



Security and Privacy
in the current e-mobility charging infrastructure



Where?

When?

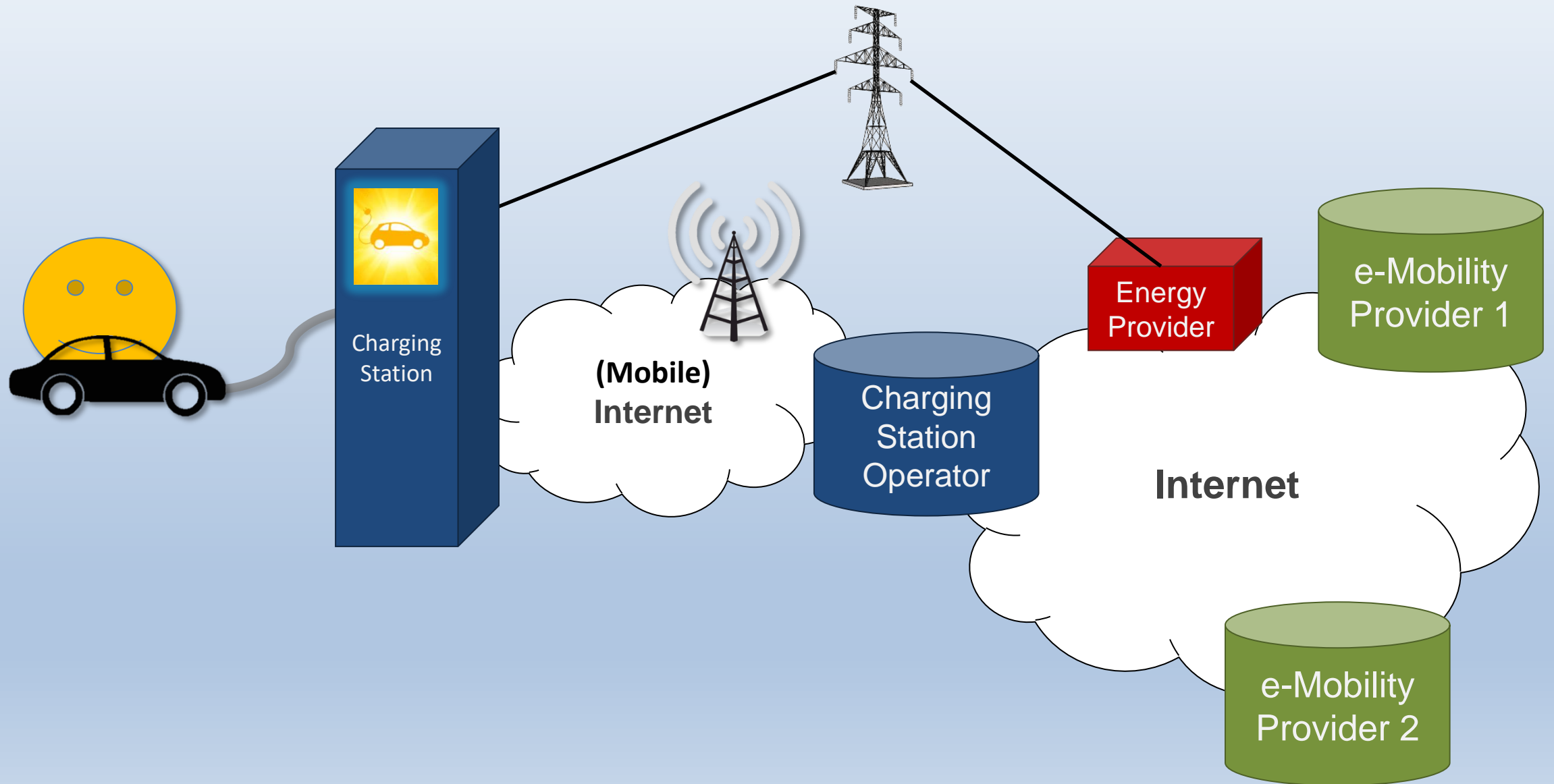
How to pay?



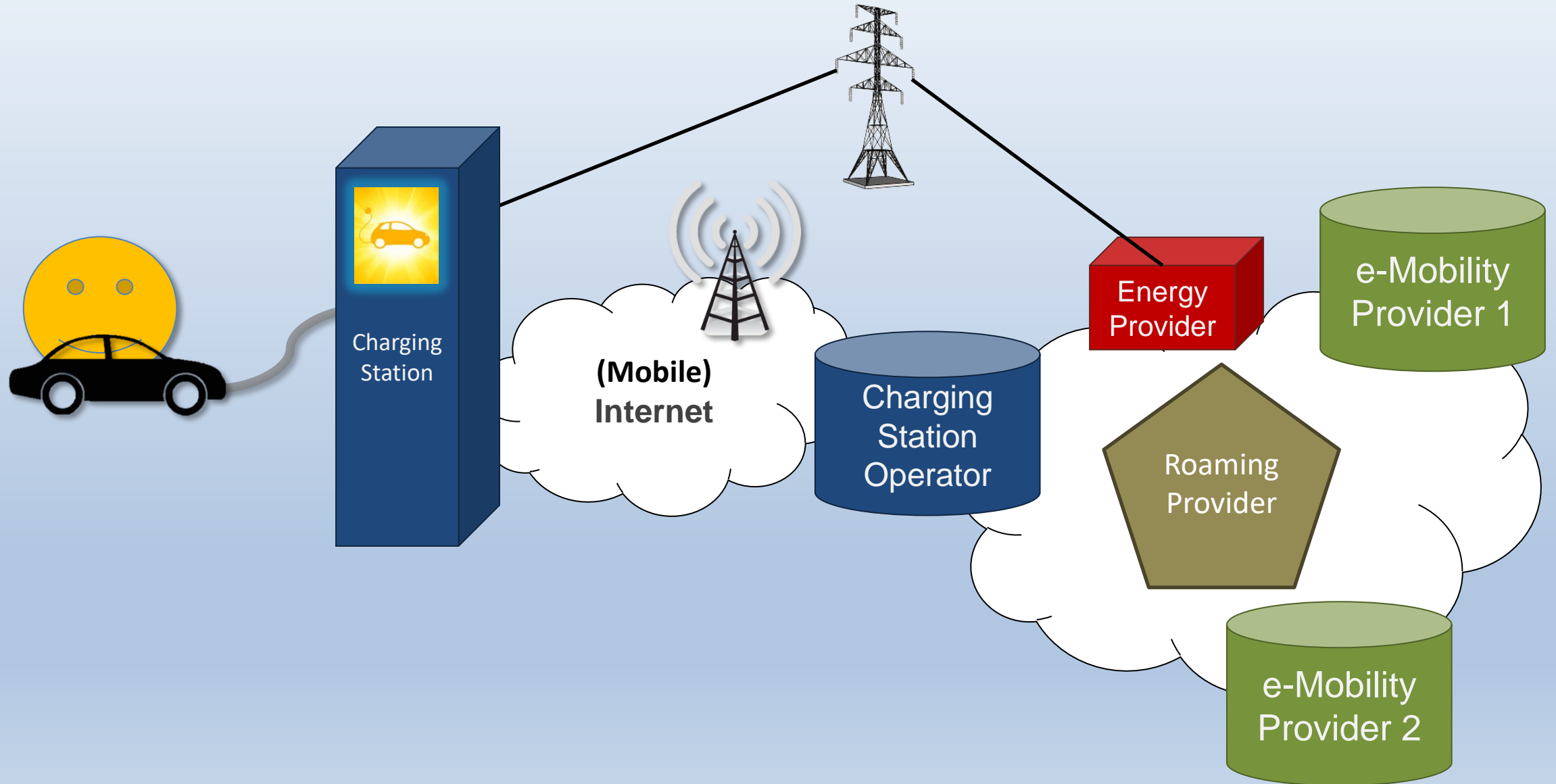
e-Mobility is 101%

IoT
eT

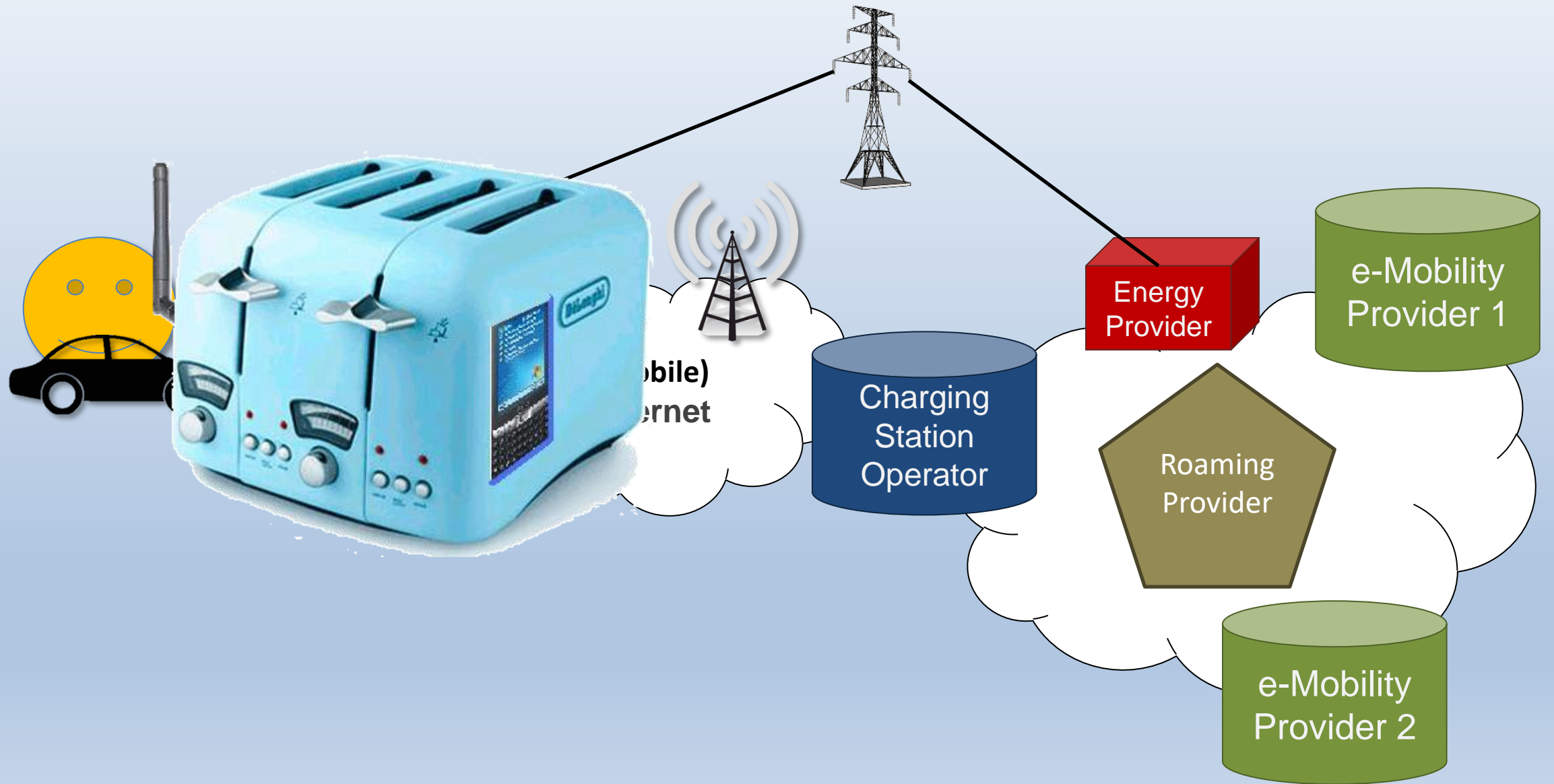
E-Mobility Network Architecture



E-Mobility Network Architecture



E-Mobility Network Architecture



Fuckup Level 1

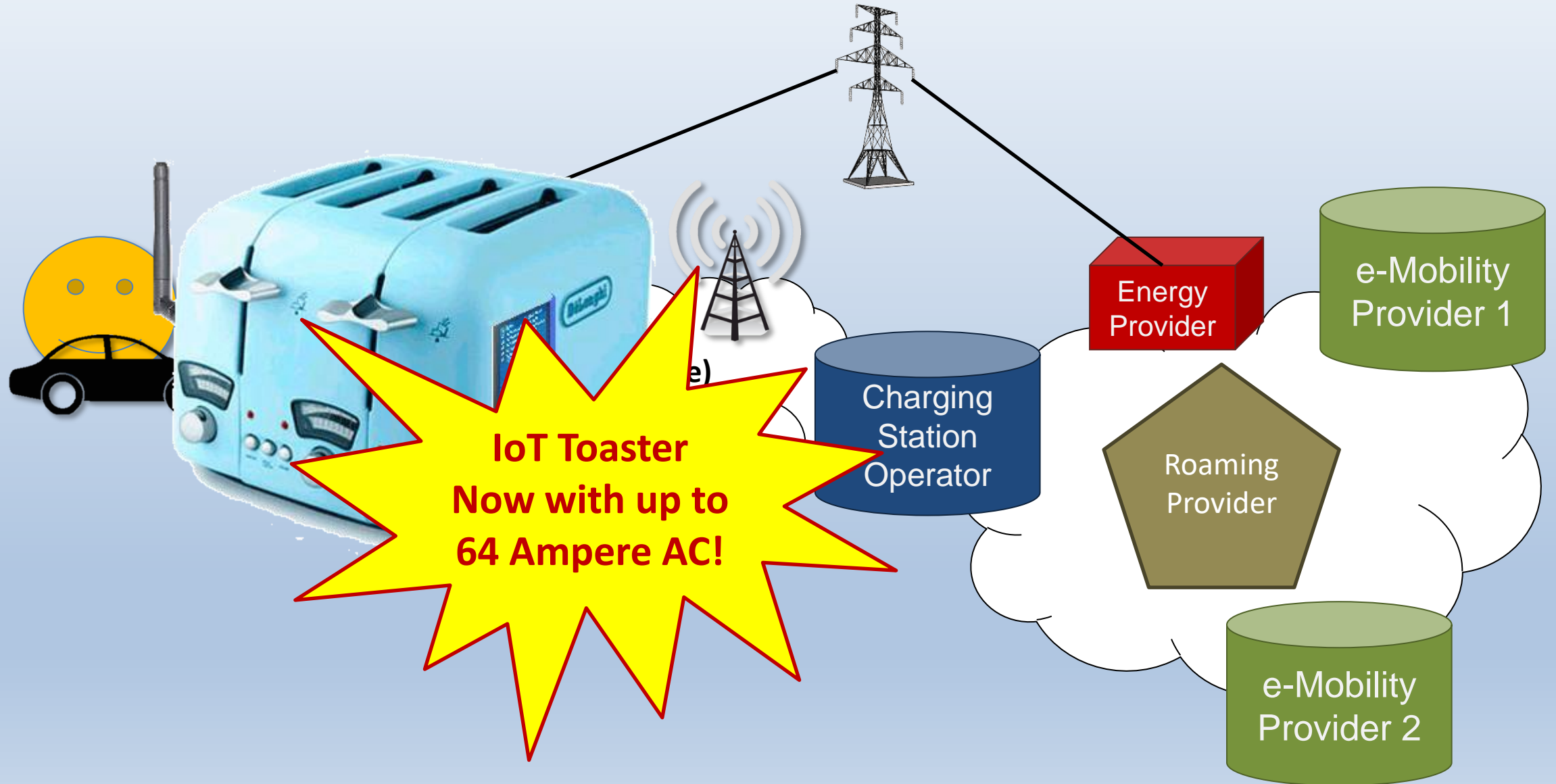
United States
of America

What could go wrong?

in the **IoT**?

Bahamas

E-Mobility Network Architecture



Fuckup Level 2

Someone „just“ stopped “smart charging”
10000 e-cars

What could go wrong?

in the **IoT**?

Fuckup Level 3

Der Staat gegen das Internet der unsicheren Dinge

Vom "digitalen Rettungsschuss" über Software-Haftung zum IT-Gütesiegel: Wie die Politik vielleicht retten kann, was der Markt im Internet der unsicheren Dinge vermasselt.

Von Jan-Peter Kleinhans

5. November 2016, 8:33 Uhr / [74 Kommentare](#)

Lät meh fix
se EloT vor u!



What could go wrong?

in the IoT?

Fuckup Level 4

What could go wrong?

in the **IoT**?

Fuckup Level n

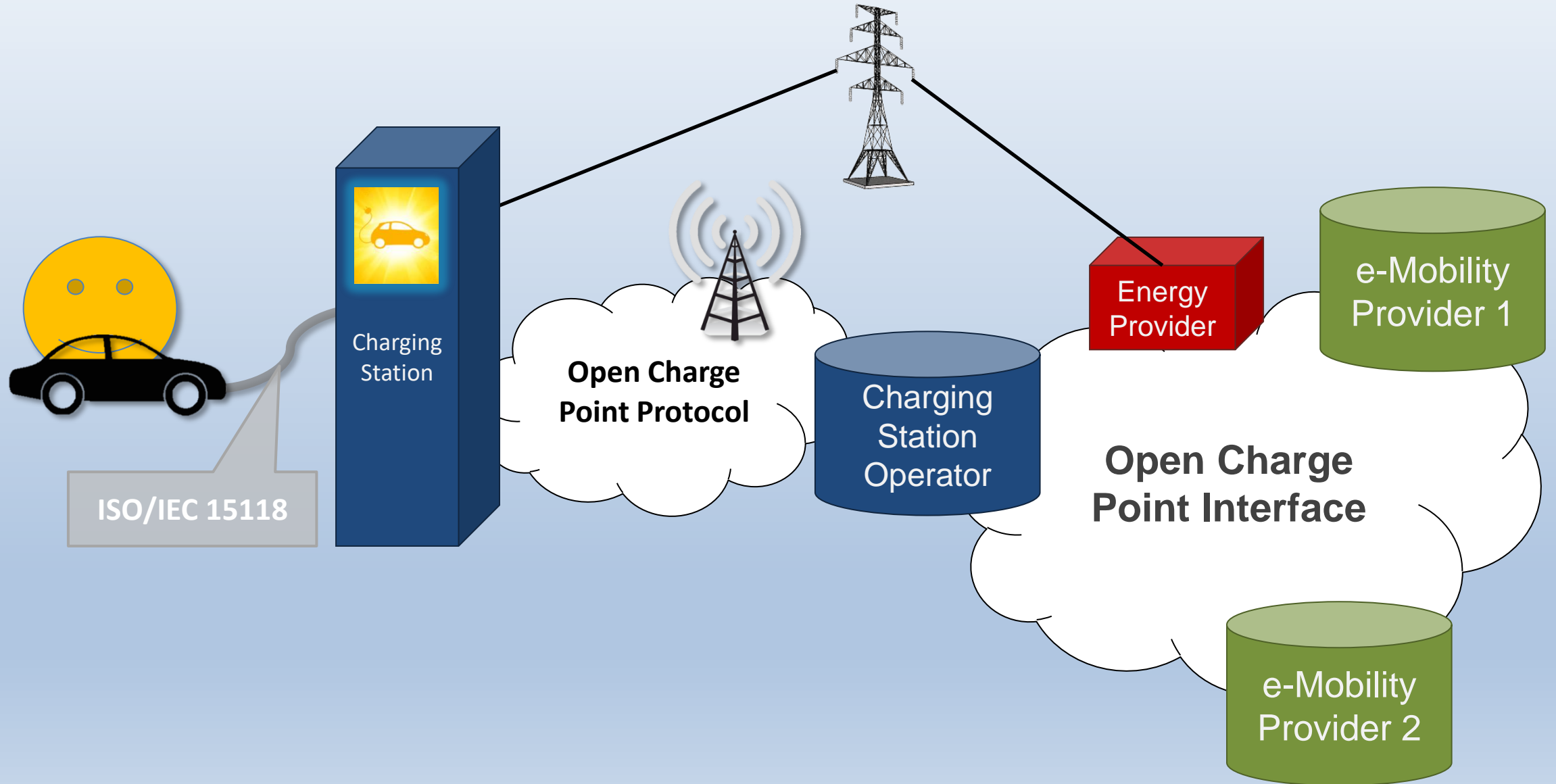
What could go wrong?

in the **IoT**?

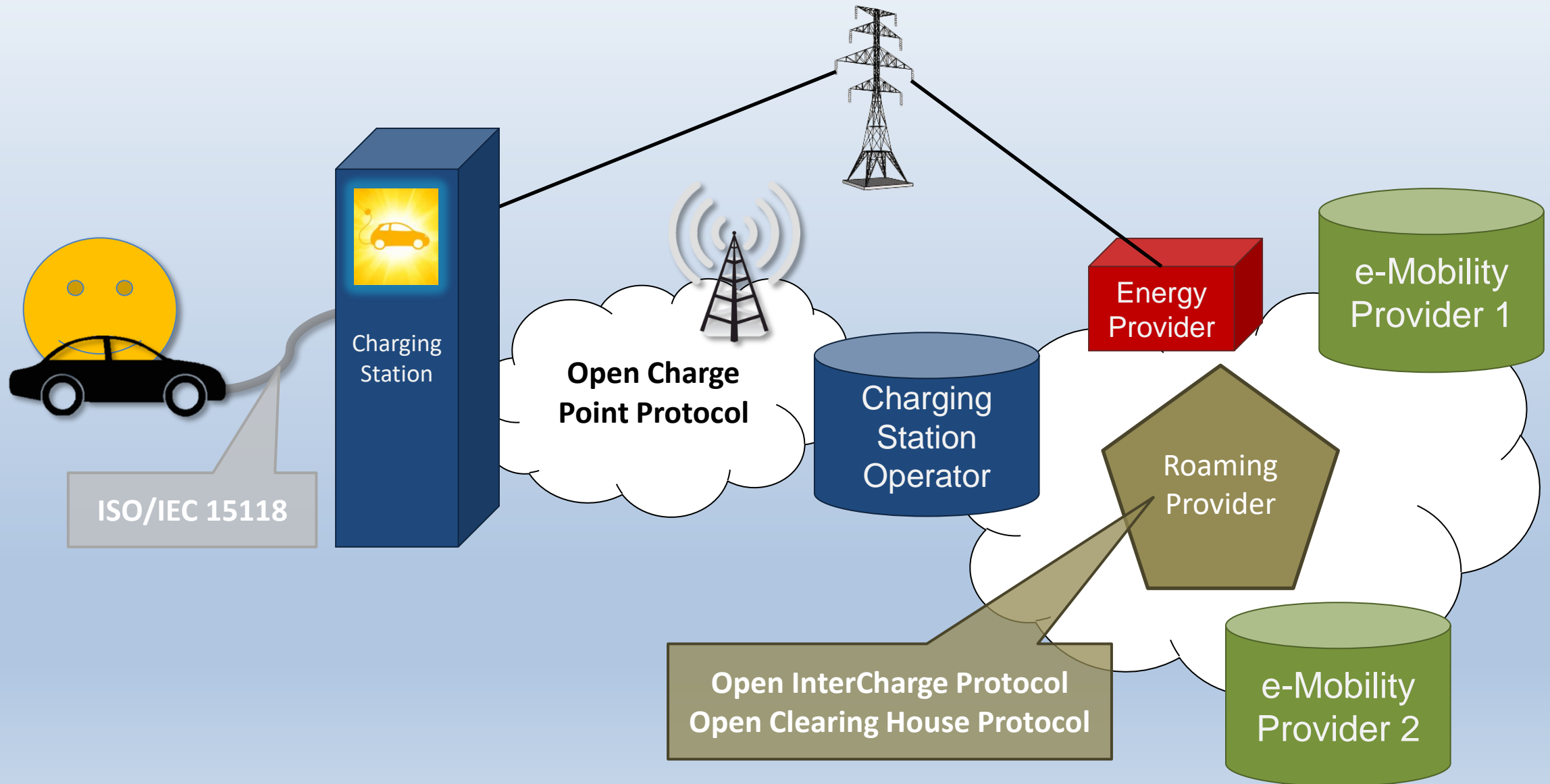
Network Architecture

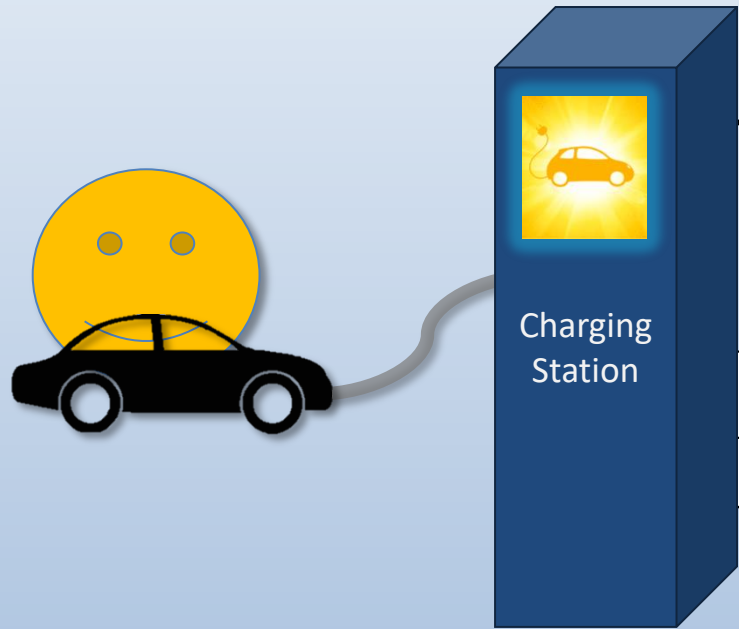
for charging e-vehicles

E-Mobility Network Architecture



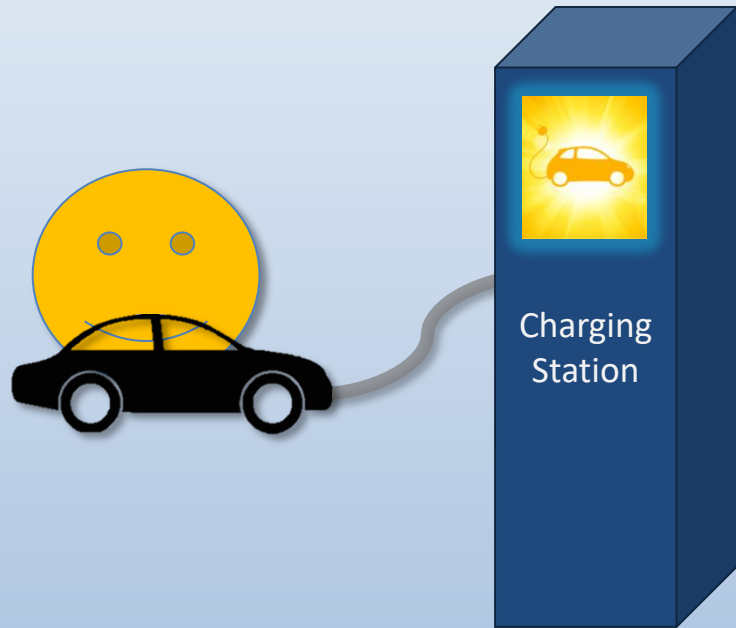
E-Mobility Network Architecture



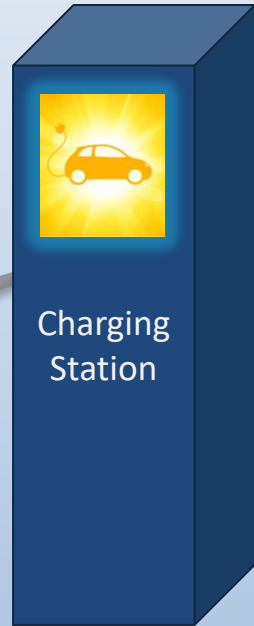


- Current version: OCPP v1.6
<http://www.openchargealliance.org>
- Worldwide utility-driven de facto ICT standard to manage charge points located in the streets
- HTTP/SOAP on both devices...
- ...or HTTP/WebSocket/JSON

Station
Operator



- Suggests use of TLS with client certs and VPNs/Private APNs when SOAP is used
- Discourages use of TLS because of communication overhead and client cert management complexity 🤪
WTF
- No standardized methods to manage network setting, certs, CA certs, ... most operators rely on network security or proprietary protocols
→ **There is no practical security at all!**



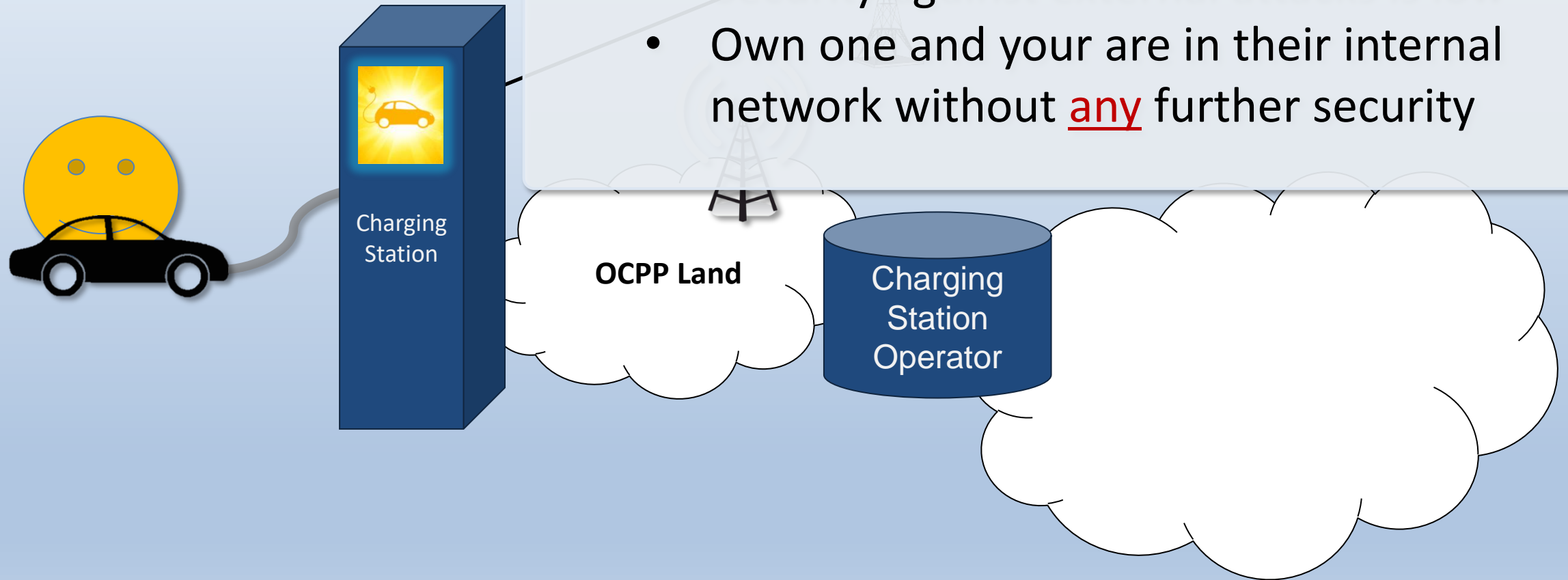
- What about firmware updates?

```
<soap:Envelope xmlns:soap = "http://www.w3.org/2003/05/soap-envelope"  
              xmlns:wsa = "http://www.w3.org/2005/08/addressing"  
              xmlns:ns = "urn://Ocpp/Cp/2015/10/">
```

```
<soap:Body>  
  <ns:updateFirmwareRequest>  
  
    <ns:retrieveDate?></ns:retrieveDate>  
    <ns:location?></ns:location>  
    <ns:retries?></ns:retries>          <!--Optional:-->  
    <ns:retryInterval?></ns:retryInterval> <!--Optional:-->
```

```
</ns:updateFirmwareRequest>  
</soap:Body>  
</soap:Envelope>
```

→ No security against even accidental mistakes



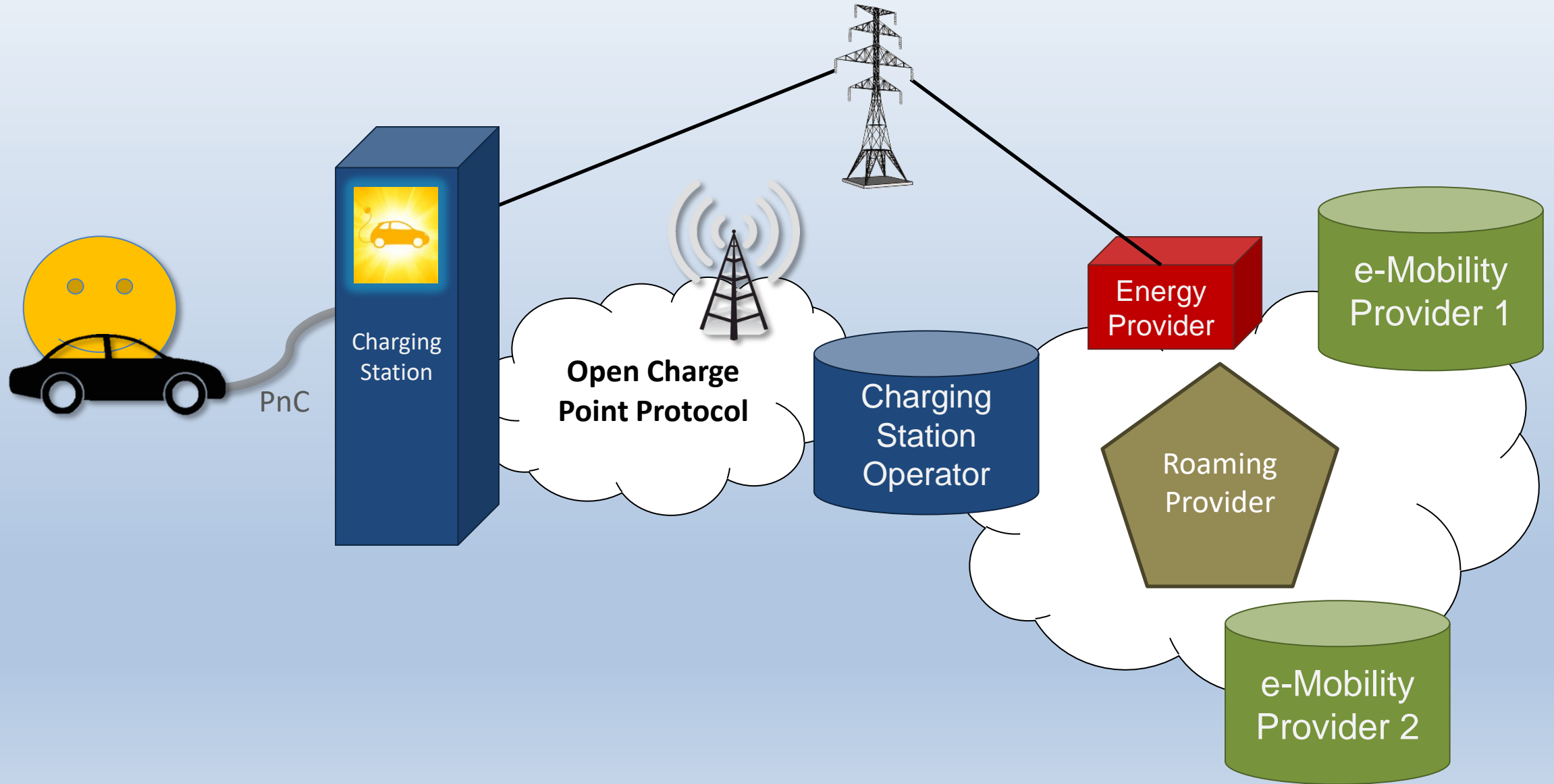
Conclusions

- Physical access to charging stations is easy
- Security against external attacks is low
- Own one and your are in their internal network without any further security

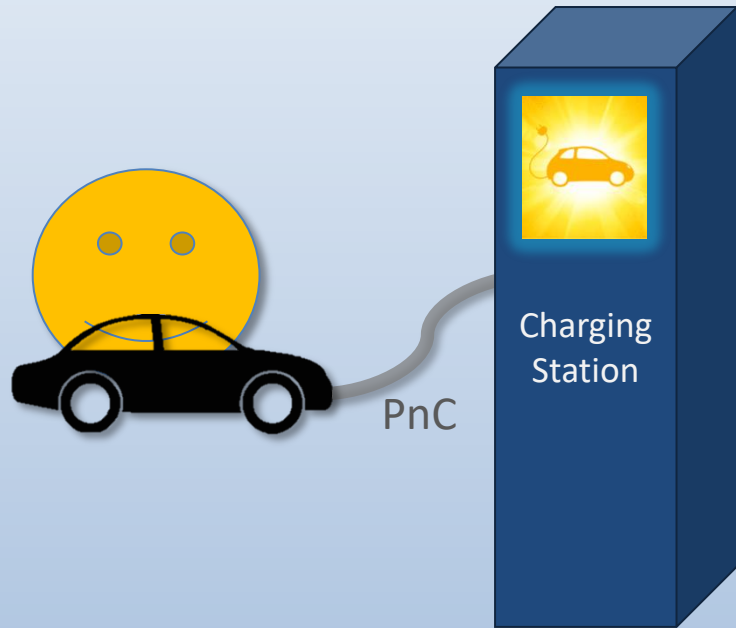
Local & Remote Authentication

at a Charging Station

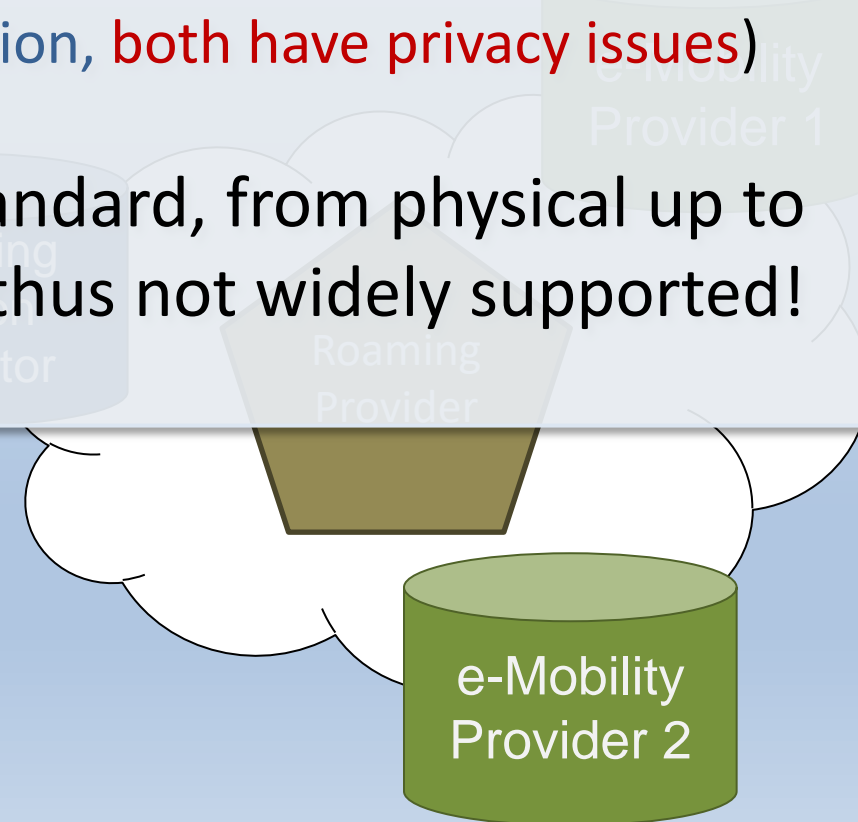
Local Authentication via PnC or RFID



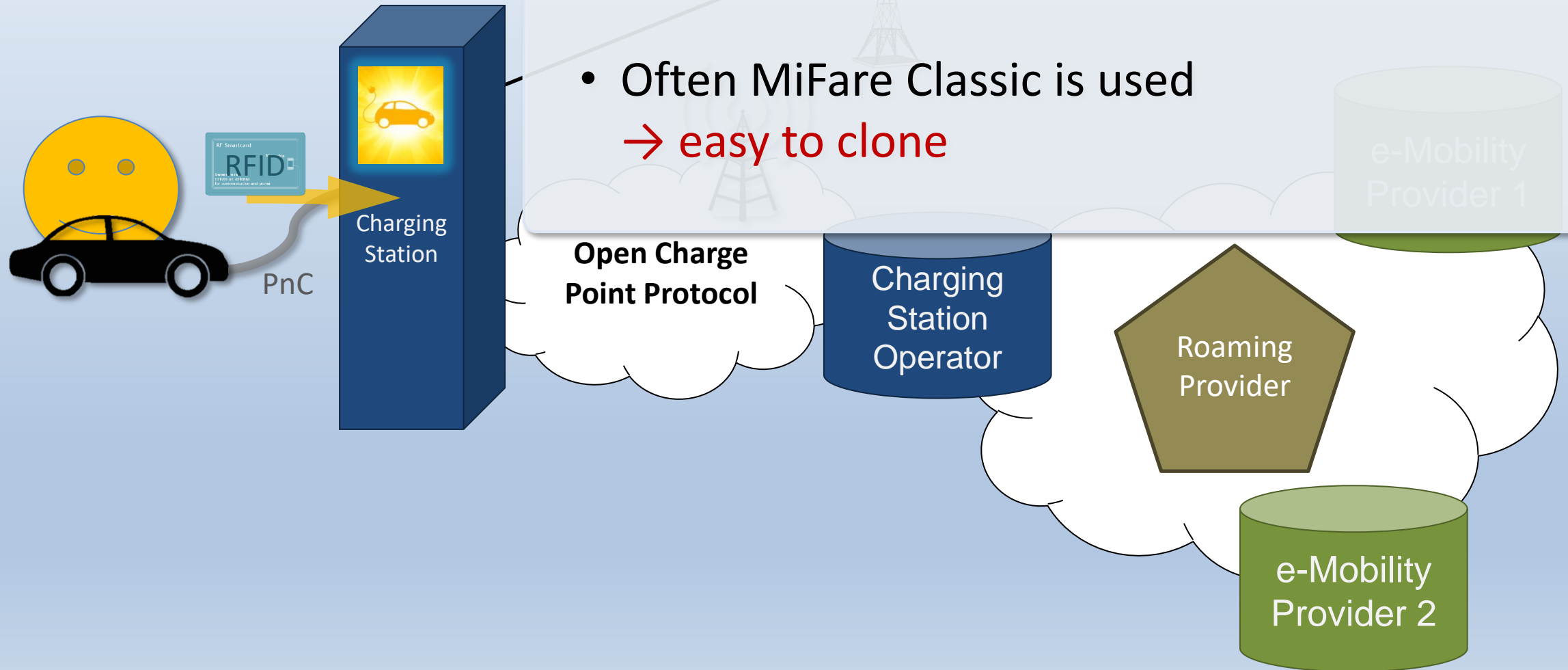
Local Authentication via PnC or RFID



- ISO/IEC 15118 Plug-and-Charge Authentication is based on e-Mobility Account/Contract Identification (eMAId / EVCOID) (online authentication)...
...and/or certificates installed in the e-vehicles (offline authentication, both have privacy issues)
- Very complex standard, from physical up to the data layer... thus not widely supported!

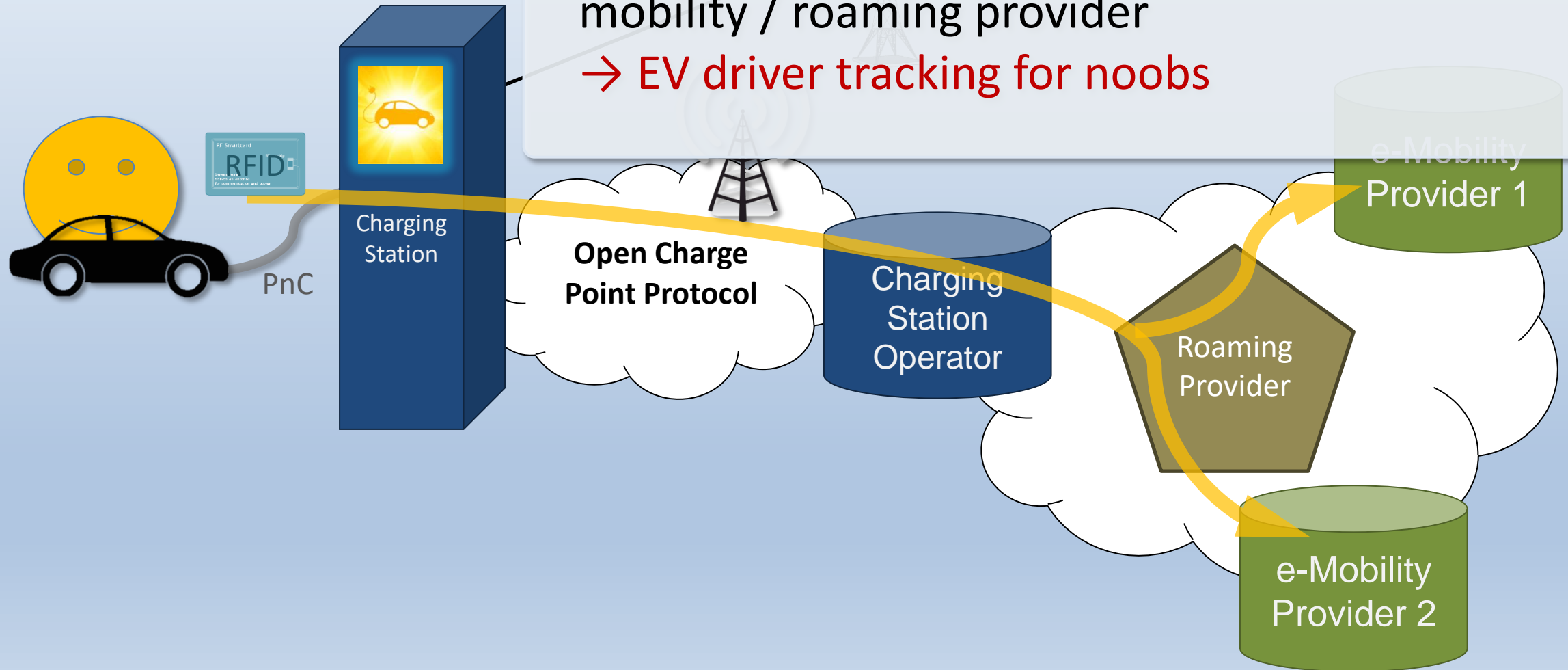


Local Authentication via PnC or RFID

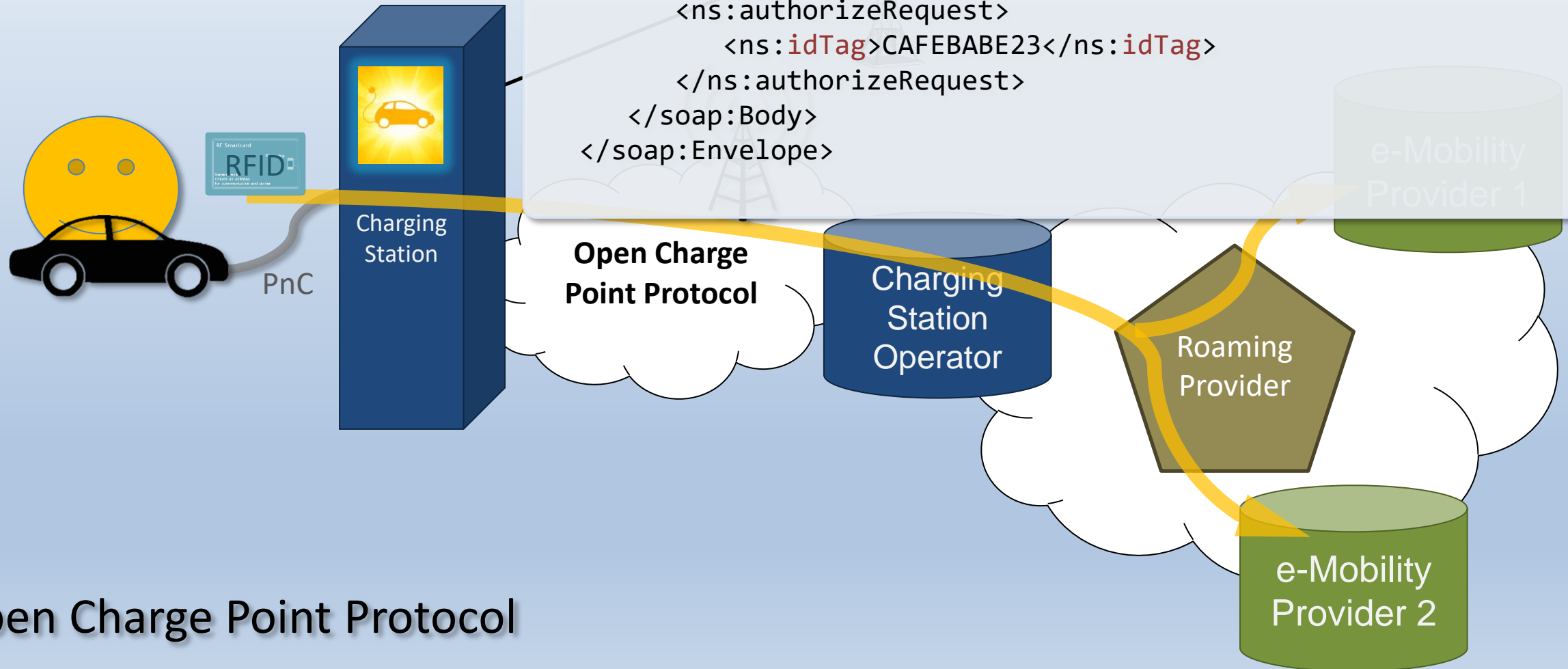


Local Authentication via PnC or RFID

Flat RFID Id schema means the related e-mobility provider is unknown and RFID Id + charging station Id is broadcasted to any e-mobility / roaming provider
→ EV driver tracking for noobs



Local Authentication via PnC or RFID



Open Charge Point Protocol

Local Authentication via PnC or RFID

```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:v2      = "http://www.hubject.com/b2b/services/authorization/v2.0"
  xmlns:v21     = "http://www.hubject.com/b2b/services/commontypes/v2.0">

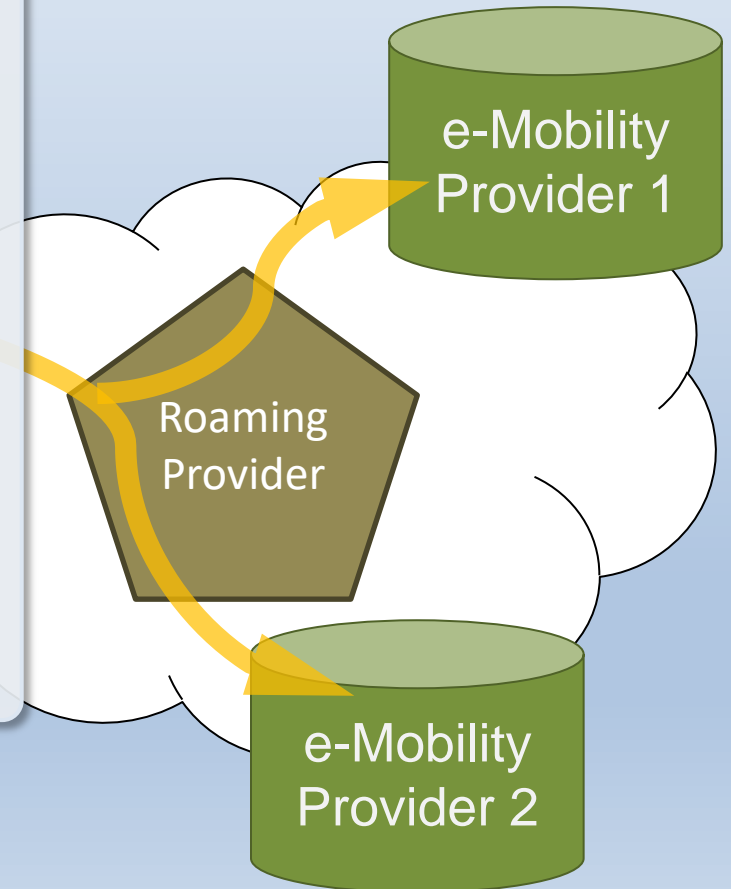
  <soapenv:Header/>
  <soapenv:Body>
    <v2:eRoamingAuthorizeStart>

      <v2:SessionID?></v2:SessionID>      <!--Optional:-->
      <v2:EVSEID>DE*GEF*1234567*1</v2:EVSEID> <!--Optional:-->
      <v2:PartnerProductID>AC1</v2:PartnerProductID> <!--Optional:-->

      <v2:Identification>
        <v21:RFIDmifarefamilyIdentification>
          <v21:UID>CAFEBABE23</v21:UID>
        </v21:RFIDmifarefamilyIdentification>
      </v2:Identification>

    </v2:eRoamingAuthorizeStart>
  </soapenv:Body>
</soapenv:Envelope>
```

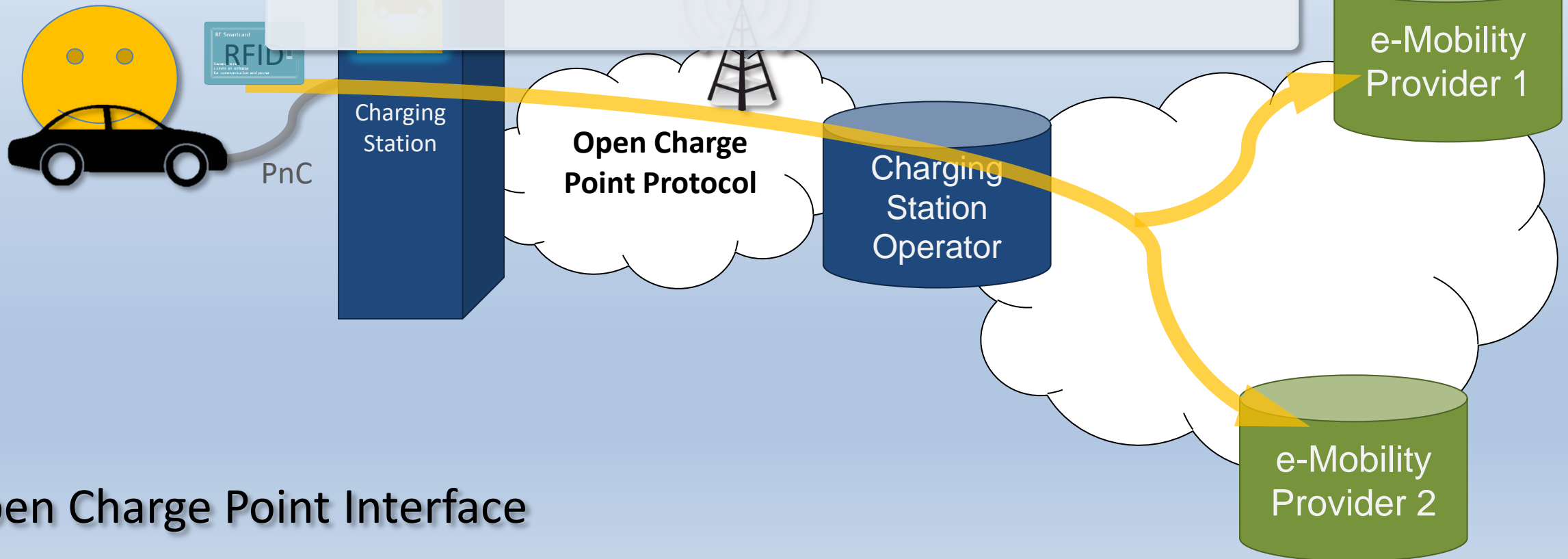
Open InterCharge Protocol



Local Authentication via PnC or RFID

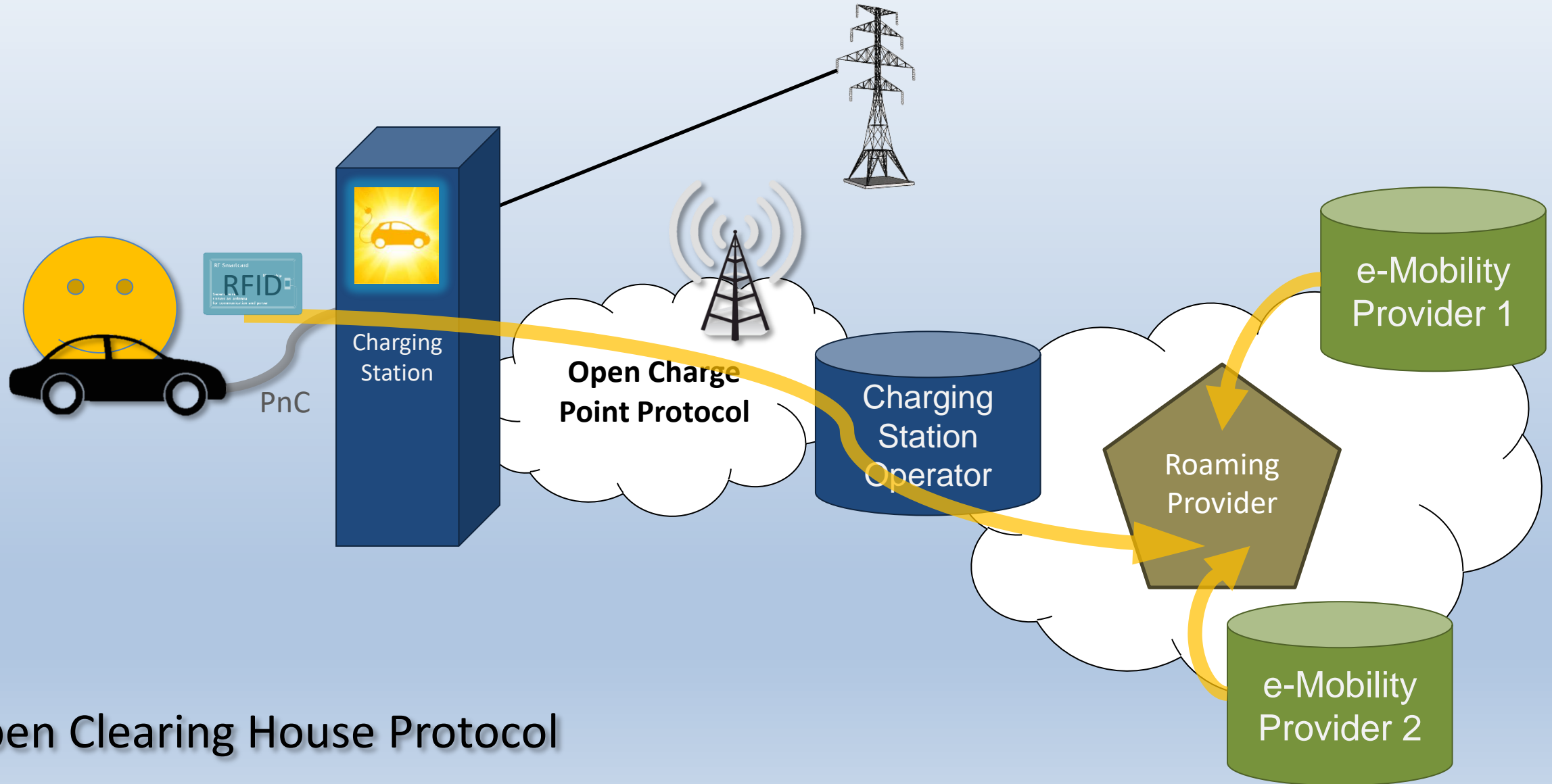
```
POST /ocpi/emsp/2.0/tokens/{token_uid}/authorize
```

```
{  
  "location_id",    ...  
  "evse_uids",     [...]  
  "connector_ids", [...]  
}
```



Open Charge Point Interface

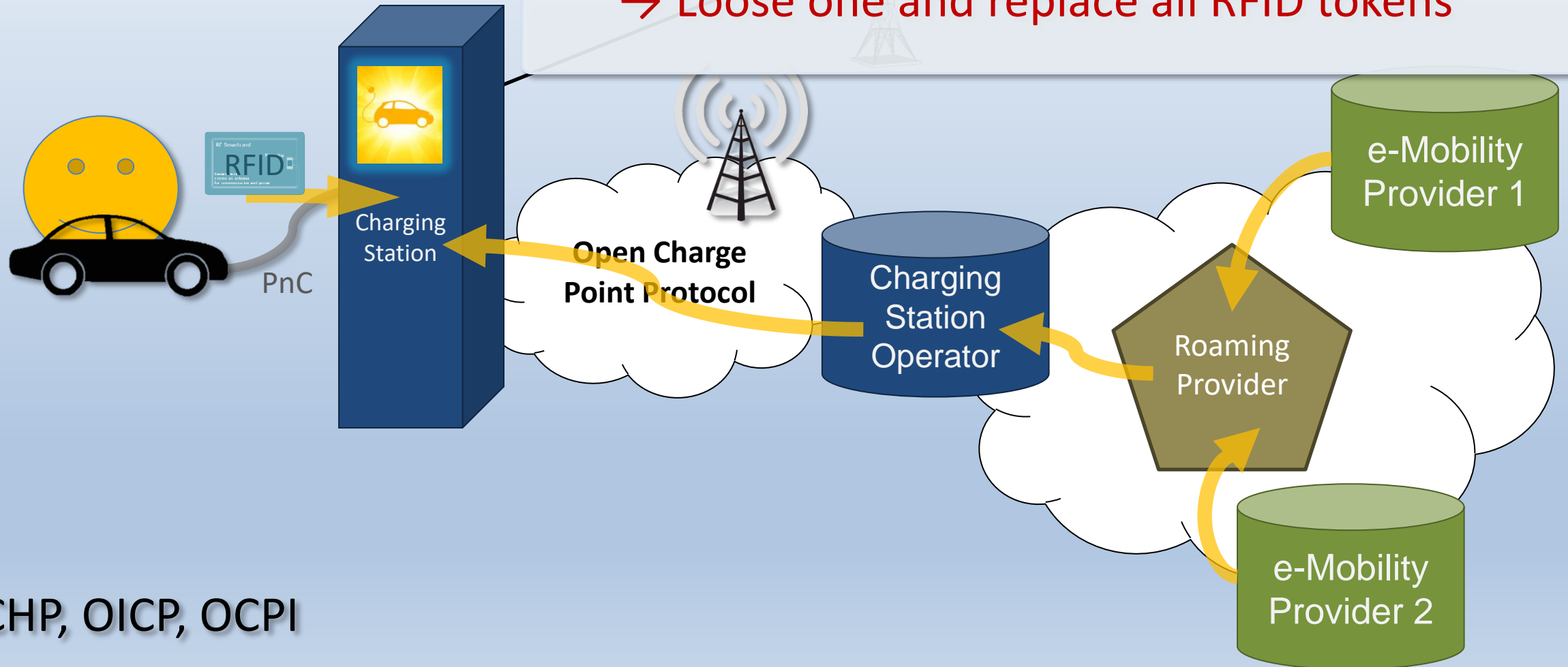
Local Authentication via PnC or RFID



Open Clearing House Protocol

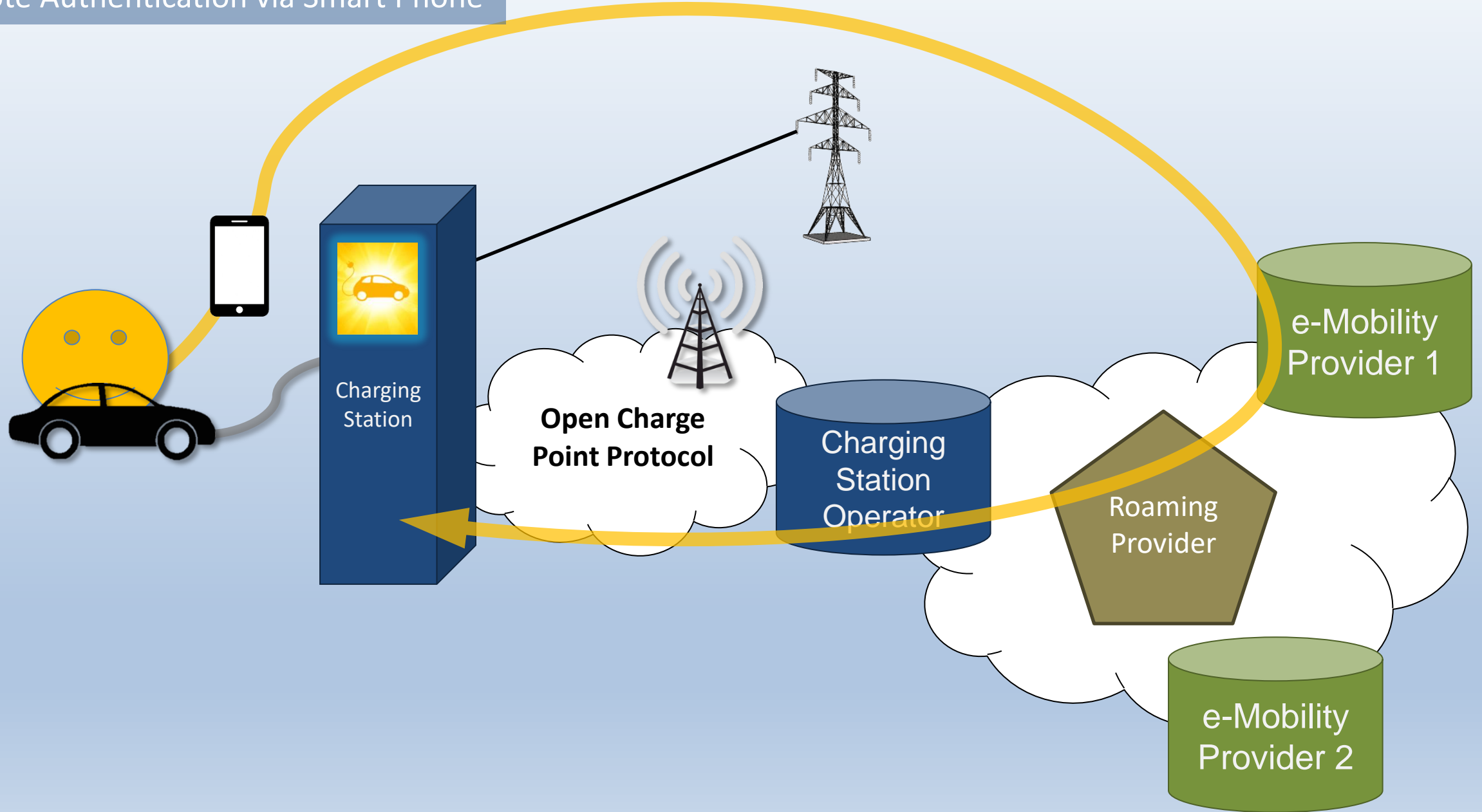
Local Authentication via PnC or RFID

- RFID Id is checked against a local whitelists
 - Ids of 10000s of customers in 10000s of IoT devices in 10000s of streets
 - Loose one and replace all RFID tokens



OCHP, OICP, OCPI

Remote Authentication via Smart Phone



Remote Authentication via Smart Phone

```
<soapenv:Envelope xmlns:soapenv      ="http://schemas.xmlsoap.org/soap/envelope/"
                    xmlns:Authorization="http://www.hubject.com/b2b/services/authorization/v2.0"
                    xmlns:CommonTypes  ="http://www.hubject.com/b2b/services/commontypes/v2.0">

  <soapenv:Body>
    <Authorization:eRoamingAuthorizeRemoteStart>

      <Authorization:SessionID?></Authorization:SessionID>           <!--Optional:-->
      <Authorization:PartnerProductID?></Authorization:PartnerProductID> <!--Optional:-->
      <Authorization:EVSEID>DE*GEF*123456789*1</Authorization:EVSEID>

      <Authorization:Identification>
        <CommonTypes:RemoteIdentification>
          <CommonTypes:EVCOID>DE-GDF-123456789-X</CommonTypes:EVCOID>
        </CommonTypes:RemoteIdentification>
      </Authorization:Identification>

    </Authorization:eRoamingAuthorizeRemoteStart>

  </soapenv:Body>
</soapenv:Envelope>
```

Open InterCharge Protocol

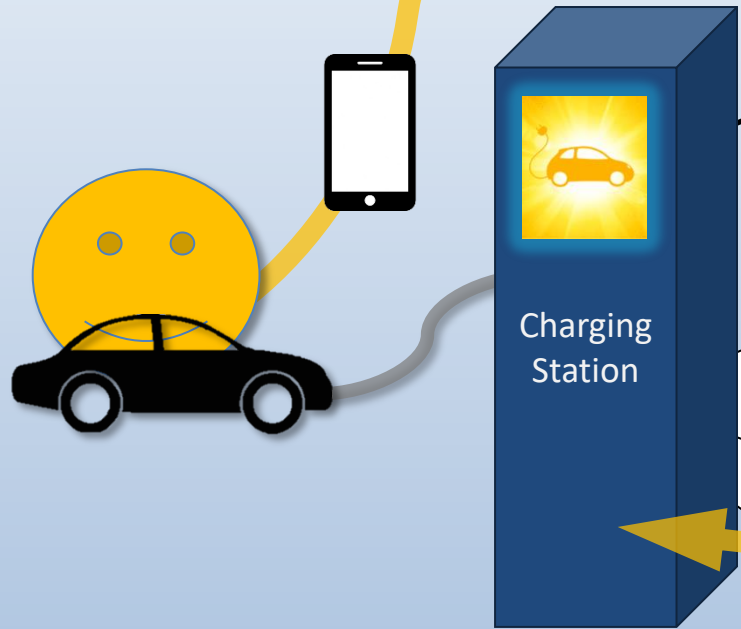


The diagram illustrates the Open InterCharge Protocol architecture. It features a central 'Station Operator' represented by a blue cylinder. To its right is a 'Roaming Provider' represented by a grey pentagon. On the far right, there are two 'e-Mobility Provider' entities, labeled 'e-Mobility Provider 1' (top) and 'e-Mobility Provider 2' (bottom), both represented by green cylinders. A yellow curved arrow originates from the 'Station Operator' and points towards the 'e-Mobility Provider 1' and 'e-Mobility Provider 2'. The background includes faint icons of a car, a mobile phone, and a cell tower.

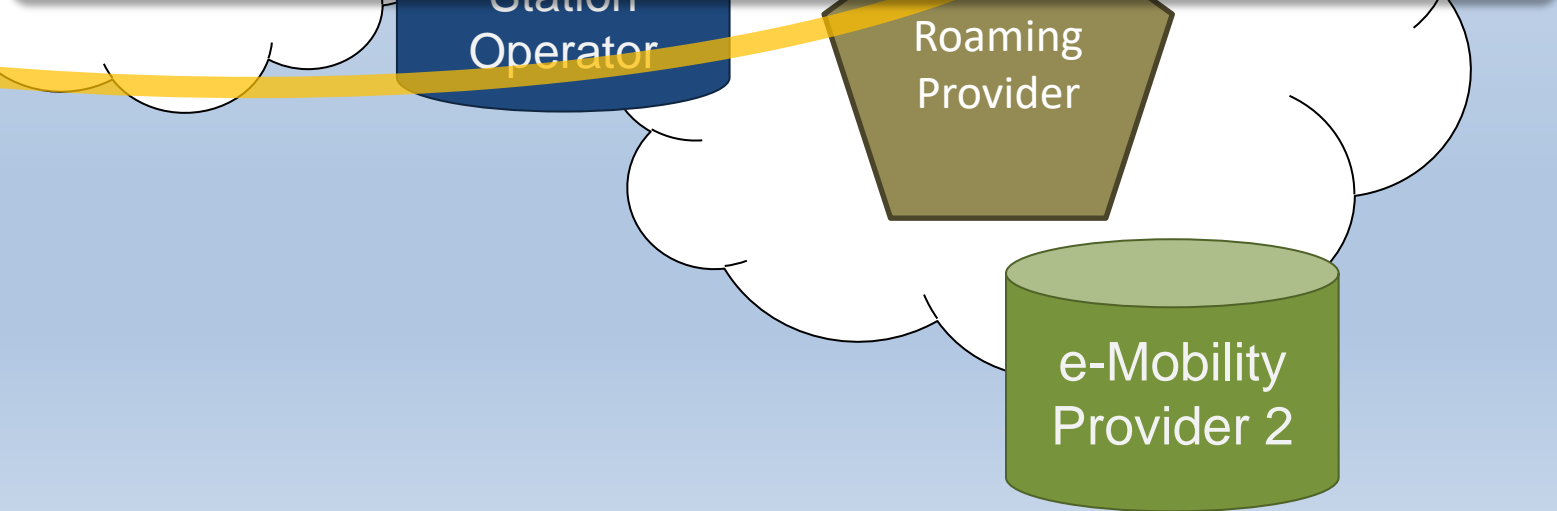
e-Mobility Provider 1

e-Mobility Provider 2

Remote Authentication via Smart Phone

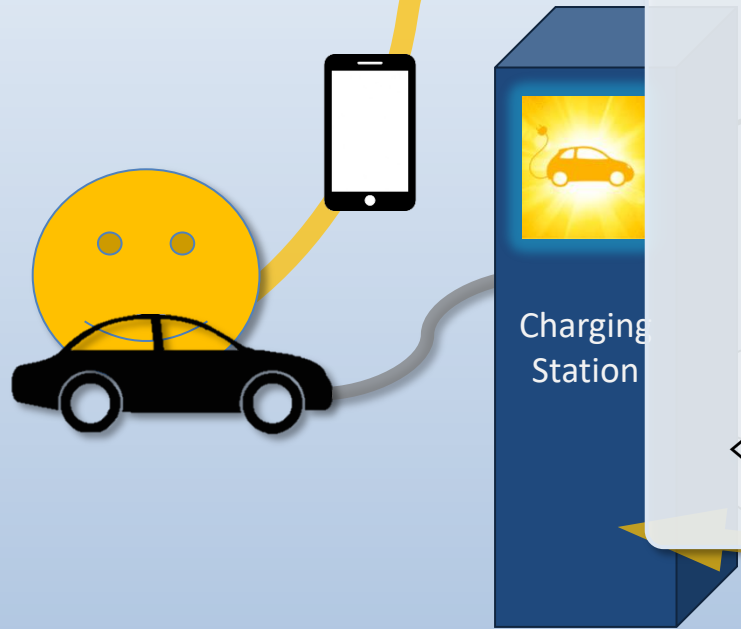


```
<soap:Envelope xmlns:soap="http://www.w3.org/2003/05/soap-envelope"
  xmlns:wsa = "http://www.w3.org/2005/08/addressing"
  xmlns:ns  = "urn://Ocpp/Cp/2015/10/">
  <soap:Body>
    <ns:remoteStartTransactionRequest>
      <ns:connectorId>1</ns:connectorId>
      <ns:idTag>DE-GDF-123456789-X</ns:idTag>
      <ns:chargingProfile />
    </ns:remoteStartTransactionRequest>
  </soap:Body>
</soap:Envelope>
```

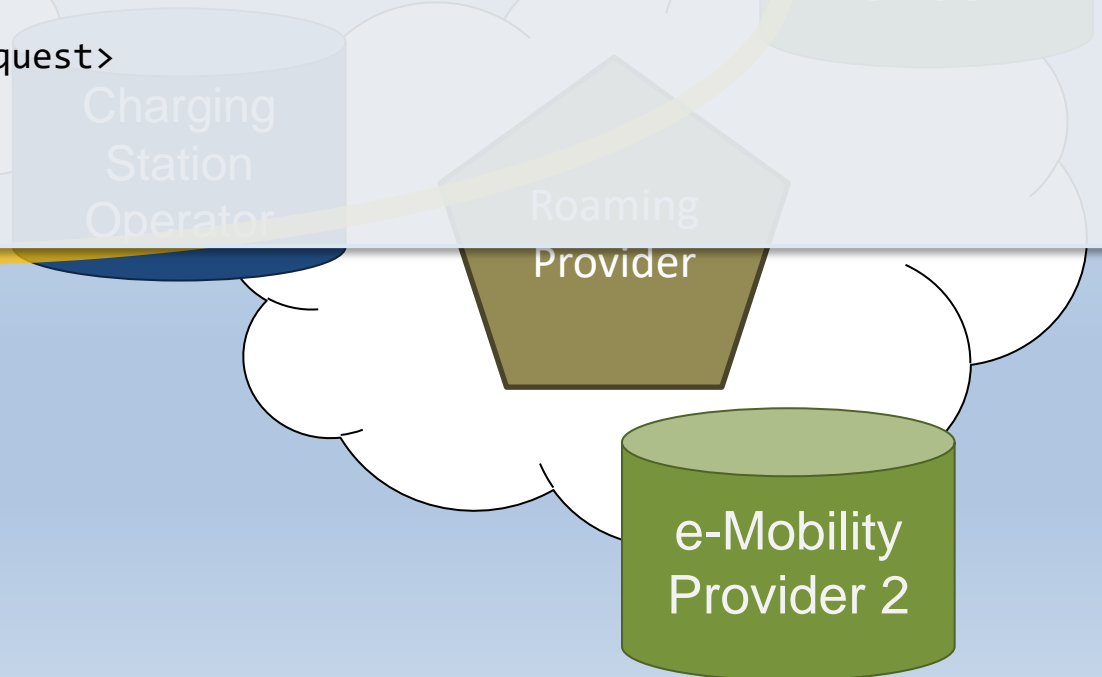


Open Charge Point Protocol

Remote Authentication via Smart Phone

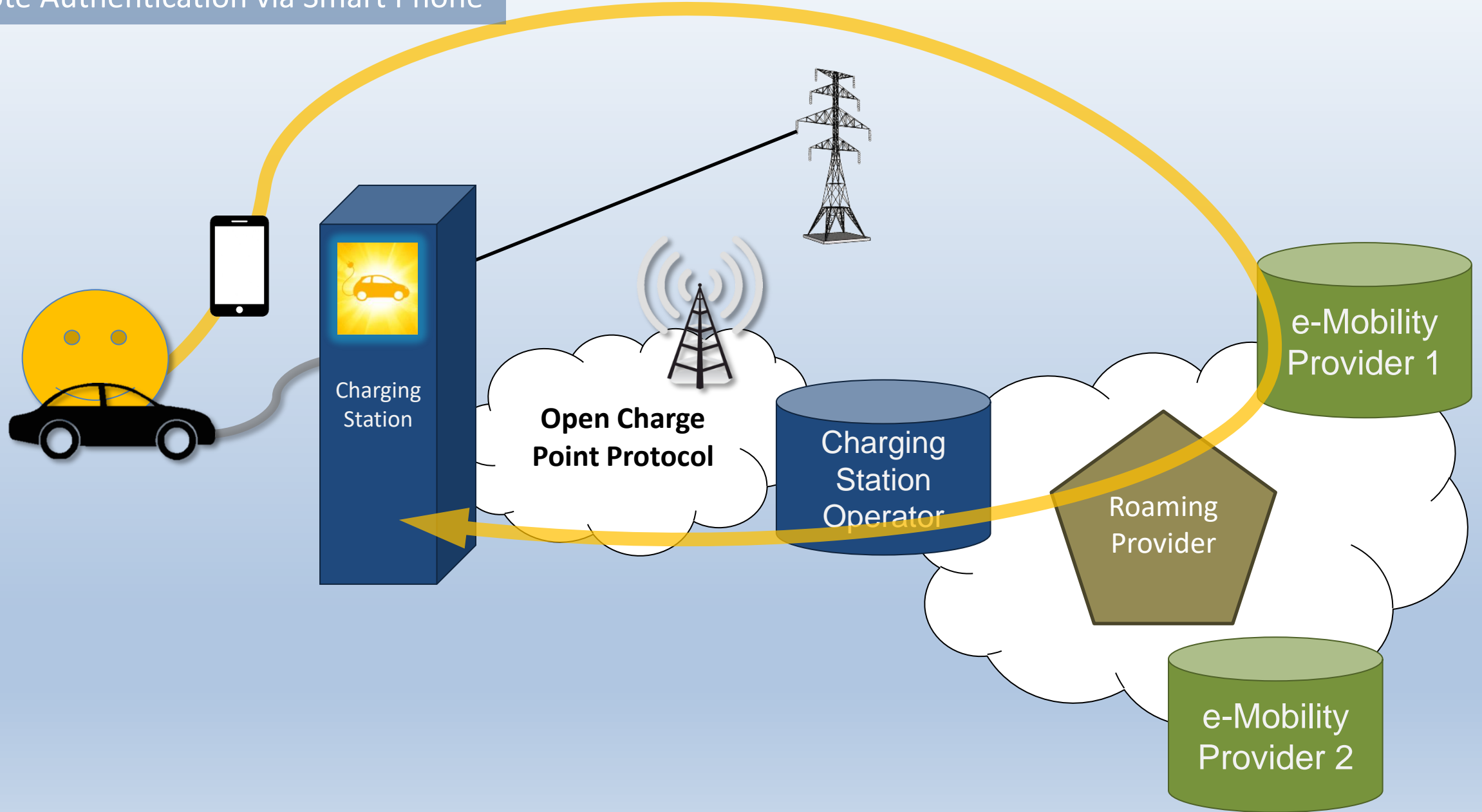


```
<soapenv:Envelope xmlns:soapenv="http://schemas.xmlsoap.org/soap/envelope/"
  xmlns:ns="http://ochp.eu/1.4">
  <soapenv:Body>
    <ns:SelectEvseRequest>
      <ns:evseId>DE*GEF*123456789*1</ns:evseId>
      <ns:contractId>DE-GDF-123456789-X</ns:contractId>
      <!--Optional:-->
      <ns:reserveUntil>
        <ns:DateTime>?</ns:DateTime>
      </ns:reserveUntil>
    </ns:SelectEvseRequest>
  </soapenv:Body>
</soapenv:Envelope>
```



Open Clearing House Protocol

Remote Authentication via Smart Phone





Little sisters are watching!

They are willing to change...

The image shows a banner for the website of Stiftung Datenschutz. The background is a dark blue gradient with a pattern of binary code (0s and 1s) and a white silhouette of a human head profile on the left side. Inside the head silhouette, there are several interlocking gears of various sizes. In the top left corner, there is a white circular logo with the text "STIFTUNG DATENSCHUTZ" and four colored dots (black, grey, red, yellow). A white rectangular box on the right side of the banner contains the title "Mehr Privatsphäre" and a paragraph of text. At the bottom of the banner, there is a white navigation bar with a home icon, the text "Über uns", "Aufgaben", "Themen", "Veranstaltungen", "Termine", "Presse/Media", a search icon, and a Twitter icon.

STIFTUNG
DATENSCHUTZ

Mehr Privatsphäre

Nur wer die Möglichkeiten zum Schutz seiner Privatsphäre kennt, kann sie auch nutzen. Die Stiftung Datenschutz klärt auf, wie man sicher mit seinen Daten umgeht.

Über uns Aufgaben Themen Veranstaltungen Termine Presse/Media

Stiftung Datenschutz agrees that it seems very likely, that the current e-mobility charging infrastructure violates privacy laws.

Maybe a better future...

[Kontakt](#) [Impressum](#) [Datenschutz](#)



[Projekt](#) [News](#) [Konsortium](#)

Selbstdatenschutz im vernetzten Fahrzeug



Sadly, in the past it did not work out very well...

IT-Sicherheit meets Elektromobilität



Mit dem Projekt SecMobil zum weltweiten Vorreiter in dem Bereich IT-Sicherheit für Elektromobilität

Elektromobilität ist in aller Munde und viele Politiker bekennen Farbe zu der neuen Art der Fortbewegung. Technische Entwicklungen zur Elektromobilität werden in vielen deutschen Unternehmen mit Hochdruck vorangetrieben.

Das „Secure eMobility“-Konsortium bestehend aus Automobilhersteller, Zulieferer und Forschungseinrichtungen hat erkannt, dass bei den heutigen Entwicklungen und Feldversuchen im Bereich der Elektromobilität der Aspekt der IT-Sicherheit nicht ausreichend behandelt wird.

Im Rahmen der Ausschreibung „IKT für Elektromobilität II – Smart Car – Smart Grid – Smart Traffic“ des Bundesministeriums für Wirtschaft und Technologie (BMWi) wird das „Secure eMobility“-Konsortium IT-Sicherheitstechnologien für die Elektromobilität entwickeln und die deutsche Vorreiterrolle sichern.



Projektziele:

Sicheres eMetering

- ▶ Manipulationssicheres Messen von Strom
- ▶ eMetering-Funktionalität
- ▶ Sichere Kommunikation

Sichere Infrastruktur

- ▶ Security-Basistechnologien für Ladesäule und Fahrzeuge
- ▶ Security-Basistechnologien für die Infrastruktur

Sichere Dienste und Security-Basistechnologien

- ▶ Auto-Applikationen
- ▶ Abrechnungssysteme
- ▶ Software-Aktualisierung
- ▶ Funktionsfreischaltung
- ▶ Identitätsmanagement mit dem neuen Personalausweis

Breitenwirkung

- ▶ Technologietransfer
- ▶ KnowHow Transfer

Projektlaufzeit:

1.1.2012 – 31.08.2014



Konsortium:

DAIMLER

ELMOS

escrypt
Embedded Security

Getragen durch:
Bundesministerium für Wirtschaft und Technologie

Kontakt:

Konsortialführer ESCRYPT GmbH – Embedded Security
info@secmobil.com, +49 234 43870219

if(is)
Informationsicherheit

RUHR
UNIVERSITÄT
BOCHUM

RUB

smartlab

gefördert durch:
Konsortium der Partner

secmobil



Open Charging Cloud

GraphDefined GmbH

mail@open.charging.cloud

PGP/GPG 065B 20E3 1FDC C624 C438 907D D977 5D7B 13F6 7088

<https://open.charging.cloud>

Twitter: @OCCloud

GitHub: OpenChargingCloud