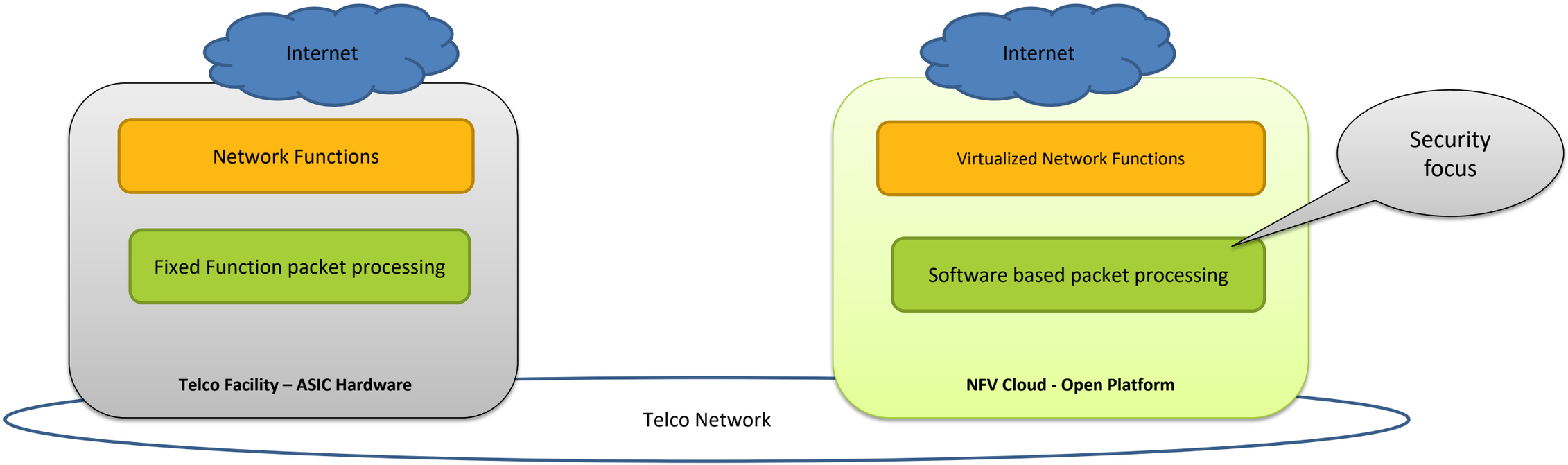
Protecting EPC User plane & Charging with Intel® Software Guard Extensions (Intel® SGX)

Somnath Chakrabarti - Security & Privacy Research/Intel Labs

ONF Connect 2019

Background - Network Functions Evolving For NFV Cloud



Physical Appliance

Built into Telco HW Function

In-Building Access

Protection from Insiders

Distributed SW Infra-

Automated instantiation w/ VNFs

+ Secured Remote Access

+ Protection from Outsiders

Virtual Network Function – Software Building Blocks

Fixed network functions on proprietary hardware

Router

EPC

VPN

Firewall

Load Balancer

Deep Packet Inspection/ IDS

VS.

Virtual network functions on commodity hardware

Router | EPC | VPN | Firewall | Load Balancer | DPI/IDS

Software Building Blocks

N-tuple Lookup | State Machines | Policy Manager | …

Filters | Key Manager | Hash Table | …

Reducing the “Attack Surface” with Software Guard Extensions (SGX)

Application gains ability to defend its own secrets

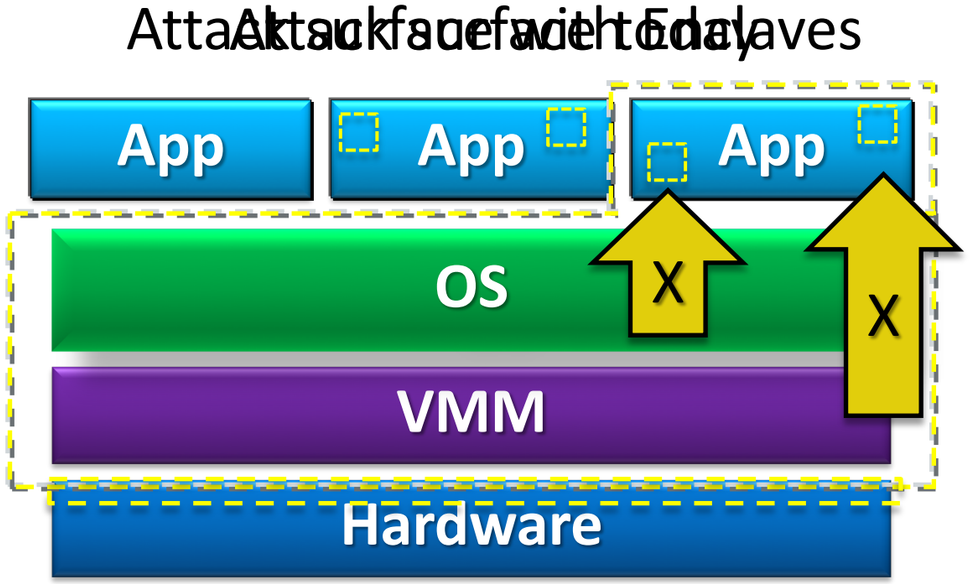
- Smallest attack surface (App Memory + processor)
- Malware that subverts OS/VMM, BIOS, Drivers etc. cannot steal app secrets

Familiar development/debug

- Single application environment
- Build on existing ecosystem expertise

Familiar deployment model

- Platform integration not a bottleneck to deployment of trusted apps



Attack Surface

Scalable security within mainstream environment

Security sensitive VNF Hardening with Intel® SGX – Use cases

* Potential Security-Performance Trade-offs

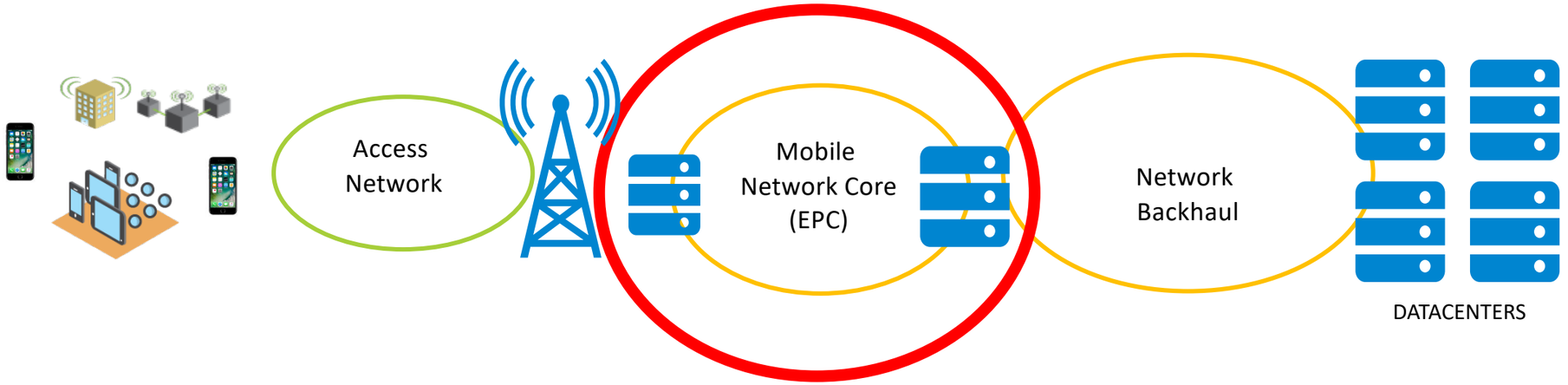
NFV/SDN Building Blocks	SGX Value Add*	
	Software Isolation	Runtime Physical Attacks
N-tuple lookup	Y	Y
Filter Packets, State Machines	Y	Y
MEC/Cloudlets/Edge cloud/5G VNFs	Y	Y
Protection of Keys (Encryption keys, Certificates, IPSec keys)	Y	Y
IP Protection of Algorithms, Data (SIG Files, Policies, Hash Tables, Analytics Meta Data)	Y	Y

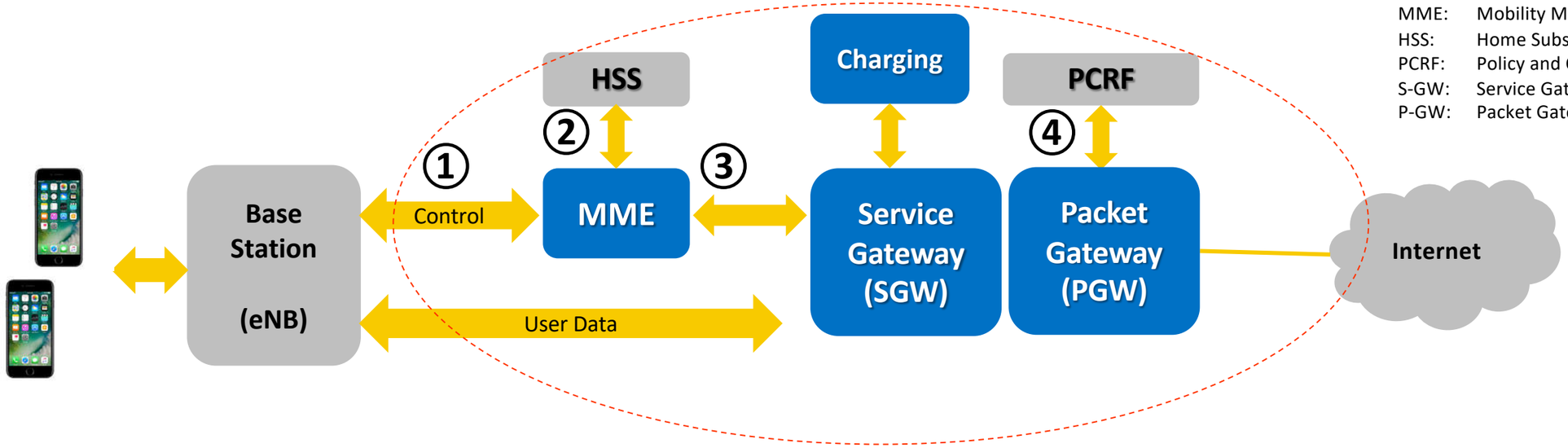
- Software Isolation: Encrypted & protected pages, OS/VMM not in TCB, contained impact of leaky VNFs
- Runtime Physical Attacks: System administrators, operators not in TCB
- Other SGX Cloud usages applicable to NFV: Keys Protection, DB protection, SSL termination

Design choices : Packet processing inside SGX enclave

- Enclave packet access mechanisms
  - 1 core - Calling into enclave to transfer every packet or burst of packets (bad idea)
  - 1 core - Calling into enclave everytime to transfer pointers to packets (still bad)
  - 2 cores – I/O core outside the enclave. Packet processing core inside the enclave
    - call into enclave just once to initialize Rx and Tx ring pointers (current Prototype)
  - 1 core – setup the NIC/DMA outside the enclave.
    - call into enclave and run I/O engine inside enclave (new prototype)

Goal of OMEC - Open Mobile Evolved Core

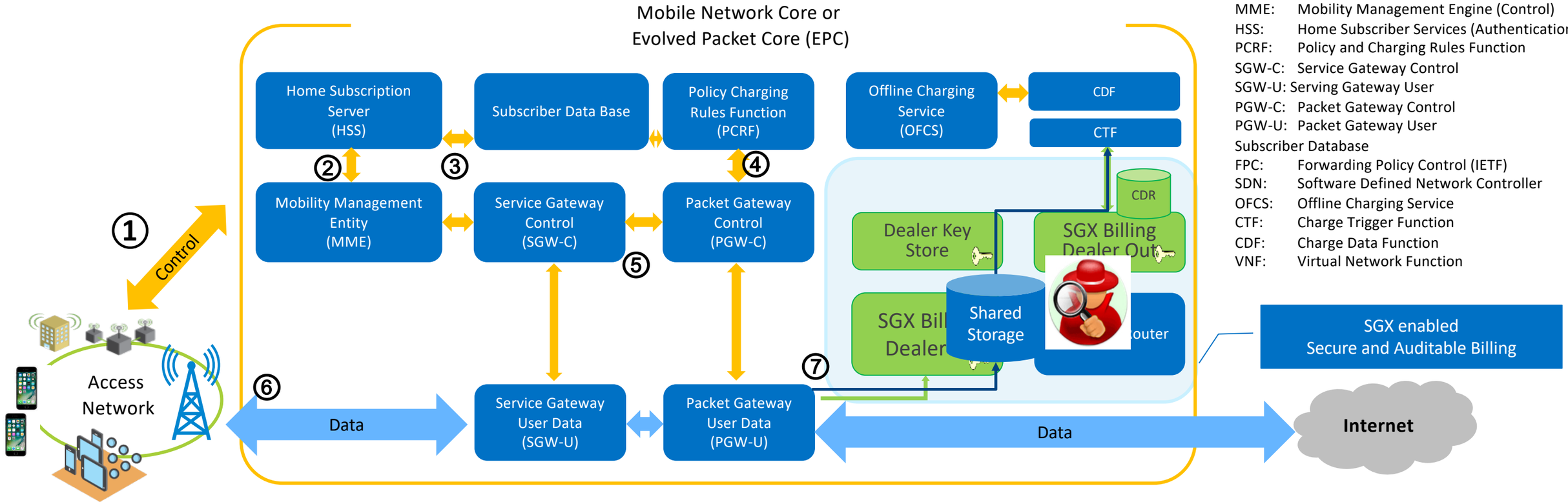




MME: Mobility Management Engine (Control)
HSS: Home Subscriber Services (Authentication)
PCRF: Policy and Charging Rules Function
S-GW: Service Gateway (Charging, services, …)
P-GW: Packet Gateway (Router)

Can we securely run Telco core infrastructure on high volume servers to deliver operational capacity?

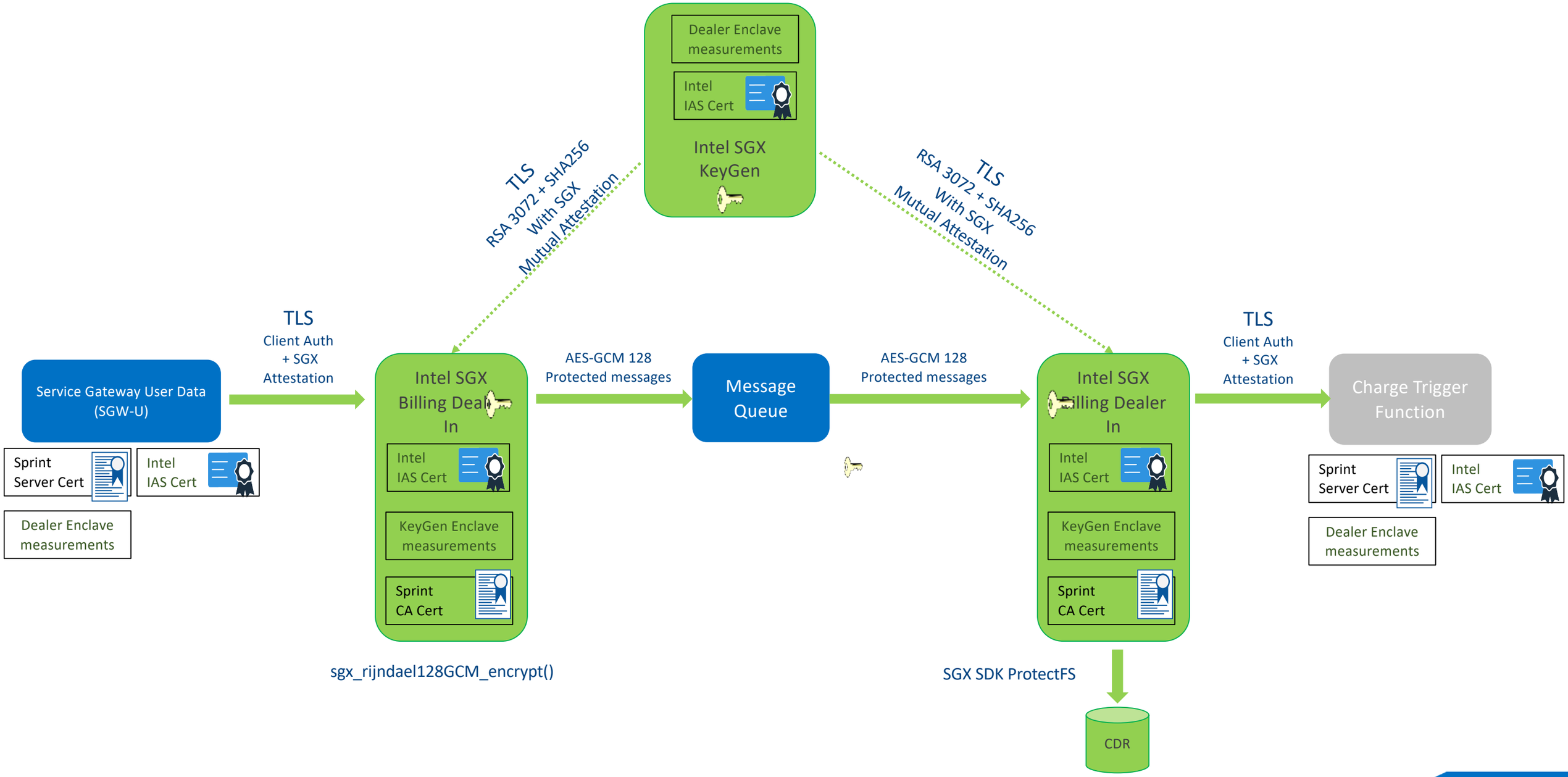
OMEC 1.0 – Fully Featured & Intel® SGX Hardened Charging



E2E Comprehensive EPC Infrastructure:

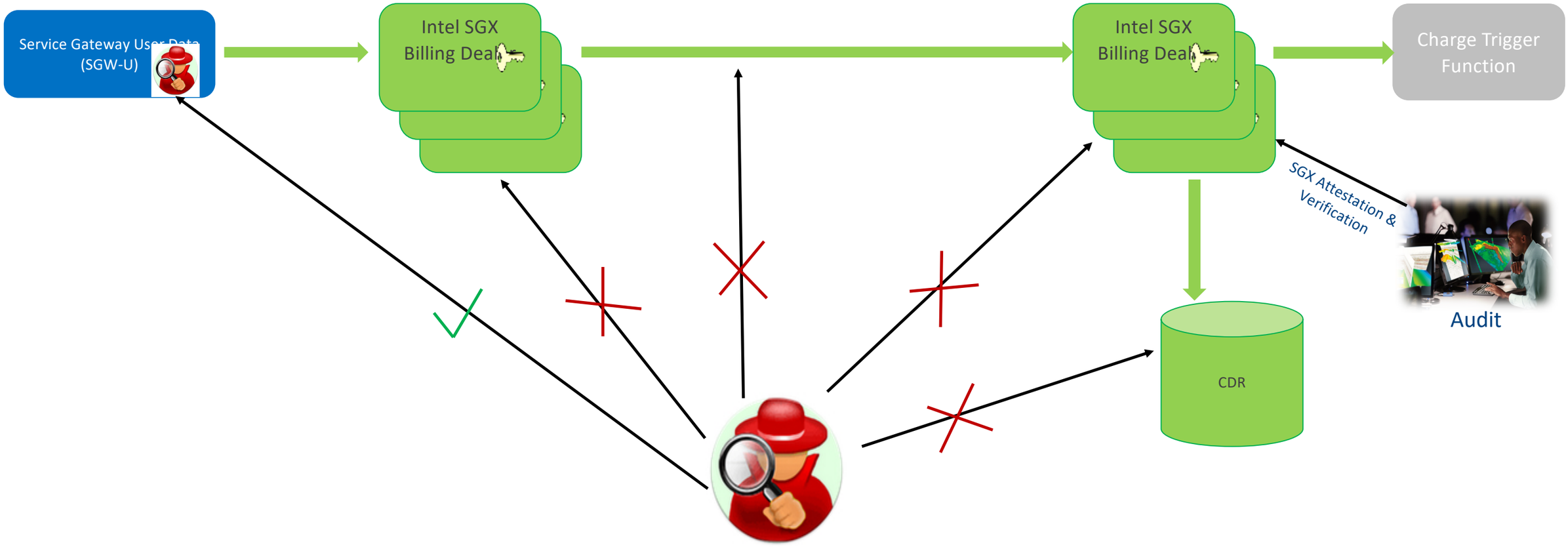
- https://github.com/omec-project
- Fully protected & distributed Xeon E3 based SGX enabled billing system, automated, real time billing data collection and storage.
- SGX based auditable mutual attestation. Provides confidentiality and integrity of Charge Data Records (CDRs)
- Cross platform deployment orchestration, provisioning and network configuration tools ready- KVM, AWS, Docker, K8, …

OMEC – Charge Data Security

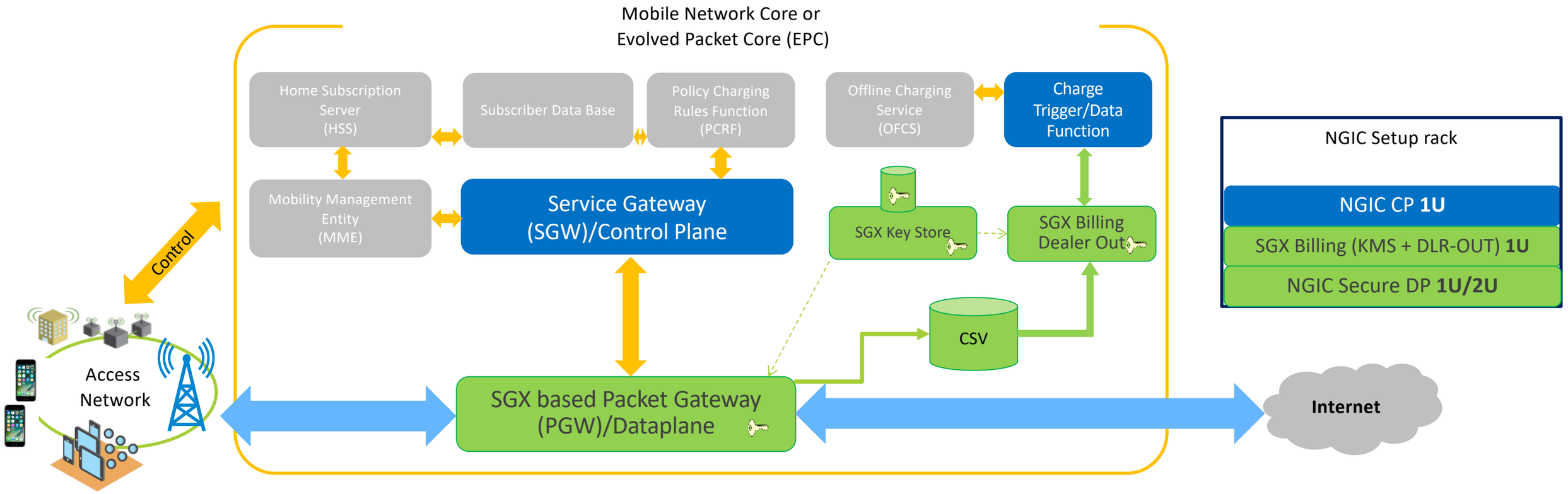


OMEC – Charge Data Security contd.

- Provides Confidentiality and Integrity of CDR Records
- Telco out of trust boundary provides ease of auditability
- Scalable



Mobile Infra Core Control/Data plane configuration – With Intel® SGX Dataplane and Billing

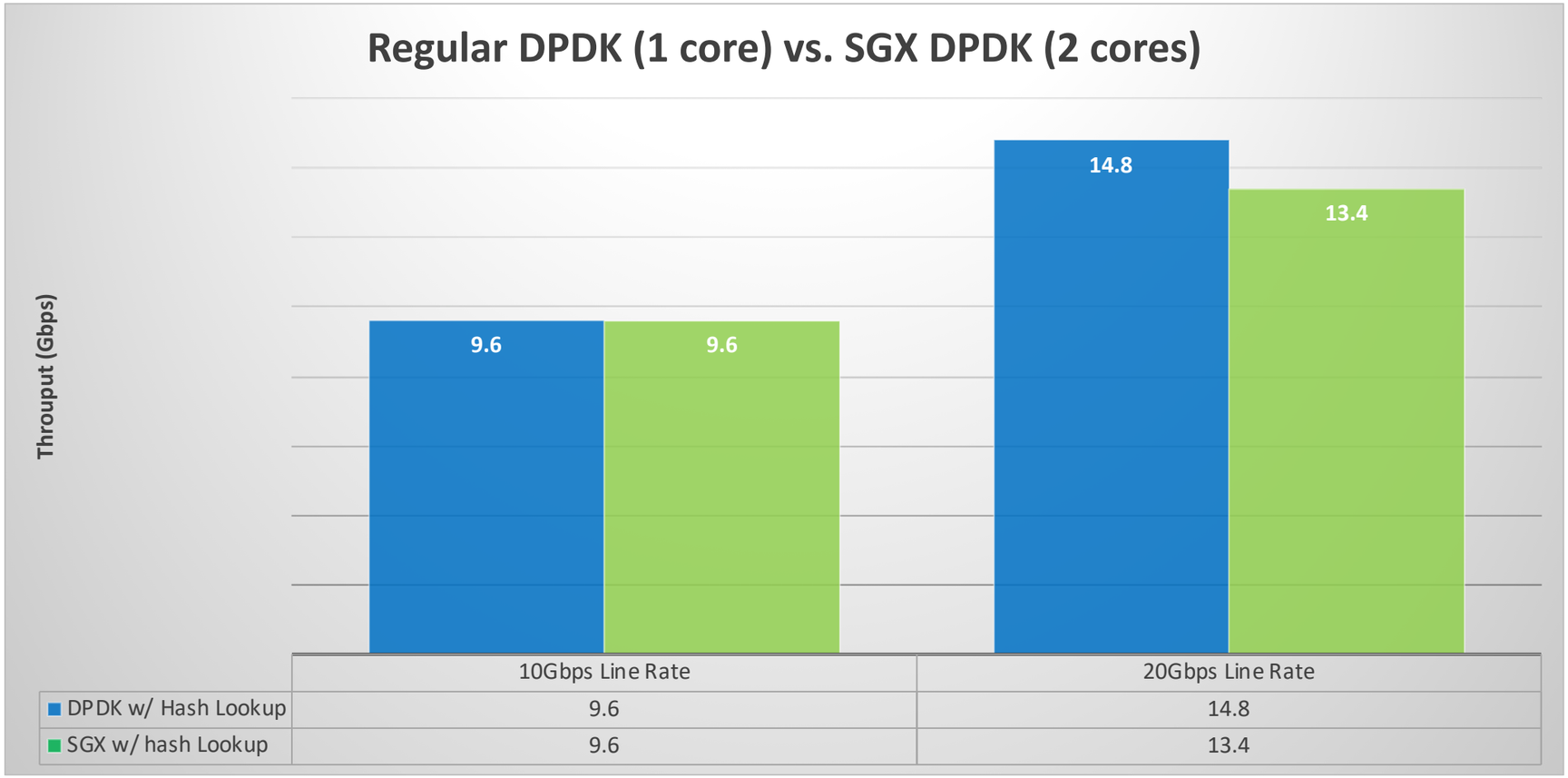


- Requires minimum 1+1 SGX server per dataplane frame of capacity
- n+1 SGX servers required for upto n dataplane frames of capacity

Current prototype performance numbers with hash table lookup

Application : L2FWD
Lookup type : Hash table (1M 5-tuple entries, ~13MB)

* Lab research data. potential Security-Performance Trade-offs

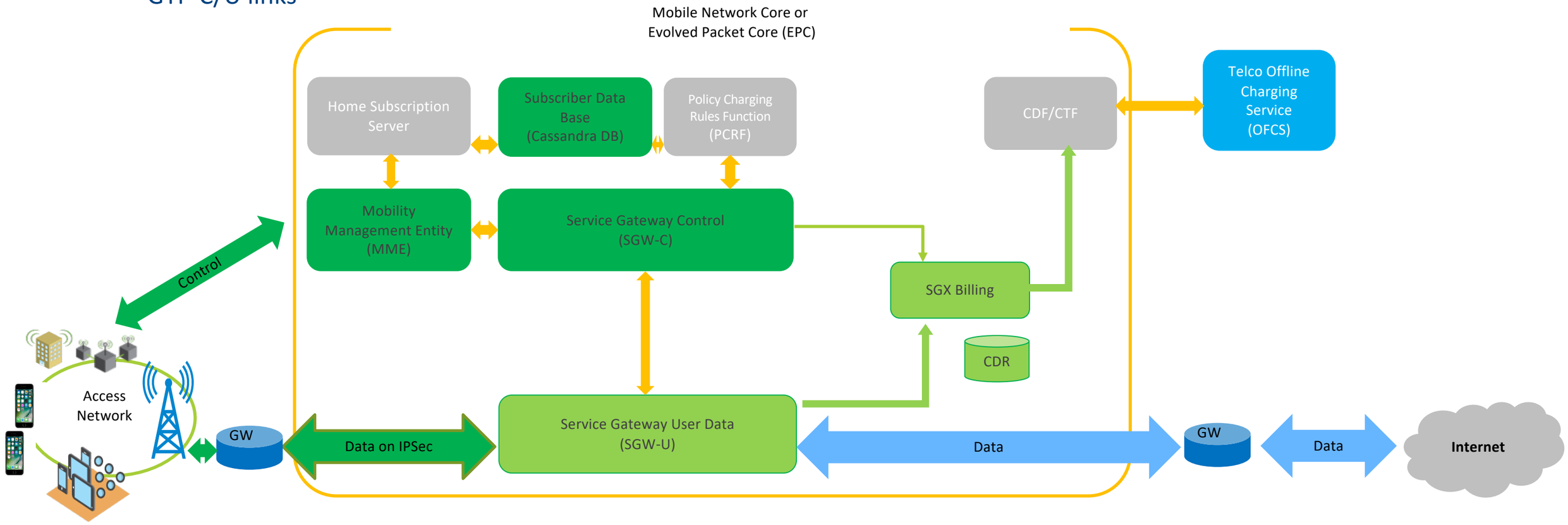


- Additional SGX threads can enhance performance.
- Queuing/de-queuing adds additional overhead (queuing theory)

Future OMEC Mobile Infra Core Control/Data plane – WIP

Protecting

- SPGW-U and SPGW-C
- Subscriber databases
- Transient databases
- MME
- GTP-C/U links



Thank You
Questions ?