

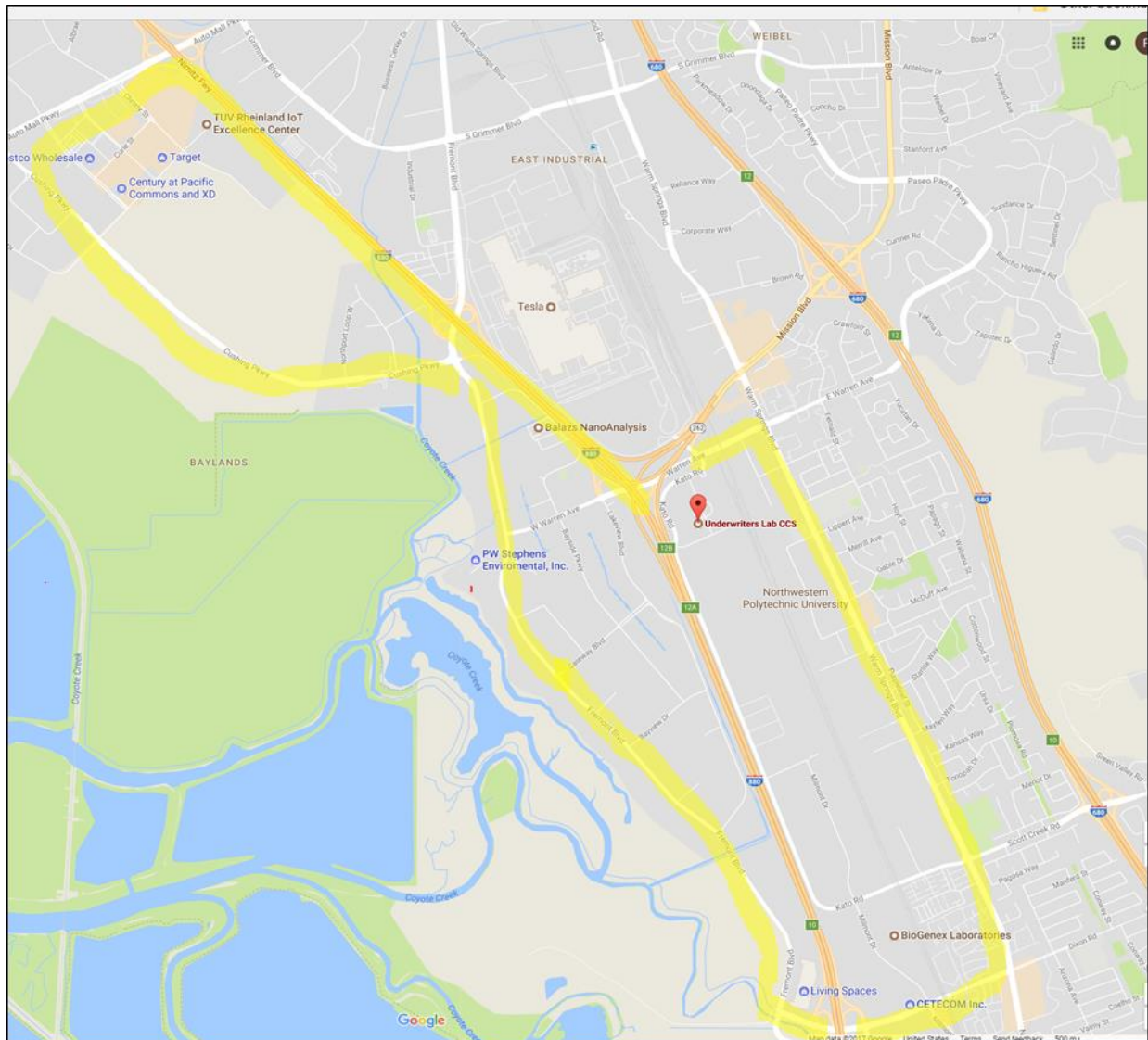
# Certificate Changing with Vehicle In-Motion Instructions

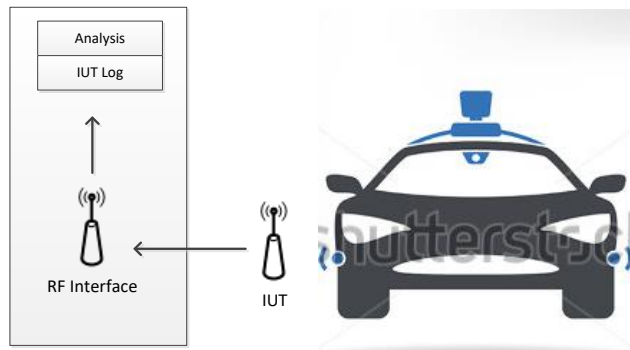
## Test Case Verification Objective:

- BSM: TP-BSM-ST-BV-02 thru 03-x, TP-BSM-ST-BV-08, TP-BSM-ST-BV-09
- Certificate Change per Distance: TP-BSM-MV-BV-01
- RadiusOfCurve: All

## Test Location:

- 12mile mixture traffic route around UL-Fremont location giving ~ 26 minutes.



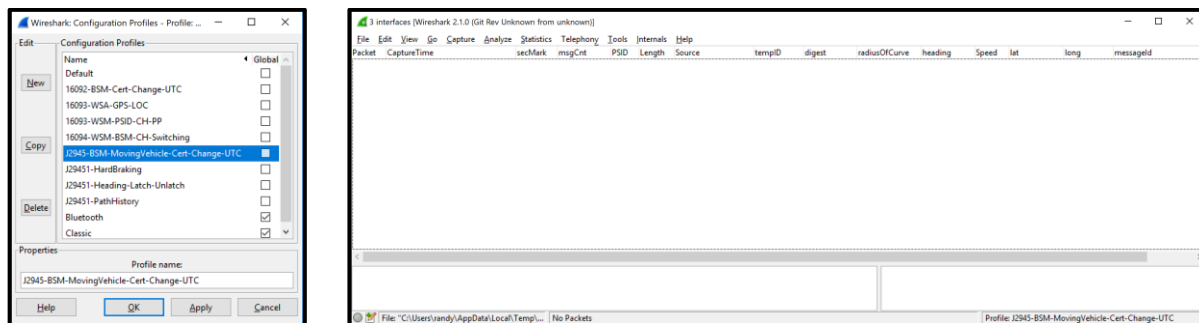


## States in Initial Conditions

- IUT is powered up and transmitting.
- GNSS in open-sky conditions is being received and lock.
- IUT has security enabled with certificates and digests to successfully transmit BSMs.
- N-Type Headers enabled for power, channel and data rate.
- IUT is configured to transmit BSMs on a 10 MHz channel vChannelNumber (CH172), data rate vDataRate (6 Mbps) and power vPowerLevel (20 dBm) at 10 Hz transmission rate.

## Setup Verification with Test Tool

1. Verify time correlation of Test Computer and UTC Network time at day start.
2. Verify time correlation of Test Tool (GPS PPS – Second value) and Test Computer at each test session.
3. Verify PCAP packet capture date/time stamp with the test computer at each test.
4. Select Configuration Profile “J29451-CertificateChanging” in Wireshark for this test.



BSM Capture Population Example of Certificate Changing.

**Certificate Change Test start with vehicle stationary for five minutes.**

Packet	CaptureTime	secMark	PSID	Length	Source	tempID	digest	CertSignature	Speed	lat	long	radiusOfCurve	Se
1	2017-09-13 19:50:56.346	55100	32	344	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		0	294425297	-986268203	32767	
2	2017-09-13 19:50:56.446	55200	32	344	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		0	294425297	-986268203	32767	
3	2017-09-13 19:50:56.547	55300	32	344	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		0	294425297	-986268203	32767	
4	2017-09-13 19:50:56.647	55400	32	415	02:8f:32:3d:18:c6	04780182		ff42fae66cfd7c1d	0	294425296	-986268205	32767	
5	2017-09-13 19:50:56.748	55500	32	344	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		0	294425297	-986268203	32767	
6	2017-09-13 19:50:56.847	55600	32	344	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		0	294425296	-986268203	32767	
7	2017-09-13 19:50:56.948	55700	32	344	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		0	294425296	-986268205	32767	
8	2017-09-13 19:50:57.048	55800	32	344	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		0	294425296	-986268205	32767	
9	2017-09-13 19:50:57.148	55900	32	415	02:8f:32:3d:18:c6	04780182		ff42fae66cfd7c1d	0	294425296	-986268205	32767	
10	2017-09-13 19:50:57.249	56000	32	344	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		0	294425296	-986268205	32767	
11	2017-09-13 19:50:57.348	56100	32	344	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		0	294425296	-986268205	32767	

```

Frame 1: 344 bytes on wire (2752 bits), 344 bytes captured (2752 bits)
Radiotap Header v0, Length 42
802.11 radio information
IEEE 802.11 QoS data, Flags: .....C
Logical-Link control
WSP IEEE 1609.3r2016 PSID: (32)
security
  protocolVersion: 3
  choice tag: 10... context-specific: choice index 1
  content: 1
    signedData

```

**Vehicle starts moving (speed increasing) at packet 3009 and shows no changes in Mac Address, Digest and TempID.**

Packet	CaptureTime	secMark	PSID	Length	Source	tempID	digest	CertSignature	Speed	lat	long	radiusOfCurve	Sequence
3004	2017-09-13 19:55:57.672	56400	32	415	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	ff42fae66cf7c1d	0	294425166	-986268218	32767	
3005	2017-09-13 19:55:57.772	56500	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	0	294425166	-986268220	32767		
3006	2017-09-13 19:55:57.873	56600	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	0	294425167	-986268218	32767		
3007	2017-09-13 19:55:57.973	56700	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	0	294425169	-986268218	32767		
3008	2017-09-13 19:55:58.074	56800	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	0	294425171	-986268218	32767		
3009	2017-09-13 19:55:58.176	56900	32	415	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	ff42fae66cf7c1d	0	294425172	-986268218	32767	
3010	2017-09-13 19:55:58.274	57000	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	3	294425174	-986268220	32767		
3011	2017-09-13 19:55:58.377	57100	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	11	294425177	-986268220	32767		
3012	2017-09-13 19:55:58.477	57200	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	15	294425179	-986268220	32767		
3013	2017-09-13 19:55:58.576	57300	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	16	294425182	-986268220	32767		
3014	2017-09-13 19:55:58.678	57400	32	415	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	ff42fae66cf7c1d	20	294425187	-986268220	32767	
3015	2017-09-13 19:55:58.777	57500	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	23	294425191	-986268220	32767		
3016	2017-09-13 19:55:58.877	57600	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	25	294425196	-986268220	32767		
3017	2017-09-13 19:55:58.980	57700	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	28	294425201	-986268220	32767		
3018	2017-09-13 19:55:59.079	57800	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	33	294425207	-986268222	32767		
3019	2017-09-13 19:55:59.179	57900	32	415	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	ff42fae66cf7c1d	36	294425212	-986268222	32767	
3020	2017-09-13 19:55:59.280	58000	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	40	294425221	-986268222	32767		
3021	2017-09-13 19:55:59.378	58100	32	344	02:8f:32:3d:18:c6	04780182	909d03e04fa6e3fe	43	294425229	-986268223	32767		

Frame 3009: 415 bytes on wire (3320 bits), 415 bytes captured (3320 bits)

Radiotap Header v0, Length 42

802.11 radio information

IEEE 802.11 QoS Data, Flags: .....C

Logical-Link Control

WSP IEEE 1609.3r2016 PSID: (32)

Security

protocolVersion: 3

choice tag: 10, ... context-specific: choice index 1

content: 1

signedData

**Packet 5083 shows Mac Address, Digest and TempID changes and randomized msgCount.**

Packet	CaptureTime	SecMac	PSID	msgCnt	Length	Source	tempId	digest	CertSignature	Speed	lat	long	radiusOfCurve
5078	2017-09-13 19:59:25.769	24500	32	67	257	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		668	294442496	-9860662806	478
5079	2017-09-13 19:59:25.870	24600	32	68	328	02:8f:32:3d:18:c6	04780182		ff42fae66cdfc1d	669	294442483	-9860662671	457
5080	2017-09-13 19:59:25.970	24700	32	69	257	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		669	294442467	-9860662396	438
5081	2017-09-13 19:59:26.070	24800	32	70	257	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		669	294442452	-9860662536	424
5082	2017-09-13 19:59:26.171	24900	32	71	257	02:8f:32:3d:18:c6	04780182	909d03e04f46e3fe		671	294442437	-9860662623	412
5083	2017-09-13 19:59:26.271	25000	32	72	328	02:8f:32:3d:18:c6	45810182		f42fae66cdfc1d	672	294442420	-9860662496	402
5084	2017-09-13 19:59:26.372	25100	32	22	257	8e:0a:c3:0a:8f:54	45810182	dec96d8dd688e9a7		673	294442403	-9860661991	392
5085	2017-09-13 19:59:26.472	25200	32	23	257	8e:0a:c3:0a:8f:54	45810182	dec96d8dd688e9a7		673	294442384	-9860661855	383
5086	2017-09-13 19:59:26.572	25300	32	24	257	8e:0a:c3:0a:8f:54	45810182	dec96d8dd688e9a7		676	294442366	-9860661718	374
5087	2017-09-13 19:59:26.672	25400	32	25	257	8e:0a:c3:0a:8f:54	45810182	dec96d8dd688e9a7		676	294442347	-9860661583	373
5088	2017-09-13 19:59:26.772	25500	32	26	328	8e:0a:c3:0a:8f:54	45810182		ff42fae66cdfc1d	674	294442327	-9860661446	369
5089	2017-09-13 19:59:26.872	25600	32	27	257	8e:0a:c3:0a:8f:54	45810182	dec96d8dd688e9a7		678	294442306	-9860661310	366
5090	2017-09-13 19:59:26.971	25700	32	28	257	8e:0a:c3:0a:8f:54	45810182	dec96d8dd688e9a7		679	294442284	-9860661172	362
5091	2017-09-13 19:59:27.073	25800	32	29	257	8e:0a:c3:0a:8f:54	45810182	dec96d8dd688e9a7		678	294442262	-9860661033	361
5092	2017-09-13 19:59:27.173	25900	32	30	257	8e:0a:c3:0a:8f:54	45810182	dec96d8dd688e9a7		680	294442240	-9860660987	359
5093	2017-09-13 19:59:27.274	26000	32	31	328	8e:0a:c3:0a:8f:54	45810182		ff42fae66cdfc1d	678	294442216	-9860660760	359
5094	2017-09-13 19:59:27.375	26100	32	32	257	8e:0a:c3:0a:8f:54	45810182	dec96d8dd688e9a7		680	294442193	-9860660624	358
5095	2017-09-13 19:59:27.476	26200	32	33	257	8e:0a:c3:0a:8f:54	45810182	dec96d8dd688e9a7		682	294442166	-9860660482	358

Frame 5083: 328 bytes on wire (2624 bits), 328 bytes captured (2624 bits)

- Radiotap Header v0, Length 42
- 802.11 radio information
- IEEE 802.11 QoS Data, Flags: .....C
- Logical-Link control
- WSPM IEEE 1609.3r2016 PSD: (32)
- Security
  - protocolVersion: 3
  - choice tag: 10, .... context-specific: choice index 1
  - content: 1
  - signedData

## Setup OBU Verification while Vehicle Stationary

1. Three Sharkfin magnet mount dual “DSRC/GNSS” antennas with 10M cables with fakra connectors mounted on vehicle’s roof in organized alignment across vehicle directional center line. 10m cables These components are consistent with all tests and testing sessions.
2. Three IUTs should use center mounted antennas.
3. Each IUT should provide their power cable if cable is not available.
4. IUT verifies its UTC Time Correlation (TP-BSM-ST-BV-20-V) with its system clock and BSM capture of the test tool.
5. IUT verifies vehicle’s length and width (TP-BSM-MV-BV-14) in BSM that matches vehicle used in the test.

## Test Procedure

1. Start packet sniffer with CH172 enabled and GPS/Time synchronized to record PCAP and WireShark in “J29451-BSM-HardBraking” configuration profile.
2. Start OBUs under test with BSMs transmitting.
3. Vehicle is stationary for five minutes and then start driving in the route (~26 minutes) below.
  - Start at UL facility
  - Right on Kato, Right on Warren Avenue, right on Warm Springs, right on Dixon Road, right on Fremont Blvd, left on Cushing Parkway, right on Auto Mall Parkway, right on I880 South, exit on Warren Exit, left on Warren Avenue, Right on Kato Road, right on Benicia Street and left into UL Building # 2 lot
  - Finish at UL Facility Buliding 2.
4. Drive until certificate, digest, mac address, tempID changes and msgCount randomizes. It should change at 2 km based on GPS coordinates (line of sight). Save PCAP.
5. Save PCAP as “CertChanging-OBU-[Manufacturer’s Name]- [Manufacturer’s Name] -[Manufacturer’s Name] and show analysis.