When Cryptography Needs a Hand: Practical Post-Quantum Authentication for V2V Communications

Geoff Twardokus — RIT Rochester Institute of Technology

Nina Bindel — SANDBOXAQ

Hanif Rahbari — RIT Rochester Institute of Technology

Sarah McCarthy — UNIVERSITY OF WATERLOO

NDSS SYMPOSIUM/2024

Presented by Internet Society

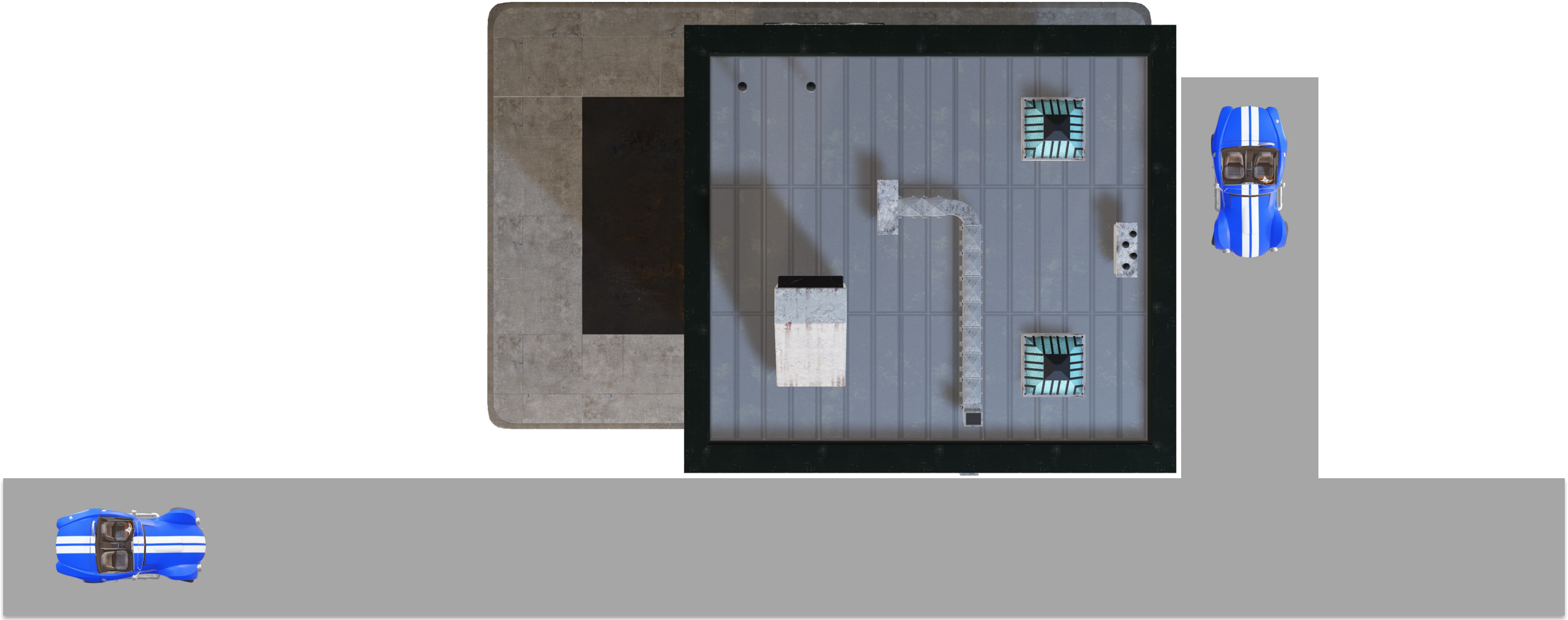
February 27-29, 2024

Vehicle-to-Vehicle (V2V) Communication

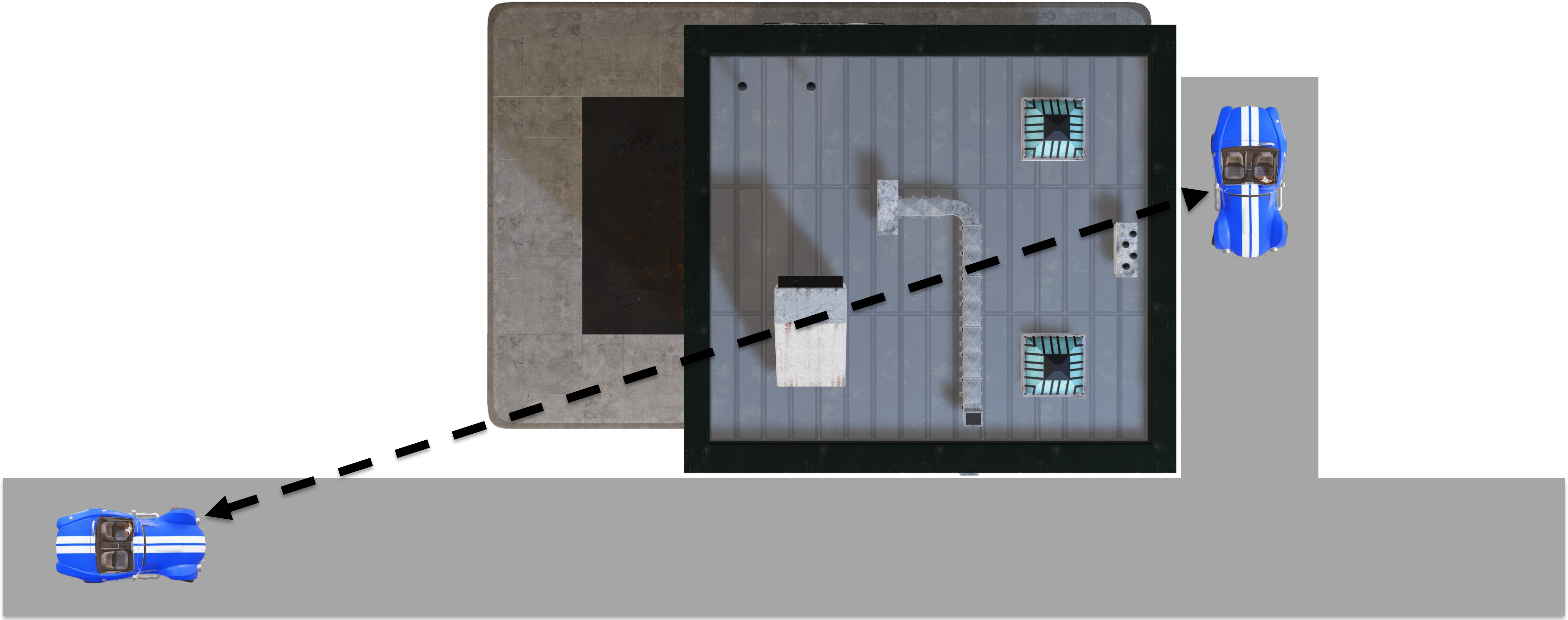
Direct wireless communication between vehicles for safety could prevent 600,000 car crashes every year[1]

[1] National Highway Transportation Safety Administration (NHTSA), “Federal Motor Vehicle Safety Standards; V2V Communications,” Notice of Proposed Rulemaking (NPRM) for FMVSS No. 150, V2V Communications; 88 FR 80685, Nov. 2023.

Vehicle-to-Vehicle (V2V) Communication

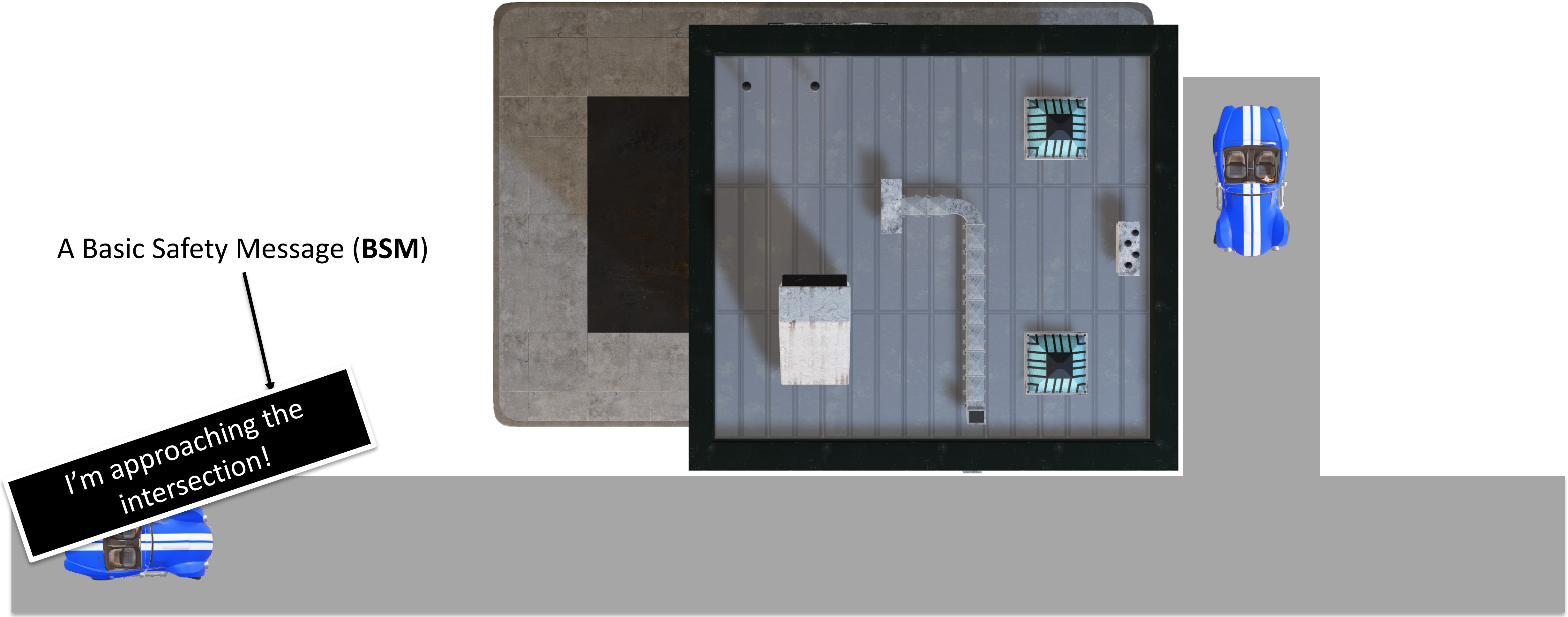


Vehicle-to-Vehicle (V2V) Communication



Vehicle-to-Vehicle (V2V) Communication

Vehicle-to-Vehicle (V2V) Communication



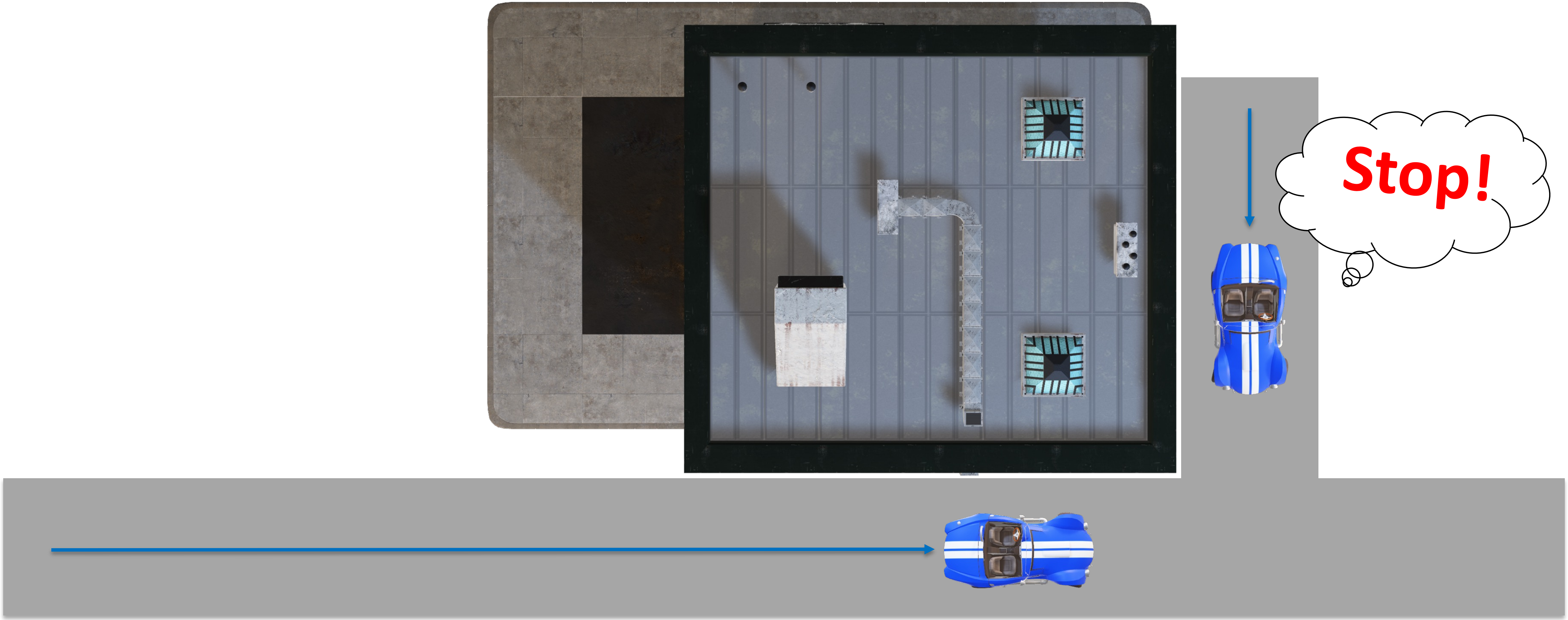
A Basic Safety Message (**BSM**)

I'm approaching the intersection!

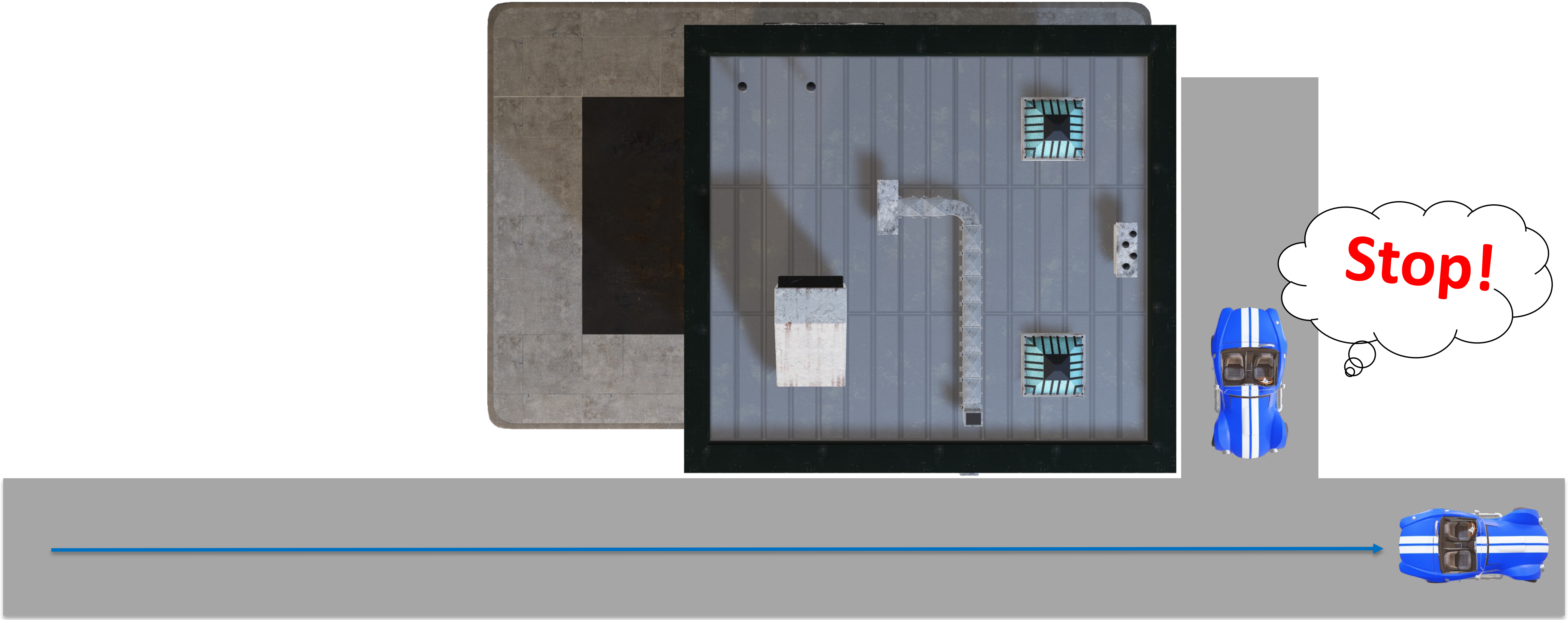
Vehicle-to-Vehicle (V2V) Communication

I'm approaching the intersection!

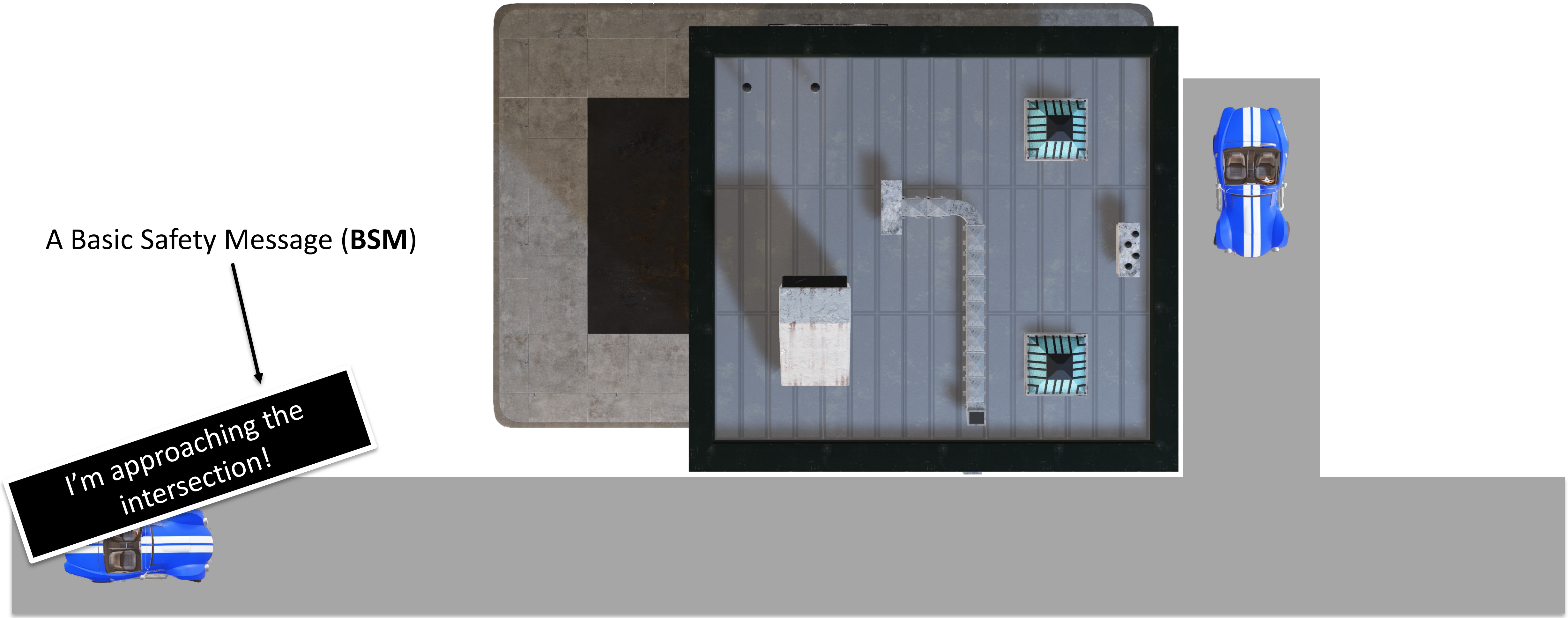
Vehicle-to-Vehicle (V2V) Communication



Vehicle-to-Vehicle (V2V) Communication

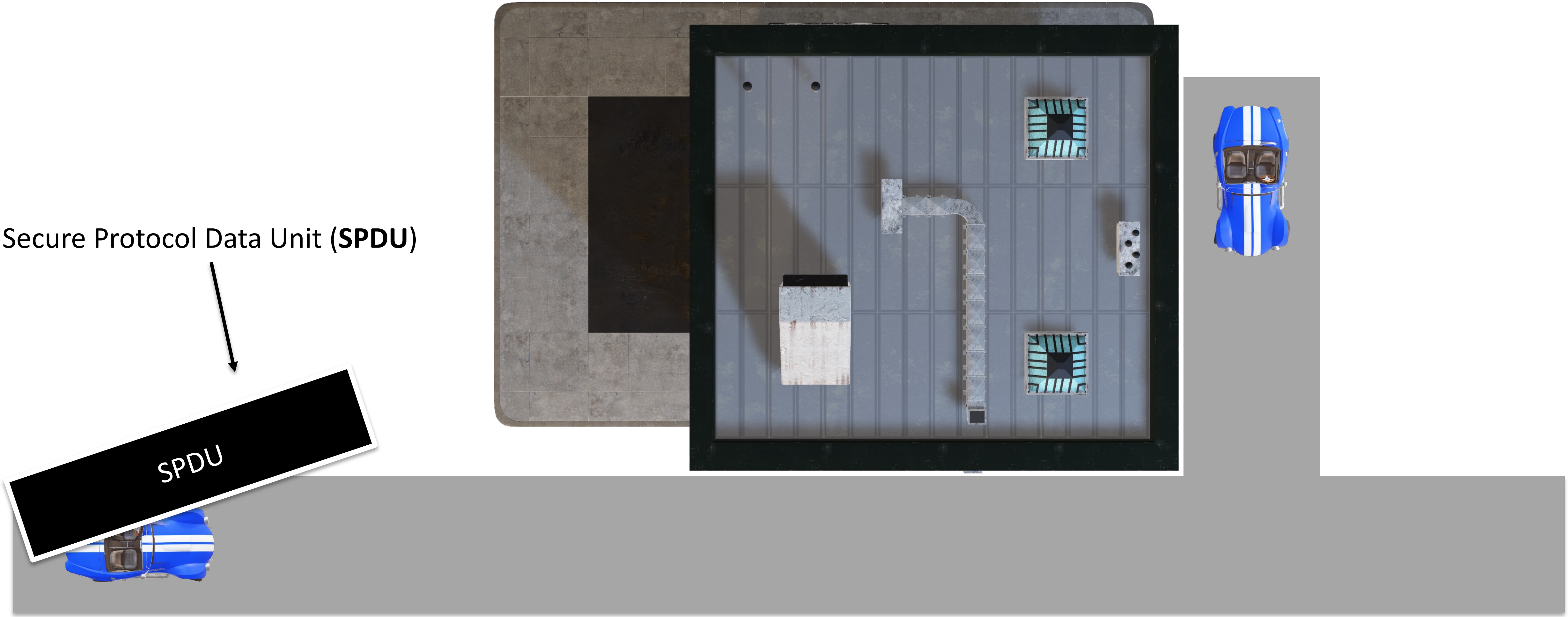


V2V Authentication



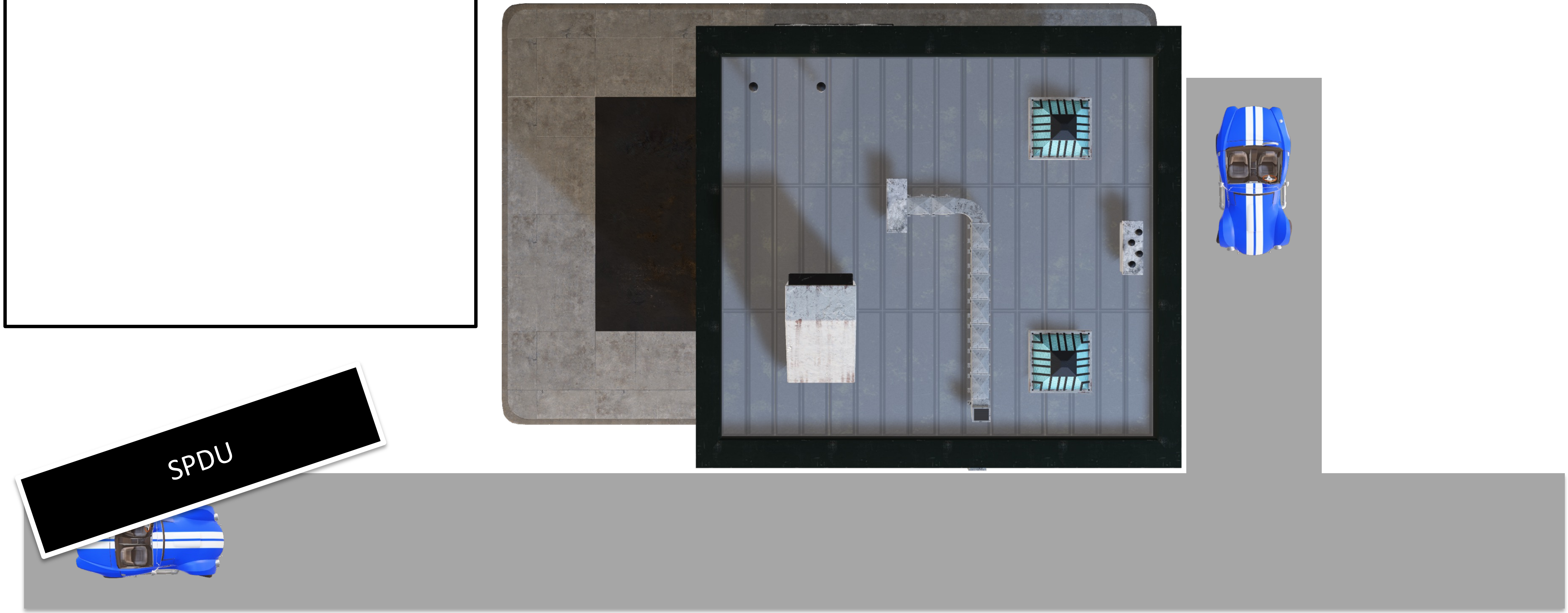
A Basic Safety Message (**BSM**)

V2V Authentication



V2V Authentication

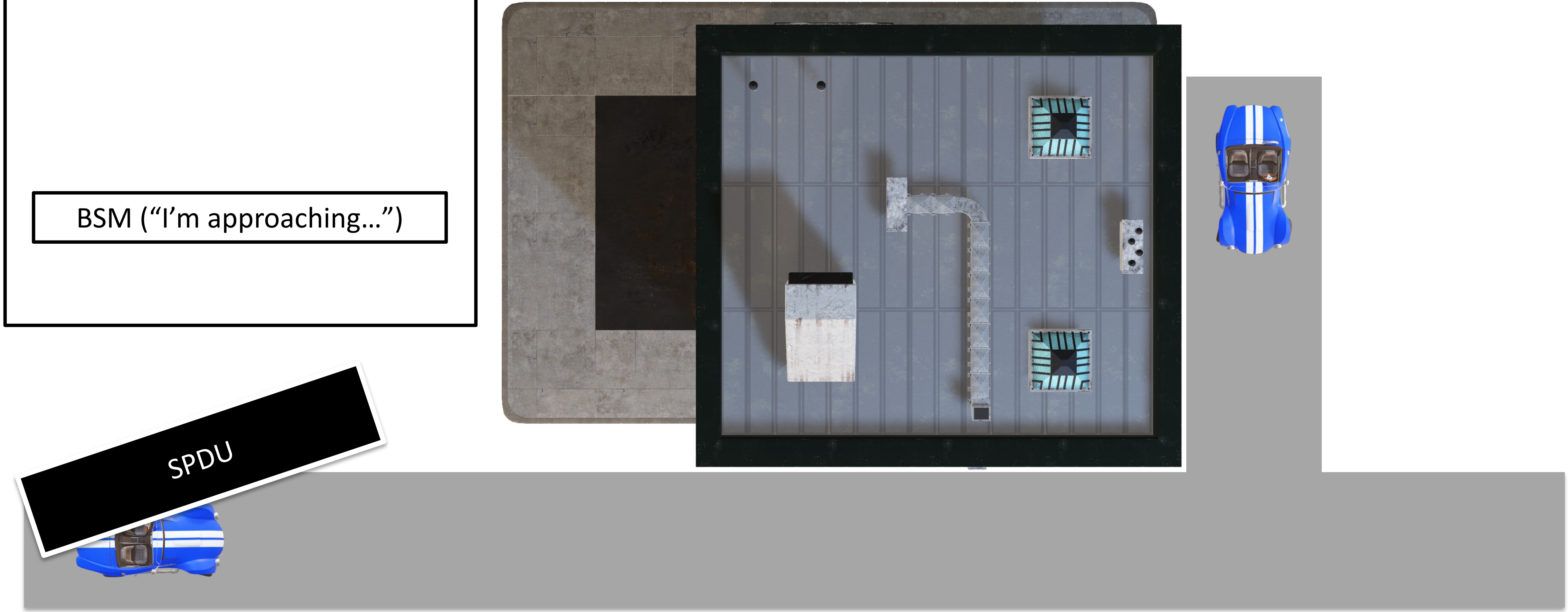
Secure Protocol Data Unit (SPDU)



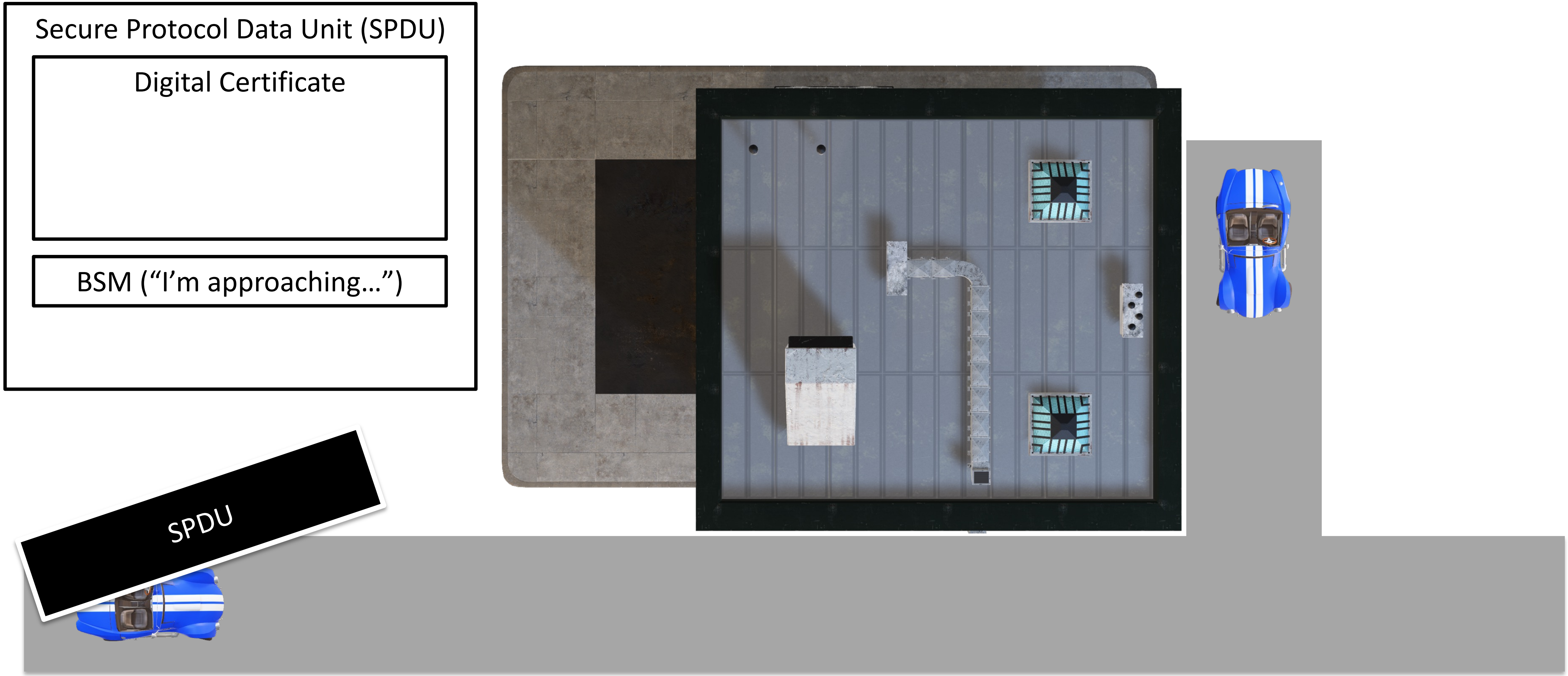
V2V Authentication

Secure Protocol Data Unit (SPDU)

BSM (“I’m approaching…”)



V2V Authentication



Secure Protocol Data Unit (SPDU)

Digital Certificate

BSM (“I’m approaching…”)

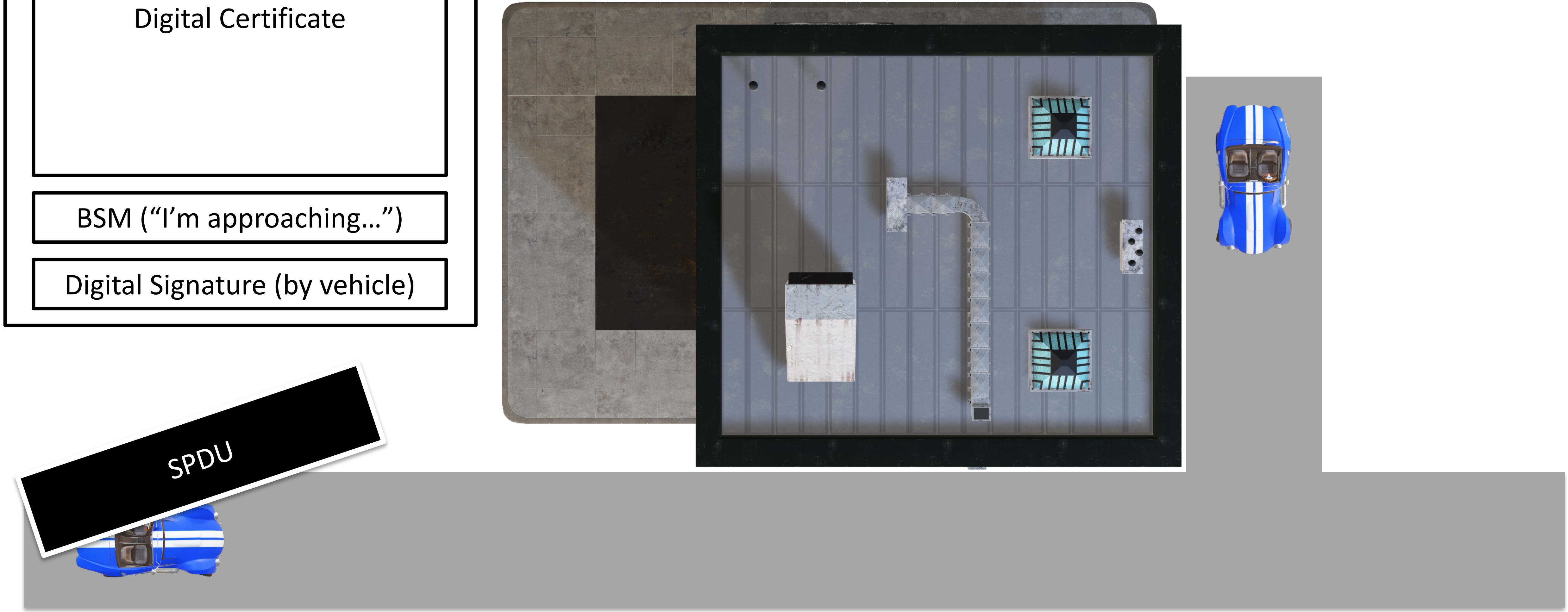
V2V Authentication

Secure Protocol Data Unit (SPDU)

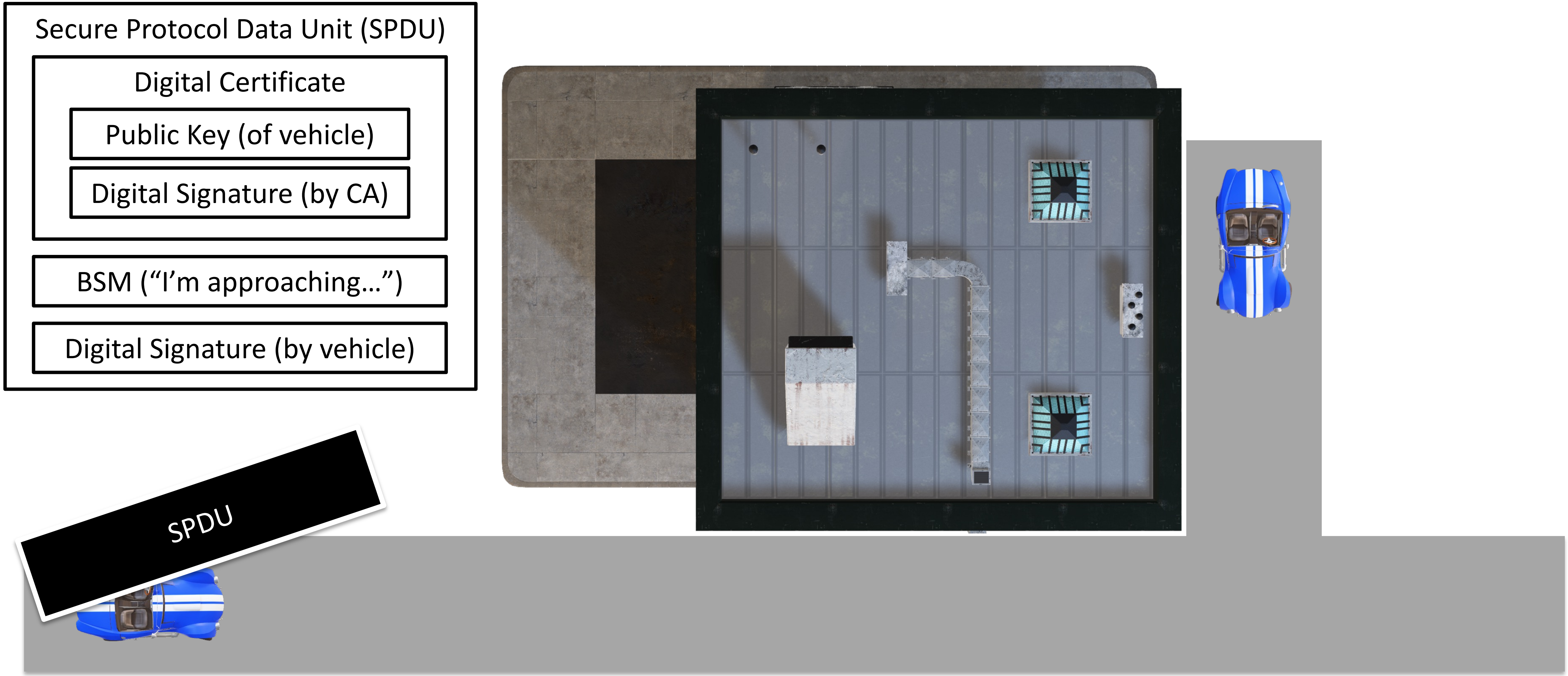
Digital Certificate

BSM (“I’m approaching…”)

Digital Signature (by vehicle)



V2V Authentication



Secure Protocol Data Unit (SPDU)

Digital Certificate

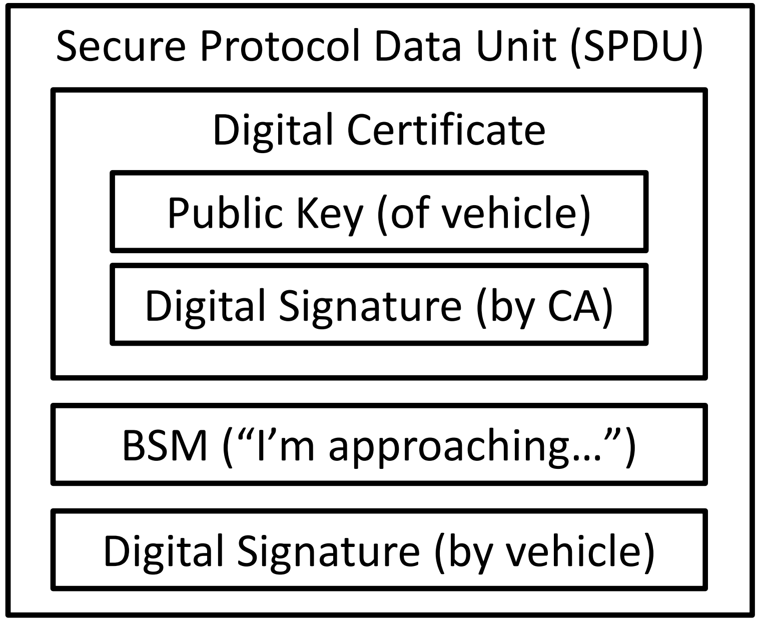
Public Key (of vehicle)

Digital Signature (by CA)

BSM (“I’m approaching…”)

Digital Signature (by vehicle)

V2V Authentication



Secure Protocol Data Unit (SPDU)

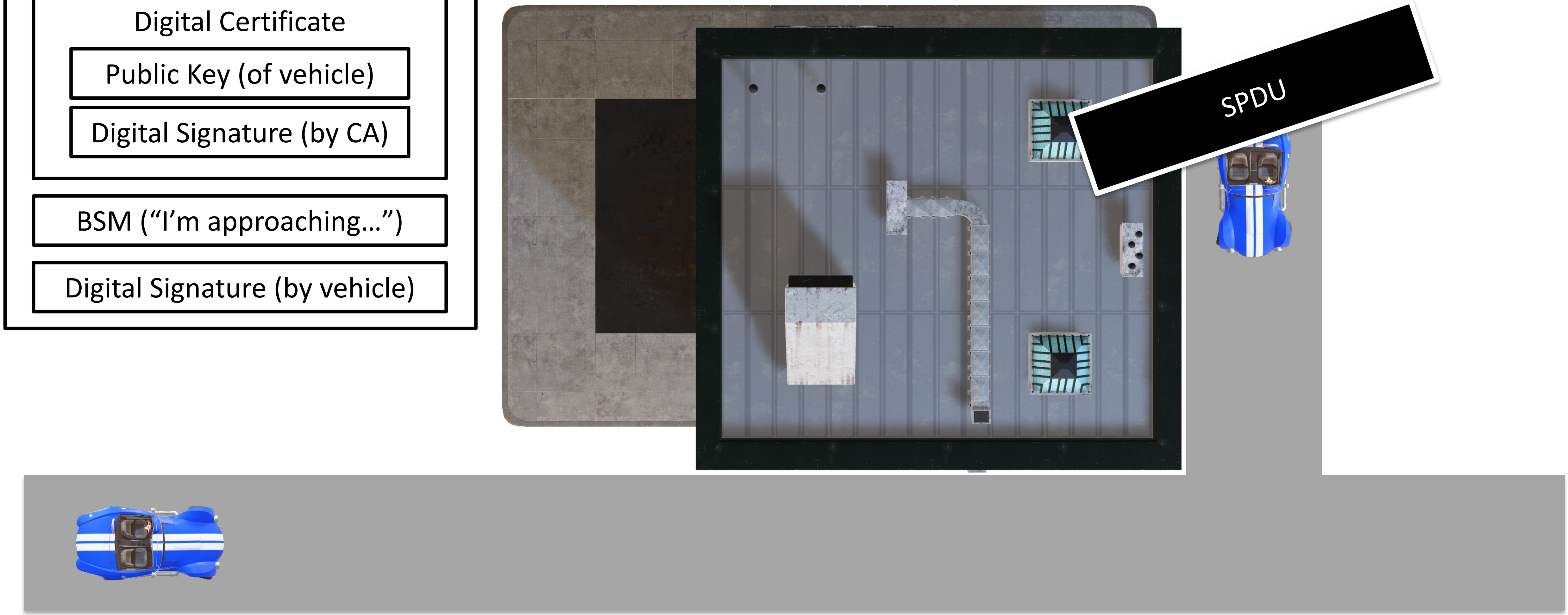
Digital Certificate

Public Key (of vehicle)

Digital Signature (by CA)

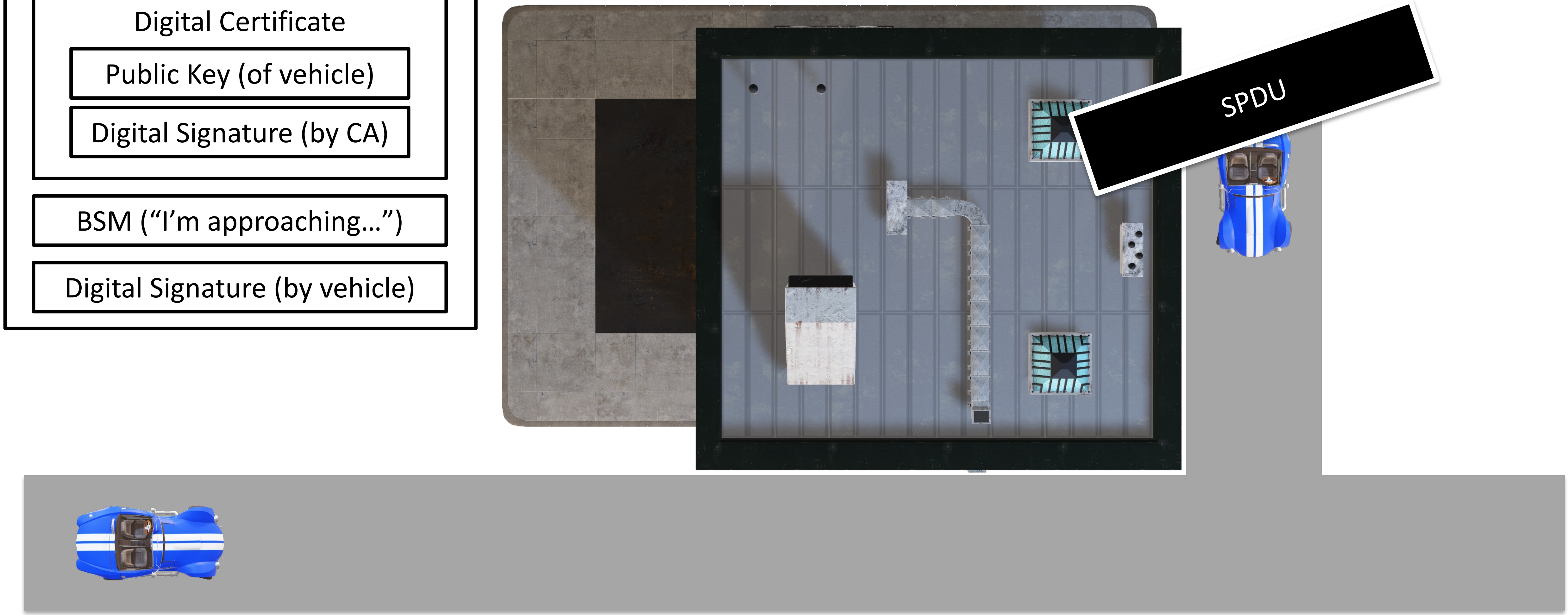
BSM (“I’m approaching…”)

Digital Signature (by vehicle)



V2V Authentication

- Secure Protocol Data Unit (SPDU)
  - Digital Certificate
    - Public Key (of vehicle)
    - Digital Signature (by CA)
  - BSM (“I’m approaching…”)
  - Digital Signature (by vehicle)



V2V Authentication

Certificate Valid?

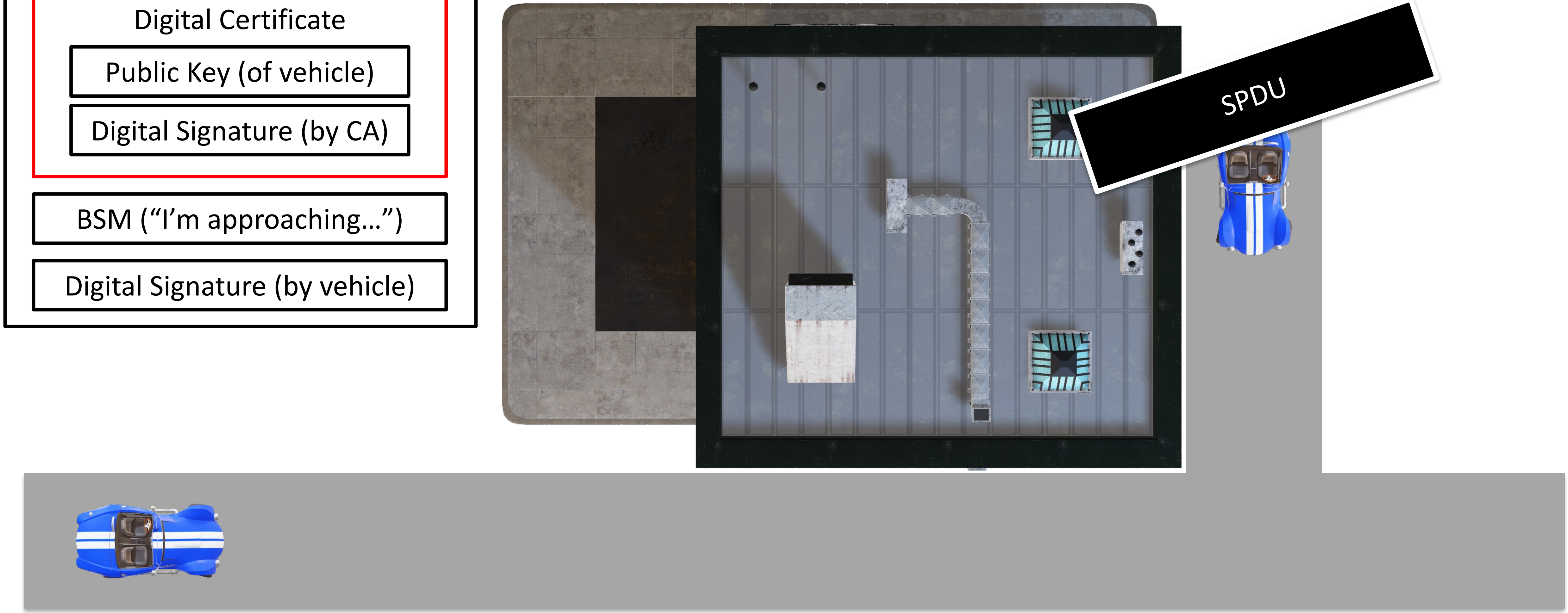
Secure Protocol Data Unit (SPDU)

Digital Certificate

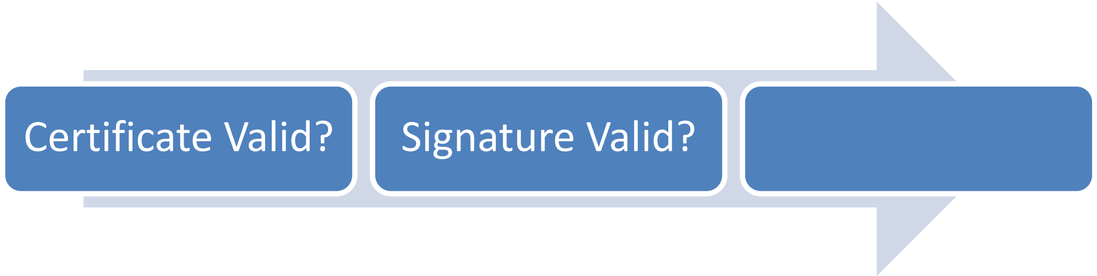
- Public Key (of vehicle)
- Digital Signature (by CA)

BSM (“I’m approaching…”)

Digital Signature (by vehicle)

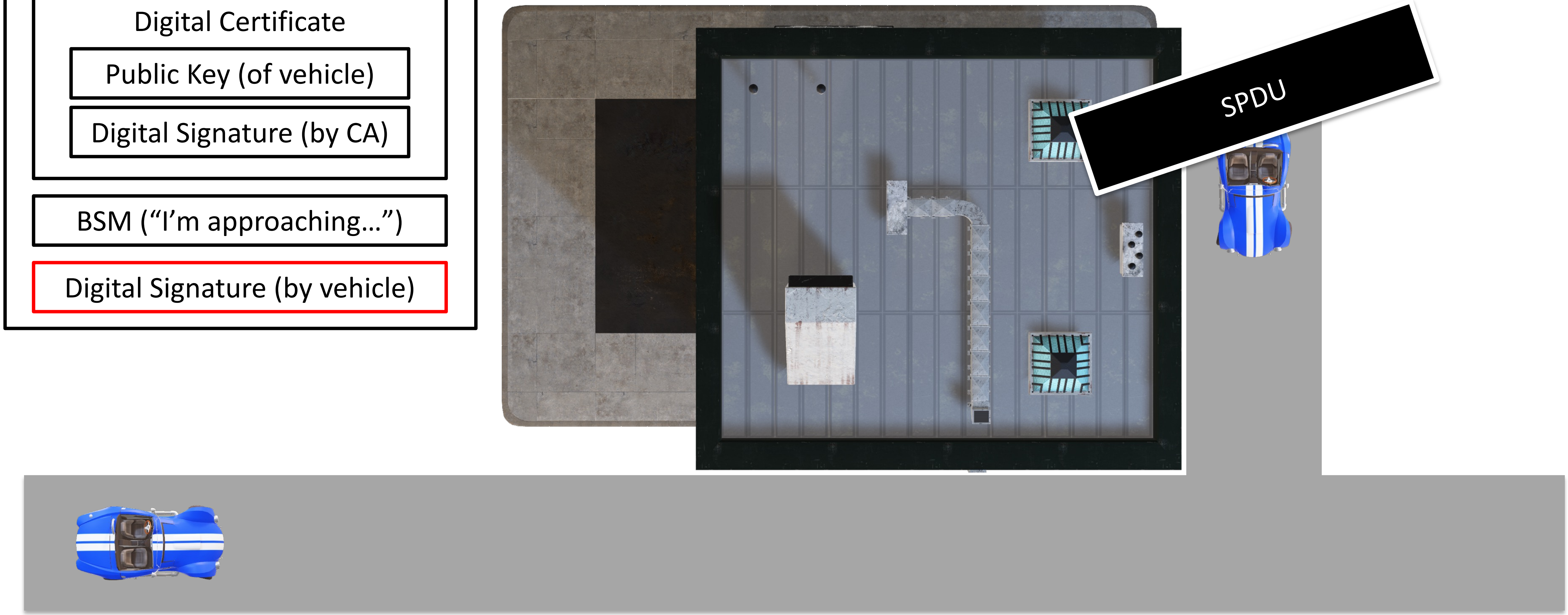


V2V Authentication

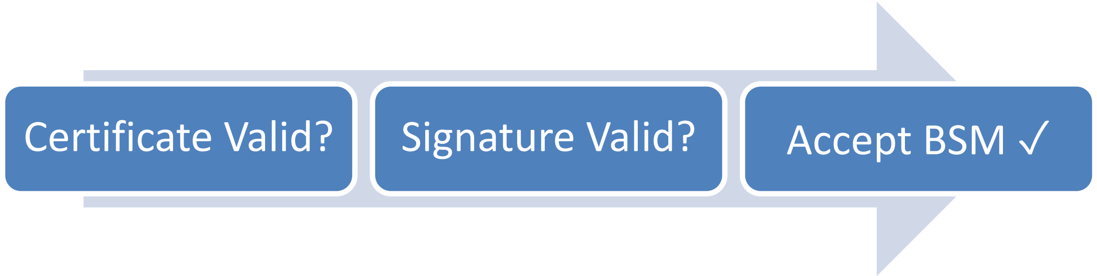


Secure Protocol Data Unit (SPDU)

- Digital Certificate
  - Public Key (of vehicle)
  - Digital Signature (by CA)
- BSM ("I'm approaching…")
- Digital Signature (by vehicle)



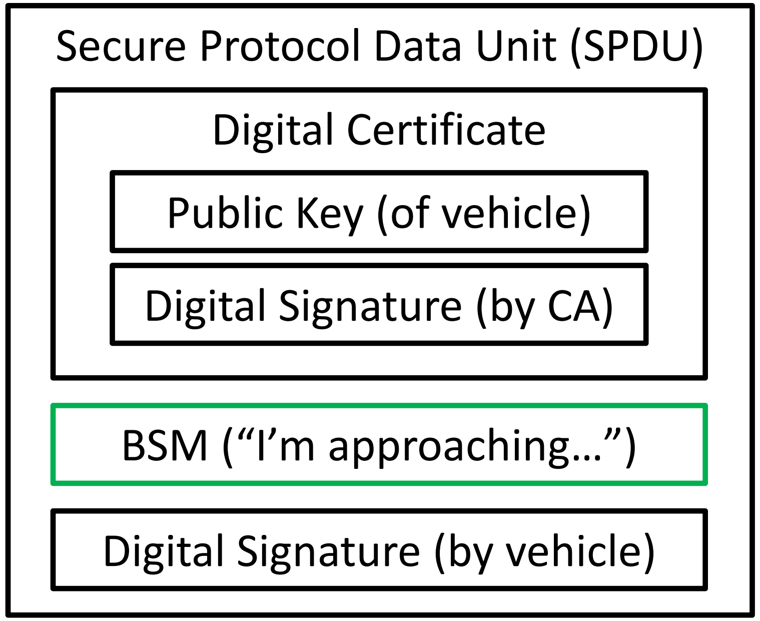
V2V Authentication



Certificate Valid?

Signature Valid?

Accept BSM ✓



Secure Protocol Data Unit (SPDU)

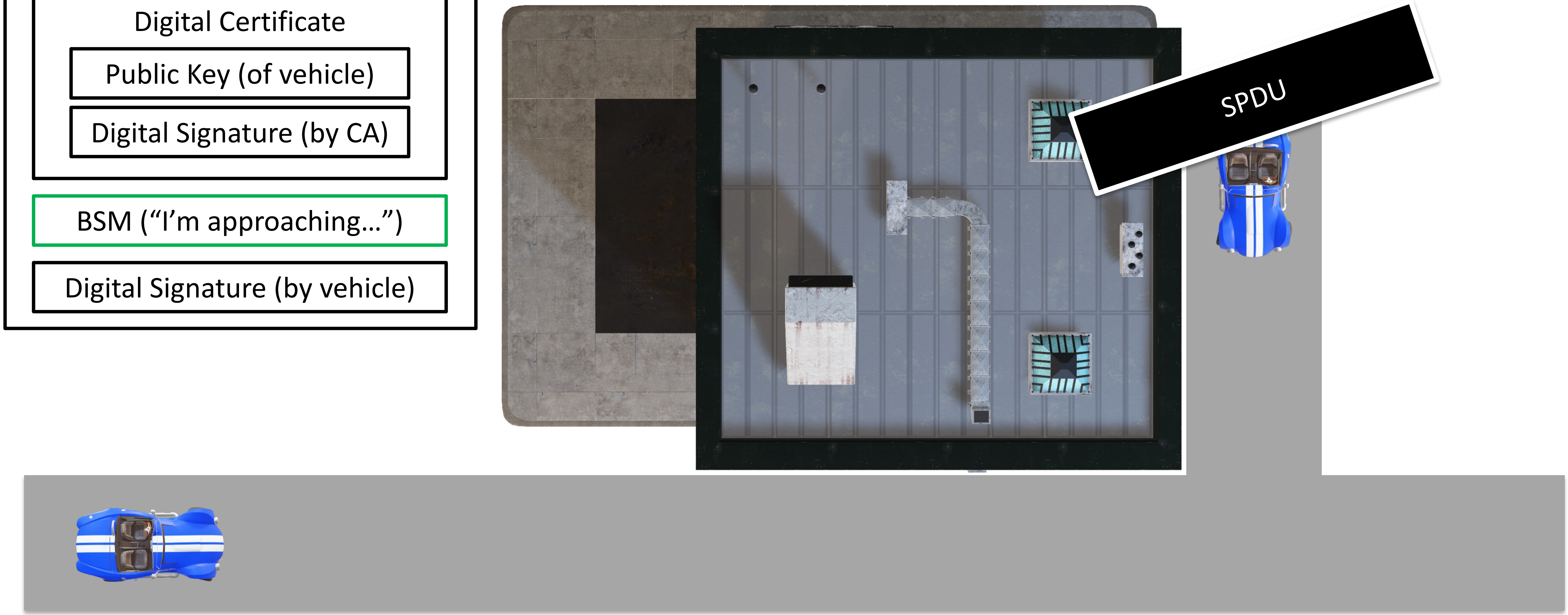
Digital Certificate

Public Key (of vehicle)

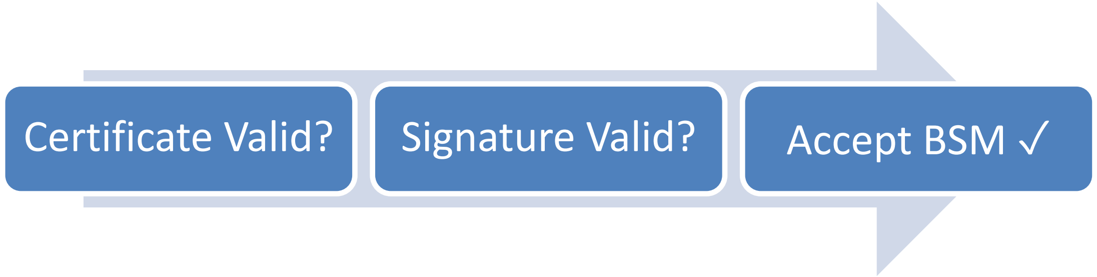
Digital Signature (by CA)

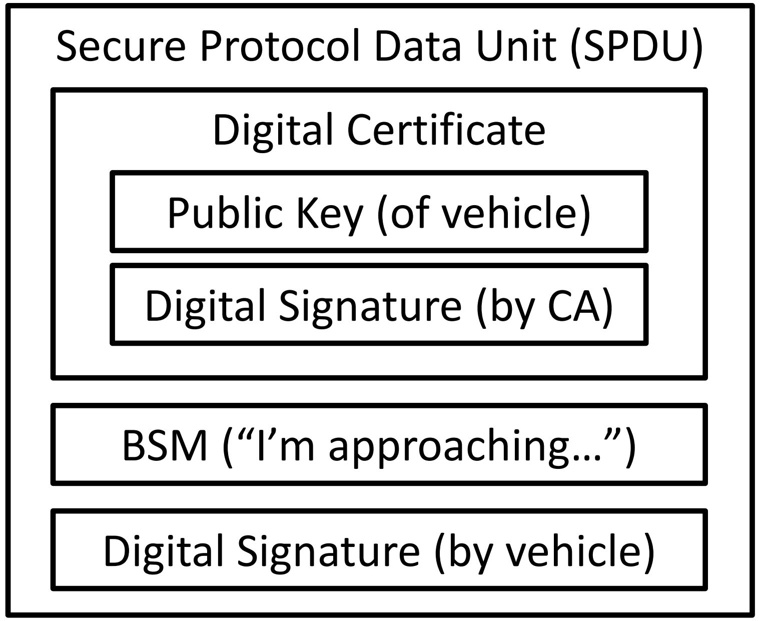
BSM (“I’m approaching…”)

Digital Signature (by vehicle)



V2V Authentication




Secure Protocol Data Unit (SPDU)

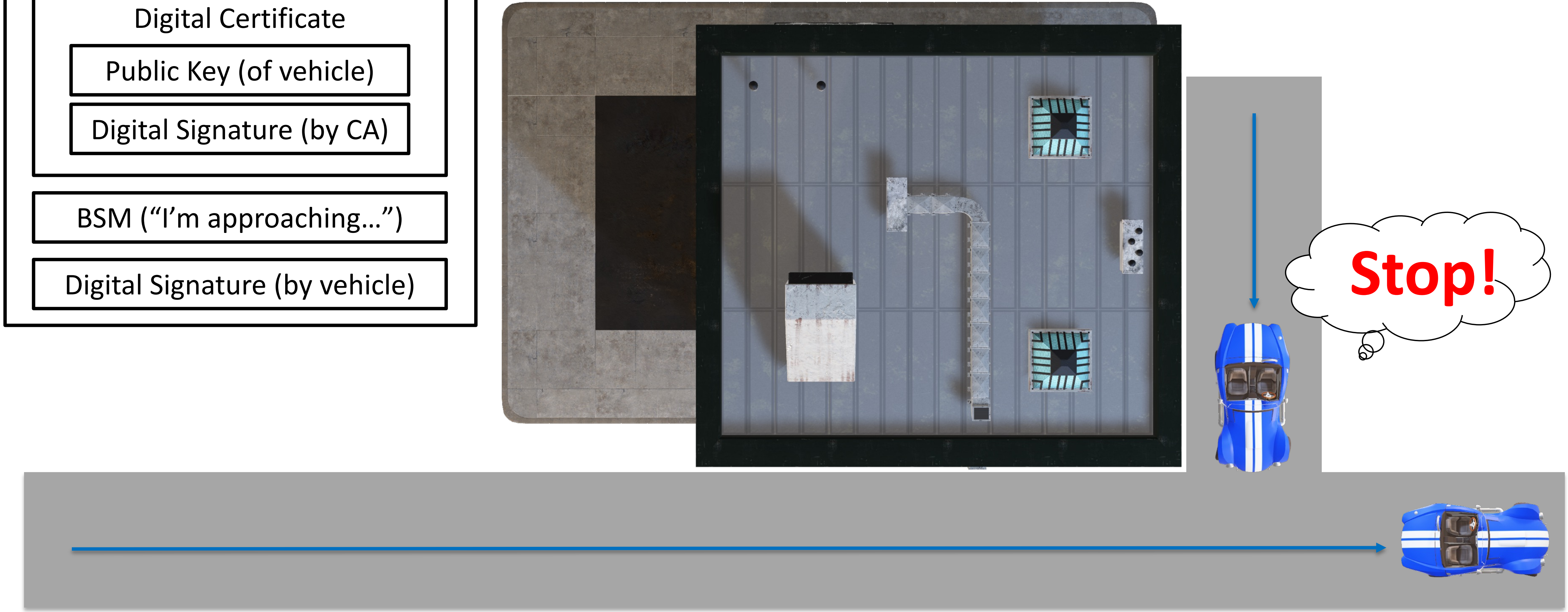
Digital Certificate

Public Key (of vehicle)

Digital Signature (by CA)

BSM (“I’m approaching…”)

Digital Signature (by vehicle)



Quantum Computers (QCs) Threaten V2V

Digital signatures in V2V use elliptic curves (ECDSA)

Quantum Computers (QCs) Threaten V2V

Digital signatures in V2V use elliptic curves (ECDSA)

QCs will break ECDSA → forge signatures, issue bogus certificates

Quantum Computers (QCs) Threaten V2V

Digital signatures in V2V use elliptic curves (ECDSA)

QCs will break ECDSA → forge signatures, issue bogus certificates

Good news: NIST is standardizing post-quantum (PQ) algorithms

Quantum Computers (QCs) Threaten V2V

Digital signatures in V2V use elliptic curves (ECDSA)

QCs will break ECDSA → forge signatures, issue bogus certificates

Good news: NIST is standardizing post-quantum (PQ) algorithms

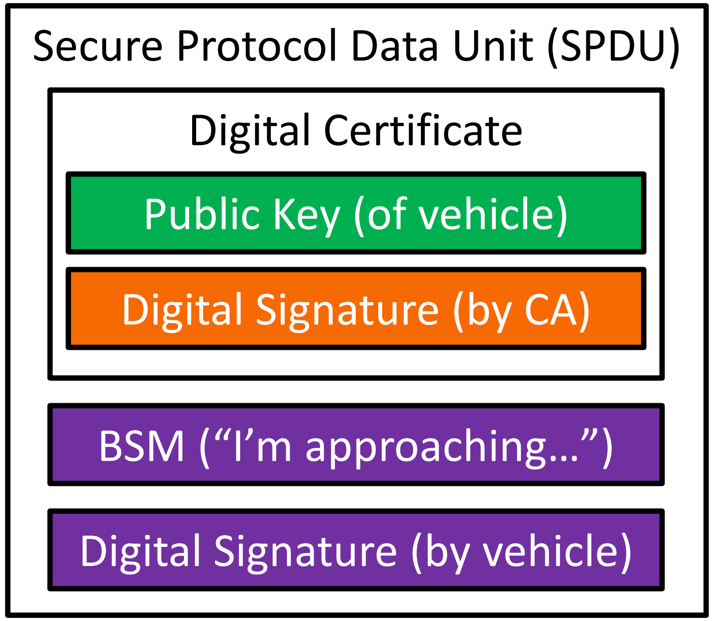
Problem: V2V protocols cannot easily adopt these PQ signatures

Why Isn’t PQ “Plug-and-Play” in V2V?

- PQ signatures and keys are much larger than ECDSA

Why Isn't PQ "Plug-and-Play" in V2V?

- PQ signatures and keys are much larger than ECDSA



Secure Protocol Data Unit (SPDU)

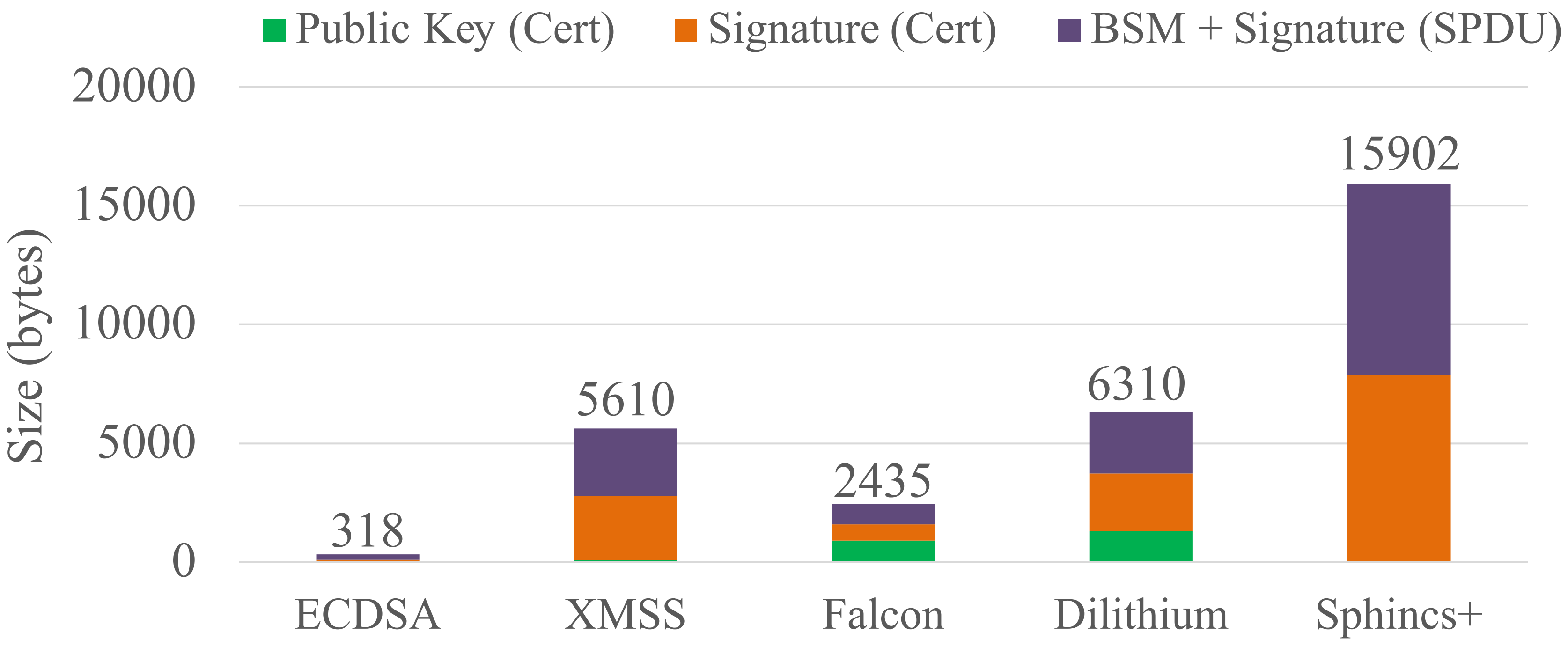
Digital Certificate

Public Key (of vehicle)

Digital Signature (by CA)

BSM ("I'm approaching…")

Digital Signature (by vehicle)

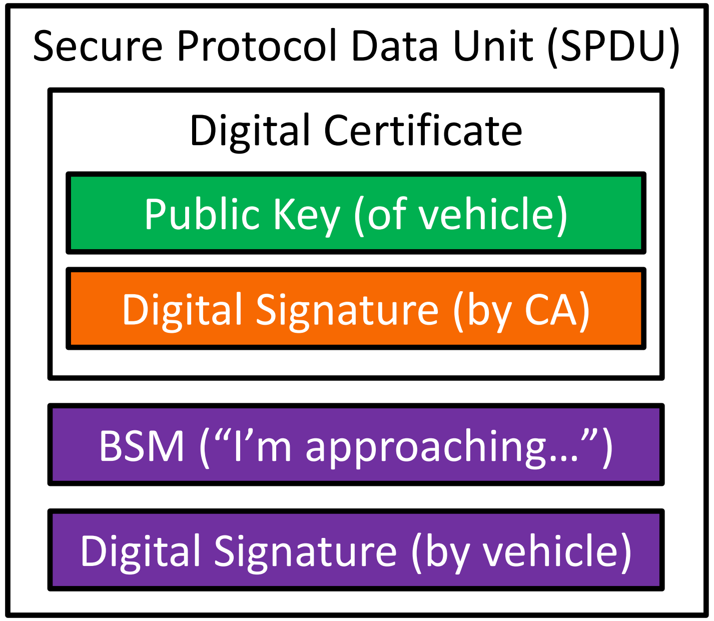


NIST-approved algorithms

PQ algorithms we consider for V2V

Why Isn’t PQ “Plug-and-Play” in V2V?

- ❑ PQ signatures and keys are much larger than ECDSA



Secure Protocol Data Unit (SPDU)

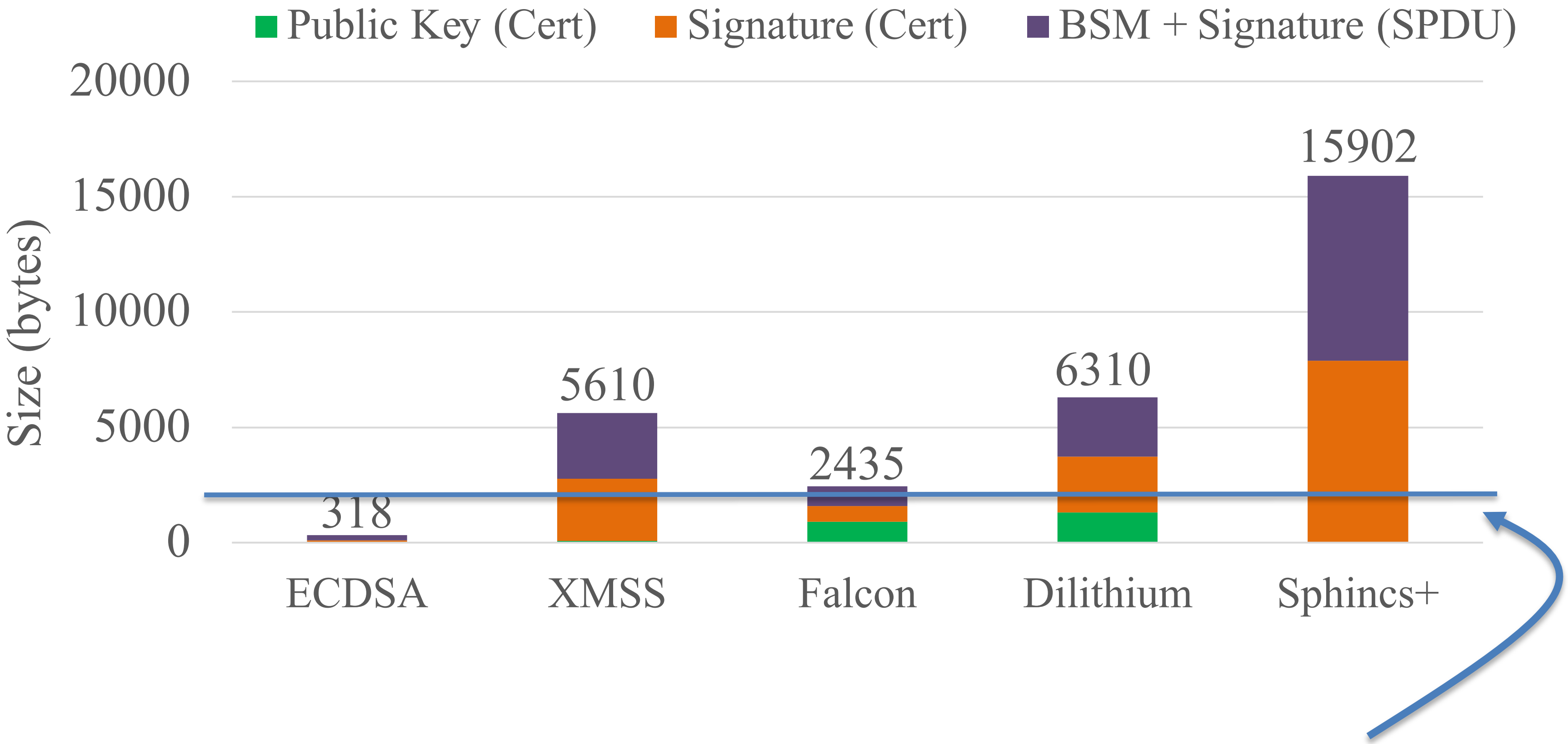
Digital Certificate

Public Key (of vehicle)

Digital Signature (by CA)

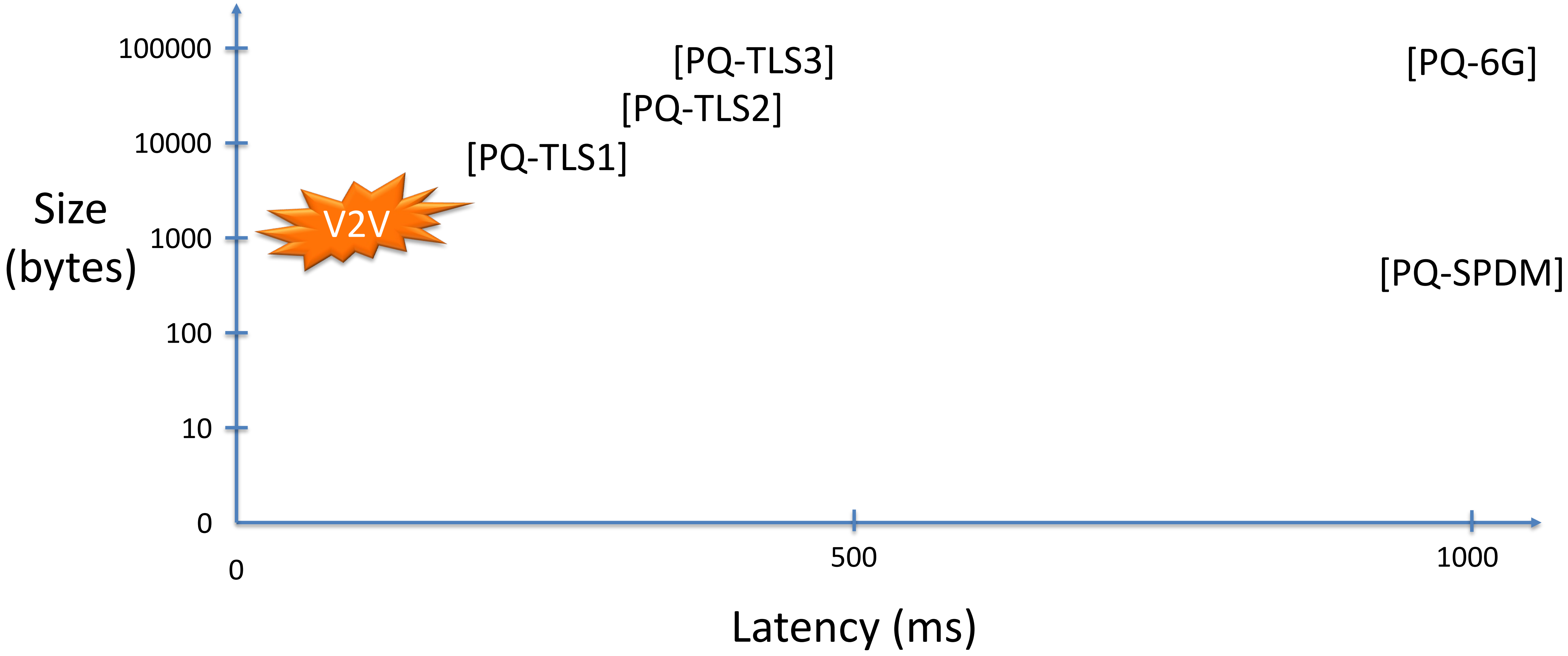
BSM (“I’m approaching…”)

Digital Signature (by vehicle)



- ❑ Dedicated Short-Range Communication (DSRC) → 2,304-byte limit

V2V is (Uniquely) More Constrained



Our Contributions

Analyze quantum threat
&
Identify V2V constraints for PQC

Our Contributions

Hybrid (PQ/EC) Authentication Protocol
&
AI-based Transmission Optimization

Analyze quantum threat
&
Identify V2V constraints for PQC

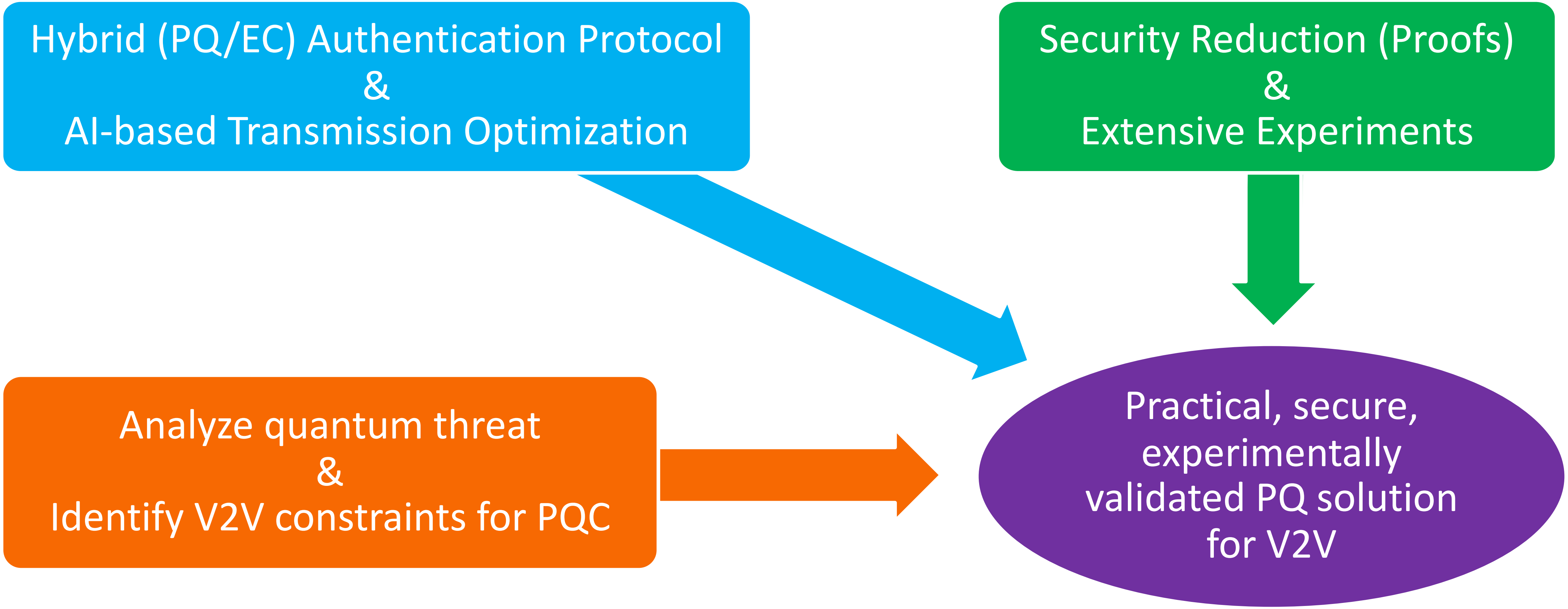
Our Contributions

Hybrid (PQ/EC) Authentication Protocol
&
AI-based Transmission Optimization

Security Reduction (Proofs)
&
Extensive Experiments

Analyze quantum threat
&
Identify V2V constraints for PQC

Our Contributions



Hybrid (PQ/EC) Authentication Protocol
&
AI-based Transmission Optimization

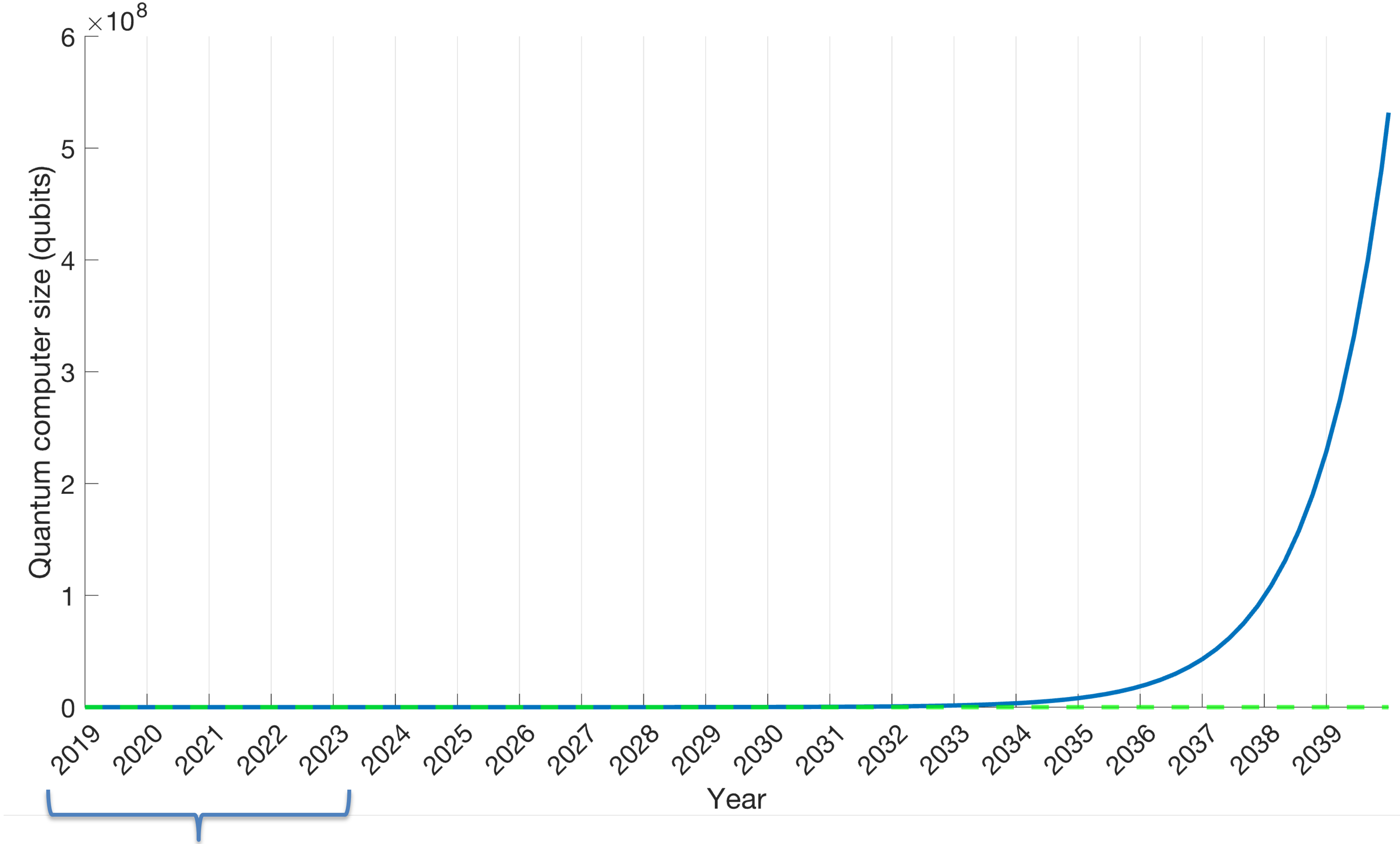
Security Reduction (Proofs)
&
Extensive Experiments

Analyze quantum threat
&
Identify V2V constraints for PQC

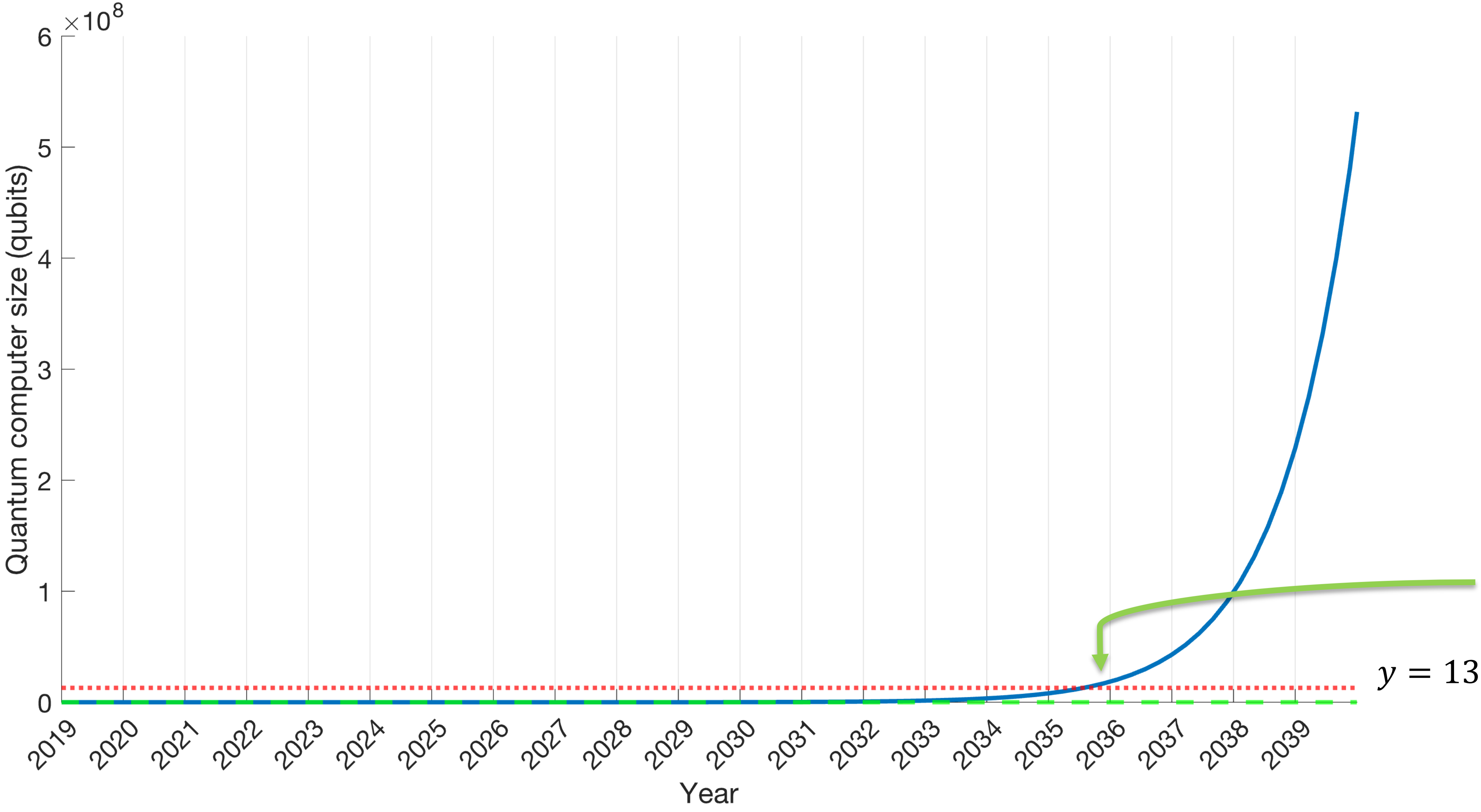
Practical, secure, experimentally validated PQ solution for V2V

How Much PQ Security Do We Need *Now*?

- ❑ Quantum computers (QCs) can’t break much (yet)

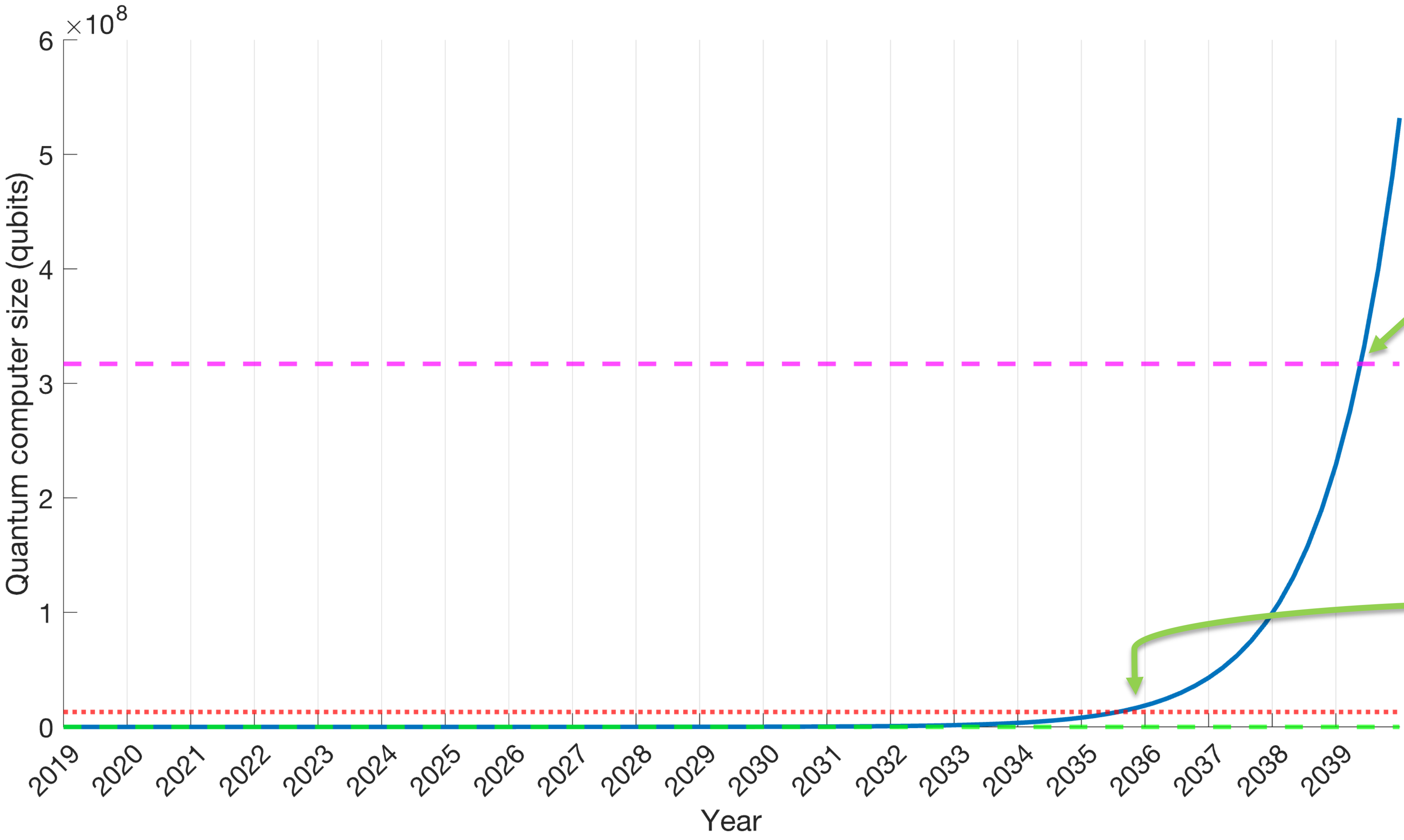


Extrapolation from 2019-2023 IBM data and forecast



Break ECDSA in one day ~2035

$y = 13{,}000{,}000$ qubits



Break ECDSA in one hour ~2039

$y = 317{,}000{,}000$ qubits

Break ECDSA in one day ~2035

$y = 13{,}000{,}000$ qubits

So, why worry about this now?

Unlikely to have quantum threat before ~ 2035

So, why worry about this now?

Unlikely to have quantum threat before ~ 2035

Average vehicle lifetime is 12-15 years

So, why worry about this now?

Unlikely to have quantum threat before ~ 2035

Average vehicle lifetime is 12-15 years

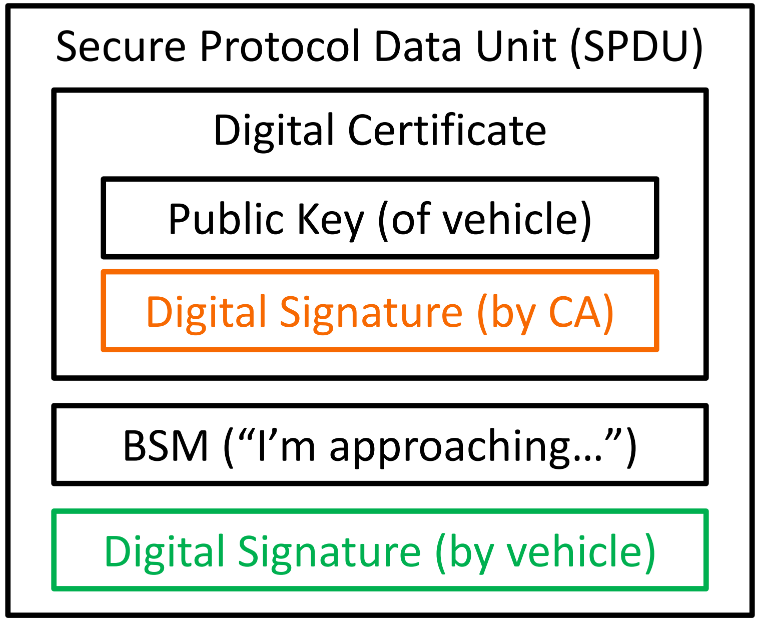
Today’s V2V wireless protocols and vehicle hardware need quantum resistance

How Much PQ Security Do We Need *Now*?

- ❑ Quantum computers (QCs) can’t break much (yet)
- ❑ Two critical message elements have digital signatures:

How Much PQ Security Do We Need *Now*?

- Quantum computers (QCs) can’t break much (yet)
- Two critical message elements have digital signatures:
  - Payload (BSM) signature valid for ~30 seconds
  - Digital certificate signature valid for 1 week



Secure Protocol Data Unit (SPDU)

Digital Certificate

Public Key (of vehicle)

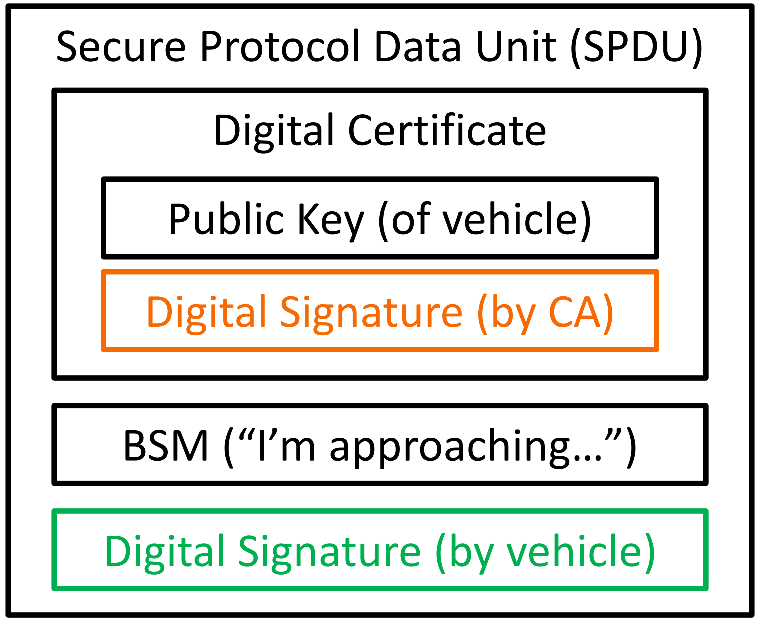
Digital Signature (by CA)

BSM (“I’m approaching…”)

Digital Signature (by vehicle)

How Much PQ Security Do We Need *Now*?

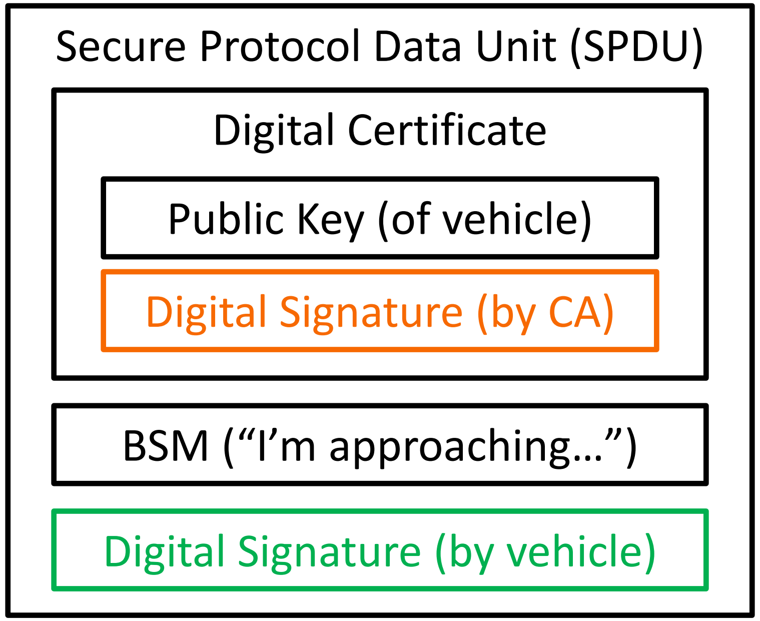
- Quantum computers (QCs) can't break much (yet)
- Two critical message elements have digital signatures:
  - Payload (BSM) signature valid for ~30 seconds
  - Digital certificate signature valid for 1 week
- Certificate forgery possible by 2035!


Secure Protocol Data Unit (SPDU)
Digital Certificate
Public Key (of vehicle)
Digital Signature (by CA)
BSM ("I'm approaching…")
Digital Signature (by vehicle)

How Much PQ Security Do We Need *Now*?

- Quantum computers (QCs) can’t break much (yet)
- Two critical message elements have digital signatures:
  - Payload (BSM) signature valid for ~30 seconds
  - Digital certificate signature valid for 1 week
- Certificate forgery possible by 2035!

For the near future, focus on protecting certificates from quantum attacks in a hybrid solution for PQ V2V


Secure Protocol Data Unit (SPDU)
Digital Certificate
Public Key (of vehicle)
Digital Signature (by CA)
BSM (“I’m approaching…”)
Digital Signature (by vehicle)

Partially Hybrid Authentication Protocol

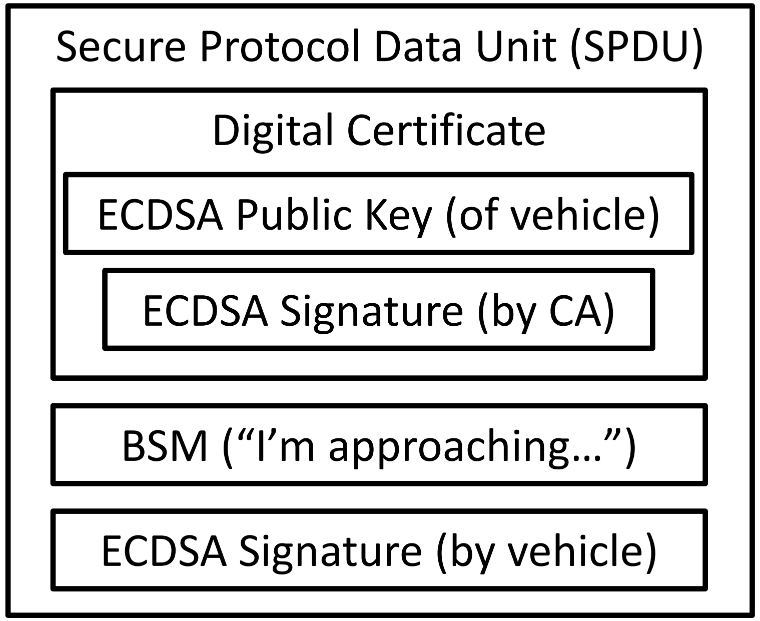
- PQC protects what is most imminently at risk: certificates

Partially Hybrid Authentication Protocol

- ❑ PQC protects what is most imminently at risk: certificates
- ❑ Kickstart transition to PQ hardware and protocols

Partially Hybrid Authentication Protocol

- PQC protects what is most imminently at risk: certificates
- Kickstart transition to PQ hardware and protocols



Secure Protocol Data Unit (SPDU)

Digital Certificate

ECDSA Public Key (of vehicle)

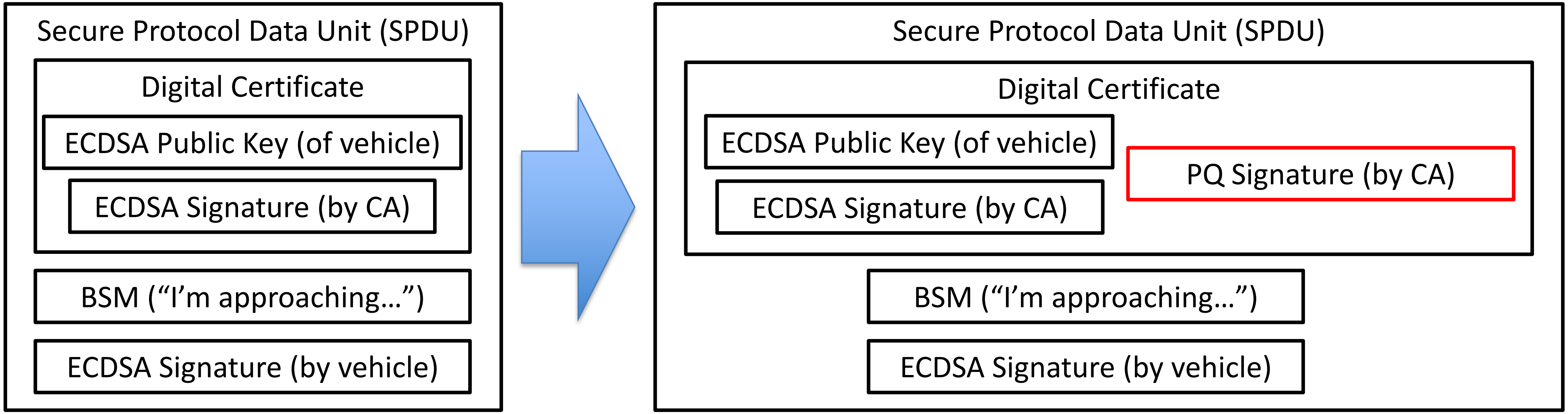
ECDSA Signature (by CA)

BSM ("I'm approaching…")

ECDSA Signature (by vehicle)

Partially Hybrid Authentication Protocol

- PQC protects what is most imminently at risk: certificates
- Kickstart transition to PQ hardware and protocols
- Use PQ signature for certificate, keep EC signature for message


Secure Protocol Data Unit (SPDU)
Digital Certificate
ECDSA Public Key (of vehicle)
ECDSA Signature (by CA)
BSM ("I'm approaching…")
ECDSA Signature (by vehicle)
Secure Protocol Data Unit (SPDU)
Digital Certificate
ECDSA Public Key (of vehicle)
ECDSA Signature (by CA)
PQ Signature (by CA)
BSM ("I'm approaching…")
ECDSA Signature (by vehicle)

For Every Message, (Not) a Certificate

- Certificates are transmitted in every fifth SPDU
  - Certificate must be shared every 500ms

For Every Message, (Not) a Certificate

- Certificates are transmitted in every fifth SPDU
  - Certificate must be shared every 500ms

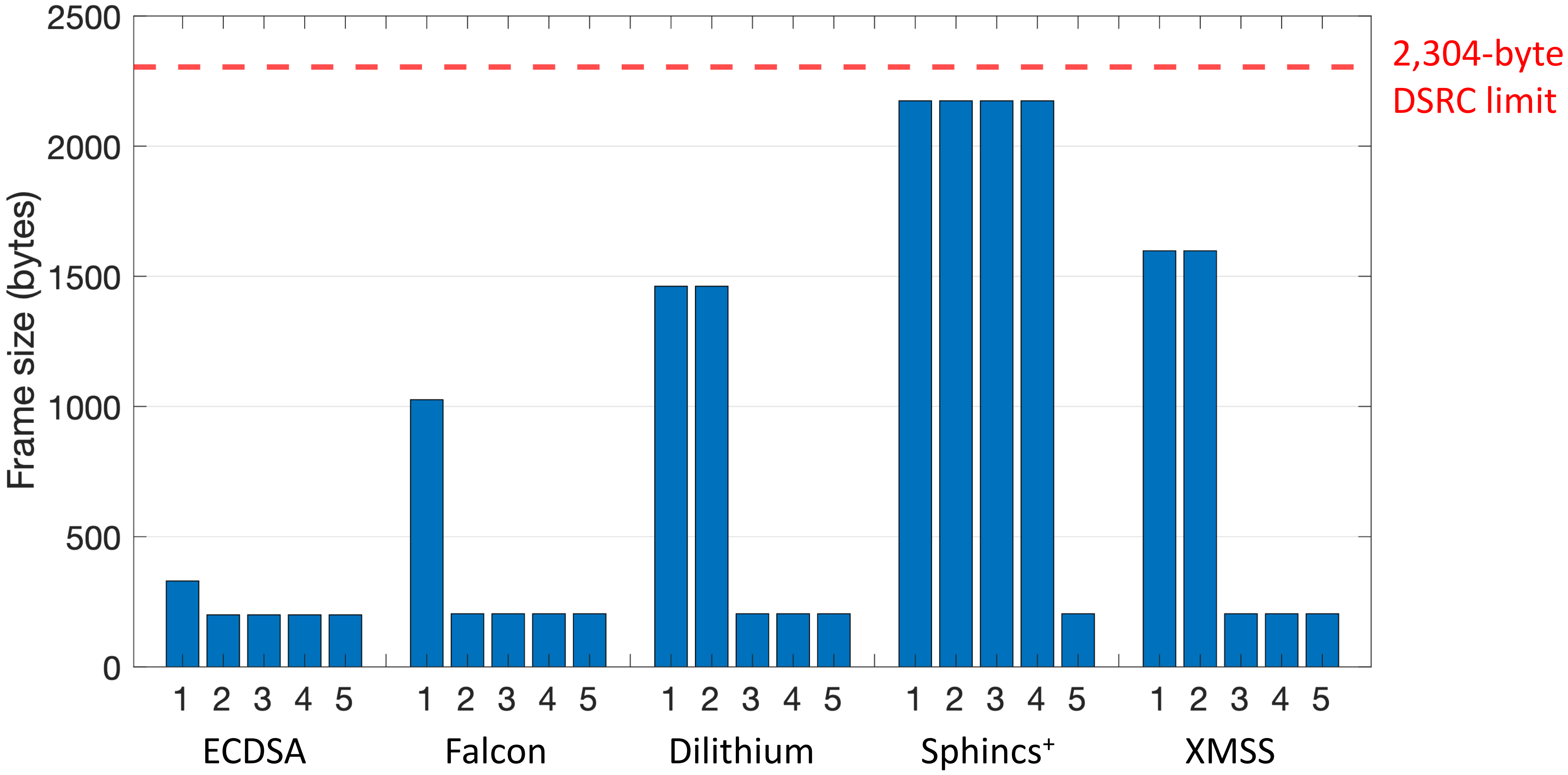
- Insight: fragment hybrid certificates across up to 5 SPDUs

For Every Message, (Not) a Certificate

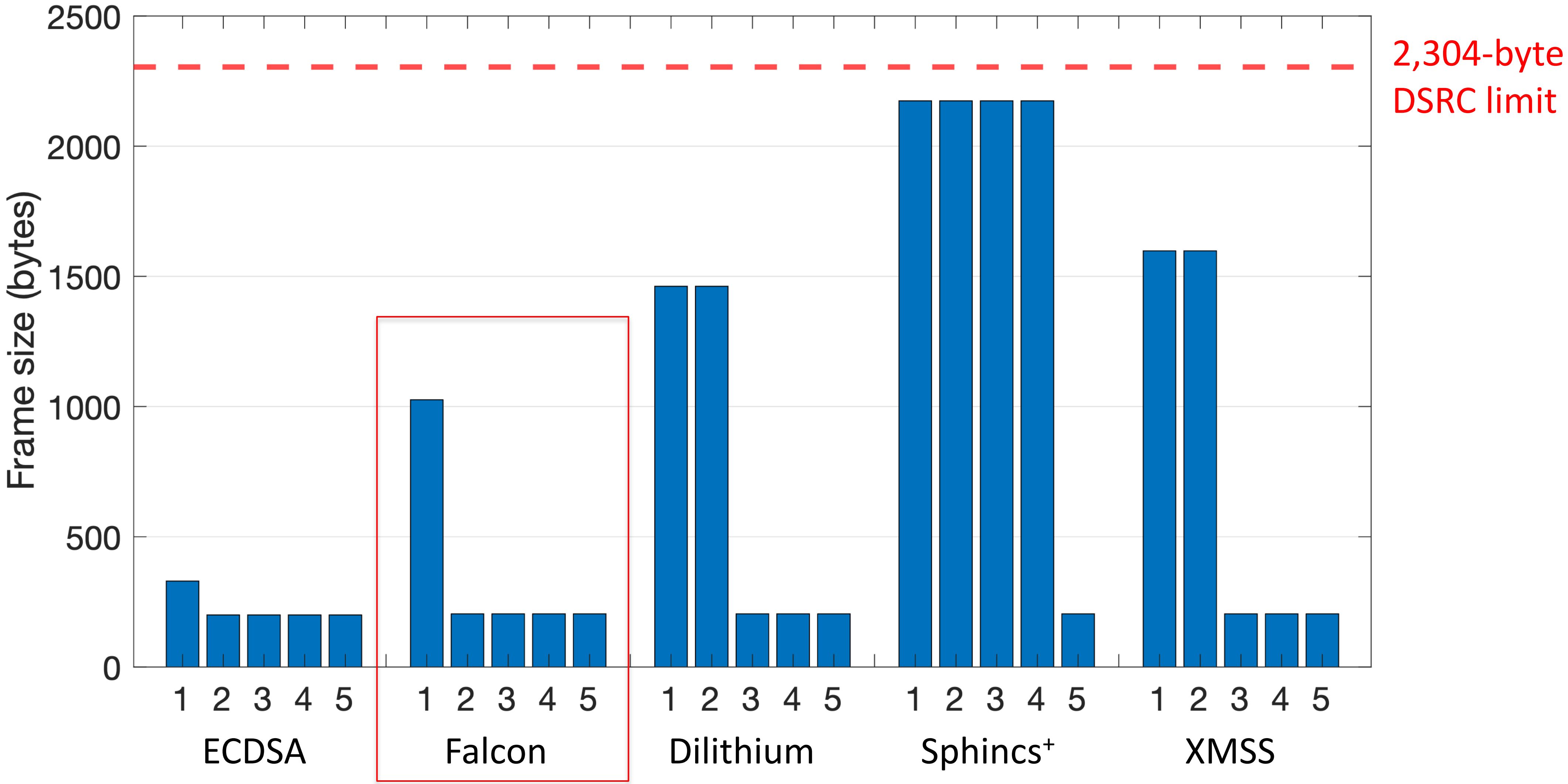
- Certificates are transmitted in every fifth SPDU
    - Certificate must be shared every 500ms

- Insight: fragment hybrid certificates across up to 5 SPDUs

- Goal: Minimize message size



5-SPDU certificate cycle for ECDSA and selected PQ algorithms



5-SPDU certificate cycle for ECDSA and selected PQ algorithms

Larger Frames → Less Reliable

- Medium contention, hidden terminals in mobile network

Larger Frames → Less Reliable

- ❑ Medium contention, hidden terminals in mobile network
- ❑ Frame Loss Rate (FLR): $\frac{\#\ lost\ frames}{\#\ total\ frames}$ for entire system

Larger Frames → Less Reliable

- ❑ Medium contention, hidden terminals in mobile network
- ❑ Frame Loss Rate (FLR): $\frac{\#\,lost\ frames}{\#\,total\ frames}$ for entire system

Problem: In high-density scenarios (100 vehicles/km), FLR is $+63\%$ when ECDSA replaced with *Partially Hybrid* design (using Falcon)

Source: https://bit.ly/3UPmBCG

Solution: Optimize Transmissions

- Insight: > 95% of certificate transmissions are unnecessary!
    - Vehicles do not move very far in ~500 ms

Solution: Optimize Transmissions

- Insight: > 95% of certificate transmissions are unnecessary!
  - Vehicles do not move very far in ~500 ms

- Idea: send certificates less frequently, decrease spectrum waste

Use AI to Optimize Transmissions

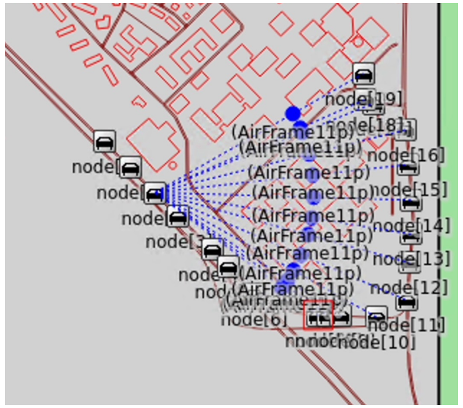
- Insight: > 95% of certificate transmissions are unnecessary!
  - Vehicles do not move very far in ~500 ms
- Idea: send certificates less frequently, decrease spectrum waste
- Use distributed AI to dynamically adjust certificate interval

Use AI to Optimize Transmissions

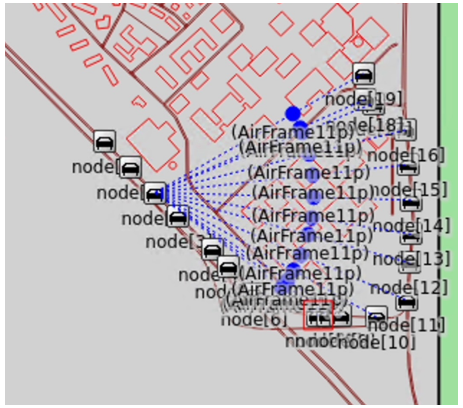
- Insight: > 95% of certificate transmissions are unnecessary!
  - Vehicles do not move very far in ~500 ms
- Idea: send certificates less frequently, decrease spectrum waste
- Use distributed AI to dynamically adjust certificate interval
- Also optimize peer-to-peer certificate sharing protocol (P2PCD)

Experiments

- Extensive simulations in VEINS
  - Custom PQ-V2V module

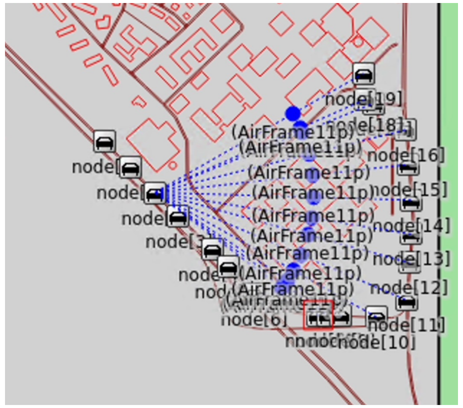


Experiments

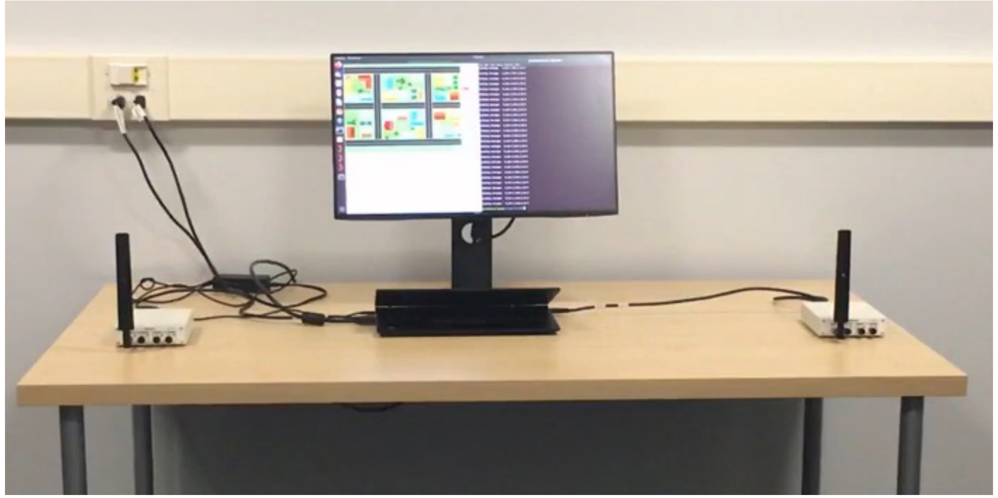


- ❑ Extensive simulations in VEINS
  - Custom PQ-V2V module
- ❑ Benchmarking PQ algorithms on ARM-based V2V chipset

Experiments



- ❑ Extensive simulations in VEINS
  - Custom PQ-V2V module
- ❑ Benchmarking PQ algorithms on ARM-based V2V chipset
- ❑ USRP experiments in the lab and on real roadways
  - New testbed: *PQ-V2Verifier*



Experimental Results

- Combining hardware benchmarks, over-the-air measurements, and infusing data into VEINS simulations:

	Metric (vs. ECDSA)	Low-density (60 vehicles/km)	High-density (100 vehicles/km)
Partially Hybrid	Per-BSM delay	+0.66 ms	+0.67 ms
	Δ FLR	+29%	+61%

Experimental Results

- Combining hardware benchmarks, over-the-air measurements, and infusing data into VEINS simulations:

	Metric (vs. ECDSA)	Low-density (60 vehicles/km)	High-density (100 vehicles/km)
Partially Hybrid	Per-BSM delay	+0.66 ms	+0.67 ms
	Δ FLR	+29%	+61%
Partially Hybrid w/ Spectrum Optimization	Δ FLR	+7.9%	+7.1%

Conclusions

- ❑ Forecasted and assessed quantum risk to V2V

Conclusions

❑ Forecasted and assessed quantum risk to V2V

❑ Developed practical, hybrid authentication protocol

Conclusions

- ❑ Forecasted and assessed quantum risk to V2V

- ❑ Developed practical, hybrid authentication protocol

- ❑ Identified Falcon as best PQ algorithm for V2V

Conclusions

- Forecasted and assessed quantum risk to V2V
- Developed practical, hybrid authentication protocol
- Identified Falcon as best PQ algorithm for V2V
- Applied AI to optimize spectrum, improve reliability

Conclusions

- ❑ Forecasted and assessed quantum risk to V2V
- ❑ Developed practical, hybrid authentication protocol
- ❑ Identified Falcon as best PQ algorithm for V2V
- ❑ Applied AI to optimize spectrum, improve reliability
- ❑ Validated through simulations and hardware experiments

Key Contributions

Forecast/assessment of quantum risk

Hybrid authentication protocol

Falcon is best PQ algorithm for V2V

AI to optimize spectrum, reliability

Simulations + hardware experiments

Thank You! Questions?

← Our paper

← Artifacts

Artifact Evaluated NDSS SYMPOSIUM
Available
Functional

Geoff Twardokus
geoff.twardokus@mail.rit.edu

RIT ESL Global Cybersecurity Institute Wireless and IoT Security and Privacy Lab

Nina Bindel

SANDBOXAQ

Hanif Rahbari

RIT ESL Global Cybersecurity Institute Wireless and IoT Security and Privacy Lab

Sarah McCarthy

UNIVERSITY OF WATERLOO