SIM Evolution: Keeping Pace with 5G Phasing

Published by simalliance now Trusted Connectivity Alliance

February 2019

5G continues to evolve…

- This is the need to evolve data throughput through network (10 Gbps)
- High reactivity of the network is required

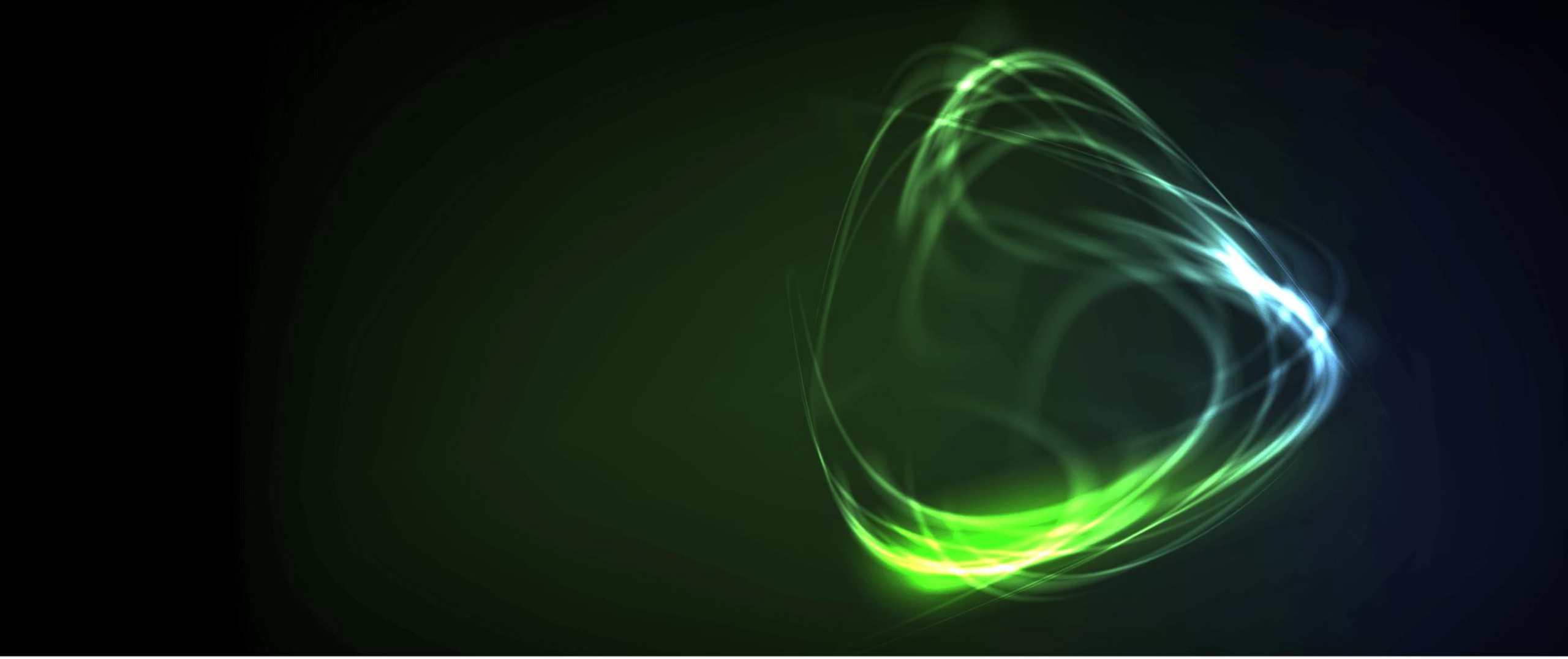
- Use cases that need high reliability / low latency (1ms)
- E.g. V2X, robotics in industry

- Addressing connected object explosion
- Lots of connections (1 million connections per km2)

The continued evolution of 5G is being powered by three key drivers:

In the same manner, the SIM needs to evolve….

Release 15 (R15) → **Release 16 (R16)** →



What are the challenges specific to each driver which can be addressed by an evolved SIM?

Mobile broadband: Multiple MNO challenges

Mobile broadband is driving the first phase of 5G (R15). SIMalliance's recommended 5G SIM is already positioned to address many of the challenges faced by MNOs.

The challenge for MNOs:

- Ensuring good Quality of Experience
- Subscriber privacy
- Delivery of all IP services
- Network resource optimisation
- Security

How the 5G SIM helps:

- Quality of Experience monitoring
- Subscriber ID encrypted
- Authentication to the IMS / SIM can be refreshed through HTTPs
- Service prioritisation stored in the SIM
- 5G network access security

As we move forward into the next phase of 5G (R16), the SIM will continue to evolve to meet the new requirements of massive IoT and critical communications….

Massive IoT: Protecting access and services

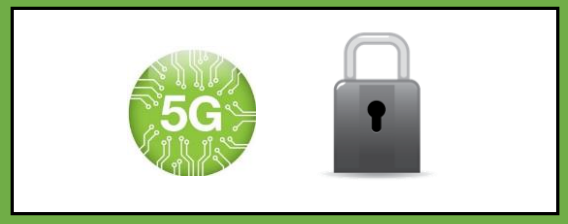
The increasing number of end-points in cellular IoT will create a number of challenges:

The challenge for MNOs:

- Economically viable deployments require that device bill of materials cost is controlled (e.g. smoke detector)
- As each device widens the deployment's attack surface, each device must be protected to ensure service (or even national) security
- Device identity must be validated in order to authenticate data sources

Evolved SIM: The requirements:

- Depending on security feature, evolved SIM could be integrated in other semiconductor components in order to reduce device bill of materials
- Security is provided by a tamper-resistant hardware component
- Evolved SIM security capabilities can be used by IoT devices for authentication and encryption in order to secure the device and IoT services



Critical comms:
Need for high security and reactivity

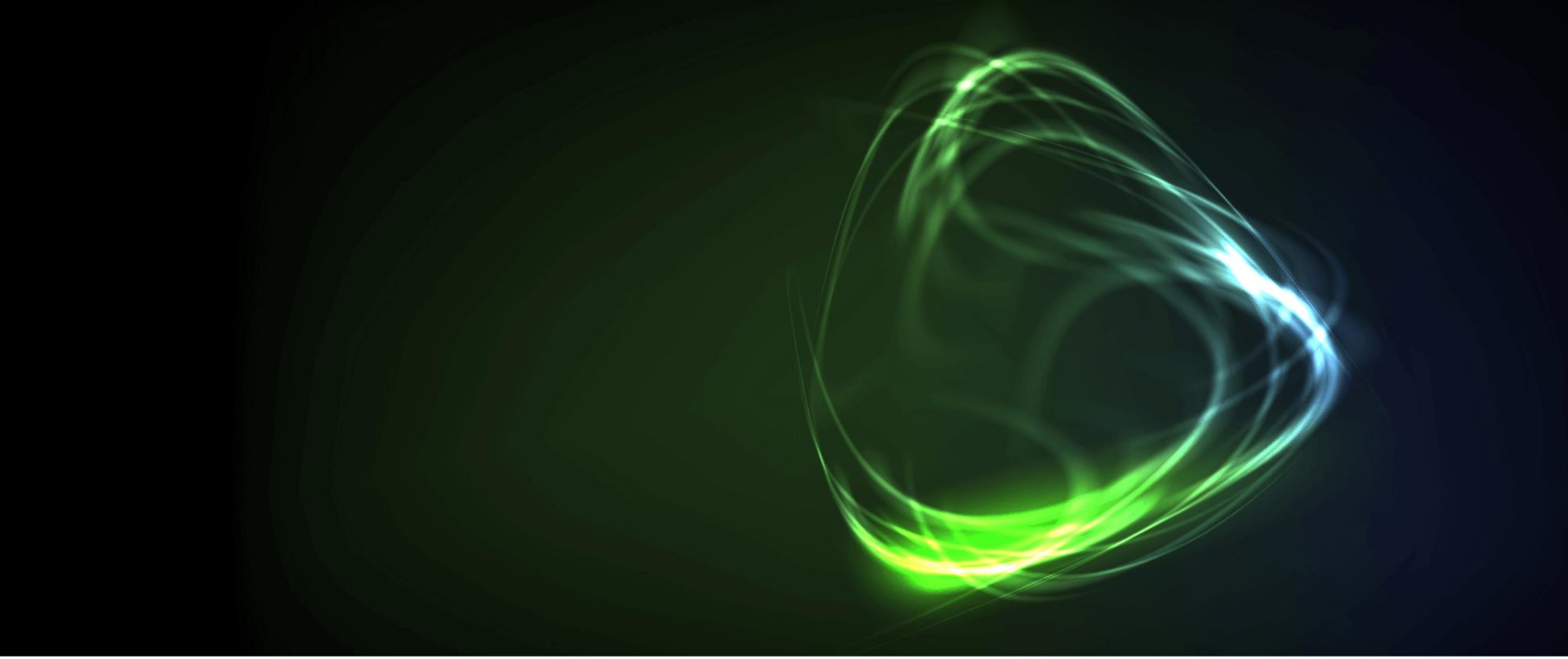
The nature of critical communications use cases (highly secure and requiring high reactivity) creates a number of challenges.

The challenge for MNOs:

- Highly secure identification is required for many critical applications (e.g. life-or-death, industrial)
- Strong security is needed at the application layer
- Communication and authentication need to be very reactive
- Strong performance is needed

Evolved SIM : The requirements:

- Stronger authentication to network: longer crypto keys and advanced algorithms.
- Additional security capabilities to secure critical communication services
- Additional certifications may be required for some applications (e.g. medical and military)
- Improved interfaces to chipset/modem for fast reactivity
- Higher performances (processing, memory, cryptographic operations etc.) to enhance overall reactivity



What additional evolved SIM features would add further value to 5G deployments?

Capability to leverage network slicing

Opportunities for MNOs to monetise network resources:

- Network slices enable MNOs sell network capability as a service to support the needs of different use case requirements
- Mobile broadband, IoT and critical communication are examples of custom network slice categories defined by MNOs to cover different vertical industries

Software partitions

- Robotic factory
- Massive IoT
- Critical comms
- V2X

Evolved SIM: Associated expectations:

- Service-specific authentication offered by slice may be supported
- Evolved SIM may manage different security parameters depending on service-specific security requirements offered by slice
- MNO preferences which ensure proper device configuration to the service offered by the slice

Stronger device and subscriber security

Opportunities for MNOs to enhance ecosystem security:

- A device ID can be hacked, presenting security risks for some applications
- Attacks are evolving on existing authentication procedures
- A device can be used by several users; authentication of subscriber should be enhanced (versus current PIN)
- A device can be stolen; user data should be protected
- Increased need for MNO / service provider to better control global security policy throughout SIM lifecycle (relevant to subscriber and device)

Evolved SIM: Associated expectations:

- Highest level of security is provided by a tamper-resistant hardware component that protects the device ID
- Further reinforcements of authentication through SIM evolution are expected
- Biometric user authentication could be a solution to replace the PIN
- SIM evolution could be used to protect user data and applications in the device
- Risk manager policy could be stored and managed through SIM evolution

Support for SMS replacement in all IP networks

Opportunity for MNOs to save SMS infrastructure cost:

- Retaining legacy SMS infrastructure is transitional and costly
- Methods to target the SIM Over-The-Air (OTA) have limitations and require enhancements to fully benefit from new network capabilities

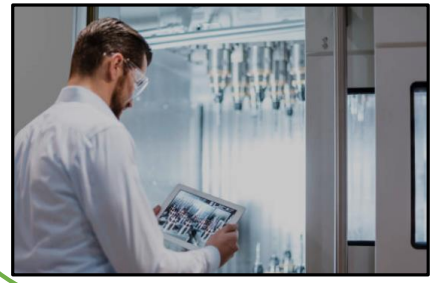
Evolved SIM: Associated expectations:

- Evolved SIM requires an alternative to SMS to directly and remotely deliver or receive messages in an all IP network
- Expectations include:
  - Full disassociation from current SMS infrastructure
  - The provision of improved reliability and performance in content delivery, even in roaming scenarios

Long term key update

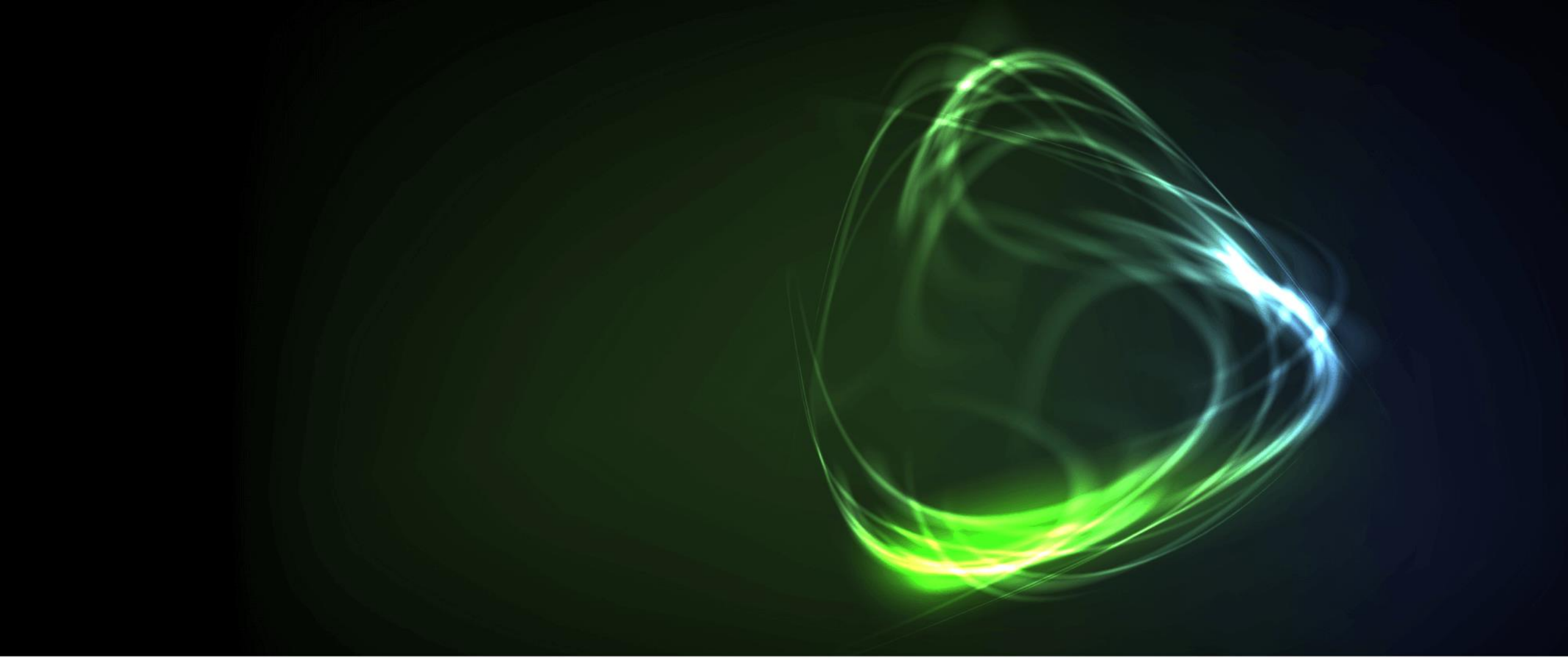
Opportunity for MNOs to maintain trusted environment over time:

- Current mobile security architectures rely almost entirely on the secrecy of the long term secret key that is stored in the SIM
- Authentication key and algorithm might be accidentally exposed to a hacker



Evolved SIM: Associated expectations

- Evolved SIM will allow remote update of authentication credentials and algorithm upon MNO security policy decision
- Such a mechanism will allow for remotely re-establishing a trusted security level without re-issuance of the physical evolved SIM



Conclusion

Conclusion

1

The evolved SIM will address the challenges and opportunities facing the MNO as 5G evolves…

- Mobile broadband, critical communication, massive IoT
- Network slicing
- Device and subscriber security
- SMS replacement in all IP networks
- Long term key update

2

5G specifications for 3GPP R16 are in development. When they are, other opportunities for the evolved 5G SIM may emerge…