Automotive Group Key Agreement and Secure Service & Client Authentication Using DNSSEC with DANE

Mehmet Mueller

Master Project

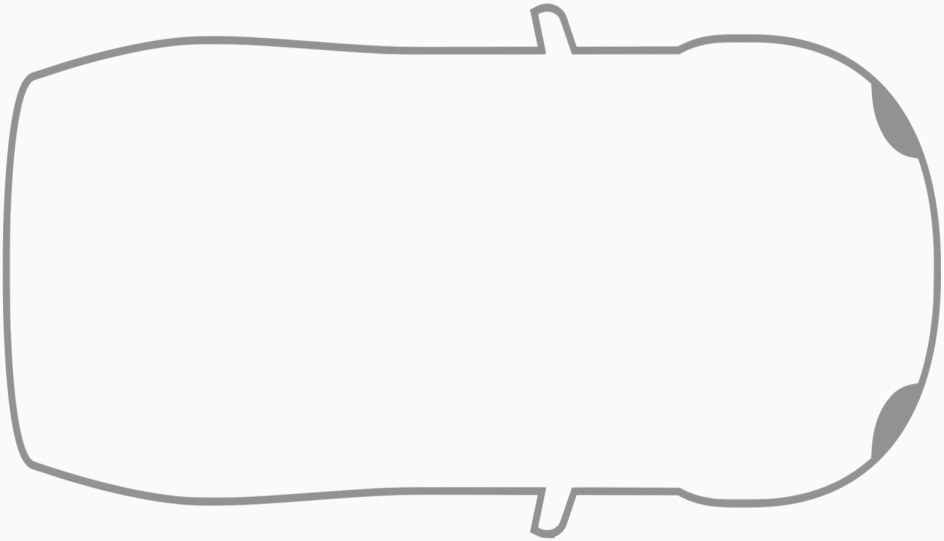
23 April 2024, Hamburg, Germany

Dept. Computer Science, *Hamburg University of Applied Sciences*, Germany
mehmet.mueller@haw-hamburg.de

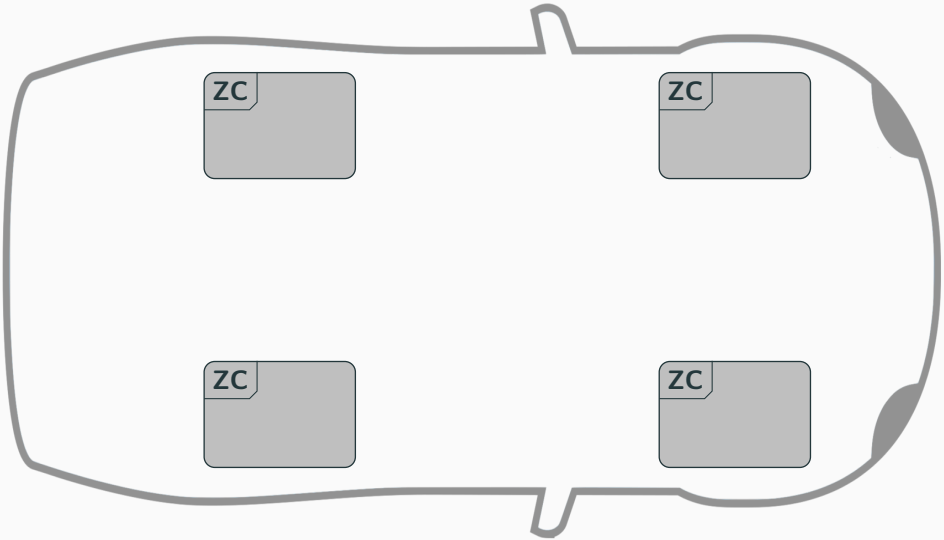
Outline

1. Introduction to In-Vehicle Networks
2. DNSSEC-based Service and Client Authenticity
3. Management of Group Keying
4. DNSSEC-based Authenticity and GKA Performance
5. Conclusion & Outlook

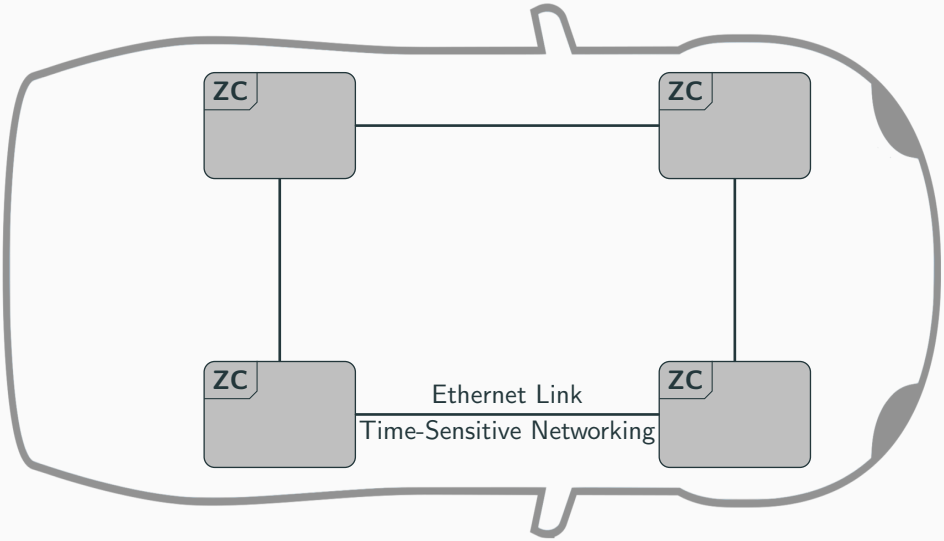
Future In-Vehicle Networks



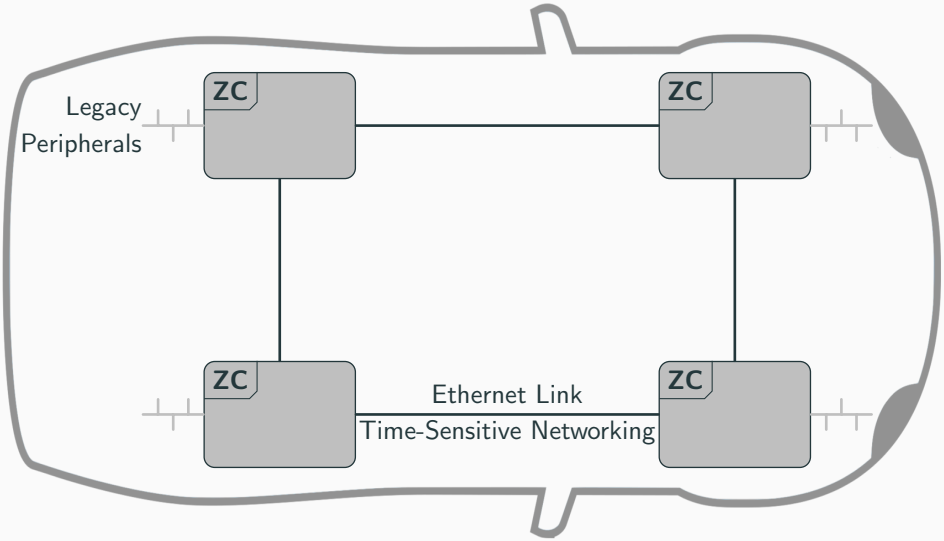
Future In-Vehicle Networks



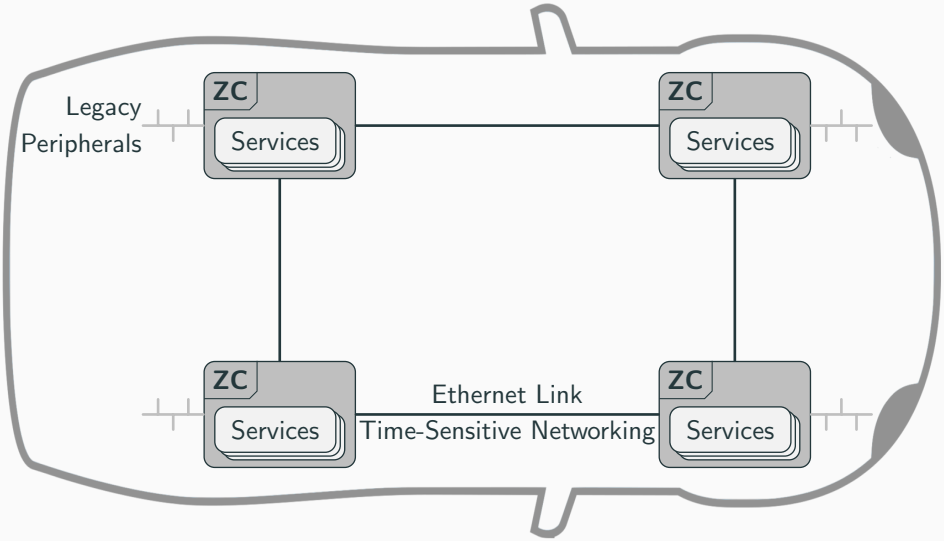
Future In-Vehicle Networks



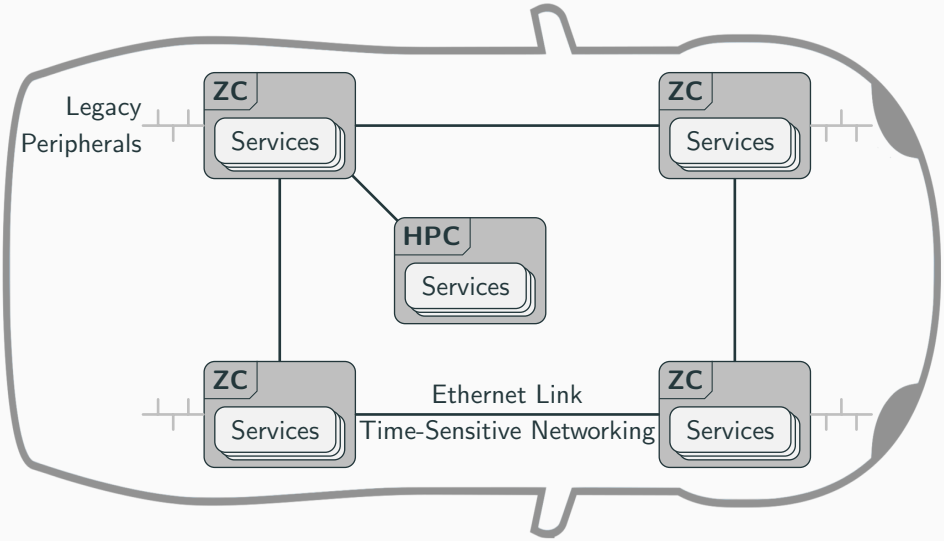
Future In-Vehicle Networks



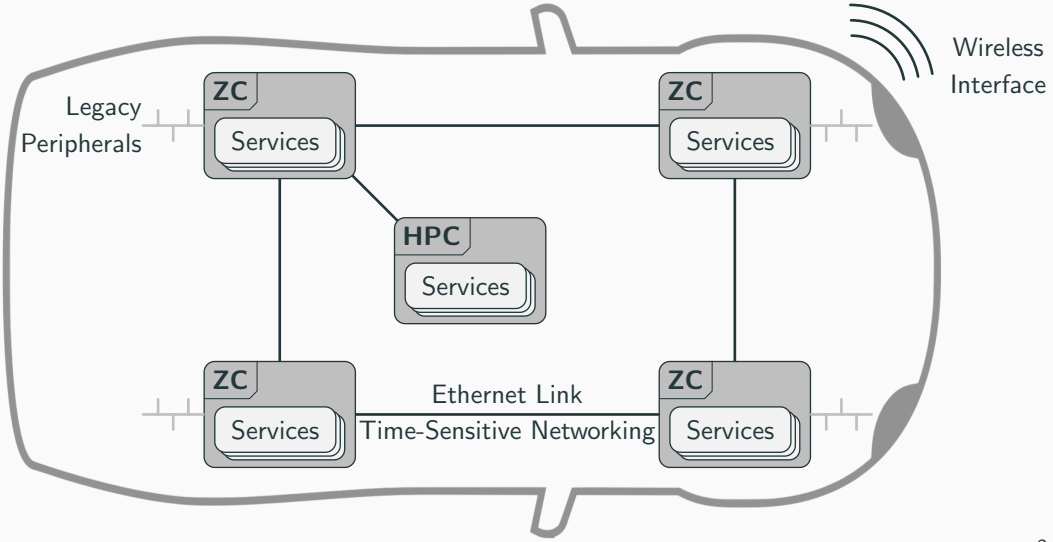
Future In-Vehicle Networks



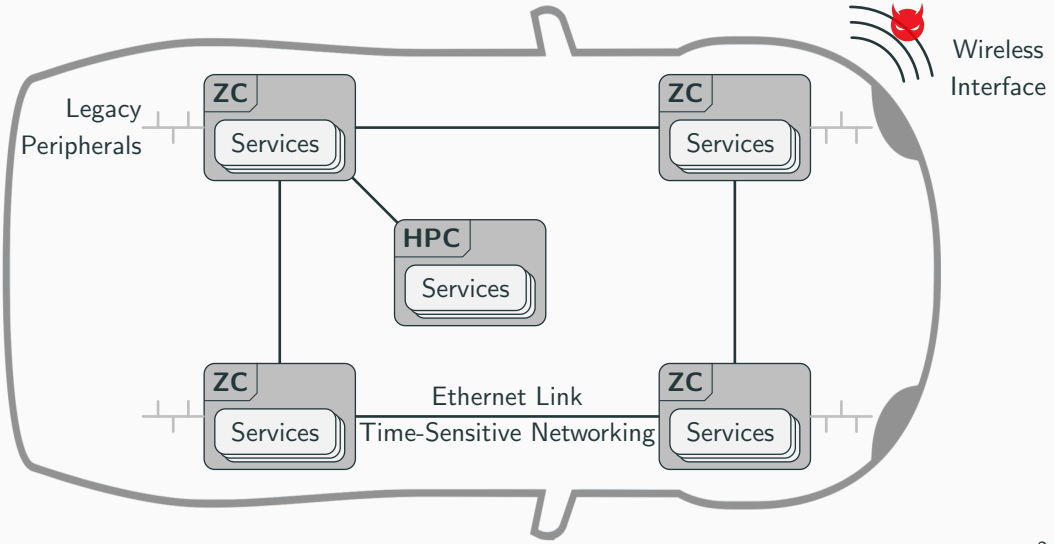
Future In-Vehicle Networks



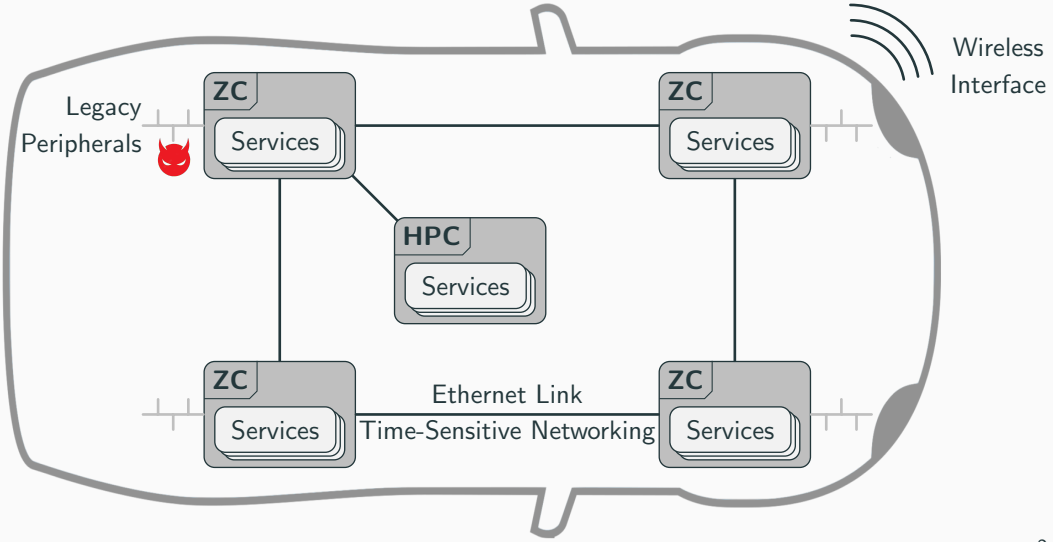
Future In-Vehicle Networks



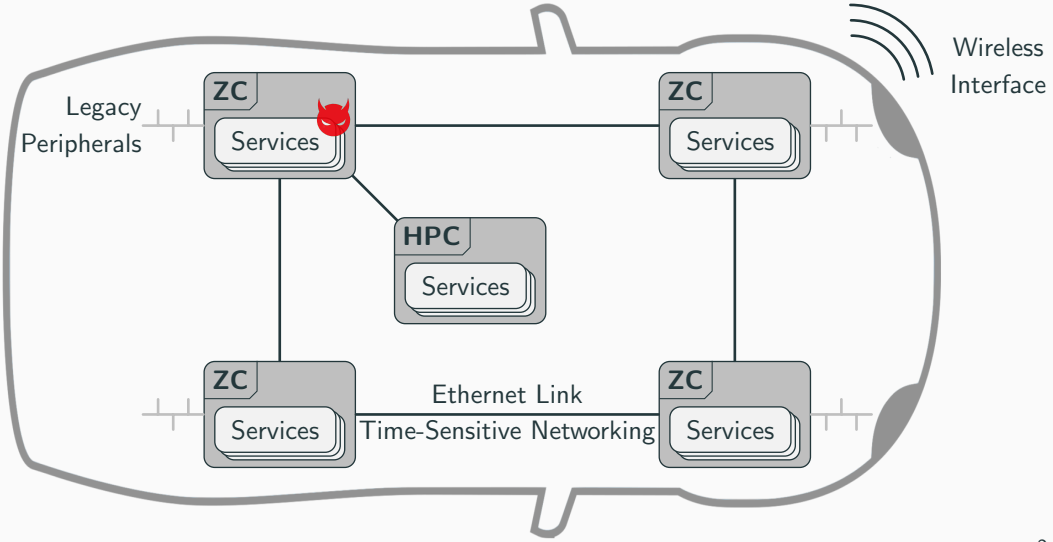
Future In-Vehicle Networks



Future In-Vehicle Networks



Future In-Vehicle Networks



Automotive Security Issues

Automotive Security Issues

- Previous automotive protocols target closed network environments – no security

Automotive Security Issues

- Previous automotive protocols target closed network environments – no security
- SOME/IP is a widely accepted automotive SOA middleware

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

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

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
  - No confidentiality or encryption of SOME/IP traffic

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
  - No confidentiality or encryption of SOME/IP traffic

- Related work introduces custom security measures based on pre-deployed certificates

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
  - No confidentiality or encryption of SOME/IP traffic

- Related work introduces custom security measures based on pre-deployed certificates
- Not proven, complex in managing and updating certificates

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
  - No confidentiality or encryption of SOME/IP traffic

- 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

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
  - No confidentiality or encryption of SOME/IP traffic

- 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
- Common network traffic encryption on the Internet bases on DH including PFS

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
  - No confidentiality or encryption of SOME/IP traffic

- 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
- Common network traffic encryption on the Internet bases on DH including PFS
- Related work introduces group key agreement based on DH including PFS

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
  - No confidentiality or encryption of SOME/IP traffic

- 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
- Common network traffic encryption on the Internet bases on DH including PFS
- Related work introduces group key agreement based on DH including PFS

$\rightarrow$ DNSSEC with DANE feature robust service authenticity w/ certificate and key management

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
  - No confidentiality or encryption of SOME/IP traffic

- 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
- Common network traffic encryption on the Internet bases on DH including PFS
- Related work introduces group key agreement based on DH including PFS

→ DNSSEC with DANE feature robust service authenticity w/ certificate and key management
→ DANCE supplements DNSSEC with DANE by client authenticity

Automotive Security Issues

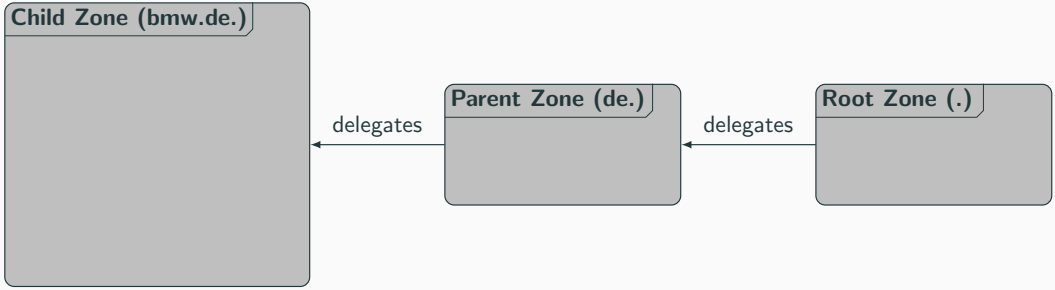
- Previous automotive protocols target closed network environments – no security
- SOME/IP is a widely accepted automotive SOA middleware
  - Provides a complementary service discovery protocol
  - Service discovery lack security mechanisms
  - No confidentiality or encryption of SOME/IP traffic

- 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
- Common network traffic encryption on the Internet bases on DH including PFS
- Related work introduces group key agreement based on DH including PFS

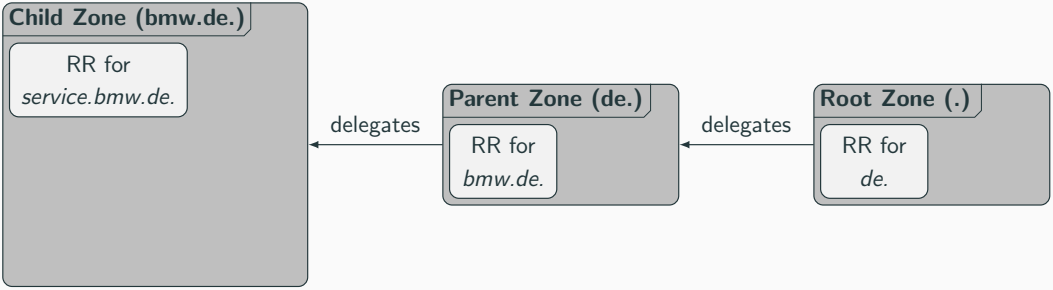
→ DNSSEC with DANE feature robust service authenticity w/ certificate and key management
→ DANCE supplements DNSSEC with DANE by client authenticity
→ GKA scheme following DH-based PFS like in TLS 1.3 or DTLS 1.3

Service and Client Authenticity Based on DNSSEC and DANE

Service and Client Authenticity Based on DNSSEC and DANE

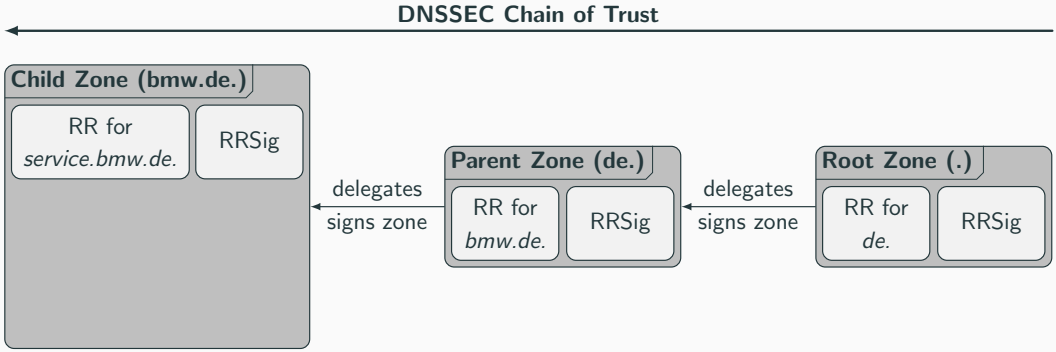


Service and Client Authenticity Based on DNSSEC and DANE



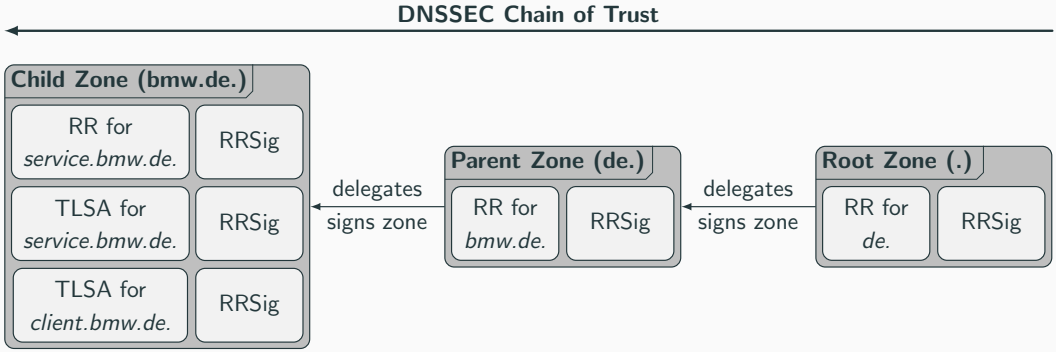
- Resource Records (RRs) contain endpoint information

Service and Client Authenticity Based on DNSSEC and DANE



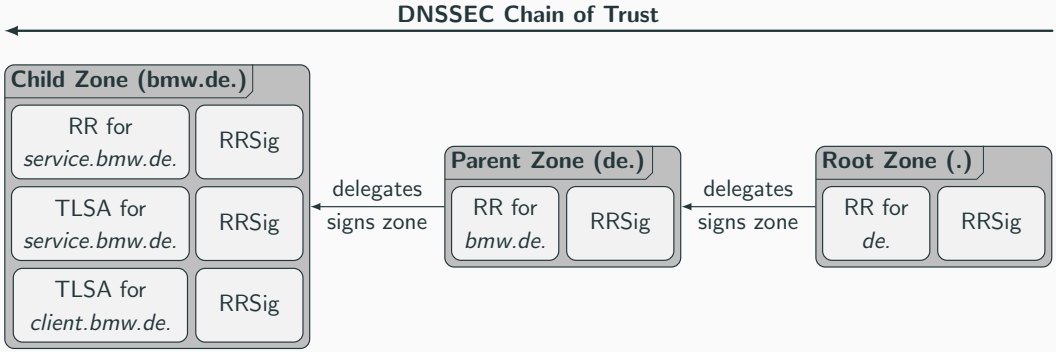
- Resource Records (RRs) contain endpoint information
- DNSSEC ensures integrity and authenticity of all RRs with signature records (RRSigs)

Service and Client Authenticity Based on DNSSEC and DANE



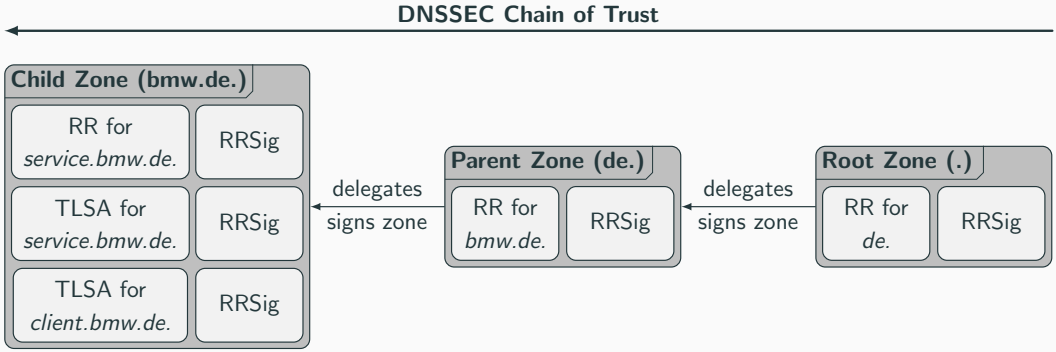
- Resource Records (RRs) contain endpoint information
- DNSSEC ensures integrity and authenticity of all RRs with signature records (RRSigs)
- DANE introduces TLSA RR to store certificates

Service and Client Authenticity Based on DNSSEC and DANE



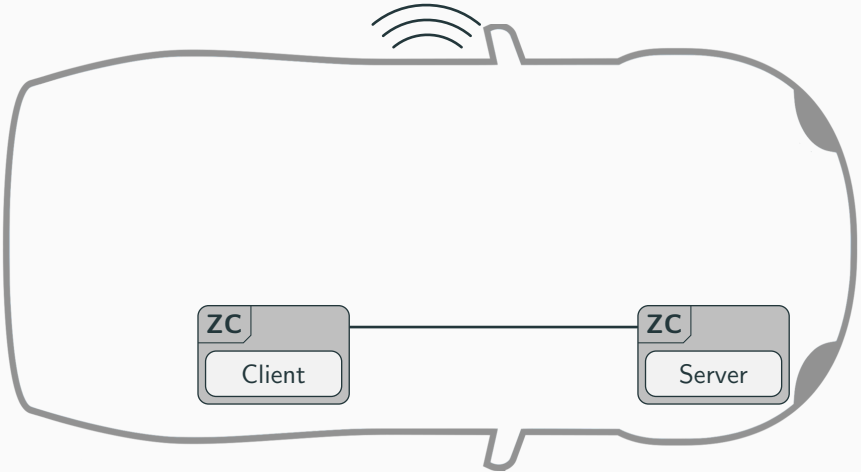
- Resource Records (RRs) contain endpoint information
- DNSSEC ensures integrity and authenticity of all RRs with signature records (RRSigs)
- DANE introduces TLSA RR to store certificates
- Robust security solution with established key and certificate management mechanisms

Service and Client Authenticity Based on DNSSEC and DANE

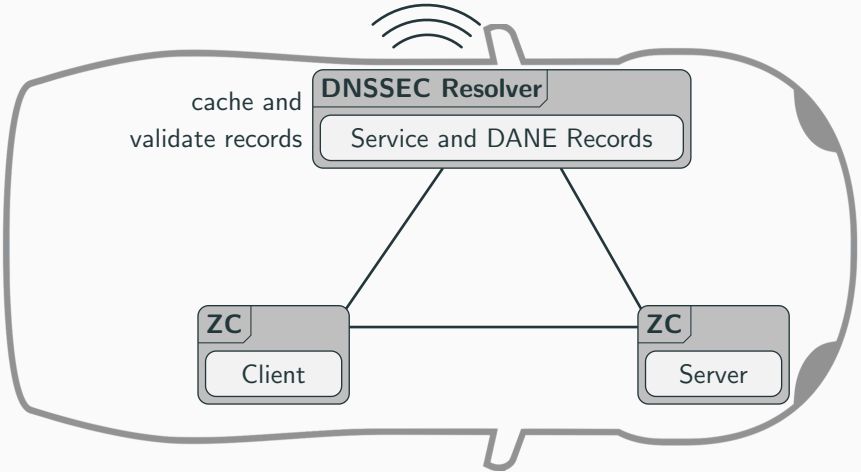


- Resource Records (RRs) contain endpoint information
- DNSSEC ensures integrity and authenticity of all RRs with signature records (RRSigs)
- DANE introduces TLSA RR to store certificates
- Robust security solution with established key and certificate management mechanisms
- Possibility for private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

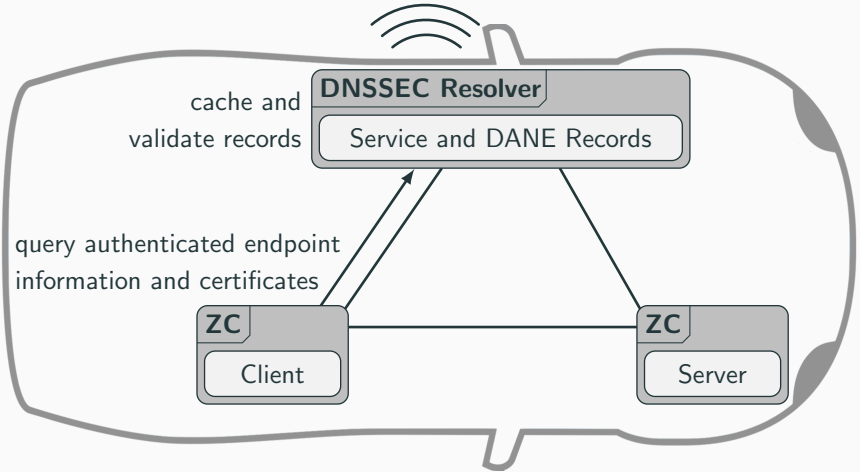
Envisioned Deployment Scenario



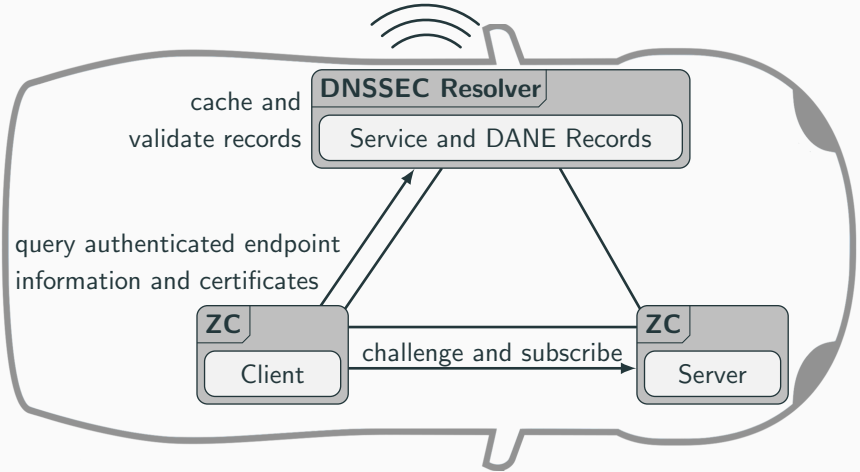
Envisioned Deployment Scenario



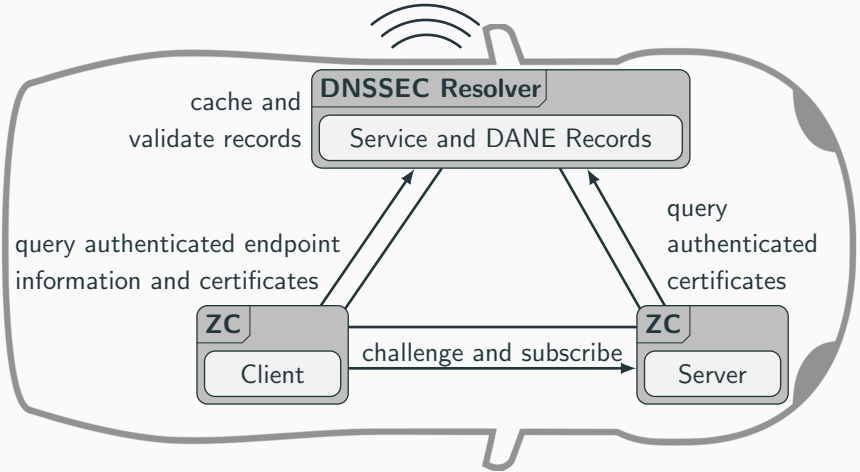
Envisioned Deployment Scenario



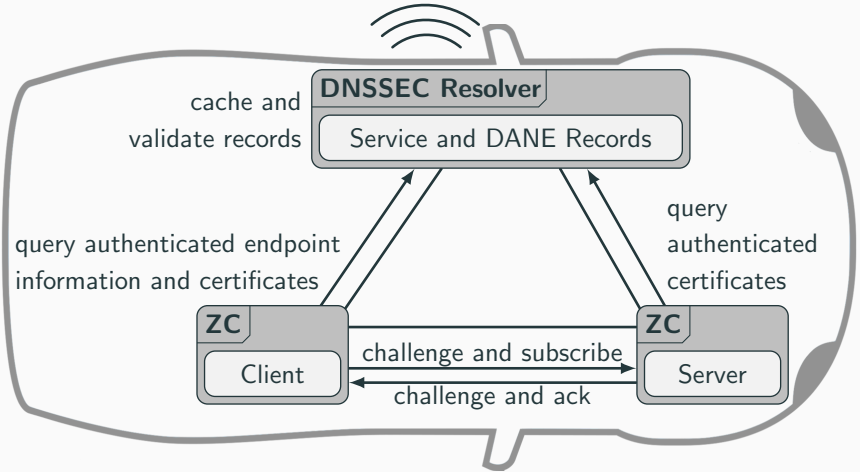
Envisioned Deployment Scenario



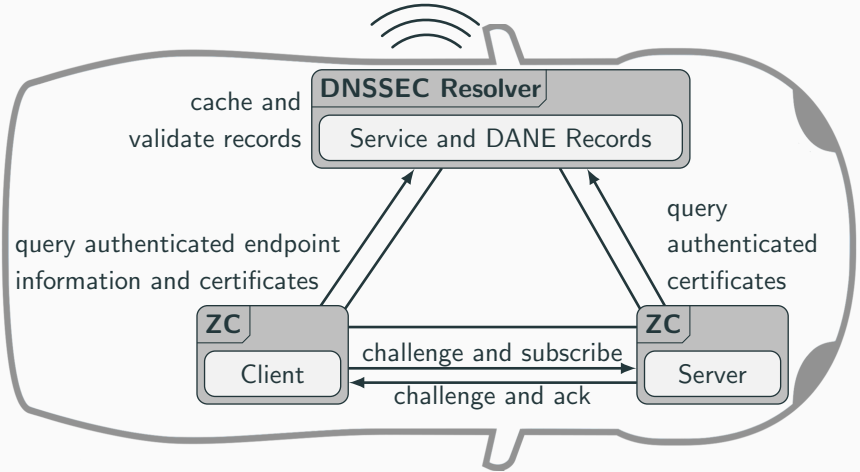
Envisioned Deployment Scenario



Envisioned Deployment Scenario

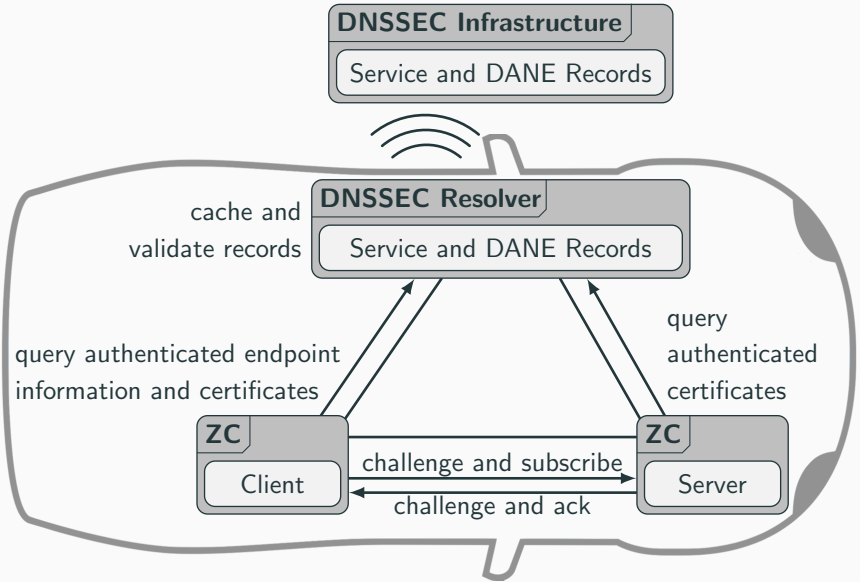


Envisioned Deployment Scenario



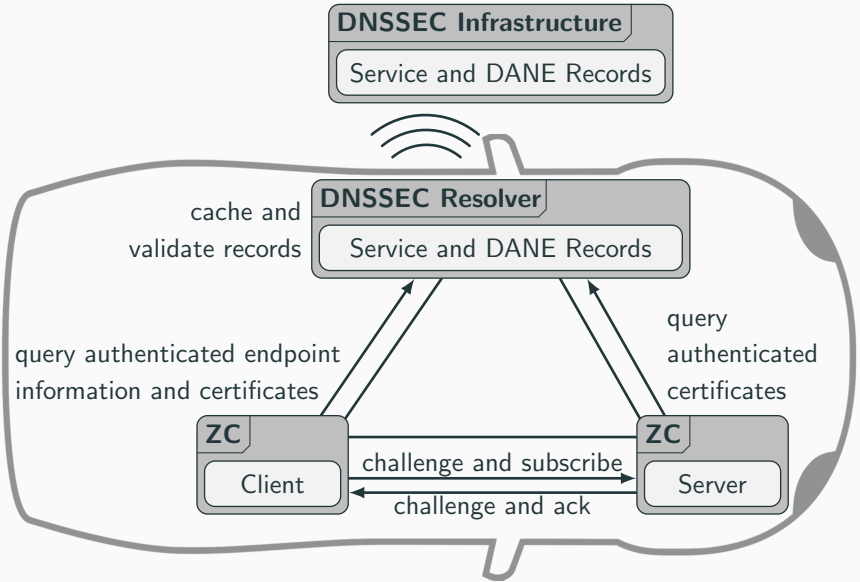
→ **Offline operation w/o pre-deployed certificates**

Envisioned Deployment Scenario



→ **Offline operation w/o pre-deployed certificates**

Envisioned Deployment Scenario



→ **Offline operation w/o pre-deployed certificates**

→ **Secure, established update scheme**

Group Key Agreement

Group Key Agreement

- Internet standards TLS 1.3 and DTLS 1.3 use DH-based PFS for key agreement

Group Key Agreement

- Internet standards TLS 1.3 and DTLS 1.3 use DH-based PFS for key agreement
- TLS 1.3 and DTLS 1.3 do not support management of group keys or GKA schemes

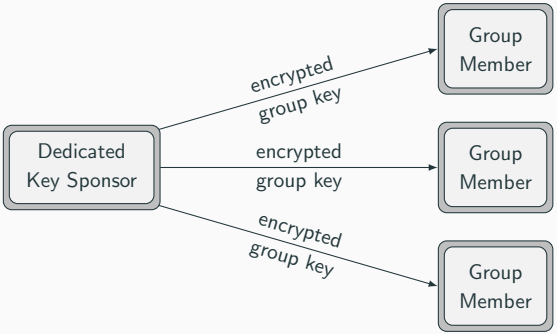
Group Key Agreement

- Internet standards TLS 1.3 and DTLS 1.3 use DH-based PFS for key agreement
- TLS 1.3 and DTLS 1.3 do not support management of group keys or GKA schemes
- Re-keying is done while the car is not operating (e.g., idling, reconfiguring, updating, charging etc.)

Group Key Agreement

- Internet standards TLS 1.3 and DTLS 1.3 use DH-based PFS for key agreement
- TLS 1.3 and DTLS 1.3 do not support management of group keys or GKA schemes
- Re-keying is done while the car is not operating (e.g., idling, reconfiguring, updating, charging etc.)

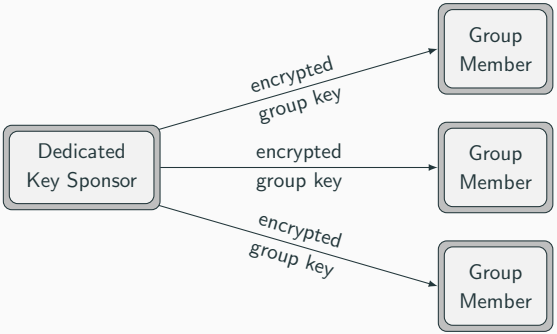
GKA schemes fall generally into three categories: **Centralized**



Group Key Agreement

- Internet standards TLS 1.3 and DTLS 1.3 use DH-based PFS for key agreement
- TLS 1.3 and DTLS 1.3 do not support management of group keys or GKA schemes
- Re-keying is done while the car is not operating (e.g., idling, reconfiguring, updating, charging etc.)

GKA schemes fall generally into three categories: **Centralized**

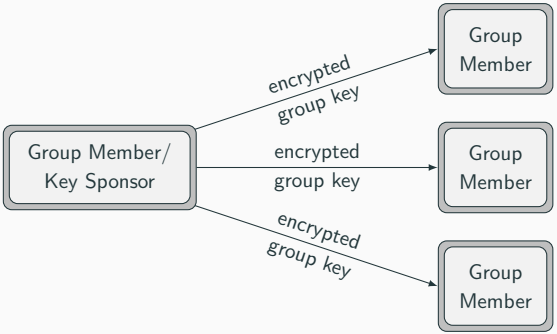


→ Less load on group members, but SPOF

Group Key Agreement

- Internet standards TLS 1.3 and DTLS 1.3 use DH-based PFS for key agreement
- TLS 1.3 and DTLS 1.3 do not support management of group keys or GKA schemes
- Re-keying is done while the car is not operating (e.g., parking, idling, reconfiguring, updating, charging etc.)

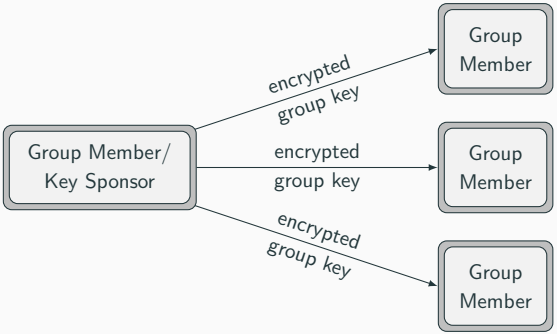
GKA schemes fall generally into three categories: Centralized, **Distributed**



Group Key Agreement

- Internet standards TLS 1.3 and DTLS 1.3 use DH-based PFS for key agreement
- TLS 1.3 and DTLS 1.3 do not support management of group keys or GKA schemes
- Re-keying is done while the car is not operating (e.g., parking, idling, reconfiguring, updating, charging etc.)

GKA schemes fall generally into three categories: Centralized, **Distributed**

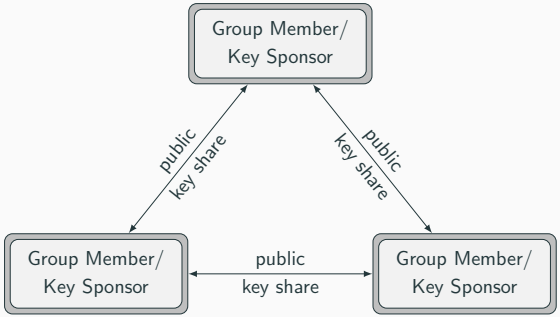


→ More load on group members who sponsor the group key, but is more robust against host failures

Group Key Agreement

- Internet standards TLS 1.3 and DTLS 1.3 use DH-based PFS for key agreement
- TLS 1.3 and DTLS 1.3 do not support management of group keys or GKA schemes
- Re-keying is done while the car is not operating (e.g., parking, idling, reconfiguring, updating, charging etc.)

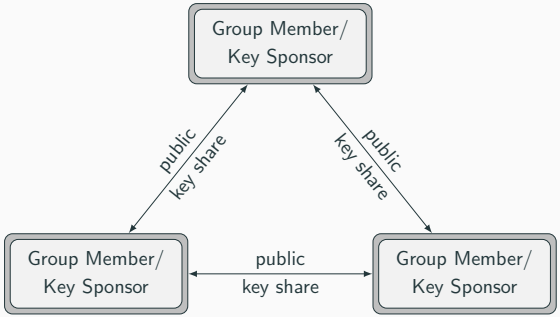
GKA schemes fall generally into three categories: Centralized, Distributed, **Contributory**



Group Key Agreement

- Internet standards TLS 1.3 and DTLS 1.3 use DH-based PFS for key agreement
- TLS 1.3 and DTLS 1.3 do not support management of group keys or GKA schemes
- Re-keying is done while the car is not operating (e.g., parking, idling, reconfiguring, updating, charging etc.)

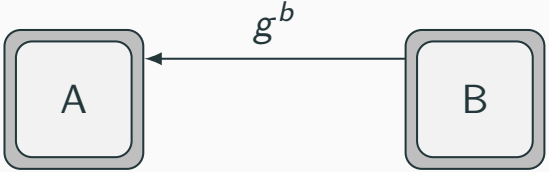
GKA schemes fall generally into three categories: Centralized, Distributed, **Contributory**



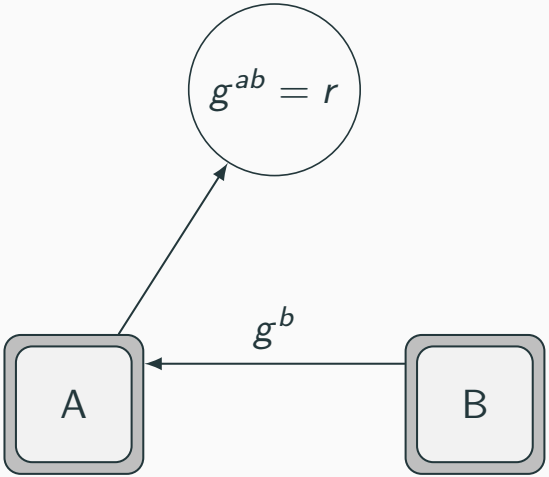
→ More load on all group members since all of them are involved and additional communication rounds for synchronizing, but allows key agreement without a secure channel (e.g., DH)

Distributed Diffie-Hellman Group Key Agreement Example

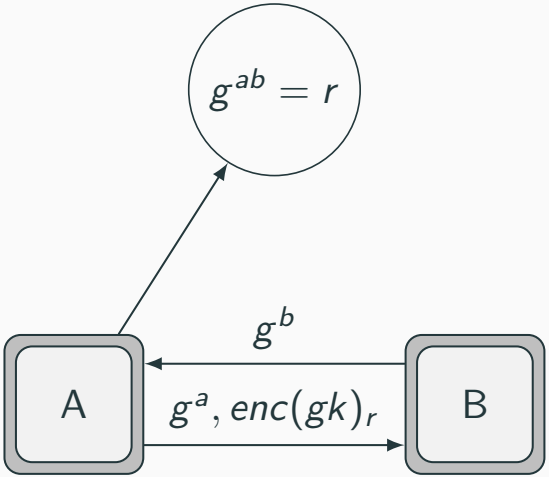
Distributed Diffie-Hellman Group Key Agreement Example



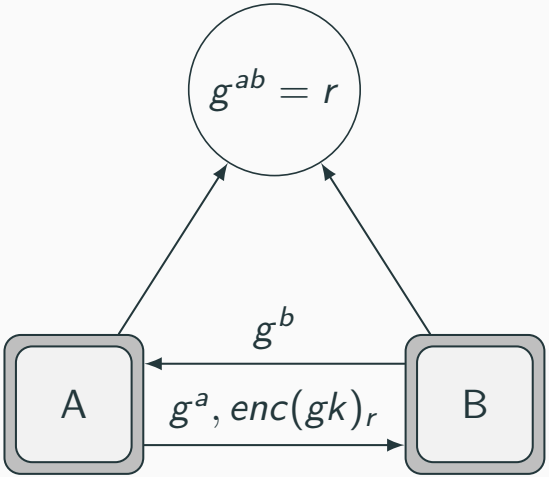
Distributed Diffie-Hellman Group Key Agreement Example



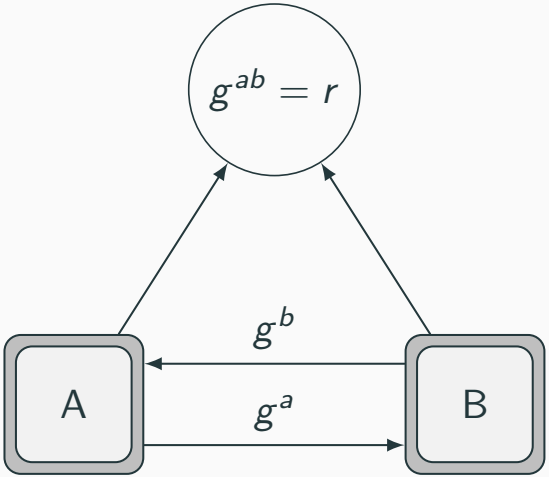
Distributed Diffie-Hellman Group Key Agreement Example



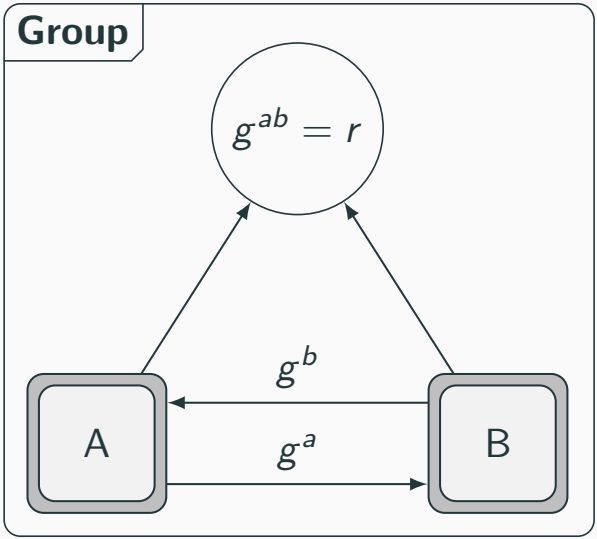
Distributed Diffie-Hellman Group Key Agreement Example



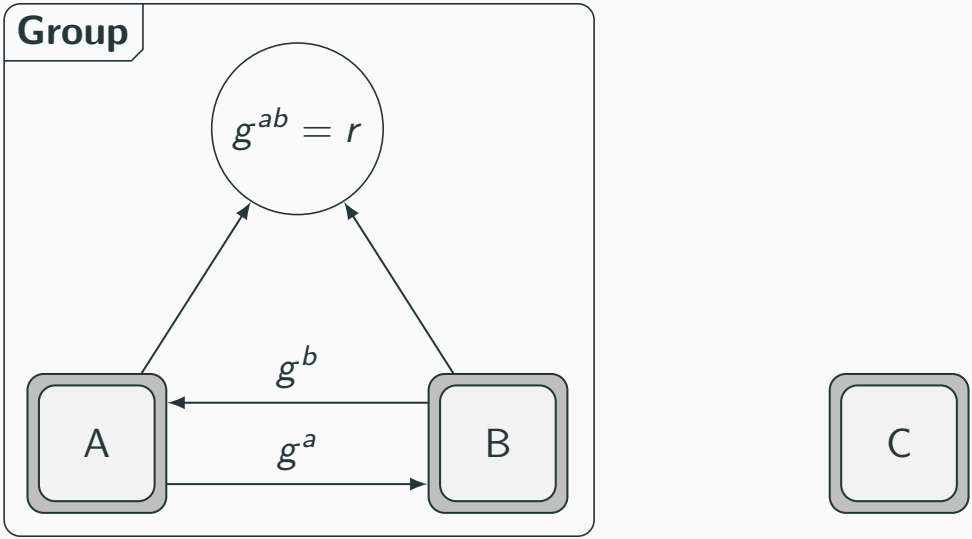
Contributory Diffie-Hellman Group Key Agreement Example



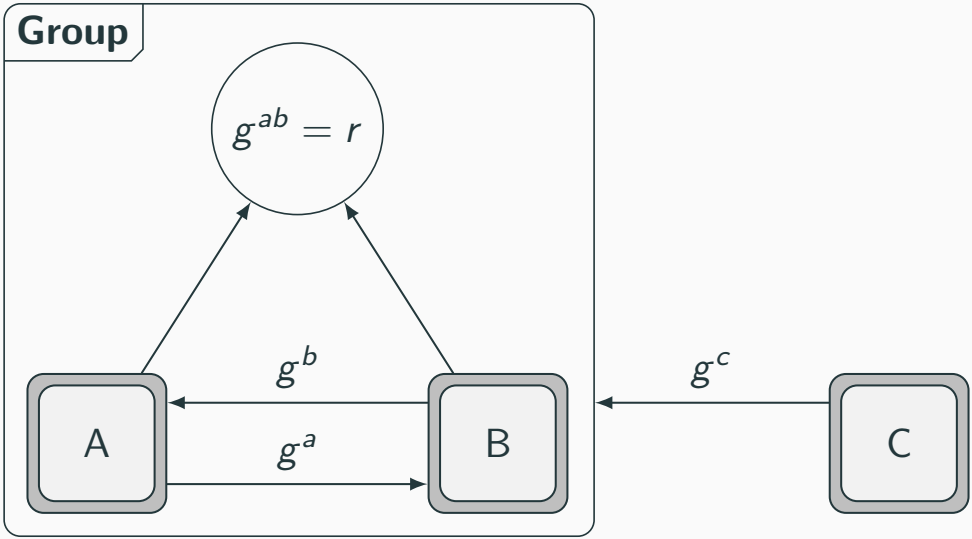
Contributory Diffie-Hellman Group Key Agreement Example



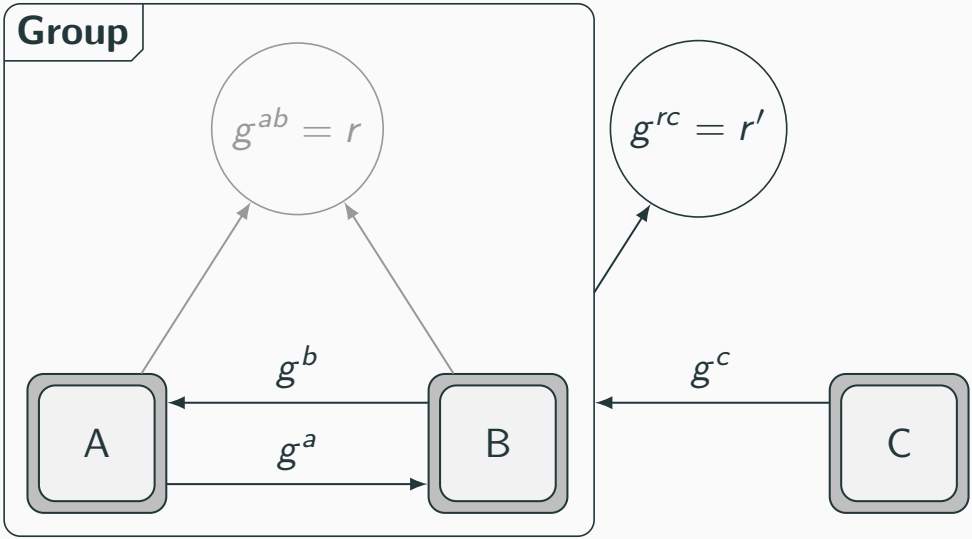
Contributory Diffie-Hellman Group Key Agreement Example



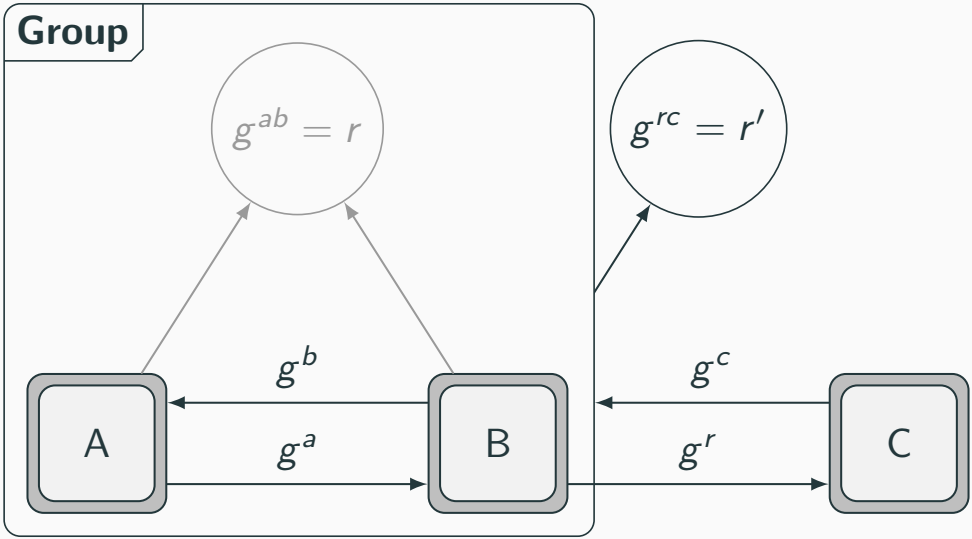
Contributory Diffie-Hellman Group Key Agreement Example



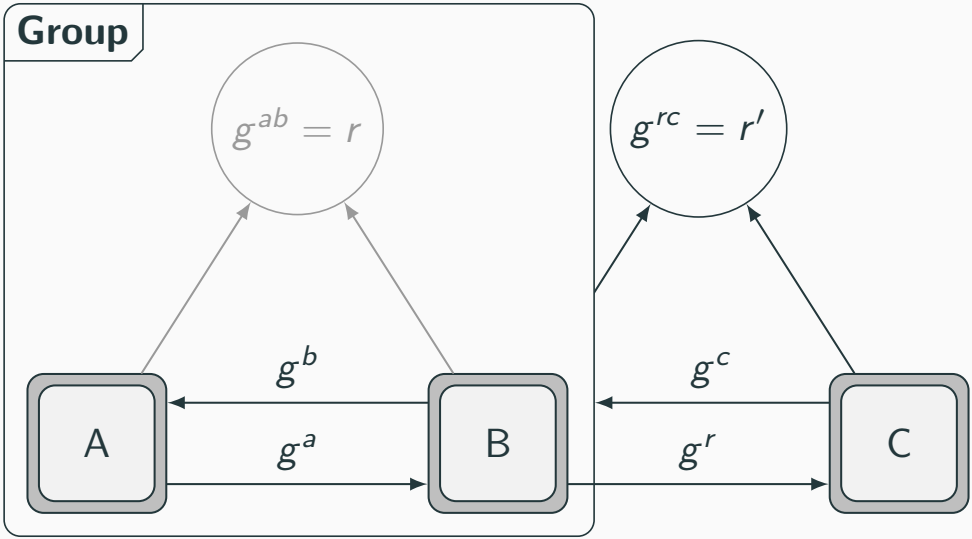
Contributory Diffie-Hellman Group Key Agreement Example



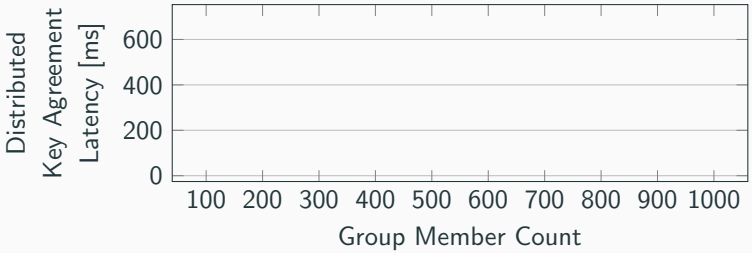
Contributory Diffie-Hellman Group Key Agreement Example

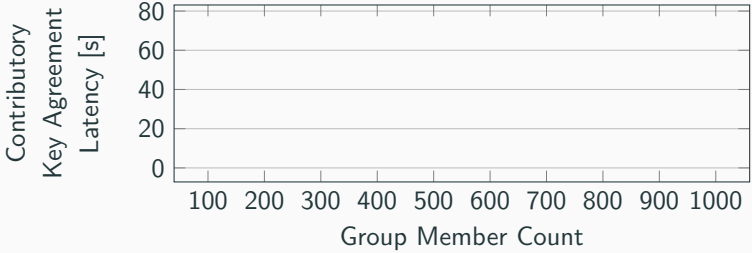


Contributory Diffie-Hellman Group Key Agreement Example

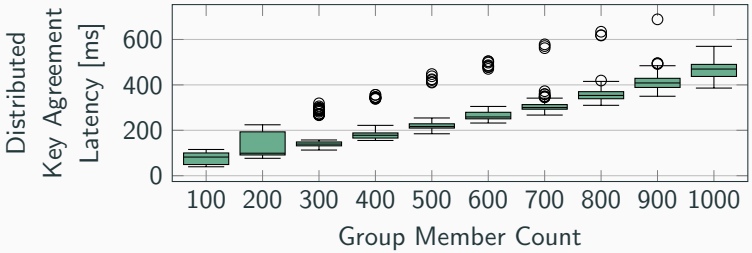


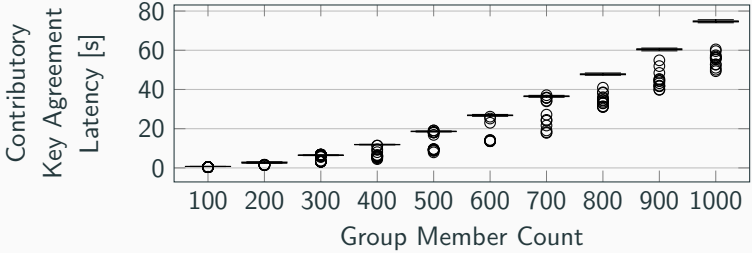
Diffie-Hellman Performance: Distributed vs. Contributory



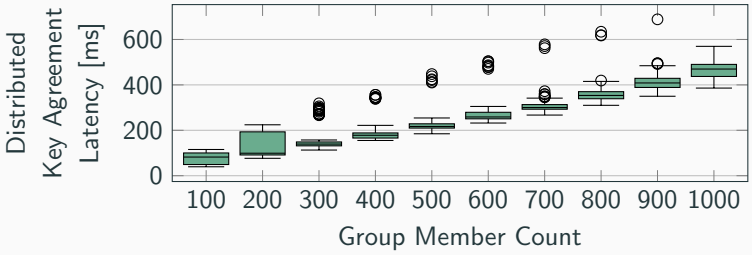


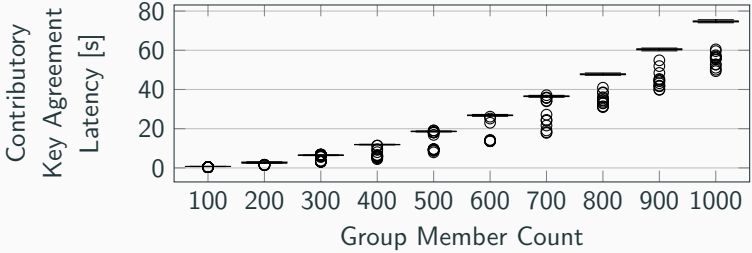
Diffie-Hellman Performance: Distributed vs. Contributory





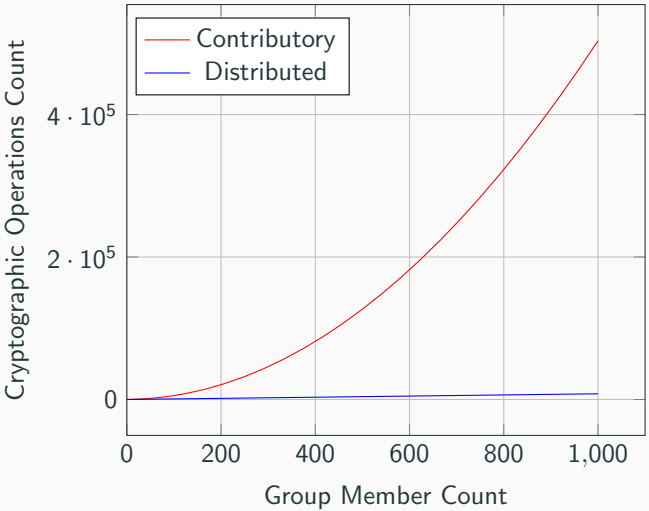
Diffie-Hellman Performance: Distributed vs. Contributory



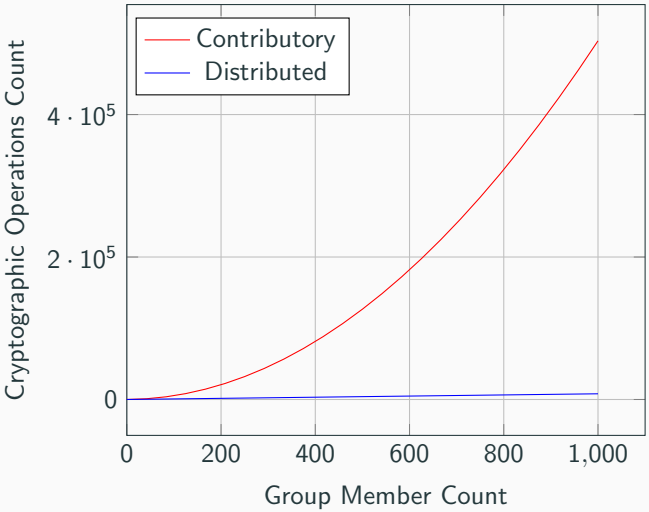


→ **The distributed key agreement latency remains in the ms range while the contributory key agreement begins significantly earlier in the seconds range**

Diffie-Hellman Cryptographic Operations Count: Distributed vs. Contributory

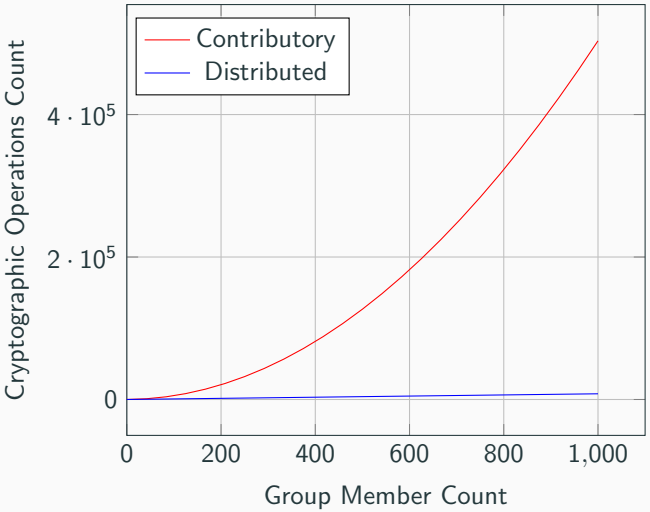


Diffie-Hellman Cryptographic Operations Count: Distributed vs. Contributory



→ **The distributed approach involves just the key sponsor and the joining group member**

Diffie-Hellman Cryptographic Operations Count: Distributed vs. Contributory

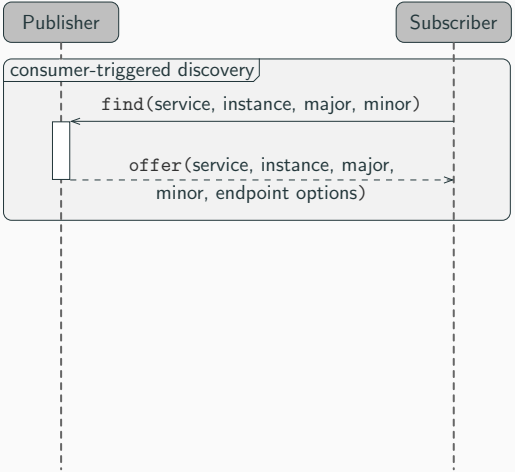


→ **The distributed approach involves just the key sponsor and the joining group member**

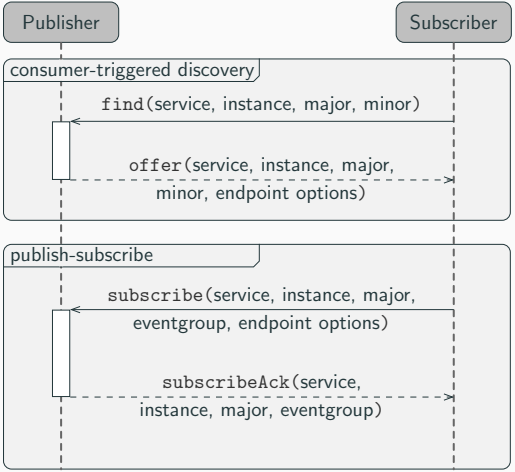
→ **The contributory approach also involves group members who have already joined in addition to the key sponsor and the joining group member**

SOME/IP Service Discovery

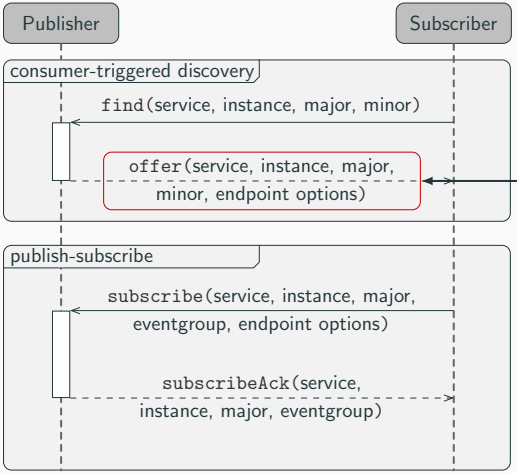
SOME/IP Service Discovery



SOME/IP Service Discovery

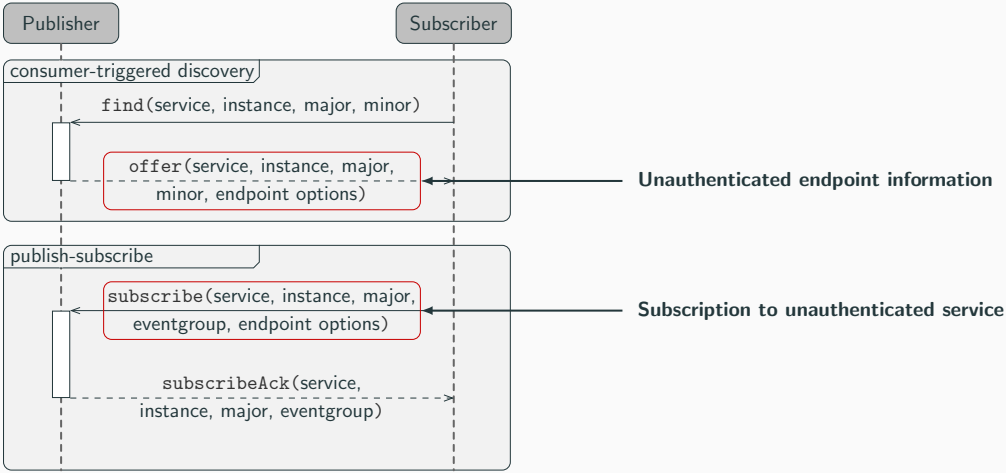


SOME/IP Service Discovery

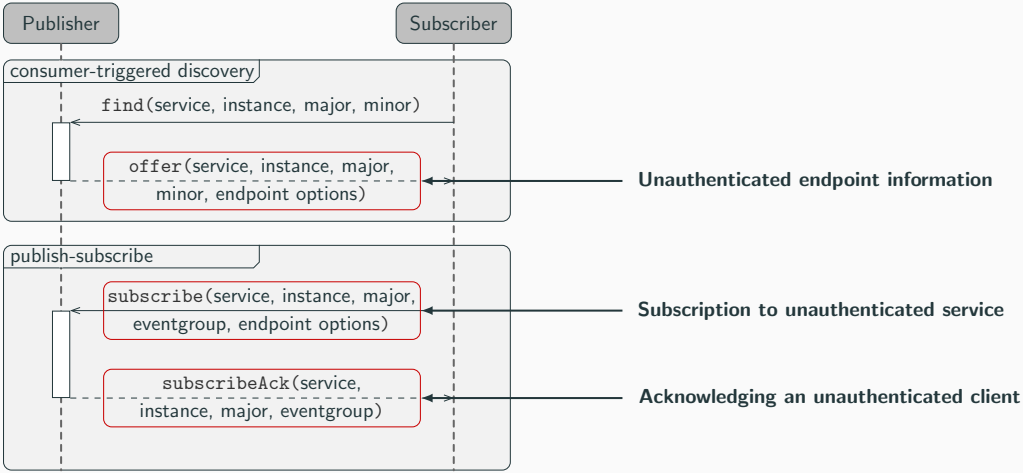


Unauthenticated endpoint information

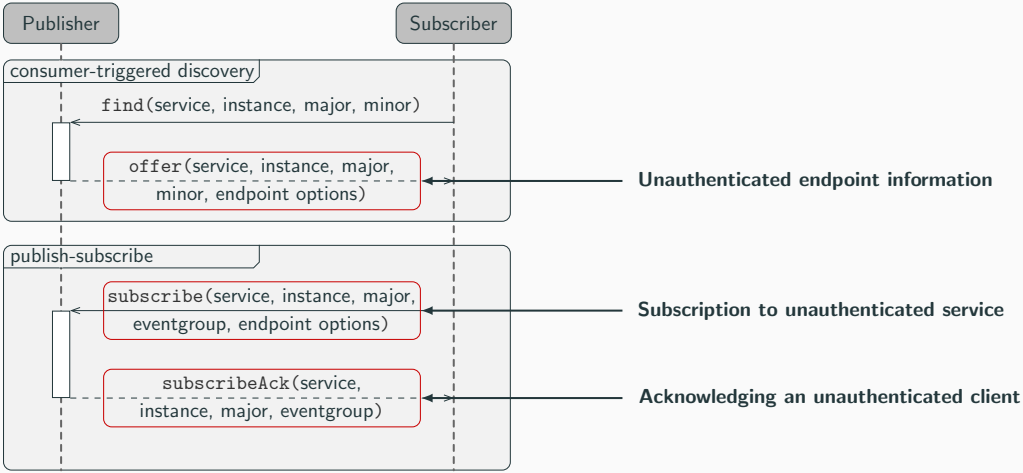
SOME/IP Service Discovery



SOME/IP Service Discovery

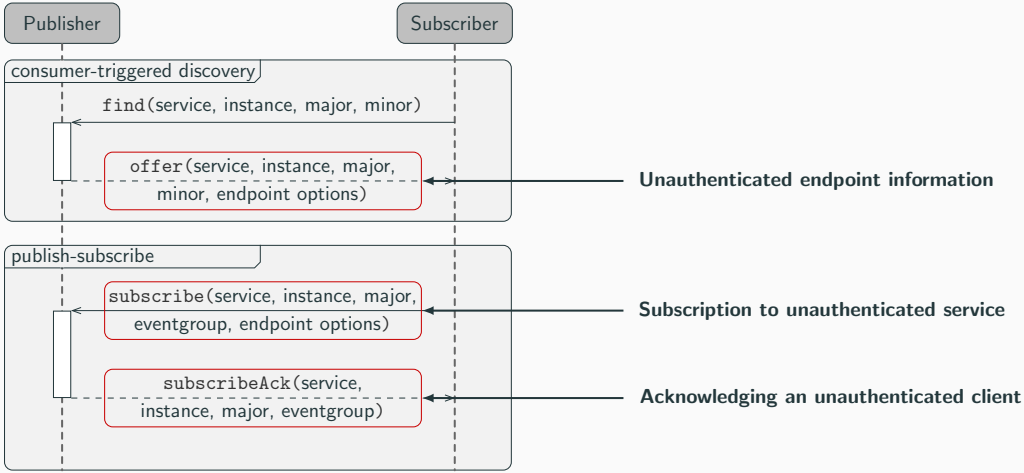


SOME/IP Service Discovery



→ **SOME/IP lacks authenticity, key agreement mechanisms and encryption**

SOME/IP Service Discovery

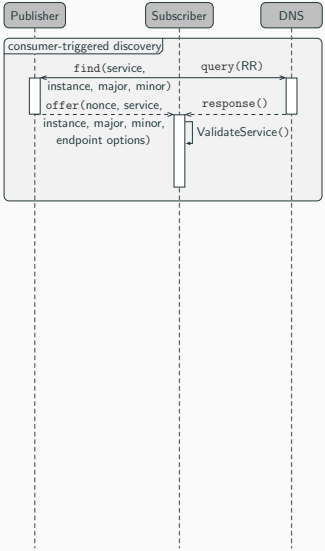


→ **SOME/IP lacks authenticity, key agreement mechanisms and encryption**

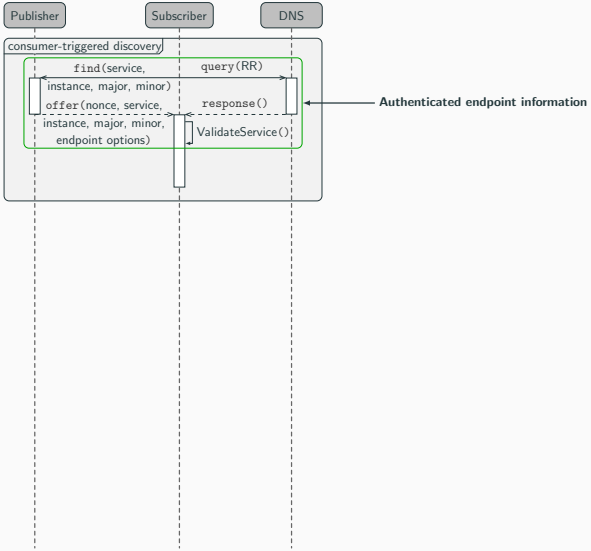
→ **Distributed DH GKA fits better than the contributory scheme**

Our Approach: DNSSEC and Distributed GKA in SOME/IP Service Discovery

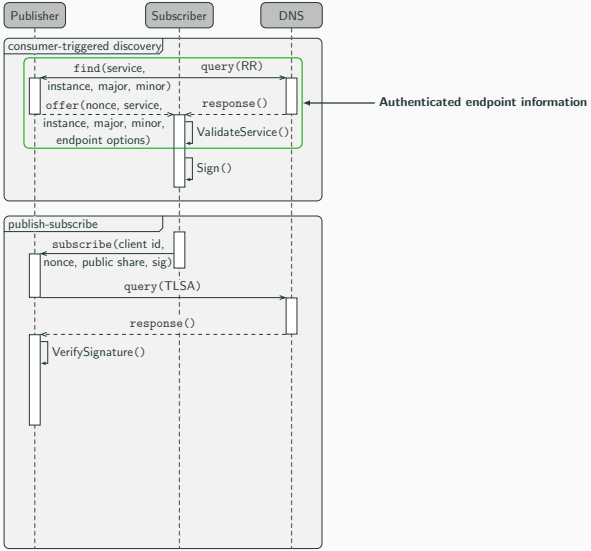
Our Approach: DNSSEC and Distributed GKA in SOME/IP Service Discovery



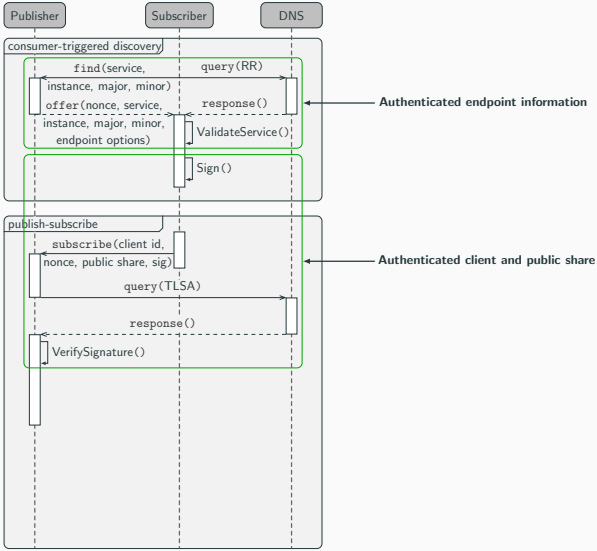
Our Approach: DNSSEC and Distributed GKA in SOME/IP Service Discovery



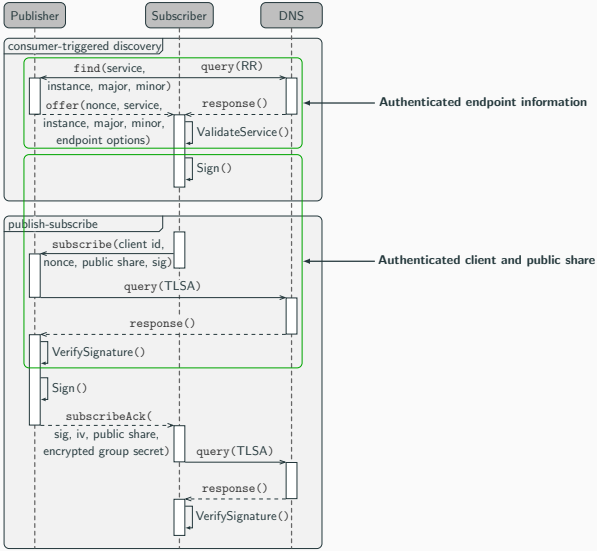
Our Approach: DNSSEC and Distributed GKA in SOME/IP Service Discovery



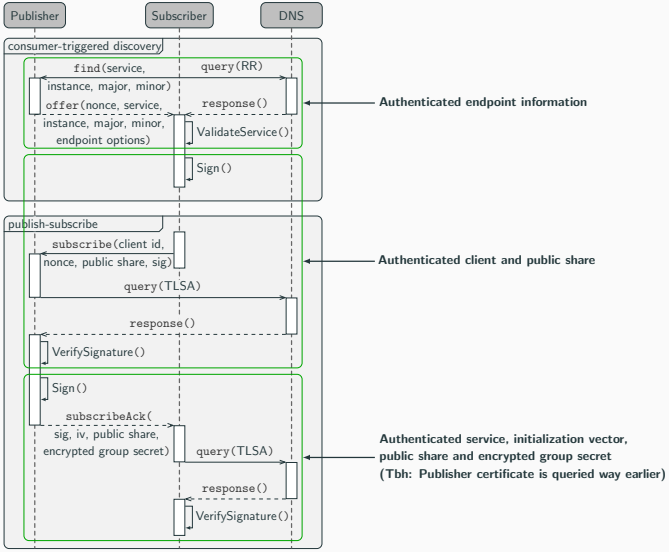
Our Approach: DNSSEC and Distributed GKA in SOME/IP Service Discovery



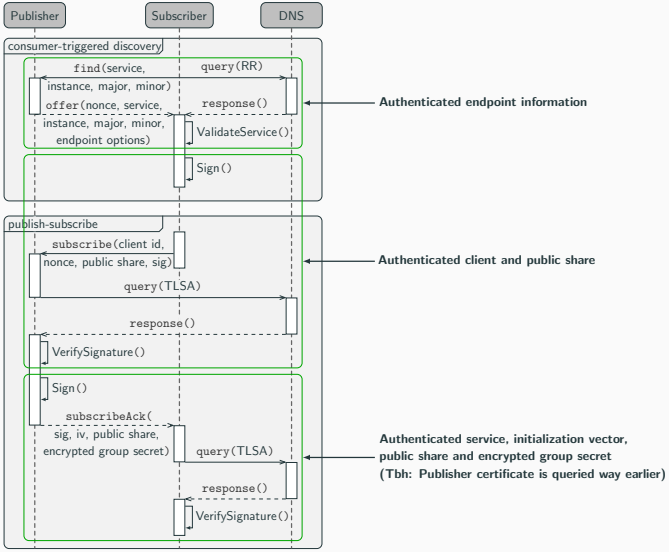
Our Approach: DNSSEC and Distributed GKA in SOME/IP Service Discovery



Our Approach: DNSSEC and Distributed GKA in SOME/IP Service Discovery

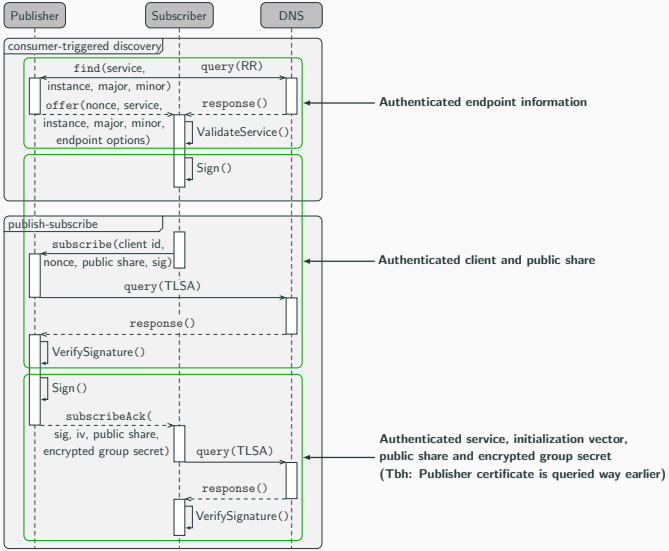


Our Approach: DNSSEC and Distributed GKA in SOME/IP Service Discovery



→ **DNSSEC with DANE ensures authenticity and integrity of endpoint information and certificates**

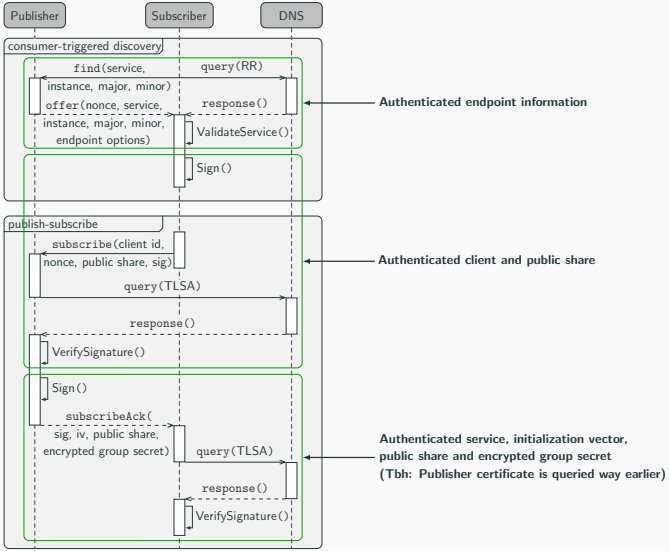
Our Approach: DNSSEC and Distributed GKA in SOME/IP Service Discovery



→ **DNSSEC with DANE ensures authenticity and integrity of endpoint information and certificates**

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

Our Approach: DNSSEC and Distributed GKA in SOME/IP Service Discovery



→ DNSSEC with DANE ensures authenticity and integrity of endpoint information and certificates

→ Challenge-response mechanism ensures publisher and subscriber authenticity

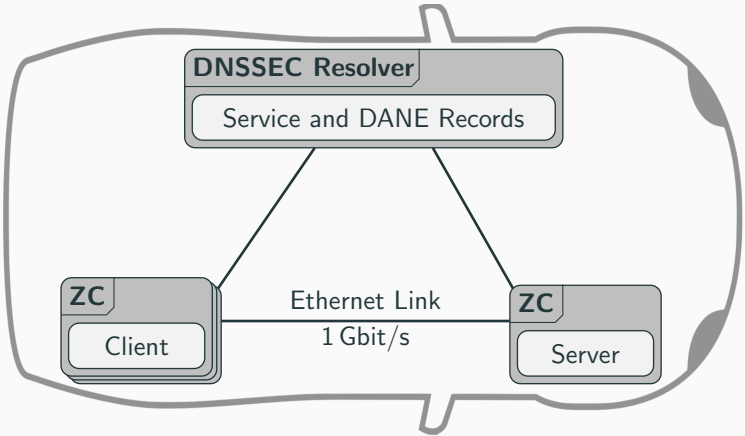
→ Seamless distributed Diffie-Hellman group key agreement enables encryption of subsequent SOME/IP session traffic

DNSSEC and GKA Implementation in SOME/IP Service Discovery

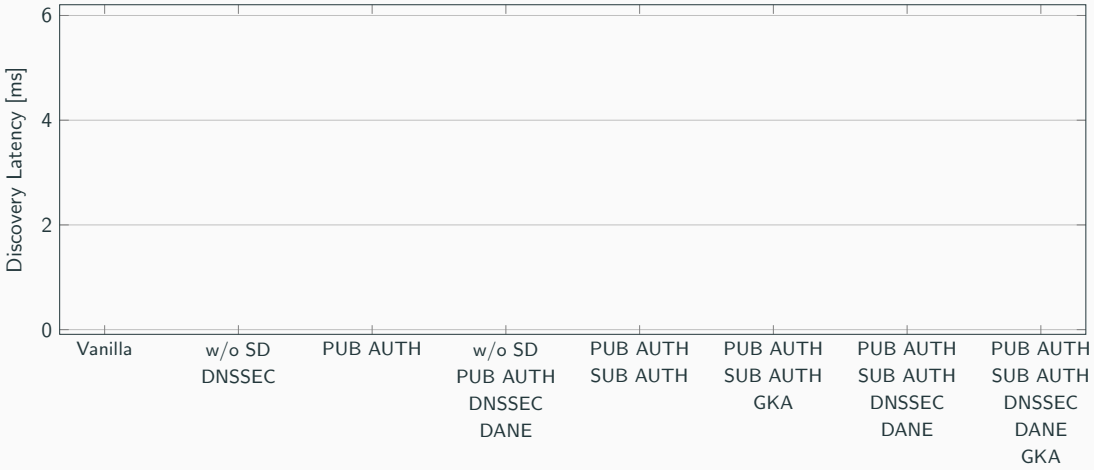
- Implementation based on vsomeip reference implementation
- Integrated standard DNS resolver in vsomeip
- Integrated standard cryptographic operations and algorithms for service and client authentication as well as for seamless distributed Diffie-Hellman group key agreement

DNSSEC and GKA Implementation in SOME/IP Service Discovery

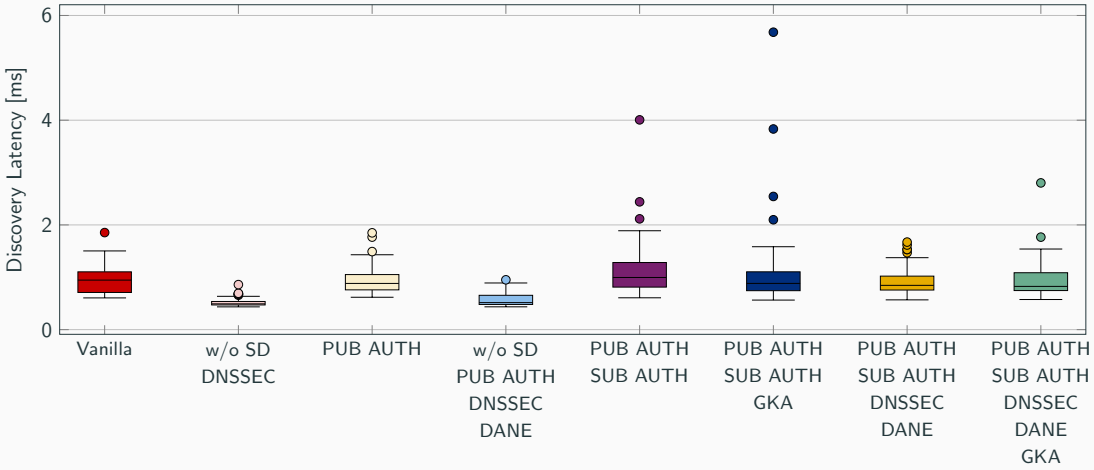
- Implementation based on vsomeip reference implementation
- Integrated standard DNS resolver in vsomeip
- Integrated standard cryptographic operations and algorithms for service and client authentication as well as for seamless distributed Diffie-Hellman group key agreement



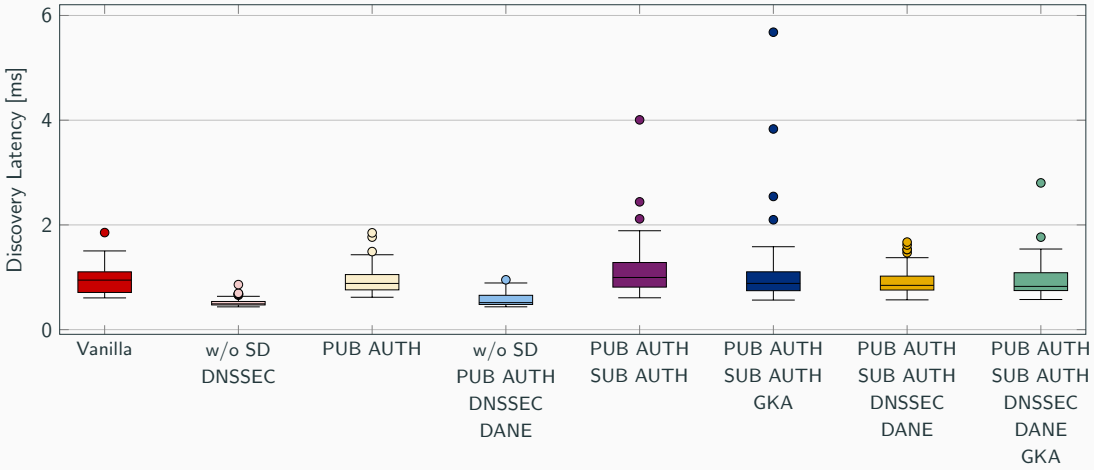
Performance Analysis Based on SOME/IP Reference Implementation with One Publisher and One Subscriber



Performance Analysis Based on SOME/IP Reference Implementation with One Publisher and One Subscriber

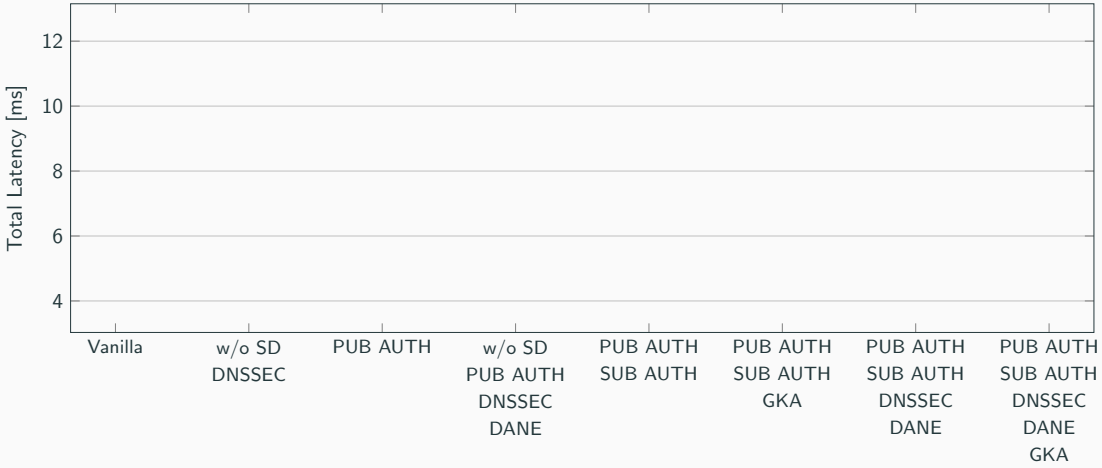


Performance Analysis Based on SOME/IP Reference Implementation with One Publisher and One Subscriber

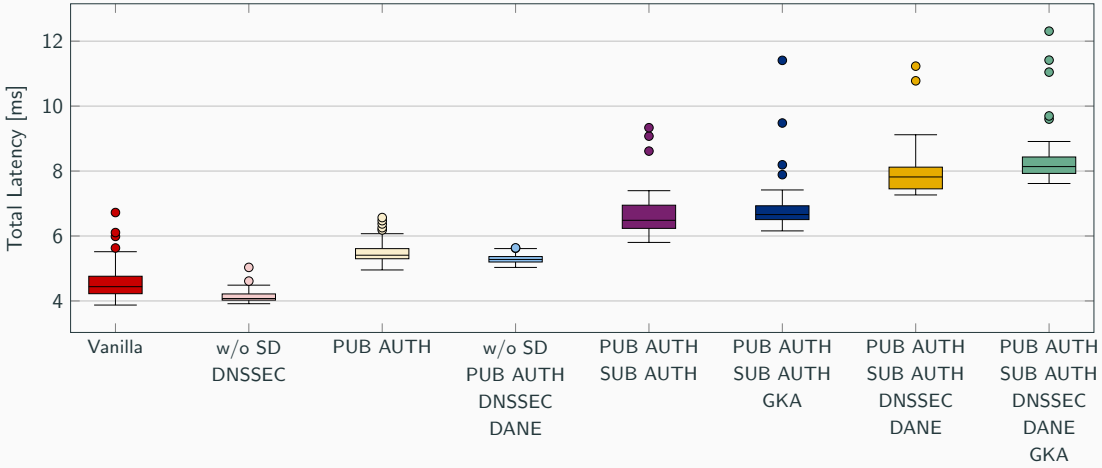


→ **No significant penalty on discovery performance**

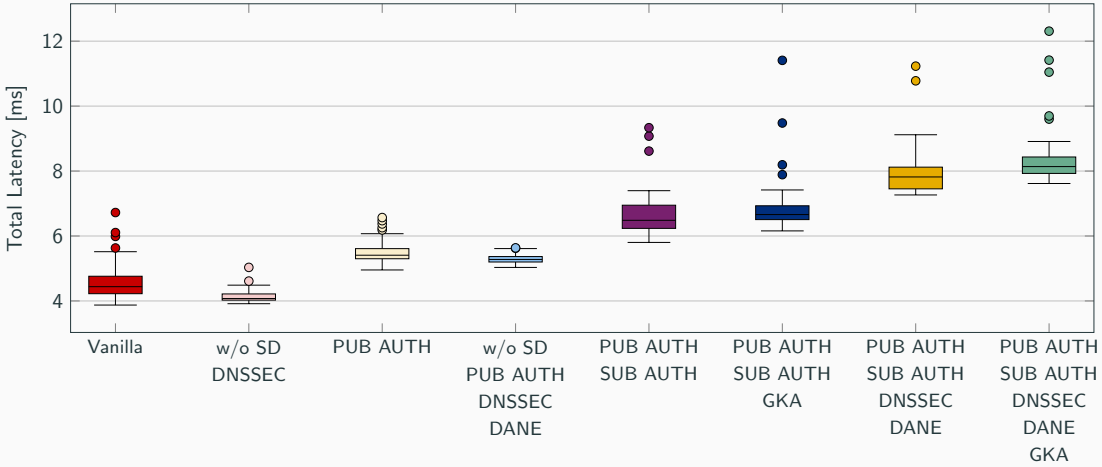
Performance Analysis Based on SOME/IP Reference Implementation with One Publisher and One Subscriber



Performance Analysis Based on SOME/IP Reference Implementation with One Publisher and One Subscriber

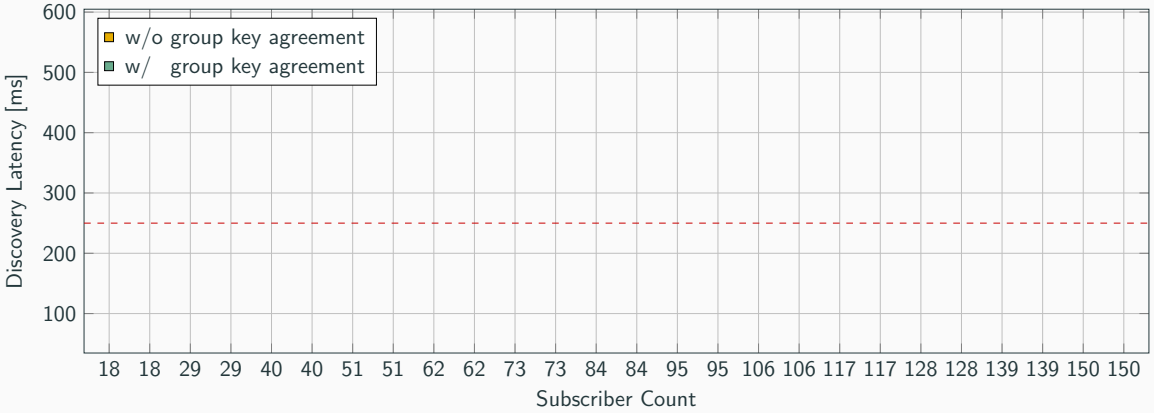


Performance Analysis Based on SOME/IP Reference Implementation with One Publisher and One Subscriber

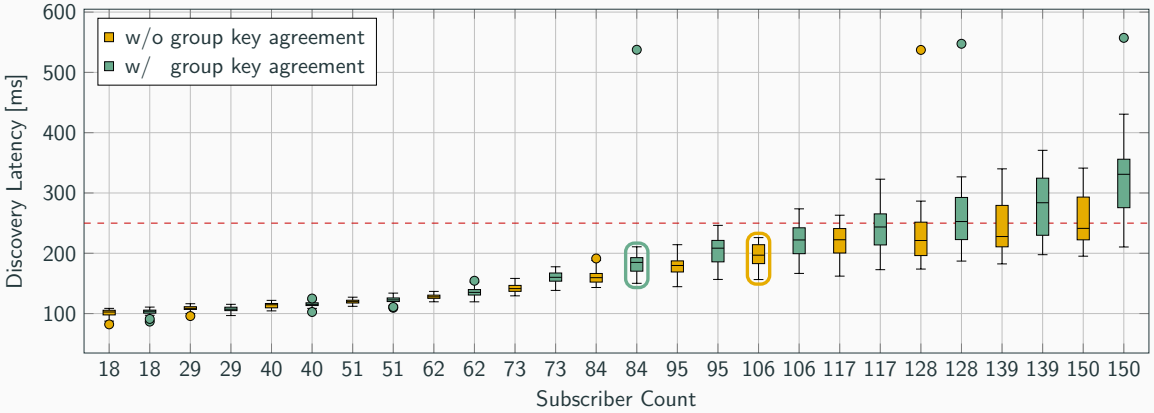


→ **Penalty in performance due to the request of subscriber certificates compared to pre-deployed certificates**

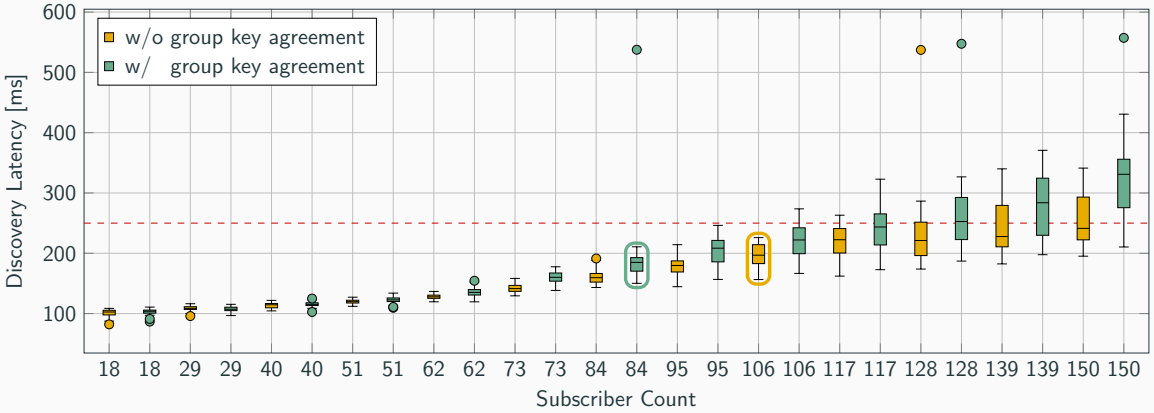
Performance Analysis Based on SOME/IP Reference Implementation with One Publisher and Multiple Subscribers (PUB/SUB AUTH, DNSSEC, DANE, GKA)



Performance Analysis Based on SOME/IP Reference Implementation with One Publisher and Multiple Subscribers (PUB/SUB AUTH, DNSSEC, DANE, GKA)

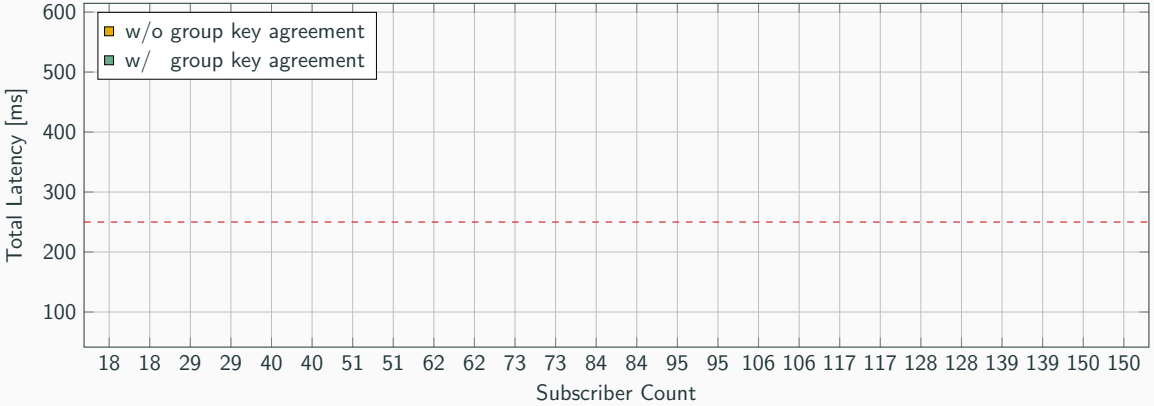


Performance Analysis Based on SOME/IP Reference Implementation with One Publisher and Multiple Subscribers (PUB/SUB AUTH, DNSSEC, DANE, GKA)

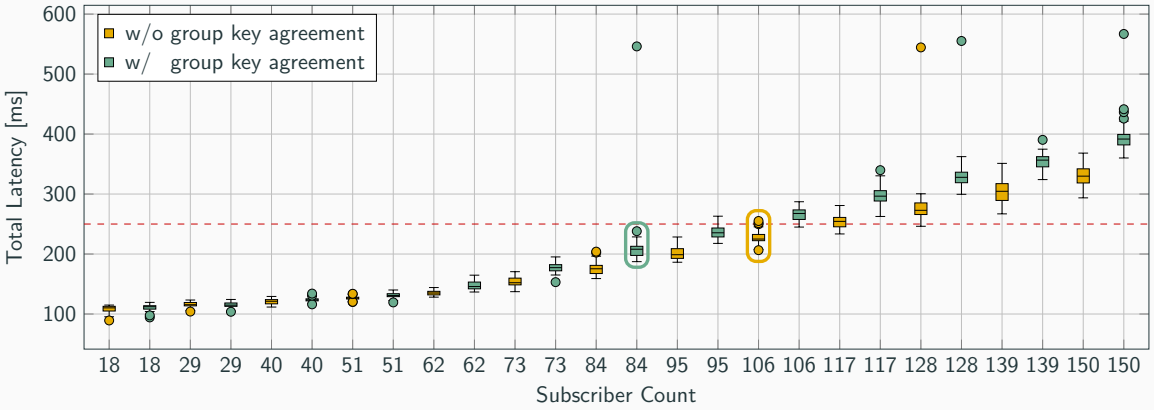


→ **Discovery latency for subscriber counts of 106 without GKA and 84 with GKA remain below the satisfactory user experience threshold**

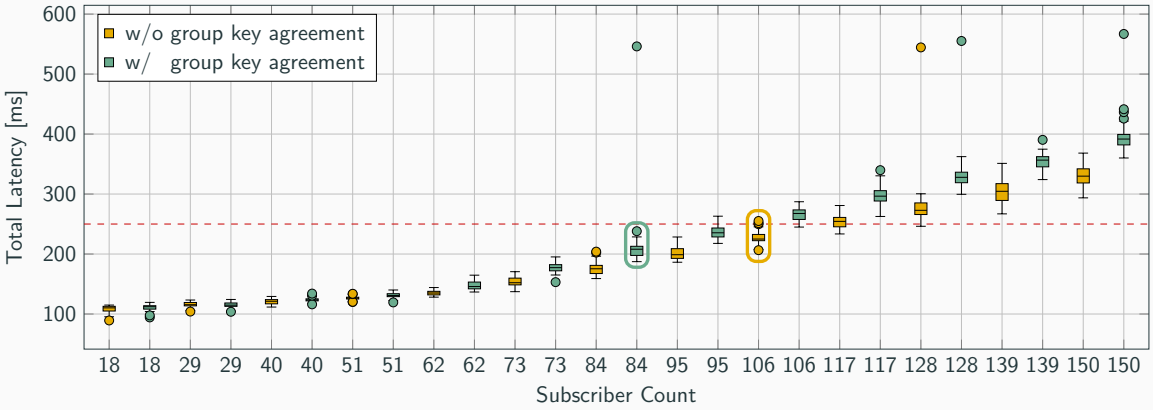
Performance Analysis Based on SOME/IP Reference Implementation with One Publisher and Multiple Subscribers (PUB/SUB AUTH, DNSSEC, DANE, GKA)



Performance Analysis Based on SOME/IP Reference Implementation with One Publisher and Multiple Subscribers (PUB/SUB AUTH, DNSSEC, DANE, GKA)



Performance Analysis Based on SOME/IP Reference Implementation with One Publisher and Multiple Subscribers (PUB/SUB AUTH, DNSSEC, DANE, GKA)



→ **Subscriber counts of 106 without GKA and 84 with GKA comply with satisfactory user experience, which likely improves with parallelization on actual nodes and cryptographic hardware acceleration**

Benefits of DNSSEC-based Authenticity and Distributed DH GKA

- 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 and client authenticity using a challenge-response mechanism
- Scalable without delay penalty for service discovery
- Established mechanisms for seamless integrated group encryption key distribution

Conclusion & Outlook

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
- Group Key Agreement complies with current security requirements

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
- Group Key Agreement complies with current security requirements

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
- Risk assessment of storing encryption keys in unprotected memory
- Assessment of which services actually require which type of security measures

Automotive Group Key Agreement and Secure Service & Client Authentication Using DNSSEC with DANE

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