Side Meeting
@IETF124

TESLA Update for GNSS SBAS

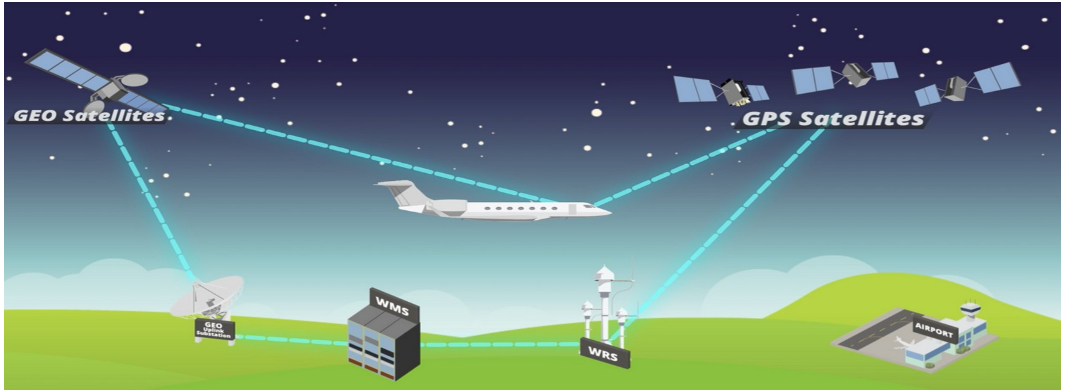
draft-moskowitz-tesla-update-gnss-sbas

And SBAS PKI

Robert Moskowitz
HTT Consulting
AX Enterprize

What is SBAS?

Satellite-Based Augmentation System (SBAS) Functional Diagram



Aircraft using SBAS

- Process Global Navigation Satellite System (GNSS) and SBAS signals
- Apply SBAS corrections to get guaranteed accuracy and position bounds

SBAS Components

- Ground monitoring
  - Observe GNSS
- Central Processing
  - Assess Integrity
  - Develop corrections
  - Monitor Ionosphere
- Satellite uplink
- SBAS satellite downlink

L1 SBAS service on L1

DFMC SBAS service on L5

Motivation

GNSS (Global Navigation Satellite Systems) are under attack.

Little can be done for signal interference

Tremendous political pressure to stop spoofed messaging

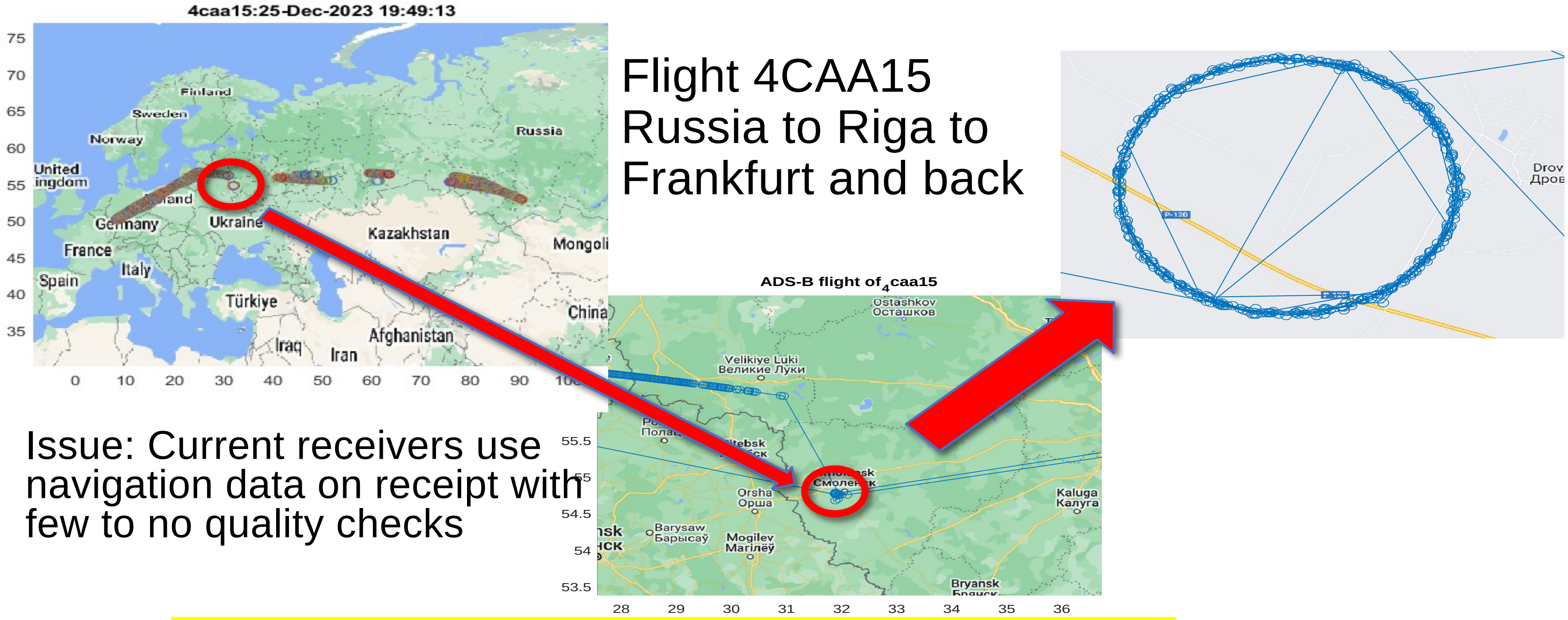
ALL GNSS CORE Constellations (GPS, GALILEO, GLONAS, Beidou) support or will support SBAS (Satellite-based augmentation system)

(SBAS is implemented on a regional basis, provides an enhanced signal for aircraft during safety-critical phases like landings)

Via SBAS (and GNSS) messaging can be authenticated.

Only GALILEO signals are authenticated for now for civil use

Spoofing Near Russian Border



Flight 4CAA15
Russia to Riga to
Frankfurt and back

Issue: Current receivers use navigation data on receipt with few to no quality checks

Solution: Provide authentication tags, delay use of data until authenticated

Motivation

The available SBAS link budget is VERY small as are the individual messages (250 bits!)

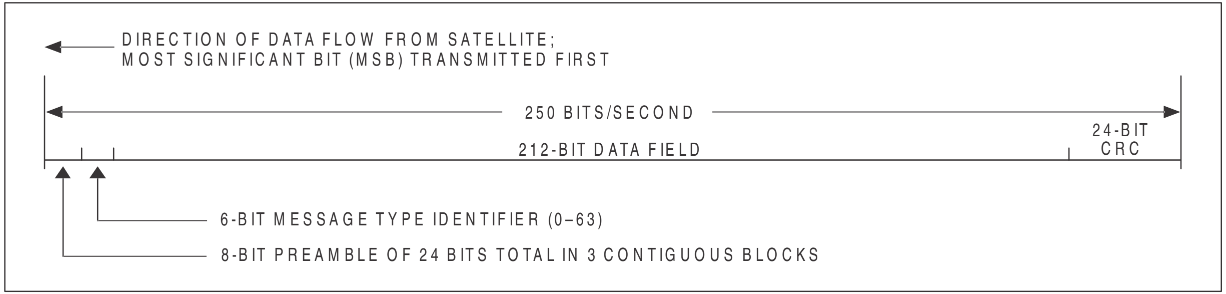
ICAO SBAS work has selected a modified TESLA authentication
(with CA for authenticating TESLA keys) to protect GNSS

This modified TESLA MAY be used for ADS-B (51 bits!, maybe bigger in 2030) as well
(but less spare link capacity and the PKI is much harder)

RFC 4082 is dated, and not exactly what is in ICAO documentation

Bring 4082 forward, cryptographically
and public review of ICAO activity

SBAS Message Characteristics



DIRECTION OF DATA FLOW FROM SATELLITE;
MOST SIGNIFICANT BIT (MSB) TRANSMITTED FIRST

250 BITS/SECOND

212-BIT DATA FIELD

24-BIT CRC

6-BIT MESSAGE TYPE IDENTIFIER (0–63)

8-BIT PREAMBLE OF 24 BITS TOTAL IN 3 CONTIGUOUS BLOCKS

SBAS Message Characteristics

- One 250-bit message every second
- Data content: 212 bits on SBAS L1, 216 bits on SBAS L5 (shorter preamble)
- 24-bit Cyclic Redundancy Check (CRC)

Message usage

- Positive report on integrity every 6-seconds (~16%)
- Can use 15-25% of bandwidth to support authentication
- SBAS authentication message (~16%)
- Leaves up to 10% for key management (21 bits per second average)

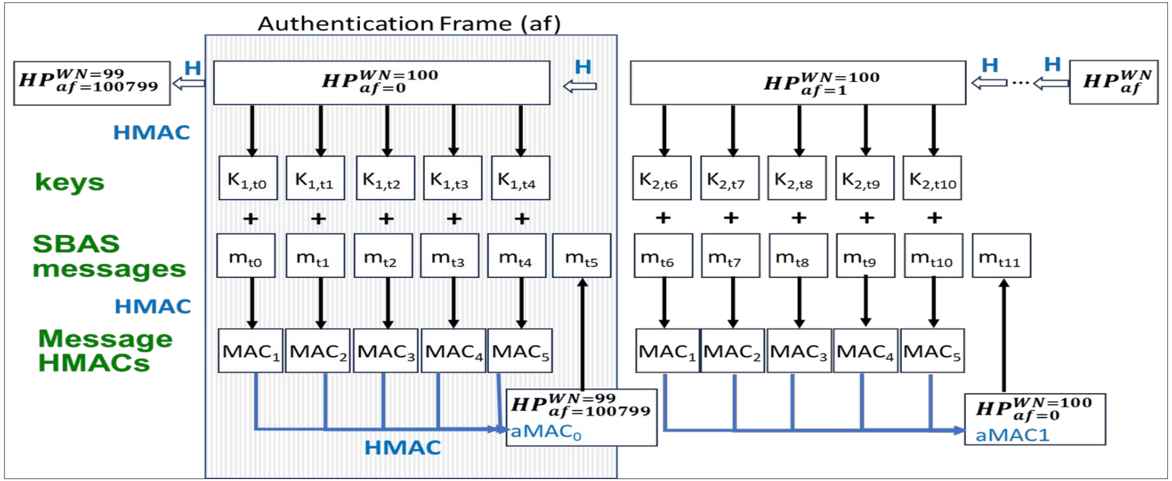
Background

- *ICAO TESLA guidance at DOI_10.33012_navi.595*
  - *Authentication of Satellite-Based Augmentation Systems with Over-the-Air Rekeying Schemes*
    - *This is the latest in a number of iterations years in the works*
- *Unfortunately, ICAO work documents not public*
  - *SBAS documents may be available on request (WiP)*
- *Initial draft:*
  - *Draft-moskowitz-tesla-update-gnss-sbas*
    - *I am reasonable embedded in the ICAO processes*

Main TESLA changes

- *Time sync based on GNSS time*
  - *Simplified synchronization*
- *“Aggregated MAC” to limit MAC transmissions*
  - *MAC of 5 MACs*
  - *Sent every 6s*
  - *Lost aMAC is “more critical” so FEC added*
    - *Call in SBAS “Block Erasure Codes”*
    - *FEC of 5 aMAC: EVENODD is one of the most commonly used double-fault tolerant coding strategies*
    - *Can recover up to two missing data fields out of five*

SBAS TESLA Authentication

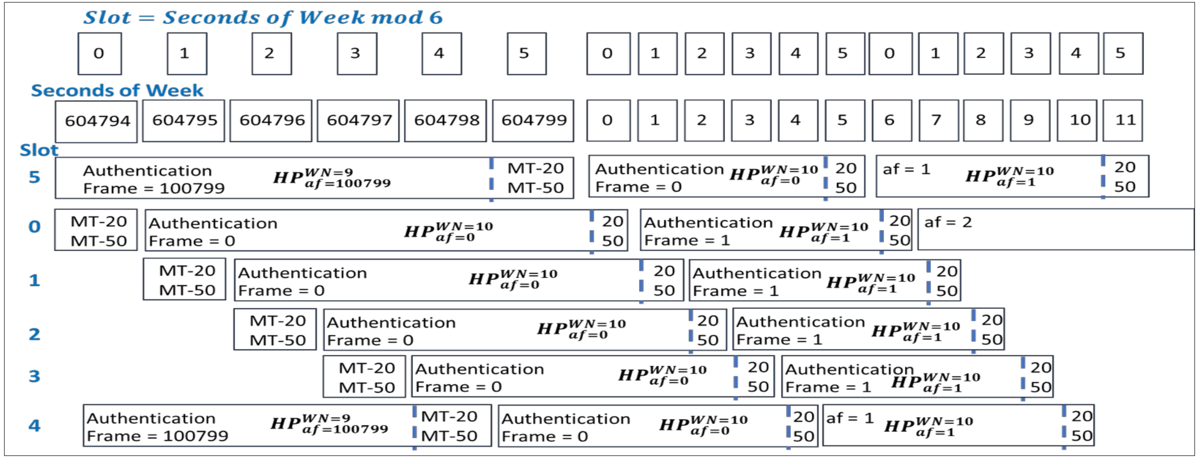


$HP_{af_i}^{WN_k}$

$$HP_{af_i}^{WN_k} = trun\left\{H\left(HP_{af_{i+1}}^{WN_k^*} \middle\| WN_k^* \middle\| af_{i+1} \middle\| S\right), 128\ bits\right\}$$

SBAS Authentication Frame (af)

- AF: 5 standard SBAS messages followed by an SBAS Authentication Message
  - Defined per week based on seconds of week and broadcast slot
  - SBAS Authentication Message has a designated slot (except during an alert)
  - af = 0 has SBAS authentication message broadcast in second 0, 1, 2, 3, 4, or 5



$Slot = Seconds\ of\ Week\ mod\ 6$

0 1 2 3 4 5 0 1 2 3 4 5 0 1 2 3 4 5

Seconds of Week

604794 604795 604796 604797 604798 604799 0 1 2 3 4 5 6 7 8 9 10 11

Slot

5: Authentication Frame = 100799 $HP^{WN=9}_{af=100799}$ | MT-20 MT-50 | Authentication Frame = 0 $HP^{WN=10}_{af=0}$ | 20 50 | af = 1 $HP^{WN=10}_{af=1}$ | 20 50

0: MT-20 MT-50 | Authentication Frame = 0 $HP^{WN=10}_{af=0}$ | 20 50 | Authentication Frame = 1 $HP^{WN=10}_{af=1}$ | 20 50 | af = 2

1: MT-20 MT-50 | Authentication Frame = 0 $HP^{WN=10}_{af=0}$ | 20 50 | Authentication Frame = 1 $HP^{WN=10}_{af=1}$ | 20 50

2: MT-20 MT-50 | Authentication Frame = 0 $HP^{WN=10}_{af=0}$ | 20 50 | Authentication Frame = 1 $HP^{WN=10}_{af=1}$ | 20 50

3: MT-20 MT-50 | Authentication Frame = 0 $HP^{WN=10}_{af=0}$ | 20 50 | Authentication Frame = 1 $HP^{WN=10}_{af=1}$ | 20 50

4: Authentication Frame = 100799 $HP^{WN=9}_{af=100799}$ | MT-20 MT-50 | Authentication Frame = 0 $HP^{WN=10}_{af=0}$ | 20 50 | af = 1 $HP^{WN=10}_{af=1}$ | 20 50

$$af_i = ceiling\left(\frac{Seconds\ of\ Week - Slot}{6}\right)$$

SBAS Authentication Equations

- Hash points could be same for all SBAS signals or different per signal
- Key is unique for SBAS signal and message, derived from the hash point

$$k_{j,SV,Freq} = \mathrm{HMAC}\left(HP_{af_i}^{WN_k}, \mathrm{Phrase}\|\mathrm{t_j}\|\mathrm{PRN\ Code\ Number}\|\mathrm{Frequency}\right)$$

	L1	L5	Notes
Phrase	MT20Key	MT50Key	
Seconds of week (t_j)			32-bit unsigned integer
PRN Code Number			9-bit unsigned integer
Frequency	1,575,420	1,176,450	23-bit unsigned integer

- Message Authentication code developed for each message

$$MAC_{j,SV,L1} = \mathrm{trunc}\left\{\mathrm{HMAC}\left(k_{j,SV,L1}, m_{j,SV,L1}\right), 28\ bits\ \right)\}$$

$$MAC_{j,SV,L5} = \mathrm{trunc}\left\{\mathrm{HMAC}\left(k_{j,SV,L5}, m_{j,SV,L5}\right), 36\ bits\ \right)\}$$

- Aggregated through same HMAC process

$$aMAC_i = \mathrm{trunc}\ [\mathrm{HMAC}\left(k_{j,SV,Freq}, \mathrm{MAC_{j-5}}\|\mathrm{MAC_{j-4}}\|\mathrm{MAC_{j-3}}\|\mathrm{MAC_{j-2}}\|\mathrm{MAC_{j-1}}\right), 28/36\ \ bits]$$

Erasure / Recovery Approach

EVENODD is one of the most commonly used double-fault tolerant coding strategies used in array storage systems

- Can recover up to two missing data fields out of five

Each HMAC is broken into four components

$$h_i = \begin{bmatrix} h_{1,i} \\ h_{2,i} \\ h_{3,i} \\ h_{4,i} \end{bmatrix} \qquad \mathbf{H} = \begin{bmatrix} h_{1,1} & h_{1,2} & h_{1,3} & h_{1,4} & h_{1,5} \\ h_{2,1} & h_{2,2} & h_{2,3} & h_{2,4} & h_{2,5} \\ h_{3,1} & h_{3,2} & h_{3,3} & h_{3,4} & h_{3,5} \\ h_{4,1} & h_{4,2} & h_{4,3} & h_{4,4} & h_{4,5} \end{bmatrix}$$

$$\mathbf{R} = \begin{bmatrix} r_{1,1} & r_{1,2} \\ r_{2,1} & r_{2,2} \\ r_{3,1} & r_{3,2} \\ r_{4,1} & r_{4,2} \end{bmatrix}$$

As are two recovery fields of the same size

EVENODD Encoding Details

The second field is formed form the following operations:

- $S = h_{4,2} \oplus h_{3,3} \oplus h_{2,4} \oplus h_{1,5}$
- $r_{1,2} = S \oplus h_{1,1} \oplus h_{4,3} \oplus h_{3,4} \oplus h_{2,5}$
- $r_{2,2} = S \oplus h_{2,1} \oplus h_{1,2} \oplus h_{4,4} \oplus h_{3,5}$
- $r_{3,2} = S \oplus h_{3,1} \oplus h_{2,2} \oplus h_{1,3} \oplus h_{4,5}$
- $r_{4,2} = S \oplus h_{4,1} \oplus h_{3,2} \oplus h_{2,3} \oplus h_{1,4}$

$r_{1,2}$	$h_{1,1}$	$h_{1,2}$	$h_{1,3}$	$h_{1,4}$	$h_{1,5}$
$r_{2,2}$	$h_{2,1}$	$h_{2,2}$	$h_{2,3}$	$h_{2,4}$	$h_{2,5}$
$r_{3,2}$	$h_{3,1}$	$h_{3,2}$	$h_{3,3}$	$h_{3,4}$	$h_{3,5}$
$r_{4,2}$	$h_{4,1}$	$h_{4,2}$	$h_{4,3}$	$h_{4,4}$	$h_{4,5}$

Decoding requires a similar number of operations

Decoding

Two missing messages

$$S = r_{1,1} \oplus r_{2,1} \oplus r_{3,1} \oplus r_{4,1} \oplus r_{1,2} \oplus r_{2,2} \oplus r_{3,2} \oplus r_{4,2}$$

$$S_u^{(0)} = r_{u,1} \oplus \left(\bigoplus_{k=1, k \neq i,j}^{5} h_{u,k} \right)$$

$$S_u^{(1)} = S \oplus r_{u,2} \oplus \left(\bigoplus_{k=1, k \neq i,j}^{5} h_{f_5(u-k),k} \right)$$

$$f_5(k) \equiv \mathrm{mod}(k-1, 5) + 1$$

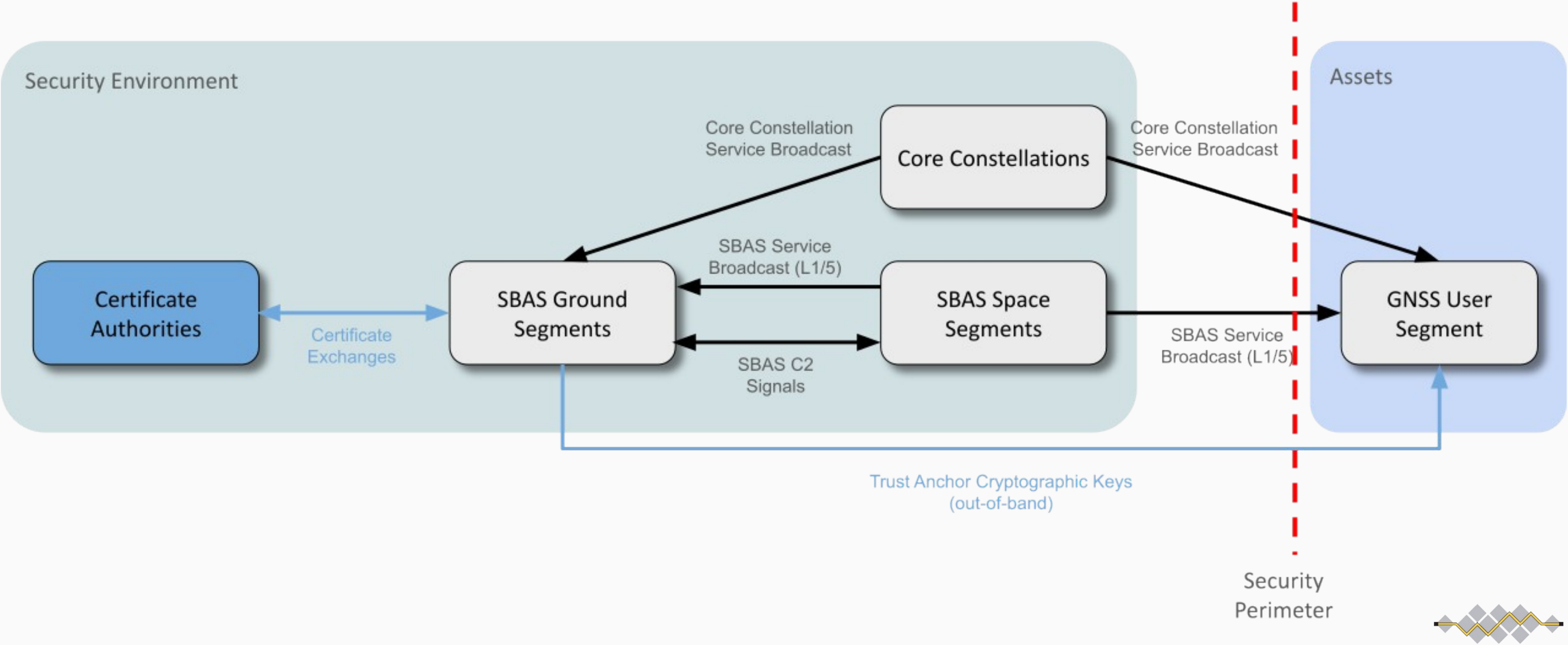
IETF work to do

- *Coordinate with Sec Area AD*
  - *Set up TESLA Update mailing list*
- *Coordinate with ICAO SBAS Auth workgroup*
  - *Gather details on TESLA process*
    - *Most of this is done*
- *Progress TESLA Update draft*
  - *SBAS process as Appendix*
- *Work with co-authors to publish Update*

The SBAS PKI Information

- *Each PRN or GNSS constellation will have its own CA for its message authentication*
  - *PRN are regional SBAS data providers. 39 In US constellation*
  - *Clients are expected to obtain all root and issuing certificates*
    - *Out-of-band*
    - *Each CA named outside of cert*
      - *DN in certs: “L1” and “L2” or similar*
- *SBAS X.509 certs in ICAO Doc 10169 (sec 10.3.3)*
  - *SBAS CA and EE certificates small*
    - *e.g. DER of 278 bytes, C509 178 bytes*

The SBAS Security Environment



Sample Issuing CA Certificate

```
Version: 3 (0x2)
Serial Number: 8148489420063590655 (0x71153ff47aeb48ff)
Signature Algorithm: ED25519
Issuer: CN=L1
Validity
    Not Before: Feb  6 00:00:00 2025 GMT
    Not After : Aug  5 23:59:59 2025 GMT
Subject: CN=L2
Subject Public Key Info:
    Public Key Algorithm: ED25519
        ED25519 Public-Key:
        pub:
            3d:4e:84:d4:37:d8:d4:f0:8e:98:74:5a:45:15:86:
            30:13:37:88:e8:15:c4:76:c3:ba:5c:a1:dc:e4:5b:
            9b:01
```

Sample Issuing CA Certificate

```
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                43:66:1C:DA:A9:B9:7E:83:BB:81:9A:7E:BF:4B:78:26:80:36:F3:9A
            X509v3 Authority Key Identifier:
                C7:26:16:2D:84:73:97:28:B1:DB:97:0E:29:62:21:06:48:0E:3A:F6
    Signature Algorithm: ED25519
    Signature Value:
        3e:b1:d9:aa:ee:9a:9f:fe:9e:8f:b4:ed:ba:16:31:54:d5:c0:
        c3:e7:0d:d4:d9:f4:ca:ea:7d:ef:a3:bf:3a:3a:27:67:e8:dd:
        72:84:b6:e3:37:45:2c:d4:90:35:92:e0:a9:5c:ca:47:f8:1f:
        de:68:e7:9c:fb:2a:38:d3:c9:0
```

DER 277 bytes, C509 178 bytes

Sample Issuing CA Certificate

```
C509 :

	[3, h'71153FF47AEB48FF', 12, [-1, "L1"], 1738800000, 1754438399, [-1, "L2"], 10,
h'3D4E84D437D8D4F08E98745A45158630133788E815C476C3BA5CA1DCE45B9B01', [1,
h'43661CDAA9B97E83BB819A7EBF4B78268036F39A', 7,
h'C726162D84739728B1DB970E29622106480E3AF6'],
h'3EB1D9AAEE9A9FFE9E8FB4EDBA163154D5C0C3E70DD4D9F4CAEA7DEFA3BF3A3A27
67E8DD7284B6E337452CD4903592E0A95CCA47F81FDE68E79CFB2A38D3C908']
```