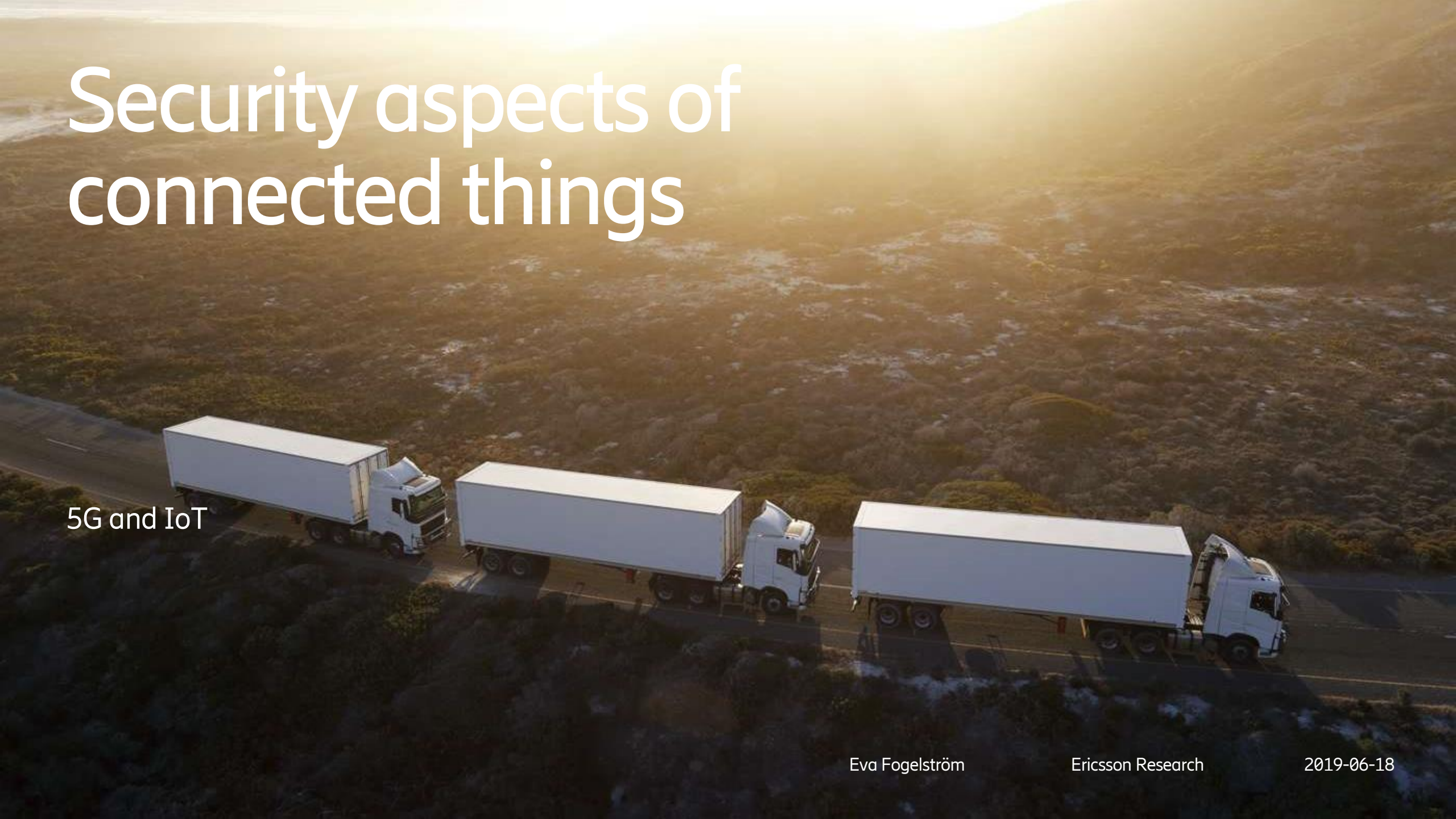
Security aspects of connected things



5G and IoT

Eva Fogelström Ericsson Research 2019-06-18

IoT features and challenges

IoT devices affect our lives
→ Intrinsic safety and privacy risks

The number of things
→ Distributed denial-of-service

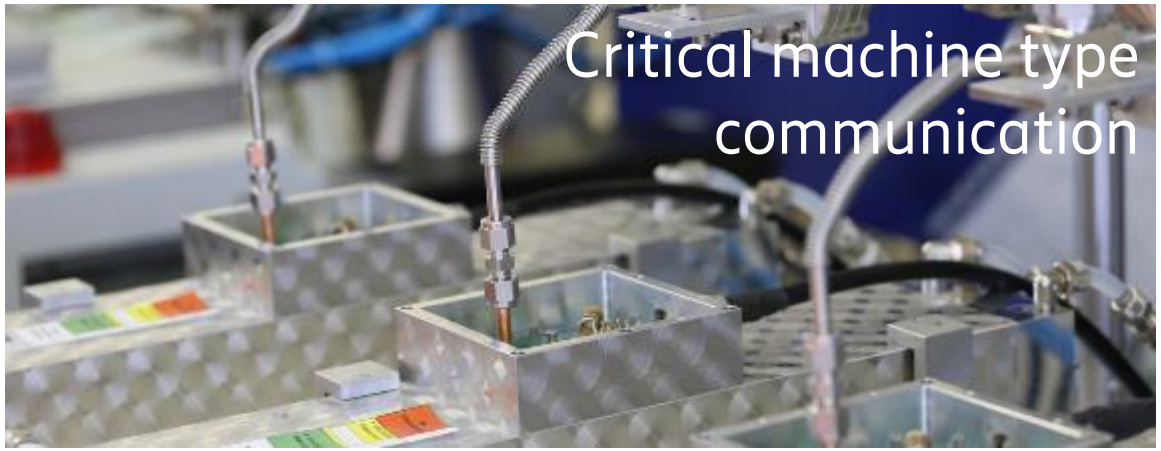
The hype and low security incentives
→ Common insecure deployments

Power constrained and sleepy devices
→ Security overhead challenges

Gateways and proxies
→ End-to-end security challenges

5G IoT use cases

- Connectivity for millions of devices
- Low volume, non-delay-sensitive data
- Low-cost devices with long battery life

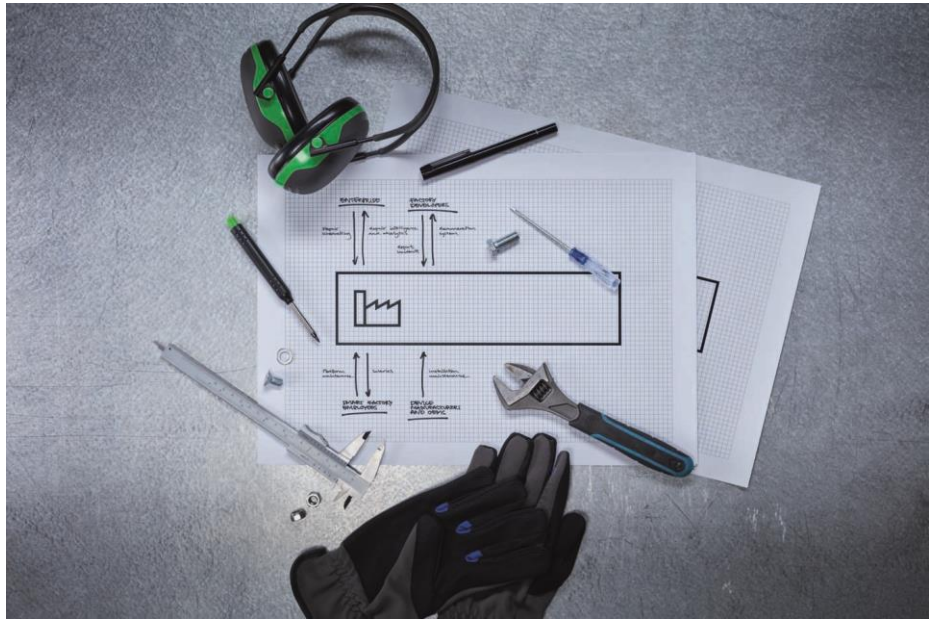


- Resilient instantaneous connectivity
- Throughput, latency, availability requirements
- Manufacturing, transportation

IoT security toolbox

- The IoT landscape is fragmented
- Large variety of things and technologies
- Different industries often use tailored security enablers
- Existing security tools are not always suitable for the IoT

→ Need for new tools and enablers in the IoT security toolbox



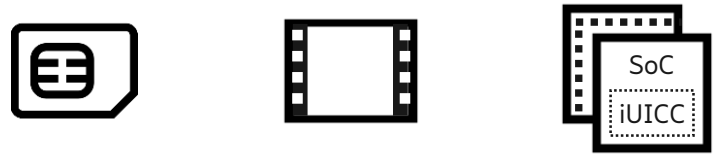
Communication security	Life cycle management
Software security	Identity managment
Hardware security	Security assurance

Identity management

— Secure identities to authenticate IoT devices and their data, and to protect them from misuse through remote attacks.

— SIM implementation optimized for low-cost constrained IoT with minimum functionality: network access authentication and download of new subscriber credentials (SIM profile).

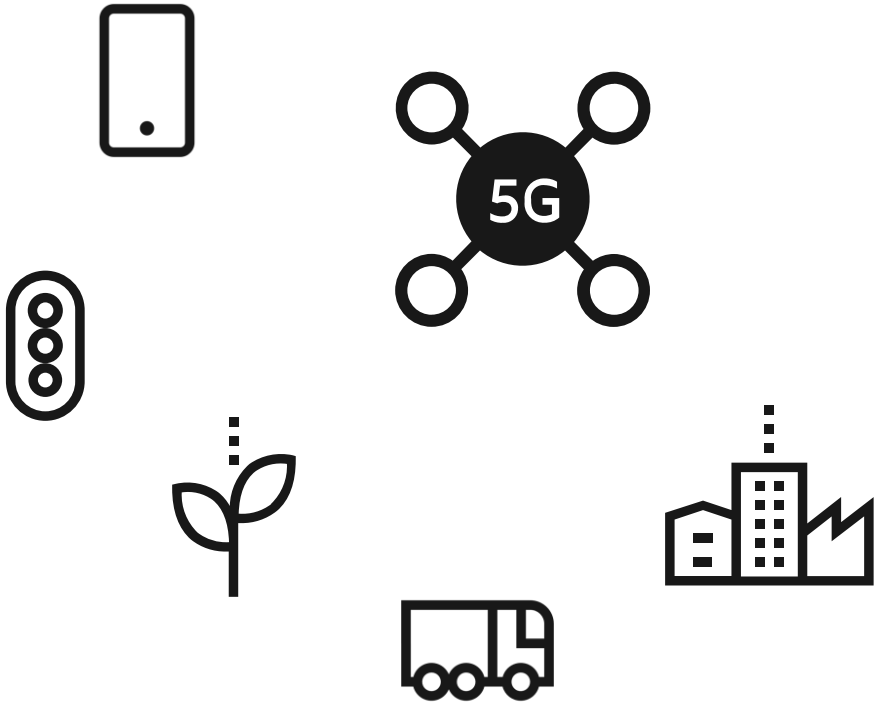
— Leverage on existing protocols in IoT device for remote SIM profile provisioning and SIM profile management.



SIM – embedded SIM – integrated SIM

5G authentication framework

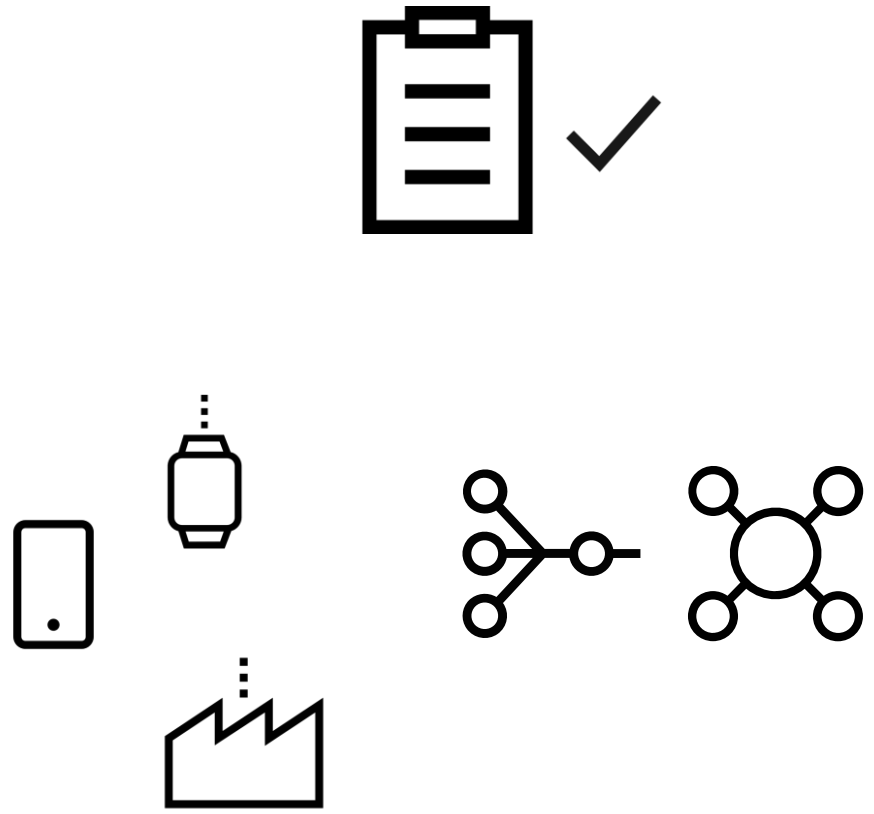
- Flexible framework allowing support of different authentication methods and authentication credentials; introducing new methods and credentials in the future.
- Standard mandates support of EAP and two authentication methods:
  - 5G AKA
  - EAP-AKA'
- Allows use of EAP-TLS, based on certificates.



Security assurance

— 3GPP security assurance – a means to ensure that network equipment meets security requirements and is implemented following secure development and product lifecycle processes.

— Certification of IoT devices – a means to ensure certain level of resistance against attacks on the devices and on the infrastructure.



Some thoughts

— Diverse security requirements

— Identity management and security assurance key components

— Unbalanced incentives for security

— Awareness and usability – make security the easy option