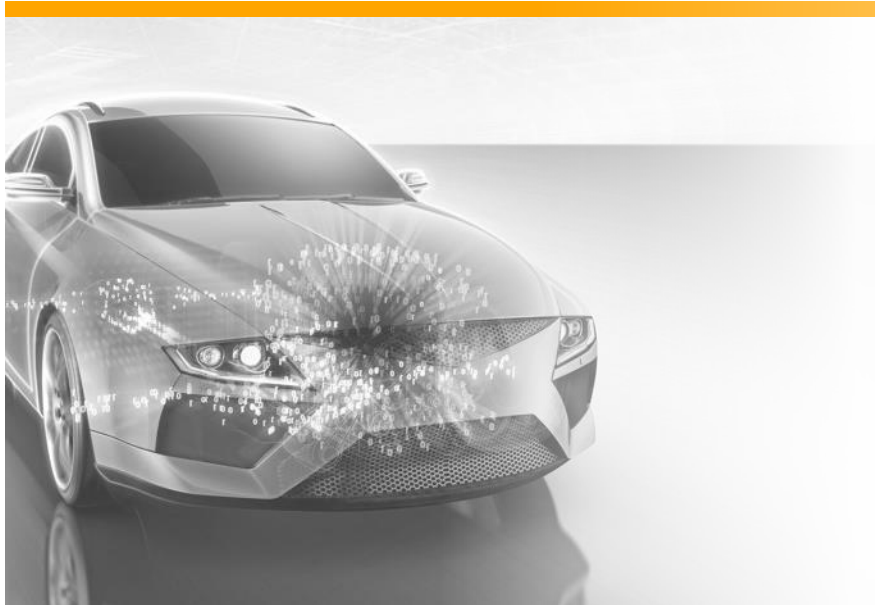# Long-term Security Challenges Ahead of Automotive Applications: An Industrial Perspective

Ahmad Sabouri | Deputy Head Security and Privacy Consulting
Marc Stöttinger | Senior Specialist Security and Privacy
Gregor H. Molter | Head of Security & Privacy Research Embedded Systems

Automotive Systems and Technology
Security & Privacy Competence Center

http://links.conti.de/SCC

Long-term Security Challenges Ahead of Automotive Applications
Agenda

1	Introduction

2	Related Work on Sustaining Security

3	Problem and Solution Space

4	Conclusion

Long-term Security Challenges Ahead of Automotive Applications
Agenda

1	**Introduction**
2	Related Work on Sustaining Security
3	Problem and Solution Space
4	Conclusion

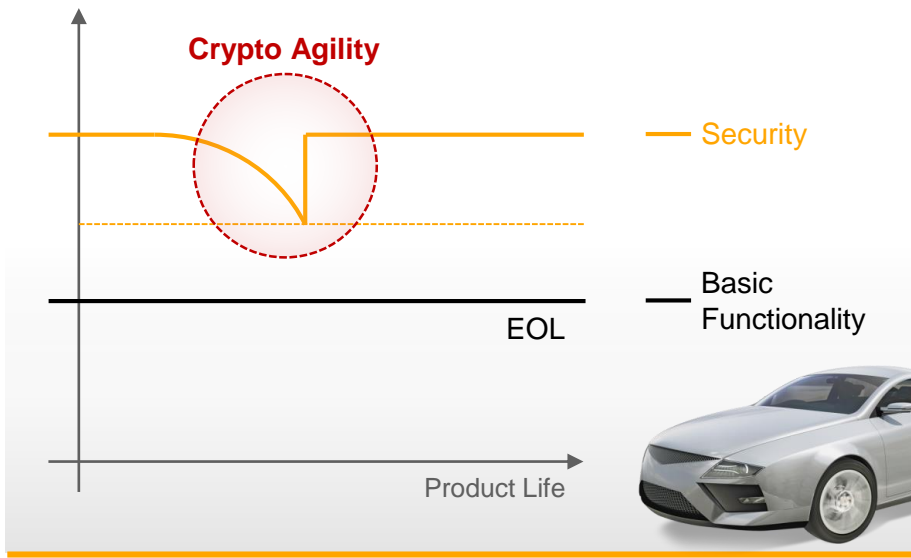# Long-term Security Challenges Ahead of Automotive Applications
Motivation

Cryptography enables security attributes
› Authenticity
› Integrity
› Confidentiality

Attacks on cryptographic methods by
› New methods to break cryptographic primitives
› New technologies to raise the power of brute force attacks
› Exploit implementation flaws

Needs for secure update/upgrade of cryptographic primitives

Crypto Agility

Security

Basic Functionality

EOL

Product Life

Long-term Security Challenges Ahead of Automotive Applications
Definition

" Crypto agility is the ability of a protocol to adapt to evolving cryptography and security requirements. "

Deploy new cryptographic algorithm and replace deprecated ones

Increase the key sizes

Fix implementation flaws

Continental

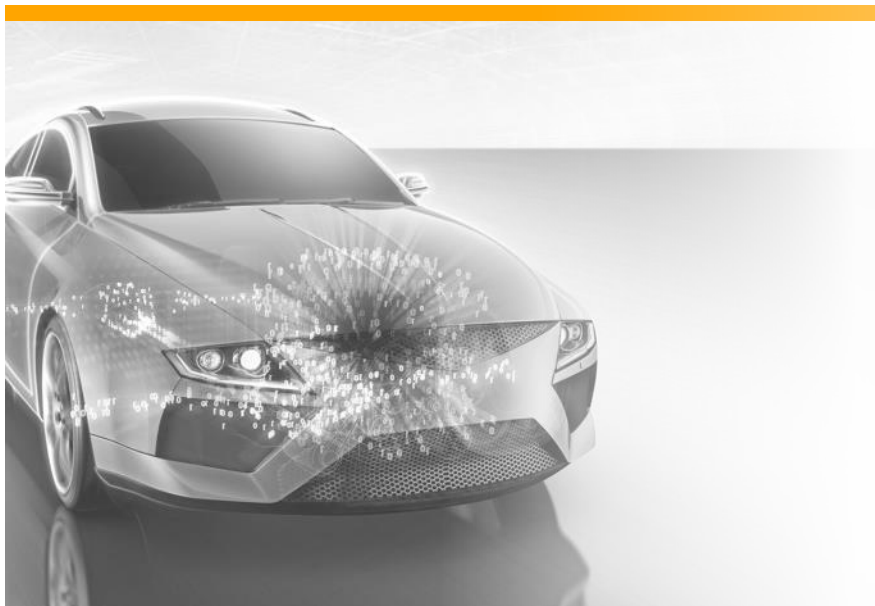# Long-term Security Challenges Ahead of Automotive Applications
Prerequisite

" A modular mechanism is necessary to allow cryptographic algorithms to be updated without substantial disruption of the applications and services using the those primitives "

Long-term Security Challenges Ahead of Automotive Applications
Agenda

| 1 | Introduction |

| 2 | **Related Work on Sustaining Security** |

| 3 | Problem and Solution Space |

| 4 | Conclusion |

Long-term Security Challenges Ahead of Automotive Applications
Related Work on Sustaining Security
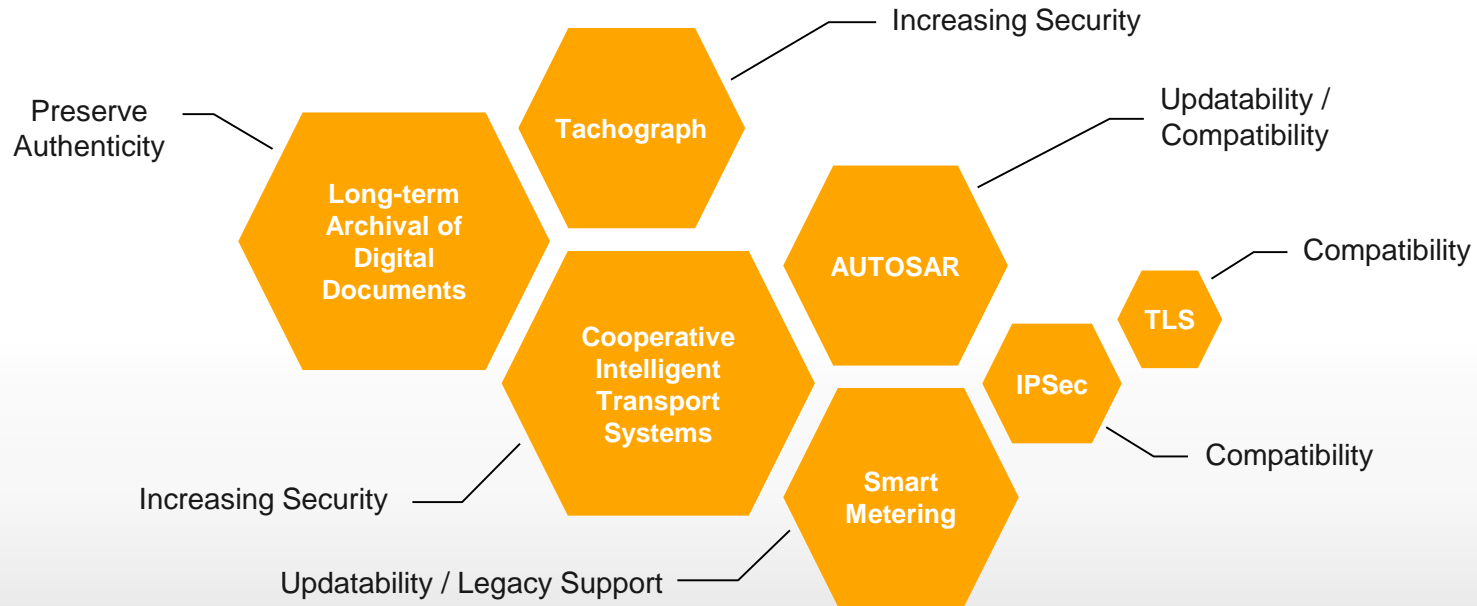
Comparision of recommandations from …

Reports contain recommendations on …

› Security levels for asymmetric (e.g. RSA, …)
› Security levels for symmetric algorithms (e.g. AES, …)

› Use of mode of operation for block ciphers (e.g. AES-CBC, …)

› Truncation settings for message authentication codes (e.g. HMAC, …)

Long-term Security Challenges Ahead of Automotive Applications
Related Work on Sustaining Security

Increasing Security

Updatability / Compatibility

Preserve Authenticity

Tachograph

Long-term Archival of Digital Documents

AUTOSAR

Compatibility

TLS

Cooperative Intelligent Transport Systems

IPSec

Smart Metering

Increasing Security

Compatibility

Updatability / Legacy Support

Long-term Security Challenges Ahead of Automotive Applications
Summary of Analyzing Existing Update Processes

› The existing schemes mainly employ two methods to migrate between different cryptographic schemes:

  › **Implementing a Crypto Suite**

  › **Implementing a replacement mechanism**

› Even though in some cases detailed information are available for the migrations that need to happen, there is no well-defined process for the update itself.

Continental

Towards Cryptographic Agility in Automotive Systems
Agenda

1	Introduction
2	Related Work on Sustaining Security
3	**Problem and Solution Space**
4	Conclusion

Ontinental

Towards Cryptographic Agility in Automotive Systems
Possible Scenarios When Update is Needed

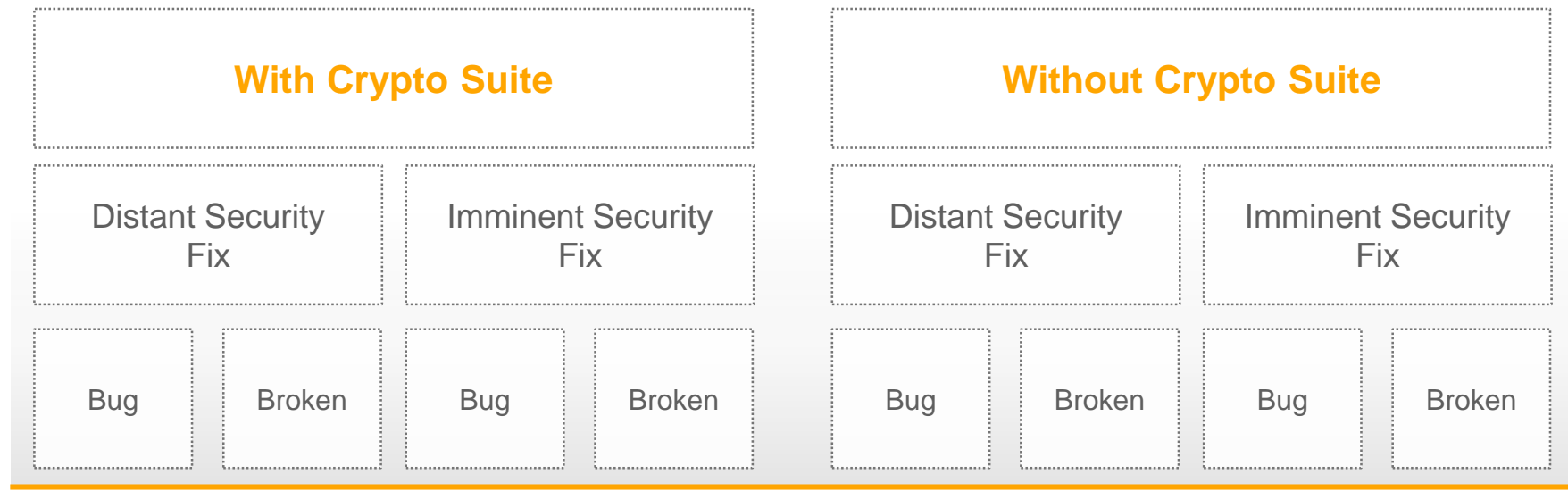|	**Distant security fix is needed**	**Imminent security fix is needed**
Algorithm **A** gets updated, the authentication and integrity check is done by algorithm **B**	**OTA** or **Repair Shop**	**OTA** or **Repair Shop**
Algorithm **A** gets updated, the authentication and integrity check is done also by **A**	**OTA** or **Repair Shop**	**Repair Shop**

Towards Cryptographic Agility in Automotive Systems
Different Mechanisms and Problem Space

With Crypto Suite				Without Crypto Suite			
Distant Security Fix		**Imminent Security Fix**		**Distant Security Fix**		**Imminent Security Fix**	
Bug	Broken	Bug	Broken	Bug	Broken	Bug	Broken

Towards Cryptographic Agility in Automotive Systems
Example Case (1)

Scenario

Algorithm **A** gets updated, the authentication and integrity check is done by algorithm **B**

| With Crypto Suite		Without Crypto Suite	
Distant Security Fix	Imminent Security Fix	Distant Security Fix	Imminent Security Fix
Bug · Broken	Bug · Broken	Bug · Broken	Bug · Broken

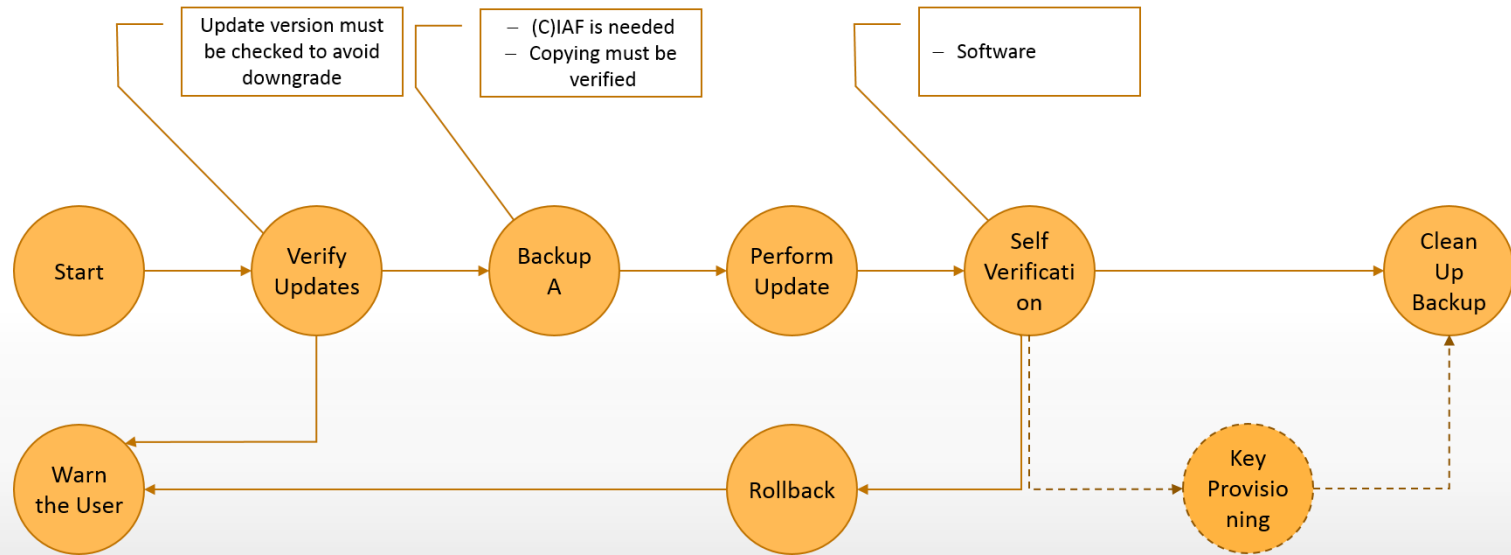# Towards Cryptographic Agility in Automotive Systems
Example Case (2)

1. Allow negotiation if the counterparts are not yet updated, but put priority to use A'

2. Apply updates on A

3. Switch back to A
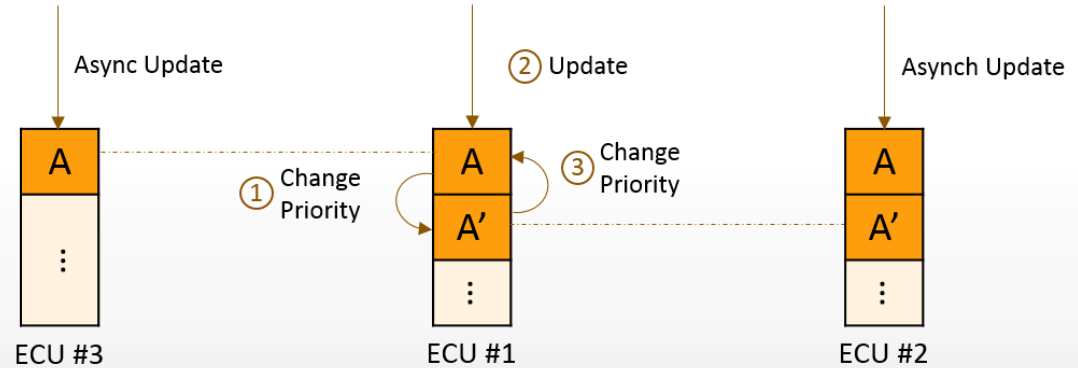
Towards Cryptographic Agility in Automotive Systems
Update Process and Orchestration

Long-term Security Challenges Ahead of Automotive Applications
Agenda

1	Introduction
2	Related Work on Sustaining Security
3	Problem and Solution Space
4	**Conclusion**

Continental

Long-term Security Challenges Ahead of Automotive Applications
Conclusion

› Considering the long age of vehicles, **Crypto Agility seems to be inevitable** in order to maintain the security of the vehicle;

› There is **no currently mature holistic solution available** to address this problem;

› Performing timely and remote update/upgrade of cryptographic primitive in a safely-critical system **without substantial disruption** of the operation is a major challenge and introduces a lot of complexity;

› Due to the cross-component effects of security protocols, the update process should be orchestrated through the entire vehicle.