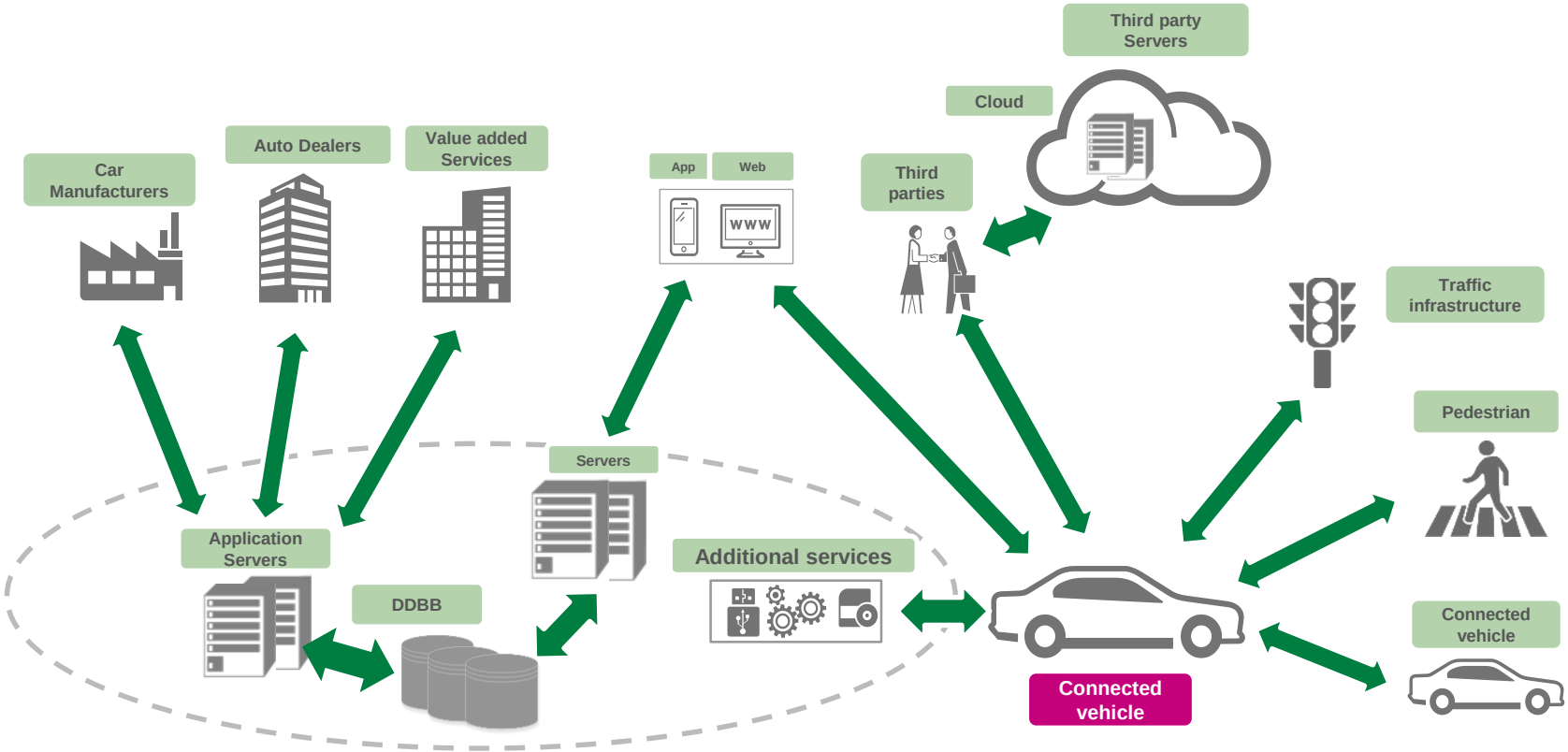
The Connected Vehicle - Challenges and Opportunities

Christoph G. Nolte
DEKRA Automotive

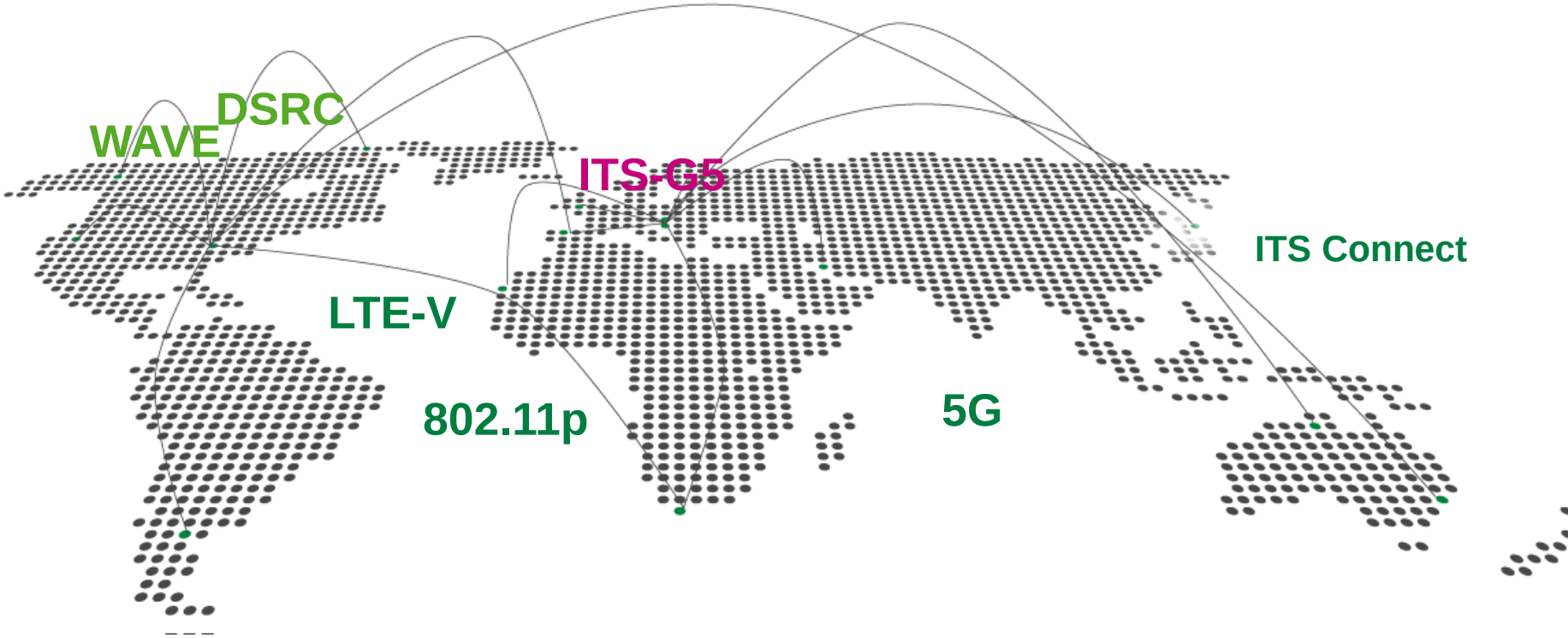
DEKRA

The connected vehicle ecosystem



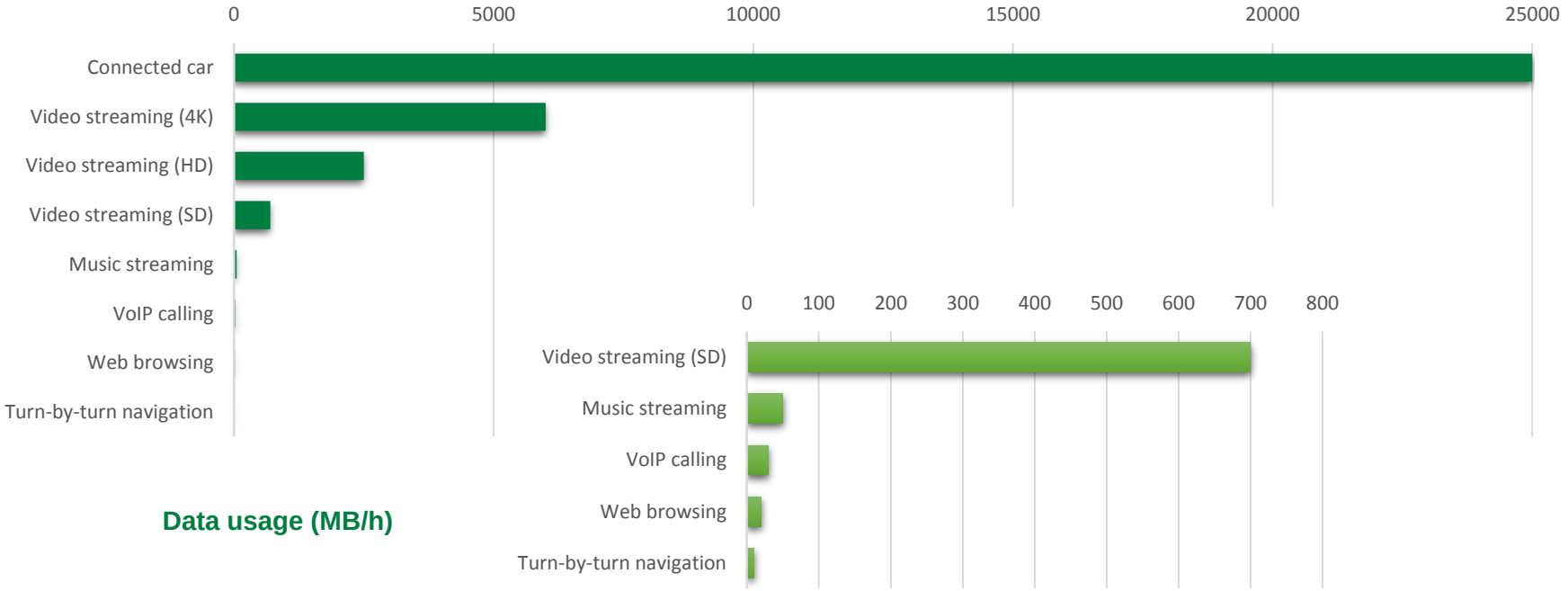
Standards

Fragmentation in standards



Data Usage

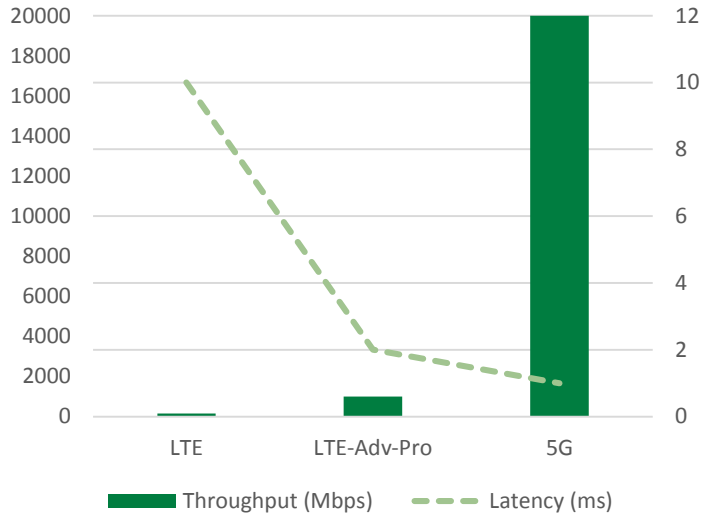
The connected vehicle – data usage



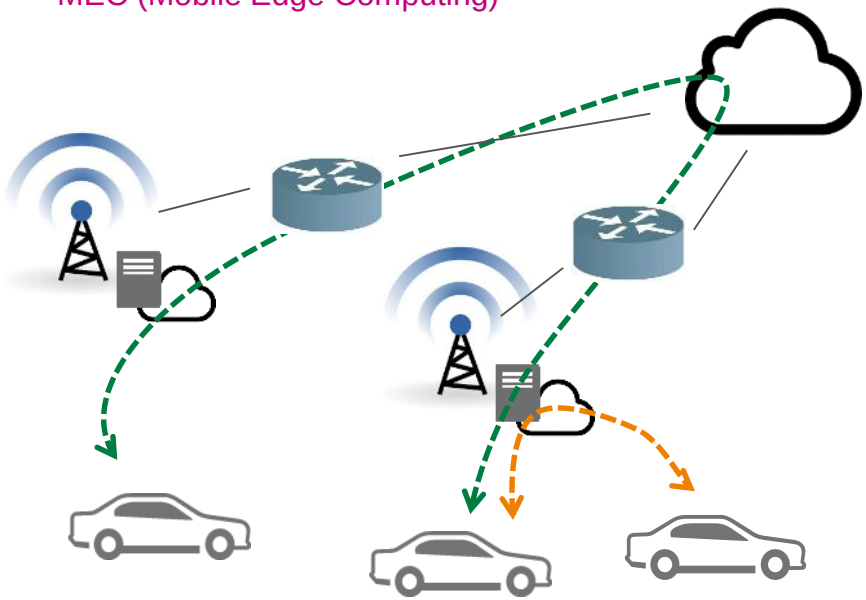
Data usage (MB/h)

Mobile network evolution

Speed and latency



MEC (Mobile Edge Computing)



Cybersecurity

Threats in the connected vehicle

Malicious firmware updates
- Through USB, CD, SD card
- Through OBD port
- Via OTA process

Attack from downloaded applications

Attack from mobile device applications

Man-in-the-middle attack

Attack to the vehicle internal bus (injection/capture)

Compromised actuators controlled by malicious software

Sniffing of user data and passwords through screens and keypads, transmitted to outside world

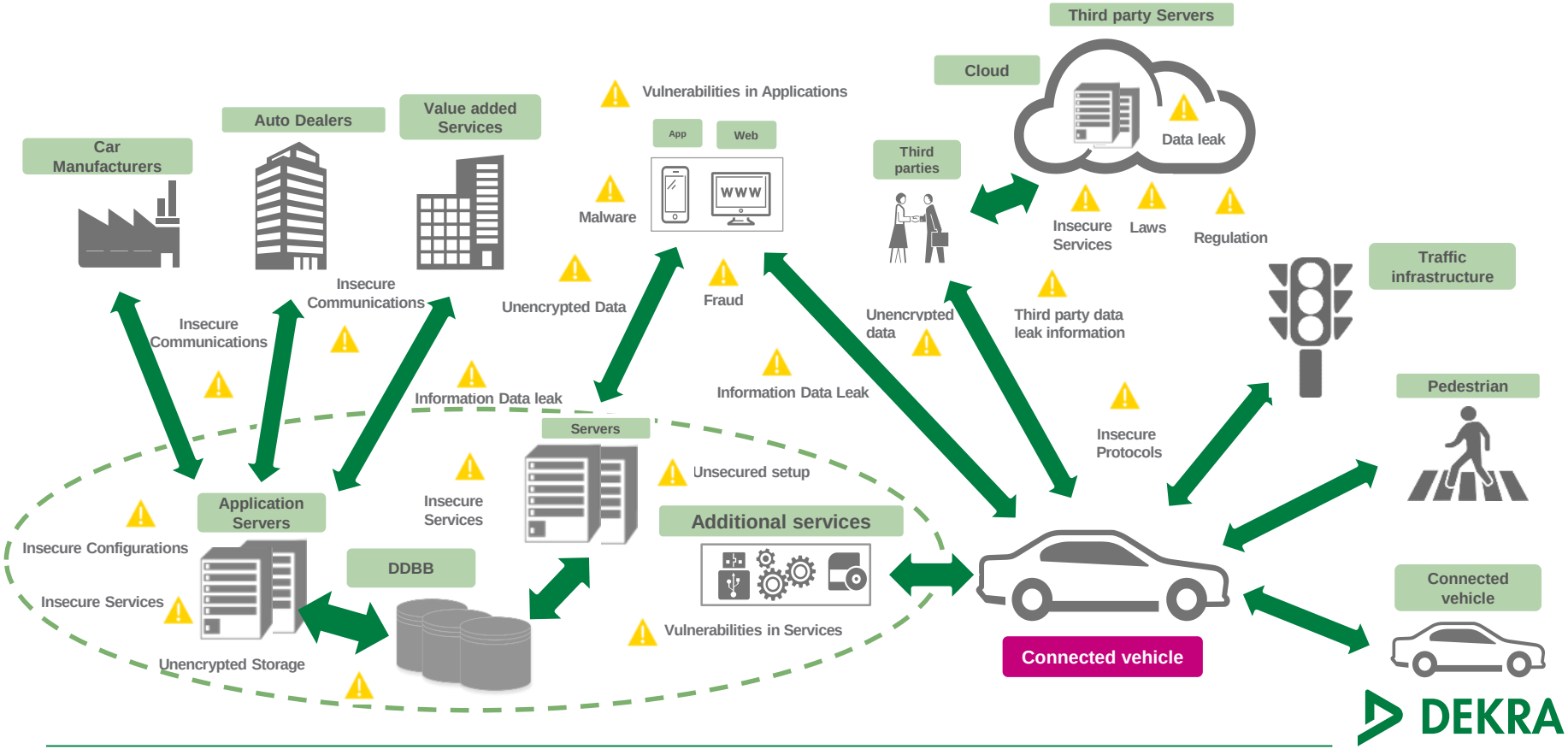
Attack on certificate and key stores

Malware delivered through encoded music

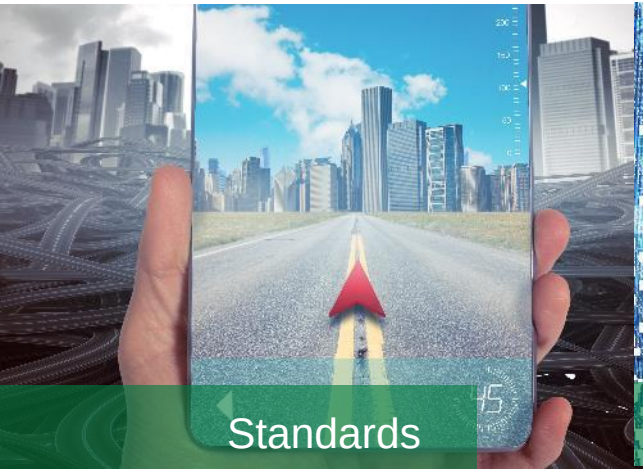
Open source software vulnerabilities

Any part of the electronic system can be an attack point

Threats in the connected vehicle ecosystem



The connected vehicle – challenges and opportunities



Christoph G. Nolte
Technical Director
DEKRA Automotive

christoph.nolte@dekra.com