Non-Repudiation and End-to-End Security for Electric-Vehicle Charging

Innovative Smart Grid Technologies Europe 2019

September 30th, 2019

Authors

Pol Van Aubel
pol.vanaubel@cs.ru.nl

Erik Poll
erikpoll@cs.ru.nl

Joost Rijneveld
joost@joostrijneveld.nl

This work is supported by the European Regional Development Fund (ERDF), Rijksoverheid, and Province of Gelderland, as part of the project Charge & Go.

iCIS | Digital Security
Radboud University

European Union

OPoost
operationeel programma oost

European Regional Development Fund

Overview

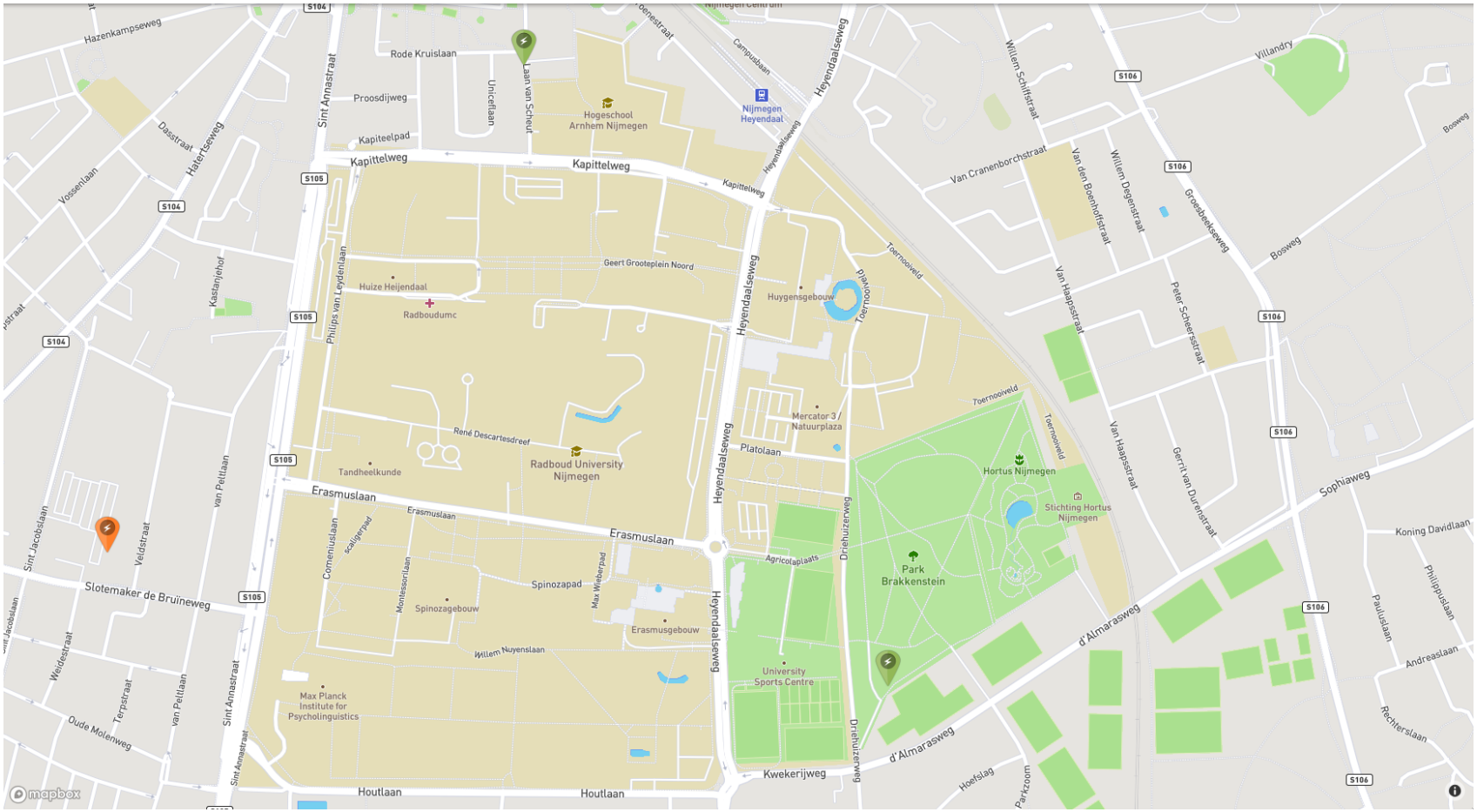
The EV-charging infrastructure

The need for security

End-to-end security

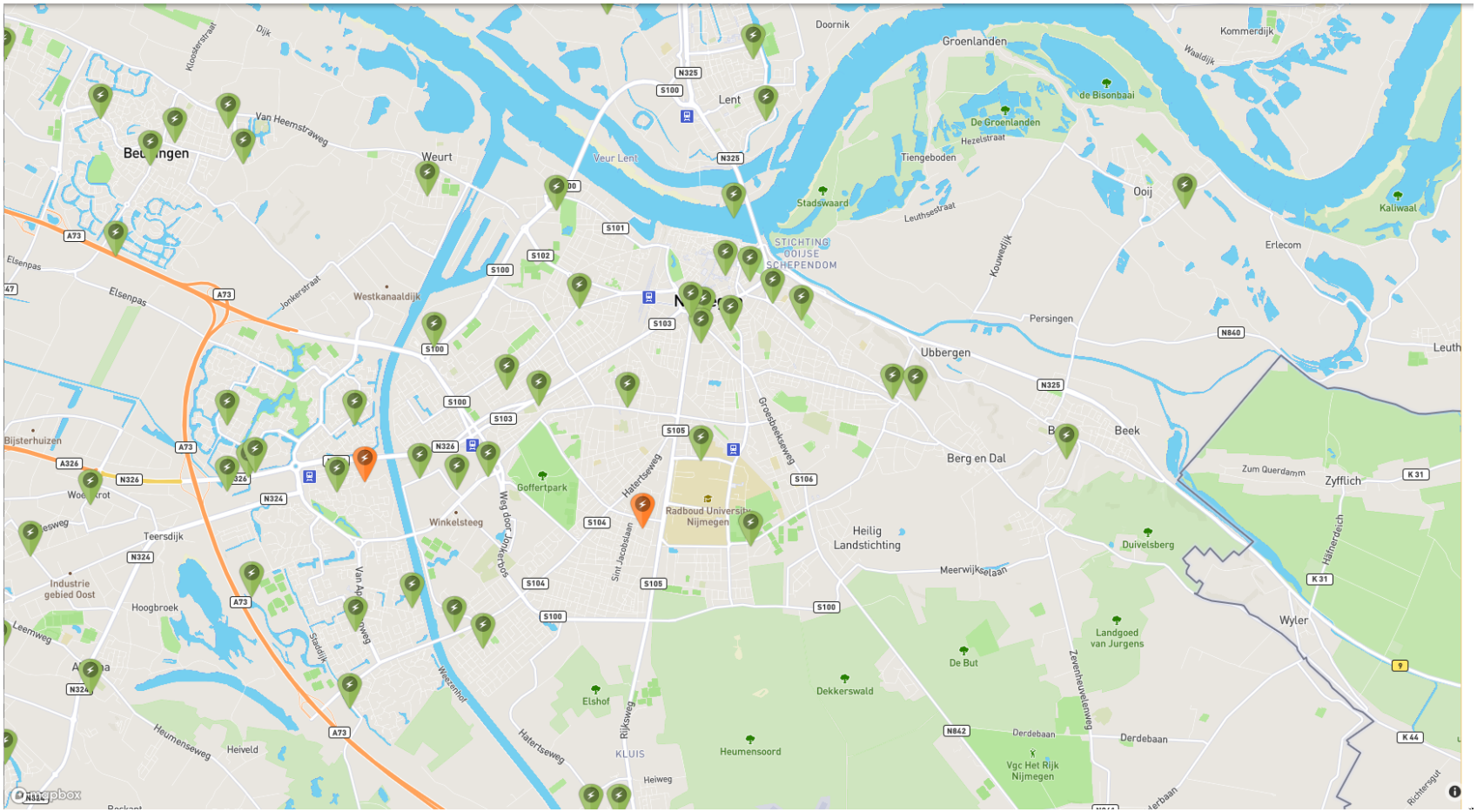
Conclusions

Where is the EV-charging infrastructure?



Source: openchargemap.io

Where is the EV-charging infrastructure?

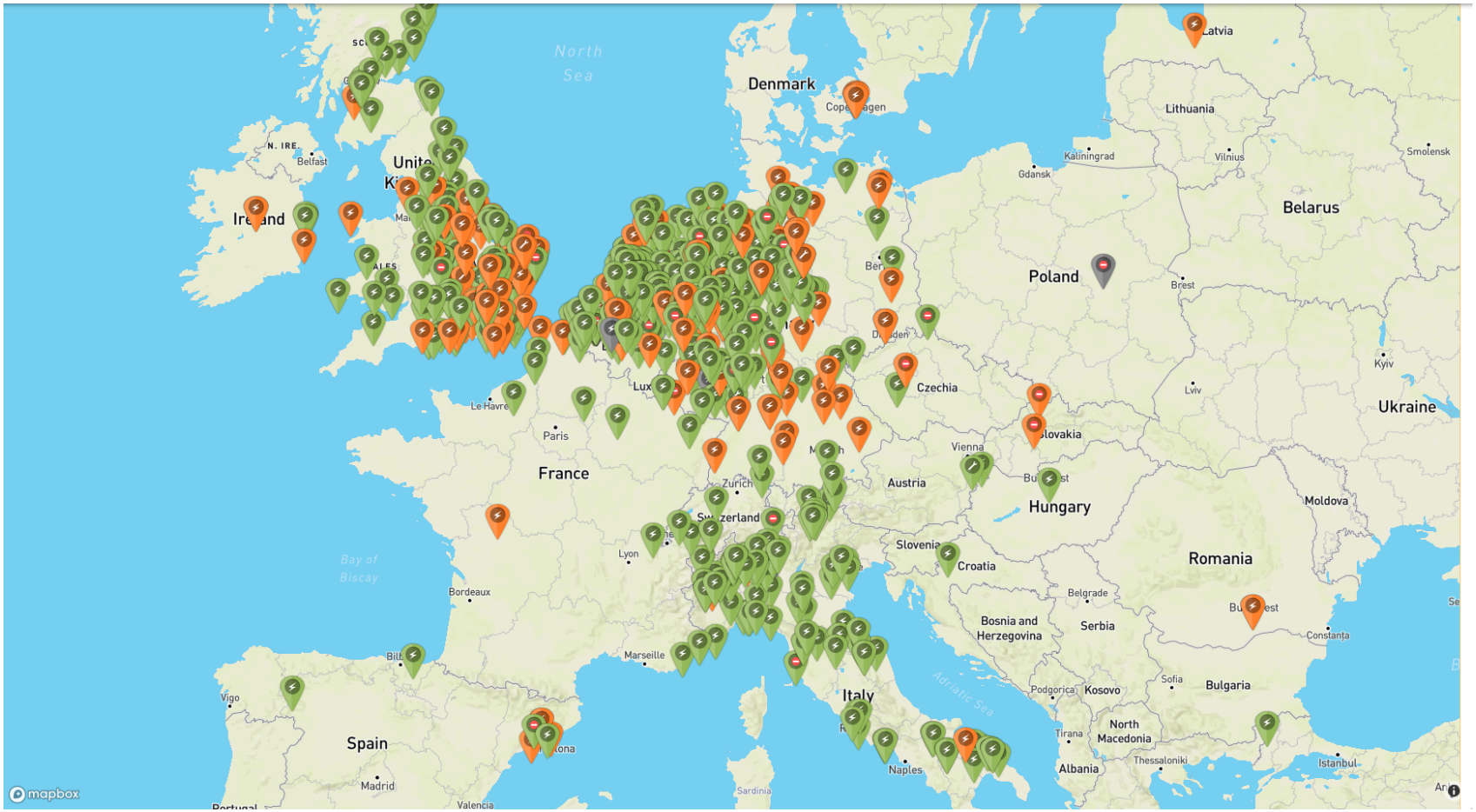


Source: openchargemap.io

Where is the EV-charging infrastructure?

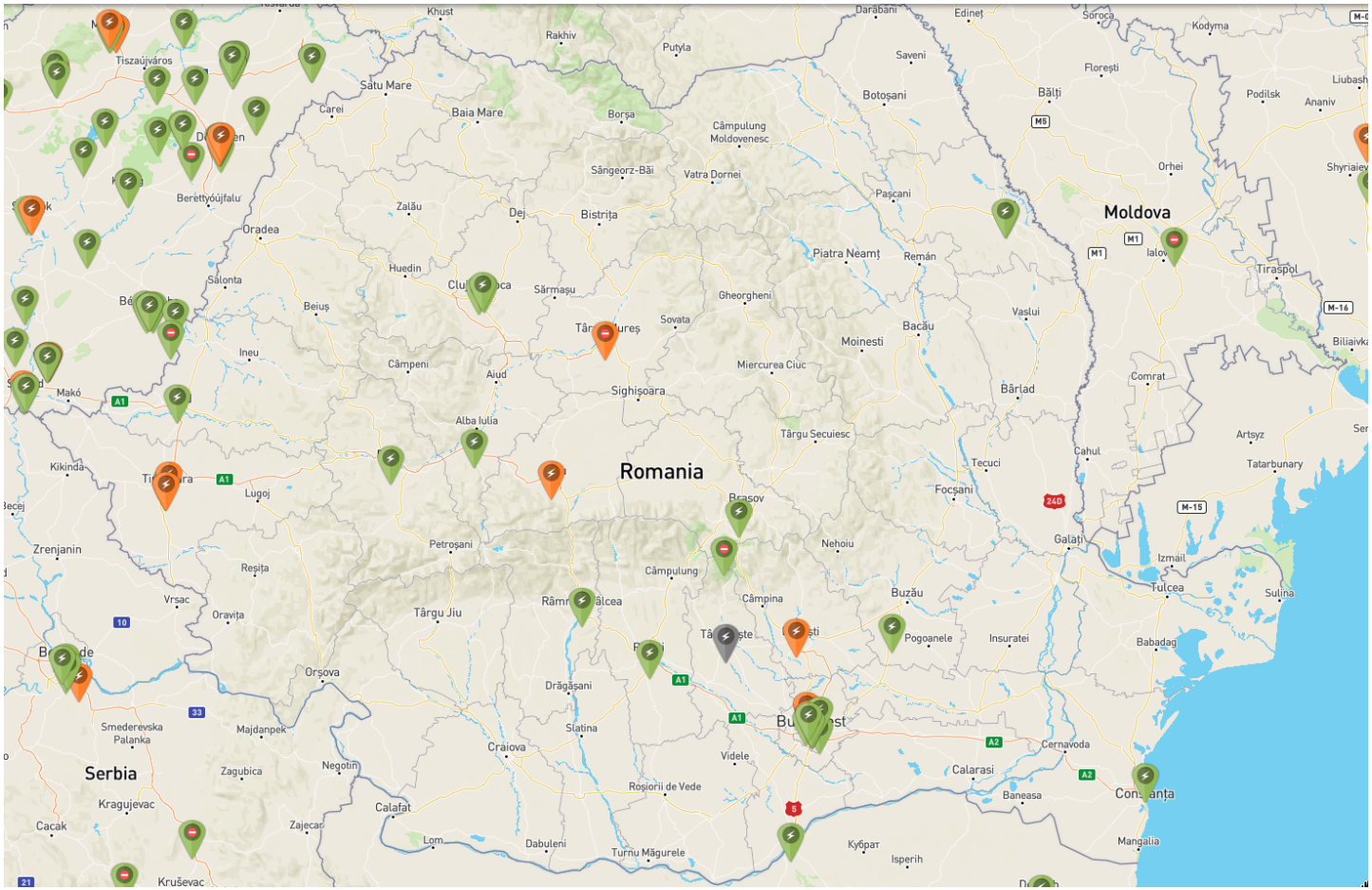
Source: openchargemap.io

Where is the EV-charging infrastructure?



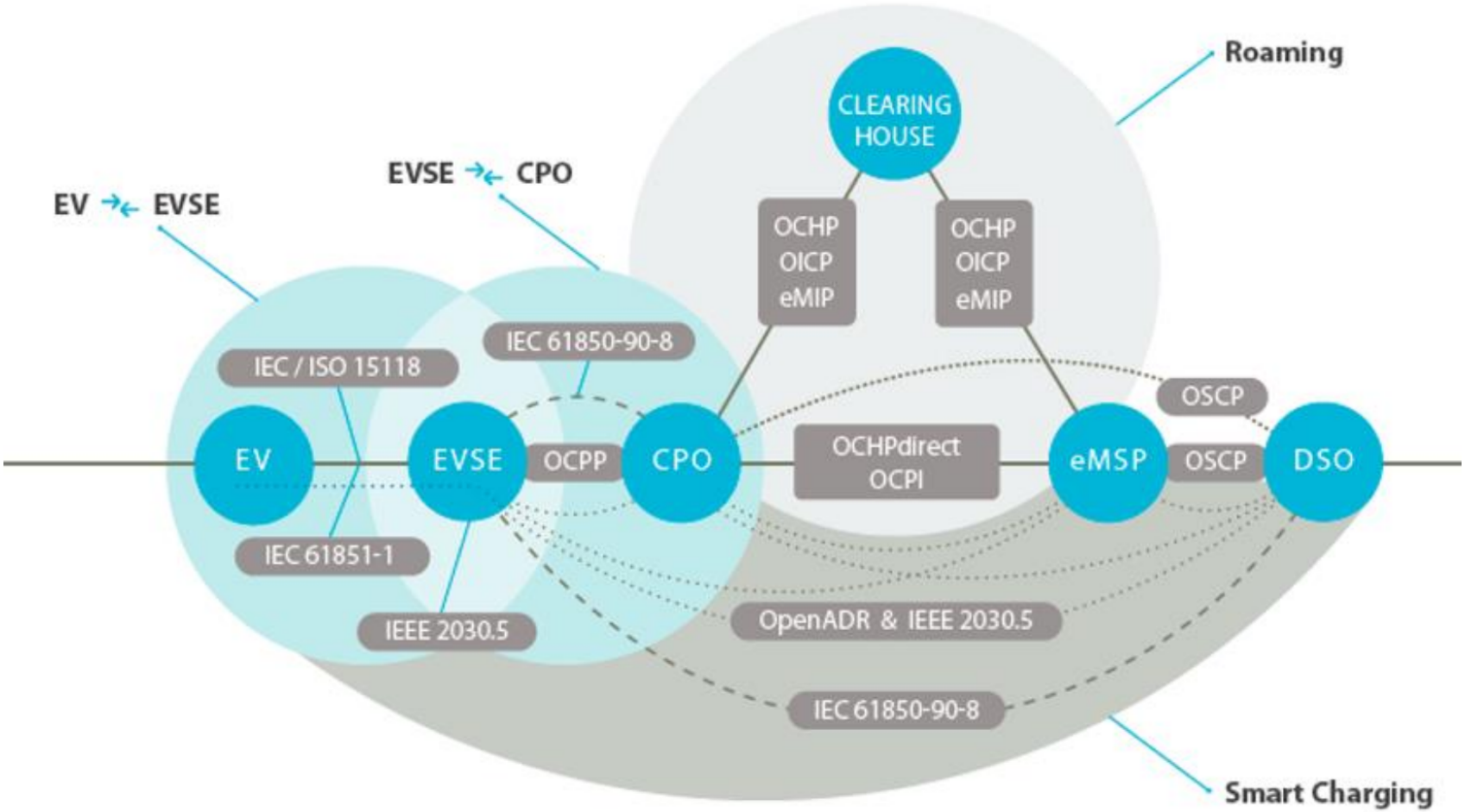
Source: openchargemap.io

Where is the EV-charging infrastructure?



Source: openchargemap.io

What is the EV-charging infrastructure?



Source: EV Related Protocol Study – ElaadNL

Most important aspects

- Many roles, fulfilled by many different parties.

Most important aspects

- Many roles, fulfilled by many different parties.
- The only way for some of these to communicate is *via other parties*.

Overview

What could go wrong?

- Fraud

What could go wrong?

- Fraud
- Vandalism

What could go wrong?

- Fraud
- Vandalism
- Activism

What could go wrong?

- Fraud
- Vandalism
- Activism
  - "Chaos Computer Club hacks e-motor charging stations" https://www.ccc.de/en/updates/2017/e-motor

What could go wrong?

- Fraud
- Vandalism
- Activism
  - "Chaos Computer Club hacks e-motor charging stations" https://www.ccc.de/en/updates/2017/e-motor
- Grid destabilization

What could go wrong?

- Fraud
- Vandalism
- Activism
  - "Chaos Computer Club hacks e-motor charging stations"
    https://www.ccc.de/en/updates/2017/e-motor
- Grid destabilization
  - Horus Scenario: hacking PV-installations
    https://horusscenario.com/

What could go wrong?

- Fraud
- Vandalism
- Activism
  - "Chaos Computer Club hacks e-motor charging stations"
    https://www.ccc.de/en/updates/2017/e-motor
- Grid destabilization
  - Horus Scenario: hacking PV-installations
    https://horusscenario.com/
  - "Public Plug-in Electric Vehicles + Grid Data:
    Is a New Cyberattack Vector Viable?"
    https://arxiv.org/abs/1907.08283

What could go wrong?

- Privacy breaches

What could go wrong?

- Privacy breaches
  - Customer location is sensitive information!

What could go wrong?

- Privacy breaches
  - Customer location is sensitive information!
  - What other information should be secret?

What could go wrong?

- Privacy breaches
  - Customer location is sensitive information!
  - What other information should be secret?
  - GDPR compliance is not straightforward.

Current state of security

- Authentication / authorization with RFID cards

Current state of security

- Authentication / authorization with RFID cards
- Some TLS, lacking clear instructions

Envisioned state of security

- Strong authentication using challenge-response

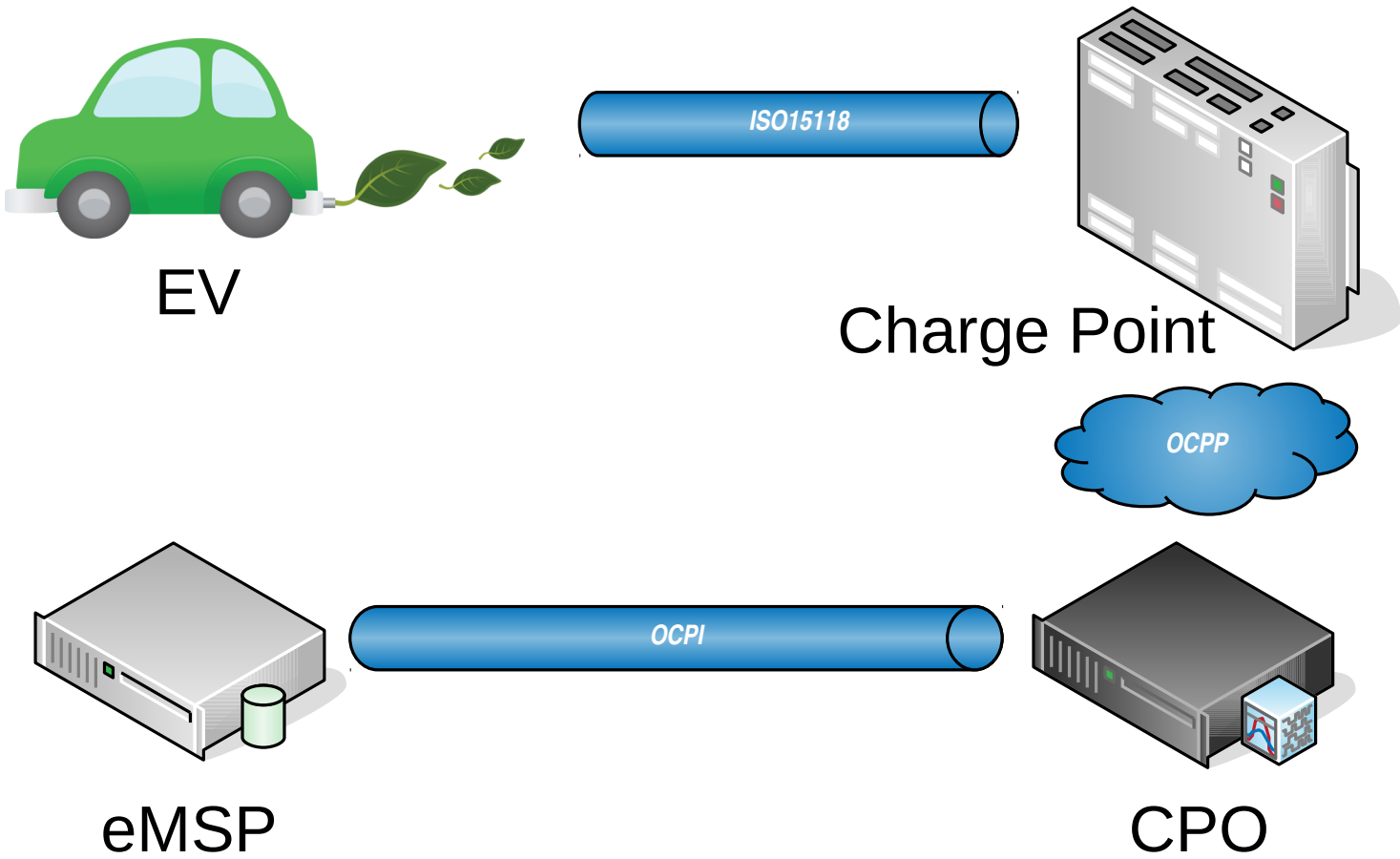
Envisioned state of security

- Strong authentication using challenge-response
- TLS everywhere, standardized & specified well

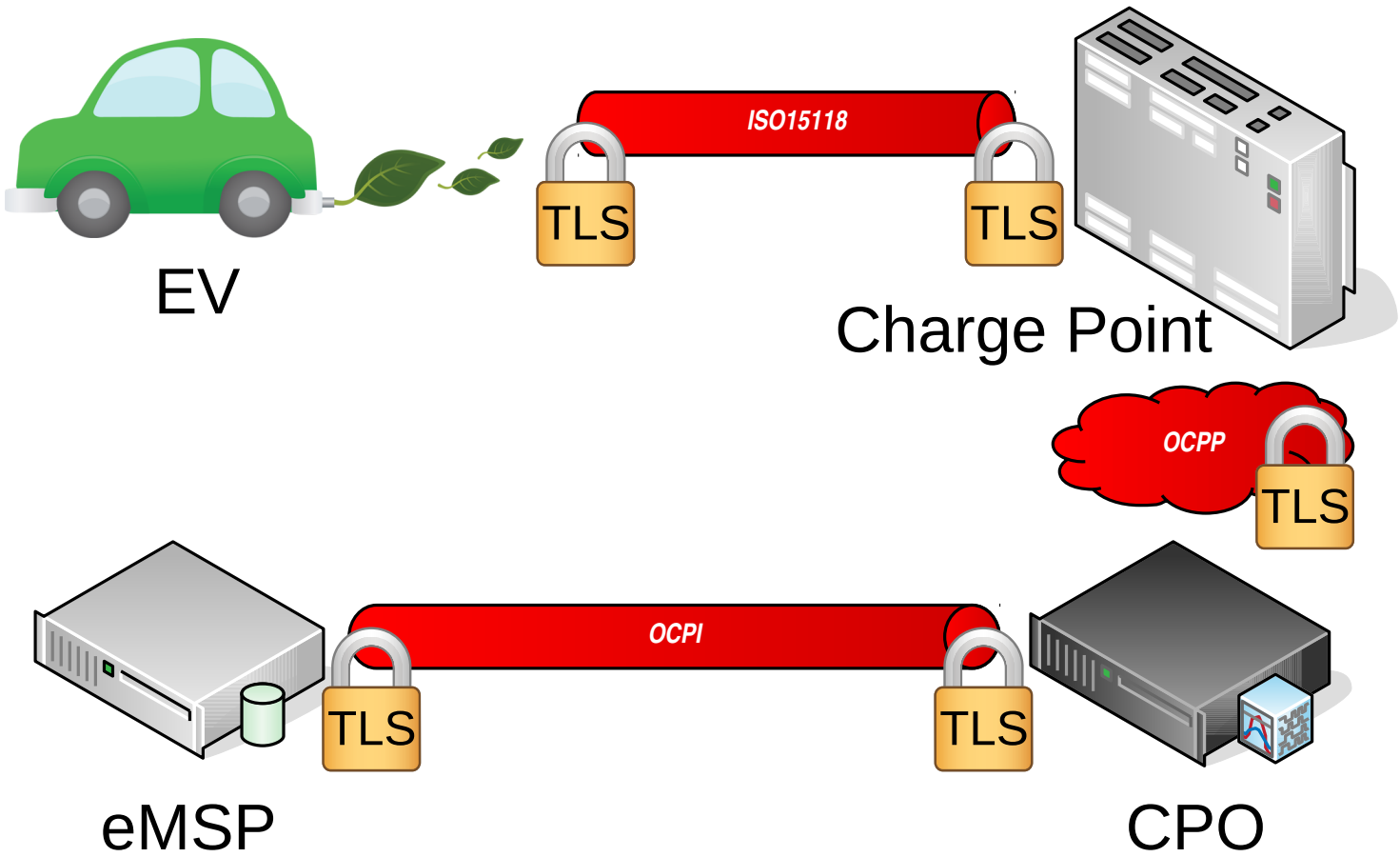
Envisioned state of security

- Strong authentication using challenge-response
- TLS everywhere, standardized & specified well
- Better implementations and testing

Are we done then?



Are we done then?



We're not done

- TLS protects the network traffic between individual parties.

We're not done

- TLS protects the network traffic between individual parties.
- Provides confidentiality and authenticity for the data *only while being communicated* between these parties.

Trust

We have to trust that every party

- doesn't send what it shouldn't,

Trust

We have to trust that every party

- doesn't send what it shouldn't,
- doesn't change what it relays,

Trust

We have to trust that every party

- doesn't send what it shouldn't,
- doesn't change what it relays,
- doesn't peek at what it shouldn't see,

Trust

We have to trust that every party

- doesn't send what it shouldn't,
- doesn't change what it relays,
- doesn't peek at what it shouldn't see,
- doesn't later dispute sending something,

Trust

We have to trust that every party

- doesn't send what it shouldn't,
- doesn't change what it relays,
- doesn't peek at what it shouldn't see,
- doesn't later dispute sending something,

for whatever reason.

Overview

What is end-to-end security?

Main aspects:

- confidentiality.

What is end-to-end security?

Main aspects:

- confidentiality.
- authenticity.

What is end-to-end security?

Main aspects:

- confidentiality.
- authenticity.
- non-repudiation.

What is end-to-end security?

Main aspects:

- confidentiality.
- authenticity.
- non-repudiation.
- from end to end:

What is end-to-end security?

Main aspects:

- confidentiality.
- authenticity.
- non-repudiation.
- from end to end:
  - from the initial sending party on one side,

What is end-to-end security?

Main aspects:

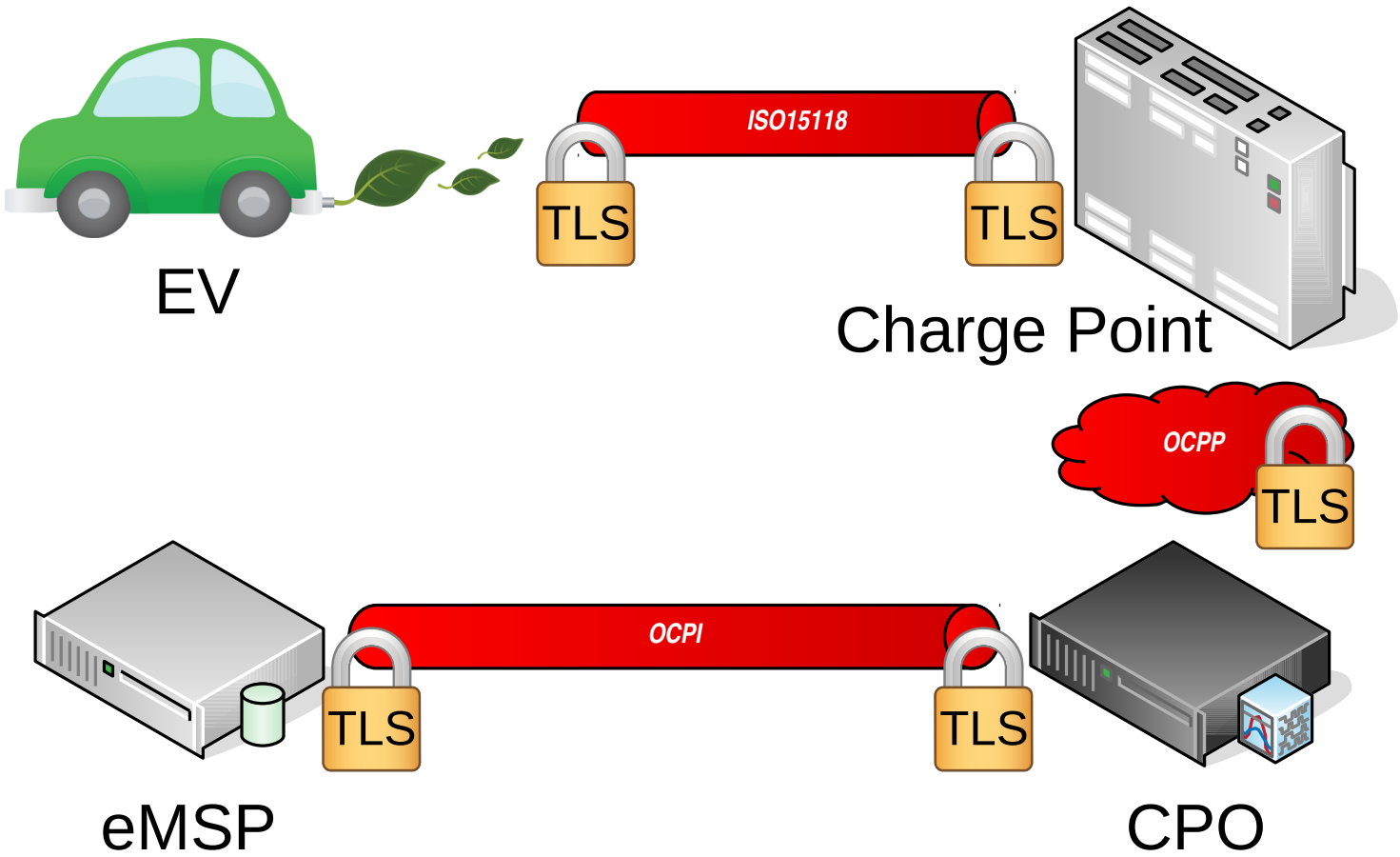
- confidentiality.
- authenticity.
- non-repudiation.
- from end to end:
  - from the initial sending party on one side,
  - to the eventual receiving party on the other side,

What is end-to-end security?

Main aspects:

- confidentiality.
- authenticity.
- non-repudiation.
- from end to end:
  - from the initial sending party on one side,
  - to the eventual receiving party on the other side,
  - regardless of how many parties are in between.

This is not end-to-end!



And it doesn't provide non-repudiation!

- Long-term guarantee of authenticity

And it doesn't provide non-repudiation!

- Long-term guarantee of authenticity
- Proof that a message was produced by that party

And it doesn't provide non-repudiation!

- Long-term guarantee of authenticity
- Proof that a message was produced by that party
  - (very useful in disputes!)

An example message

Charge Session Start sent from EV to CPO

EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21

An example message

Charge Session Start sent from EV to CPO

EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21

Charge Session Start sent from CPO to eMSP

EV ID	Time
101	2019-09-30 14:50

Contract ID	€/kWh
12501932	0.21

An example message

Charge Session Start sent from EV to CPO

EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21

Charge Session Start sent from CPO to eMSP

EV ID	Time
101	2019-09-30 14:50

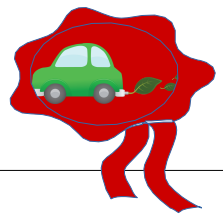
Contract ID	€/kWh
12501932	0.21

CP Location is dropped because the eMSP doesn't need it.

Adding authenticity & non-repudiation – naïvely

Charge Session Start sent from EV to CPO

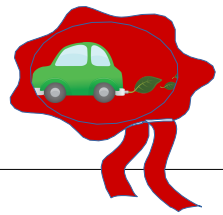
EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21



Adding authenticity & non-repudiation – naïvely

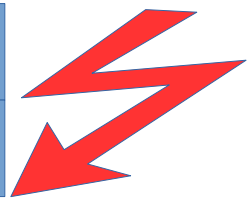
Charge Session Start sent from EV to CPO

EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21



Charge Session Start sent from CPO to eMSP

EV ID	Time
101	2019-09-30 14:50

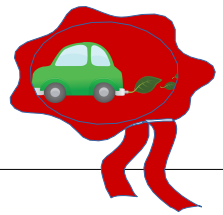


Contract ID	€/kWh
12501932	0.21

Adding authenticity & non-repudiation – naïvely

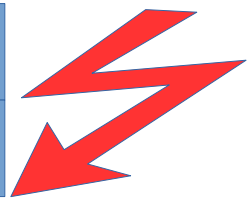
Charge Session Start sent from EV to CPO

EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21



Charge Session Start sent from CPO to eMSP

EV ID	Time
101	2019-09-30 14:50



Contract ID	€/kWh
12501932	0.21

CP Location cannot be dropped because that invalidates the signature!

Requirements:

- Authenticity & non-repudiation (signatures)

Requirements:

- Authenticity & non-repudiation (signatures)
- End-to-end secrecy (encryption)

Requirements:

- Authenticity & non-repudiation (signatures)
- End-to-end secrecy (encryption)
- Data minimization (omission)

Requirements:

- Authenticity & non-repudiation (signatures)
- End-to-end secrecy (encryption)
- Data minimization (omission)
  - GDPR-compliance: data must be removed if no longer needed

Requirements:

- Authenticity & non-repudiation (signatures)
- End-to-end secrecy (encryption)
- Data minimization (omission)
  - GDPR-compliance: data must be removed if no longer needed
  - Hard to achieve with normal signatures

Requirements:

- Authenticity & non-repudiation (signatures)
- End-to-end secrecy (encryption)
- Data minimization (omission)
  - GDPR-compliance: data must be removed if no longer needed
  - Hard to achieve with normal signatures
- Limited overhead (data billed per byte)

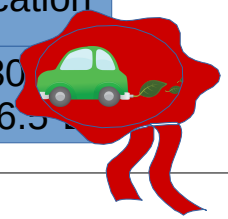
Requirements:

- Authenticity & non-repudiation (signatures)
- End-to-end secrecy (encryption)
- Data minimization (omission)
  - GDPR-compliance: data must be removed if no longer needed
  - Hard to achieve with normal signatures
- Limited overhead (data billed per byte)
- Offline operation (some parties may be offline when a message is sent)

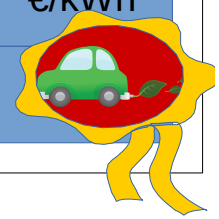
How do we solve this? Two signatures?

Charge Session Start sent from EV to CPO

EV ID	Time	CP Location
101	2019-09-30 14:50	51°49'30 5°52'06.5



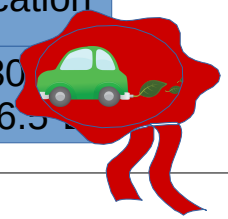
EV ID	Time	Contract ID	€/kWh
101	2019-09-30 14:50	12501932	



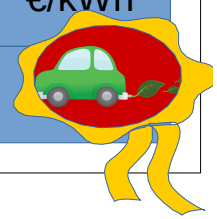
How do we solve this? Two signatures?

Charge Session Start sent from EV to CPO

EV ID	Time	CP Location
101	2019-09-30 14:50	51°49'30 5°52'06.5

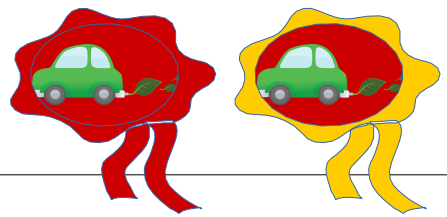


EV ID	Time	Contract ID	€/kWh
101	2019-09-30 14:50	12501932	



Charge Session Start sent from EV to CPO

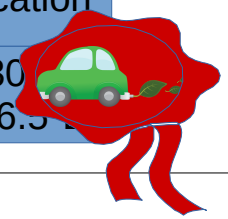
EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21



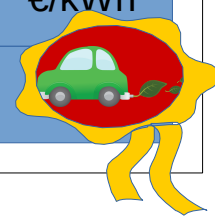
How do we solve this? Two signatures?

Charge Session Start sent from EV to CPO

EV ID	Time	CP Location
101	2019-09-30 14:50	51°49'30 5°52'06.5

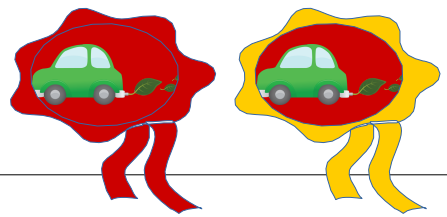


EV ID	Time	Contract ID	€/kWh
101	2019-09-30 14:50	12501932	



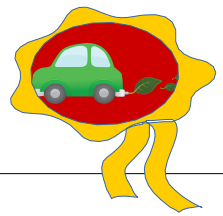
Charge Session Start sent from EV to CPO

EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21



Charge Session Start sent from CPO to eMSP

EV ID	Time	Contract ID	€/kWh
101	2019-09-30 14:50	12501932	0.21



This works, but...

- That's still a lot of overhead

This works, but...

- That's still a lot of overhead
- Doesn't solve data minimization

One signature using a hash tree

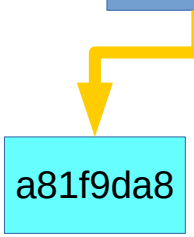
Signed Charge Session Start

EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21

We take the hashes of individual data fields

Signed Charge Session Start

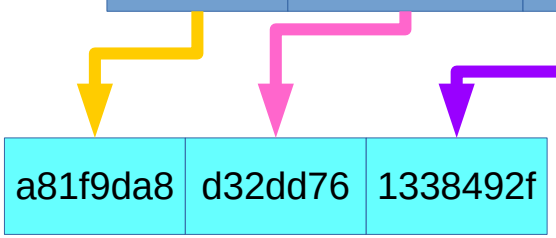
EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21



Build the collection of hashes...

Signed Charge Session Start

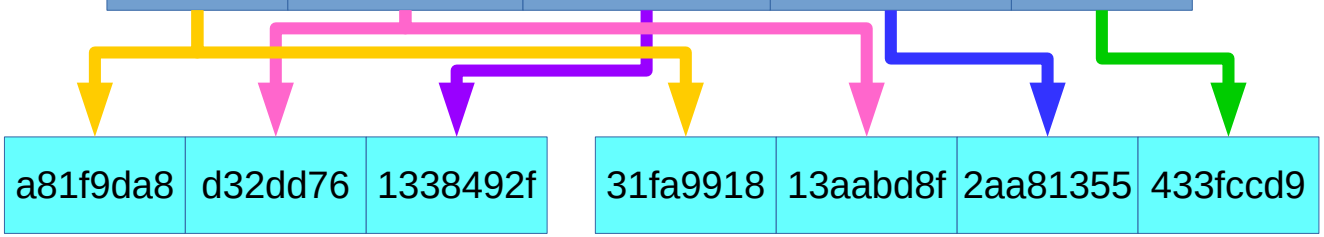
EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21



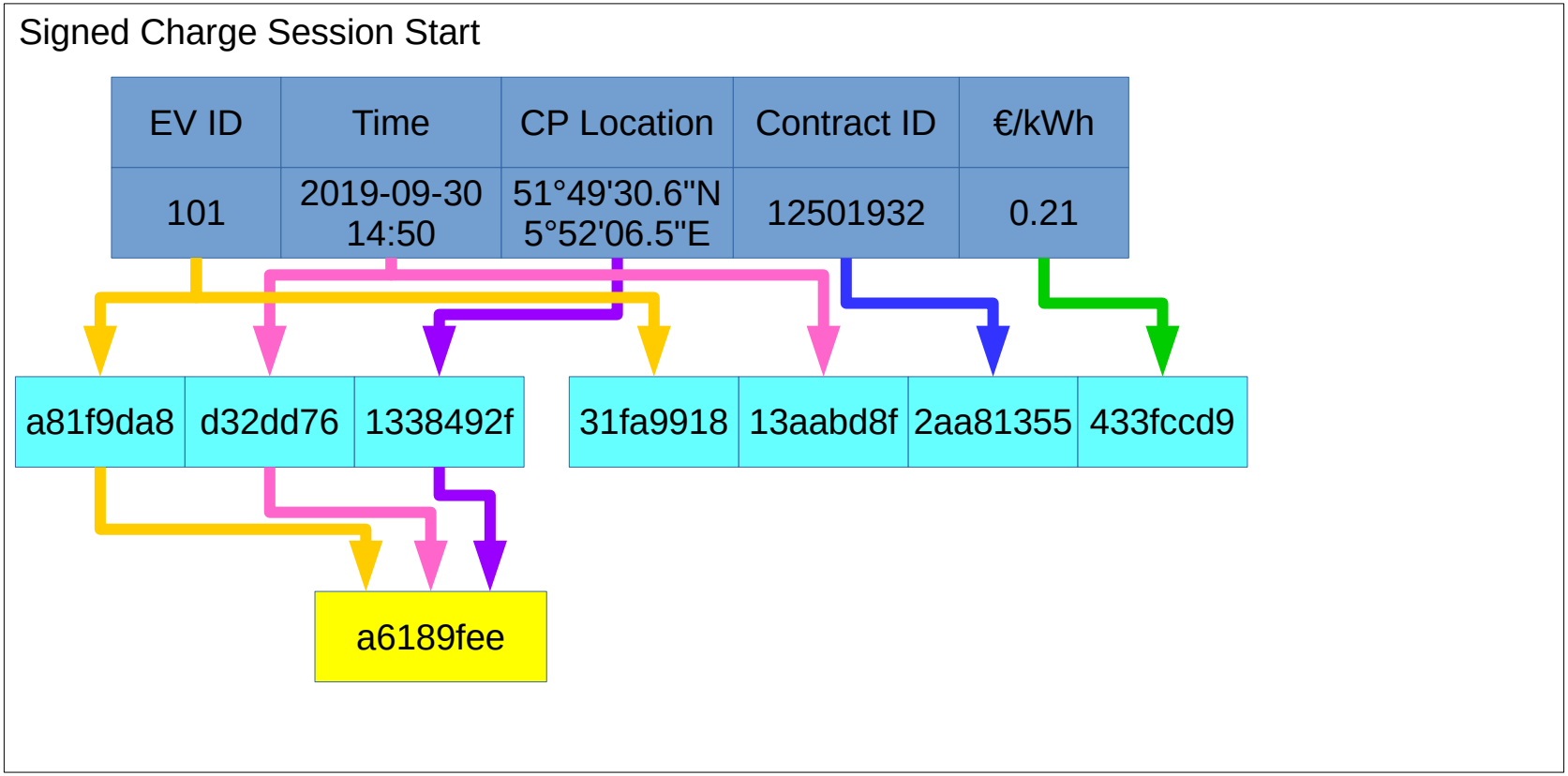
For each party that needs a signature

Signed Charge Session Start

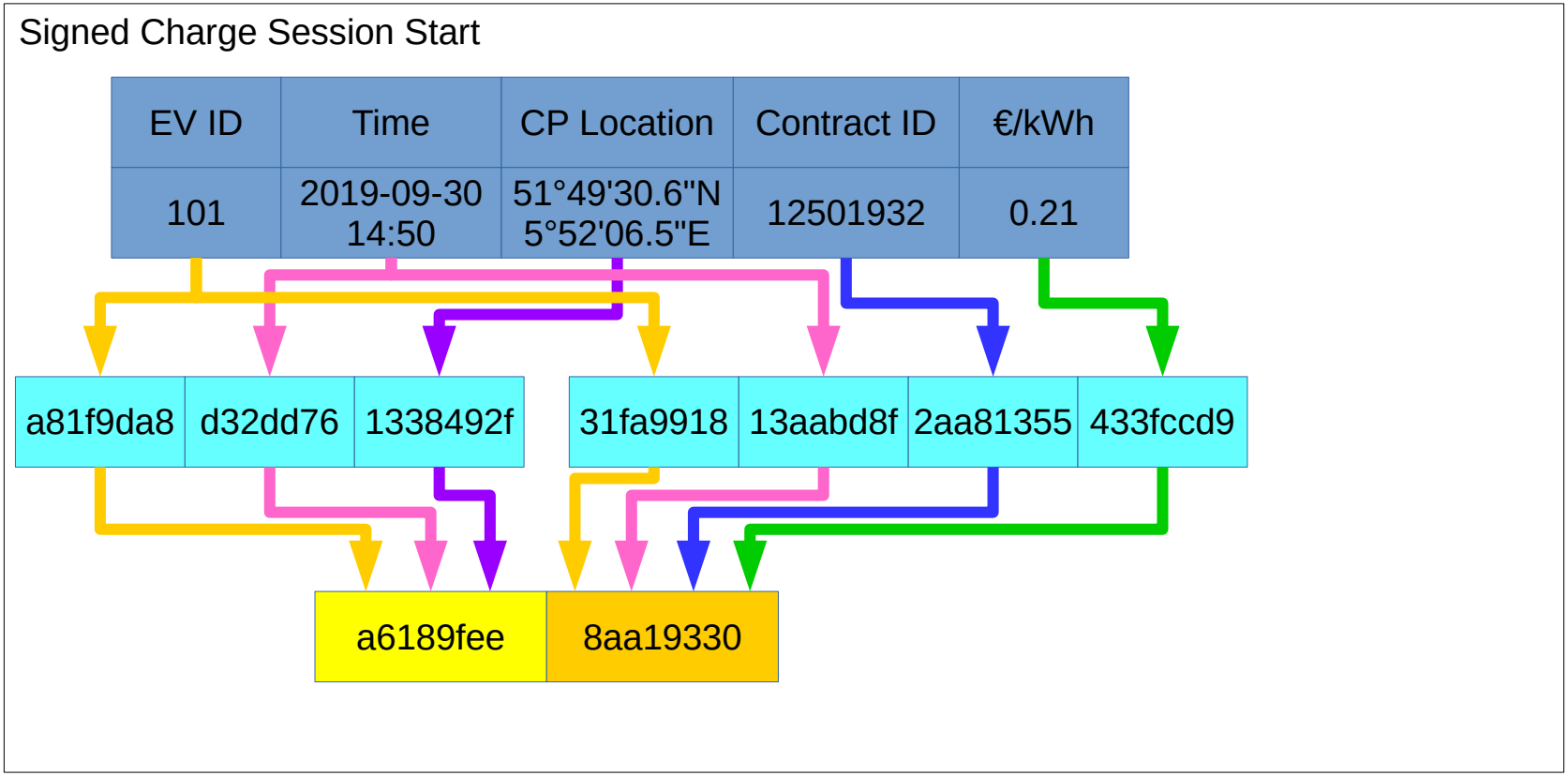
EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21



Then we hash those collections again...



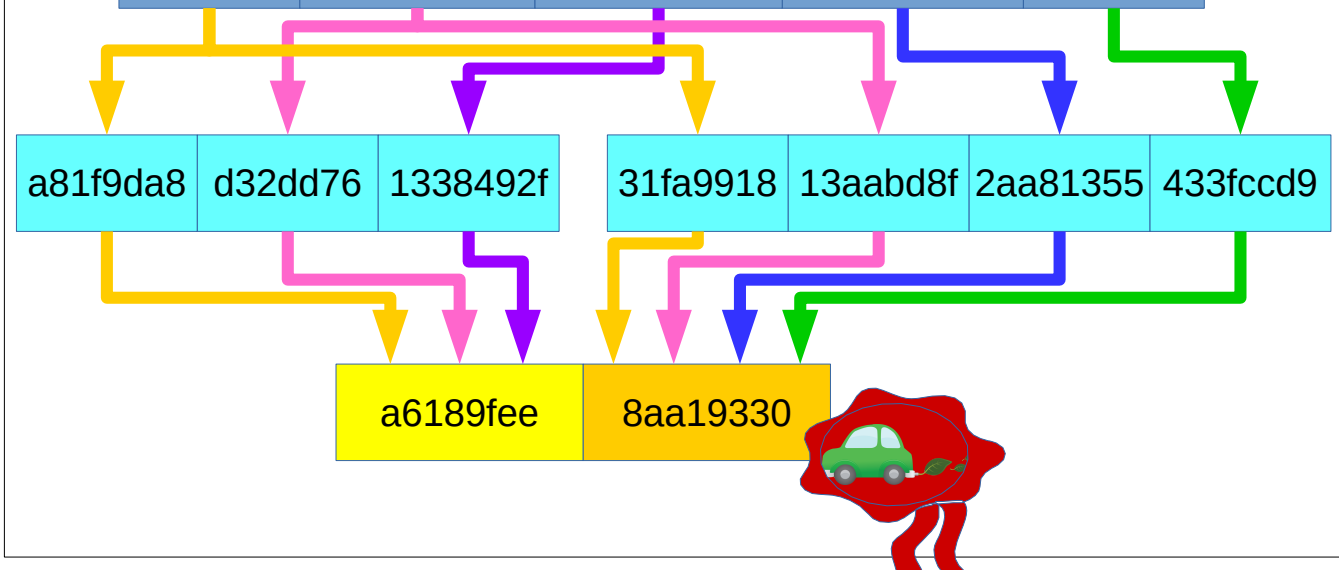
Into a final couple of hashes



And sign those hashes

Signed Charge Session Start

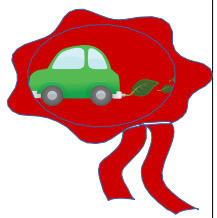
EV ID	Time	CP Location	Contract ID	€/kWh
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	12501932	0.21



Overhead is minimized

Signed Charge Session Start sent by EV to CPO

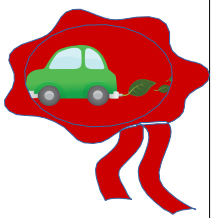
EV ID	Time	CP Location	Contract ID	€/kWh	eMSP Hash
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	Apf8da;w…	23ga…	8aa19330



CPO verification

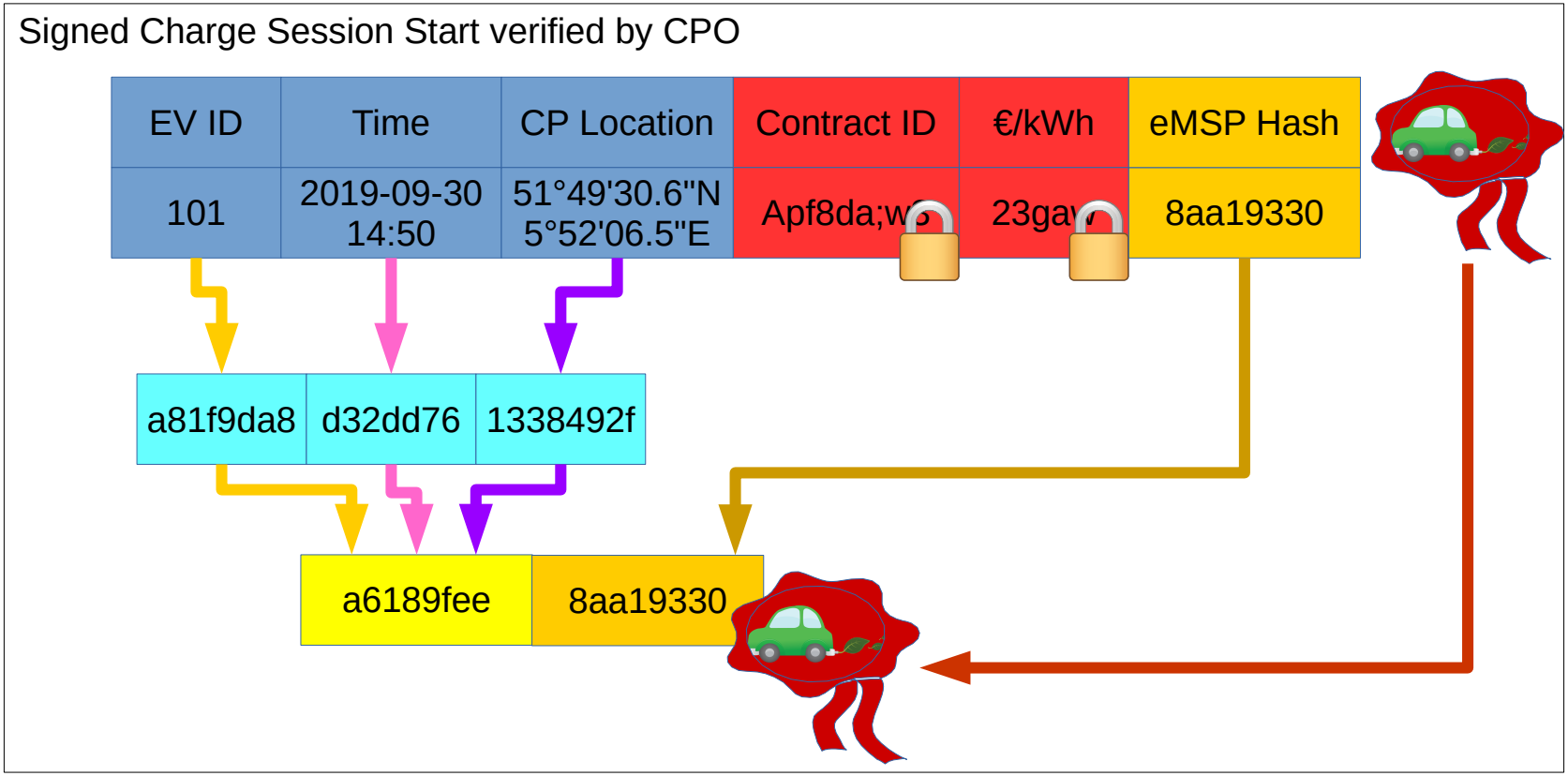
Signed Charge Session Start verified by CPO

EV ID	Time	CP Location	Contract ID	€/kWh	eMSP Hash
101	2019-09-30 14:50	51°49'30.6"N 5°52'06.5"E	Apf8da;w	23ga	8aa19330



a81f9da8	d32dd76	1338492f

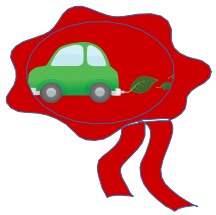
CPO verification



Dropping & encrypting data now works

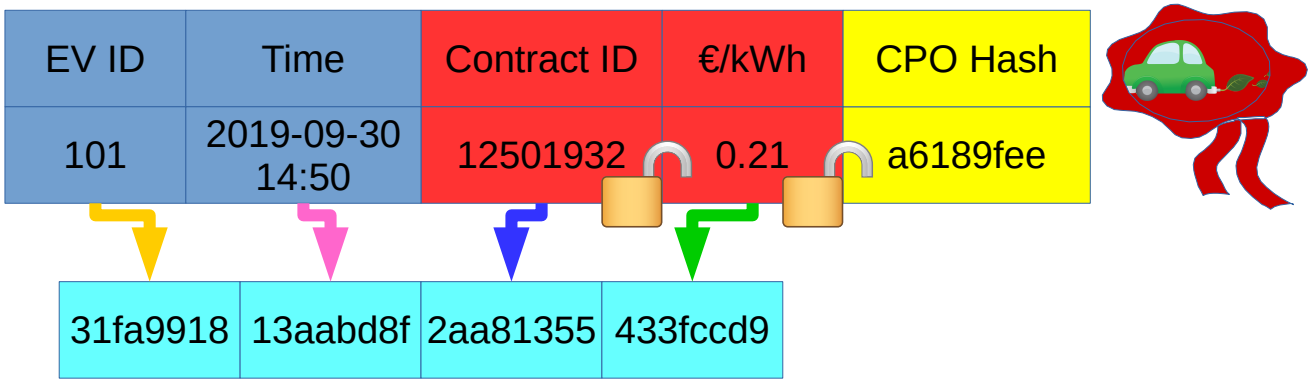
Signed Charge Session Start sent by CPO to eMSP

EV ID	Time	Contract ID	€/kWh	CPO Hash
101	2019-09-30 14:50	Apf8da;w	23gav	a6189fee

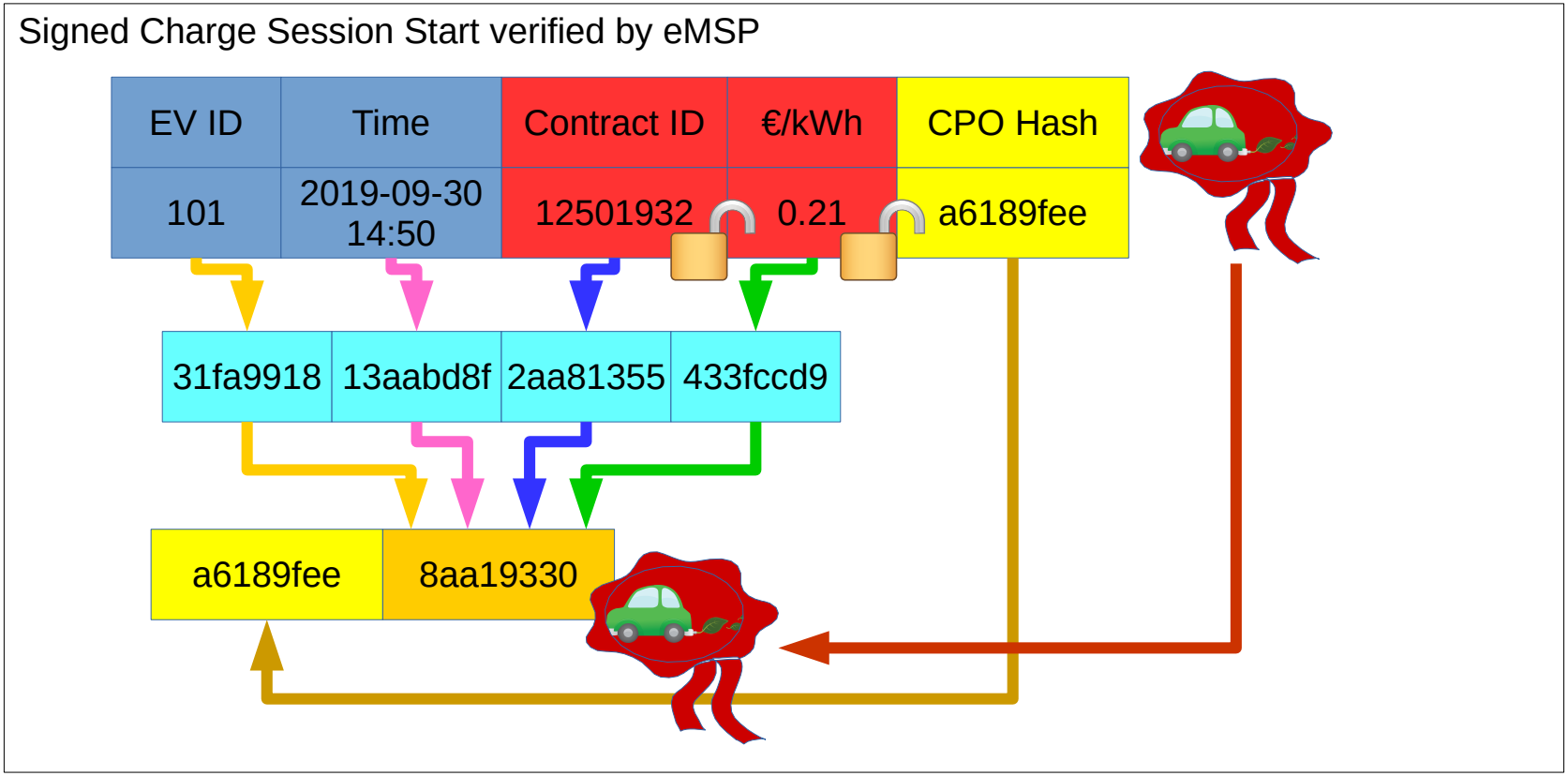


eMSP verification

Signed Charge Session Start verified by eMSP



eMSP verification



Cryptographic details

- We piggy-back on technologies that have to be present anyway:
  - Cryptographic algorithms from TLS
  - Public key infrastructure
  - JSON message formatting

Overview

The EV-charging infrastructure

The need for security

End-to-end security

Conclusions

Conclusions

- EV-charging infrastructure is complex, with many actors.

iCIS | Digital Security
Radboud University

Conclusions

- EV-charging infrastructure is complex, with many actors.
- Current security practices are not sufficient.

iCIS | Digital Security
Radboud University

Conclusions

- EV-charging infrastructure is complex, with many actors.
- Current security practices are not sufficient.
- Employing TLS everywhere is a necessary improvement, but

iCIS | Digital Security
Radboud University

Conclusions

- EV-charging infrastructure is complex, with many actors.
- Current security practices are not sufficient.
- Employing TLS everywhere is a necessary improvement, but
- TLS alone is not sufficient: We need true end-to-end security.

iCIS | Digital Security
Radboud University

Conclusions

- EV-charging infrastructure is complex, with many actors.
- Current security practices are not sufficient.
- Employing TLS everywhere is a necessary improvement, but
- TLS alone is not sufficient: We need true end-to-end security.
- This can be achieved using hash trees and selective encryption.

iCIS | Digital Security
Radboud University

Conclusions

- EV-charging infrastructure is complex, with many actors.
- Current security practices are not sufficient.
- Employing TLS everywhere is a necessary improvement, but
- TLS alone is not sufficient: We need true end-to-end security.
- This can be achieved using hash trees and selective encryption.
- Protocols will need to be changed to deal with this.

iCIS | Digital Security
Radboud University

Conclusions

- EV-charging infrastructure is complex, with many actors.
- Current security practices are not sufficient.
- Employing TLS everywhere is a necessary improvement, but
- TLS alone is not sufficient: We need true end-to-end security.
- This can be achieved using hash trees and selective encryption.
- Protocols will need to be changed to deal with this.
- The industry needs to agree on which party should see what data.

iCIS | Digital Security
Radboud University

Conclusions

- EV-charging infrastructure is complex, with many actors.
- Current security practices are not sufficient.
- Employing TLS everywhere is a necessary improvement, but
- TLS alone is not sufficient: We need true end-to-end security.
- This can be achieved using hash trees and selective encryption.
- Protocols will need to be changed to deal with this.
- The industry needs to agree on which party should see what data.
- This scheme works in other cases with similar requirements.

---

iCIS | Digital Security
Radboud University