NOKIA Bell Labs

Cloud Service Security Management

Manfred Schäfer, Iris Adam

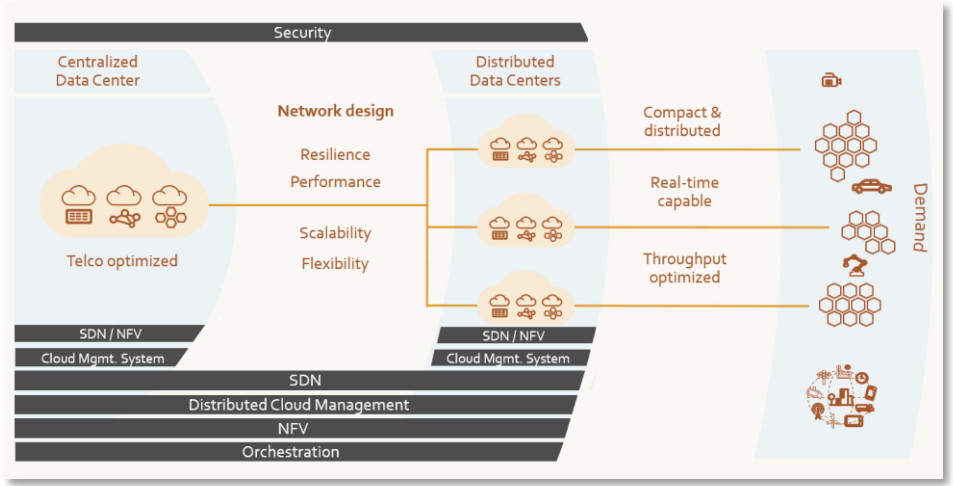
Bell Labs NAACS Security Research Munich

Version 2016-05-12

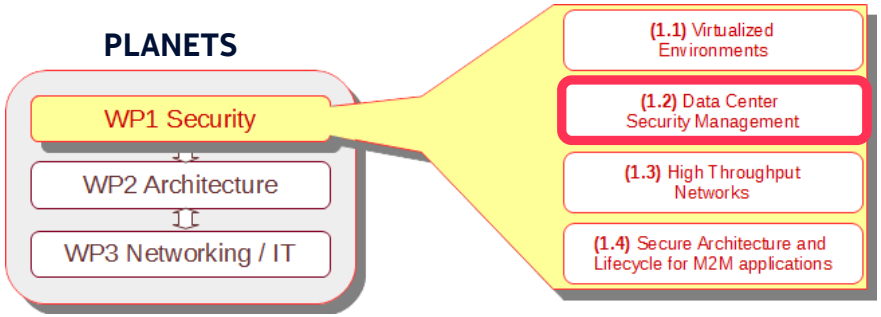
SENDATE- PLANETS*: Overview, Nokia's Security Part

PLANETS: Subproject of Celtic-Plus Project SENDATE, aiming at Techniques & Technologies for huge, Datacenter (DC) clouds in Europe. Specific focus on high flexibility, low latency, locality-awareness and **security**, convergence of Telco networks, IT and distributed DC in scope, e.g., supporting mobile connected objects, IoT, health applications, 5G, utilizing NFV, SDN technology.

March/2016-February/2019, http://www.sendate.eu/about-the-project/; http://www.sendate.eu/sendate-planets/



'Bringing content close to the user, based on optimized, distributed DC architectures … and enhance security'



Data center Security Management (SM), Nokia WP1 tasks

Architecture models for SM based on DDC and network services

Analysis of complex scenarios for the interoperability of distributed clouds / data centers and methods for SM&O

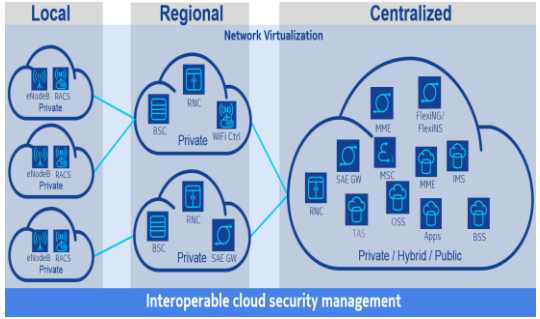
Support integration of methods for 'Information Exchange' into Telco Cloud context (Coop-UNIBW)

*SEcure Networking for a DATa Center Cloud in Europe – ProgrammabLe Architecture for distributed NETwork functions and Security

PLANETS: Initial Vison

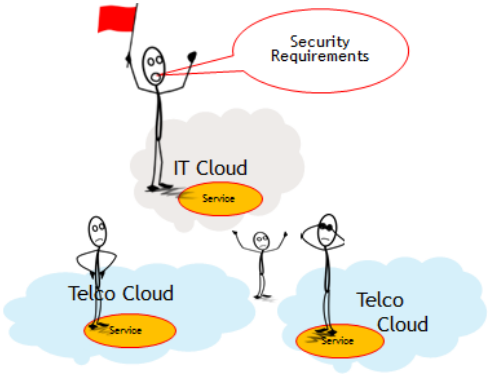
Policy driven Security Management for Distributed Clouds

"SM must be fast & consistent"



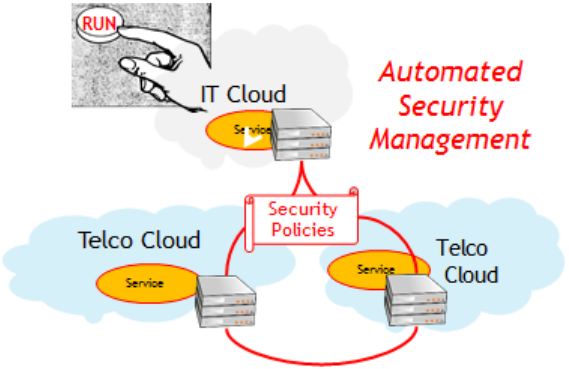
Establishing Services in Distributed Cloud architectures requires adaptive SM

SM has to cope with dynamicity, mobility, and elasticity of heterogeneous cloud and network services.



... but distributed 'SM per Admin' becomes slow, complex, and error prone

SM becomes too difficult and inefficient when triggered and conducted through admins. Interoperable inter/intra cloud security is missing so far.



Dynamic, mediated 'SLA handling & SM/SO' for cloud spanning services

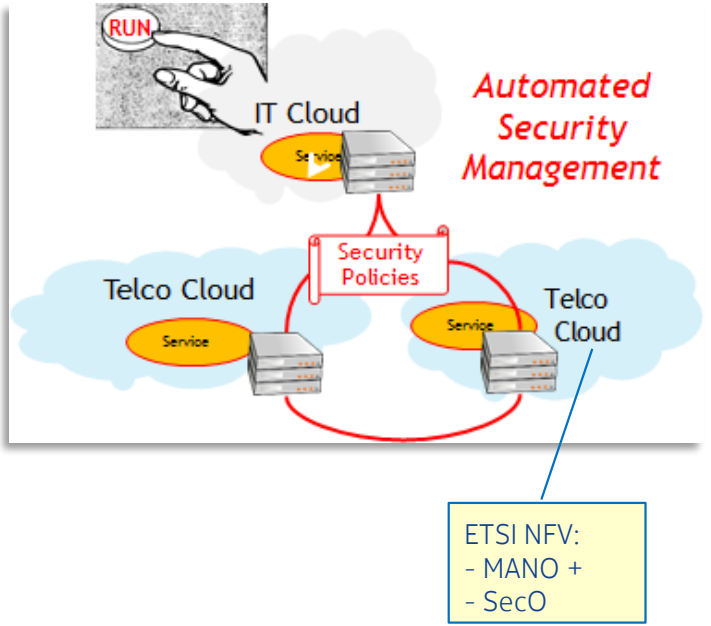
Key success factors are automated security policy management (negotiation, mediation, optimization ...) and event driven policy adaption across domains.

NOKIA Bell Labs

PLANETS: Nokia‘s Security Focus

Focus of Work: Automated Security Management (for distributed services)

- SM follows Service changes & deployment → fast, consistent, adaptive = f(service)
- SM is closed control loop with feedback path → … adaptive = f(security events)
- Major Functional Blocks (FB)
  - FBs for SM (or supporting SM)
  - FBs representing managed entities (VSF/PSF, security zones/domains, SM entities, …)
  - FBs supporting feedback (various monitoring/validation entities)



Essential Building Blocks

- Architectures and concepts for SP* / SLA based SM in multi-provider scenarios
- Interfaces, entities, functions for automated, holistic SM across admin. domains
- Security concepts and selected security functions for distributed services

Current work items

- Methods for (a) Trust Establishment between VNF and SM&O entities and
  (b) Enabling SM across administrative domains
- Analysis of various ‘domains’ in DDC, relation to ‘services’ and impacts for SM&O
- Analysis of RQ for security mechanisms and policies / SLA (in DDC scope)
- COOP: Discussions & alignments with UniBw M, on ‘monitoring’ in distributed datacenter / cloud environments

PLANETS: Security and Domains, Multi-Provider Scenarios

Several types of (administrative) domains to constitute 'distributed services'

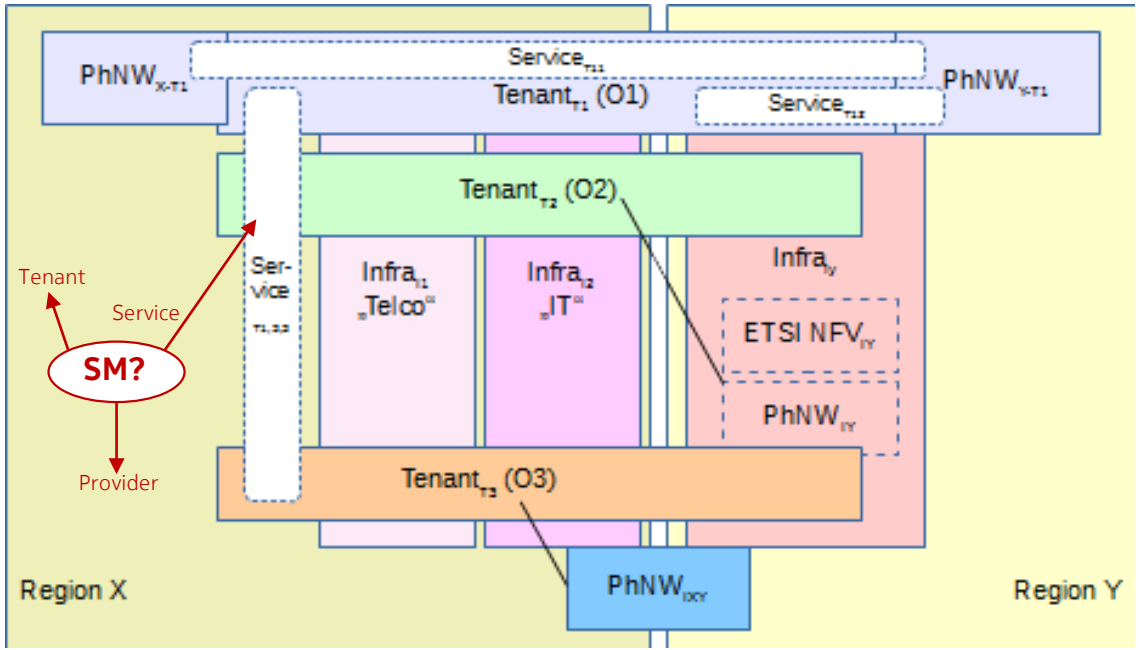
- Cloud / Infrastructure / datacenter (of type ..)
- Tenant domain (..)
- Service domain
  - Within Tenant Domains (..)
  - Across Tenant Domains (..)
  - Across Infrastructure Domains (..)

An Administrative Domain (AD) is a collection of systems and networks operated by a single organization or administrative authority ('provider'). The components within a domain .. inter-operate with a significant degree of mutual trust among them based on a stable trust relationship, while a transient .. trust relationship shall be established for co-operating with components in other domains.

.....

Domains also exist within services

- Security Zones
- Security Domain (Trust Domain)
- Entity Domains
- VNF compositions (set of VNFC)
- ....



How an optimal, 'service centric' SM architecture should look like ?
Which SM requirements apply ?
Which tasks would be required ?

PLANETS: Enabling SM Across Administrative Domains

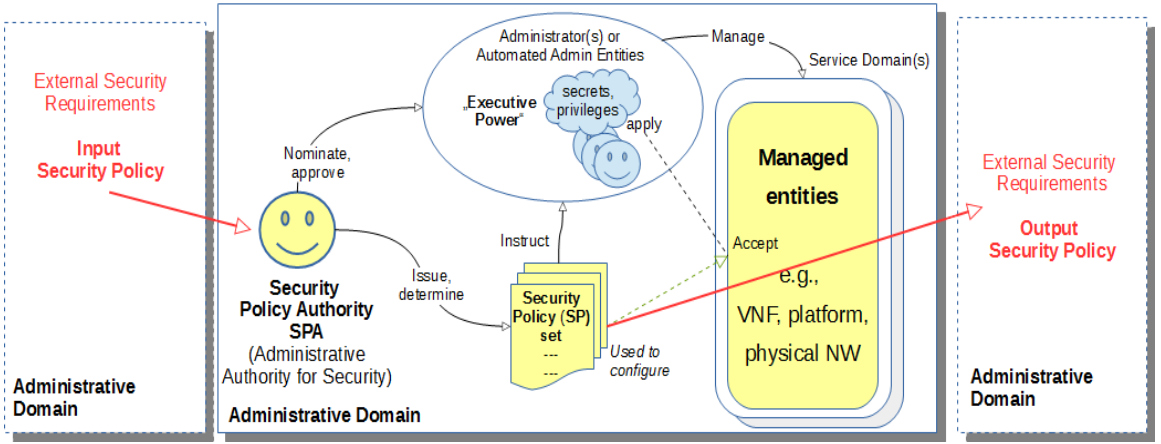
Key challenges of Security Management (SM) <u>across</u> domains and clouds

Model for Policy based SM per distributed Service

- Each domain is governed by one Security Policy Authority SPA, issuing/enforcing (only) domain specific Security Policies SP
- External SP are never directly enforceable!
- Relations to other domains need SP related coordination and agreements!

Many influencing factors

- Heterogeneous Administrative Domains
- Various Clouds types (IT and Telco)
- Different stakeholder requirements and concerns (tenants/providers)
- Various service/business/deployment models
- Various country/geographical regulation or law
- Wide variety of Platform Technology



Core requirements (Service centric view)

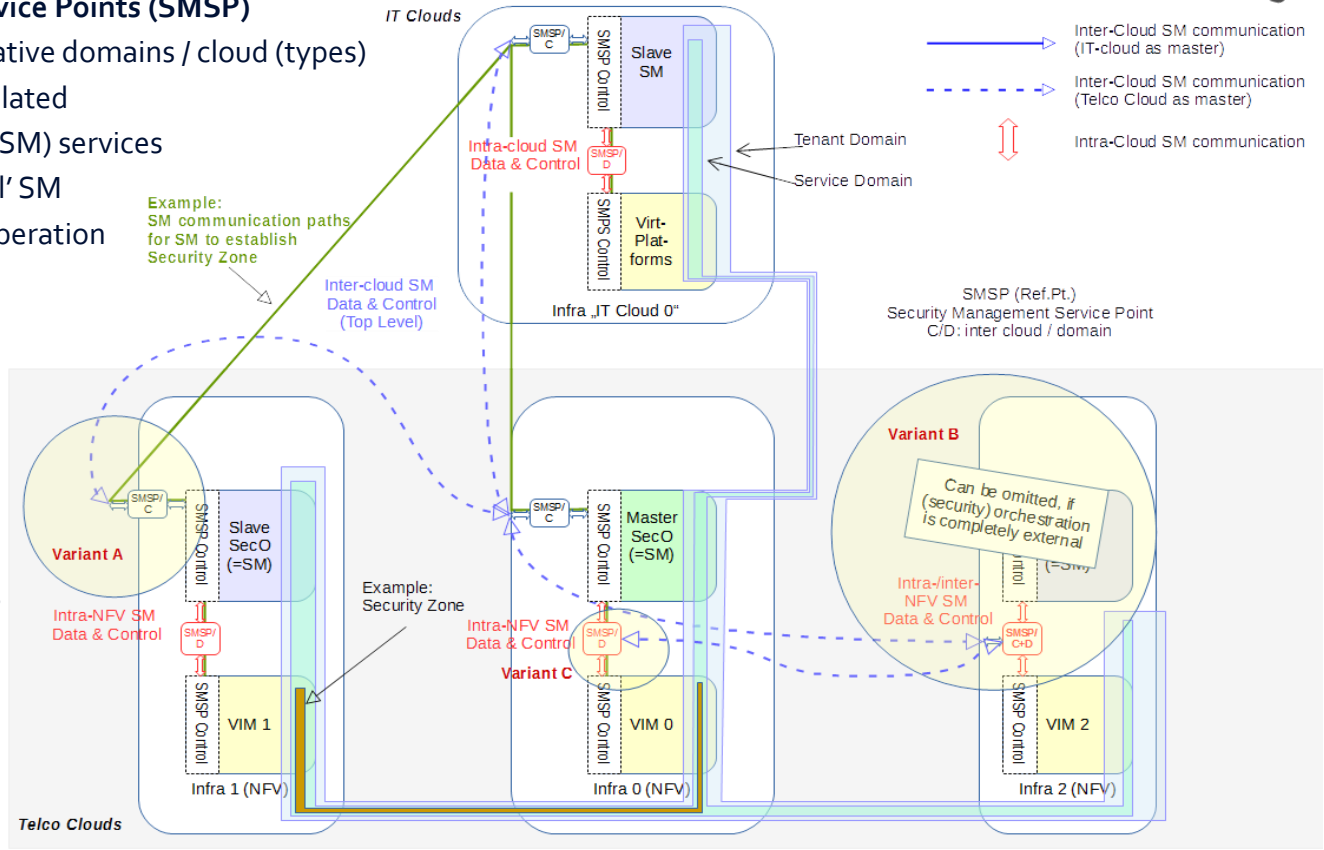
- Consistent cloud/domain spanning automation and rapid adaptiveness of (centralized) SM functions for 'mixed' services, based on agreed SLA/SP
- SP agreements trade-offs: 'granted security capabilities' vs. 'expectations on strength of security' vs. 'other RQ'

(like for NW management)

PLANETS: Enabling SM Across Administrative Domains

Proposal: Security Management Service Points (SMSP)

- New ref. points between administrative domains / cloud (types)
- Coordination & mediation of SM related capabilities, requests, constraints, (SM) services
- Allow coupling of 'global' with 'local' SM supporting design/deployment & operation
- SMSP connect SM entities in hierarchical manner
- SMSP may delegate tasks to SMSP of a lower hierarchy level
  - Cloud SM / Cloud SM (variant A)
  - Cloud SM / Infra SM (variant B)
  - Infra SM / Infra SM (variant C)?
- SMSP interact in master/slave roles
- Top layer master role (root) may correspond to 'root SPA' of a business model, anchored either
  - in IT cloud
  - or in Telco Cloud



PLANETS: SMSP architecture and functionality

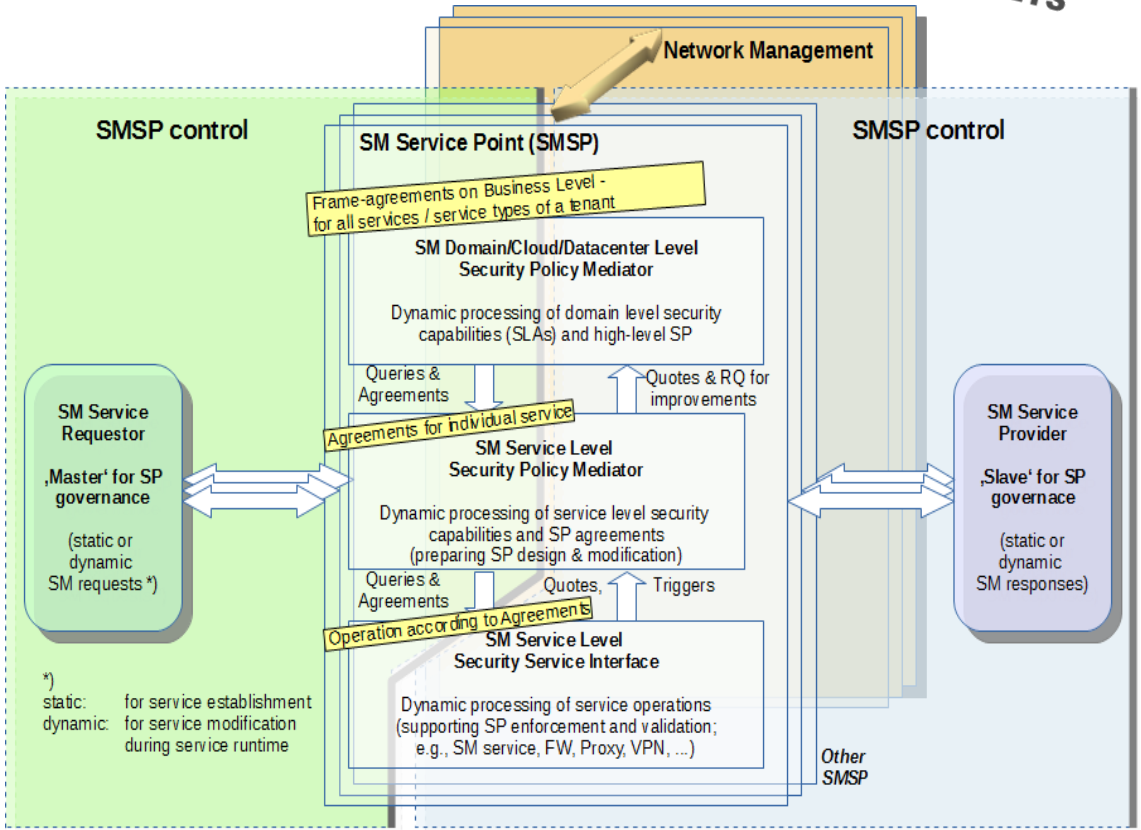
Each SMSP is shaped as internally connected
3-Tier approach to support automation of SM tasks

- statically (preparative) or
- dynamically (at service run-time)
  enabling monitoring & modifications, e.g.,
  - top down (service driven) as well as
  - bottom up (event driven)

Layers

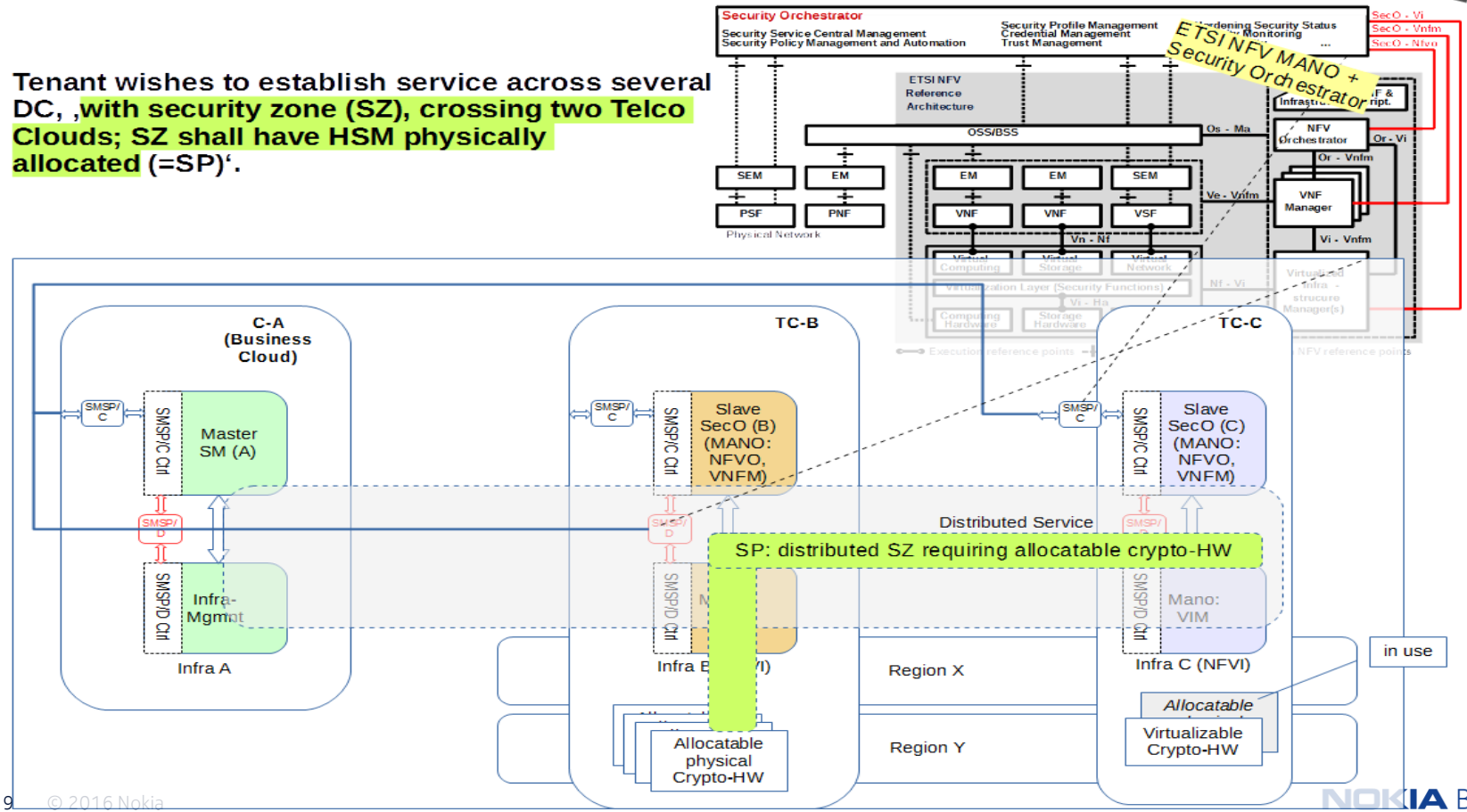
- Domain/Cloud level
  - to negotiate Security SLAs and high-level SPs for all services (e.g., of a tenant)
- Service level
  - to agree SPs per service
  - to enable authorized SM cooperation of 'SM services' across involved domains for each individual service (SM Cooperation may be based on 'API' or on SP level)
- Coordination with NW management (priority driven)

Technically SMSP are controlled by SMSP functions implemented either by service provider (server/slave) or by consumer (client/master)



PLANETS: SMSP Top Level Workflow, Example

Tenant wishes to establish service across several DC, ,with security zone (SZ), crossing two Telco Clouds; SZ shall have HSM physically allocated (=SP)'.



PLANETS: SMSP Top Level Workflow, Example

The basic request: SZ, access on HW security components

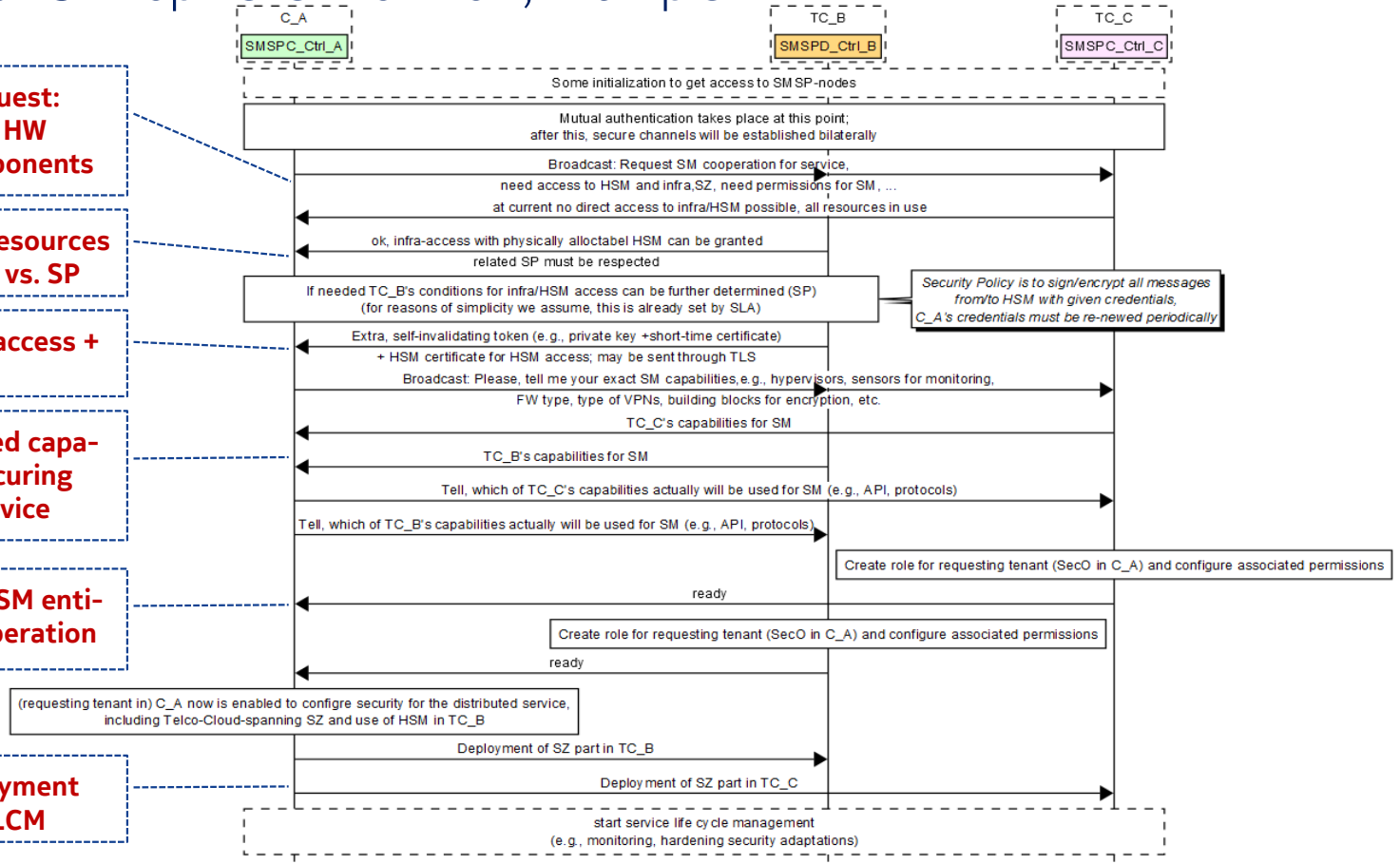
Check (sec.) resources & capabilities vs. SP

Agree SP for access + credentials

Clarify detailed capabilities for securing and SM of service

Conditioning SM entities for SM operation

Service deployment and security LCM



PLANETS: Outlook

Summarizing

- SMSP, to enable SM across domain/cloud boundaries (SM4DDC), relying on individual SM entities
- Coordinate and mediate SP and SM tasks between administrative domains

Next (based on SMSP)

- SM Architecture, functions and workflows to be refined applying use cases (from IoT/5G/SDN/NFV…SENDATE)
    - Align with FBs (from PLANET partners) into 'global' SM, while not excluding local SM
    - Align with PLANETS 'NW architecture' architecture
- Specific use cases for service security life cycle managements (under development), including
    - Unique certified life-time identifiers for VNF/C instances, with certified history
    - Protection of private keys in and for VNF/C instances
    - Trust & key management (Integrity, key distribution and PKI integration)
    - SP (controlled/targeted) adaptation as reaction of business changes / security events
- Developing SLA / Security Policy Framework