Research and Analysis of Navigation Message Authentication

Chen Xiao, Liu Ting
Aerospace Information Research Institute
Chinese Academy of Sciences

2022-10-11

CONTENTS

01 Introduction

02 Research on Navigation Message Authentication

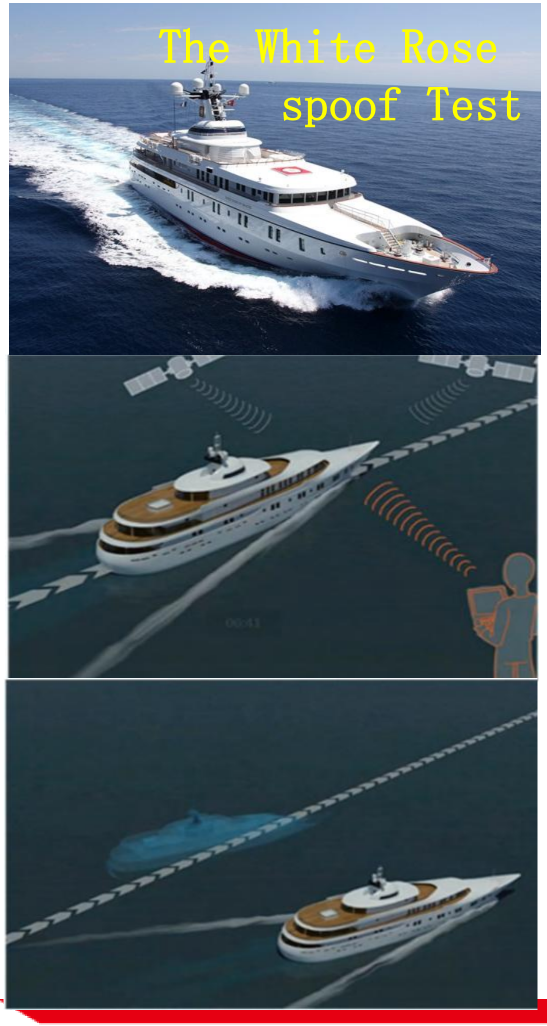
03 Conclusion and Recommendation

Introduction 01

Introduction

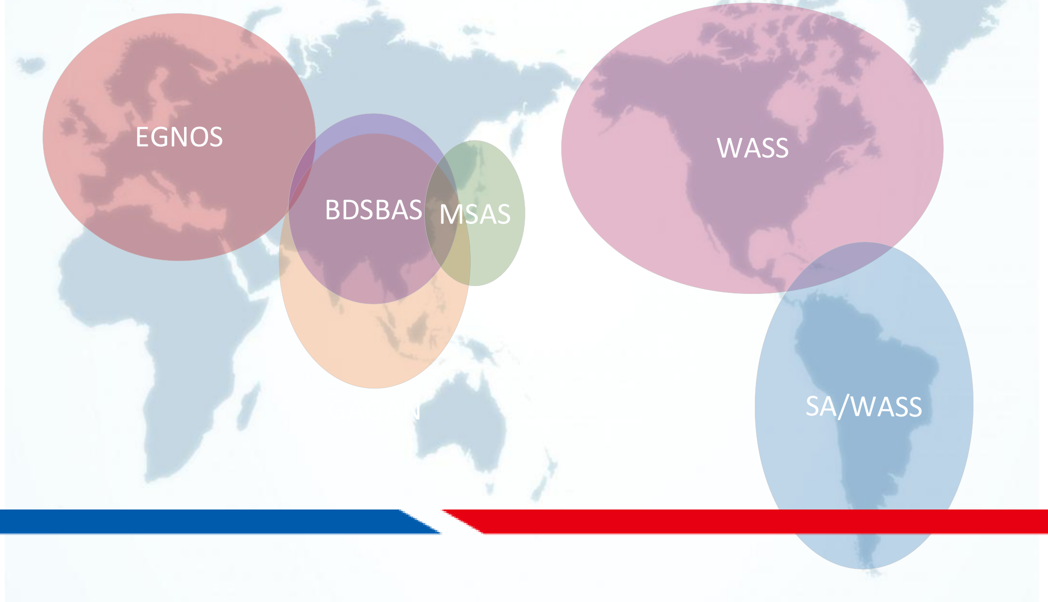
GNSS civil signal structure is public, vulnerable to be spoofed , especially for the following GNSS application scenarios with high security requirements.

- Autonomous Driving
- Unmanned Aerial Vehicles (UAVs)



Introduction

- ICG-15 proposed civil signal authentication issues.
- ICAO NSP Working Group actively promotes the standardization of SBAS authentication.
- In order to improve the trusted service capability of BDS, the research on message authentication technology for BDS civil signal is carried out.



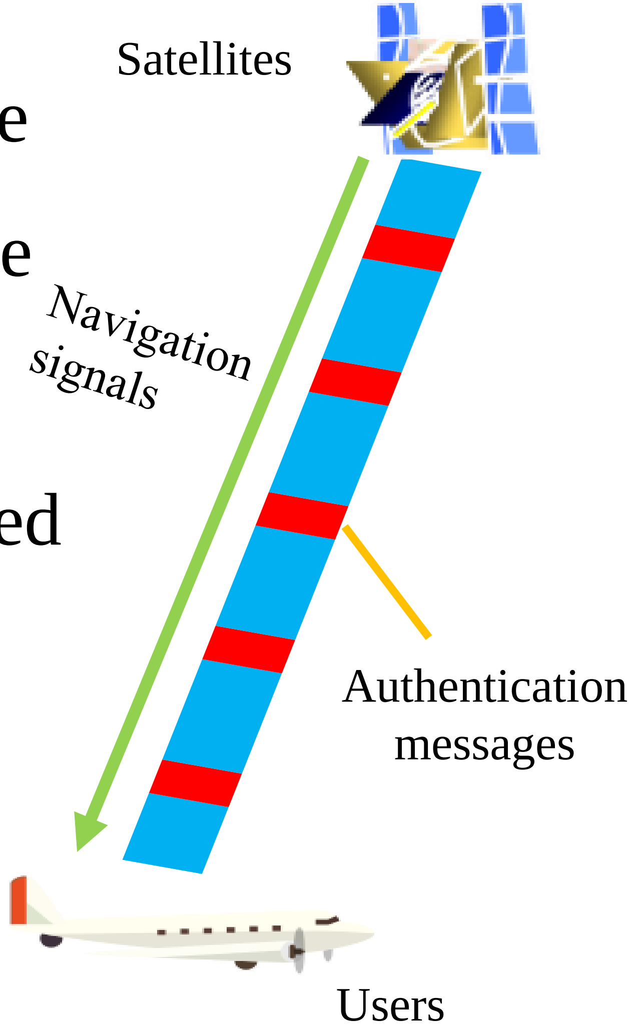
02

Research on Navigation Message Authentication

1、 The concept of navigation message authentication

Add authentication messages into navigation message frame

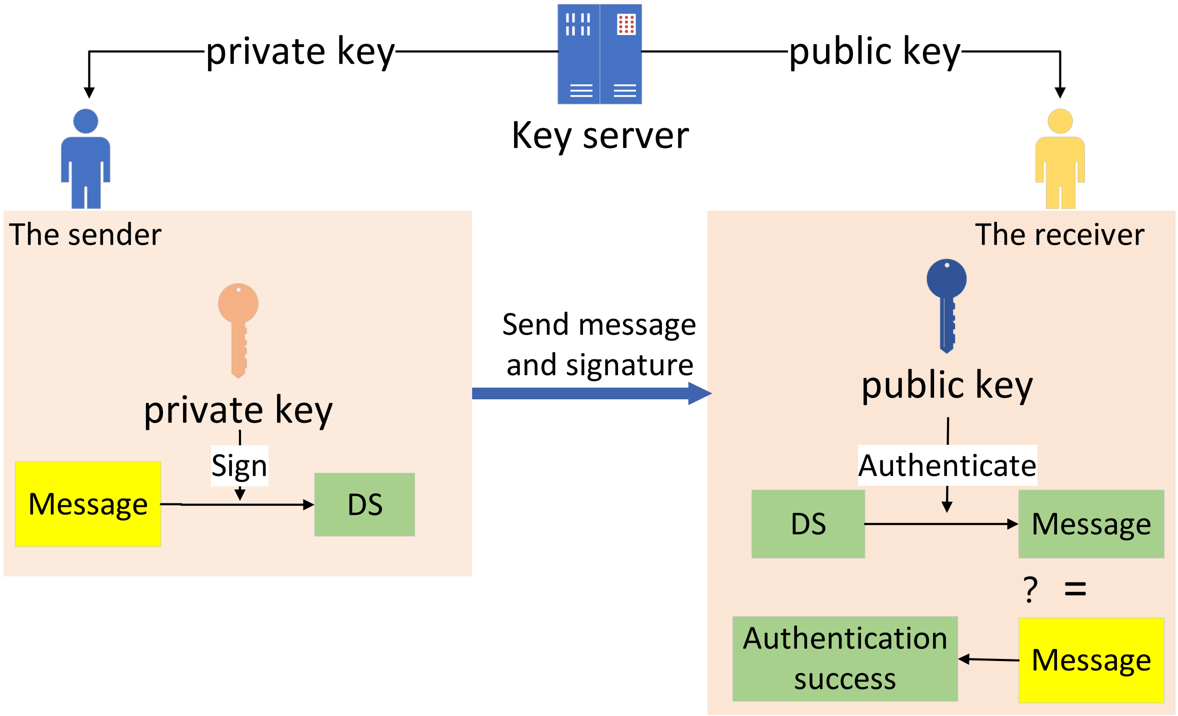
- Verify whether the received GNSS signal comes from the on-orbit GNSS satellites
- Verify whether the messages have been forged or tampered



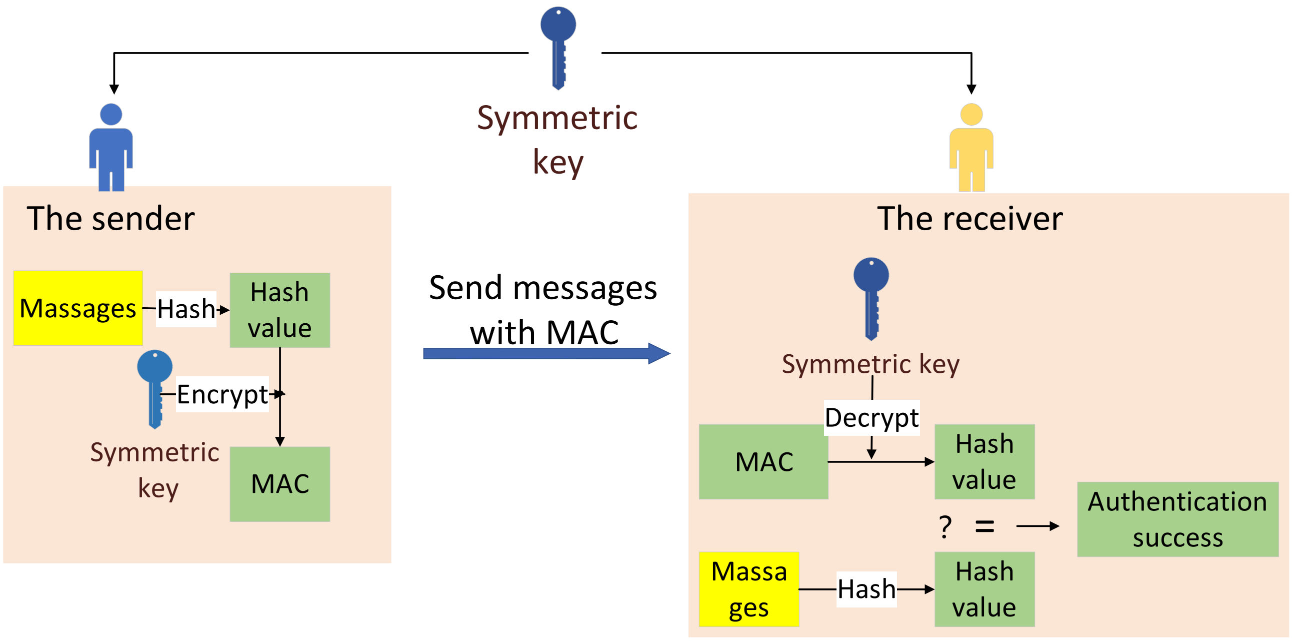
Authentication messages

- MAC(Message Authentication Code)
- Digital signature

2、 The authentication method



Digital signature



MAC

3、 Chinese commercial cryptography standards

Cryptography Law of the People’s Republic of China requires the preferential use of Chinese commercial cryptographic algorithms within China.

Chinese commercial cryptographic algorithms are ISO standards, referred to as SM standards.

	Digital Signature Algorithm		Cryptographic Hash Algorithms	
	SM2	ECDSA-P256	SM3	SHA-256
Security Level	128-bit	128-bit	128-bit	128-bit
Length of Key	Private key:256-bit Public key:512-bit	Private key:256-bit Public key:256-bit	/	/
Length of Output	Digital signature:512-bit	Digital signature:512-bit	Hash value:256-bit	Hash value:256-bit

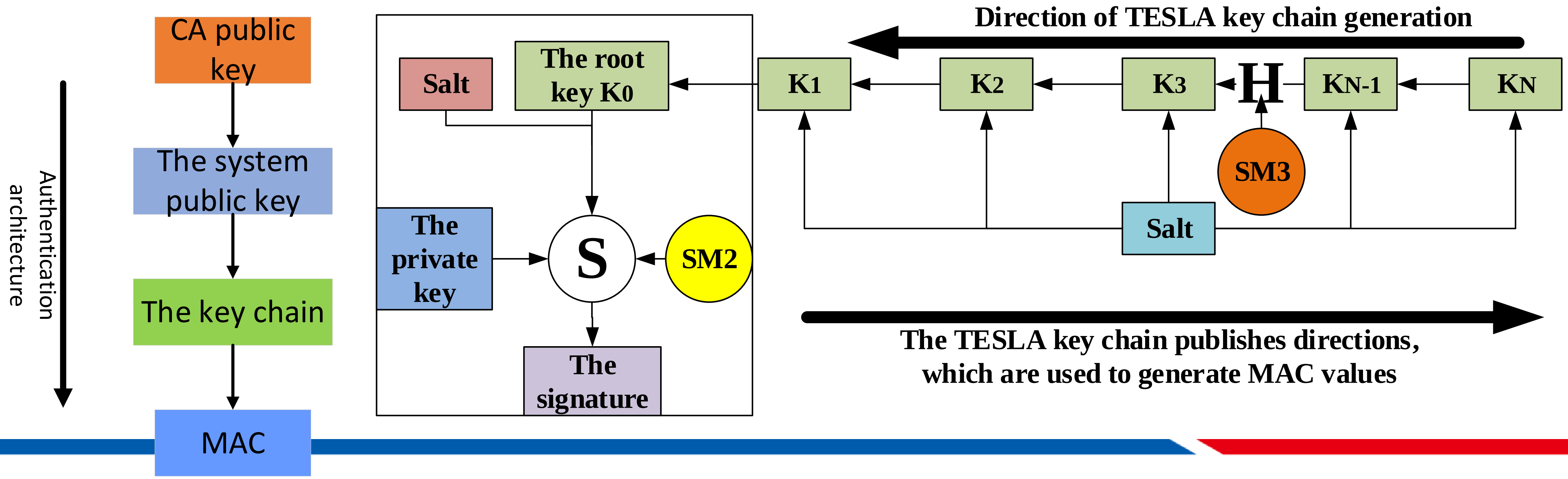
4、 Design of authentication protocol based on SM Standards

TESLA is a broadcast authentication protocol, which can be applied to GNSS signals with limited bandwidth.

1）SM3 is used to generate the key chain

2）SM2 is used for digital signature of key chain root key

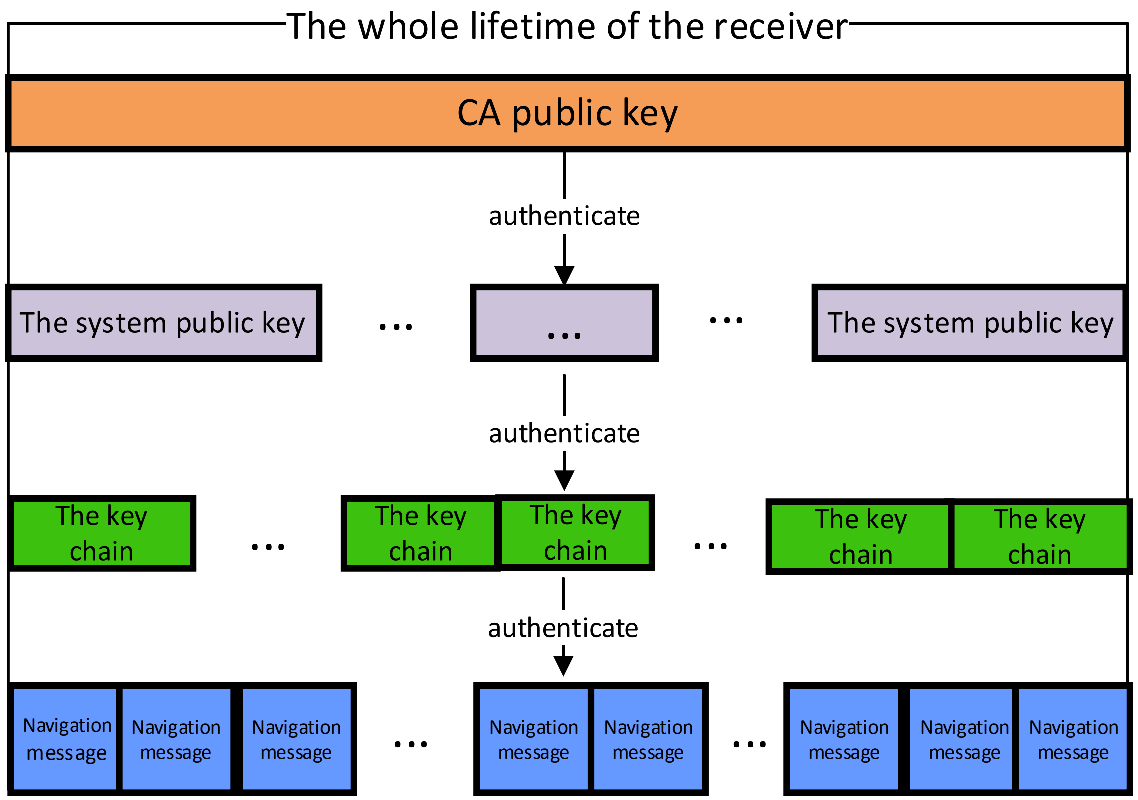
3）The public key of the system is digitally signed by a third-party CA



5、 Key management

Three-layer key management architecture is adopted：

- The third-level key is the TESLA keychain, which is used to authenticate SBAS messages.
- The second-level key is the system public/private key pair. The system private key, used to generate a digital signature for the root key.
- The first-level key is the CA's public/private key pair. The CA's private key, used to generate a digital signature for the system public key, is securely stored by the CA.



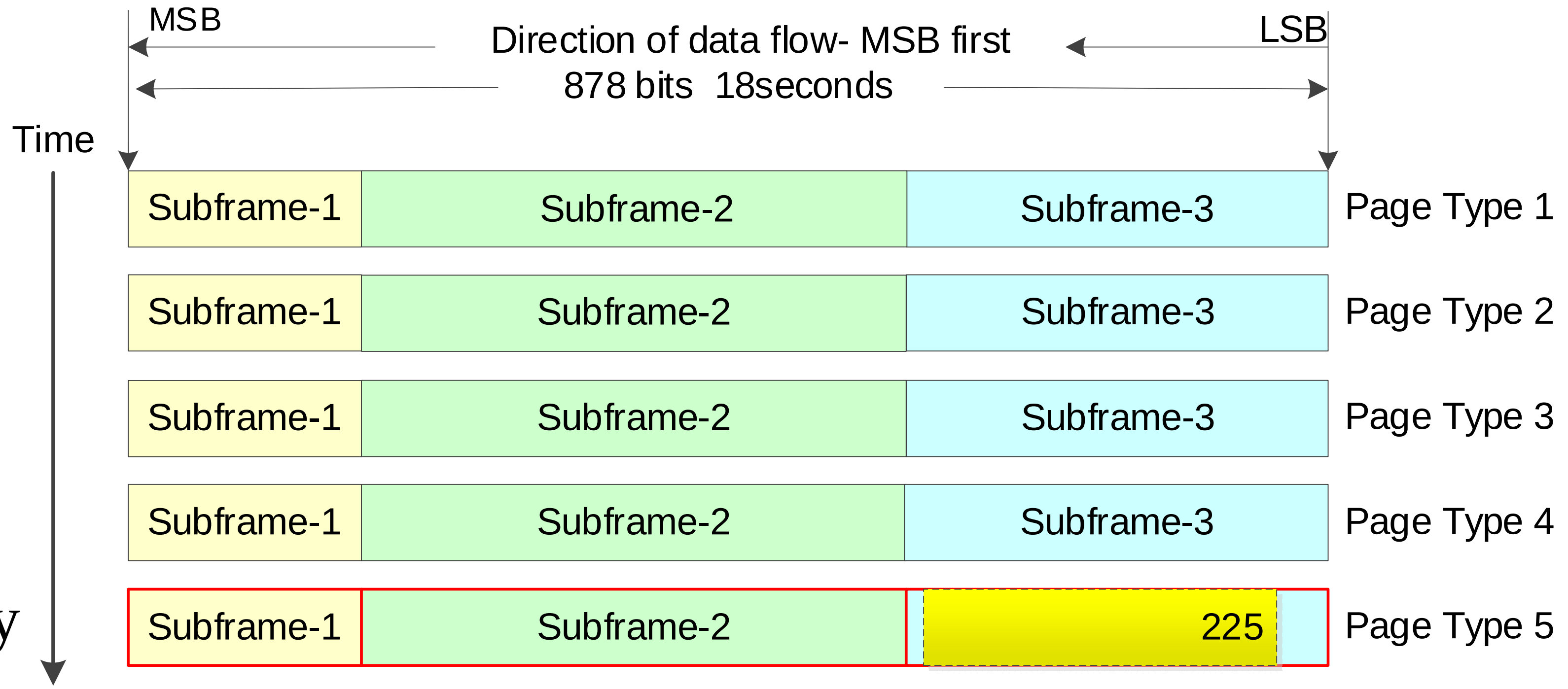
6、 Preliminary design and simulation of B1C authentication messages

Bits available for authentication

1）BDS B1C authentication message design：

Define new Page Type in B1C message -- Authentication Page (Page 5)

Message content: MAC + Key



Direction of data flow----- MSB first

264 bits

MSB | LSB

PageID	HS	DIF (B1C)	SIF (B1C)	AIF (B1C)	SISMAI	MAC-KEY information	CRC
6 bits	2 bits	1 bits	1 bit	1 bit	4 bits	225 bits	24 bits

6、 Preliminary design and simulation of B1C authentication messages

2）The simulation results

- Authentication Time to Detect (ATTD): indicates the time required for the receiver to detect an attack.
- Time Between Authentication (TBA): indicates the time between authentication verification events.

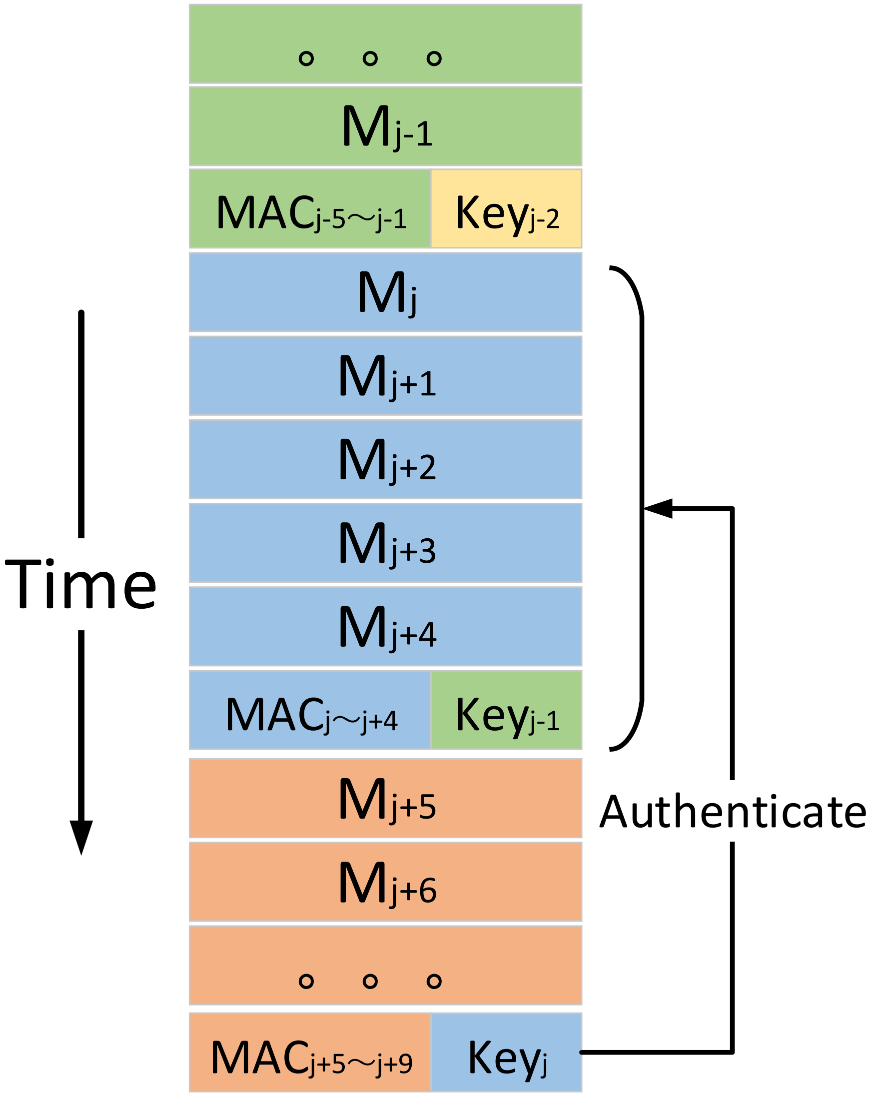
	Bandwidth usage of authentication messages：20%	**Bandwidth usage of authentication messages：50%**
TBA	90s	36s
ATTD	[108s,180s]	[54s,72s]
Subframe 3 Page broadcast order	Page1，Page2，Page3，Page4，Page5	Page1，Page5，Page2，Page5，Page3 Page5，Page4，Page5

BDS B2a has a larger bandwidth and is expected to achieve TBA of 12s.

7、 Preliminary design and simulation of SBAS authentication messages

1） Design of SBAS-DFMC authentication messages

Considering the 6s TTA(Time To Alert), SBAS messages need to be authenticated once every 6s.



7、 Preliminary design and simulation of SBAS authentication messages

2）The simulation results

- Time Between Authentication（TBA）: indicates the time between authentication verification events.
- Maximum Authentication Latency（MAL）: indicates the maximum time delay for a single authentication.
- Time for First Authentication (TTFA): indicates the time needed by the receiver to detect whether data is authentic or falsified after first signal acquisition;

a）Cold start: the receiver has no key except the CA public key.

b）Warm start: the receiver has the current system public key and its CA signature, but no current TESLA key chain information.

c）Hot start: the receiver has the current TESLA key chain information and the current system public key and its CA signature.

KPI	TESLA scheme performance
Cryptographic Security Level	115bit
TBA	6s
MAL	11s

7、 Preliminary design and simulation of SBAS authentication messages

2）The simulation results

KPI	TESLA scheme performance		
TTFA	Cold start	System normal operation period	Interval:[180s,324s] Average time:212.19s
		System public key update period	Interval:[180s,432s] Average time:263.42s
		Keychain update period	Interval:[180s,396s] Average time:260.58s
	Warm start	System normal operation period	Interval:[67s,180s] Average time:112.02s
		System public key update period	Interval:[67s,294s] Average time:142.87s
		Keychain update period	Interval:[67s,252s] Average time:135.84s
	Hot start	System normal operation period	Interval:[11s,16s] Average time:13.5s
		System public key update period	
		Keychain update period	

Conclusion and Recommendation

03

Conclusion and Recommendation

1) GNSS broadcast signal compatibility and interoperability on L1 band, it is recommended that GNSS service providers consider to provide message authentication services on L1 band;

2) Chinese commercial cryptographic standards meet the needs of navigation message authentication. It is recommended that all members pay attention to the authentication technology based on SM algorithm;

3) In the future, multi-system message authentication services will involve the interoperability of multinational cryptographic algorithm standards. It is recommended to consider the terminal interoperability requirements in the cryptographic architecture and management methods.

Thank you!