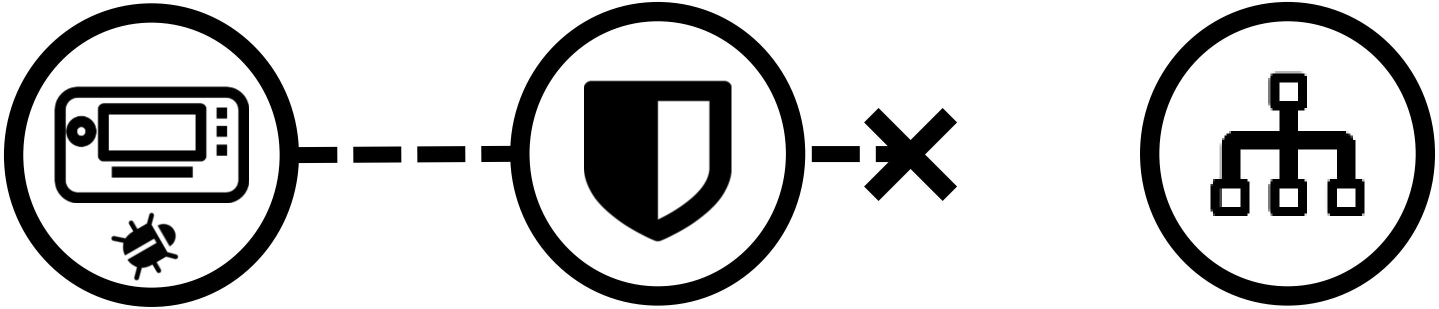
CAN Bus Firewall



GENIVI®

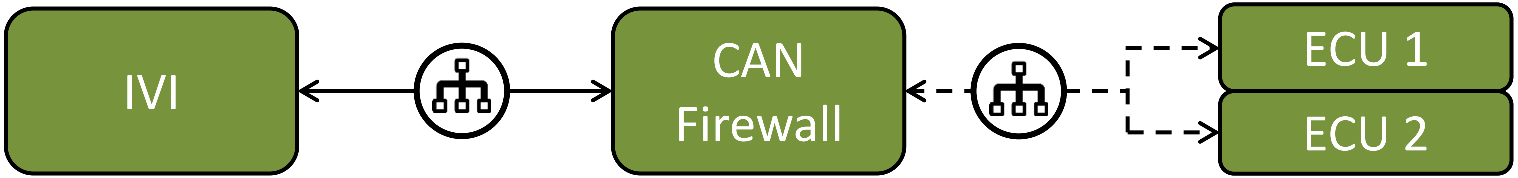
Purpose

Ensure compromised IVIs

cannot disrupt

safety critical systems

Overview



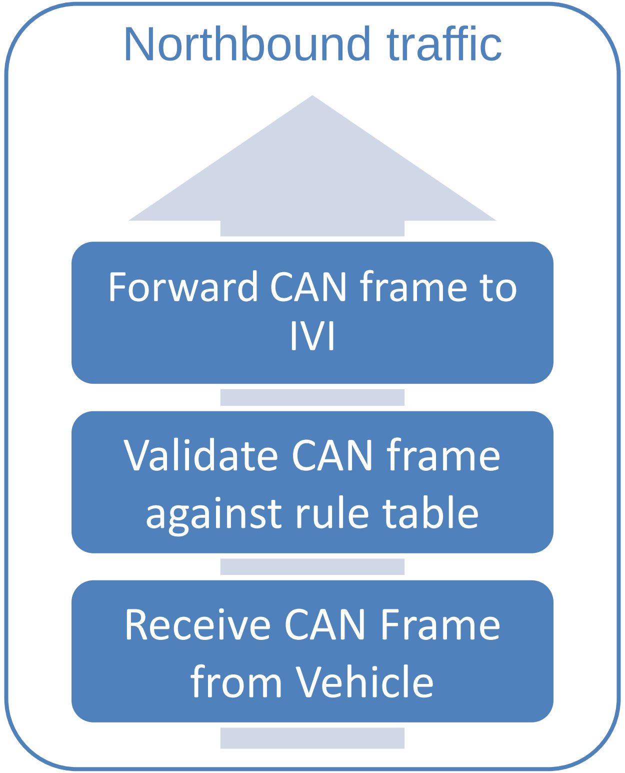
IVI
Runs a wide variety of software that may be compromised through telematics link

CAN Firewall
Hardware microcontroller on CAN bus filtering CAN traffic based on configurable rules

ECUs
Safety-critical vehicle controllers managing breaks, throttle, steering, etc.

GENIVI

Northbound vs. Southbound Traffic

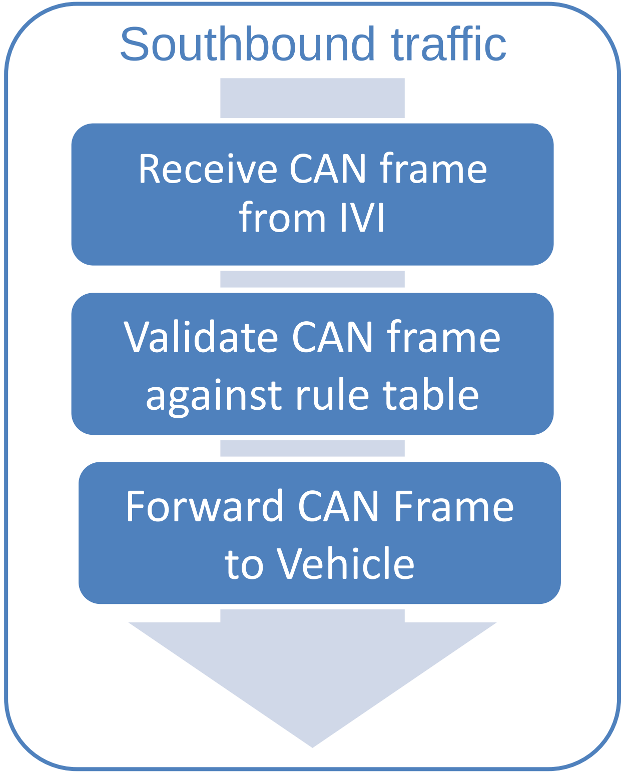


Northbound traffic

Forward CAN frame to IVI

Validate CAN frame against rule table

Receive CAN Frame from Vehicle



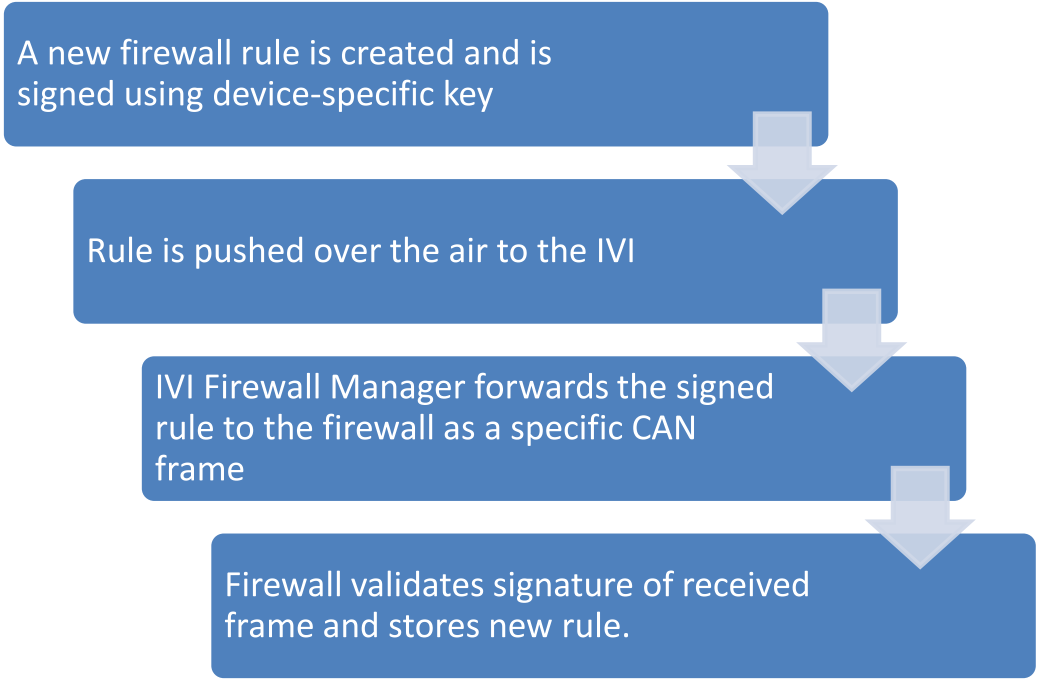
Southbound traffic

Receive CAN frame from IVI

Validate CAN frame against rule table

Forward CAN Frame to Vehicle

Use Case: Update rules

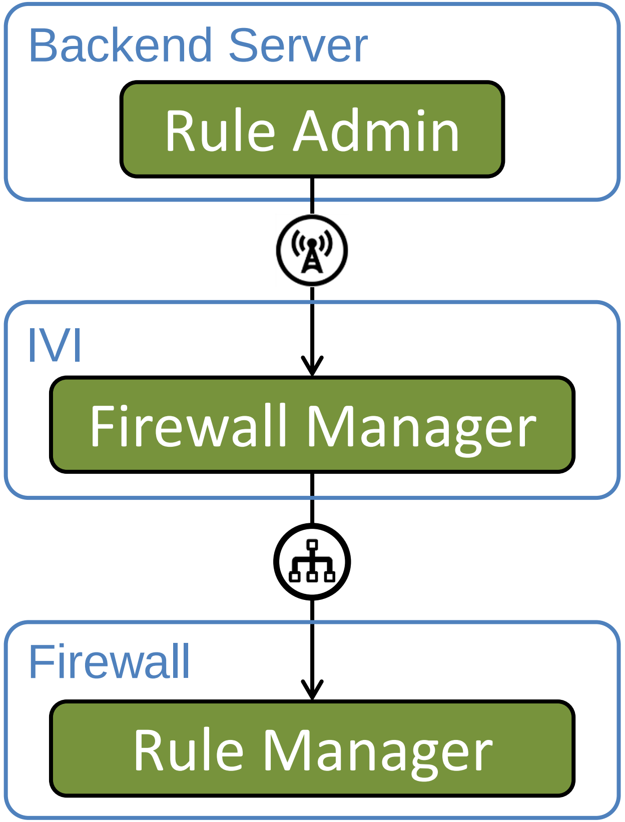


A new firewall rule is created and is signed using device-specific key

Rule is pushed over the air to the IVI

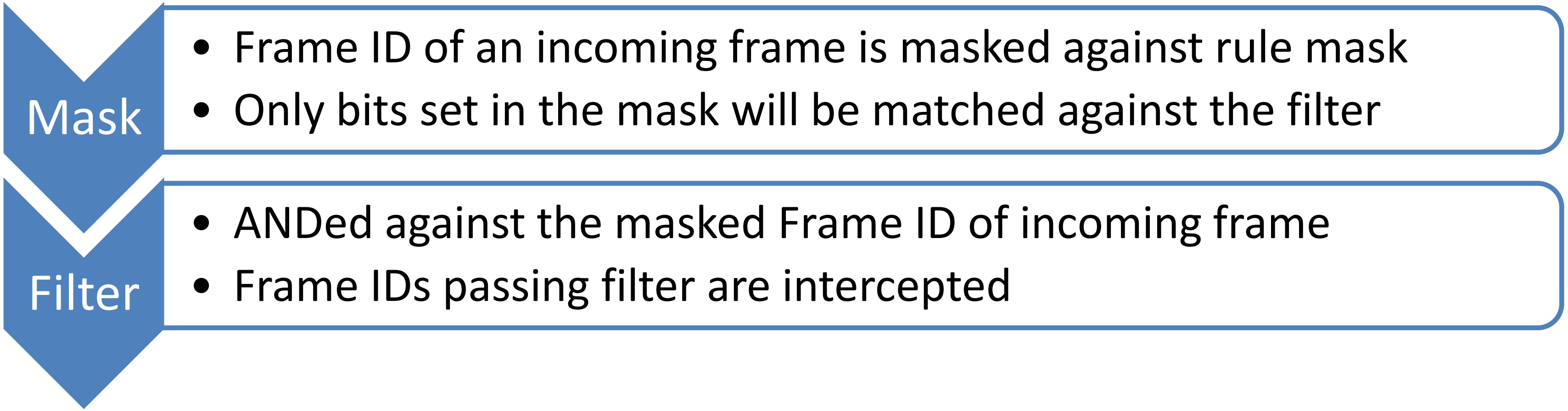
IVI Firewall Manager forwards the signed rule to the firewall as a specific CAN frame

Firewall validates signature of received frame and stores new rule.



Rule Structure [1/2]

Mask	Filter	ID XForm	Data XForm	ID Operand	Data Operand
0xFFFFFFFF	0x00000012	AND	OR	0x00FFFFFF	0x000000FFFFFFFFFF



Mask

- Frame ID of an incoming frame is masked against rule mask
- Only bits set in the mask will be matched against the filter

Filter

- ANDed against the masked Frame ID of incoming frame
- Frame IDs passing filter are intercepted

See http://www.cse.dmu.ac.uk/~eg/tele/CanbusIDandMask.html for details

Rule Structure [2/2]

Mask	Filter	ID XForm	Data XForm	ID Operand	Data Operand
0xFFFFFFFF	0x00000012	AND	OR	0x00FFFFFF	0x000000FFFFFFFFFF

ID XForm

- Determines transformation applied to outbound Frame ID (SET, AND, OR, XOR, INV)

Data XForm

- Determines transformation applied to outbound Data (SET, AND, OR, XOR, INV)

ID Operand

- Transformation operand applied to outbound Frame ID

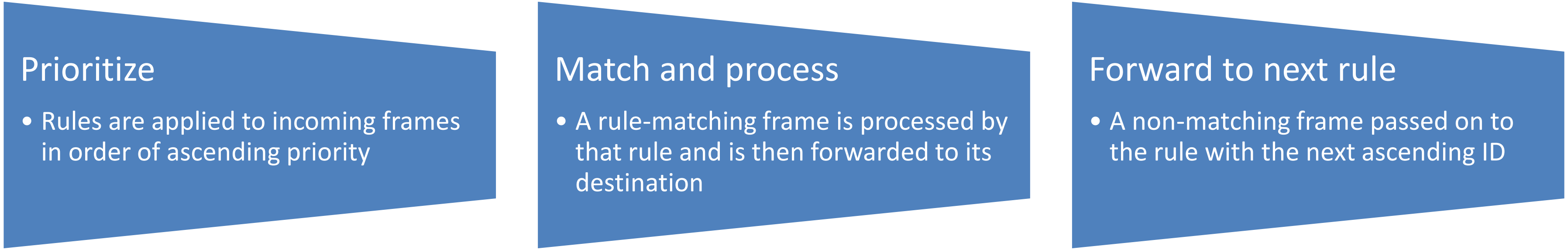
Data Operand

- Transformation operand applied to outbound Data

A Rule can also specify that the frame is to be silently dropped or passed as is.

CAN Rule Table

Prio	Mask	Filter	ID XForm	Data XForm	ID Operand	Data Operand
0x01	0xFFFFFFFF	0x00000012	AND	OR	0x00FFFFFF	0x000000FFFFFFFFFF
0x02	0xFFFFFFF0	0x00000120	SET	SET	0x01234567	0x012345678 0ABCDEF
0x7E	0x00000000	0x00000000	DROP	DROP	0x00000000	0x0000000000000000



Prioritize

- Rules are applied to incoming frames in order of ascending priority

Match and process

- A rule-matching frame is processed by that rule and is then forwarded to its destination

Forward to next rule

- A non-matching frame passed on to the rule with the next ascending ID

If no rule matches, the frame is forwarded unmodified to its destination

CAN Rule Configuration – Common Header

Frame ID	Data: Prio [1]	Data: Cmd [1]	…	…
0x00004711	0x04	[RULE]	…	…

Frame ID [32 bits]
Factory-configured CAN Frame that is intercepted and interpreted by the CAN Firewall.

Prio [0x00-0x7F | 0x80-0xFF] [1 byte]

Specifies the priority of the rule that is being prepared and which .
0x00-0x7F applies to northbound traffic. 0x80-0xFF applies to southbound traffic.
All commands setting up and storing a single rule will use the same Prio.

Cmd [PREP_RULE1, PREP_RULE2, PREP_RULE3 , PREP_RULE4, PREP_RULE5,PREP_RULE6, STORE_RULE] [1 byte]

Sets up a single rule. PREP_RULE1 – PREP_RULE6 are transmitted with the same Prio. STORE_RULE is then transmitted with the given Prio to store the single rule specified by the previous PREP rule commands.

GENIVI

CAN Rule Configuration – PREP_RULE1

Frame ID	Prio [1]	Cmd [1]	Mask [4]	XForm [1]	Rsvd [1]
0x00004711	0x04	0x01	0x0000FFFF	0x01	0x00

Cmd [PREP_RULE1] [1 byte]

PREP_RULE1 specifies the rule priority and the mask to apply, and the transform operators for the rule.

Mask [32 bit value] [4 bytes]
Mask to apply to incoming Frame ID prior to filtering.

XForm [SET_AND] [1 byte]
The transformation to apply to Frame ID and Data. Combination of SET, AND, OR, XOR, and NEG. Upper four bits defines Frame ID operator. Lower four bits defines Data operator.

Reserved for future use. Set to 0

CAN Rule Configuration – PREP_RULE2

Frame ID	Prio [1]	Cmd [1]	Filter [4]	DtOper1 [2]
0x00004711	0x04	0x02	0x0000AAC1	0x0001

Cmd [PREP_RULE2] [1 byte]

PREP_RULE2 specifies the filter to apply to incoming Frame IDs and the low 16 bits of the Data transformation operand

Filter [4] [32 bit value] [4 bytes]
Filter to apply to incoming Frame ID that has been masked.

DtOper1 [16 bit value] [2 bytes]
Specifies the little endian bits 0-15 of the data operand to provide to the data transform operator (AND, OR, XOR, NEG).

CAN Rule Configuration – PREP_RULE3

Frame ID	Prio [1]	Cmd [1]	DtOper2 [6]
0x00004711	0x04	0x03	0x020304050607

Cmd [PREP_RULE3] [1 byte]

PREP_RULE2 specifies the high 48 bits of the operand to apply to the payload transform operator.

DtOper2 [48 bit value] [6 bytes]

Specifies little endian bits 16-63 of the data operand to provide to the data transform operator (AND, OR, XOR, NEG).
DtOper1 and DtOper2 in the example above are concatenated to: 0x0706050403020100

CAN Rule Configuration – PREP_RULE4

Frame ID	Prio [1]	Cmd [1]	IDOper [4]	HMAC1 [2]
0x00004711	0x04	0x04	0xFFFF0000	0x0001

Cmd [PREP_RULE4] [1 byte]

Specifies the Frame ID operand and the lowest2 bytes of the HMAC-SHA256 signature

IDOper [32 bit value] [4 bytes]

Specifies the Frame ID operand to provide to the Frame ID transform operator

HMAC1 [16 bit value] [2 bytes]

Specifies little endian bits 0-15 bits of the HMAC-SHA256 signature, generated with the key flashed into the Firewall at the factory.

CAN Rule Configuration – PREP_RULE5

Frame ID	Prio [1]	Cmd [1]	HMAC2 [6]
0x00004711	0x04	0x05	0x020304050607

Cmd [PREP_RULE5] [1 byte]

Specifies six bytes of the HMAC-SHA256 signature

HMAC2 [48 bit value] [6 bytes]

Specifies little endian bits 16-63 of the HMAC-SHA256 signature

CAN Rule Configuration – PREP_RULE6

Frame ID	Prio [1]	Cmd [1]	HMAC3 [6]
0x00004711	0x04	0x06	0x08090A0B0C0D

Cmd [PREP_RULE6] [1 byte]

Specifies six bytes of the HMAC-SHA256 signature

HMAC3 [48 bit value] [6 bytes]

Specifies little endian bits 64-111 of the HMAC-SHA256 signature

CAN Rule Configuration – PREP_RULE7

Frame ID	Prio [1]	Cmd [1]	HMAC4 [6]
0x00004711	0x04	0x07	0x0E0F10111213

Cmd [PREP_RULE7] [1 byte]

Specifies six bytes of the HMAC-SHA256 signature

HMAC4 [48 bit value] [6 bytes]
Specifies little endian bits 112-159 of the HMAC-SHA256 signature

CAN Rule Configuration – PREP_RULE8

Frame ID	Prio [1]	Cmd [1]	HMAC5 [6]
0x00004711	0x04	0x08	0x141516171819

Cmd [PREP_RULE8] [1 byte]

Specifies six bytes of the HMAC-SHA256 signature

HMAC5 [48 bit value] [6 bytes]

Specifies little endian bits 160-207 of the HMAC-SHA256 signature

CAN Rule Configuration – PREP_RULE9

Frame ID	Prio [1]	Cmd [1]	HMAC6 [6]
0x00004711	0x04	0x09	0x1A1B1C1D1E1F

Cmd [PREP_RULE9] [1 byte]

Specifies six bytes of the HMAC-SHA256 signature

HMAC6 [48 bit value] [6 bytes]
Specifies little endian bits 208-255 of the HMAC-SHA256 signature

CAN Rule Configuration – STORE_RULE

Frame ID	Prio [1]	Cmd [1]	Seq [4]	Unused [2]
0x00004711	0x04	0x10	0x00000001	0x0000

Cmd [STORE_RULE] [1 byte]

Stores the rule specified by PREP_RULE1 to PREP_RULE6

Seq [32 bit value] [4 byte]
Unique sequence number for this given Prio. Value must be greater than previously received value for the given Prio in order for the rule to be processed. Stops replay attacks.

Unused [16 bit value] [2 bytes]
Not used. Must be 0x0000

CAN Rule Configuration – Example

Frame ID	Prio	Cmd	Command Parameters		
0x00004711	0x04	0x01 [PREP_RULE1]	Mask: 0x0000FFFF	XForm: 0x01	Rsvd: 0x00
0x00004711	0x04	0x02 [PREP_RULE2]	Filter: 0x0000AAC1	DtOper1: 0x0001	
0x00004711	0x04	0x03 [PREP_RULE3]	DtOper2: 0x020304050607		
0x00004711	0x04	0x04 [PREP_RULE4]	IDOper: 0xFFFF0000	HMAC1: 0x0001	
0x00004711	0x04	0x05 [PREP_RULE5]	HMAC2: 0x020304050607		
0x00004711	0x04	0x06 [PREP_RULE6]	HMAC3: 0x08090A0B0C0D		
0x00004711	0x04	0x07 [PREP_RULE7]	HMAC4: 0x0E0F10111213		
0x00004711	0x04	0x08 [PREP_RULE8]	HMAC5: 0x141516171819		
0x00004711	0x04	0x09 [PREP_RULE9]	HMAC6: 0x1A1B1C1D1E1F		
0x00004711	0x04	0x10 [STORE_RULE]	Seq: 0x00000001	Unused: 0x0000	

↓

Prio	Mask	Filter	ID XForm	Data XForm	ID Operand	Data Operand
0x04	0x0000FFFFF	0x0000AAC1	SET	AND	0xFFFF0000	0x0706050403020100

Signature Payload used by HMAC-SHA256

Frame ID	Prio	Cmd	Command Parameters		
0x00004711	*0x04*	0x01 [PREP_RULE1]	Mask: *0x0000FFFF*	XForm: *0x01*	Rsvd: *0x00*
0x00004711	0x04	0x02 [PREP_RULE2]	Filter: *0x0000AAC1*	DtOper1: *0x0001*	
0x00004711	0x04	0x03 [PREP_RULE3]	DtOper2: *0x020304050607*		
0x00004711	0x04	0x04 [PREP_RULE4]	IDOper: *0xFFFF0000*	HMAC1: 0x0001	
0x00004711	0x04	0x05 [PREP_RULE5]	HMAC2: 0x020304050607		
		...			
0x00004711	0x04	0x10 [STORE_RULE]	Seq: *0x00000001*	Unused: *0x0000*	

Prio	Mask	XForm	Rsvd	Filter	Data Operand	ID Operand	Sequence	Unused
0x04	0x0000FFFF	0x01	0x00	0x0000AAC1	0x0706050403020100	0xFFFF0000	0x00000001	0x0000

Signature Payload string [31 bytes] (Color coded fields)
0x040000FFFF01000000AAC10706050403020100FFFF0000000000010000

Thank You

Magnus Feuer

Lead System Architect – Open Software Initiative
mfeuer@jaguarlandrover.com
+1-949-294 7871

GENIVI