



# Navigation Message Authentication (NMA) for NavIC SPS

*Pravin Patidar*

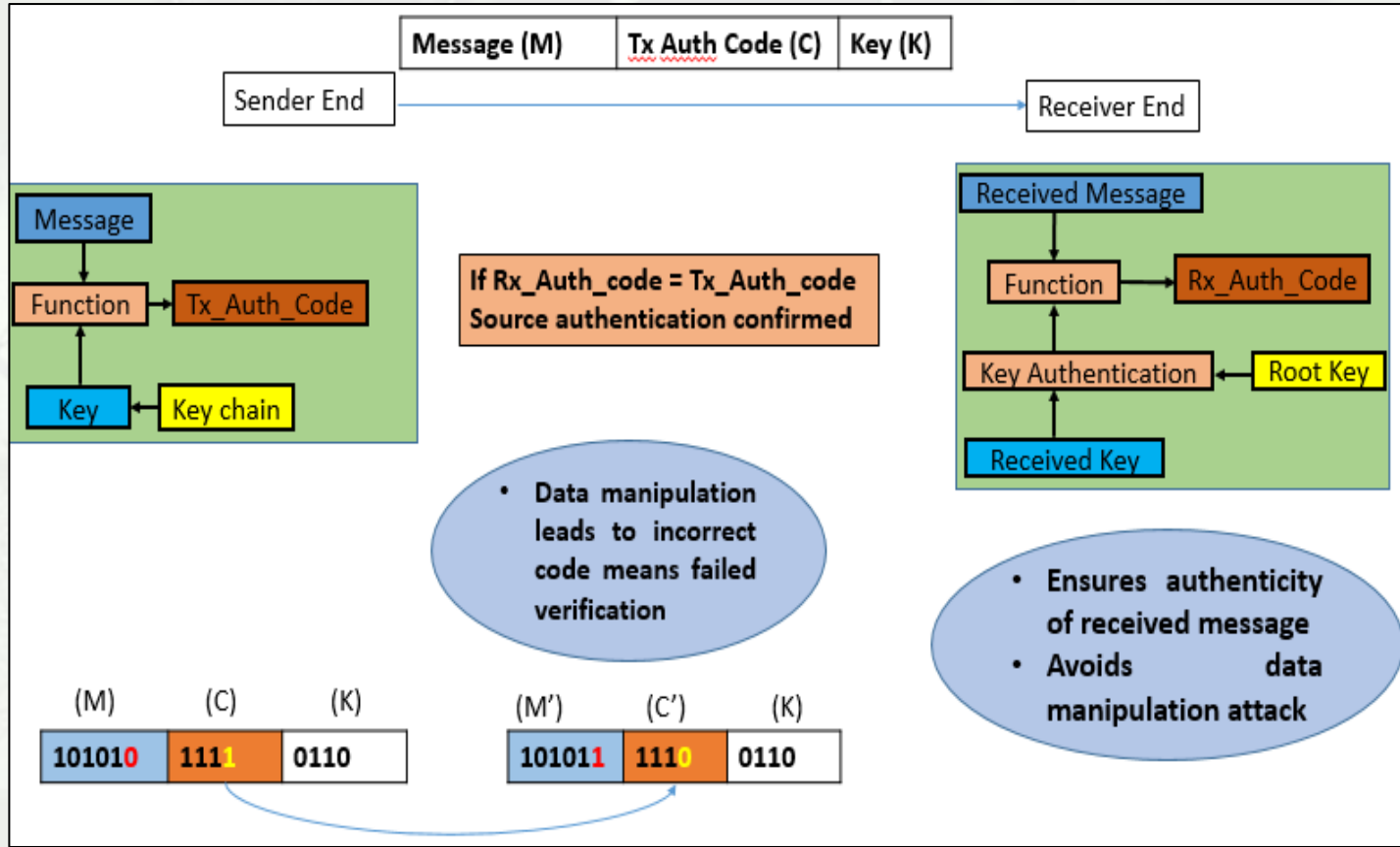
*Space Applications Centre*

*Indian Space Research Organisation*

*Ahmedabad, India*

- Spoofing involves simple repeater attacks - moderate signal generation attacks - highly sophisticated signal estimation attacks.
  - Data manipulation attack: wherein the spoofer alters the navigation data containing satellite ephemeris and clock corrections.
- The ***Navigation Message Authentication (NMA) in NavIC SPS*** proposes to provide data authentication as value added provision.
  - The NMA shall provide NavIC receivers with the assurance that the received navigation message is coming from the system itself and has not been modified.

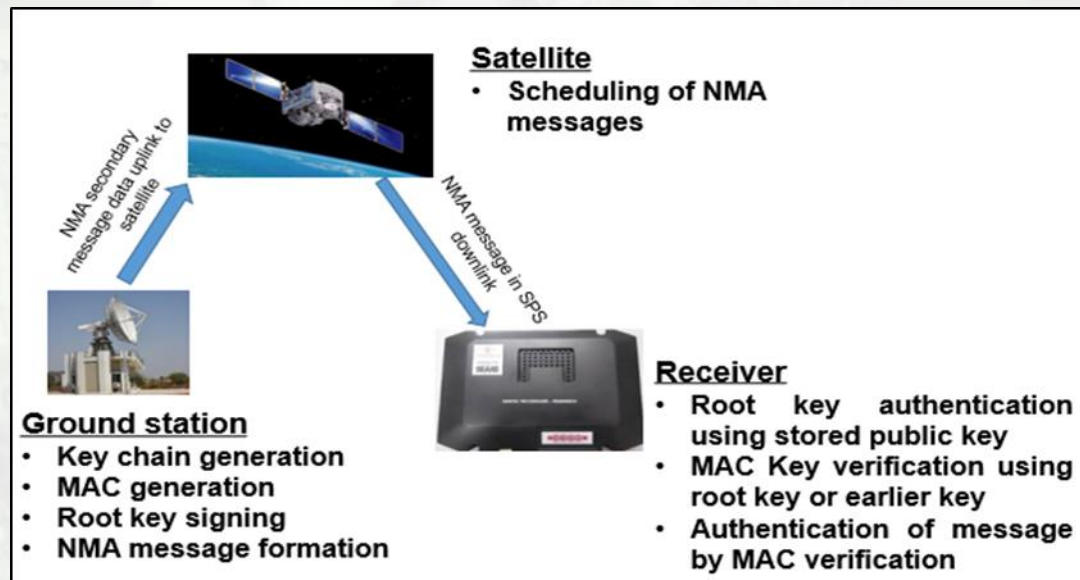
# NMA Concept



**Major Constraint:**  
The receiver and sender should be in *loose synchronization*.

# NMA for NavIC SPS

- The functional elements of NavIC –SPS NMA scheme are distributed over control, space and user segments.
  - The apportionment is done considering minimum change at the space segment.
- The NMA in NavIC SPS is proposed to be offered by defining a new secondary message.
  - Utilizing the flexibility of NavIC SPS data structure
  - The generation of such secondary message shall be done by control segment.
  - The space segment will only transmit it as per the scheduling requirements.





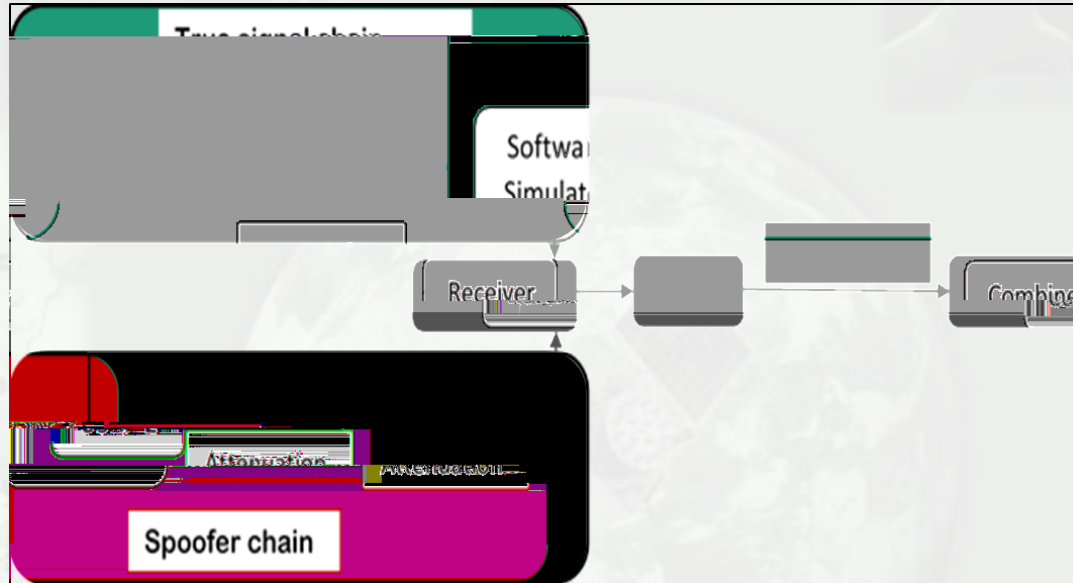
# NMA for NavIC SPS

- The NavIC SPS data structure consists of four sub frames: Two Primary and Two Secondary.
  - Secondary sub frames are proposed to be used for transmission of NMA messages containing authentication code, key and root key.
- In best possible case NMA messages can be transmitted in one secondary sub frame of alternate frames.
- By incorporating the NMA secondary messages, spoofing detection capability is possible with present satellites, without altering existing data structure.

SF1 (292 bits)	SF2 (292 bits)	SF3 (292 bits) Data: 220 bits	SF4 (292 bits) Data : 220 bits
Data for Navigation Message		Other Secondary Messages	NMA Message

Attribute	Description
Key Disclosure Delay (KDD)	>96 Seconds
Time To First Authenticated Fix (TTFAF)	>144 Seconds
Time between Authentication (TBA)	>96 Seconds
Size of MAC	30 bits
Size of key	116 bits
Time Synchronisation Requirement	<48 seconds

The root key distribution will be done through slow rate data embedded into the NMA message.



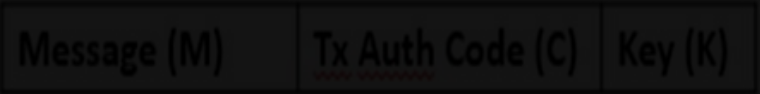
The proposed scheme is end to end tested under various attack scenarios using NavIC simulator and NavIC receiver.

- Navigation data manipulation test
- Time synchronisation test
- Key manipulation test

# Summary

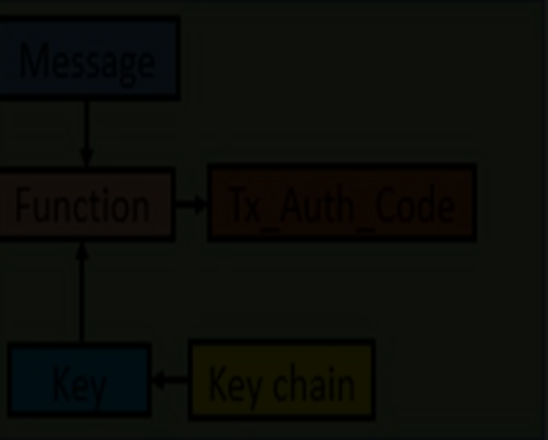
- NMA for NavIC SPS users have been proposed as value added service.
- NavIC shall be able to support the civil signal authentication within the existing SPS signals and with existing satellites.
- The SIS experiments for NavIC SPS NMA are currently being worked out.
- The experimental transmission of new NMA message is expected by 2023.





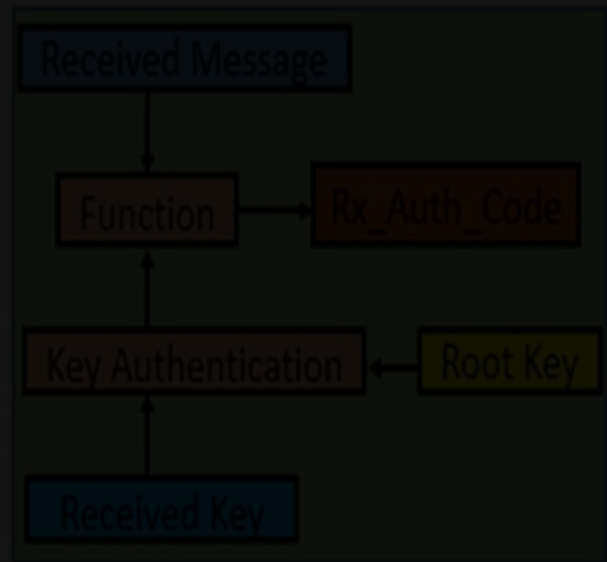
Sender End

Receiver End



If Rx\_Auth\_code = Tx\_Auth\_code  
Source authentication confirmed

# Thank You



- Data manipulation leads to incorrect code means failed verification

- Ensures authenticity of received message
- Avoids data manipulation attack

[pravinpatidar@sac.isro.gov.in](mailto:pravinpatidar@sac.isro.gov.in)

