

TOWARDS A STANDARDISED FRAMEWORK FOR SECURING CONNECTED VEHICLES

LICENTIATE SEMINAR 20/09/2019

THOMAS ROSENSTATTER



CHALMERS

SECURITY IN CARS

ANDY GREENBERG SECURITY 08.10.2019 02:50 PM

A Remote-Start App Exposed Thousands of Cars to Hackers

The bugs could have let an industrious hacker locate cars, unlock them, and start them up from anywhere with an internet connection.



GETTY IMAGES

Last winter, a hacker who goes by the handle Jmaxxz was looking for his girlfriend. She'd recently flown back from a work trip and

A Deep Flaw in Your Car Lets Hackers Shut Down Safety Features

A new wrinkle in auto-hacking research points to a fundamental vulnerability in the CAN protocol cars' innards use to communicate.



GETTY IMAGES

Since two security researchers showed they could hijack a moving Jeep on a highway three years ago, both automakers and the cybersecurity industry have accepted that connected cars are as vulnerable to hacking as anything else linked to the internet. But one new car-hacking trick illustrates that while awareness helps, protection can be extremely complex.

ANDY GREENBERG SECURITY 08.10.16 4:29 PM

A New Wireless Hack Can Unlock 100 Million Volkswagens



ANDY GREENBERG SECURITY 08.04.16 09:00 AM

Hackers Fool Tesla S's Autopilot to Hide and Spoof Obstacles



QILAI SHEN/BLOOMBERG/GETTY IMAGES

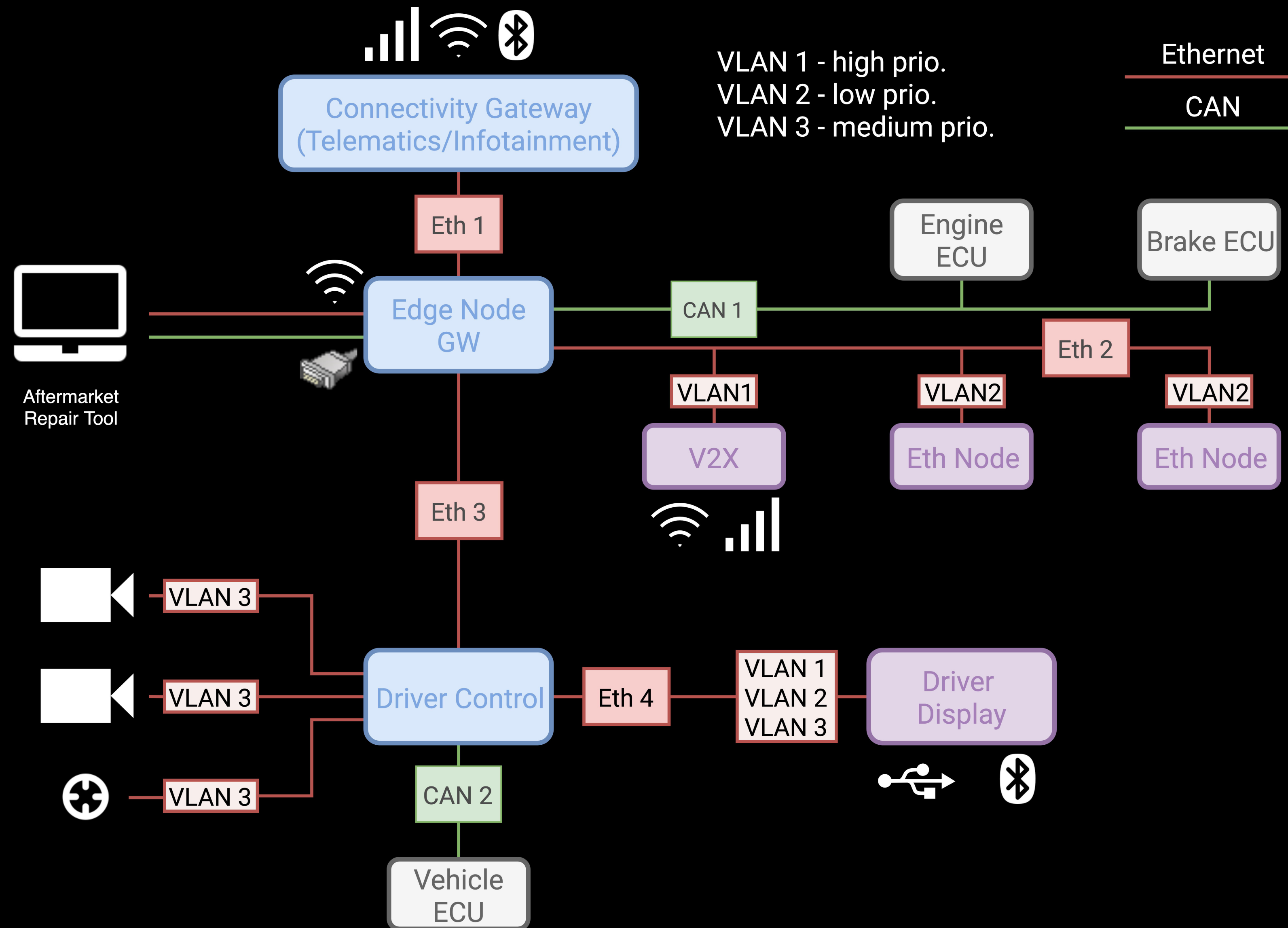
IN MAY, WHEN a Tesla S in autopilot mode failed to detect a white tractor-trailer turning into its path and careened into the rig's side at

M

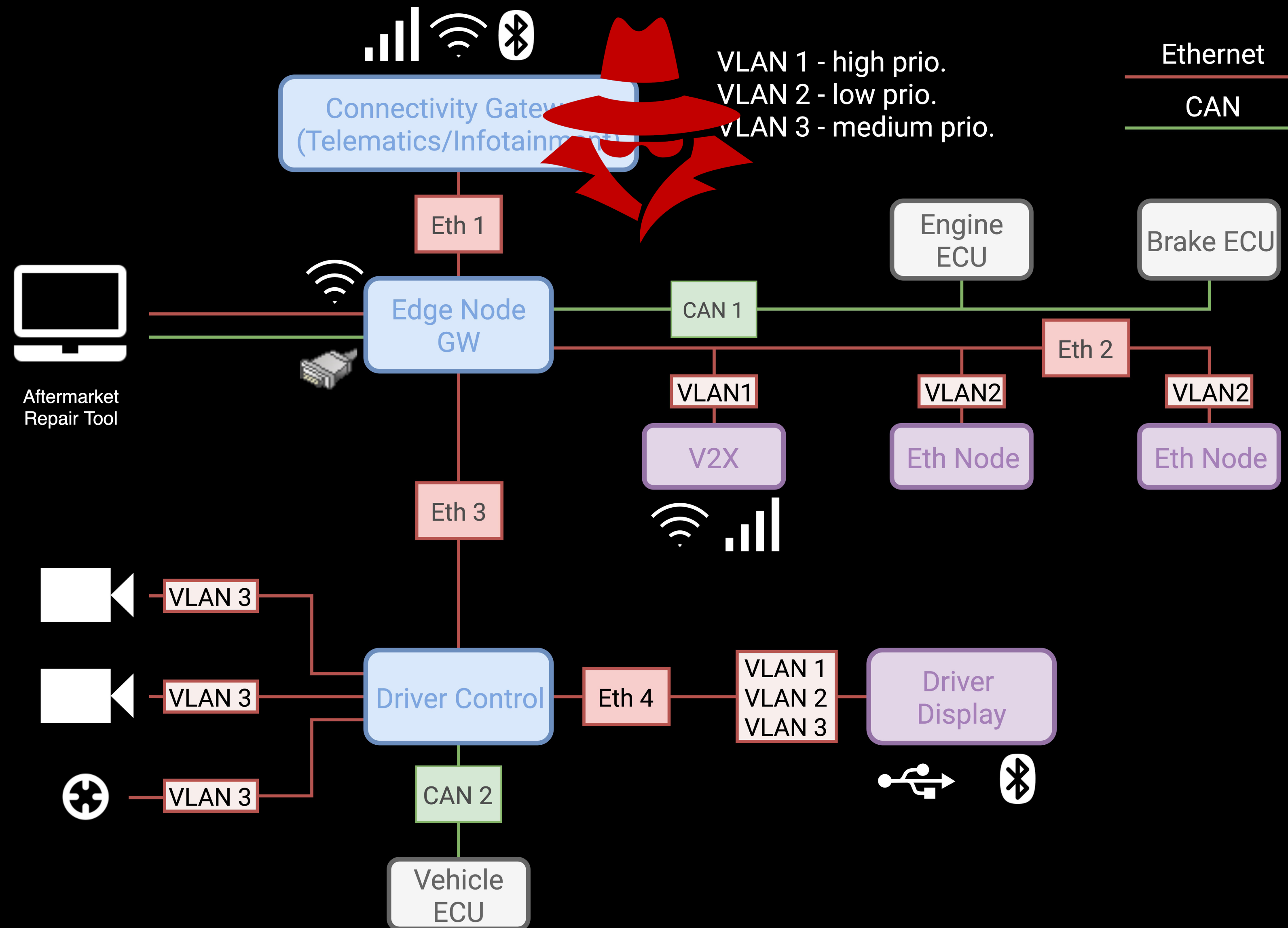


ham computer scientist Flavio
re preparing to reveal a
art the ignition of millions of
without a key, they were hit with
n of their research for two years.

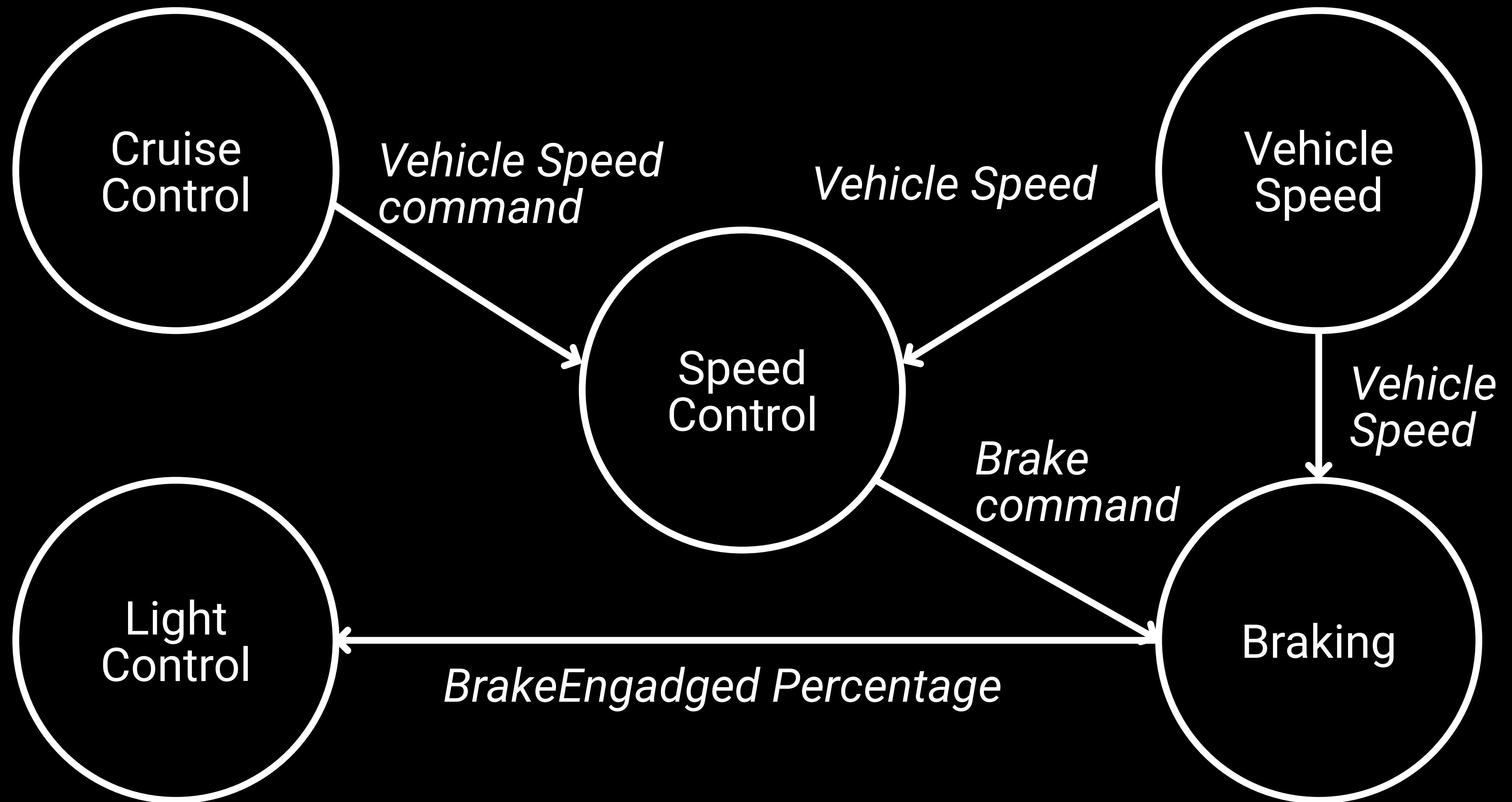
IN-VEHICLE NETWORK



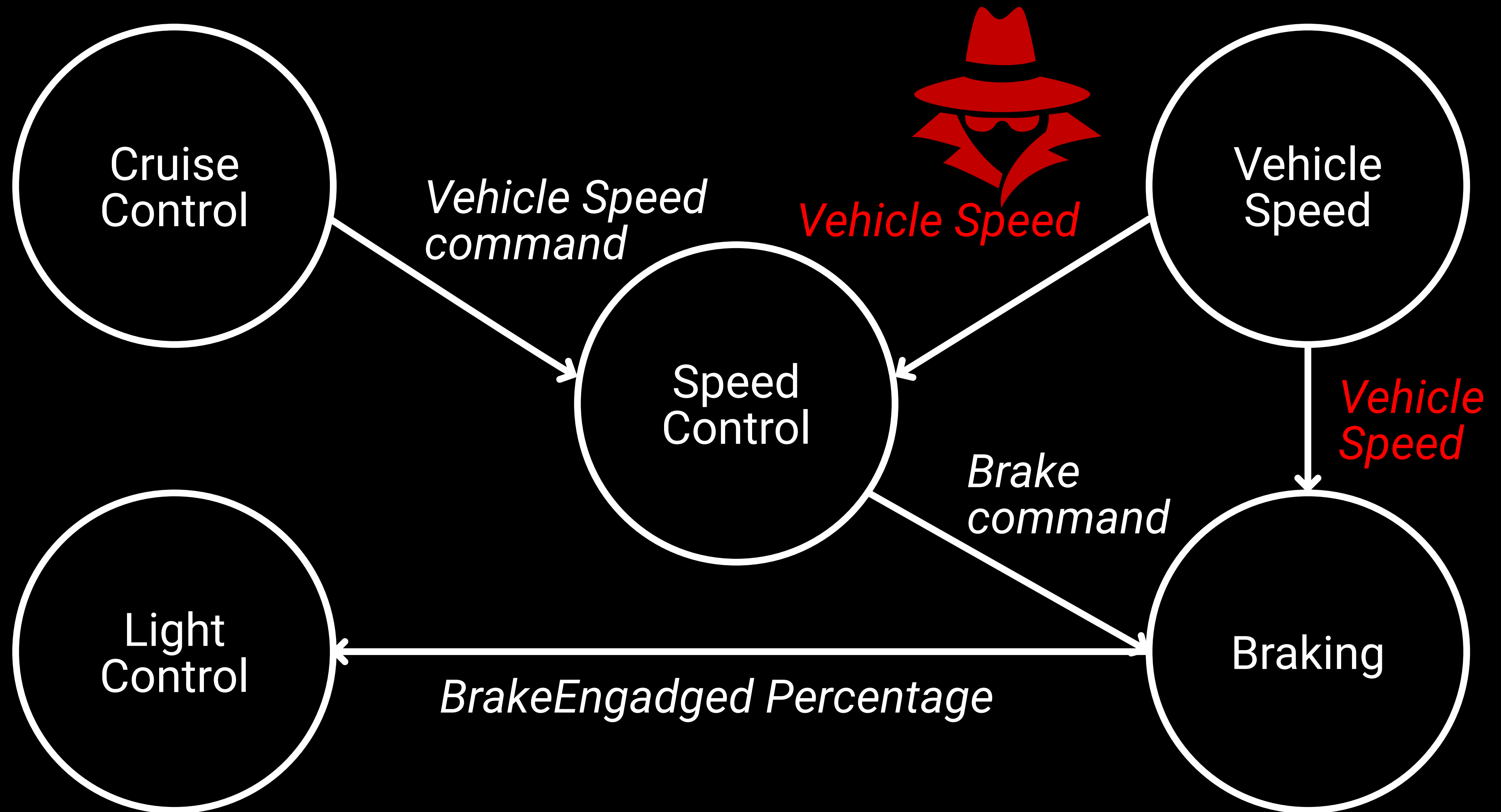
IN-VEHICLE NETWORK



USE CASE: CRUISE CONTROL

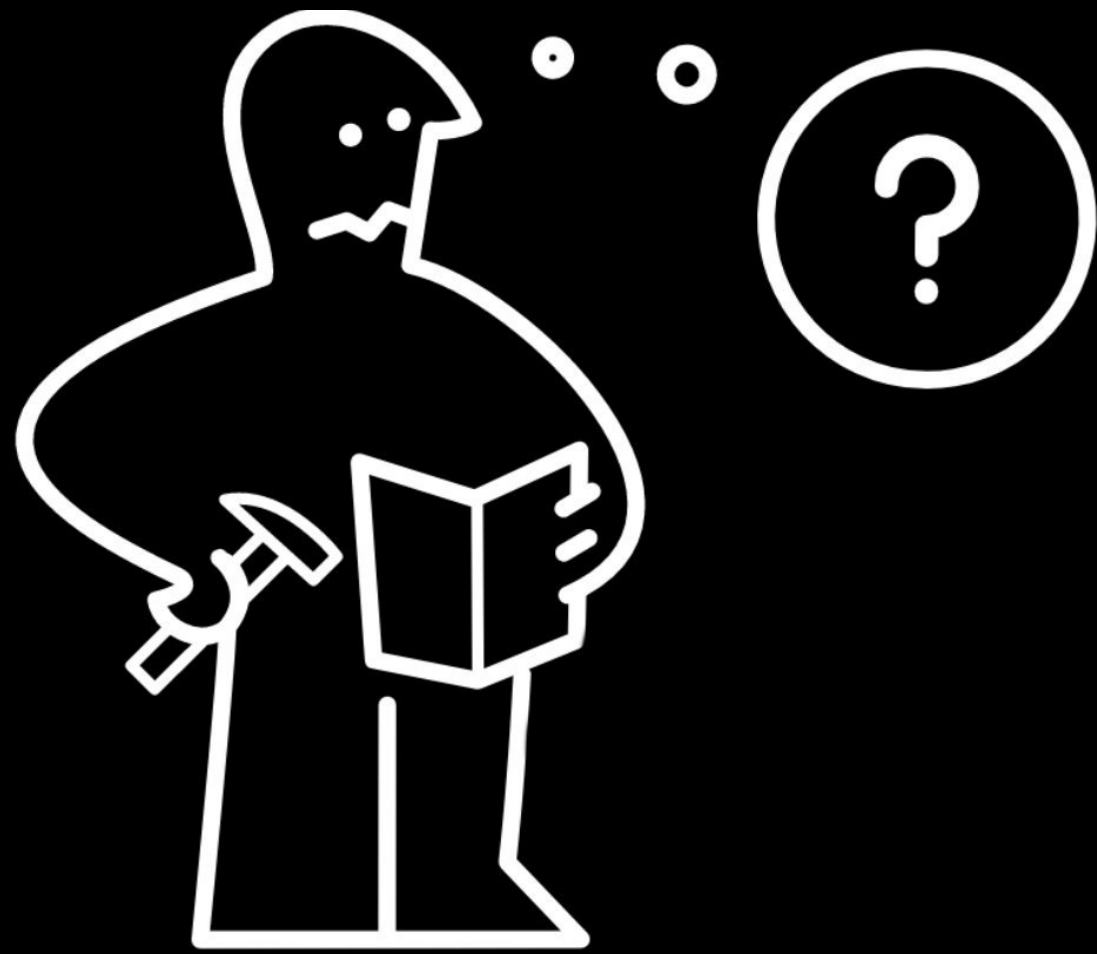


USE CASE: CRUISE CONTROL



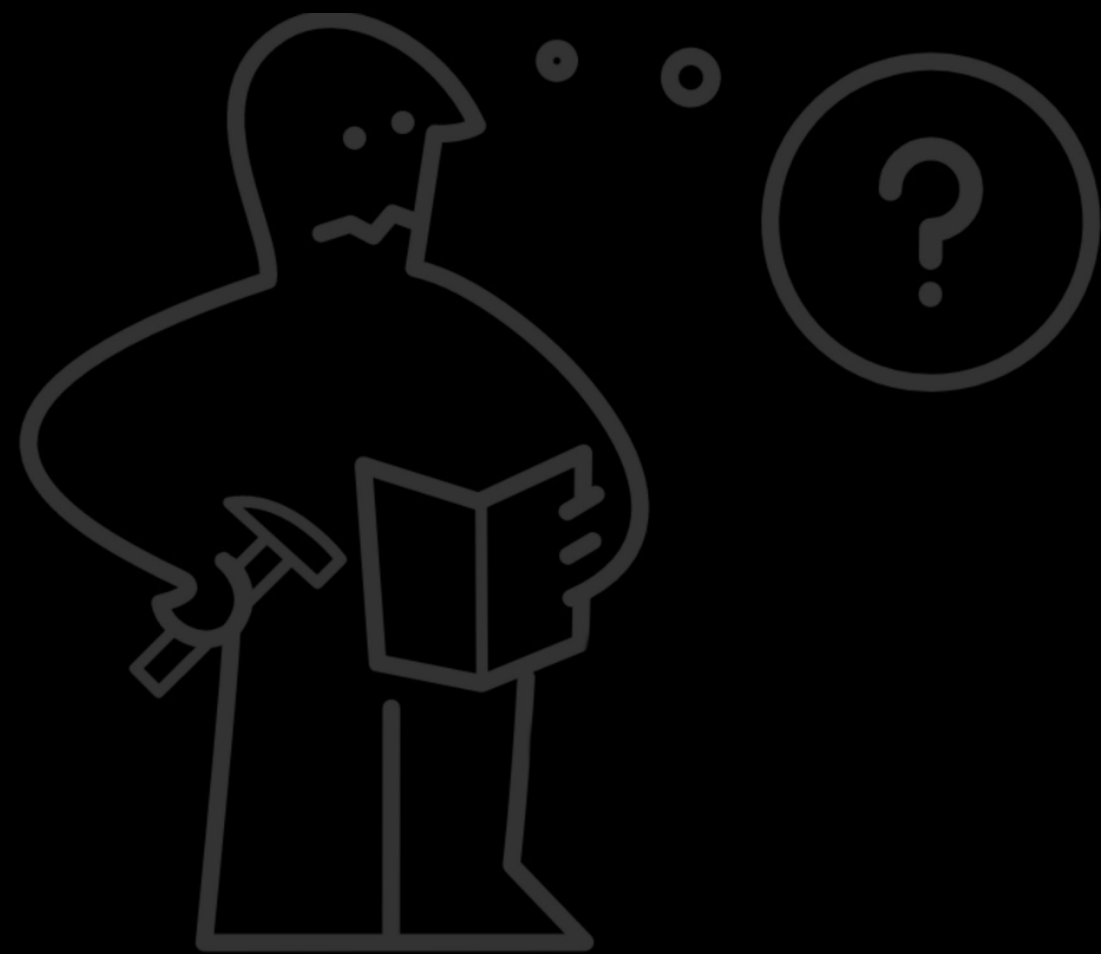
OVERVIEW

How?

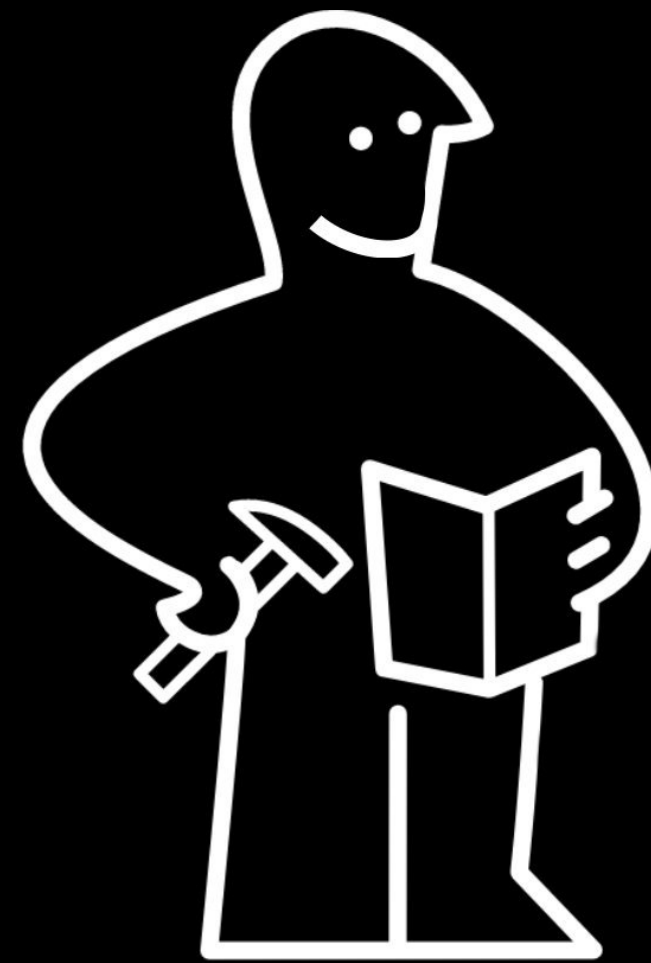


OVERVIEW

How?

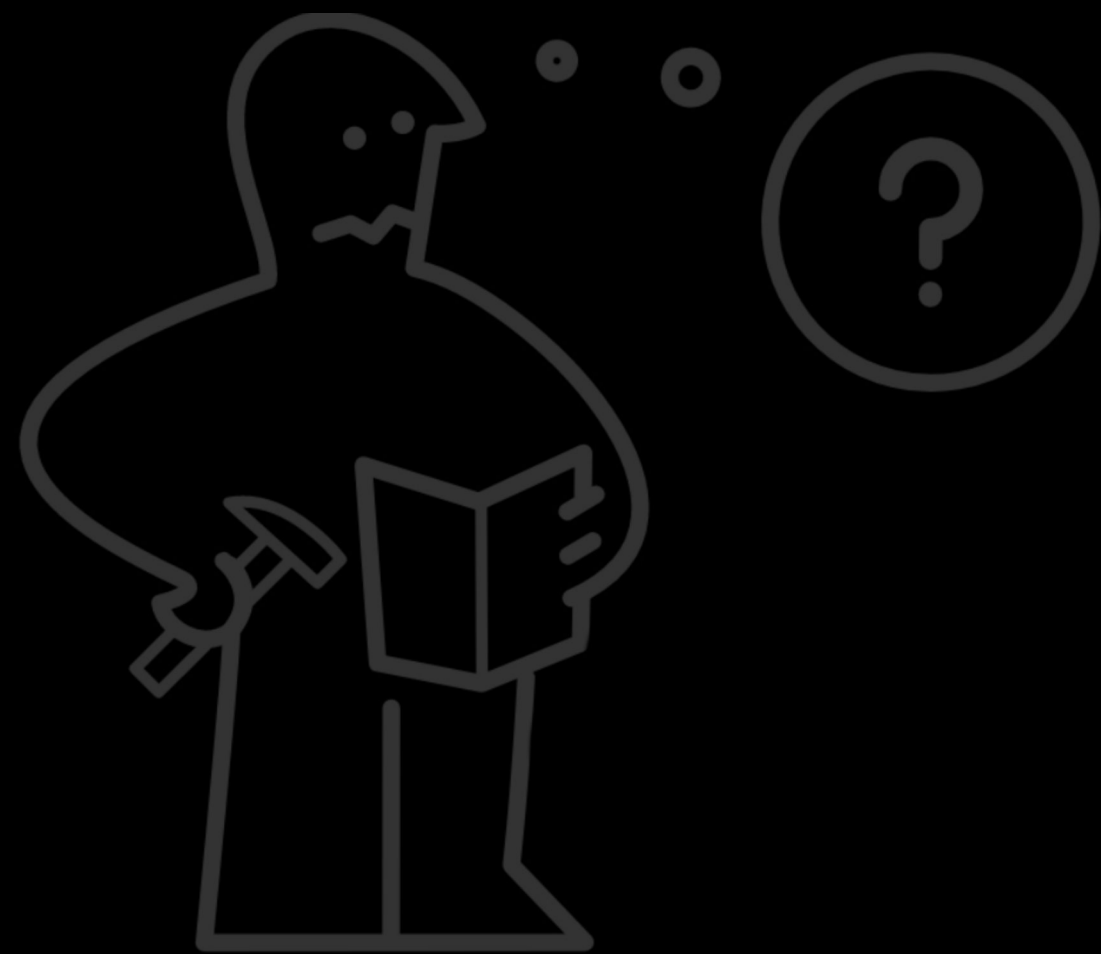


WHAT?



OVERVIEW

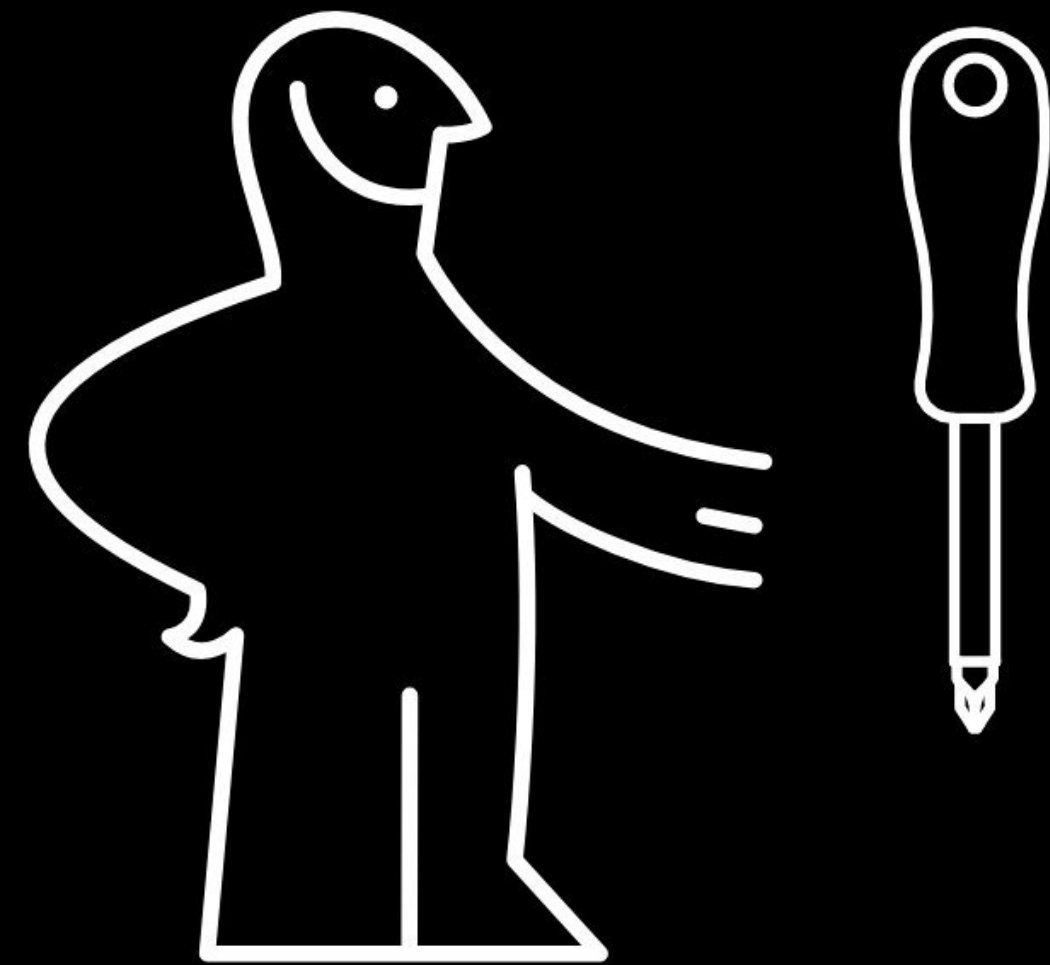
How?



WHAT?

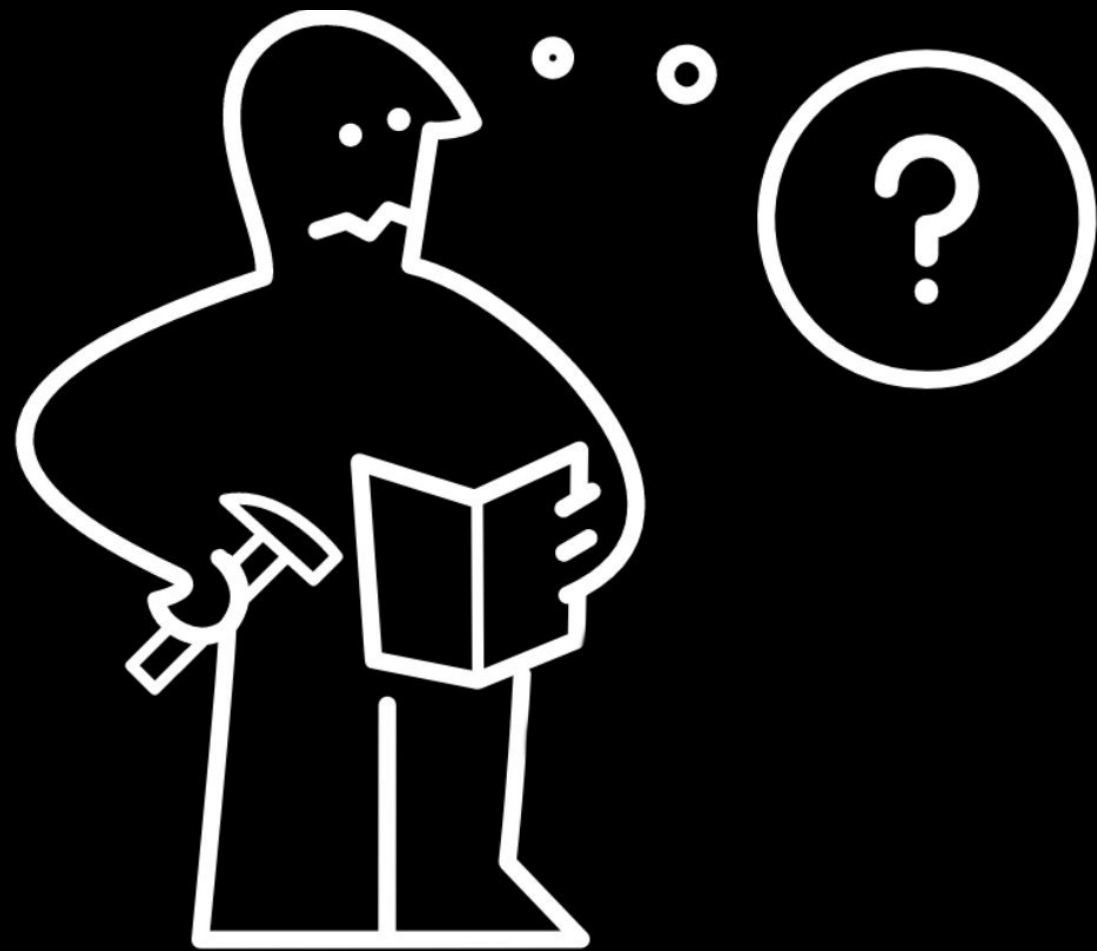


TOOL

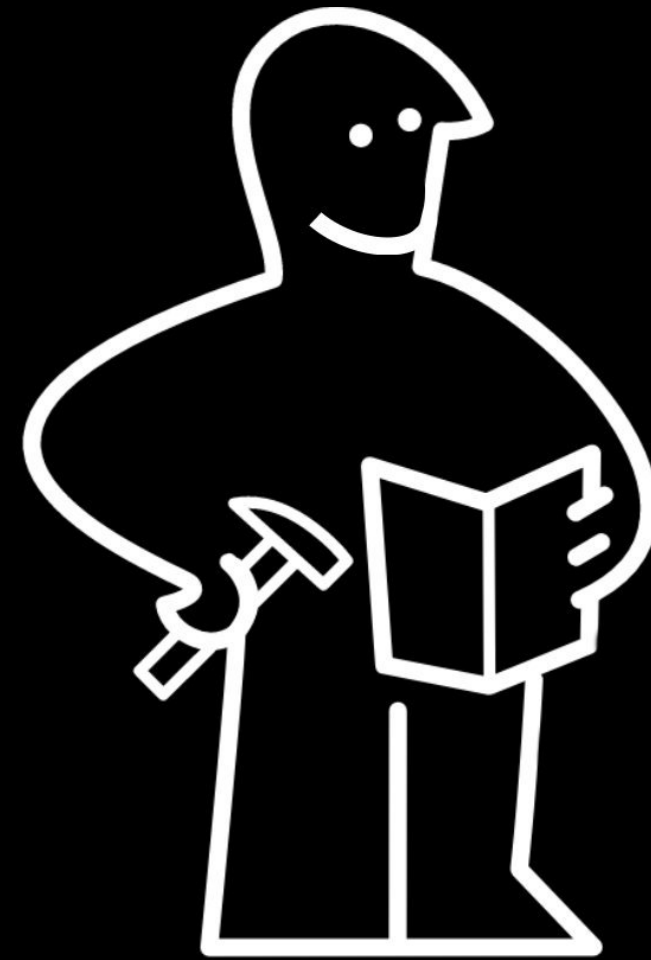


OVERVIEW

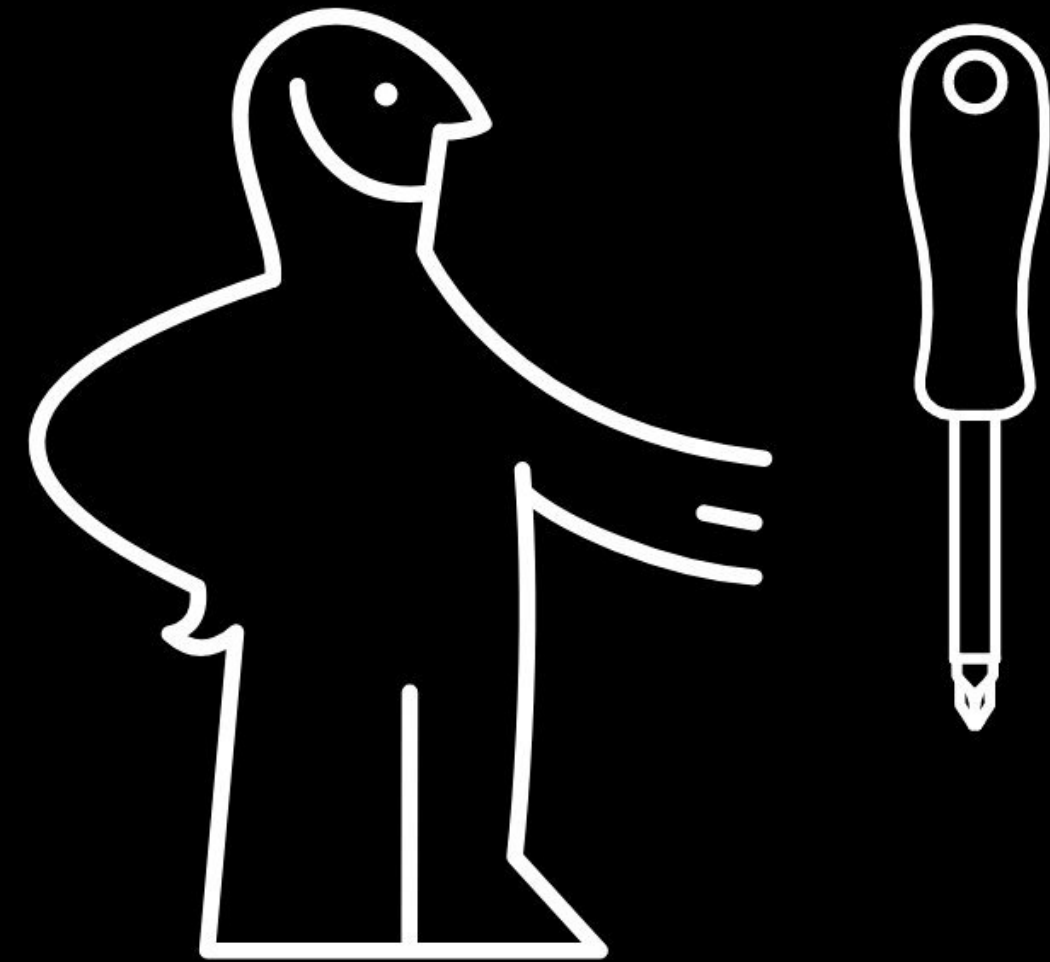
How?



WHAT?

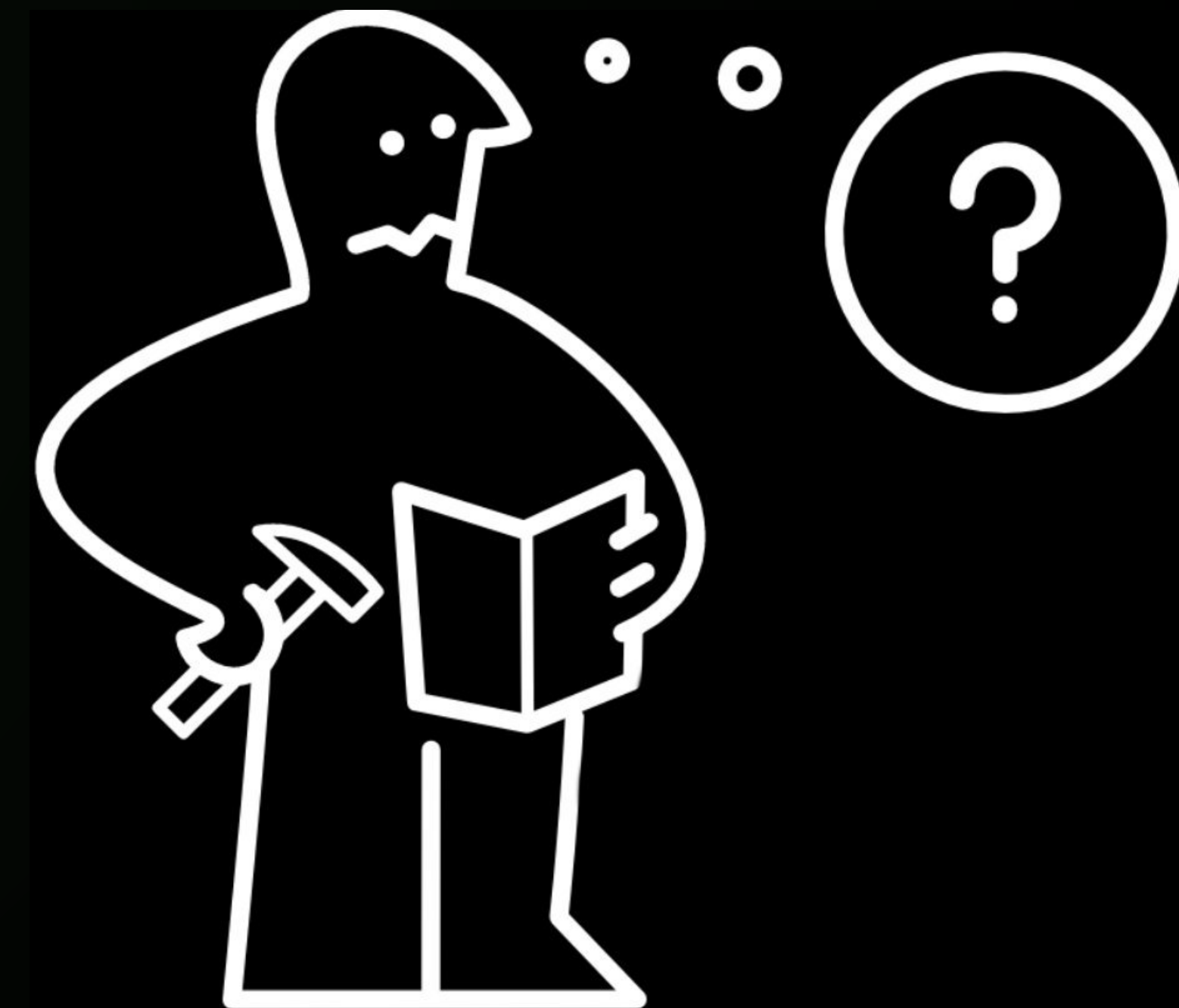
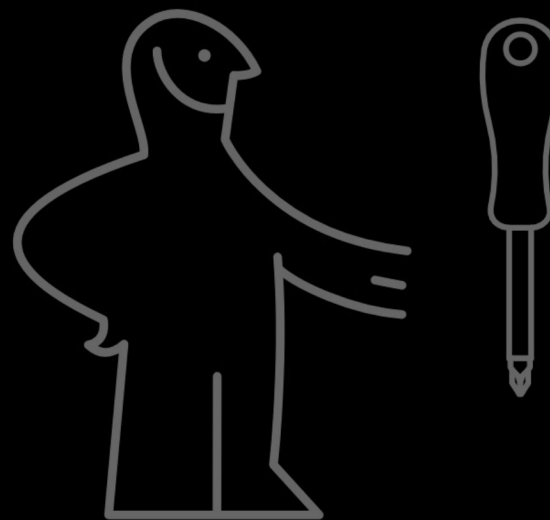
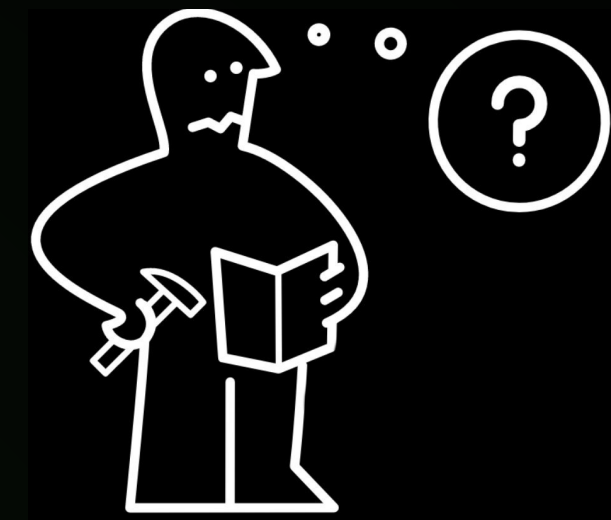


TOOL

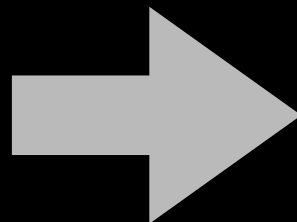
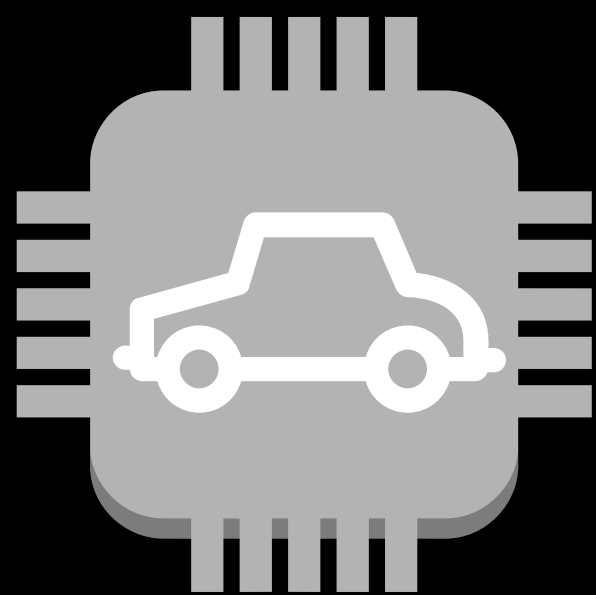


HOW

TO EXPRESS SECURITY DEMANDS?

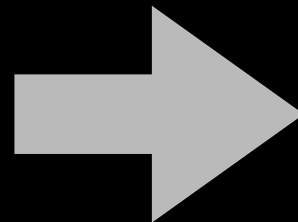


FROM SECURITY LEVELS TO MANDATORY SECURITY MECHANISMS



TARA

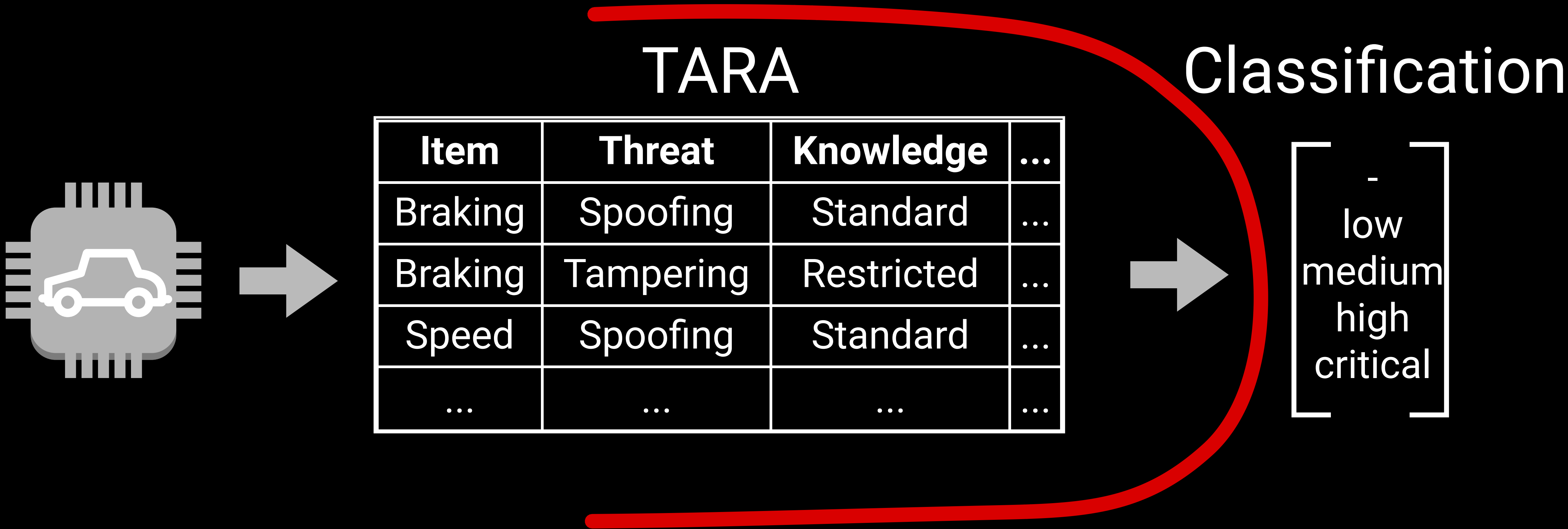
Item	Threat	Knowledge	...
Braking	Spoofing	Standard	...
Braking	Tampering	Restricted	...
Speed	Spoofing	Standard	...
...	...	...	...



Classification

-
low
medium
high
critical

FROM SECURITY LEVELS TO MANDATORY SECURITY MECHANISMS



MAPPING TO SECURITY MECHANISMS

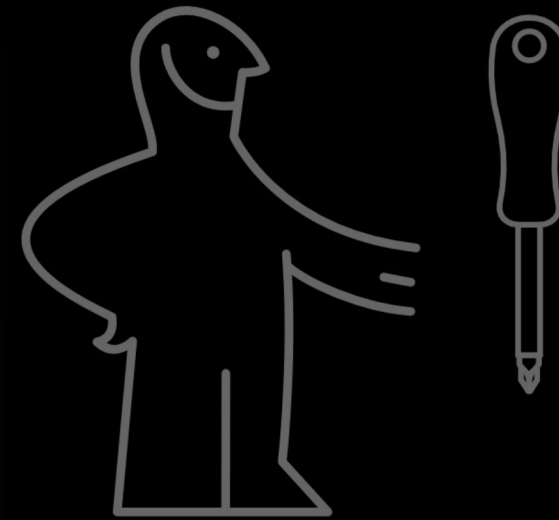
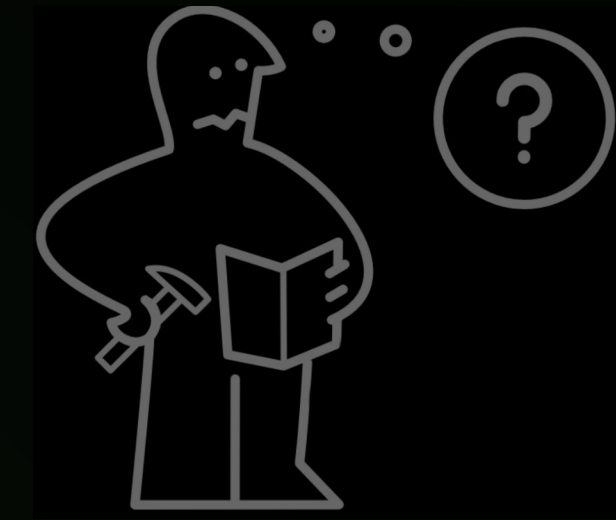
- ▶ Structure to classify security demands

MAPPING TO SECURITY MECHANISMS

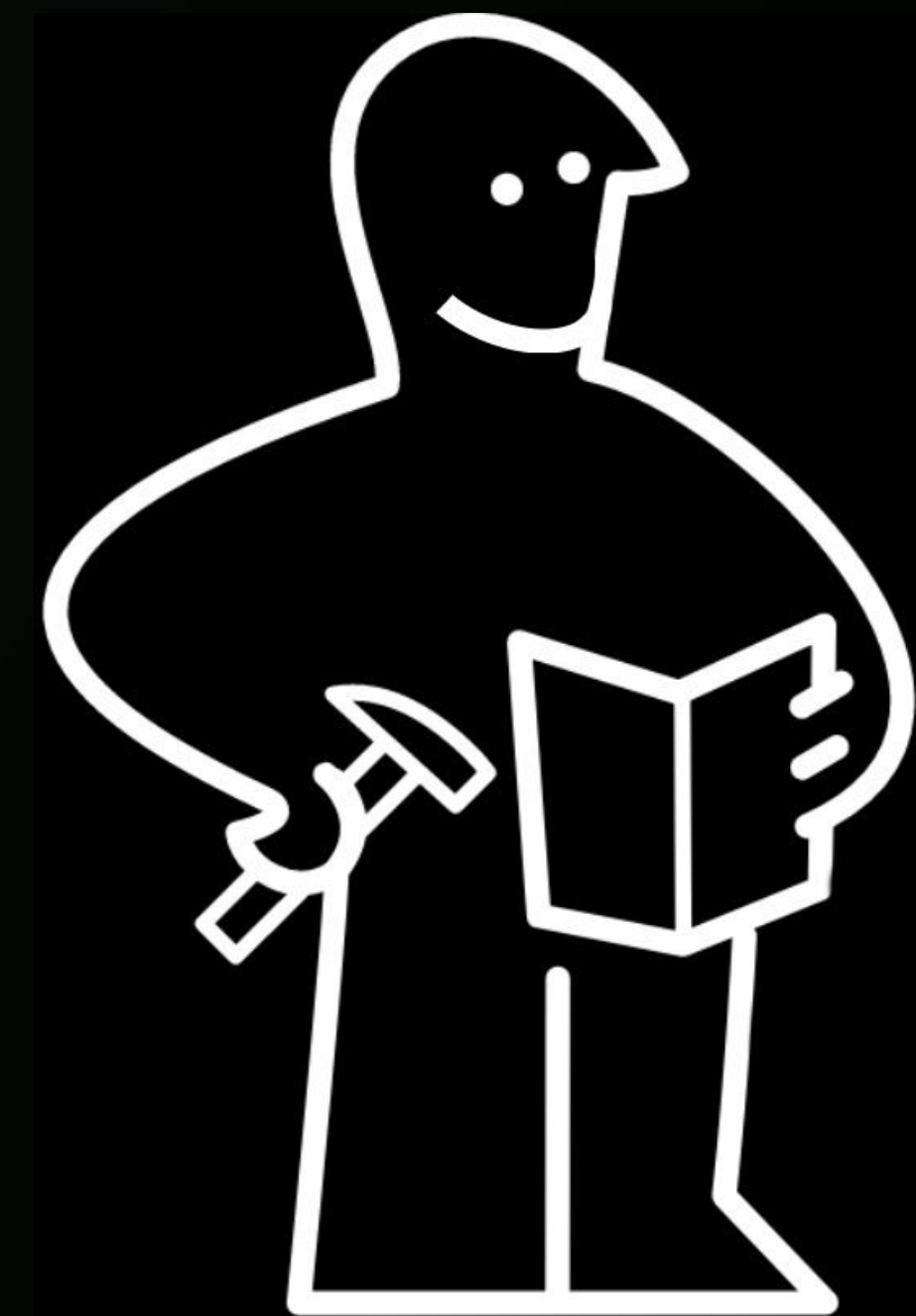
- Structure to classify security demands

$$SL = \begin{bmatrix} \textit{Authenticity} \\ \textit{Integrity} \\ \textit{Non - Repudiation} \\ \textit{Confidentiality} \\ \textit{Availability} \\ \textit{Authorisation} \end{bmatrix} = \begin{bmatrix} 0 & \dots & 4 \\ 0 & \dots & 4 \\ 0 & \dots & 4 \\ 0 & \dots & 4 \\ 0 & \dots & 4 \\ 0 & \dots & 4 \end{bmatrix}$$

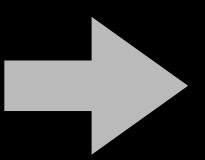
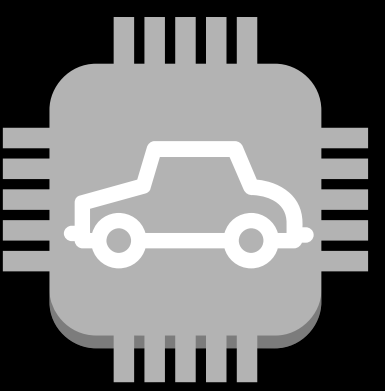
WHAT



SECURITY MECHANISMS
ARE NECESSARY
TO BE
IMPLEMENTED?

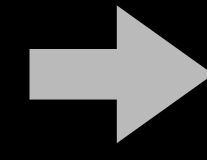


MAPPING TO SECURITY MECHANISMS



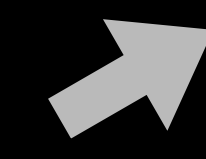
TARA

Item	Threat	Knowledge	...
Braking	Spoofing	Standard	...
Braking	Tampering	Restricted	...
Speed	Spoofing	Standard	...
...	...	...	...



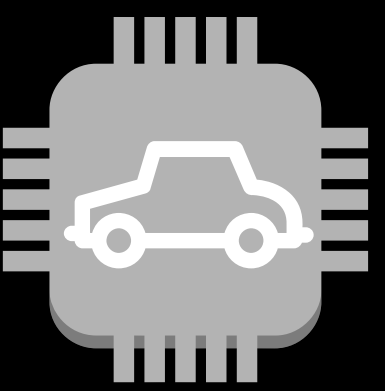
Classification

-
low
medium
high
critical



Selection of security mechanisms				
	SL 1	SL 2	SL 3	SL 4
Authenticity				
Message auth.			•	•
Firmware auth.	•	•	•	•
Hardware auth.				•

MAPPING TO SECURITY MECHANISMS



TARA

Item	Threat	Knowledge	...
Braking	Spoofing	Standard	...
Braking	Tampering	Restricted	...
Speed	Spoofing	Standard	...
...	...	...	...

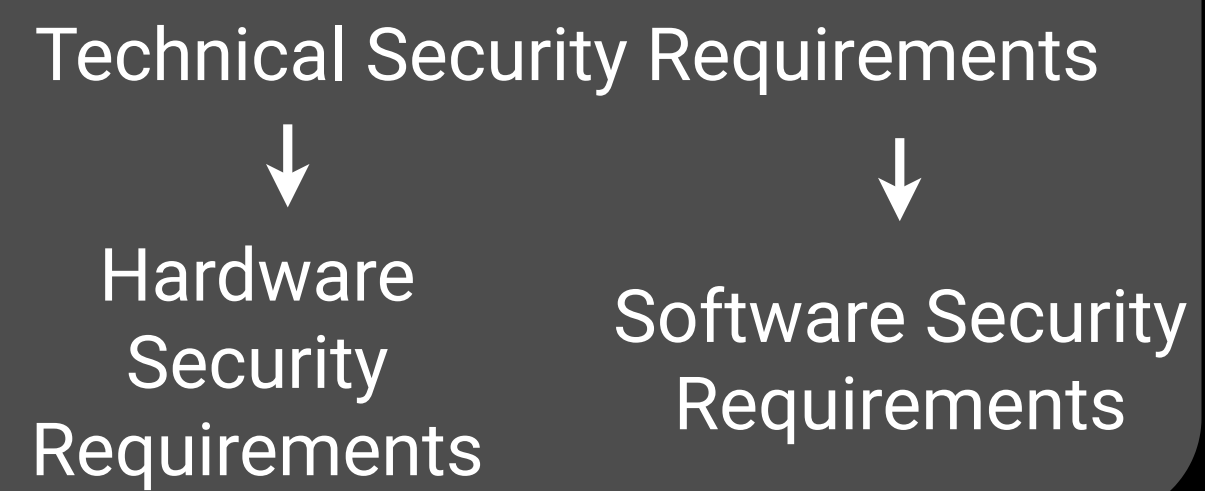
Classification

-
low
medium
high
critical

Selection of security mechanisms

	SL 1	SL 2	SL 3	SL 4
Authenticity				
Message auth.			•	•
Firmware auth.	•	•	•	•
Hardware auth.				•

Derive specific requirements



IDENTIFIED SECURITY MECHANISMS

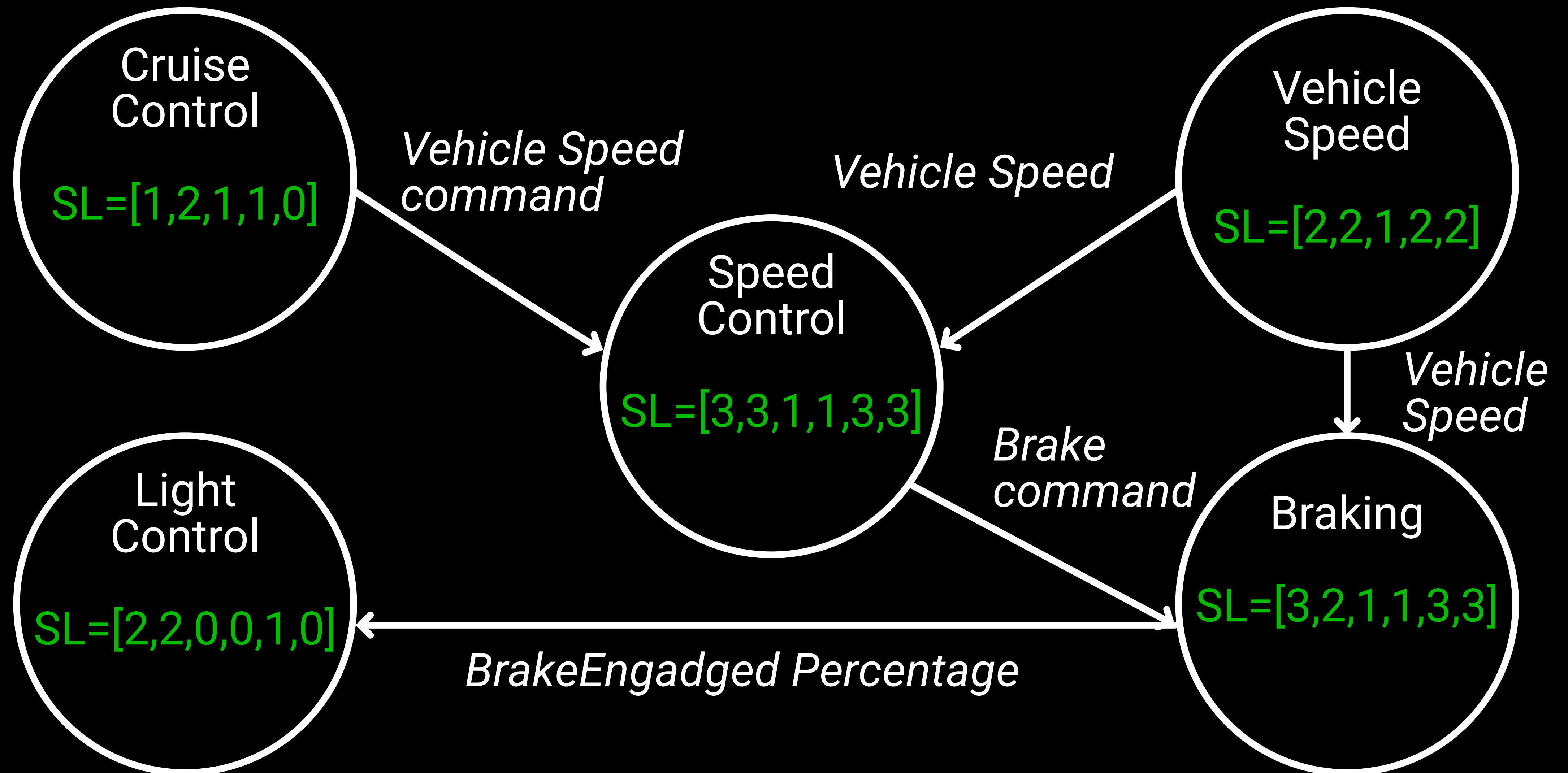
		SL 0	SL 1	SL 2	SL 3	SL 4
Integrity	IN.1 [MSG] Message Authentication Code (MAC) with pre-shared key			•	•	•
	IN.2 [FW] Verify cryptographic hash of firmware when upgrading		•	•	•	•
	IN.3 [FW] Verify cryptographic hash of firmware/functions on boot				•	•
	IN.4 [HW] Physical protection against tampering				•	•
	IN.5 [HW] Detection of physical tampering		•	•	•	•
Authenticity	AU.1 [MSG] Message Authentication Code (MAC) with session key				•	•
	AU.2 [FW] Verify authenticity of firmware when upgrading using digital signatures ^a		1	1	2	2
	AU.3 [FW] Verify authenticity of firmware/functions on boot using digital signatures ^a				1	2
	AU.4 [HW] Verify hardware authenticity					•
Non-repudiation	NR.1 [MSG] Freshness using counter or timestamp in authenticated message				•	•
	NR.2 [MSG] Audit logging				•	•
	NR.3 [MSG] Use of digital signatures for messages (signals)					•
Confidentiality	CO.1 [MSG] Encryption of messages				•	•
	CO.2 [FW] Encryption of firmware during transmission ^a				1	2
Availability	AV.1 [MSG] Limited network access – Quality of Service				•	•
	AV.2 [FW] Watchdog timer			•	•	•
Authorization and Access Control	AC.1 [MSG] Whitelisting of messages (signals) on gateways		•	•	•	•
	AC.2 [MSG] Whitelisting of messages (signals) on nodes				•	•
	AC.3 [MSG] Access control on function level				•	•
	AC.4 [MSG] Deployment of Intrusion Detection Systems				•	•
	AC.5 [MSG, FW, HW] Logical separation ^a			1	1	2
	AC.6 [MSG, FW, HW] Domain isolation				•	•
Other requirements ^b	OR.1 Fail in known state					
	OR.2 Information Input Validation					
	OR.3 Operate with least set of privileges that are necessary					
	OR.4 Compliance to secure coding guidelines					
	OR.5 Secure Logging					



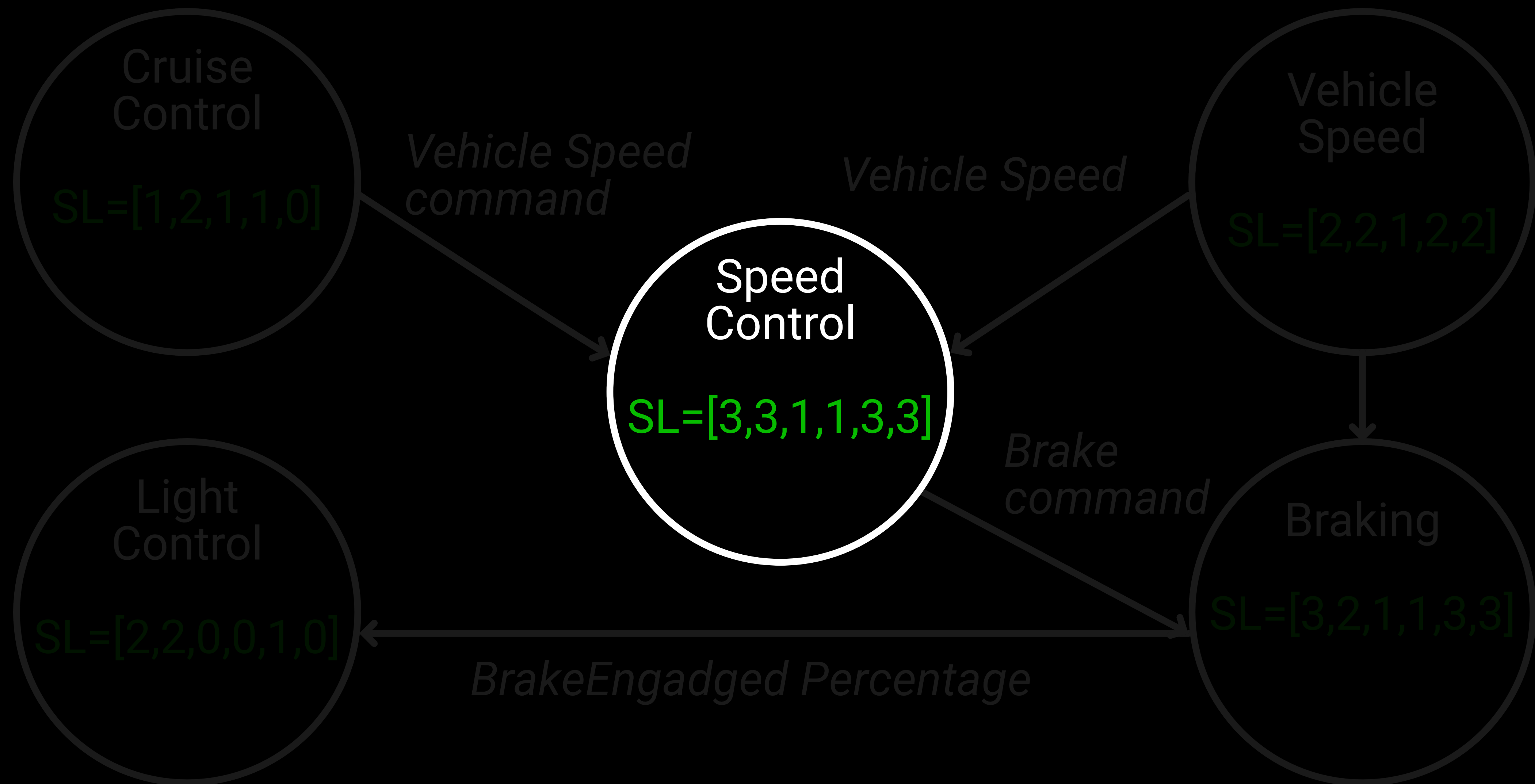
EXAMPLE: AUTHORISATION

	SL 1	SL 2	SL 3	SL 4
AC.1 Whitelisting of messages on gateways	•	•	•	•
AC.2 Whitelisting of messages on nodes			•	•
AC.3 Access control on function level			•	•
AC.4 Deployment of Intrusion Detection Systems			•	•
AC.5 Logical separation		1	1	2
AC.6 Domain isolation			•	•

USE CASE: CRUISE CONTROL



APPLYING THE MAPPING



APPLYING THE MAPPING

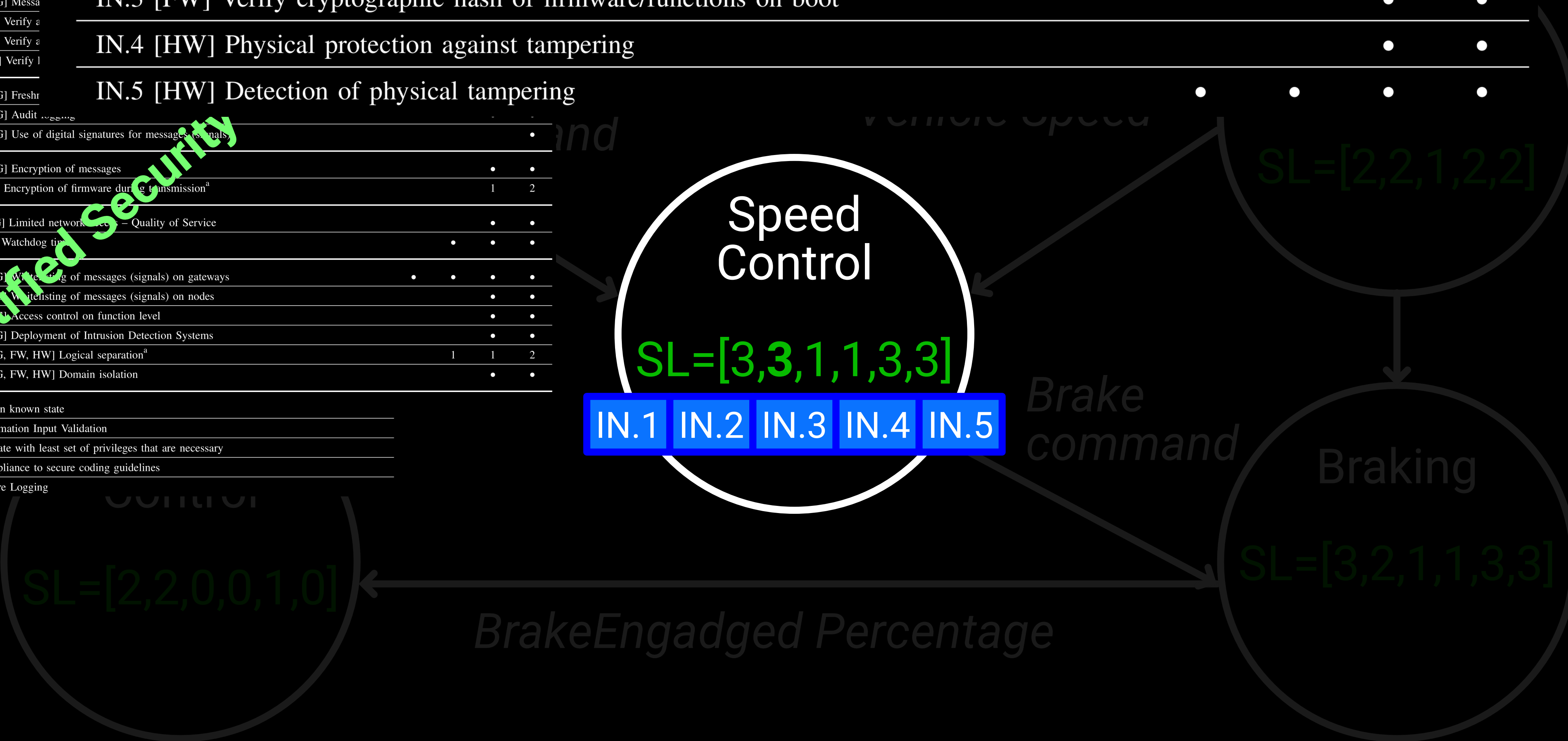
		SL 0	SL 1	SL 2	SL 3	SL 4
Integrity	IN.1 [MSG] Message Authentication Code (MAC) with pre-shared key			•	•	•
	IN.2 [FW] Verify cryptographic hash of firmware when upgrading		•	•	•	•
	IN.3 [FW] Verify cryptographic hash of firmware/functions on boot				•	•
	IN.4 [HW] Physical protection against tampering				•	•
	IN.5 [HW] Detection of physical tampering			•	•	•
Authenticity	AU.1 [MSG] Message Authentication Code (MAC) with session key				•	•
	AU.2 [FW] Verify authenticity of firmware when upgrading using digital signatures		1	1	2	2
	AU.3 [FW] Verify authenticity of firmware/functions on boot using digital signatures				1	2
	AU.4 [HW] Verify hardware authenticity					•
Non-repudiation	NR.1 [MSG] Freshness using counter or timestamp in authentication message				•	•
	NR.2 [MSG] Audit logging				•	•
	NR.3 [MSG] Use of digital signatures for messages (signals)					•
Confidentiality	CO.1 [MSG] Encryption of messages				•	•
	CO.2 [FW] Encryption of firmware during transmission ^a				1	2
Availability	AV.1 [MSG] Limited network access – Quality of Service				•	•
	AV.2 [FW] Watchdog timer			•	•	•
Authorization and Access Control	AC.1 [MSG] Whitelisting of messages (signals) on gateways		•	•	•	•
	AC.2 [MSG] Whitelisting of messages (signals) on nodes				•	•
	AC.3 [MSG] Access control on function level				•	•
	AC.4 [MSG] Deployment of Intrusion Detection Systems				•	•
	AC.5 [MSG, FW, HW] Logical separation ^a			1	1	2
	AC.6 [MSG, FW, HW] Domain isolation				•	•
Other requirements ^b	OR.1 Fail in known state					
	OR.2 Information Input Validation					
	OR.3 Operate with least set of privileges that are necessary					
	OR.4 Compliance to secure coding guidelines					
	OR.5 Secure Logging					



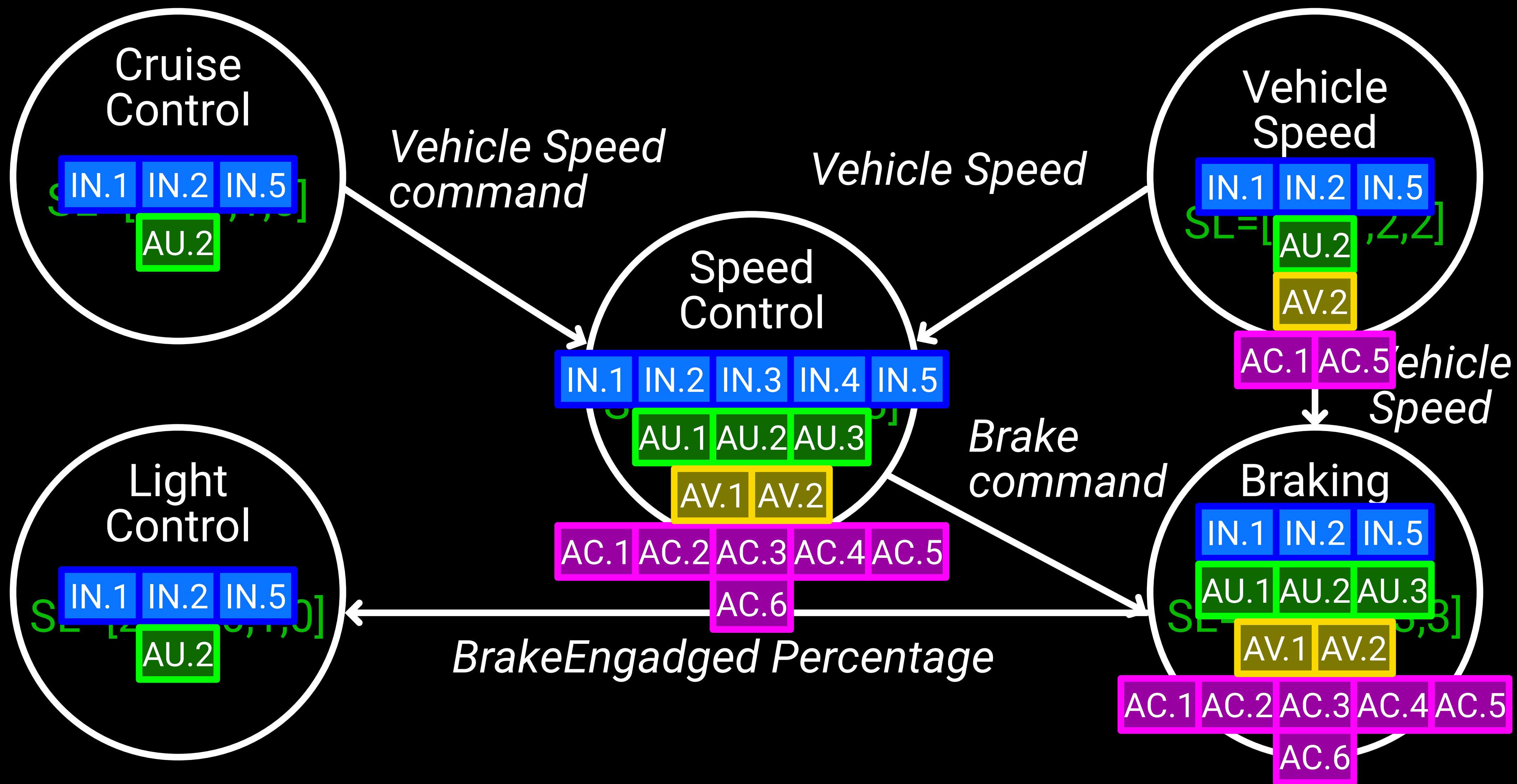
APPLYING THE MAPPING

			SL 0	SL 1	SL 2	SL 3	SL 4
Integrity	IN.1 [MSG] Message Authentication Code (MAC) with pre-shared key				•	•	•
	IN.2 [FW] Verify cryptographic hash of firmware when upgrading			•	•	•	•
	IN.3 [FW] Verify cryptographic hash of firmware/functions on boot					•	•
	IN.4 [HW] Physical protection against tampering					•	•
	IN.5 [HW] Detection of physical tampering		•	•	•	•	•
Authenticity	AU.1 [MSG] Message Authentication Code (MAC) with pre-shared key						
Non-repudiation	NR.1 [MSG] Freshness						
	NR.2 [MSG] Audit logs						
	NR.3 [MSG] Use of digital signatures for messages (signals)						
Confidentiality	CO.1 [MSG] Encryption of messages	•	•				
	CO.2 [FW] Encryption of firmware during transmission ^a	1	2				
Availability	AV.1 [MSG] Limited network access – Quality of Service	•	•				
	AV.2 [FW] Watchdog timer	•	•	•			
Authorization and Access Control	AC.1 [MSG] Whitelisting of messages (signals) on gateways	•	•	•	•		
	AC.2 [MSG] Whitelisting of messages (signals) on nodes			•	•		
	AC.3 [MSG] Access control on function level			•	•		
	AC.4 [MSG] Deployment of Intrusion Detection Systems			•	•		
	AC.5 [MSG, FW, HW] Logical separation ^a	1	1	2			
	AC.6 [MSG, FW, HW] Domain isolation		•	•			
Other requirements ^b	OR.1 Fail in known state						
	OR.2 Information Input Validation						
	OR.3 Operate with least set of privileges that are necessary						
	OR.4 Compliance to secure coding guidelines						
	OR.5 Secure Logging						

Identified security



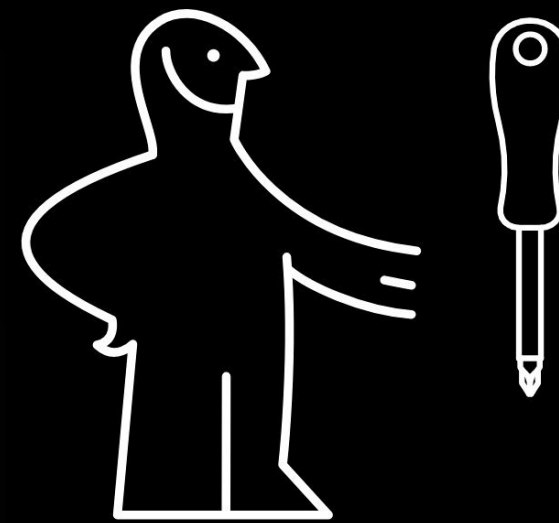
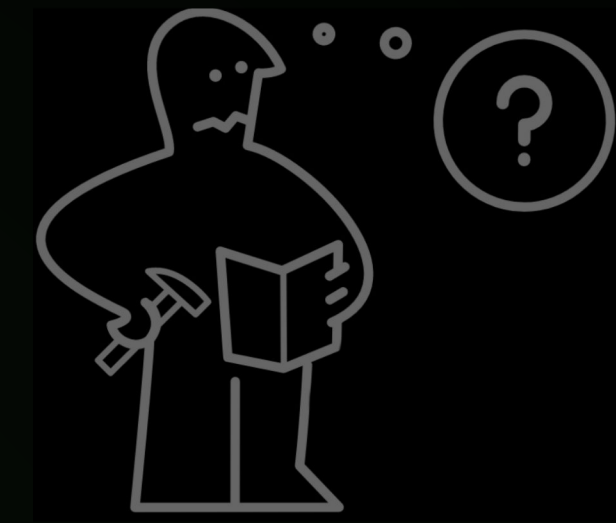
USE CASE: CRUISE CONTROL



ADVANTAGES

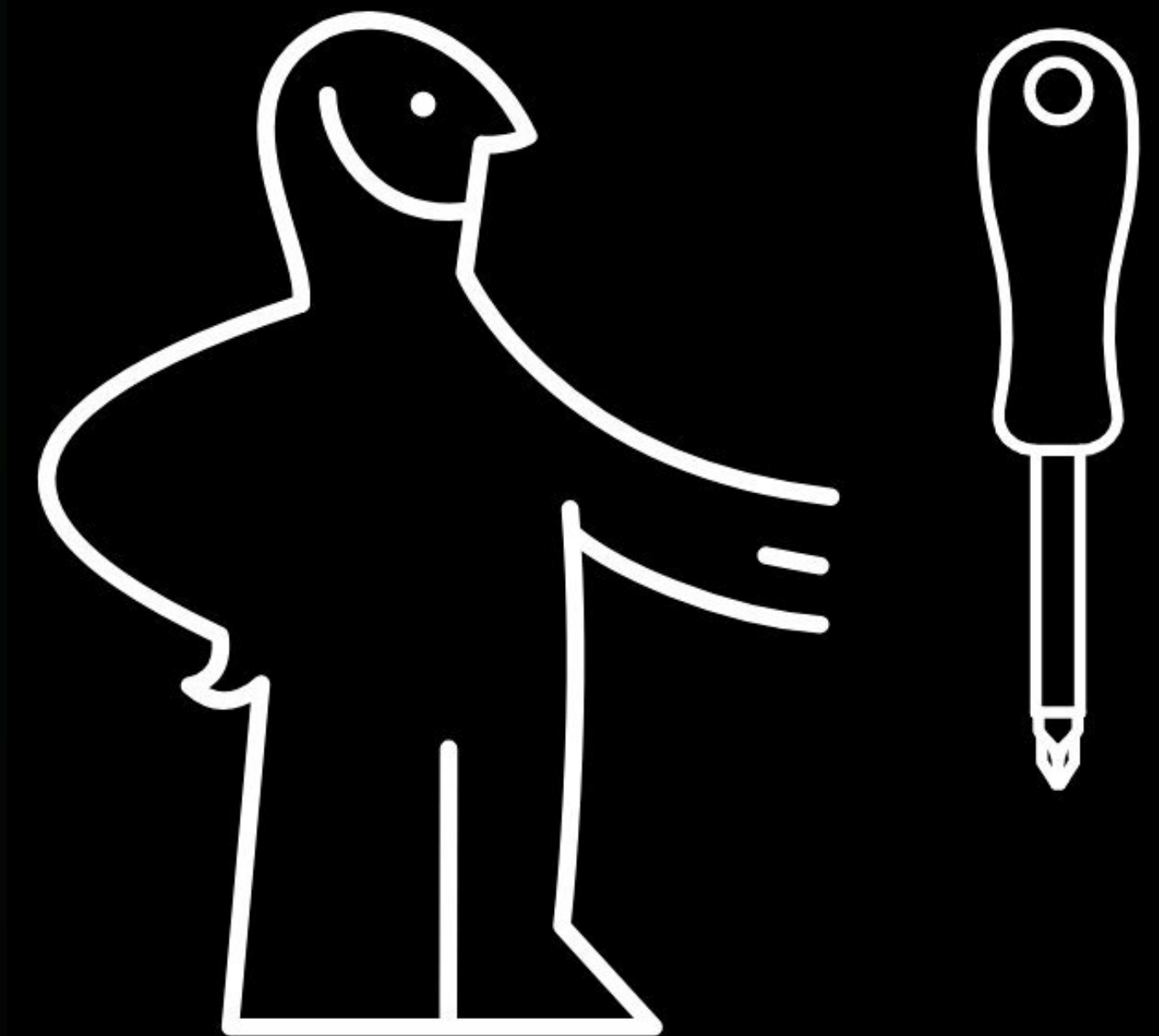
- ▶ Strict rule-set to fulfil basic security requirements
- ▶ Better understanding of the required mechanisms between different parties
- ▶ See dependencies between safety and security in an early stage

TOOL



IMPROVING AUTOSAR SecOC PROFILE 3

TO BE IMPLEMENTED?



AUTHENTIC MESSAGES IN CAN

- ▶ Developed 1983
- ▶ Restrictions on CAN bus
 - ▷ Highly limited bandwidth
 - ▷ Max. 64 bits payload
 - ▷ Designed without security in mind

WHY FRESHNESS?

- ▶ Prevents replays of old messages
- ▶ Implemented using
 - ▷ Counter/Freshness Value
 - ▷ Current time

WHY FRESHNESS?

- ▶ Prevents replays of old messages
- ▶ Implemented using
 - ▷ Counter/Freshness Value
 - ▷ Current time

- ▶ Truncation is required

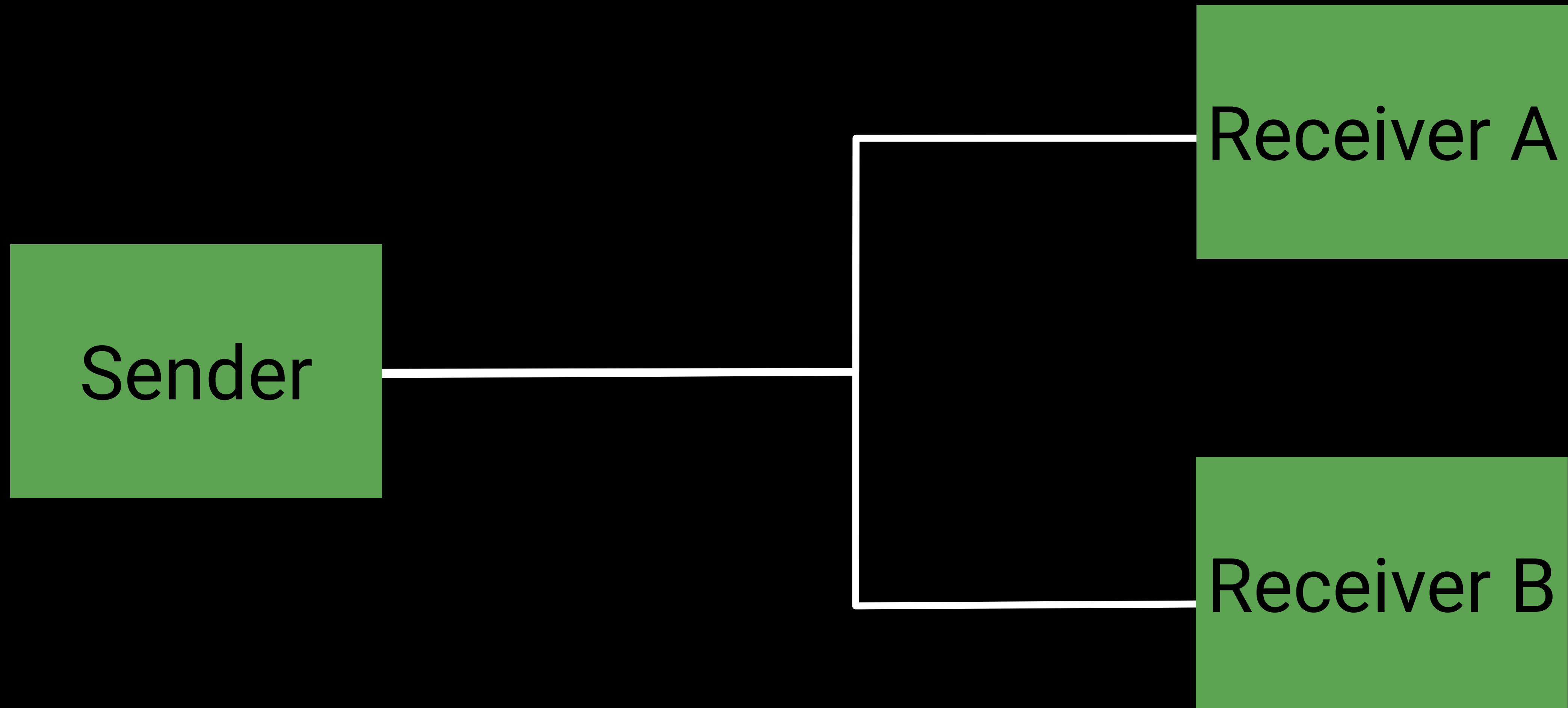
Message Authentication Code

Truncated MAC Authentication Code

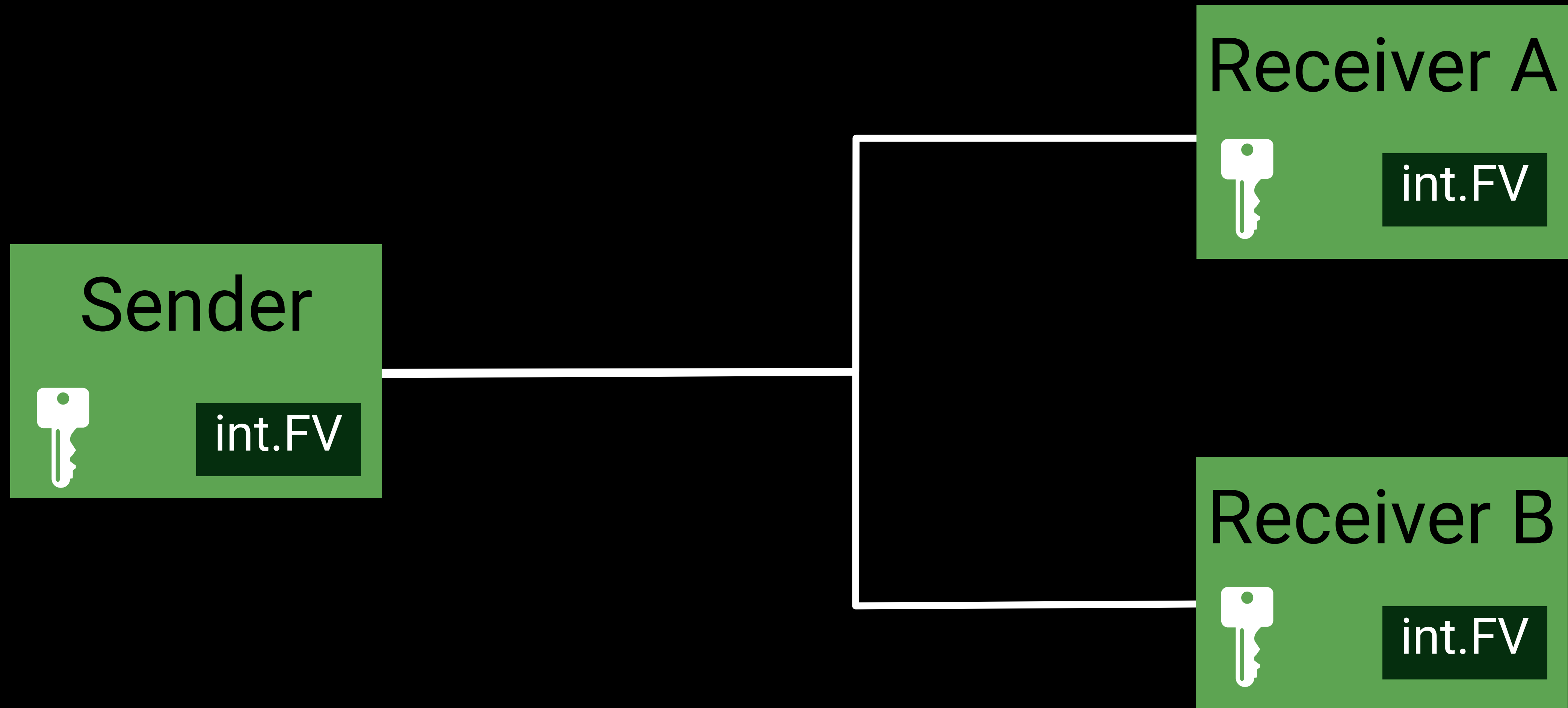
Counter/Freshness Value

Counter/Freshness Value Truncated FV

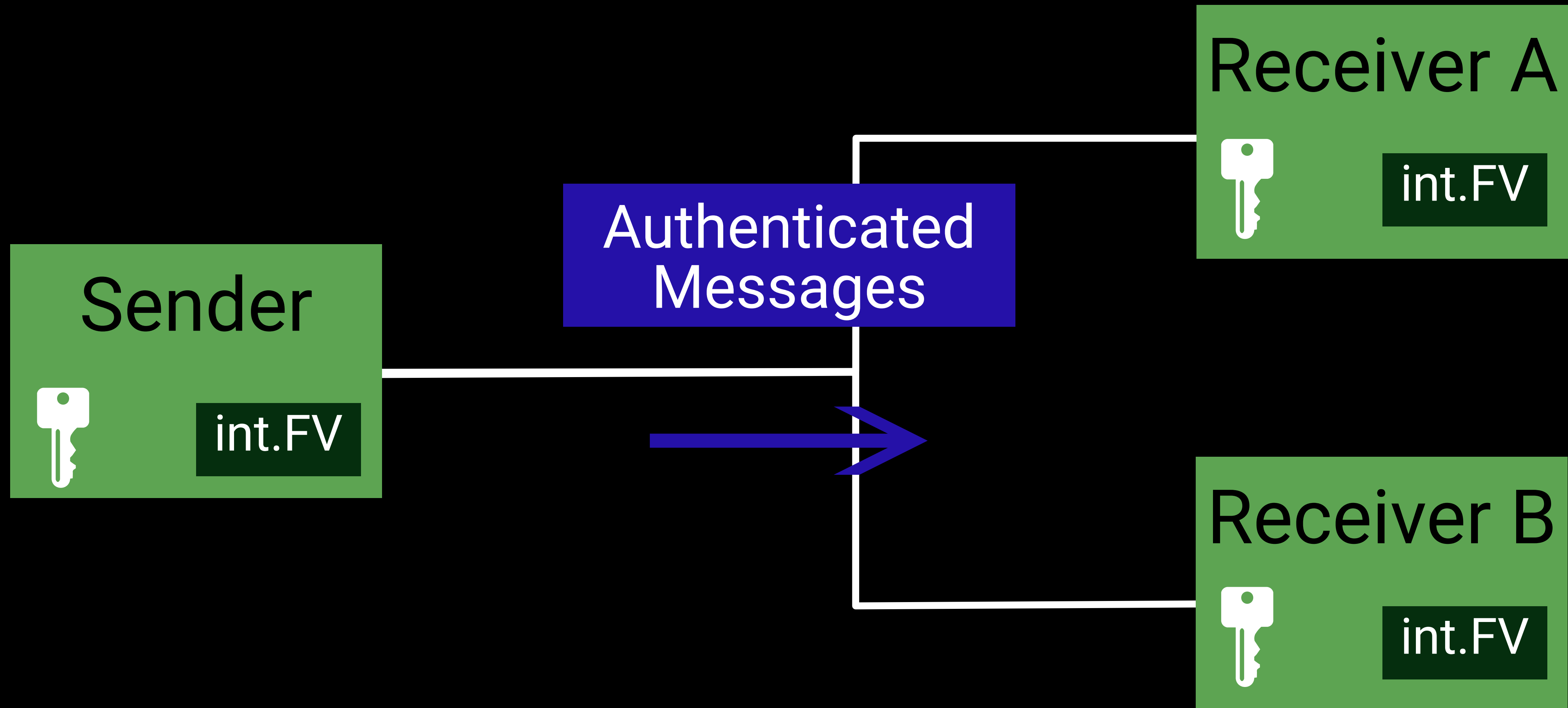
JASPAR (AUTOSAR SecOC PROFILE 3)



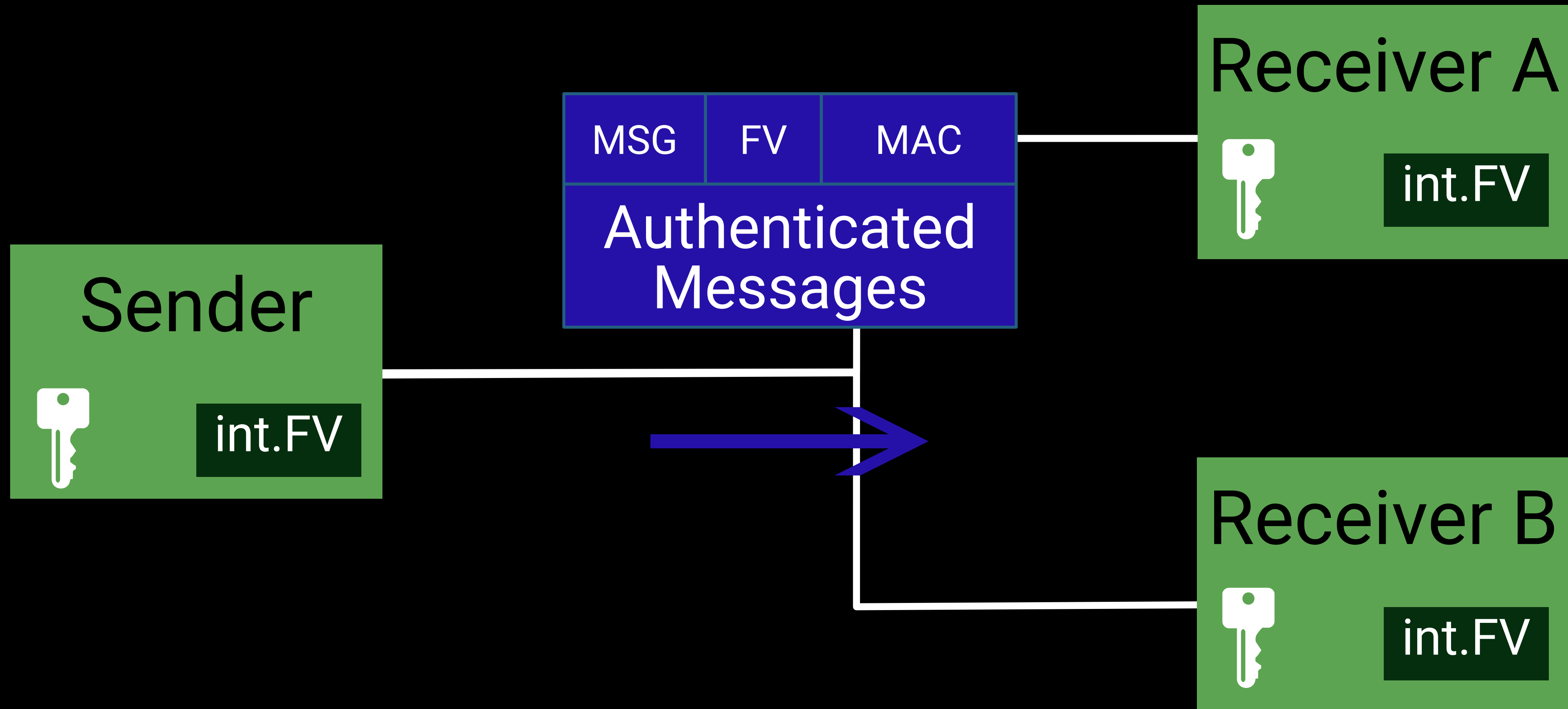
JASPAR (AUTOSAR SecOC PROFILE 3)



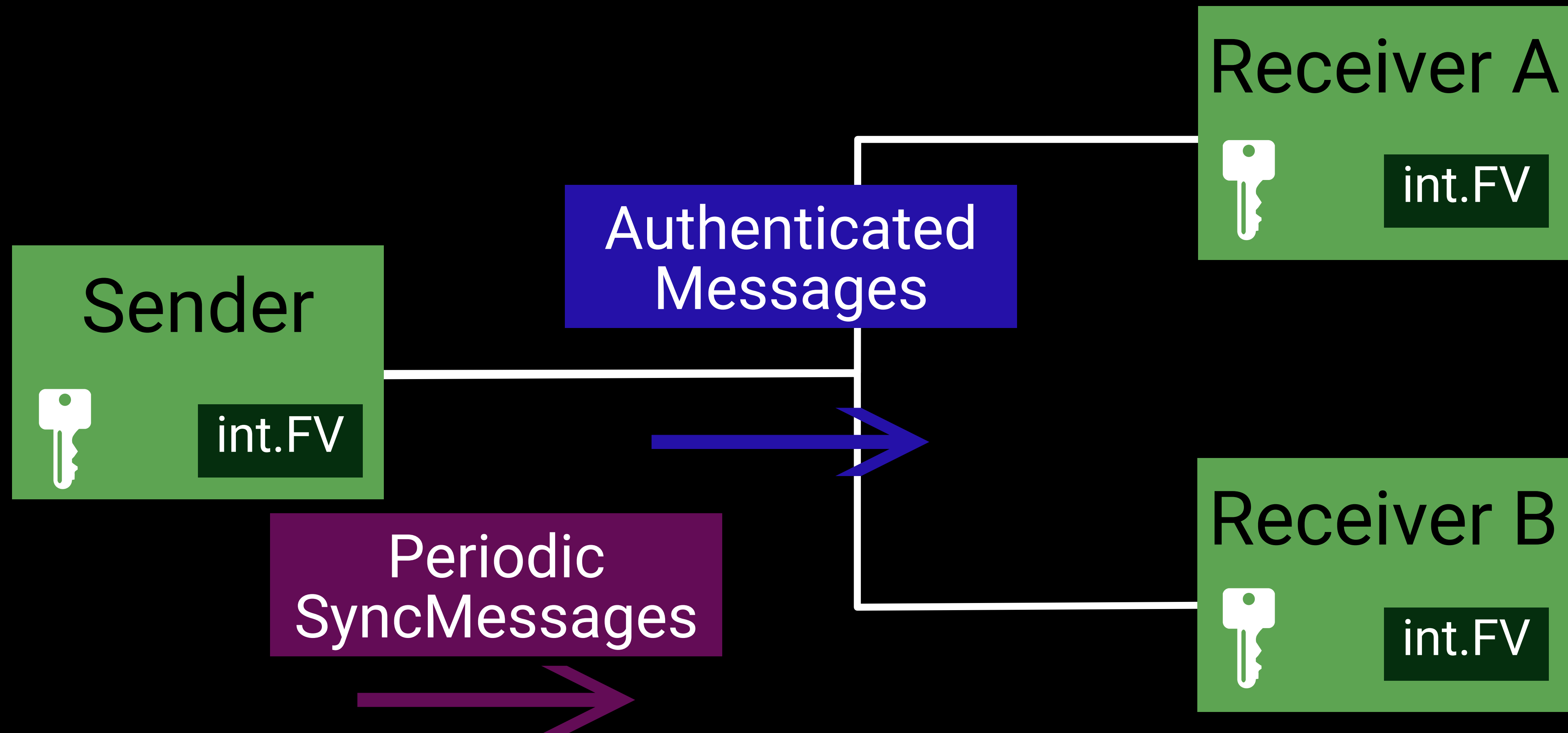
JASPAR (AUTOSAR SecOC PROFILE 3)



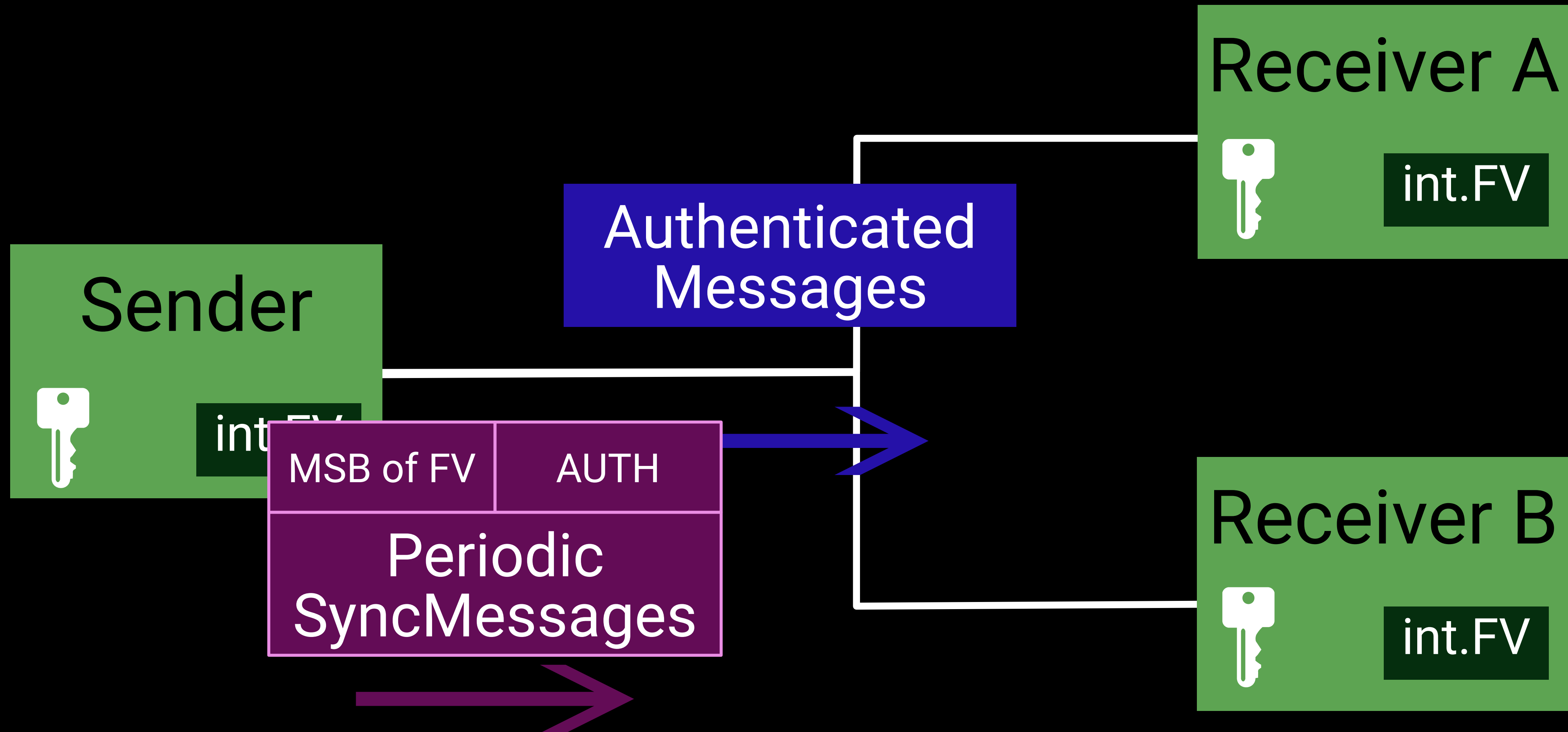
JASPAR (AUTOSAR SecOC PROFILE 3)



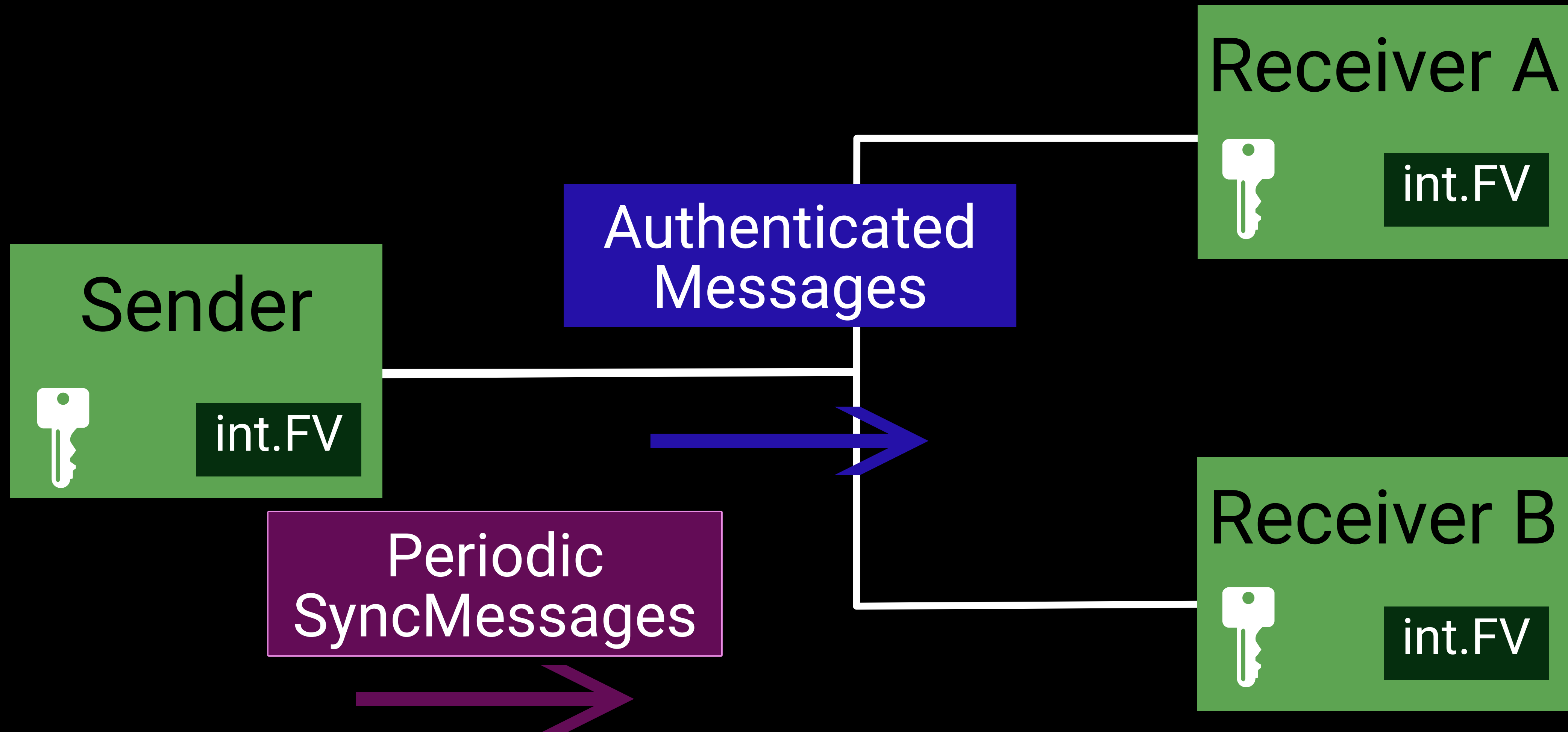
JASPAR (AUTOSAR SecOC PROFILE 3)



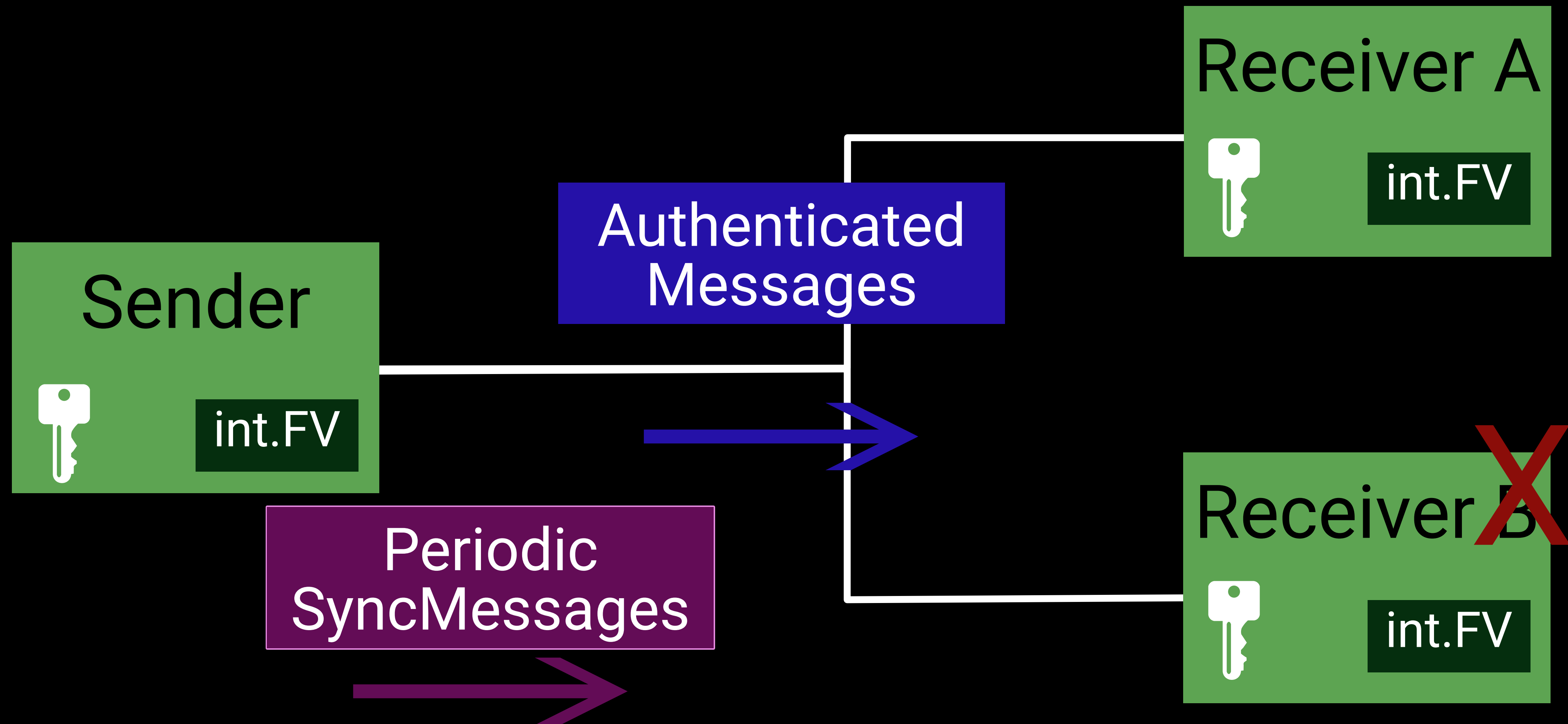
JASPAR (AUTOSAR SecOC PROFILE 3)



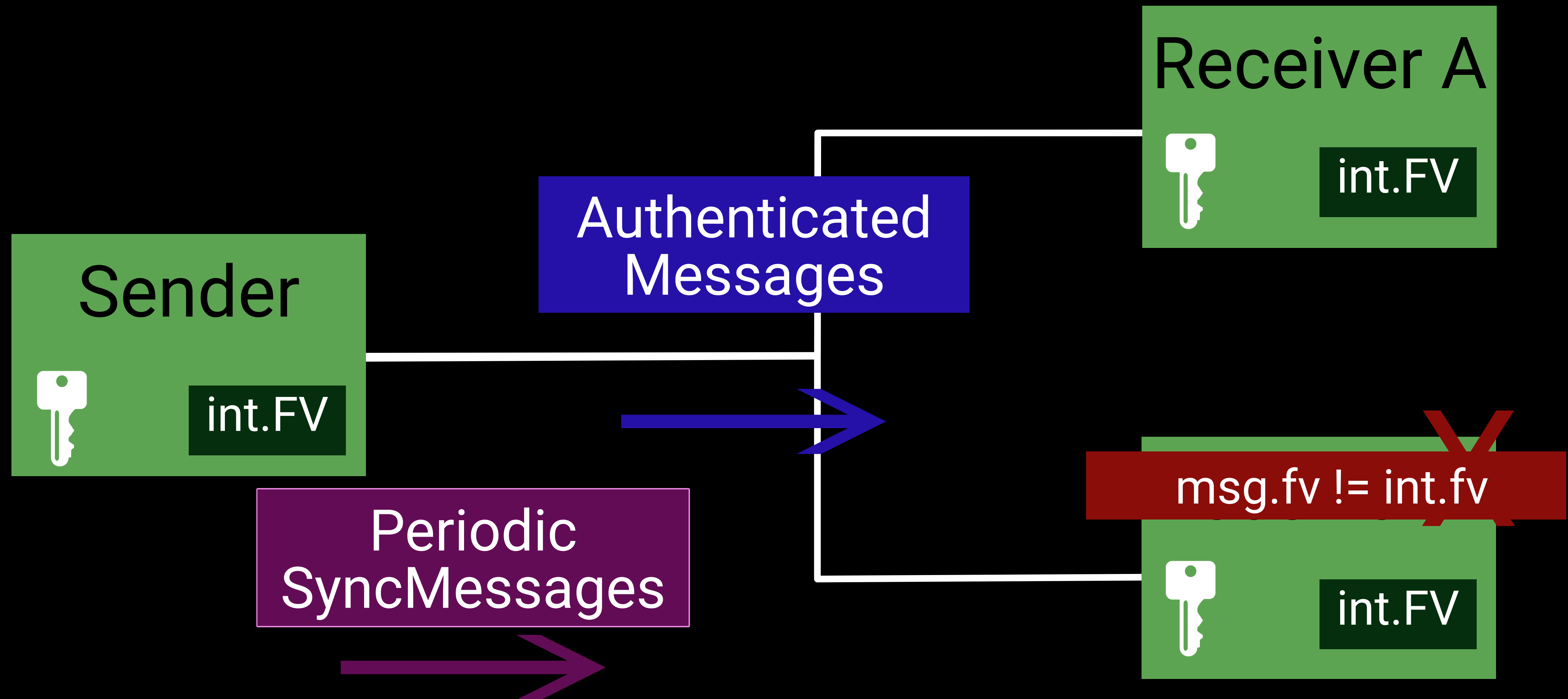
JASPAR (AUTOSAR SecOC PROFILE 3)



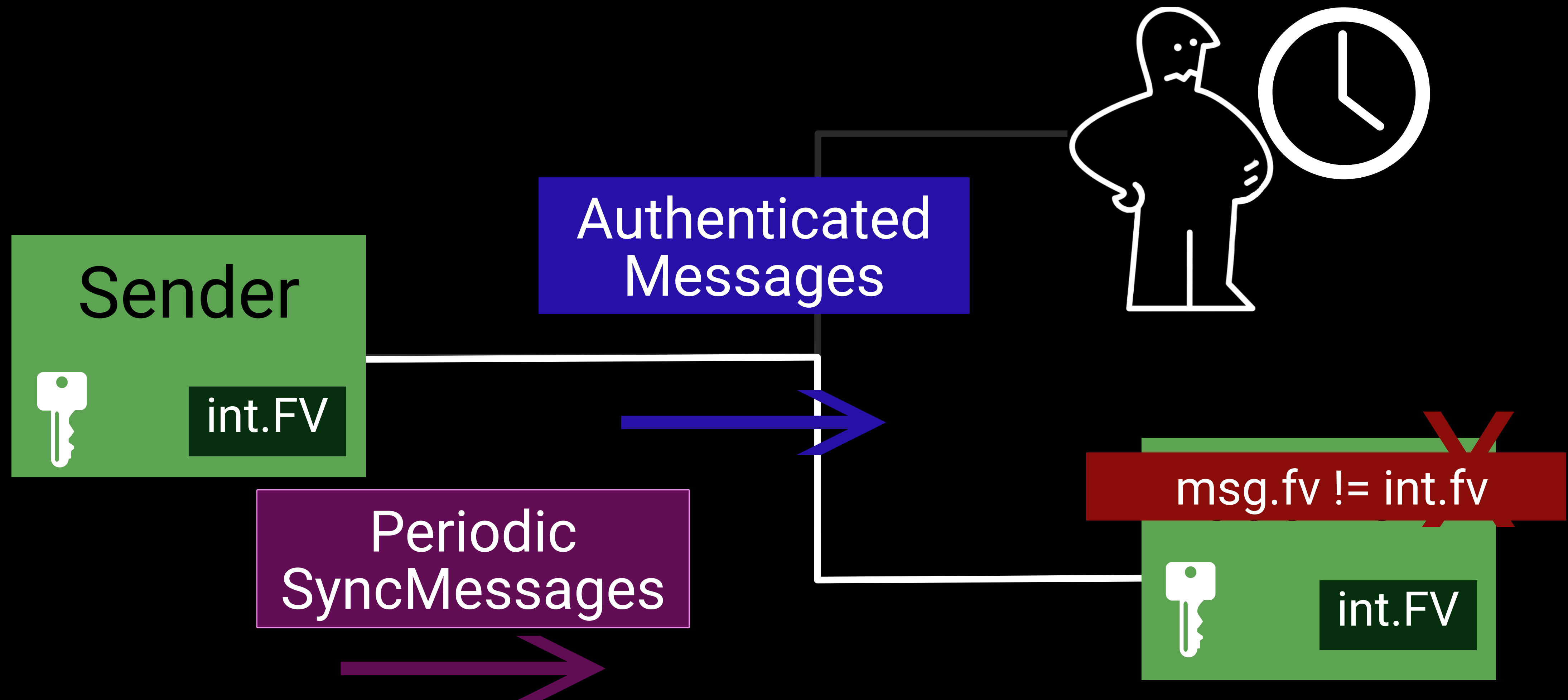
JASPAR (AUTOSAR SecOC PROFILE 3)



JASPAR (AUTOSAR SecOC PROFILE 3)



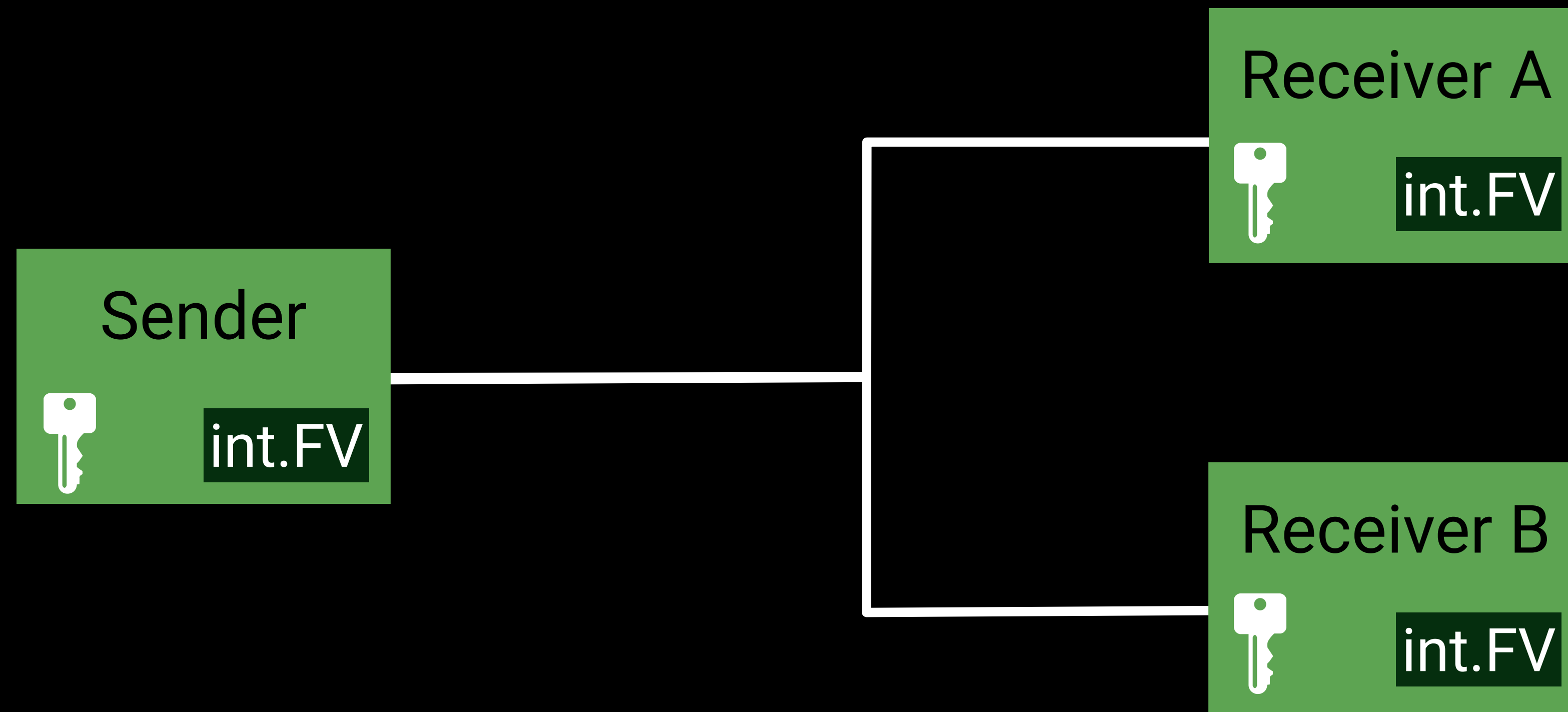
JASPAR (AUTOSAR SecOC PROFILE 3)



DESIGN CONSIDERATIONS & LIMITATIONS

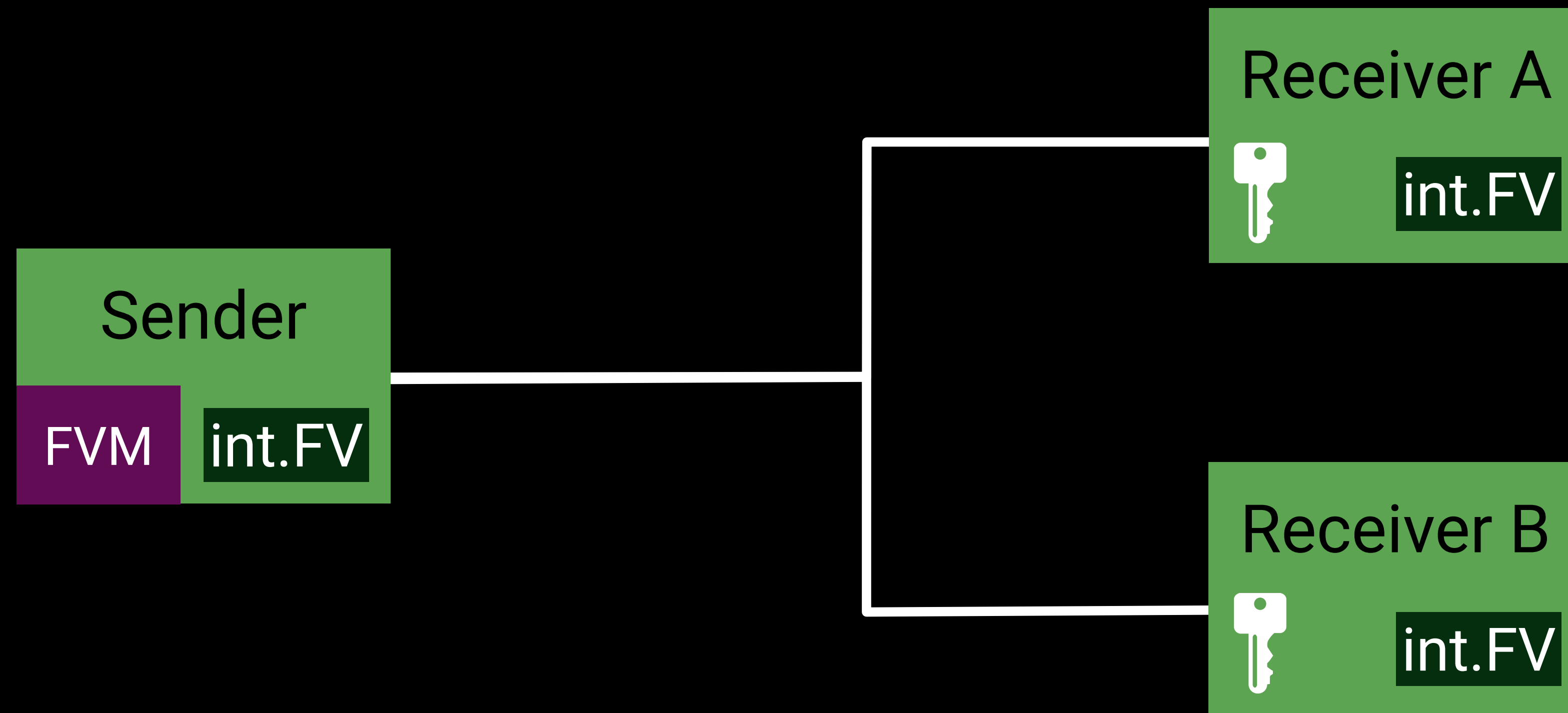
DESIGN CONSIDERATIONS & LIMITATIONS

► Placement of the Freshness Value Manager (FVM)



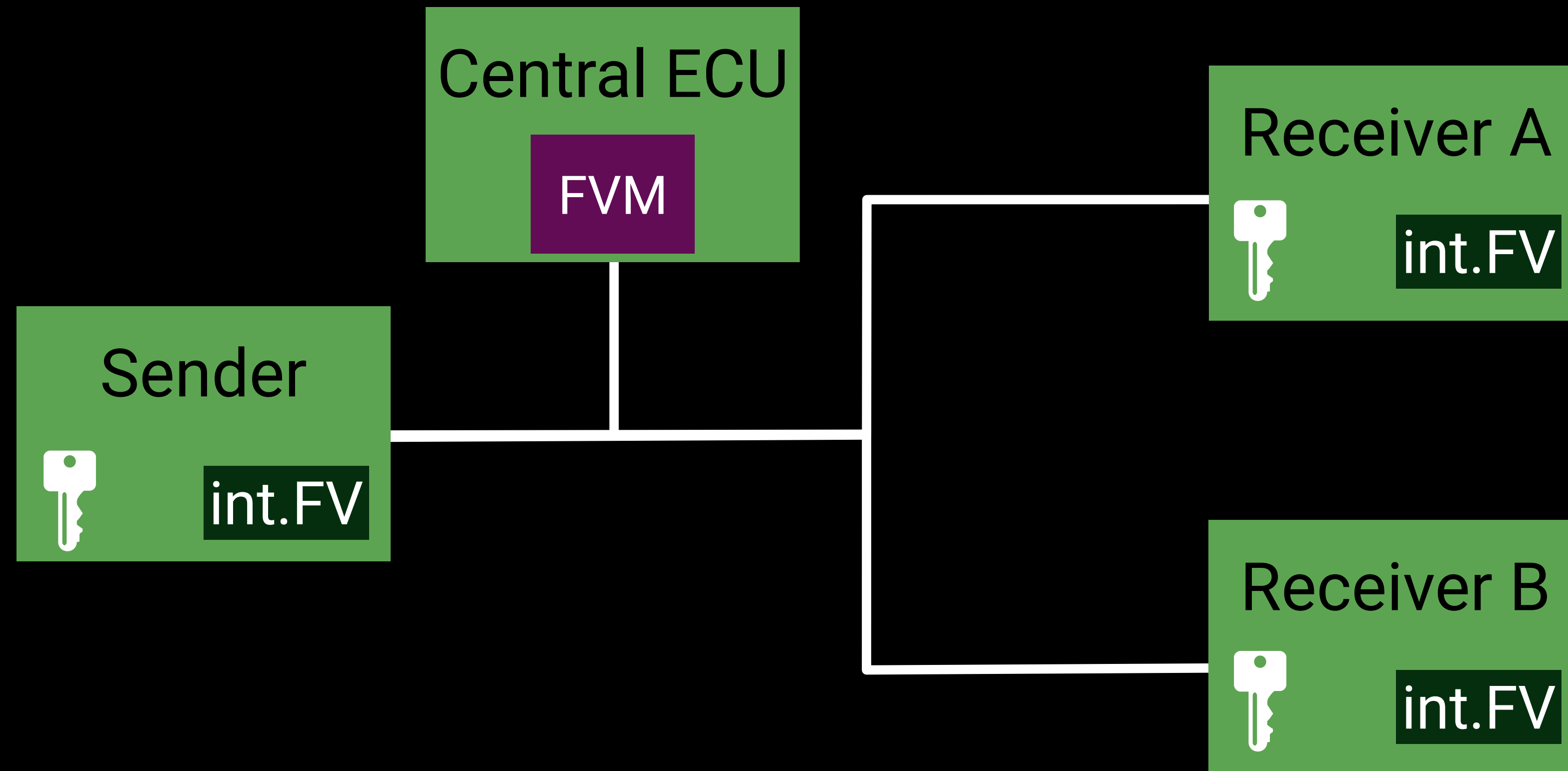
DESIGN CONSIDERATIONS & LIMITATIONS

► Placement of the Freshness Value Manager (FVM)



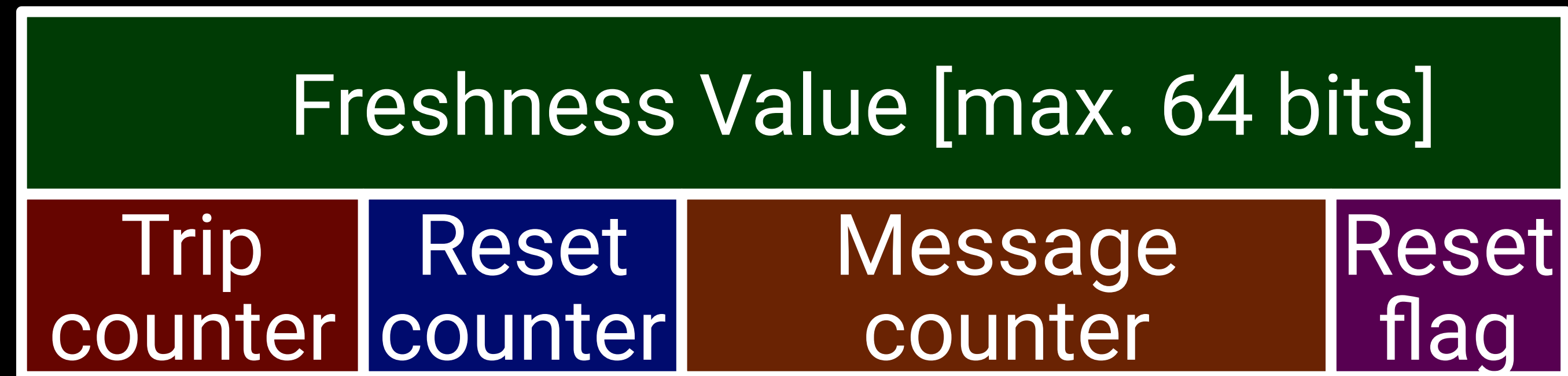
DESIGN CONSIDERATIONS & LIMITATIONS

► Placement of the Freshness Value Manager (FVM)



DESIGN CONSIDERATIONS & LIMITATIONS

- ▶ Placement of the Freshness Value Manager (FVM)
- ▶ Complex Structure of the FV



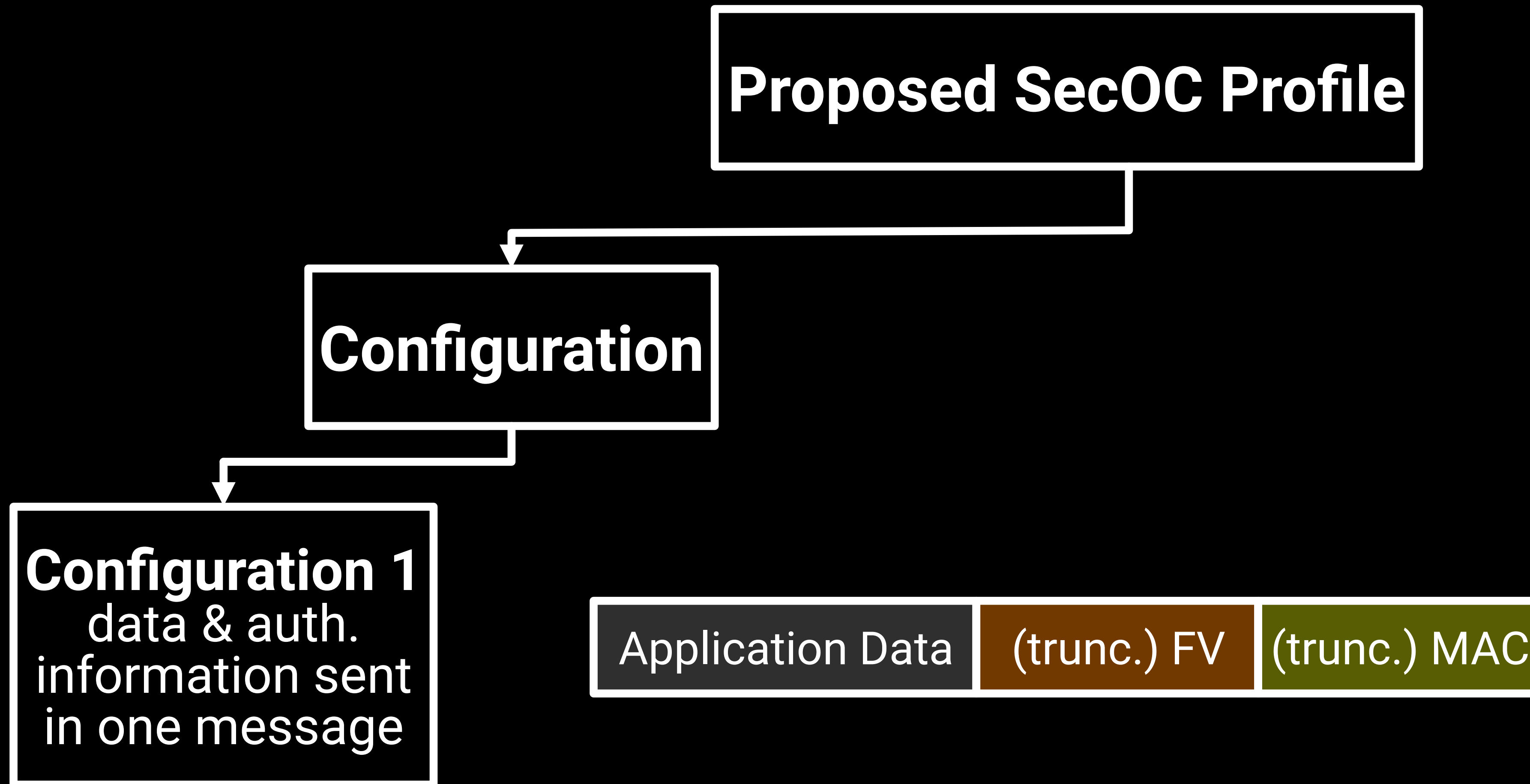
DESIGN CONSIDERATIONS & LIMITATIONS

- ▶ Placement of the Freshness Value Manager (FVM)
- ▶ Complex Structure of the FV
- ▶ Determining the Period for sending SyncMessages
 - ▷ *Safety critical functions have different requirements*
 - ▷ *One frequency does not fit all*

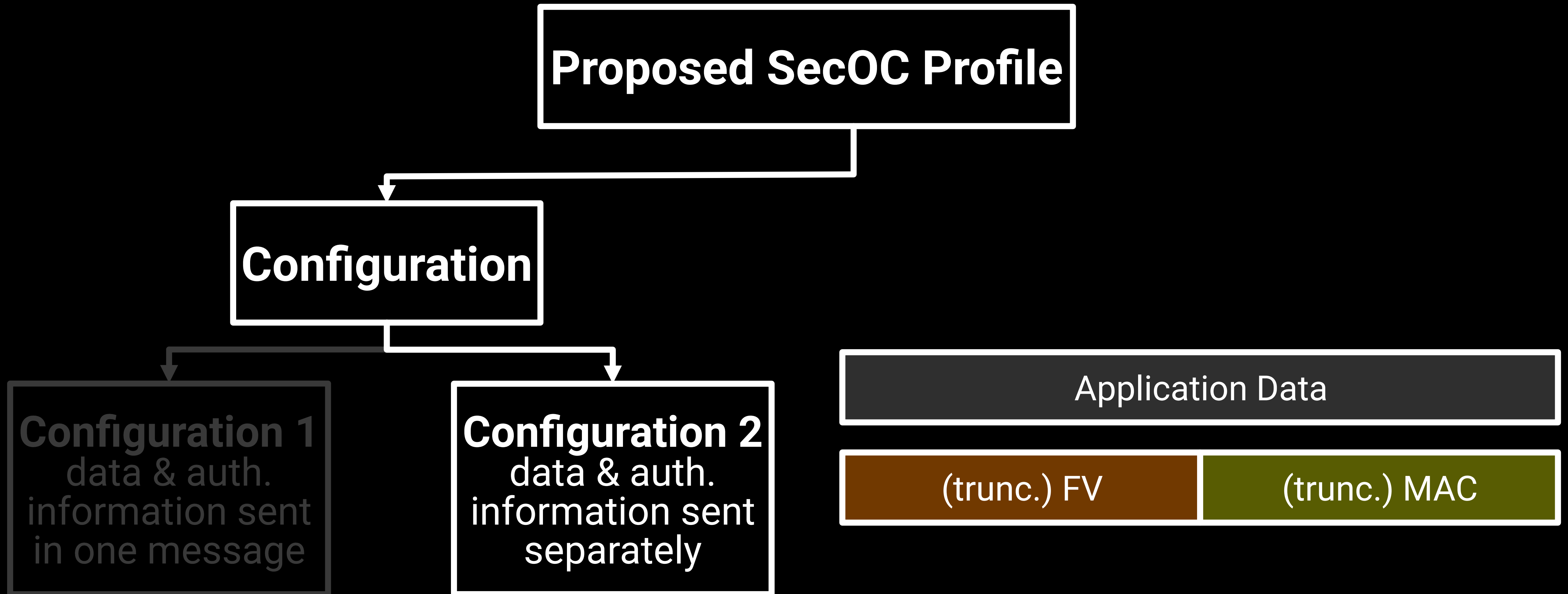
DESIGN CONSIDERATIONS & LIMITATIONS

- ▶ Placement of the Freshness Value Manager (FVM)
- ▶ Complex Structure of the FV
- ▶ Determining the Period for sending SyncMessages
- ▶ Periodicity of SyncMessages
 - ▷ *Worst case: ECU needs to wait an entire period*
 - ▷ *No way to request synchronisation*

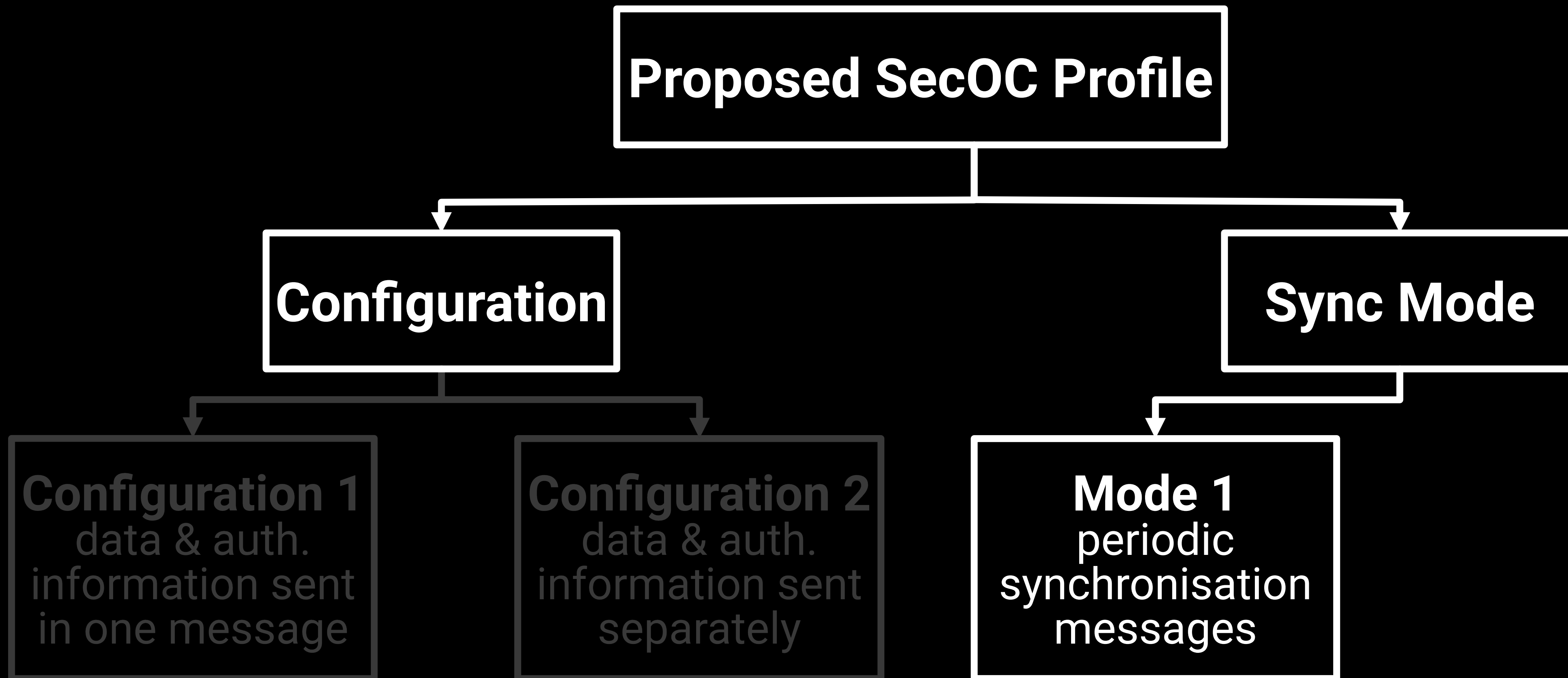
PROPOSED SecOC PROFILE



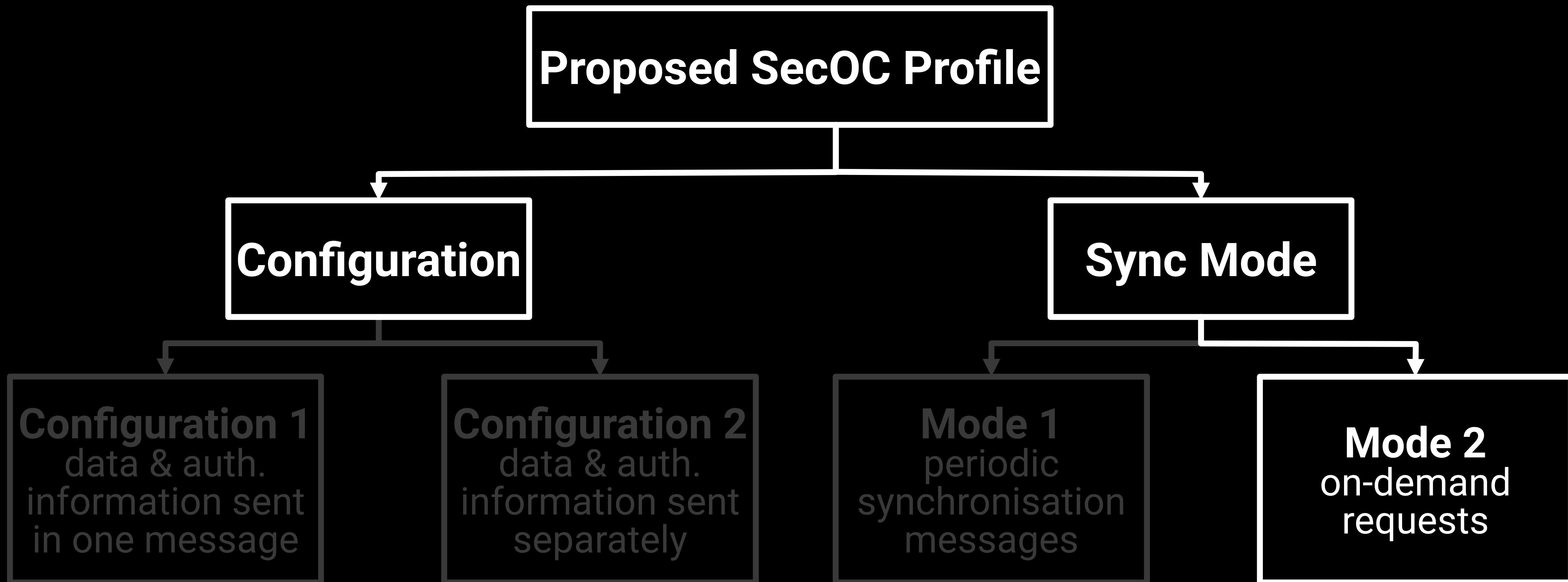
PROPOSED SecOC PROFILE



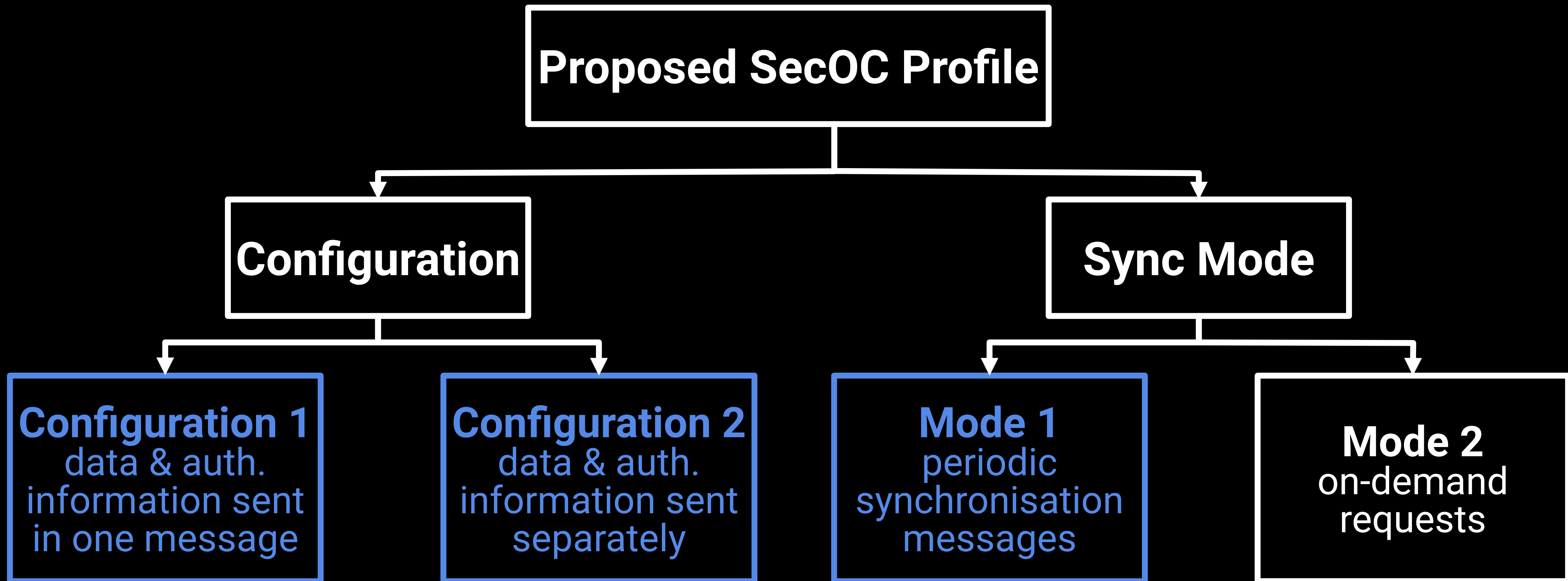
PROPOSED SecOC PROFILE



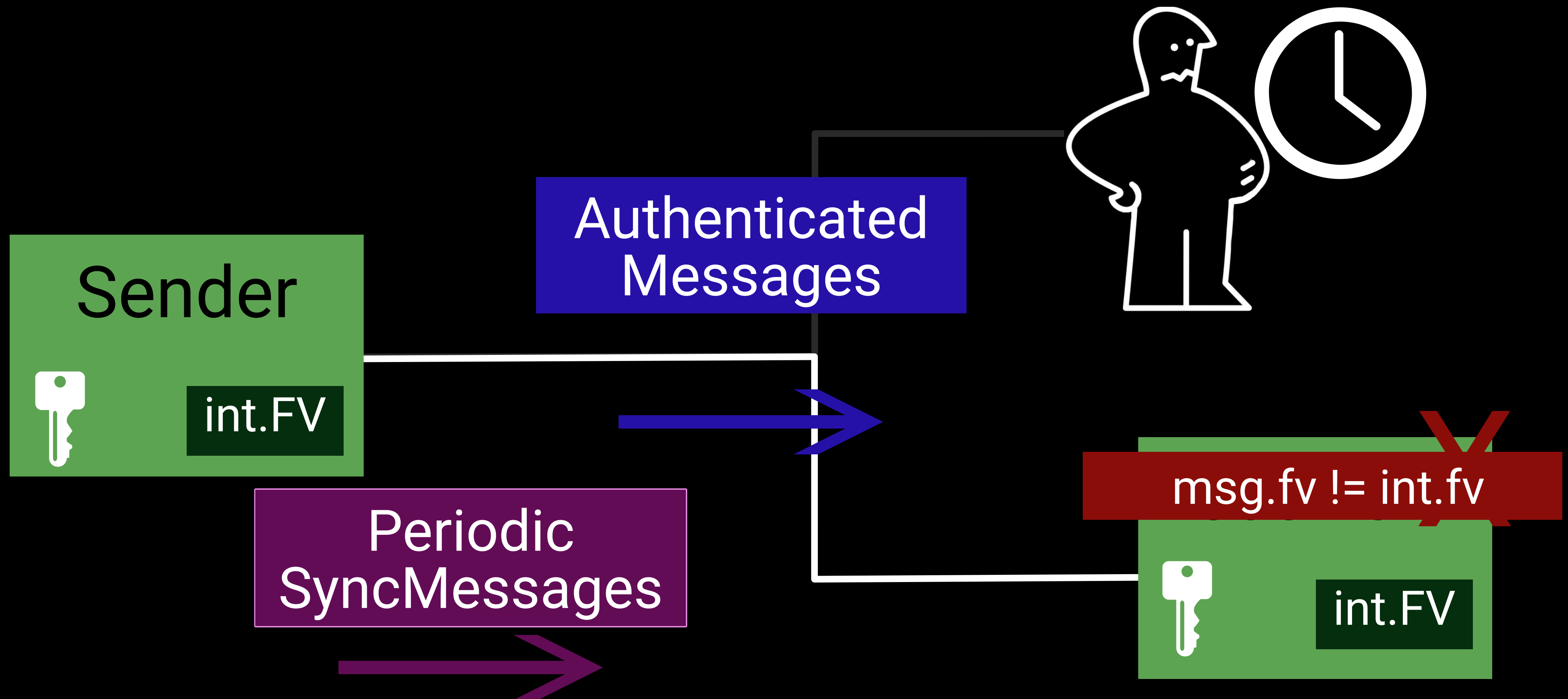
PROPOSED SecOC PROFILE



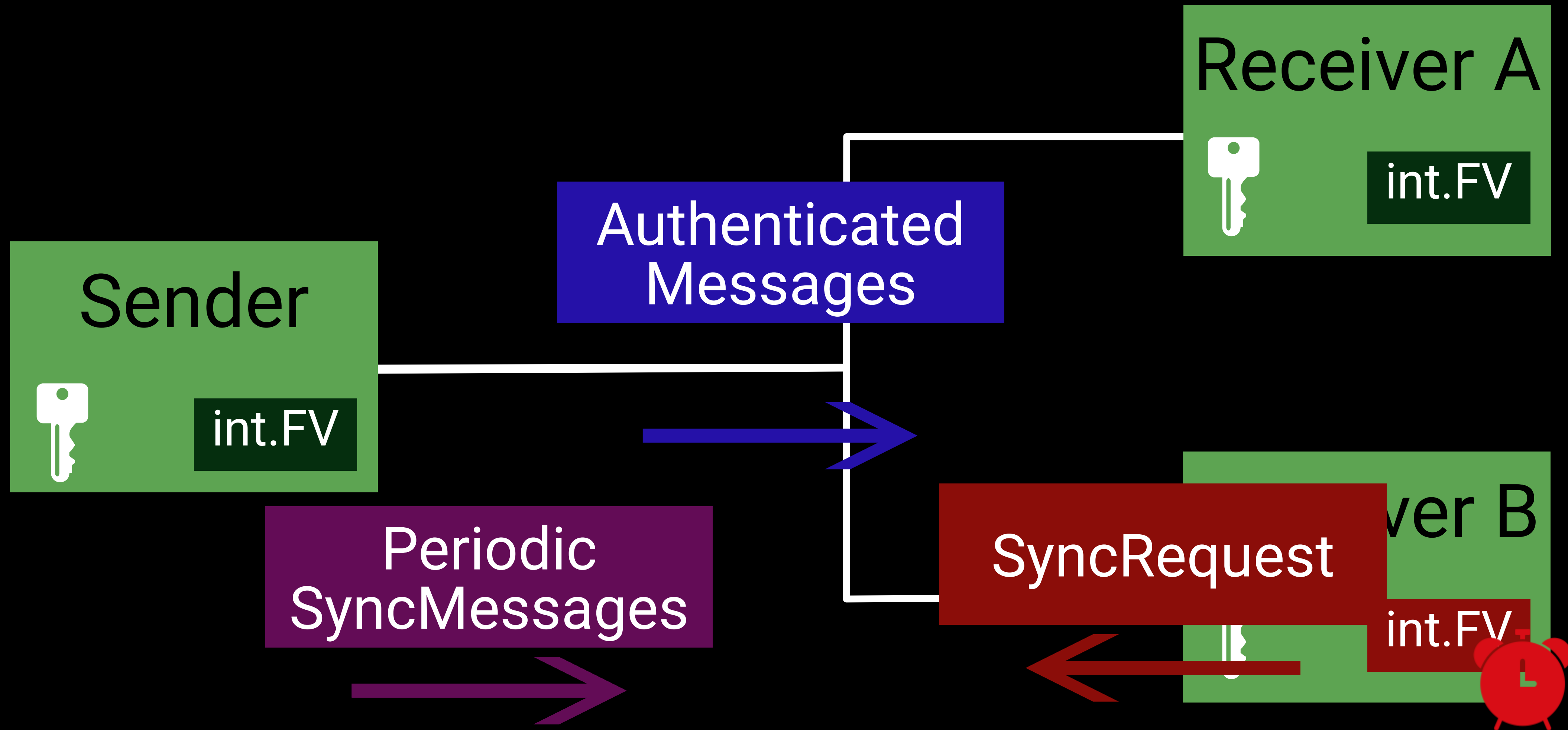
PROPOSED SecOC PROFILE



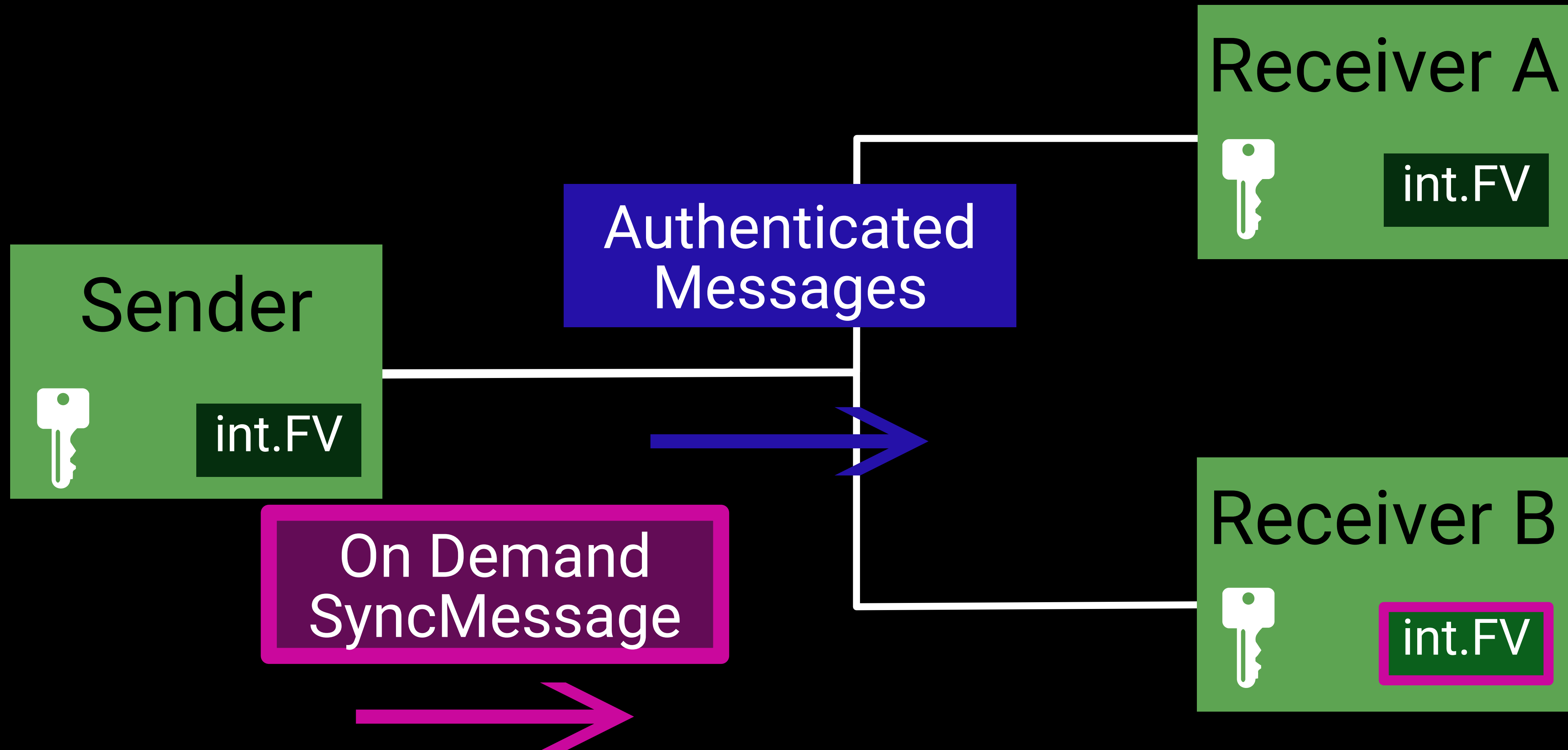
JASPAR (AUTOSAR SecOC PROFILE 3)



PROPOSED SecOC PROFILE



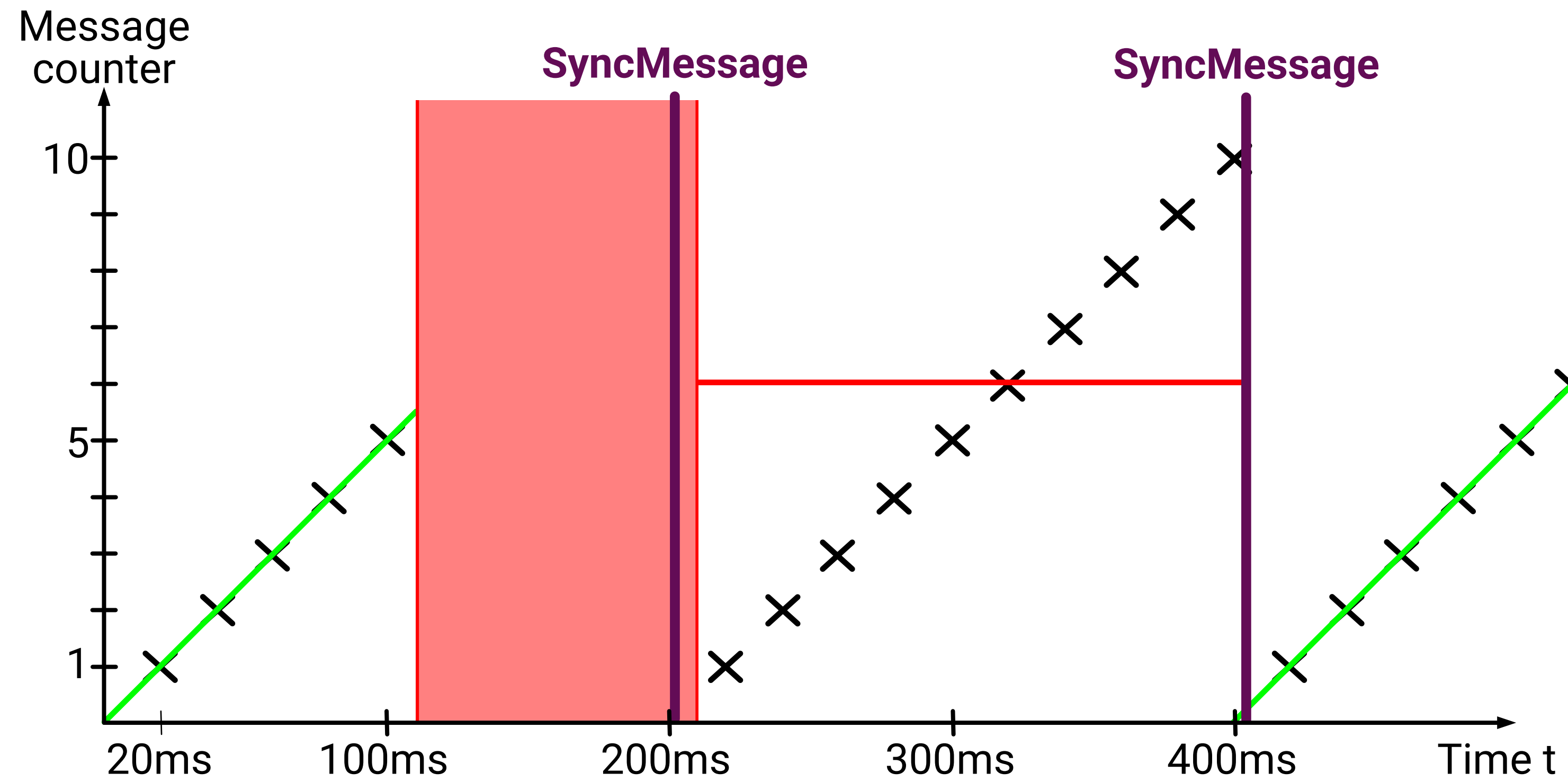
PROPOSED SecOC PROFILE



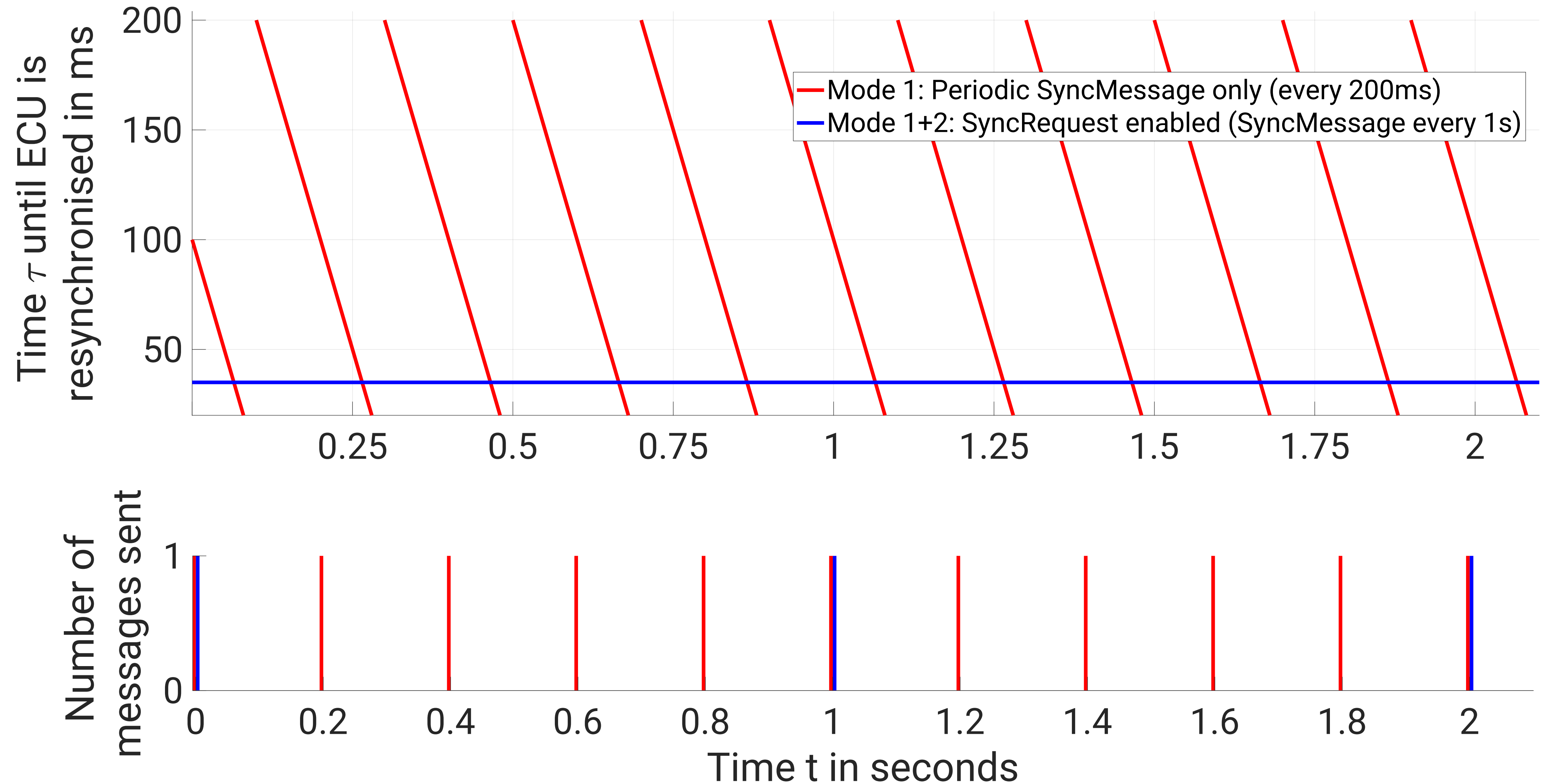
PROPOSED SecOC PROFILE

- ▶ Faster synchronisation of the FV
- ▶ Alignment with ISO 26262 (Functional Safety Standard for Road Vehicles)
- ▶ Less bandwidth usage
- ▶ Simplified structure of the FV

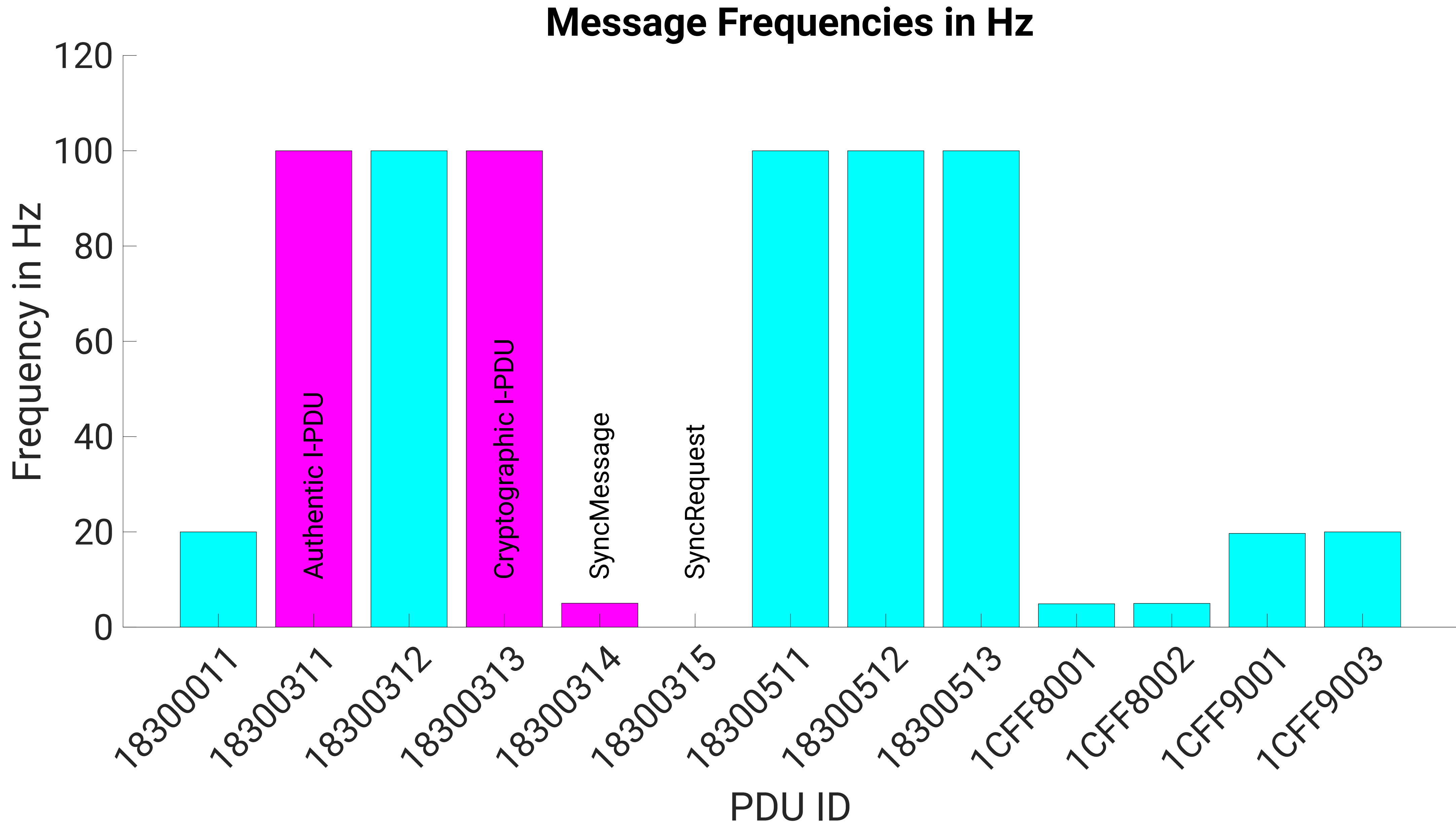
ANALYSIS JASPAR



ANALYSIS JASPAR AND MODE1+2

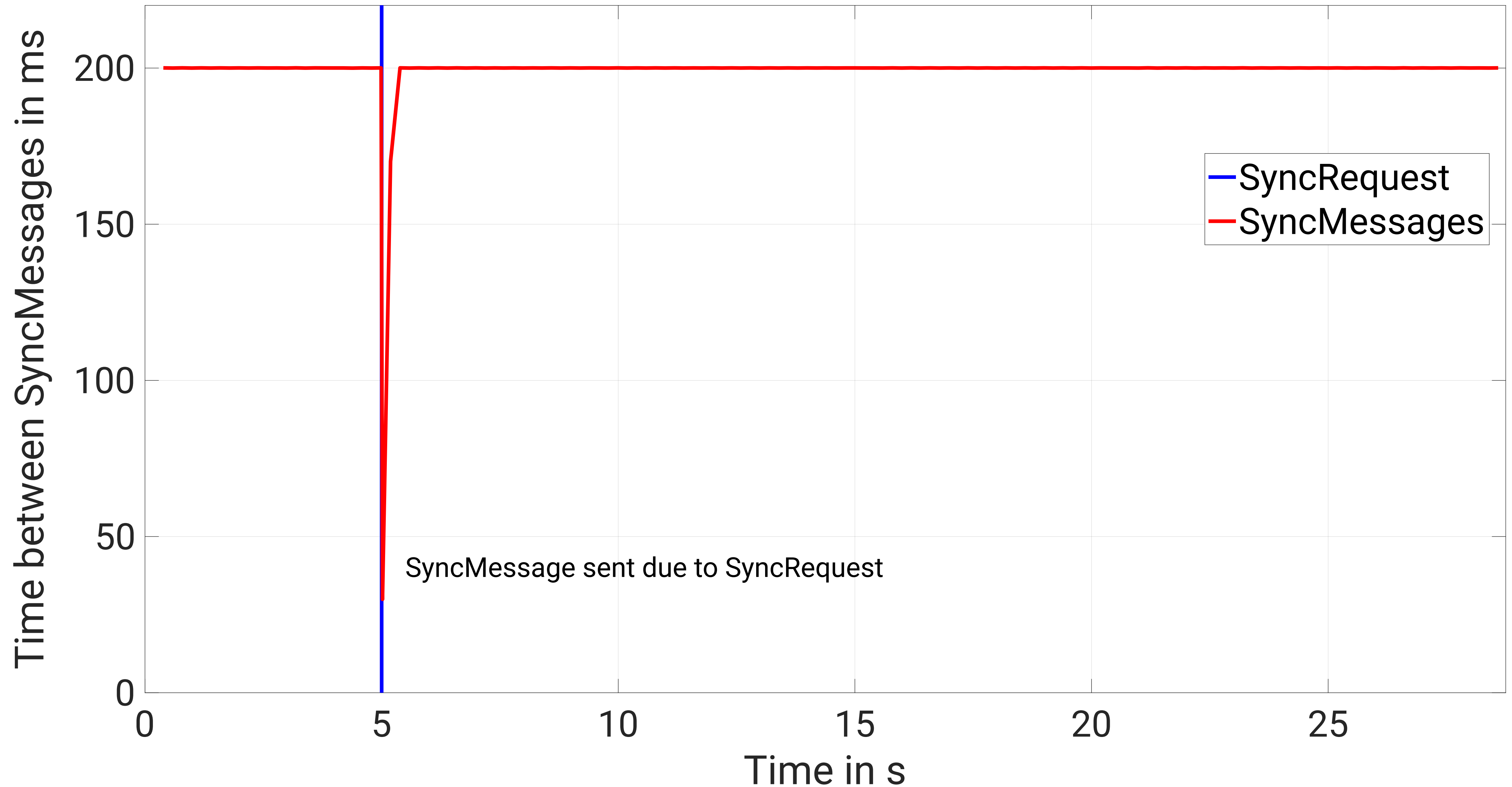


EXPERIMENTAL RESULTS (MODE 1+2)



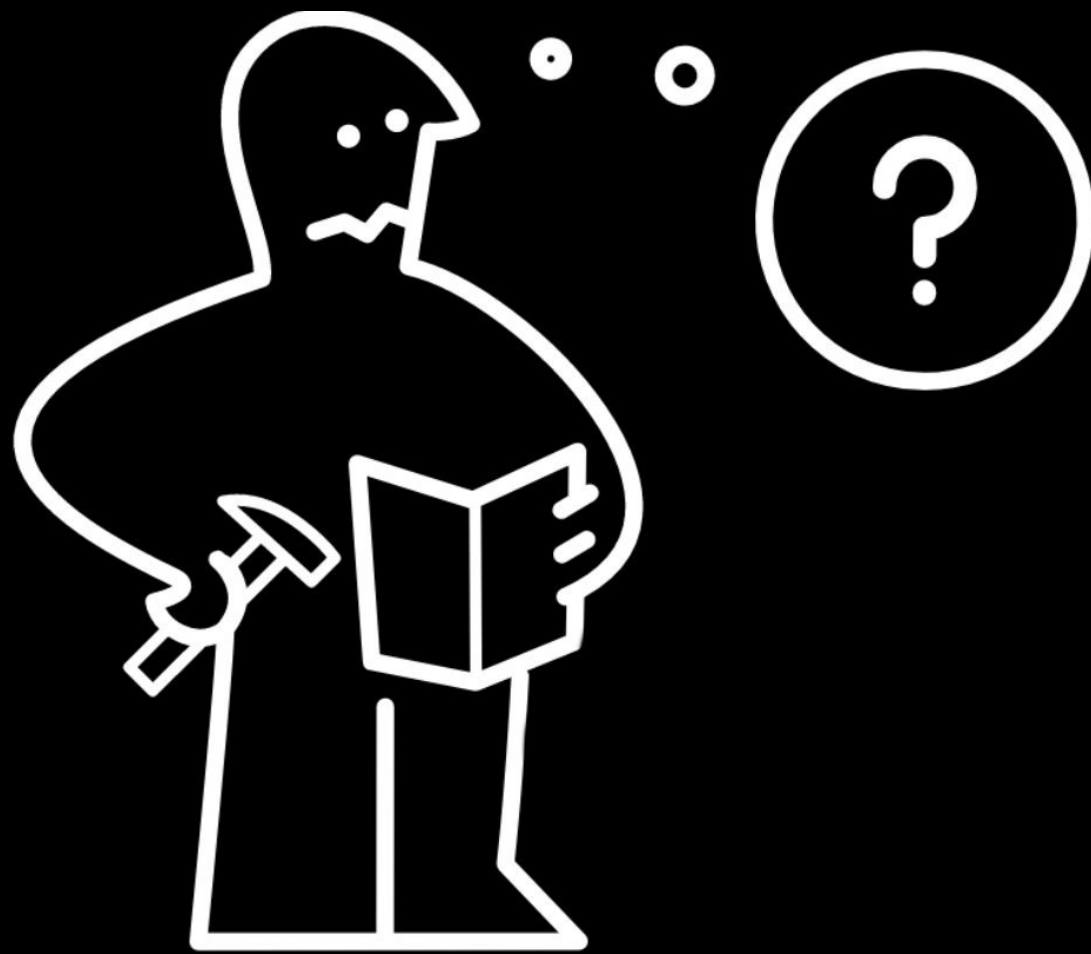
EXPERIMENTAL RESULTS (MODE 1+2)

Frequency of SyncMessages over time



OVERVIEW

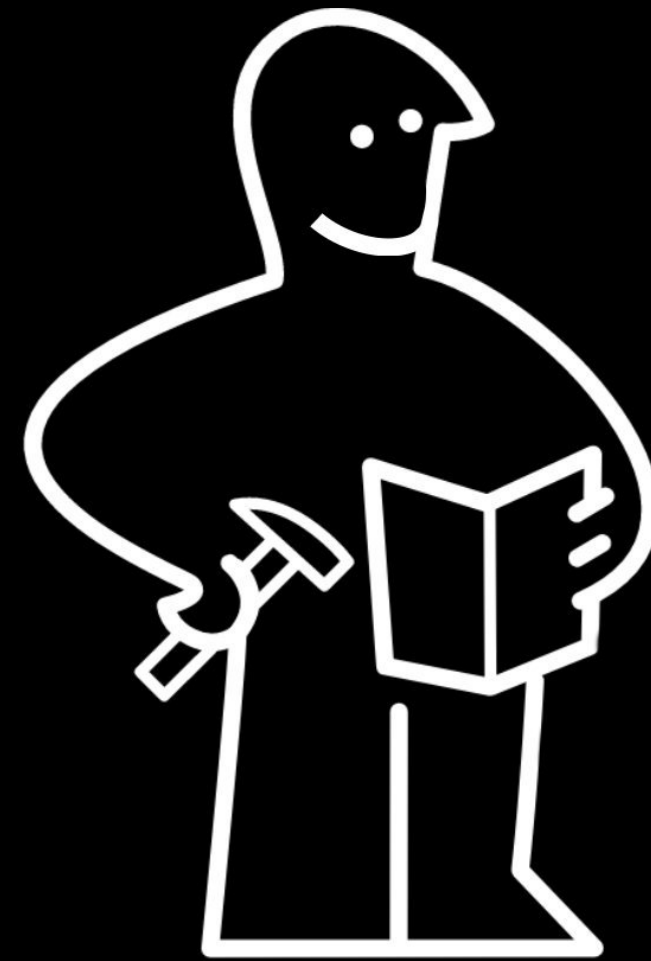
PAPER 1



RQ.2 *How to move forward from unique security requirements of individual systems to predefined security requirements?*

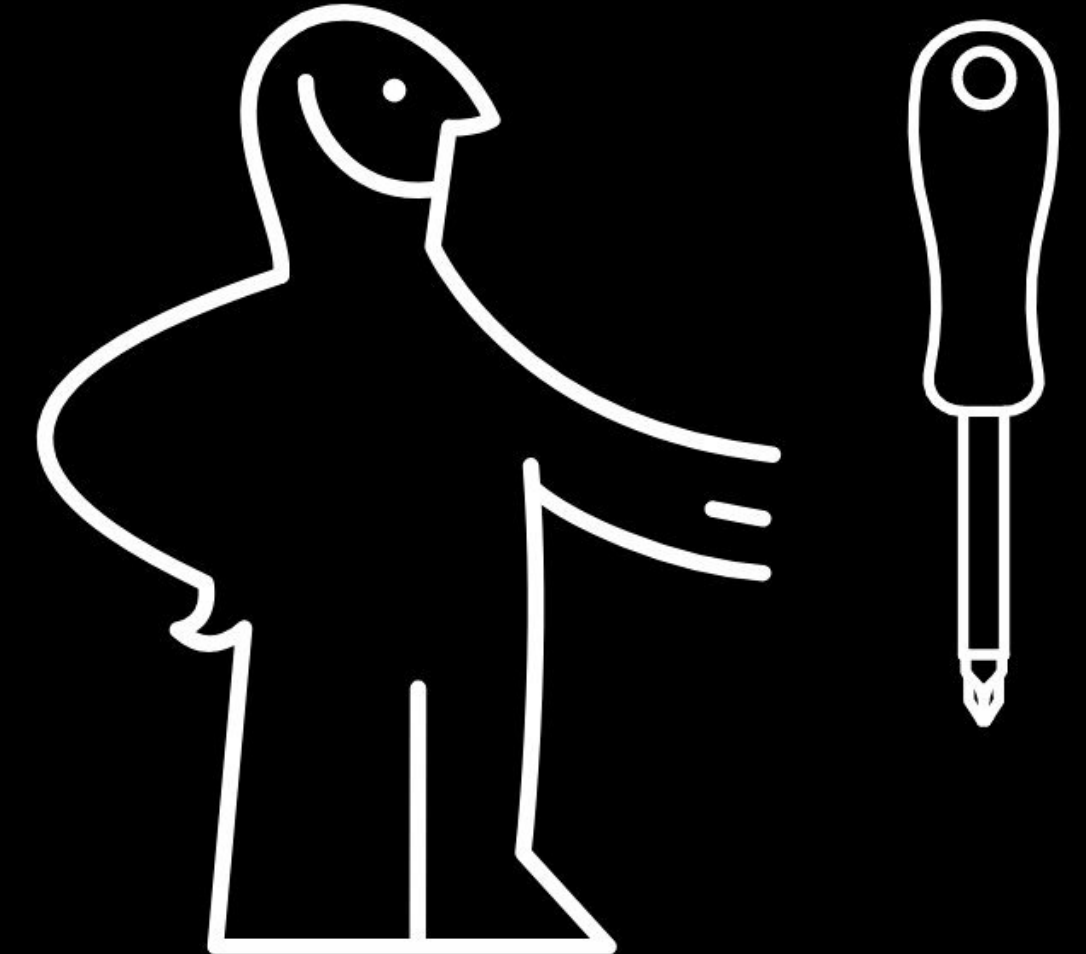
RQ.1 *How to express security demands for the design and development of connected vehicles?*

PAPER 2



RQ.3 *What are suitable security mechanisms for the automotive domain and how can they be used in a framework?*

PAPER 3



RQ.4 *What are the limitations and possible design considerations when implementing a freshness mechanism for authenticated messages in automotive systems?*

OVERVIEW

PRESENTATION OVERVIEW

INTRO

IN-VEHICLE NETWORK

USE CASE

OVERVIEW

How?

OVERVIEW TARA

STRUCTURE SECURITY LEVELS

WHAT?

MAPPING OVERVIEW

IDENTIFIED SECURITY MECHANISMS

APPLIED ON USE CASE

TOOL

AUTHENTIC MESSAGES IN CAN

WHY FRESHNESS?

JASPAR

DESIGN CONSIDERATIONS & LIMITATIONS

PROPOSED SECOC PROFILE

ANALYSIS JASPAR

EXPERIMENTAL RESULTS

OVERVIEW

PAPER I: ANALYSED STANDARDS

- ▶ ISO 26262 Road Vehicles -- Functional Safety
- ▶ DO-178 Software Considerations in Airborne Systems and Equipment Certification
- ▶ IEC 62443/ISA 99 Industrial Communication Networks -- Network and System Security
- ▶ TAL Trust Assurance Levels
- ▶ EVITA -- European Project 2009
- ▶ HEAVENS -- Swedish Project 2016
- ▶ (Common Criteria)

PAPER II: ANALYSED STANDARDS

- ▶ IEC 62443/ISA 99 Industrial Communication Networks -- Network and System Security
- ▶ NIST FIPS PUB 199 -- Standard for Security Categorization Federal Information and Information Systems
- ▶ NIST SP 800-53 -- Security and Privacy Controls for Federal Systems and Organizations
- ▶ Connected Vehicles Pilot Development -- New York City
- ▶ UNECE task force on cybersecurity and over-the-air issues
- ▶ (NHTSA Cybersecurity Best Practices for Modern Vehicles)