

QZSS Navigation Message Authentication Service Status

Quasi-Zenith Satellite System,
Japanese Regional Navigation Satellite System

17th ICG WG-S

17 October, 2023

Motohisa KISHIMOTO

Senior Coordinator

QZSS Strategy Office

National Space Policy Secretariat

Cabinet Office, Government of Japan





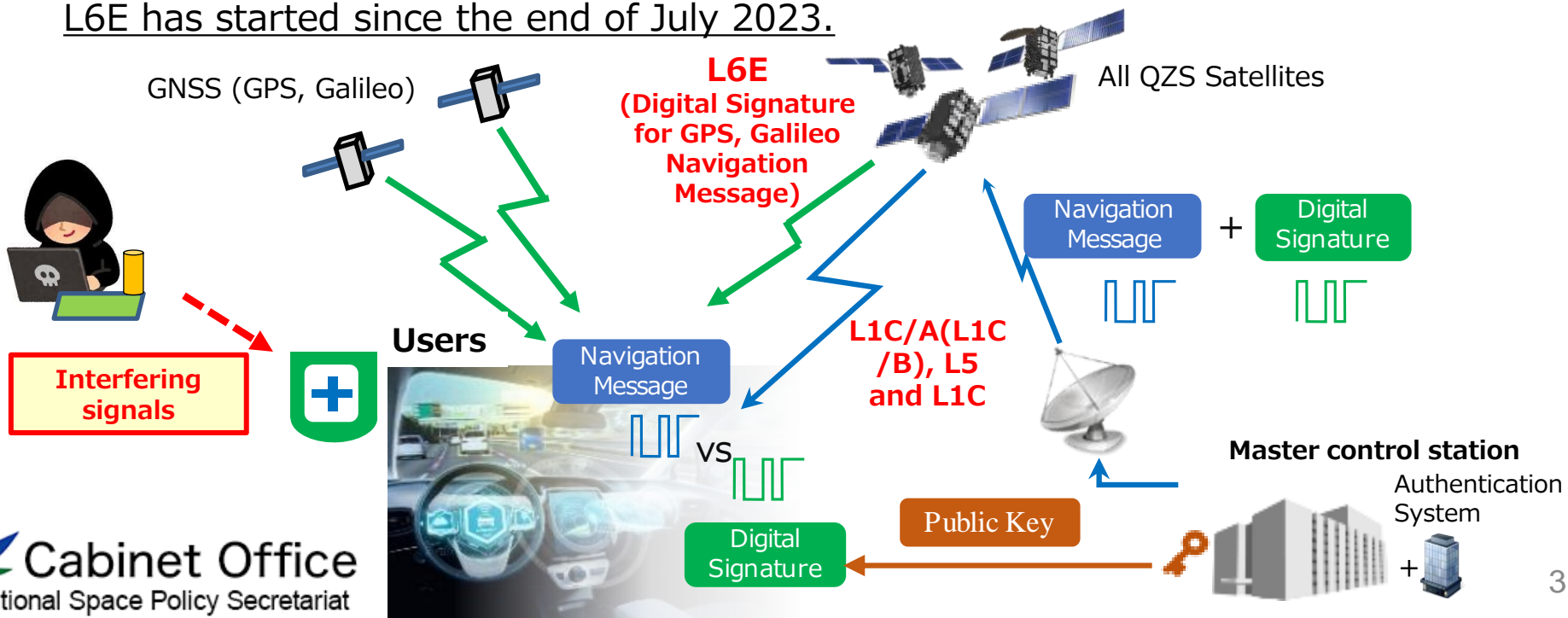
• Navigation Message Authentication by QZSS

- Uses L1C/A(C/B), L1C and L5 to authenticate QZSS positioning signals
- Also Uses L6E signal to authenticate GPS and Galileo positioning signals

Signal	Frequency MHz	Service	Compatibility	QZS-1R	QZS-2/4	QZS-3
				IGSO	IGSO	GEO
L1C/A	1575.42	Positioning	Complement GPS	✓	✓	✓
L1C		Positioning	Complement GPS	✓	✓	✓
L1C/B		Positioning	Complement GPS	✓	-	-
L1S		Augmentation(SLAS)	DGPS (Code Phase Positioning)	✓	✓	✓
		Messaging	Short Messaging	✓	✓	✓
L1Sb		Augmentation(SBAS)	SBAS (L1) Service	-	-	✓
L2C	1227.60	Positioning	Complement GPS	✓	✓	✓
L5 I/Q	1176.45	Positioning	Complement GPS	✓	✓	✓
L5S		Experimental(L5 SBAS)	L5 SBAS (DFMC)	✓	✓	✓
L6D	1278.75	Augmentation(CLAS)	PPP-RTK (Carrier Phase Positioning)	✓	✓	✓
L6E		Augmentation(MADOCA)	PPP, PPP-AR (Carrier Phase Positioning)	✓	✓	✓



- QZSS Navigation Message Authentication service, QZNMA, will launch in JFY2024 to enhance the resilience against spoofing attacks.
- Navigation messages in the following signals are authenticated with using Elliptic Curve Digital Signature Algorithm (ECDSA P256).
 - QZSS signals (L1C/A(C/B), L1C, L5) are directly protected by self-authentication
 - GNSS signals (GPS: L1C/A, L1C, L5, Galileo:E1b, E5a) are protected by cross-authentication (L6E)
- The Interface Specification (IS-QZSS-SAS-001)(draft-002) is now available on our website (https://qzss.go.jp/en/technical/ps-is-qzss/is_qzss_sas_agree.html), and trial transmission of L6E has started since the end of July 2023.





QZSS CLAS Authentication

- Correction Message Authentication (CMA) will be provided for QZSS CLAS.
- It increases the resilience of high-accuracy positioning against spoofing.

