Authenticated and Secure Automotive Service Discovery with DNSSEC and DANE

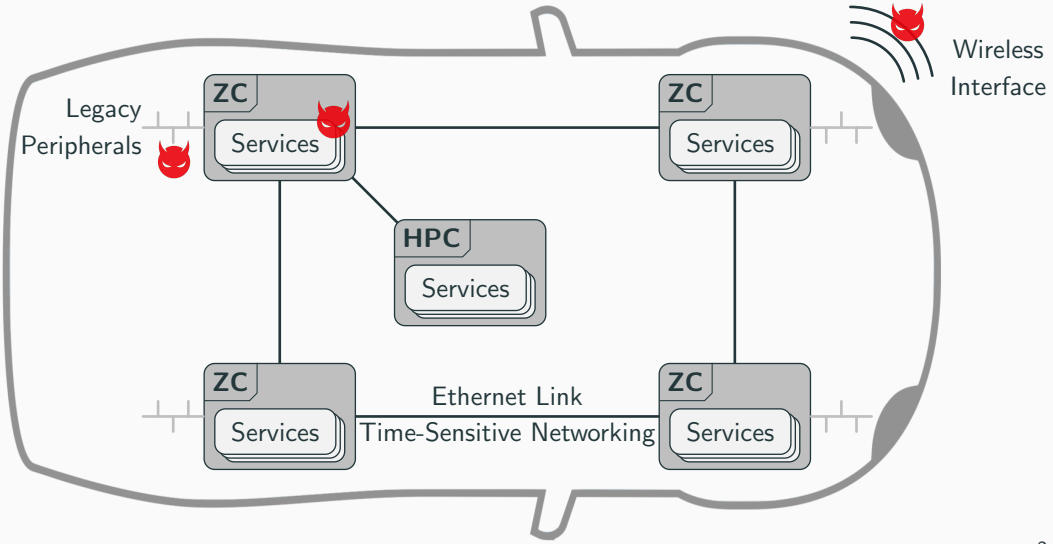
Mehmet Mueller, Timo Häckel, Philipp Meyer, Franz Korf and Thomas C. Schmidt

26 April – 28 April 2023, Istanbul, Türkiye
2023 IEEE Vehicular Networking Conference (VNC)

Dept. Computer Science, *Hamburg University of Applied Sciences*, Germany
{mehmet.mueller, timo.haeckel, philipp.meyer, franz.korf, t.schmidt}@haw-hamburg.de

Outline

Future In-Vehicle Networks



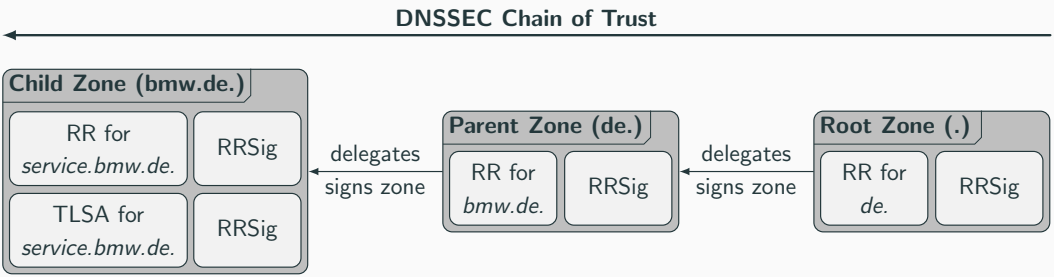
Automotive Security Issues

- Previous automotive protocols target closed network environments – no security
- SOME/IP is a widely accepted automotive SOA middleware
  - Provides a complementary service discovery protocol
  - Service discovery lack security mechanisms

- Related work introduces custom security measures based on pre-deployed certificates
- Not proven, complex in managing and updating certificates
- Common service authenticity on the Internet uses certificates or keys

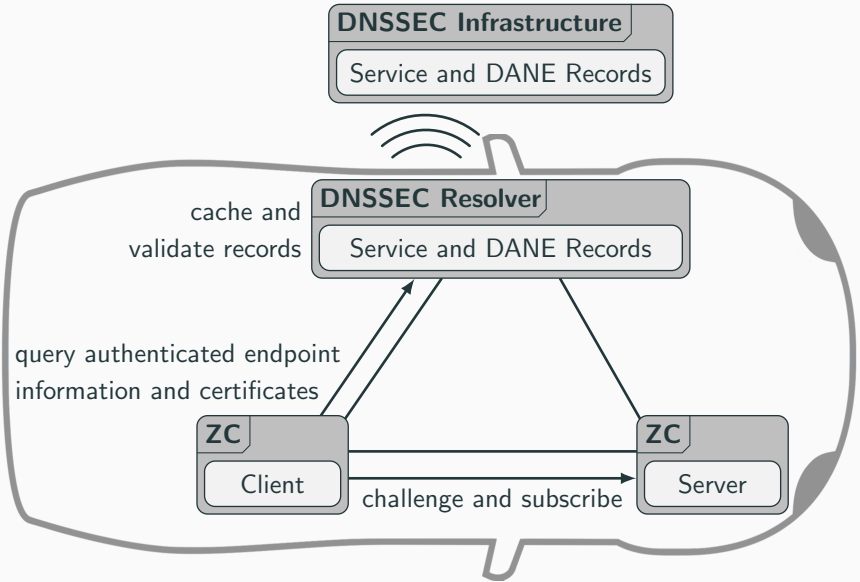
→ DNSSEC with DANE feature robust service authenticity w/ certificate and key management

Service Authenticity Based on DNSSEC and DANE



- Resource Records (RRs) contain endpoint information
- DNSSEC ensures integrity and authenticity of all RRs with signature records (RRSigs)
- DANE introduces TLSA RR to store service certificates
- Robust security solution with established key and certificate management mechanisms
- Possibility for private DNSSEC namespaces

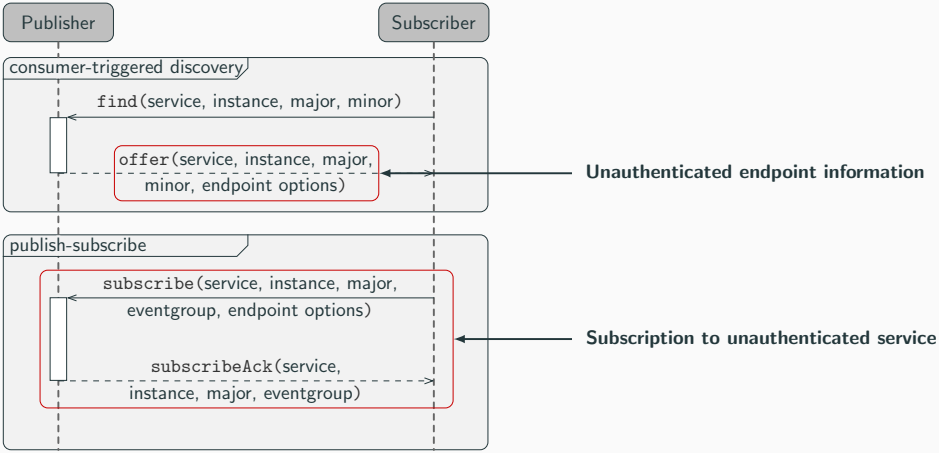
Envisioned Deployment Scenario



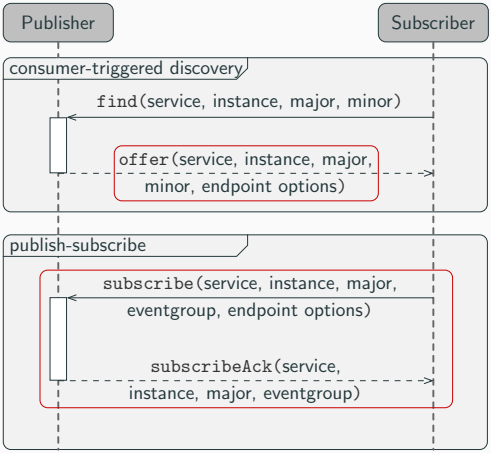
→ Offline operation w/o pre-deployed certificates

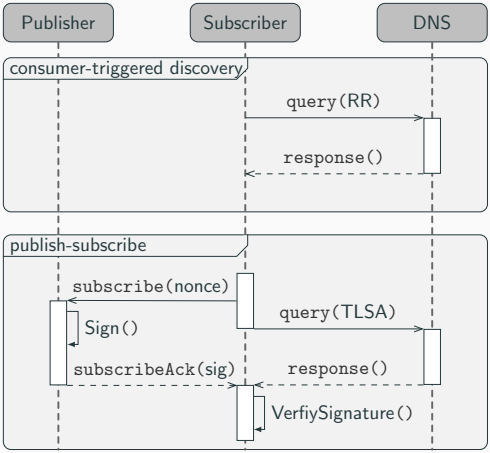
→ Secure, established update scheme

SOME/IP Service Discovery



Our Approach: DNSSEC in SOME/IP Service Discovery



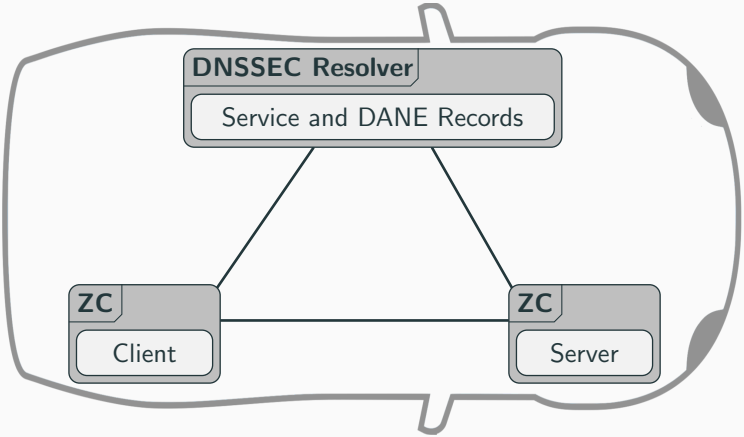


→ **DNSSEC ensures authentic endpoint information**

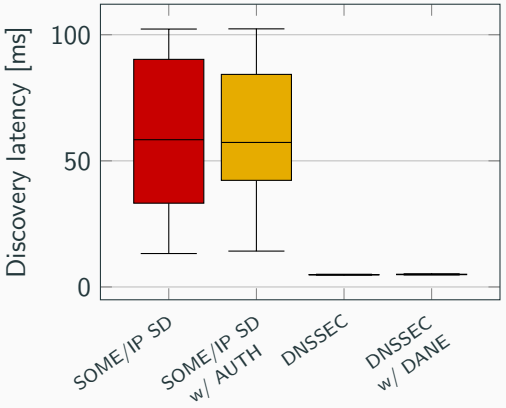
→ **Challenge-response mechanism ensures publisher authenticity**

DNSSEC-based SOME/IP Service Discovery Implementation

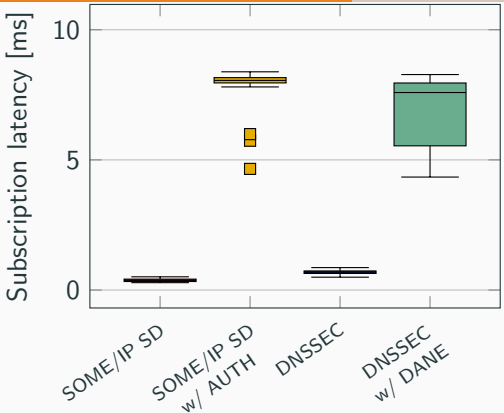
- Implementation based on vsomeip reference implementation
- Integrated standard DNS resolver in vsomeip
- Integrated standard cryptographic operations and algorithms for service authentication



Performance Analysis Based on SOME/IP Reference Implementation



→ **Discovery performance negligible compared to multicast scattering**



→ **Crypto operations main impact on subscription latency**

Benefits of Secure Service Discovery with DNSSEC and DANE

- Over 15 years of operational experience of DNSSEC
- Hardened for global deployment
- Pre-deployed certificates not needed
- Established mechanisms for key and certificate management
- Assured service authenticity using a challenge-response mechanism
- Scalable without delay penalty for service discovery

Conclusion & Outlook

Summary

- SOME/IP is widely accepted but lacks service authenticity
- DNSSEC with DANE contribute a robust security solution and key management
- DNS namespace preserving SOME/IP SD query properties
- Endpoint authentication with a challenge-response mechanism

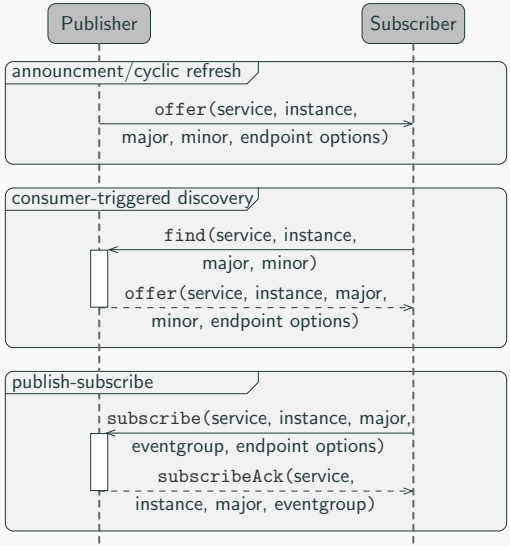
Future Work

- Security design and assessment for remaining SOME/IP service primitives
- Operational guidelines for namespace management and service updates
- Evaluation of scalability in a production-grade vehicle

Authenticated and Secure Automotive Service Discovery with DNSSEC and DANE

Contact: Mehmet Mueller
mehmet.mueller@haw-hamburg.de
Dept. Computer Science, Hamburg University of Applied Sciences, Germany

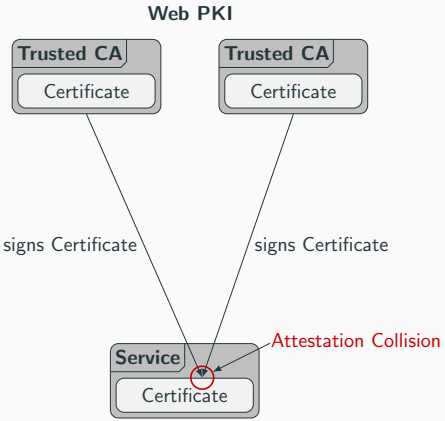
SOME/IP Service Discovery Protocol

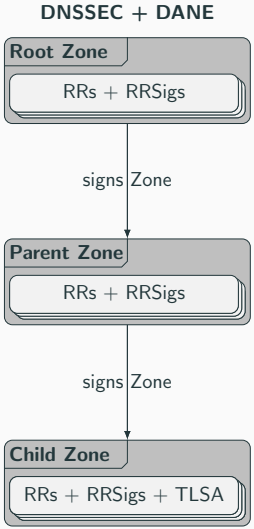


- Endpoint information from offers is not authenticated
- Endpoint itself is not authenticated during subscription
- No protection against Man-In-The-Middle attacks

SOME/IP lacks service authentication.

Service Authenticity with Asymmetric Cryptography (Simple View)





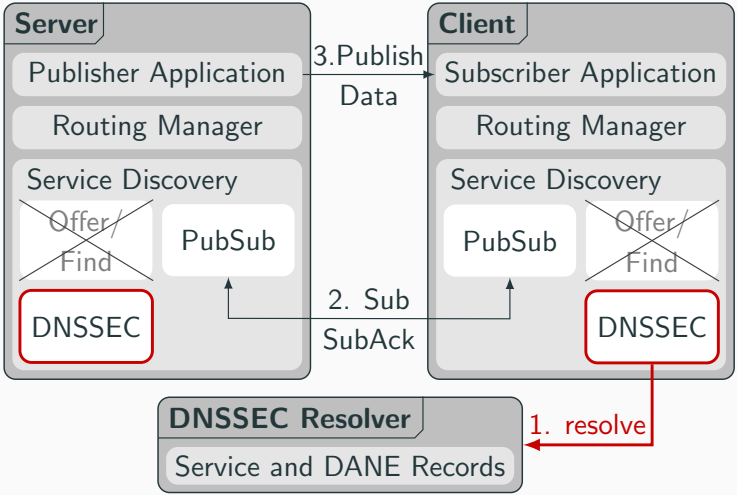
DNS Namespace

service ID (2 Byte)	instance ID (2 Byte)	major version (1 Byte)	minor version (4 Byte)
0x0001	0x0002	0x01	0x00000002

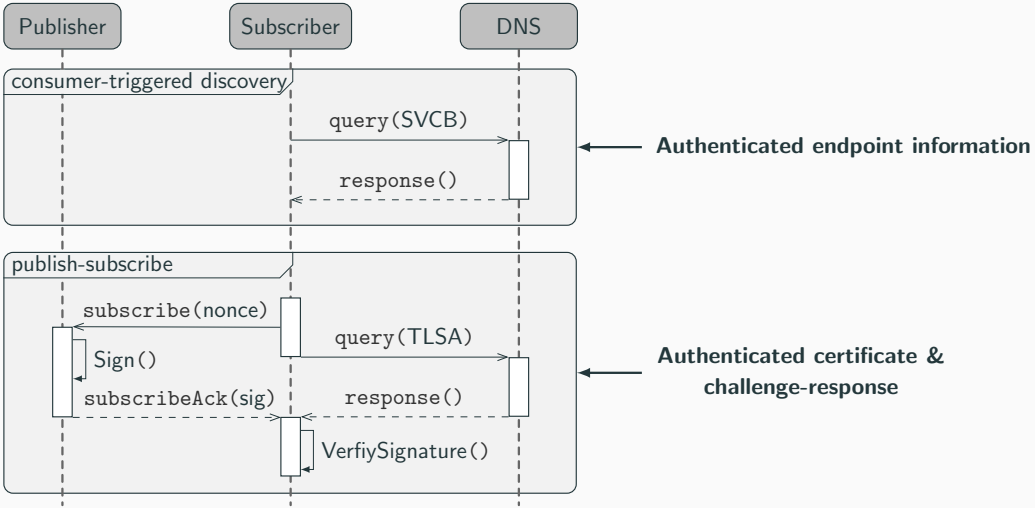
IP address (4 Byte)	L4-protocol (1 Byte)	port number (2 Byte)
10.0.0.5	UDP	30509

QNAME	RDATA (SVCB)
_someip.minor.major.instance.id.service.	port=30509 ipv4hint=10.0.0.5 protocol=UDP instance=2 major=1 minor=2
_someip.major.instance.id.service.	
_someip.minor.instance.id.service.	
_someip.minor.major.id.service.	
_someip.instance.id.service.	
_someip.major.id.service.	
_someip.minor.id.service.	
_someip.id.service.	

SOME/IP SD Modification for Using DNSSEC



SOME/IP SD Modification for Using DNSSEC



Feature Comparison

Feature	**SOME/IP SD** (and related work)	**SD w/ DNSSEC and DANE** (our approach)
Introduction and deployment	AUTOSAR, Nov. 2016	IETF, DNSSEC 1997
Target environment	Local in-vehicle network	Global Internet deployment
Service discovery scheme	Multicast	Unicast DNS
Endpoint detail distribution	Offers w/ runtime location	Consumer requested records
Authentication scheme	None by default, challenge-response, central authorization server	Challenge-response during subscription
Certificate distribution and update procedure	Pre-deployed certificates, no automated mechanism	Consumer requested, established mechanism