Open Charing Cloud

February 2024

FOSDEM'24

Enhancing OCPP with E2E-Security and Binary Data Streams

…for a more secure energy ecosystem

#SecurityByDesign

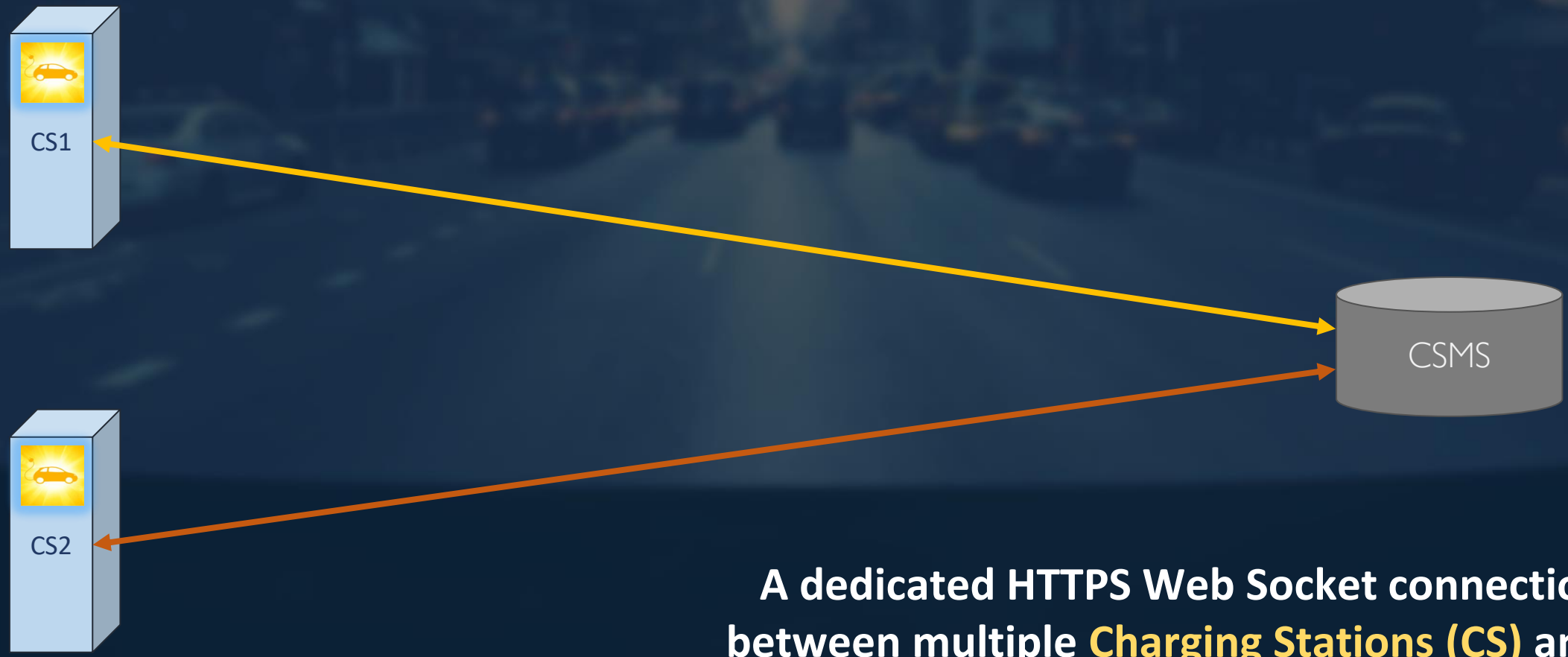
#SichererAlsDasBSIErlaubt

achim.friedland@graphdefined.com

/me

- Studied Computer Science (medical CS, network security) at TU Ilmenau, Germany
- Developing the student campus network, e.g. WLAN Point-to-Point links
- Worked for multiple startups
  (GraphDBs, Renewables, e-Health, PV, EV, …)
- Started my own Open Source & Open Data company in 2014

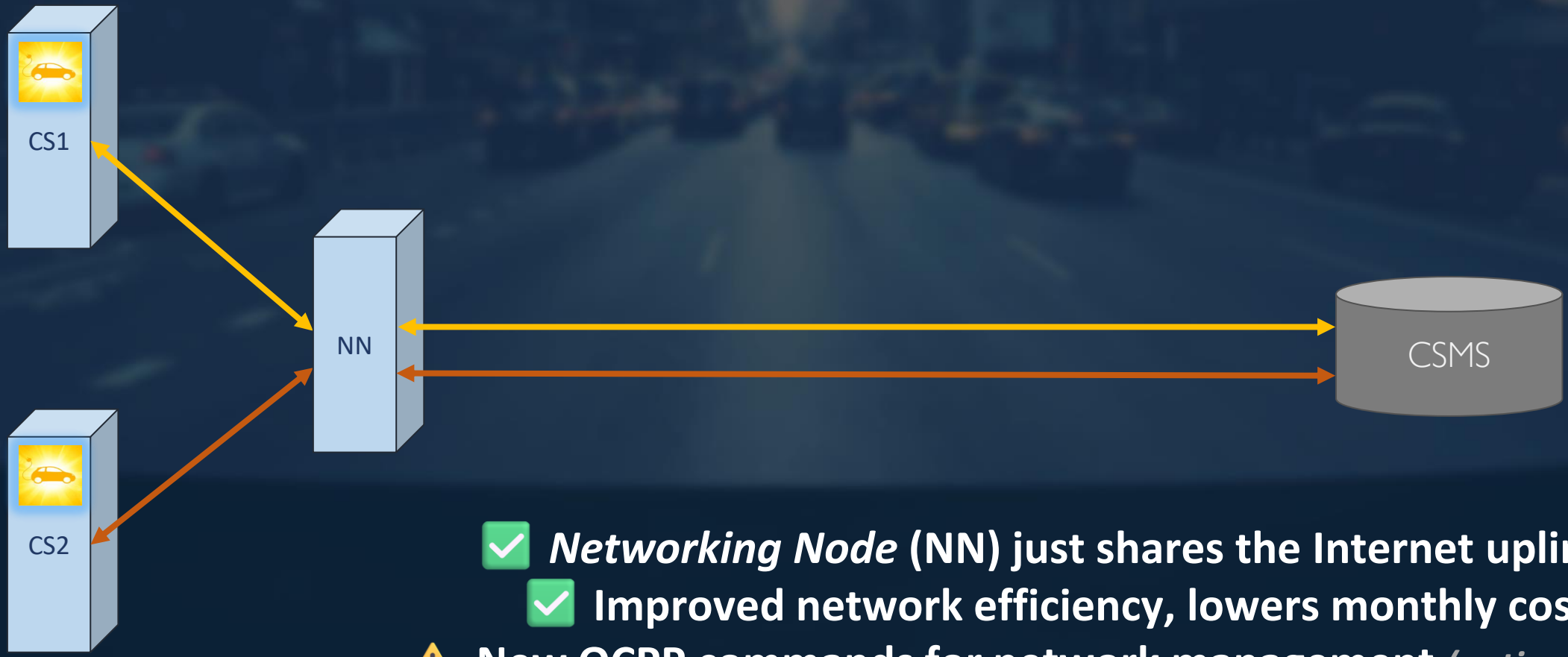
Historical background



A dedicated HTTPS Web Socket connection between multiple Charging Stations (CS) and a single Charging Station Management System (CSMS)

Local Networking

(Local Proxy in OCPP v2.0.1)



✅ *Networking Node* (NN) just shares the Internet uplink

✅ Improved network efficiency, lowers monthly costs

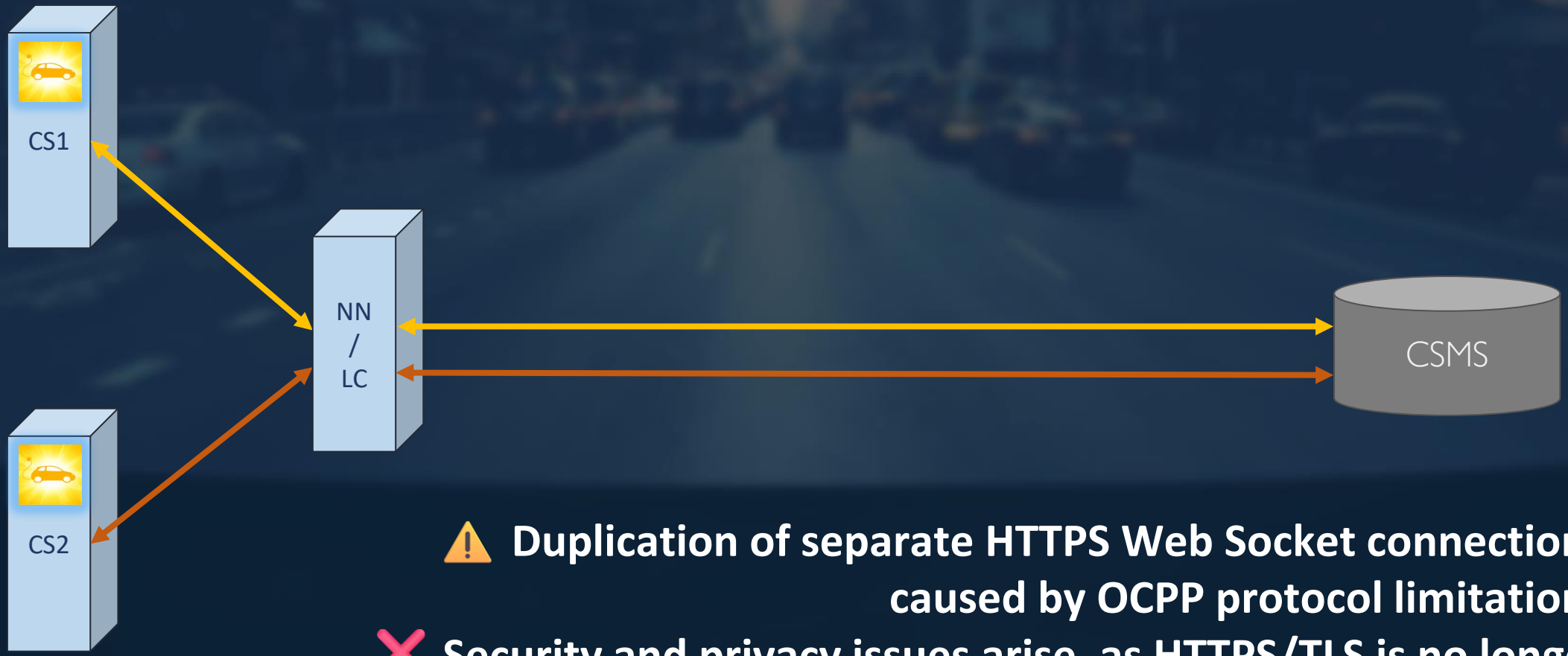
⚠️ New OCPP commands for network management *(optional)*

⚠️ Charging Stations also offer HTTP Web Socket Access *(optional)*

Local Controller

- ***Local Controller*** **(LC) might have own energy meter(s) for monitoring the *Grid Connection Point (GCP)***
- **LC in charge of the Dynamic Load Management (DLM)**
- ***LC* connected to a *Smart Meter Gateway* (SMGW, Germany)**

Local Networking/Controllers



⚠️ **Duplication of separate HTTPS Web Socket connections caused by OCPP protocol limitations**

❌ **Security and privacy issues arise, as HTTPS/TLS is no longer sufficient for end-to-end security!**

Marketing-in-the-Middle

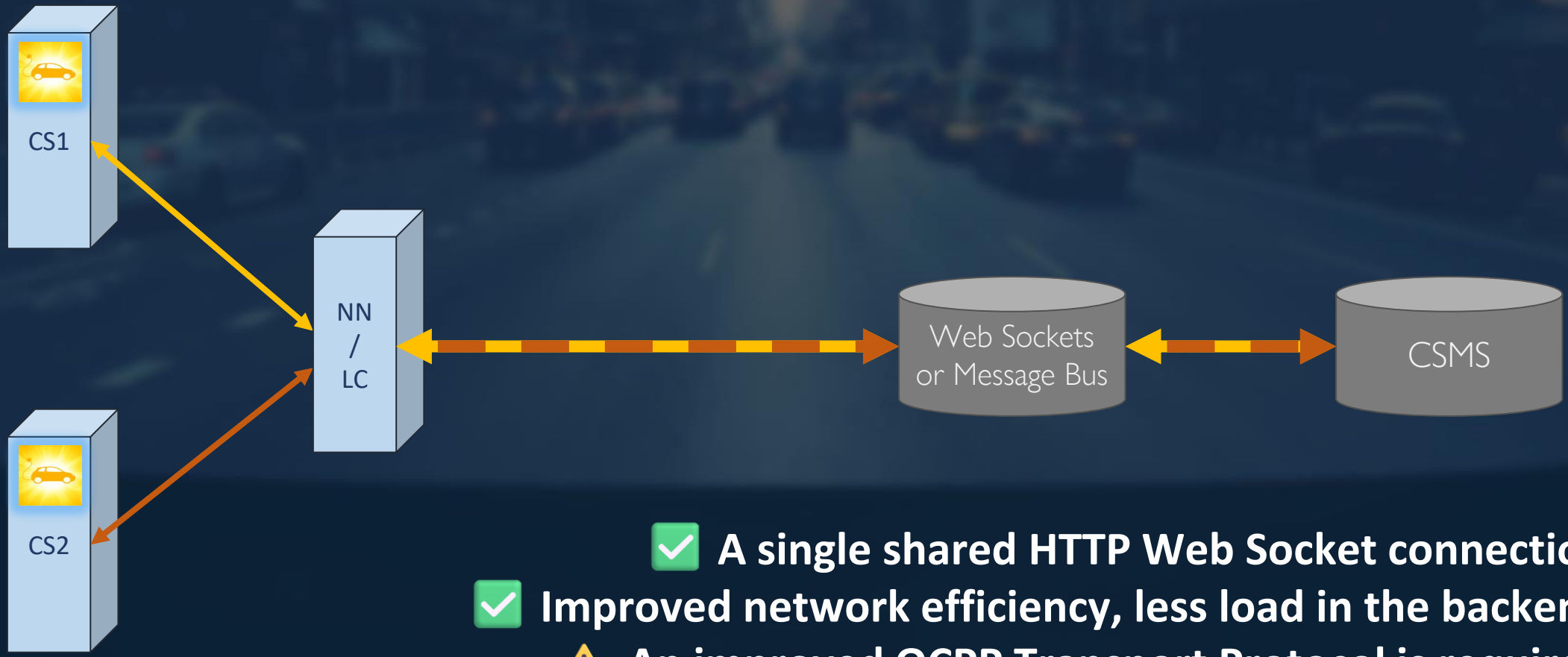
✅ Web Socket is one (Micro) Service, CSMS is another

✅ Might even be operated by <u>different companies</u>

✅ Spying for analytics while connecting to 1…n “black box” CSMSs

❌ More duplications, more security, privacy & H/A issues

Shared Web Socket Connections



✅ A single shared HTTP Web Socket connection

✅ Improved network efficiency, less load in the backend

⚠️ An improved OCPP Transport Protocol is required

⚠️ Other protocols like MQTT or kafka are possible

Improved OCPP Transport Protocol

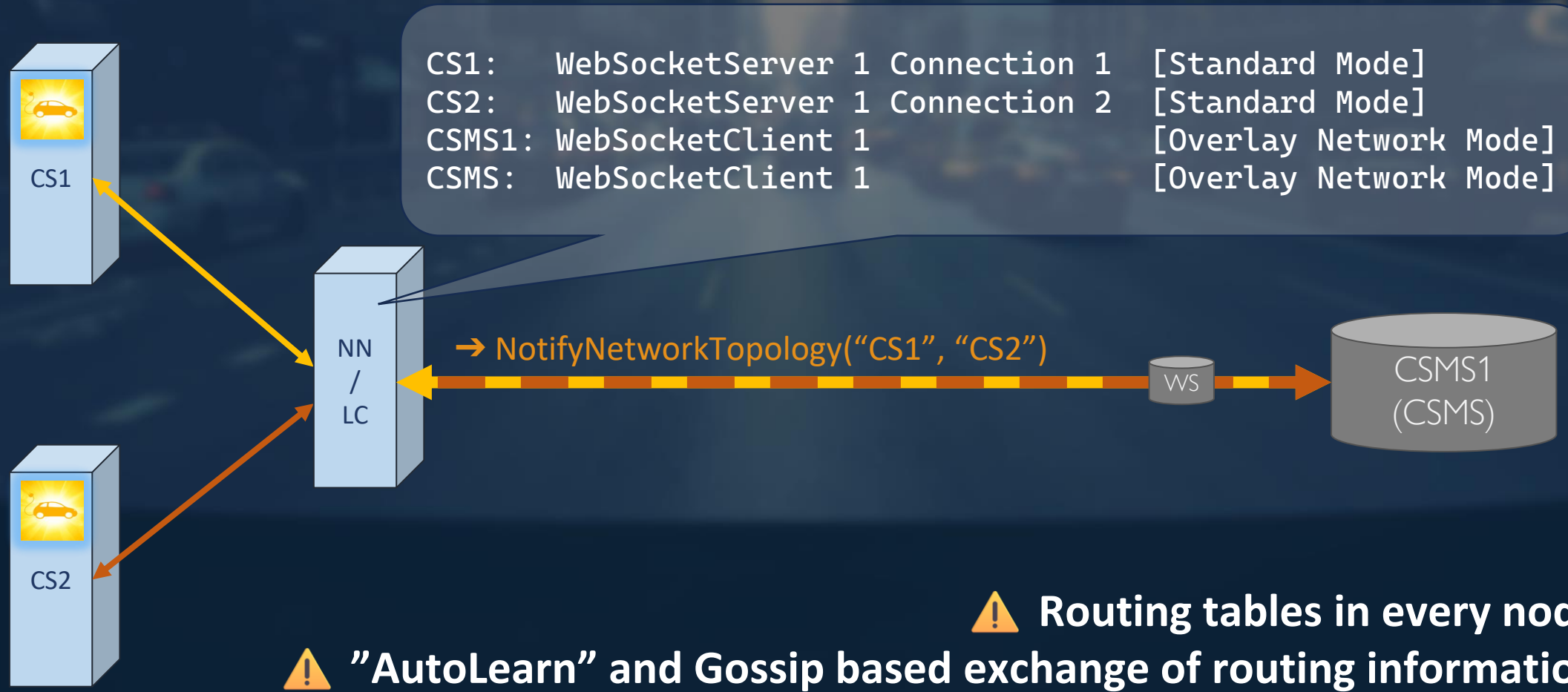
```
[
    2,                  // MessageType: CALL (Client-to-Server)
   "19223201",          // RequestId
   "BootNotification",  // Action
   {
       "chargingStation":  { ... },
       "reason":           "FirmwareUpdate"
   }
]
```

⚠️ **Additional routing information within the JSON transport array**

✅ **Network Source Path**
- **Record of the Route taken**
- **Implicit Hop Count**
- **Implicit Loop Detection**

```
[
    2,                  // MessageType: CALL (Client-to-Server)
   "CSMS",              // Destination Node Id or
                        //    Any-/Multicast Address
   [ "CS01", "NN01" ],  // Network Source Path
   "19223201",          // RequestId
   "BootNotification",  // Action
   {
       "chargingStation":  { ... },
       "reason":           "FirmwareUpdate"
   }
]
```

New OCPP Overlay Networking

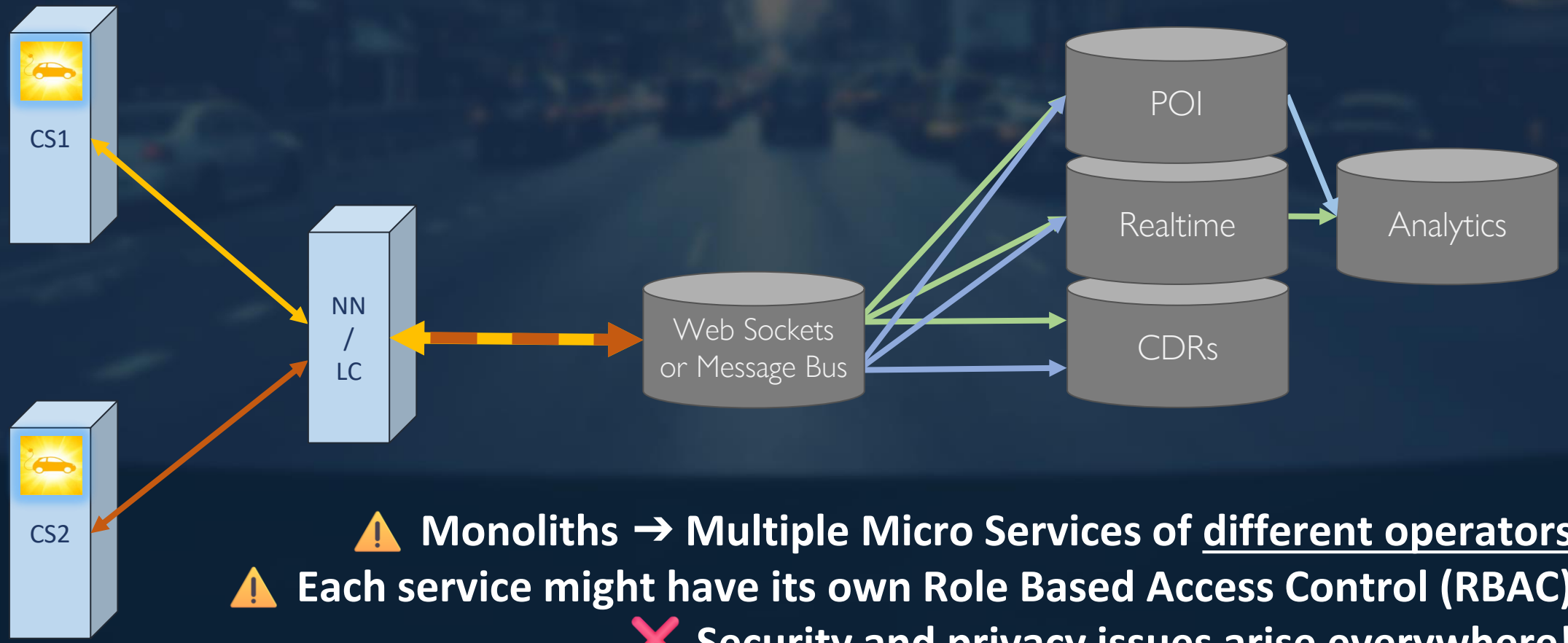


⚠️ Routing tables in every node

⚠️ "AutoLearn" and Gossip based exchange of routing information

✅ Any-/Multicast: Instead of sending data to boxes, we address services

The new CSMS Micro Service Reality



⚠️ Monoliths → Multiple Micro Services of <u>different operators</u>

⚠️ Each service might have its own Role Based Access Control (RBAC)

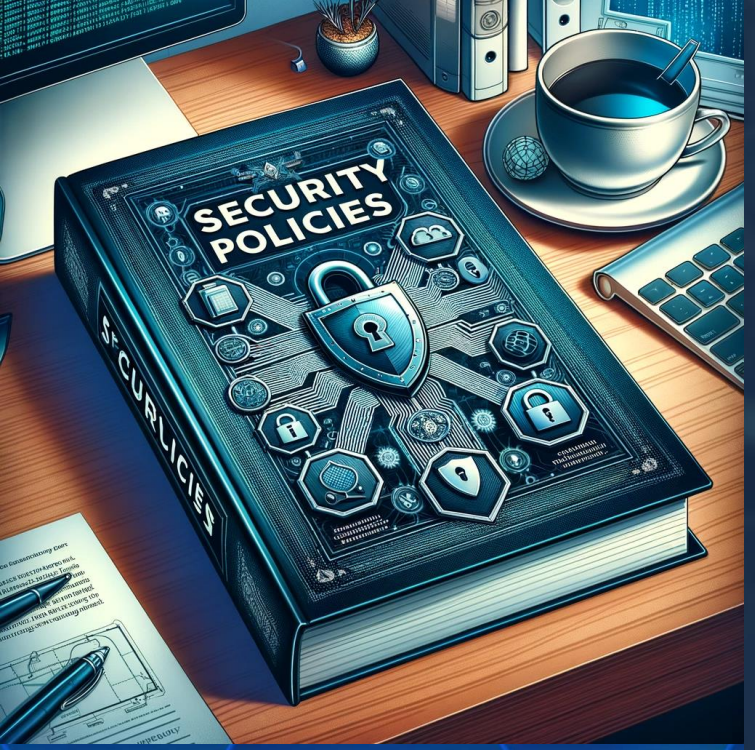
❌ Security and privacy issues arise everywhere!

❌ Traditional OCPP security model is no longer sufficient!

Signed Messages and Data

```
{

   // BootNotificationRequest

   [ ... ]

   "signatures“: [
     {
       "keyId":            " ... ",
       "value":            " ... ",
       “algorithm":        "secp521r1"| ... ,
       "signingMethod":    "json"|"binary"| ... ,
       "encoding":         "base64"|"hex"| ... ,
       "name":             " ... ",
       "description":      " ... ",
       “timestamp":        “[ISO8601]",
     }
   ]

}
```

- ✅ **Signatures are part of the OCPP requests, responses or data structures**
  (In contrast to OCPP v2.0.1 transport layer signatures)
- ✅ **0…n signatures allowed**
- ✅ **Signatures over different data representations**
- ✅ **Additional meta data within signatures to be more user friendly**



Signature Policies

OUT Which signatures must be generated for which request/response, using which data (representation) and private key?

IN Which request/response is expected to be signed by which public key(s)? Which signatures, public key chains and rules must be verified?

User Roles for OCPP

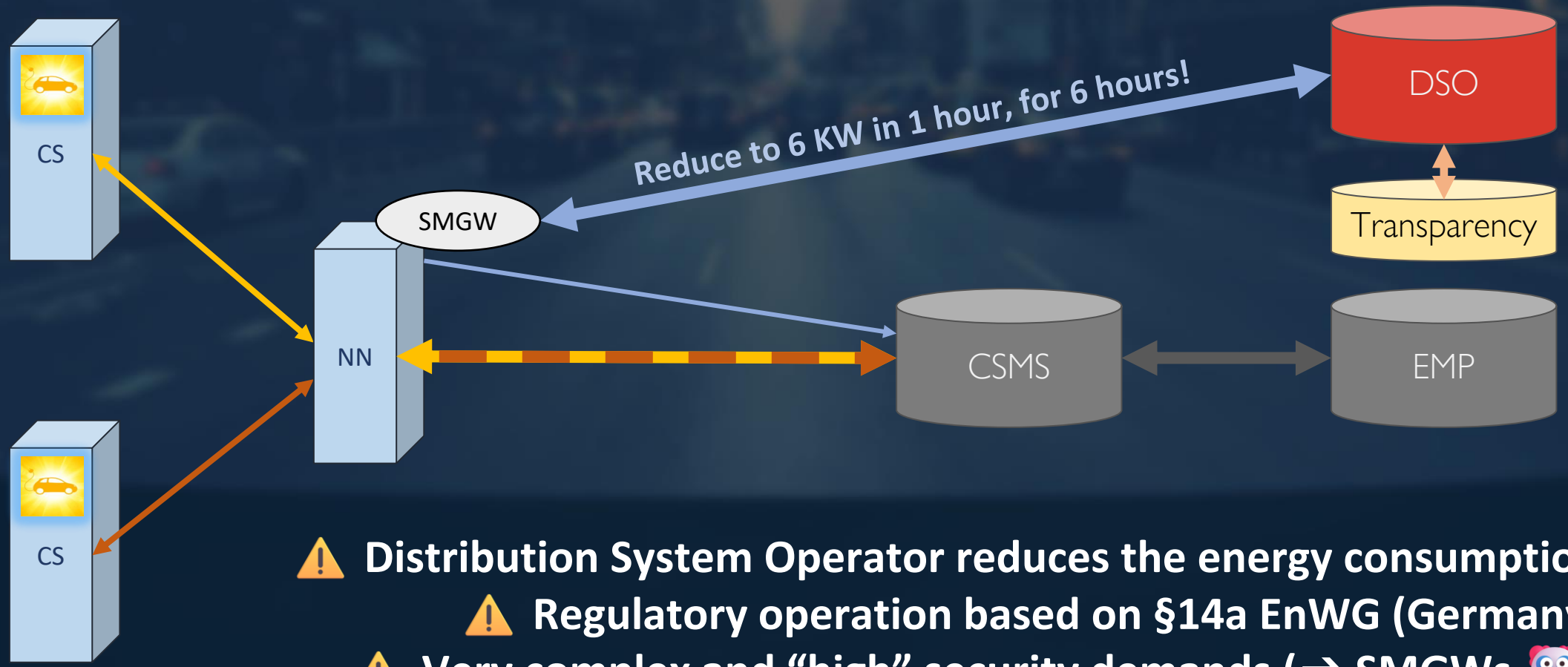
- A user role is a collection of OCPP requests having the same security level
  (admin, tech, operations, …)
- A user role defines a collection of public keys allowed to invoke the specified **OCPP Requests**
  (Later maybe down to the values of request parameters)
- The user role defines which public key can read, write, … variables of the **OCPP Device Model**
  (↔ Siemens proposal)

Binary Data Streams

- ✅ Using HTTPS Web Socket binary frames
- ✅ Generic File Transfer commands: SendFile, GetFile, …
- ✅ Safer Firmware uploads, LogFile downloads, …
  as those use external HTTP(s) requests which expose network security risks
- ✅ Used for encrypted/tunneled OCPP commands
- ⚠️ Large transfers need a proper message priority scheduling!


Nice, but why?
Many new
End-to-End Communication
Use Cases

German §14a Grid Load Management



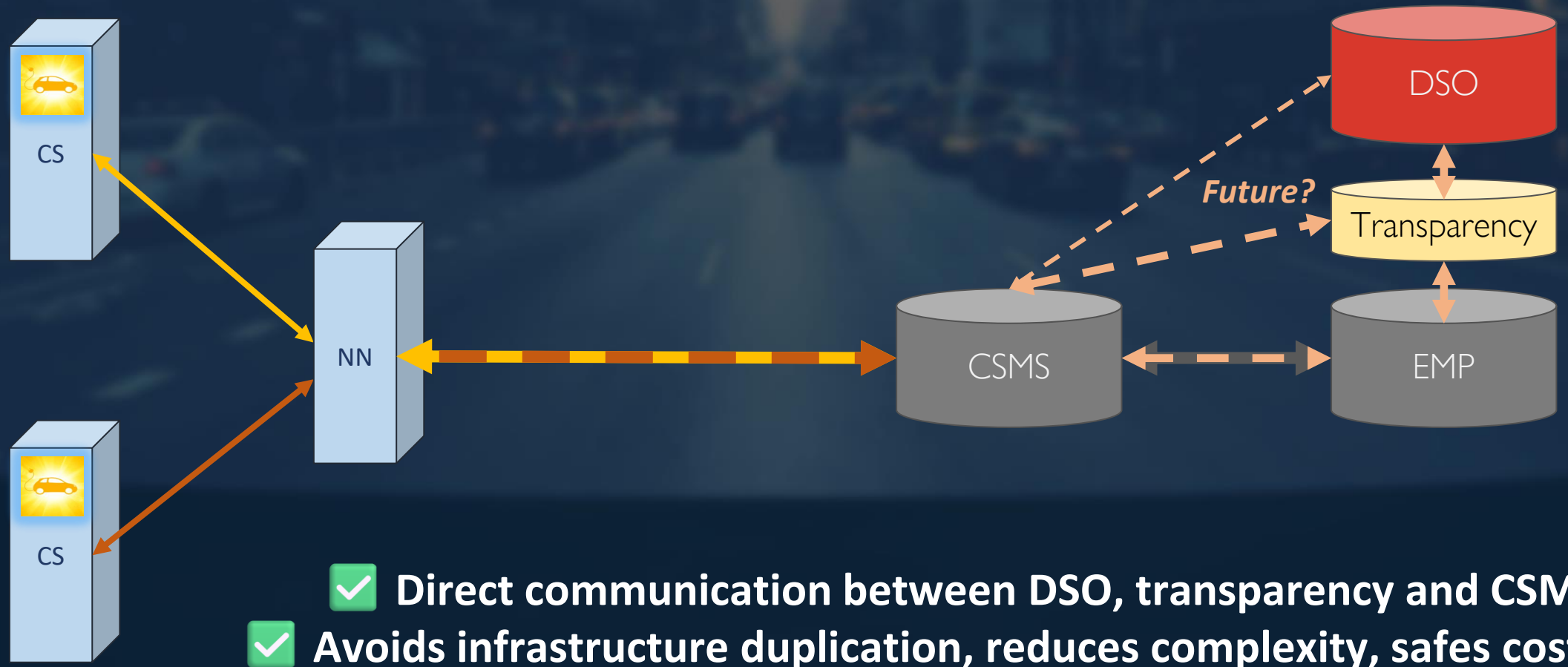
⚠️ Distribution System Operator reduces the energy consumption

⚠️ Regulatory operation based on §14a EnWG (Germany)

⚠️ Very complex and “high” security demands (→ SMGWs 🤡)

⚠️ Mandatory secure & transparent information of the CPO/EV driver

German §14a Grid Load Management (vNEXT)

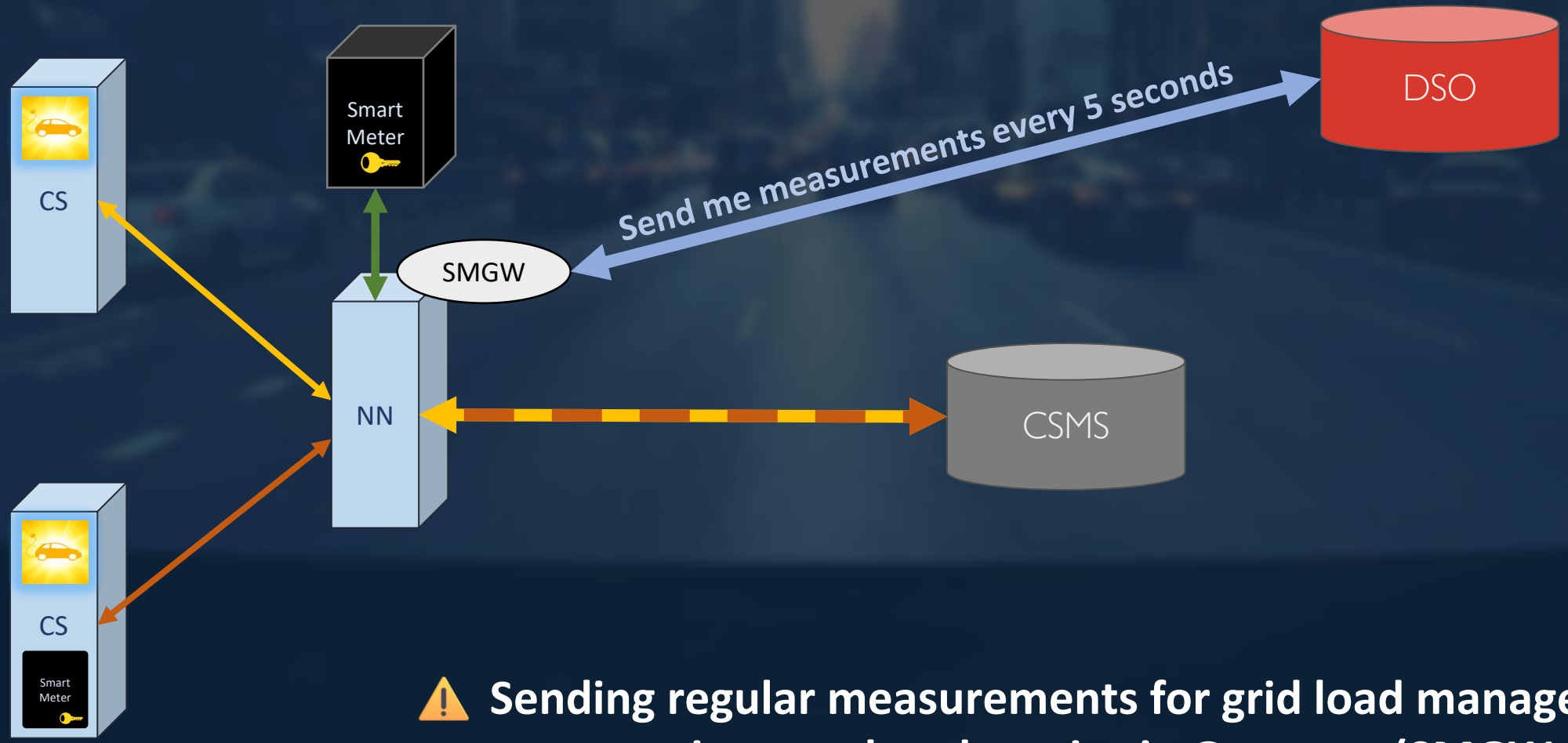


✅ Direct communication between DSO, transparency and CSMS

✅ Avoids infrastructure duplication, reduces complexity, safes costs

⚠️ But for this we need significant security & robustness improvements

Secure & Efficient Sensor Data Streams



⚠ **Sending regular measurements for grid load management is a regulated service in Germany (SMGWs et.al)**

Secure & Efficient Sensor Data Streams

✅ OCPP v2.1 already defines Periodic Event Streams

✅ We extent this to Binary Periodic Event Streams

✅ We also define a generic *"Modbus Transport (Tunnel)"* for secure remote access of e.g. Smart Meters via an OCPP Overlay Network

Charging Tariffs under AFIR

- EV driver must be informed about prices **before**, **during** and **after** a charging session
- Tariffs need to be **digital**, **immutable** and **signed** and available on **transparency platforms**
  (This will solve some major German Eichrecht problems)
- OCPP v2.1 will support OCPI++ tariff data structures, but currently **without end-to-end-semantics**

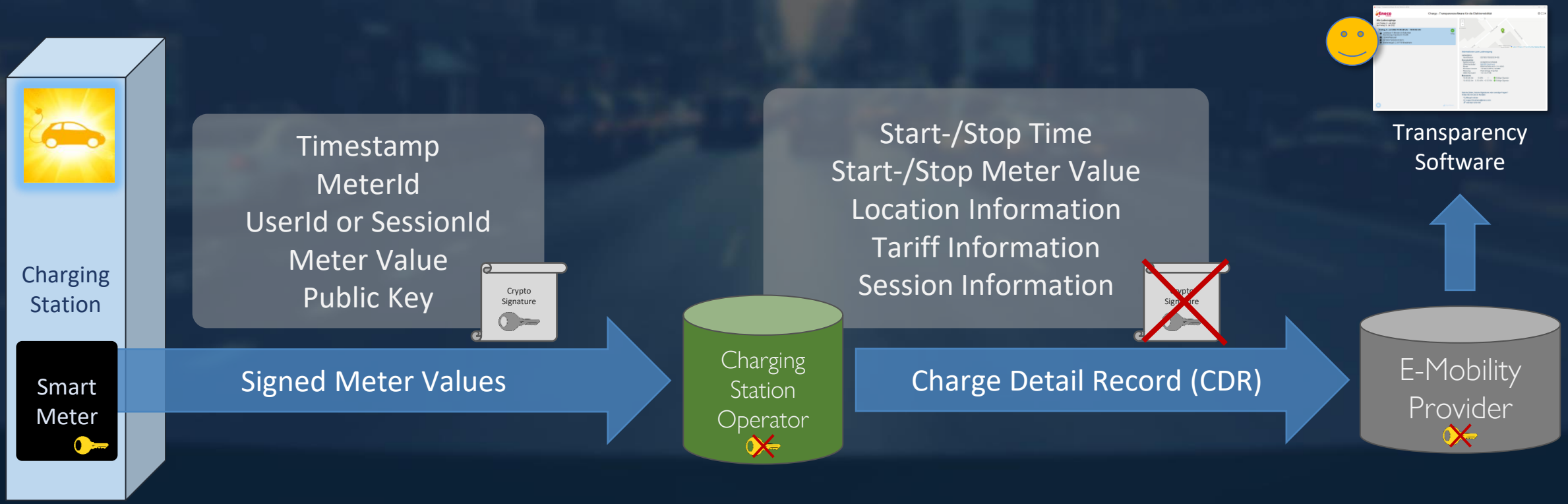
Ad hoc charging under AFIR

- Anonymous EV driver scans a dynamic QR code for payments…
- Why not a signed QR code to access a *remote display* of the charging station? EV drivers want to control their charging sessions via smartphone anyway!
- Some proprietary solutions already exist within the market, but all have regulatory, security and privacy issues!

Digital Charging Station Twins

- The CSMS is no longer the *“single source of truth”*
- CPOs/vendors often do not really know what’s going on and neither AI, nor séances can not solve missing communication and consensus in distributed systems
- As OCPP does not provide a generic way to share all information/state changes in a secure way
  → Often vendor backdoors are used
- Like a *“remote display”* for internals, diagnostics, …

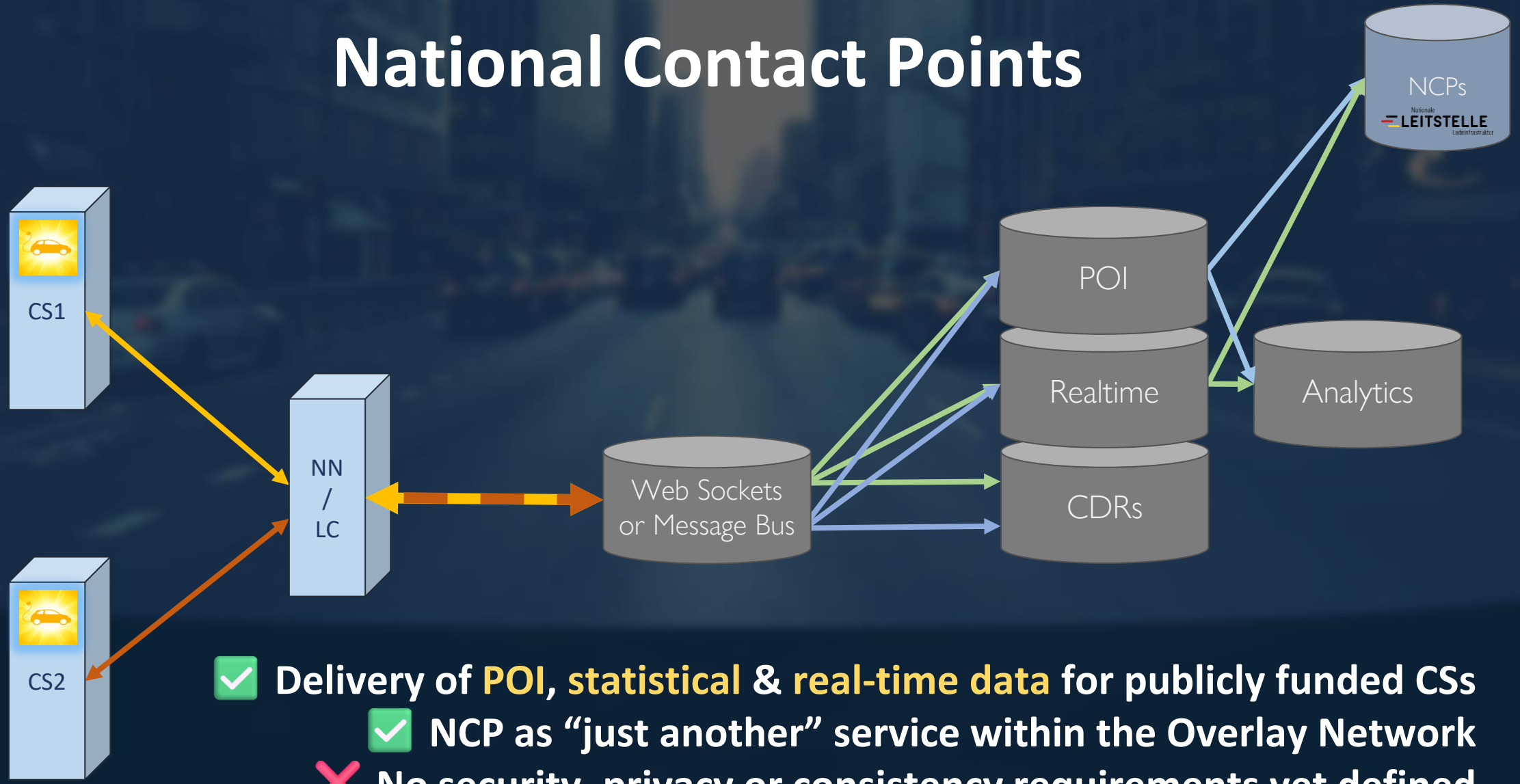
A Better German Calibration Law



✅ **Transparency Software as legally binding "remote display" for the validation of older (public) charging sessions**

⚠️ **Additional meta data should also be signed, e.g. tariffs, load reductions!**

National Contact Points



✅ Delivery of POI, statistical & real-time data for publicly funded CSs

✅ NCP as “just another” service within the Overlay Network

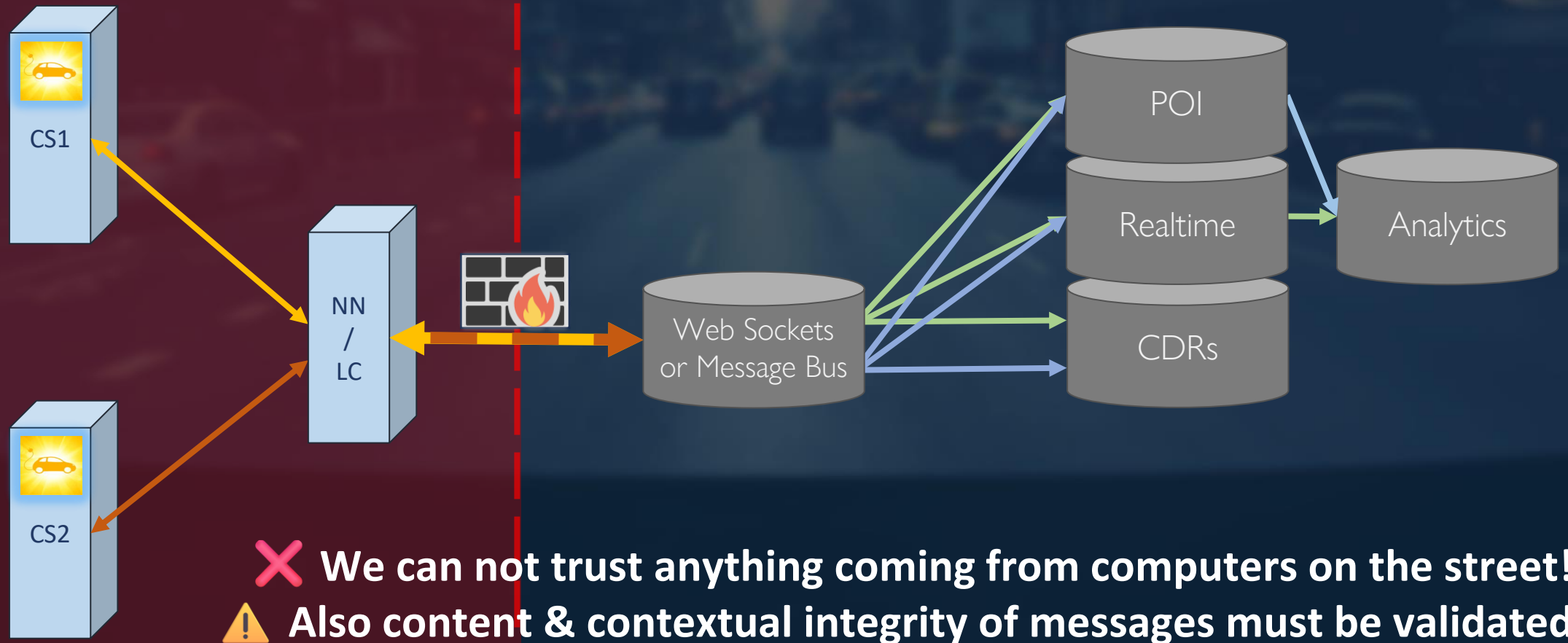
❌ No security, privacy or consistency requirements yet defined

✅ Anyway, it would be useful to send only authentic/signed data

No Physical Access Security

Realistic Physical Access Security

Physical Access (In-)Security



❌ We can not trust anything coming from computers on the street!

⚠️ Also content & contextual integrity of messages must be validated

✅ Small project how to secure against insider attacks by SMART CITY JENA

How to get this into “the market”?

- All these OCPP extensions are/will be available as *“Open Source Vendor Extensions”* on GitHub
- OCA Technical Working Group has a very conservative approach on *“backward compatibility”* and dislikes *“breaking” changes* :-/
- As usual: Many leechers, very few real contributors
  ➔ Become an OCA member to improve the situation ;)

Questions?

- https://open.charging.cloud
- https://open.charging.community

Sponsor on GitHub