# 5G for secure software/firmware updates
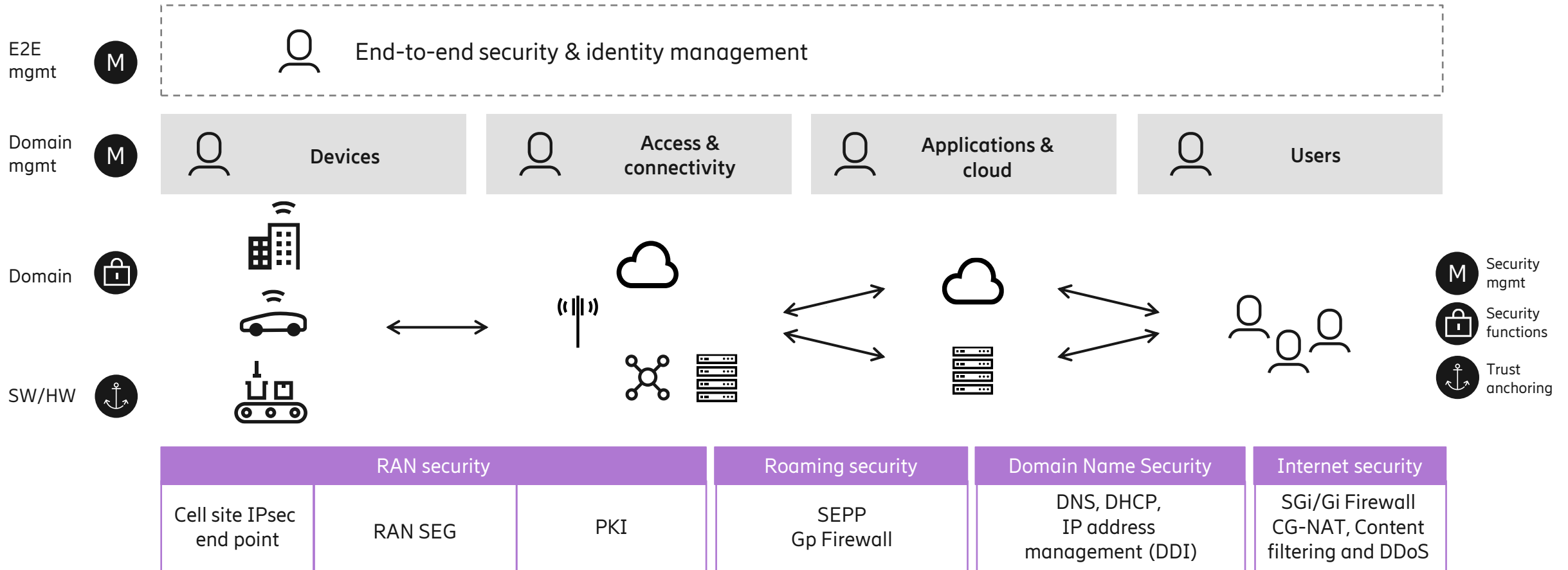
Patrik Teppo          CTO Office, Portfolio & Architecture          2021-03-26

# Connected vehicle paths

https://access.atis.org/apps/group_public/download.php/35648/ATIS-I-0000059.pdf
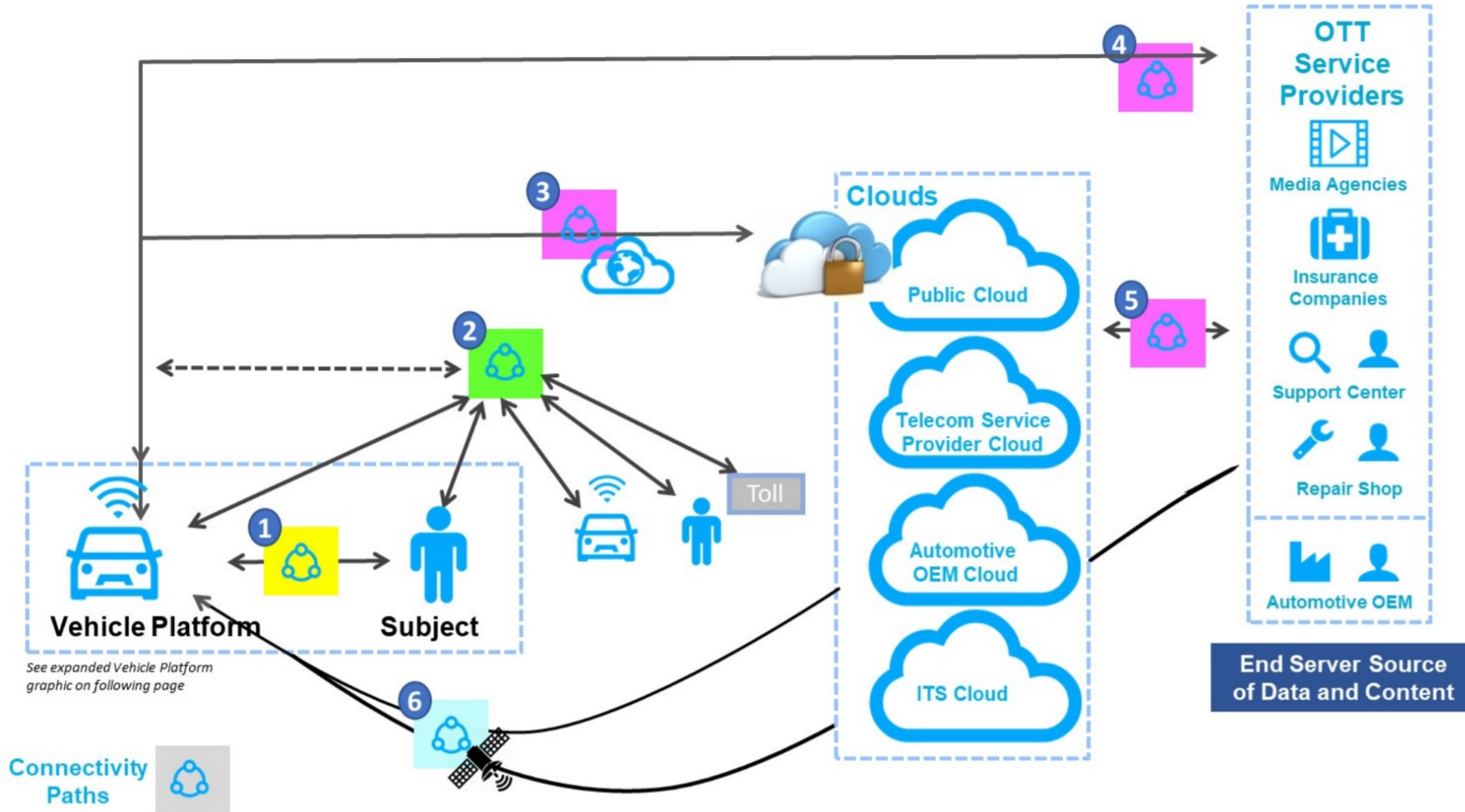
# Secure platforms & applications
## 5G End-to-end security architecture

| | | | | |
|---|---|---|---|---|
| **E2E mgmt** (M) | **End-to-end security & identity management** | | | |
| **Domain mgmt** (M) | **Devices** | **Access & connectivity** | **Applications & cloud** | **Users** |

(M) Security mgmt
🔒 Security functions
⚓ Trust anchoring

**Domain** 🔒

**SW/HW** ⚓

| RAN security | | | Roaming security | Domain Name Security | Internet security |
|---|---|---|---|---|---|
| Cell site IPsec end point | RAN SEG | PKI | SEPP Gp Firewall | DNS, DHCP, IP address management (DDI) | SGi/Gi Firewall CG-NAT, Content filtering and DDoS |

# 5G security controls

**Trusted Identities**

Credentials stored and processed in secure HW modules (SIM)

**Network built for Zero-trust**

All interfaces mutual authenticated, authorized, protected, ...

**Confidentiality & Integrity protection**

Hop-by-hop from device to data network

**Security & Identity management**

End-to-End from device to application & cloud

**Separation & Isolation**

For example, by using network slicing