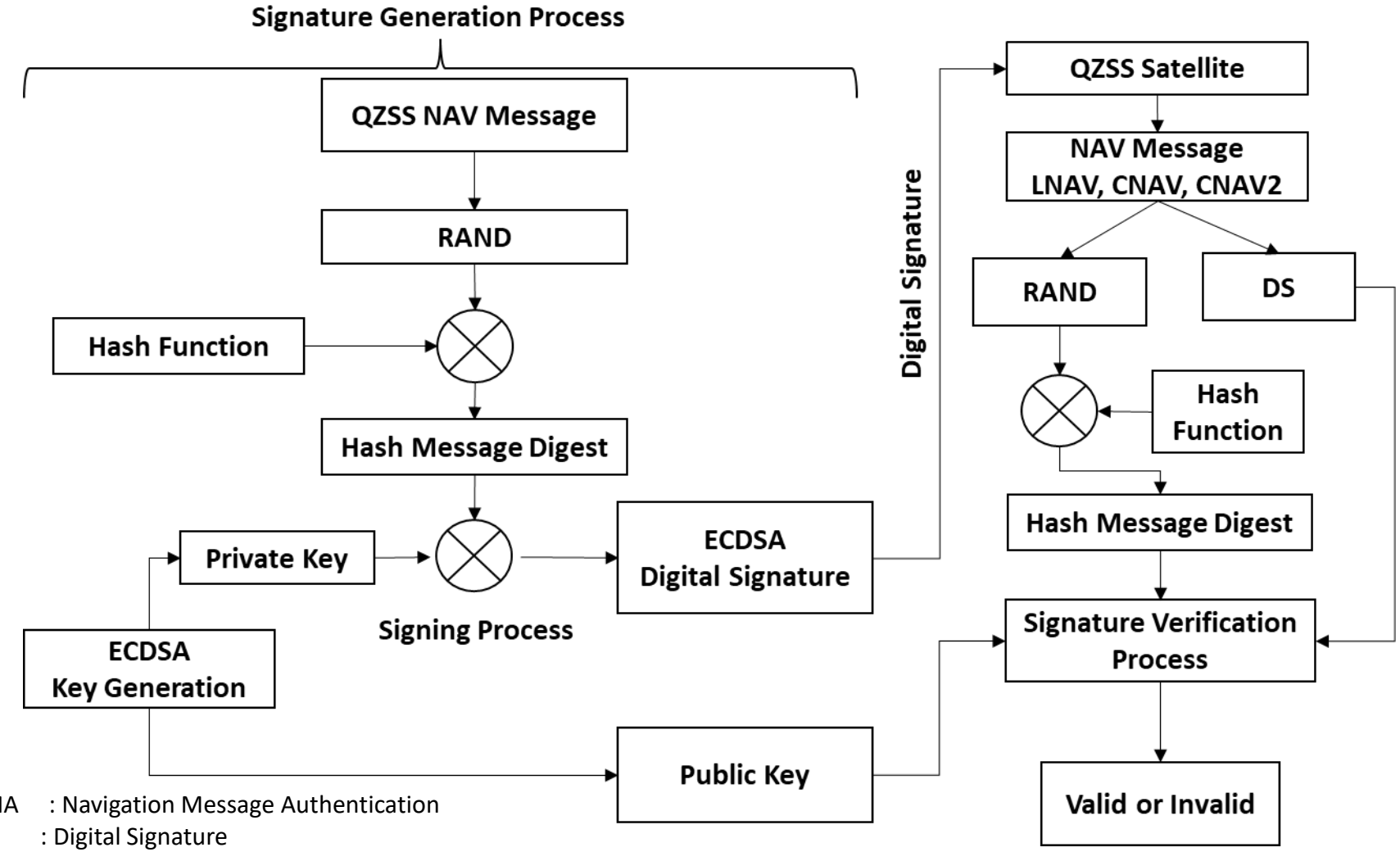


Summary and Future Works

- Authentication of GPS and Galileo signals is done successfully
- The following KPIs (Key Performance Indicators) will be conducted in the near future
  - TTFA (Time To First Authentication)
  - TBA (Time Between Authentication)
  - AER (Authentication Error Rate)
- Authentication tests will be conducted using different types of receivers
- Any receiver that outputs navigation data bits is authentication compatible

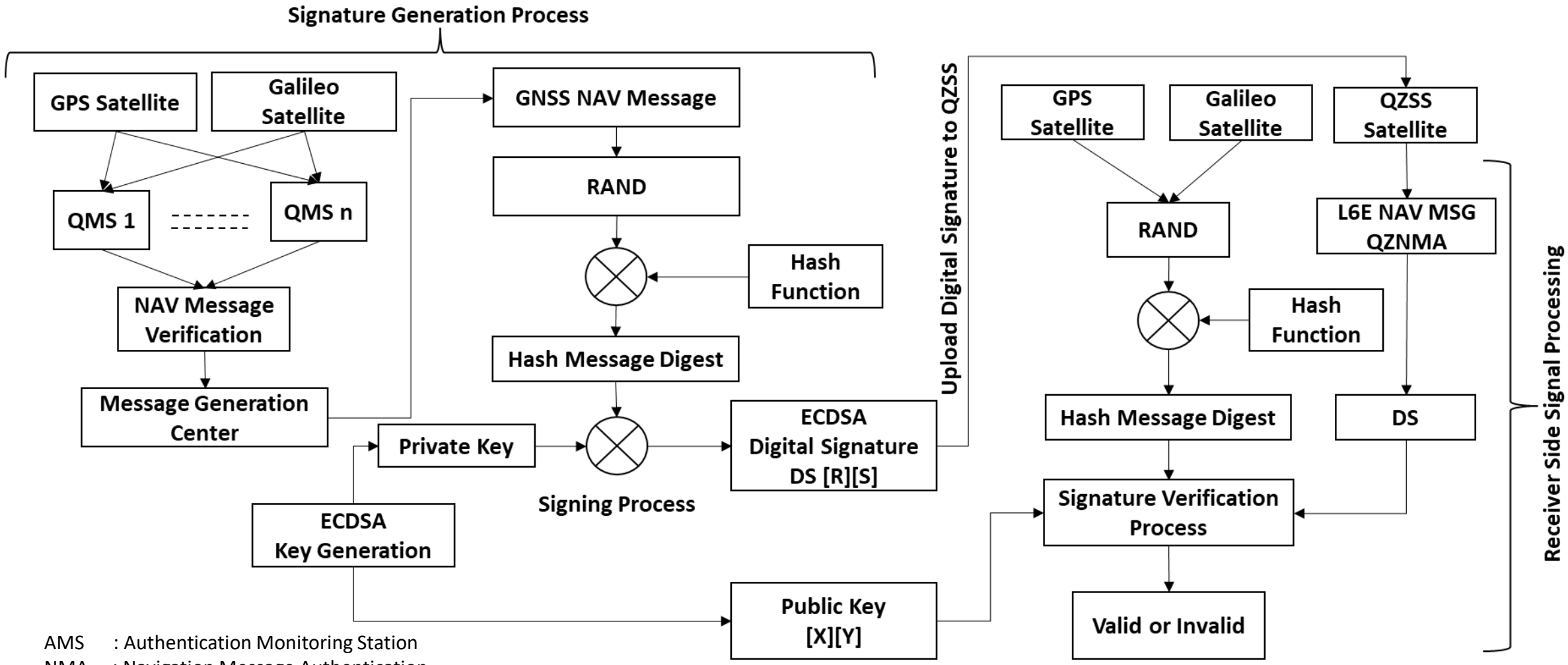
Reference Slides:
QZSS SAS IS Document Slides

QZSS Signal Authentication System



NMA : Navigation Message Authentication
DS : Digital Signature
ECDSA : Elliptical Curve Digital Signature Authentication
NAV : Navigation
QMS : QZSS Monitoring Station
RAND : Reference Authentication Navigation Data

GNSS Signal Authentication System

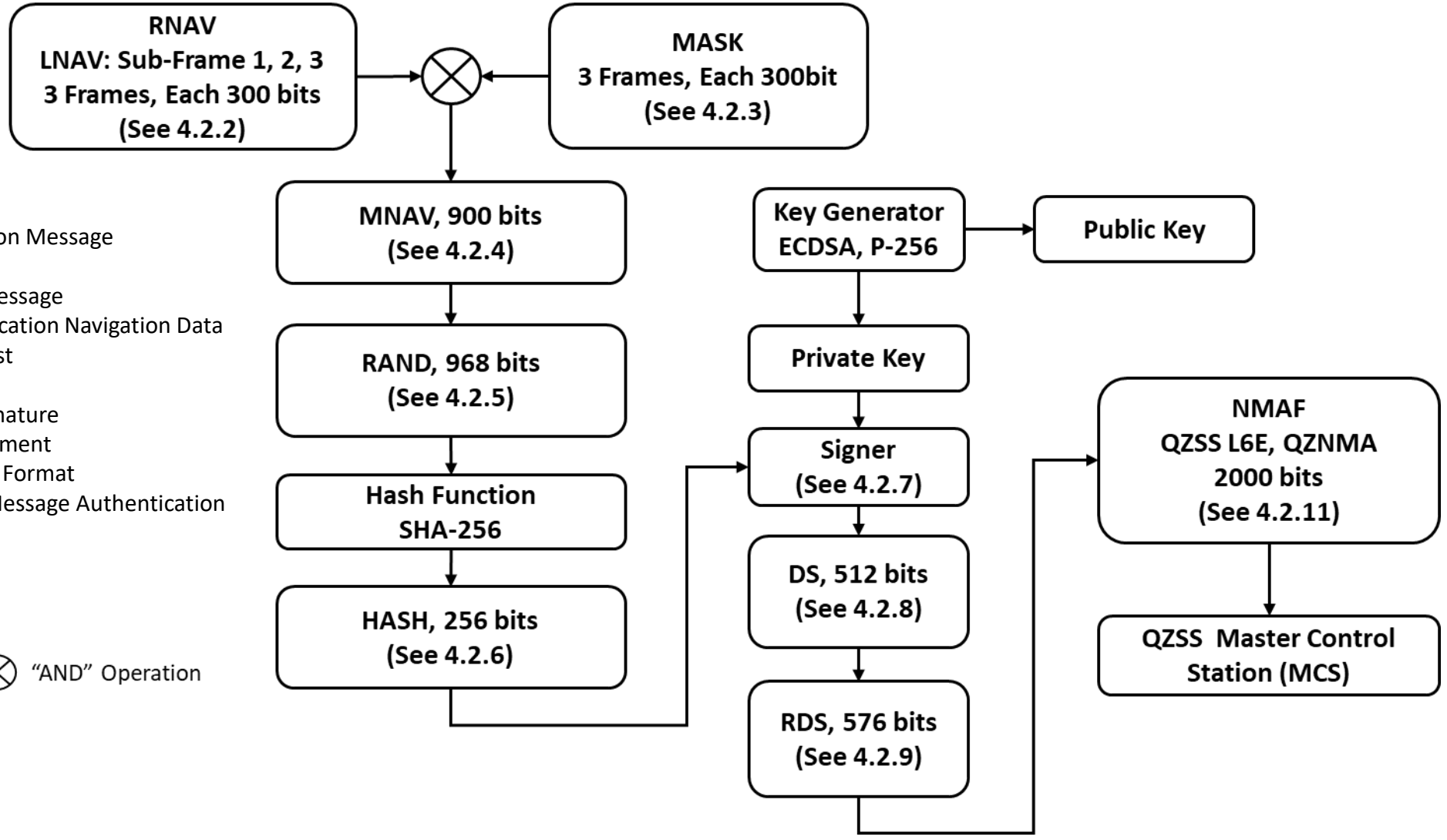


AMS : Authentication Monitoring Station
NMA : Navigation Message Authentication
DS : Digital Signature
ECDSA : Elliptical Curve Digital Signature Authentication
NAV : Navigation
RAND : Reference Authentication Navigation Data
QMS : QZSS Monitoring Station

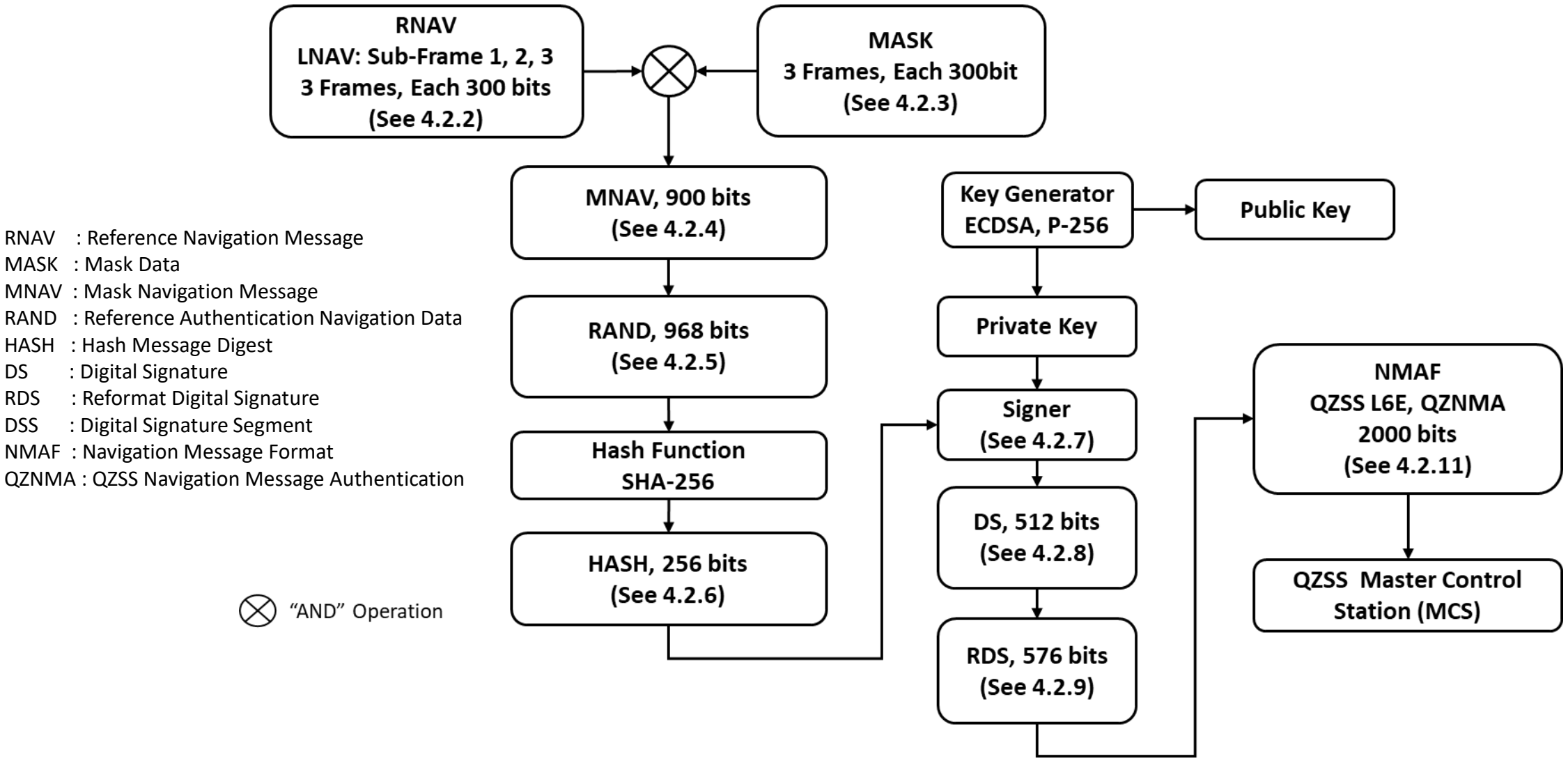
GPS Signal Authentication Overview, GPS L1C/A, LNAV

RNAV : Reference Navigation Message
MASK : Mask Data
MNAV : Mask Navigation Message
RAND : Reference Authentication Navigation Data
HASH : Hash Message Digest
DS : Digital Signature
RDS : Reformat Digital Signature
DSS : Digital Signature Segment
NMAF : Navigation Message Format
QZNMA : QZSS Navigation Message Authentication

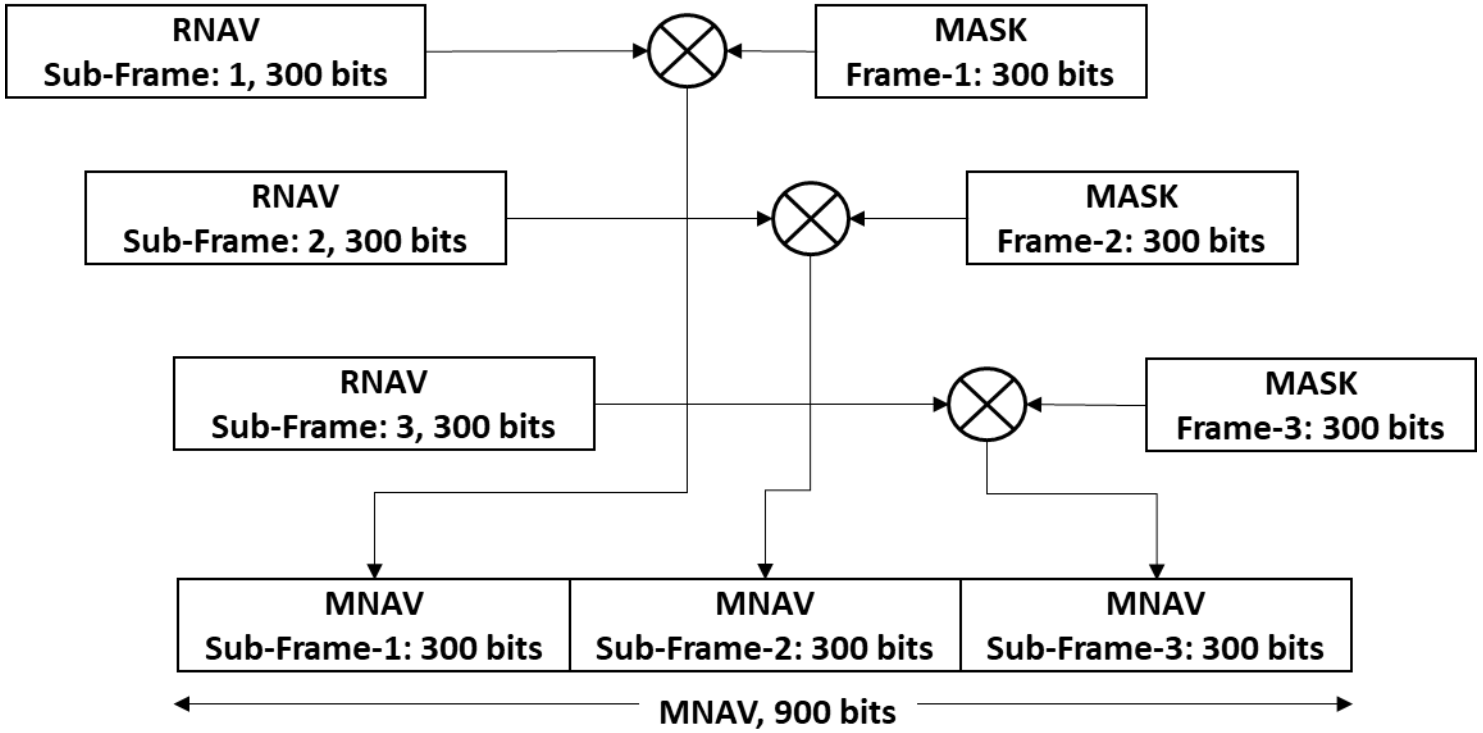
⊗ "AND" Operation



GPS Signal Authentication Overview, Signal: GPS L1C/A, Message: LNAV



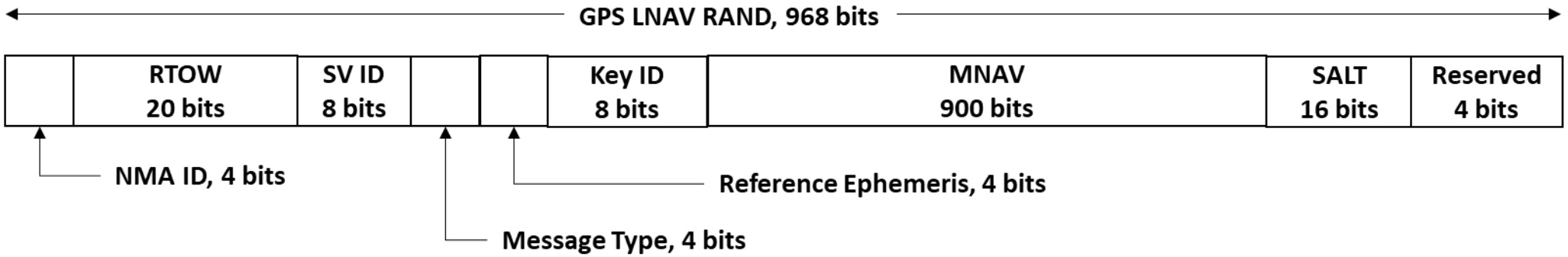
GPS LNAV : Mask Navigation Message (MASK)



⊗ "AND" Operation

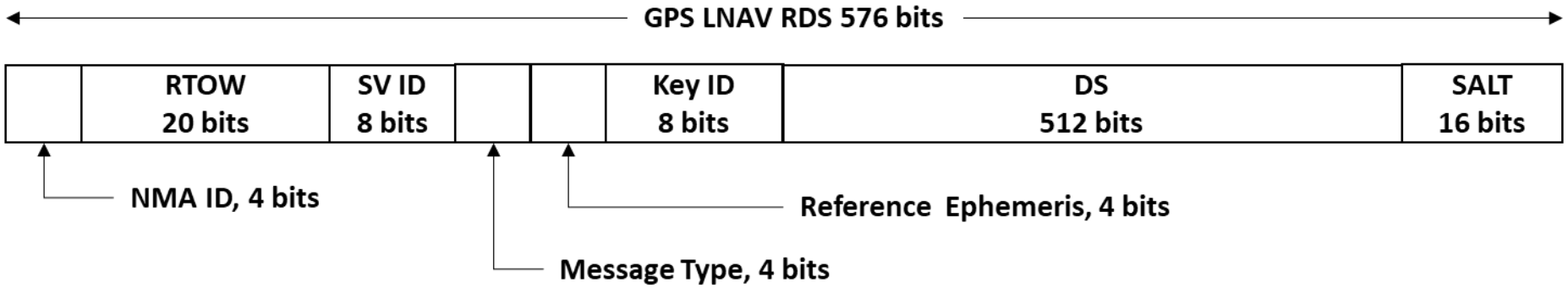
RNAV : Reference Navigation Message
MASK : Mask Data
MNAV : Mask Navigation Message

GPS LNAV: Reference Authentication Navigation Data (RAND)



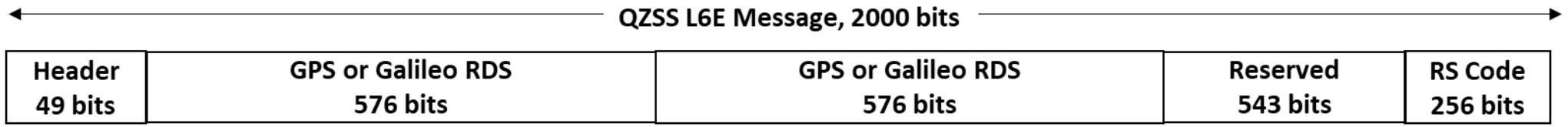
RAND : Reference Authentication Navigation Data
RTOW : Reference Time Of Week
MNAV : Mask Navigation Message

GPS LNAV: Reformat Digital Signature (RDS)



RDS : Reformat Digital Signature
RTOW : Reference Time of Week
DS : Digital Signature

GPS LNAV: L6E Navigation Message Authentication Frame (NMAF)



NMAF : Navigation Message Authentication Frame
RDS : Reformat Digital Signature
RS Code : Reed-Solomon Code