WHAT IS FASTR?

- **Automotive security** is not a problem that can be solved by a single organization or in silos → it **requires an industry-wide effort**

- **Success** in securing tomorrow’s vehicles **requires a unified approach** through knowledge exchange and technology-sharing

- FASTR is a non-profit consortium that provides a **neutral, open environment** to enable collaboration across the automotive ecosystem
ACTIVE FASTR CORPORATE MEMBERS
FASTR Guidelines for Secure Over-the-Air Updates

Initial version published by FASTR in November 2017

Intended to assist the automotive industry in evaluating platforms for secure SOTA updates, the guidelines include:

- Description of threat models & guidelines to address these threats 21
- Recommended cryptographic algorithms 18
- Key management plan 17
- A detailed step-by-step checklist for evaluating platforms 56

Access the Guidelines here [https://fastr.org/guidelines-sota/](https://fastr.org/guidelines-sota/)
Threat Models Considered

SOTA software update systems should be resistant to any attack that does not physically modify the vehicle, including:

- Spoofing attacks - emulation of SOTA component(s)
- Tampering attacks - install/use modified software
- Repudiation attacks - refute claims of proper/improper install
- Information-leakage attacks - sensitive info exposure (keys, code)
- Denial-of-service attacks - “graceful degradation” to an attack
- Escalation-of-privileges attacks - via agent/cloud compromise
Examples of Guidelines to Address These Threats

- Software updates should **include a signed certificate containing the public key of the entity providing the update**

- Software updates should **include version information to prevent rollback** to genuine but obsolete software versions

- Secure all network transactions with **TLS public key authentication**, and the public keys should be signed by a trusted Certificate Authority

- Compliant SOTA software update systems should **log all important events**, in such a way the log entries cannot be altered later

- Compliant SOTA software update systems should **deliver software updates to authorized devices only**
Recommendations for Cryptographic Algorithms

- Random number generation - TRNG entropy source
- Symmetric key encryption - @ least AES-128 & SHA-256
- Cryptographic hash algorithm - @ least SHA-256
- Digital signature - @ least ECDSA-256
- Key agreement - @ least ECDH-256
- Digital certificates - guidance on X.509 certificate fields
- Network and point-to-point cryptography - TLS
- Passwords - recommend multi-factor authentication
Detailed Key Management Plan

- List of keys - nine identified (may not need all for every case)
- Key and random data generation - use a TRNG entropy source
- Storage and backup - storage strategy is based on key type
- Key distribution - distribute keys in a secure manner
- Usage - use keys in an appropriate/secure manner
- Key and certificate updates - procedures to update keys & certs
- Key and certificate revocation - procedures to manage/revoke
Summary

FASTR has provided this resource and checklist to initiate an industry dialog on these aspects of security

We welcome input, feedback, and collaboration with GENIVI on **utilizing these guidelines, identifying joint security research topics, and developing new intellectual capital**
Potential topics for joint future research...

- Assessing the security of 5G and DSRC
- Threat models for V2X
- Standard methodology for assessing the security of TCUs
- Security concerns during potential corner cases, including:
  - Loss of network connectivity
  - Loss of authentication services
  - Loss of GPS / mapping

Could an attacker take advantage of a disruption event to do things they normally couldn’t?
Questions or Feedback?

Connectivitywg@fastr.org