National Cyber Security Centre

Hardening a (mission critical) service using 5G

Peter Haigh

Tech Director for Telecoms

UK National Cyber Security Centre

Hardening a (mission critical) service using 5G

- Intro to the Mission Critical System:

  + the security challenges of building an over-the-top service

- The Mission Critical System, 4G & 5G:

  + thoughts for security improvements in 5G phase 2.

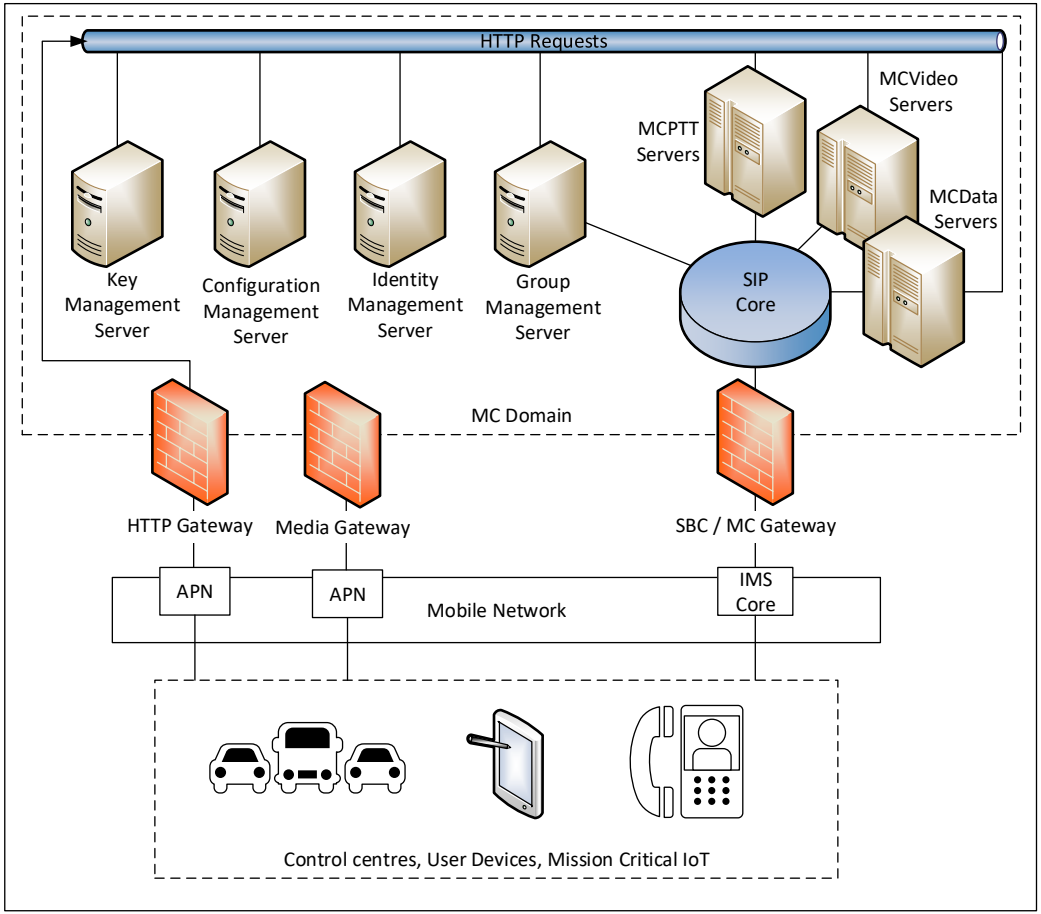
(Presentation is standards-specific, not UK-specific).

Security of the Mission Critical System

Intro to the Mission Critical System

MC system uses:

- HTTP bearer:
  - Provisioning data
  - configuration data
  - file upload/download
- Signalling bearer (SIP)
  - Majority of signalling content within embedded XML
  - Routed over IP bearer or operator's IMS core.
- Media bearer
  - Unicast or multicast
  - Routed without modification by MC Domain
- ProSe & IOPS

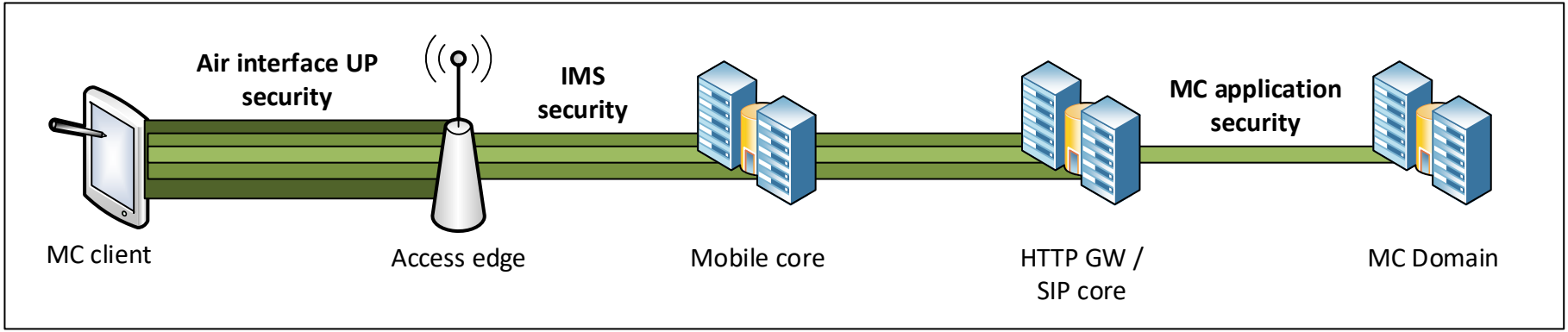


Security comparison: Mission Critical and TETRA

	TETRA Security	Mission Critical Security
Isolation	Network 'owned' by customer. Isolated from commercial network.	Shared network resource. Can run on top of commercial network
Network security	Bespoke to service (but similar to GSM)	Reuses LTE and IMS security.
Authentication	Handset-based authentication. Authentication provided by network.	Handset and user-based authentication. User authentication provided OTT.
Metadata security	Metadata within 'own' network hence is not protected	Network security does not reach MC Domain so metadata may be protected OTT.
Media security	End-to-end media security is an optional feature that can be used. By default it is not protected.	End-to-end media security mandated as part of comprehensive OTT security model.

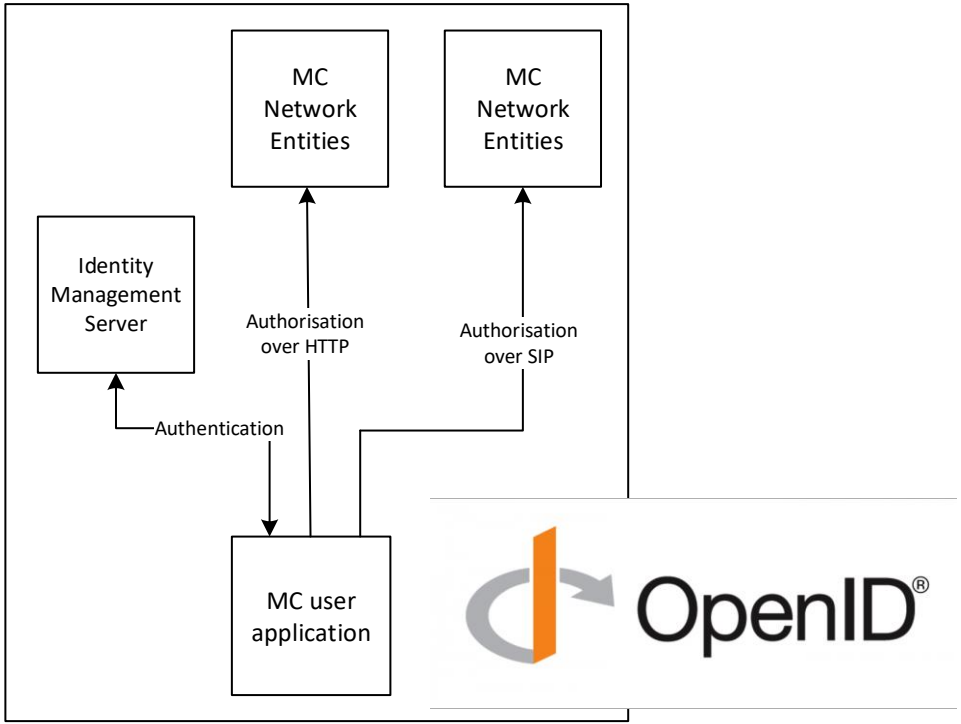
Mission Critical Security

- Three security layers:
  - LTE security
  - Signalling security (TLS for HTTP , IPSec to SIP core)
  - Application security (authentication, end-to-end media security)
- Each security layer acts independently of the others.



Mission Critical Authentication

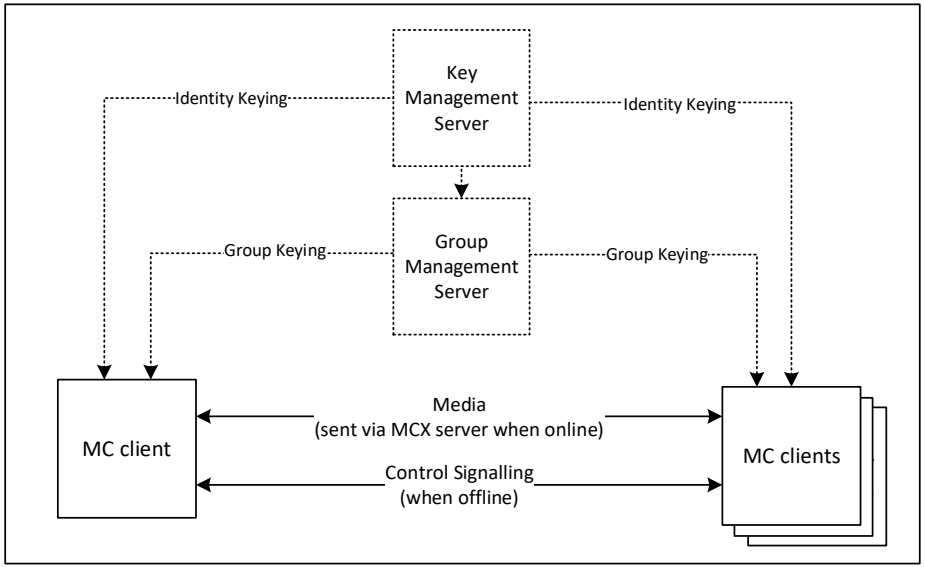
- Client authenticates to the network,
- …then the SIP Core, providing subscription authentication to the MC domain,
- …then the user authenticates to the MC Domain.
- OpenID connect 1.0 used for user authentication and authorisation.
- No restriction on the authentication methods used by the IdM.
- Tokens delivered over SIP and HTTP.



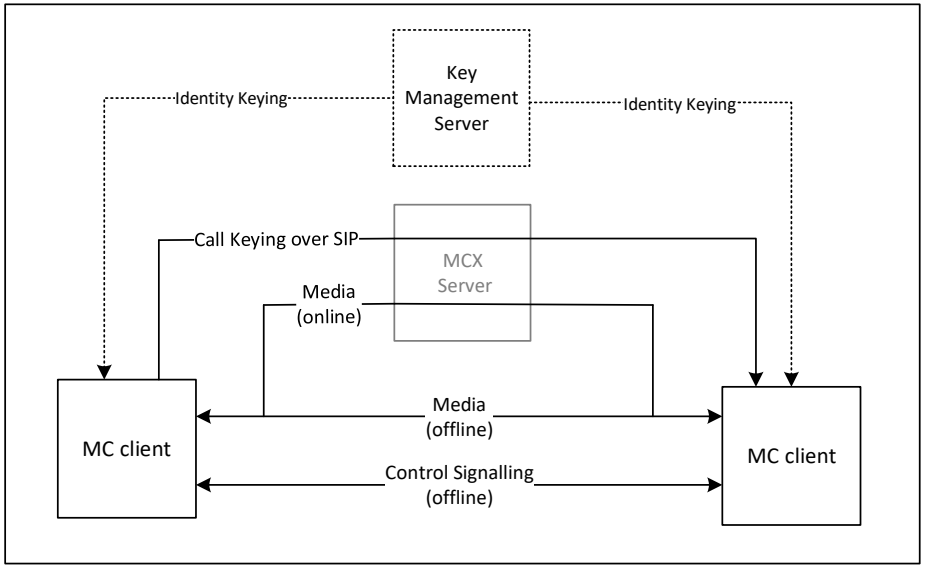
Mission Critical media protection

- Media security is client-to-client – can be routed via network or directly (ProSe).
- Requires key provision by KMS (IDPKC), and key provision by GMS for group comms.

Group comms:

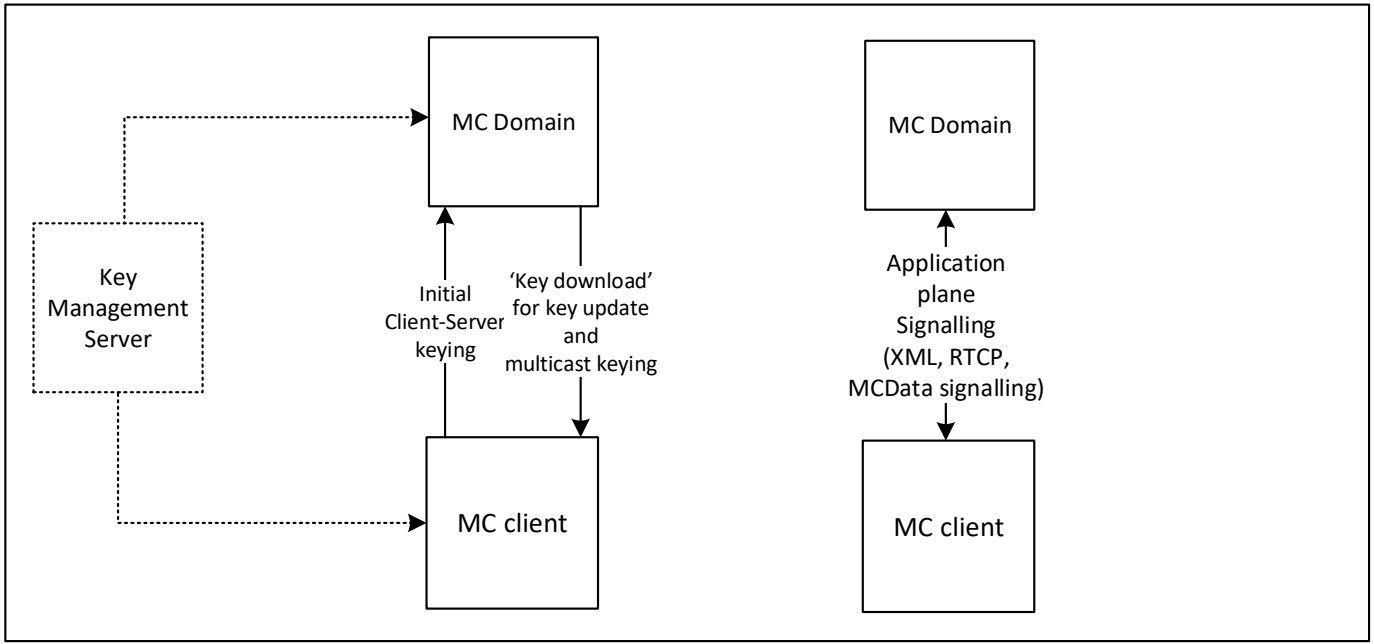


Private (one-to-one) comms:



Protection of Mission Critical metadata

- LTE/IMS network security does not protect MC metadata up to the MC Domain.
- MC System defines optional application signalling security mechanism to protect this data.



The Mission Critical System, 4G and 5G

Mission Critical and 4G

- LTE/IMS provides the following to the MC System:
  - Unicast/Multicast/IOPS/ProSe bearer
  - IMS: Subscription authentication & SIP transport
  - Prioritisation
- Integration between the LTE/IMS network and the MC domain is pretty limited.

Mission Critical and 5G Phase 1(?)

- *Use of IMS/multicast/ProSe/IOPS?*
- *Use of NEF/CAPIF?*
- *Which subscriber's data is reaching me? Use of secondary authentication?*

Looking to 5G Phase 2

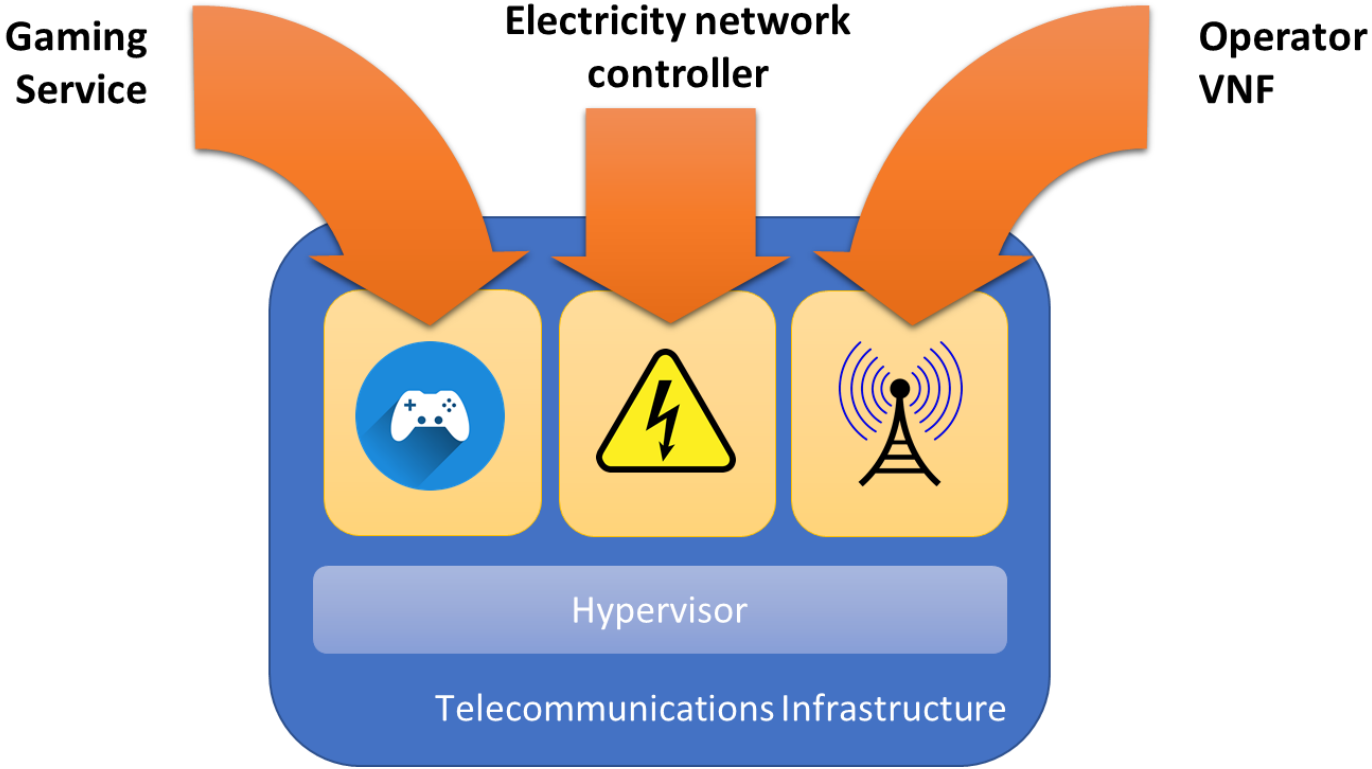
Considering the (mission critical) service as a 5G network slice:

As a customer, the slice should feel like a natural extension to my service

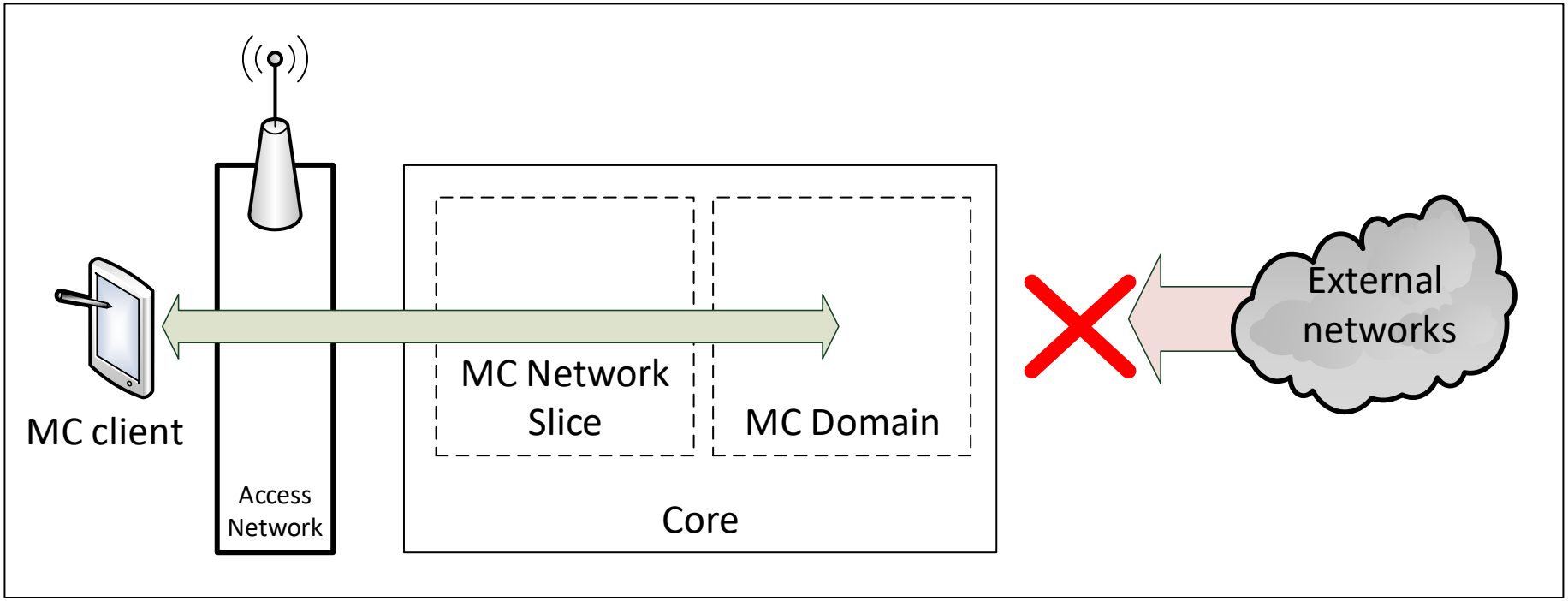
Security questions:

- Does using a slice make my life easier?
- Can I trust your network with the data in my slice?
- Is my device & slice effectively isolated from attack?
- Can I access data about my devices accessing my service?
- Is the data securely delivered to my slice?

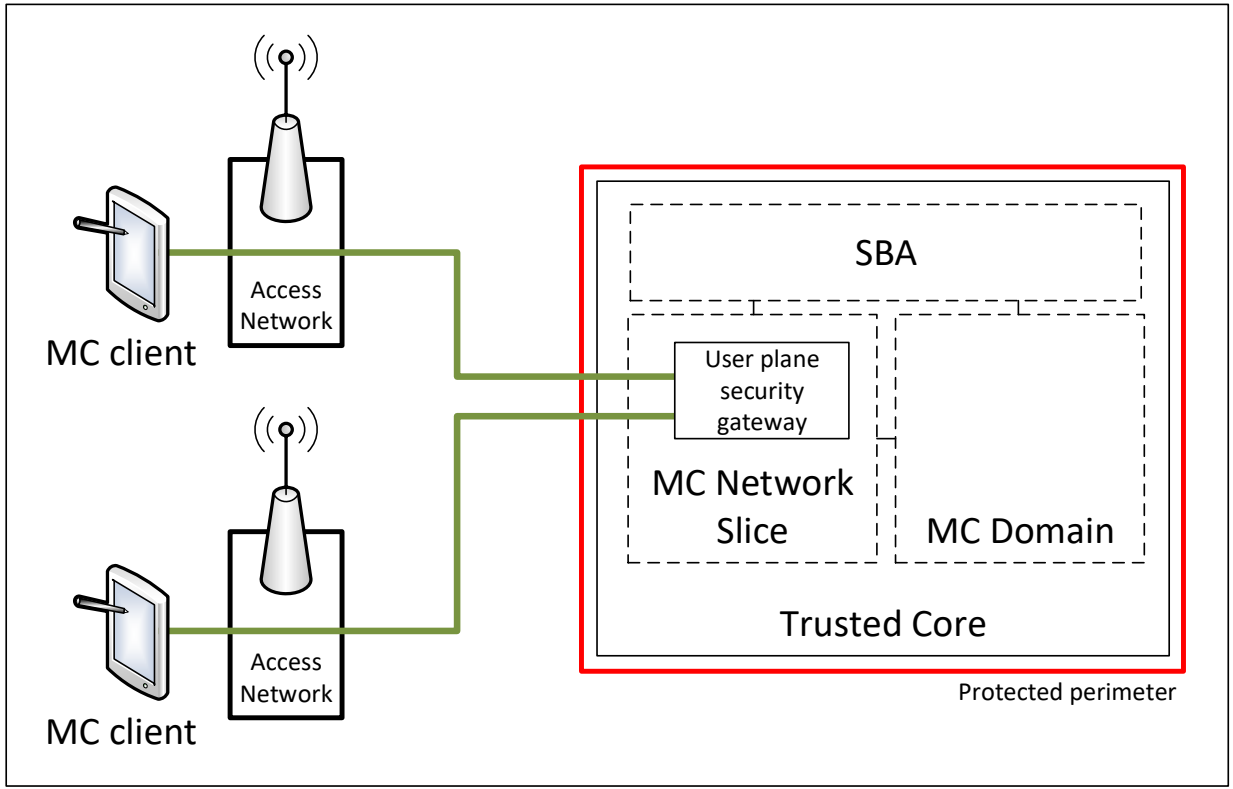
5G Phase 2: Slice virtualisation security requirements?



5G Phase 2: Isolating slices from external attack?



5G Phase 2: Consistent user plane access security?



Conclusion

Successful 5G slicing will do the following:

- **Make it easy to launch a (secure) service.**
- **Run on a trusted in a network and on trusted hosts.**
- **Slice security/isolation will be configurable dynamically.**
- **Provide a 'private line':**
  - **Deliver my user's data securely into my slice.**
  - **Automatically associate delivered data with my device/user.**
  - **Be the edge firewall for both my service and my device.**

Questions?