STRATEGY ANALYTICS
Celebrating 25 Years of Insights

5G Signaling and Control Plane Traffic Depends on Service Communications Proxy (SCP)

15 December 2021

Snapshot

Network Signaling is about to change dramatically as 5G Standalone (SA) is deployed at scale in late 2021 and 2022.
In 5G, network signaling is no longer a separate network like SS7 or Diameter. Signaling shares the Control Plane with all other Inter-Process Communications using HTTPS/HTTP/2 protocols.
In 3GPP Release 16 the Service Communication Proxy (SCP) becomes the routing control point that mediates all signaling and Control Plane messages in the network core. SCP plays a critical role in optimizing routing of NF discovery requests to the Network Repository Function (NRF) and in overall load balancing, traffic prioritization and message management.
Communications Service Providers (CSPs) need to plan for at least two orders of magnitude increase in signaling traffic with 5G SA. And SCP can improve Control Plane efficiency by 30%. CSPs are just beginning to appreciate the key role SCP plays in enabling dynamic routing and management of millions of simultaneous Control Plane message flows and signaling transactions to assure service performance and profitability.

Contents

I. *Network Signaling Overview – 5G Changes Everything*

Network Signaling is about to change dramatically as 5G Standalone (SA) is deployed at scale. In 3GPP Release 16, 5G SA signaling no longer has separate Diameter and SS7 signaling transport networks.

In 5G, network signaling shares the Control Plane with all other event triggered transactions and inter-function communications using standard HTTPS/HTTP/2 - and eventually HTTP/3 – protocols. Signaling traffic also increases dramatically in the new flat 'any to any' Service Based Architecture (SBA). Alongside many other transactions, the Control Plane must now handle all Network Function (NF) *discovery requests and responses* from the *Network Repository Function (NRF)* as well as all the Domain Name Server (DNS) IP address lookups to locate every active instance for every available NF in real time.

Previously in legacy SS7 networks the ***Signal Transfer Point (STP)*** was the node that routed signaling messages. In 4G networks, Diameter signaling was controlled by the ***Diameter Routing Agent (DRA)*** and ***Diameter Relay Agents*** that performed routing and load management for Diameter signaling traffic.

In the ***3GPP Release 15*** version of 5G signaling *NFs simply sent direct discovery requests to the NRF*. An approach that operates satisfactorily for trials and small network deployments.

In **3GPP Release 16** the ***Service Communication Proxy (SCP)*** has now been introduced to allow the Control Plane network to handle and prioritize massive numbers of requests in real time. ***5G SCP becomes the control point that mediates all signaling and Control Plane messages in the network core.*** SCP routing directs the flow of millions of simultaneous 5G function requests and responses for network slicing, microservice instantiation or edge compute access. It also plays a critical role in optimizing floods of discovery requests to the NRF and in overall Control Plane load balancing, traffic prioritization and message management.

5G SA needs to handle the massively increased signaling transactions volume that 5G generates on the Control Plane. A volume that is now projected to be at least two orders of magnitude greater than operators have experienced with Diameter. 5G signaling must also simultaneously facilitate real time interworking with legacy SS7 and Diameter to ensure seamless 4G, 3G and 2G service interoperability.

Communications Service Providers (CSPs) are just beginning to appreciate the *key role of the SCP in enabling dynamic scaling and management of millions of simultaneous service flows and the interactions between 5G SA NFs* that could determine the performance and profitability of 5G networks.

This white paper describes the requirements of 5G signaling, some of the key drivers for SCP deployment, the choice of 3GPP Model D for 'Indirect' NRF communications and the benefits of SCP adoption. It also summarizes the signaling strengths of four leading vendors – Ericsson, Huawei, Nokia and Oracle.

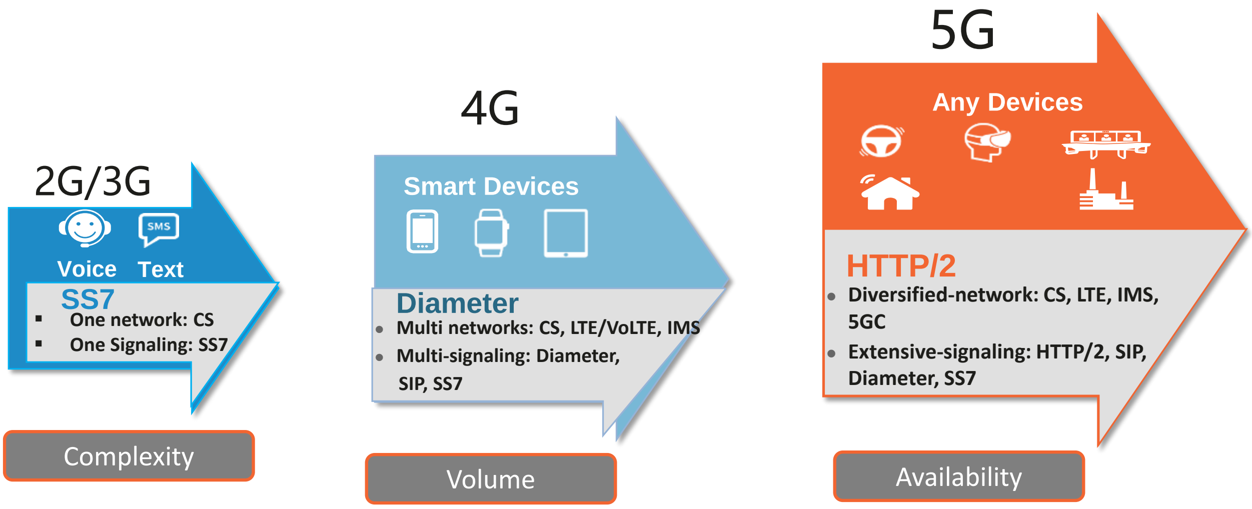
II. 5G Signaling and 3GPP Release 16

The nature of signaling has changed significantly as networks have evolved.

Evolution of Signaling

As the chart below shows 2G and 3G were *voice and text centric* networks with subscriber User Entities (UEs) based on SS7 signaling. In these networks *service availability* was the priority. In 4G, networks became *data and media centric* and needed signaling to support smartphones and Apps. *Signaling volume* grew to support these Apps. Now under 5G the network must support not only all these earlier services but many new high bandwidth, low latency *applications and massive machine to machine communications* as well as handling *complex interworking* across multiple domains. Today handling *network complexity* as well as massively increased *signaling volume* is the operators' priority.

Chart 1 Signaling Evolution Adapts to Business Transition

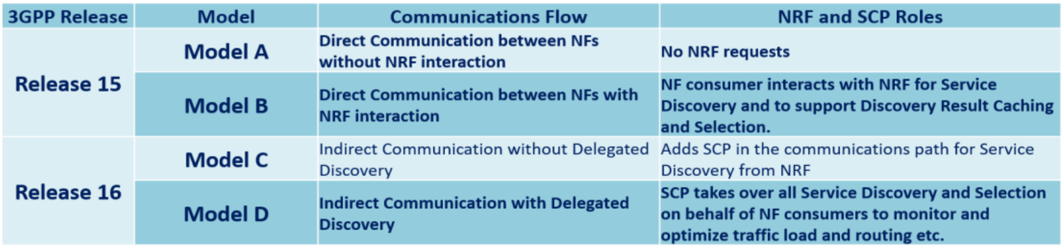

2G/3G
SMS
Voice Text
SS7
One network: CS
One Signaling: SS7
Complexity
4G
Smart Devices
Diameter
Multi networks: CS, LTE/VoLTE, IMS
Multi-signaling: Diameter, SIP, SS7
Volume
5G
Any Devices
HTTP/2
Diversified-network: CS, LTE, IMS, 5GC
Extensive-signaling: HTTP/2, SIP, Diameter, SS7
Availability

In 2021 and 2022 as new 5G SBA services become fully commercial with 3GPP Release 16, we expect signaling and associated Control Plane traffic volumes over using HTTPS or HTTP/2 to escalate exponentially as 5G network signaling shares the Control Plane with all the 'any to any' communications between NFs or App. Functions (AFs).

Critical Role of Network Repository Function (NRF) in 5G Signaling

In 5G, *NRF allows NFs to discover the active NF instances they need to create and deliver services* in the 5G Core. Originally 3GPP proposed alternate models for NRF communications flows as shown below.

Chart 2 Options for Signaling Communications Models in 3GPP Rel. 15 and 16



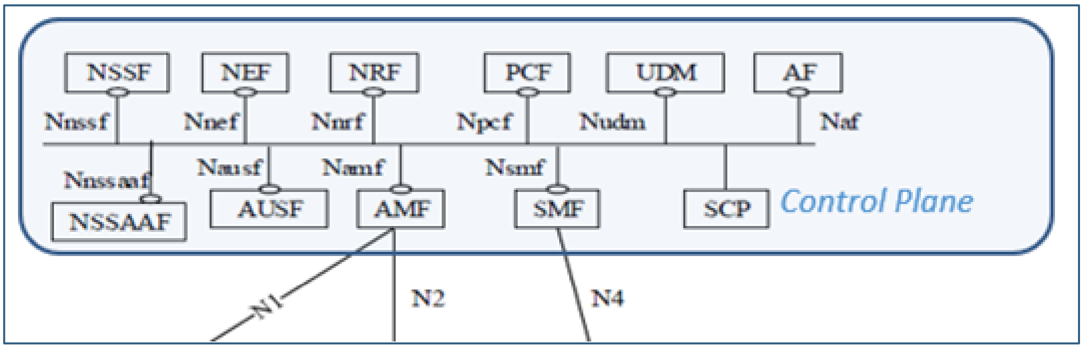
3GPP Release	Model	Communications Flow	NRF and SCP Roles
Release 15	Model A	Direct Communication between NFs without NRF interaction	No NRF requests
	Model B	Direct Communication between NFs with NRF interaction	NF consumer interacts with NRF for Service Discovery and to support Discovery Result Caching and Selection.
Release 16	Model C	Indirect Communication without Delegated Discovery	Adds SCP in the communications path for Service Discovery from NRF
	Model D	Indirect Communication with Delegated Discovery	SCP takes over all Service Discovery and Selection on behalf of NF consumers to monitor and optimize traffic load and routing etc.

Source: 3GPP and Strategy Analytics

Although the chart above shows four models for communications flows only *Model B* and *Model D* have been widely used. In 3GPP Release 15 *Model B* allowed NFs to communicate directly with NRF for *Service Discovery* and over the Control Plane to one another in a ‘flat network architecture’. Model B has typically been used by operators for early 5G trials and small networks.

In Release 16 however, 3GPP introduced *Models C and D* for larger scale production networks with indirect NRF communications via a new network function - the **Service Communications Proxy (SCP)** as shown in the chart below.

Chart 3 3GPP Introduces SCP as a new Control Plane functional element



Source: ETSI TS 123 501 V16.9.0 – 5G System architecture for the 5G System – July 2021

The chart looks familiar – but a new function has been added - the **Service Communications Proxy (SCP).** The chart also shows the standard Control Plane functions - the *Network Slice Selection Function* (NSSF), the *Network Exposure Function (NEF)*, and importantly *the Network Repository Function (NRF)* and so on. As noted above, in 5G the NRF allows discovery of the active instances of all Network Functions (NFs) in real time. It maintains a record of the services each NF can provide and of the current active NF instances. *NRF is critical to allow active NFs to discover one another and their service capabilities* – as allowed by Network Exposure Function (NEF). NRF also *allows NFs to discover other providers’ NF instances* for interworking across multiple domains in 5G Core Network.

Control Plane is shared by multiple traffic types with diverse priorities

As the chart indicates 5G Control Plane is essentially a virtual *‘network bus’*. There are multiple network (NFs) and service functions (SFs) and even 3rd. party user application functions (AFs) that send requests and responses across the *‘bus’*. A single ‘*logical bus’* is therefore handling all the Control Plane transactions for the 5G network. And unlike earlier networks, 5G network signaling network is now sharing that *‘common bus’* with all the other traffic. And all those transactions are running over unprioritized HTTPS/HTTP/2 packet streams.

Potential Bottleneck for requests to NRF

Since every NF has to talk to the NRF in real time, and since transactions requests and responses volumes may escalate rapidly, the NRF could potentially become a ‘bottleneck’ for Control Plane traffic. Similarly, occasional ‘floods’ of requests from non-signaling related ‘consumer’ NFs to ‘producer’ NFs, or between other NFs and AFs may generate traffic ‘bursts’ that conflict with high priority signaling NRF discovery requests.

Centralized Routing is Required.

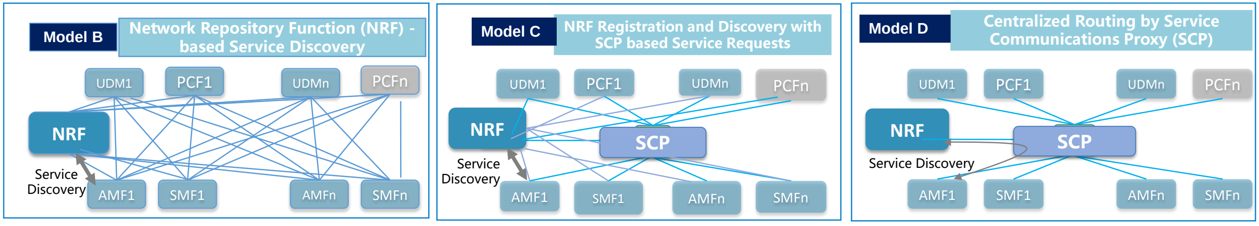
So a mechanism is needed to optimize routing priorities – as dictated by policy rules - and to minimize congestion. To play that role 3GPP specified Model D in Release 16 and defined the SCP to act as a 'Traffic Cop' that can provide routing, redirection, load management and traffic optimization.

Alternative 5G Signaling Network Models

So what issues and benefits do the different models bring?

The charts below highlight the issues that Model B with '*Direct NRF communication'* and Model C with 'indirect communication without delegated discovery' each create; and the solution that Model D brings with '*indirect communications and centralized routing*' i.e. simplicity, traffic management and cross-domain performance.

Chart 4 Importance of Logically Centralized Routing in Multi-Domain/Large Scale 5G systems



Source: Webinar 'Signaling - The Critical Nerve Center of 5G Networks' October 2021

Model B - the left hand chart above - indicates the potential for exponential growth of requests for NRF service discovery that is likely to occur in a multi-domain 5G environment with multiple entities for user data management (UDM), policy control (PCF), access and mobility (AMF) functions etc. This 'direct' communications flow to the NRF can lead to serious network issues and as a result:

- Consumer NFs may not get signalling in real time
- Load-balancing Policy for NFs may vary
- Load between different producer NFs is unbalanced

Model C – middle chart above - which is still under consideration by a few operators, offers a hybrid approach, that allows NFs to communicate directly with NRF for profile registration and discovery, while also connecting via the SCP for service requests. This model, however, results in a massive number message flows like Model B - and significant additional discovery and notification traffic.

By introducing Model D and the centralized routing via the SCP for all traffic i.e. 'indirect' flow - as shown in the right hand chart above- these issues are minimized, and network operations perform far better. Specifically operators will see benefits from Model D as a result of:

- Centralized routing by SCP
- Unified Load Balancing
- Real time delivery of NF and AF requests and responses.
- Optimized capacity in cases of 'bursty' Control Plane traffic

The addition of the ***Service Communications Proxy (SCP)*** therefore ensures that NRF discovery requests and 'lookups' do not become a choke point that slows down all 5G Control Plane transactions.

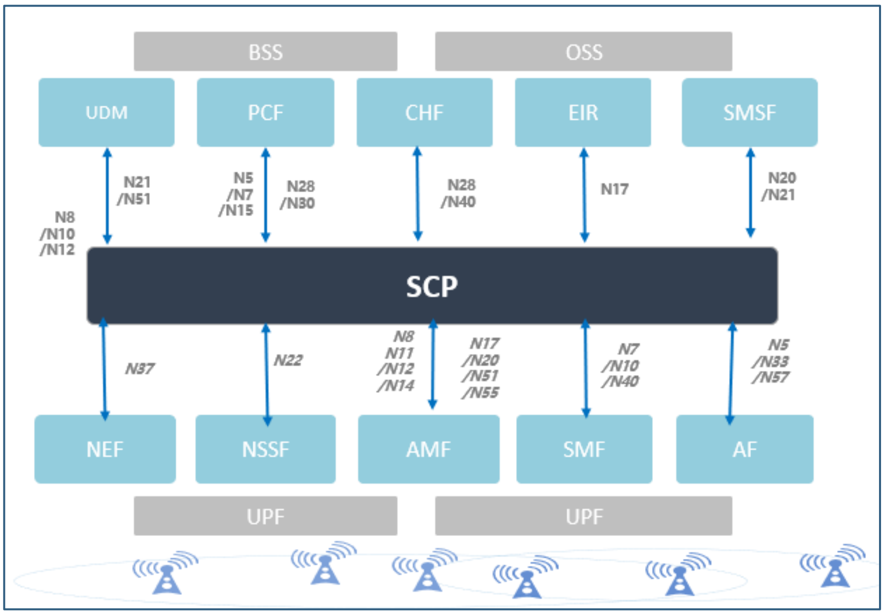
Nor will priority signaling be slowed by floods of AF or low priority NF requests.

The indirect routing approach of Model D allows massive scalability and delivery assurance for high performance commercial 5G Deployments.

Benefits of SCP Routing, Load Optimization and Delivery Assurance

It is important to look at how SCP routing and traffic optimization enhances performance.

Chart 5 SCP Simplifies Routing and Management on the Control Plane



As the chart above shows, the SCP acts as the routing intermediary that manages the requests and responses between all the Network Functions (NF) in the 5G core. The interface references are also listed for each NF.

Even though the Network Exposure Function (NEF) and the Policy Control Function (PCF) in 5G limit which NFs can communicate with one another, there are a *very large number of possible interactions if every NF can talk directly to every other authorized NF*.

However, if every function only communicates through the SCP as shown above, there are *only 10 dynamically shared, communications paths to be allocated and managed.* Diverse message types can share a common path to the same NF or the NRF, with policy controlled prioritization. The SCP dramatically simplifies flow management and aggregates traffic efficiently in a highly distributed cloud native environment, *regardless of whether NF microservice instances are in the same container or at a remote location.*

Therefore a logically centralized SCP in conjunction with policy rules that specify access priority, can pre-empt contention and route all Control Plane traffic loads efficiently and at scale.

Note: The centralized routing role of the SCP compares to that of the ***4G Diameter Routing Agent (DRA)*** and even earlier the ***Centralized SS7 Routing*** offered by several vendors.

III. SCP Plays Key Role in 5G Standalone (SA) Services

When 5G was first launched with Release 15 SCP had not yet been specified by 3GPP. As a result several early 5G SA networks have had to expend significant investment to retrofit their signaling network as they became heavily loaded. There is now evidence that this delayed implementation of the SCP cost up to 3 times more than if the SCP had been deployed initially. Operators who are deploying 5G Standalone (SA) with 3GPP Release 16 today can avoid that cost by implementing the SCP on Day Zero as they deploy the network. More importantly the SCP will save CSPs significant money by addressing many of the challenges that 5G SA presents. We discuss below how the SCP addresses four major challenges.

SCP Helps address Major Challenges for 5G Standalone (SA) services.

Beyond the optimization of Traffic Routing on the Control Plane, the SCP helps to address several critical challenges that operators will encounter as they deploy 5G SA services. Specifically SCP can help to operators deliver:

1. ***Massive Scalability of Signaling Transactions due to:***
   - Transactions Volume
   - Signaling storms
2. ***Multi-Generation Network Service Support for:***
   - 2G,3G, 4G and IP services, since SS7 and Diameter will survive for many years
   - Seamless Delivery of Converged 4G and 5G Services
3. ***End to End Service Delivery across Multiple-Domains:***
   - Multi-Carrier Domain Networking
   - Intercarrier Signaling across Multiple Carrier Domains
4. ***Security for Signaling Network***
   - Roaming Signaling Attacks
   - Edge Security

Below we describe how SCP can contribute in each area and *bring key benefits to each.*

1. *Massive Scalability for Signaling Transactions*

The first area where SCP makes a major contribution to 5G SA services is scalability.

5G SA Traffic Load on Control Plane will be very High and potentially very 'Bursty' comparable to 'Signaling Storms'.

As described above, the 'flat' 5G Service Based Architecture inherently creates more transactions volume. In a **recent report** from Strategy Analytics based on early US experience, we noted that "3GPP's adoption of HTTPS and HTTP/2 …. introduces new….text-based protocols, that …trigger performance concerns …because transaction volumes on the 5G Control Plane may be (at least).. 10x and 20x today's Diameter signaling volume." These estimates now appear to be far too low based on what operators are seeing in China's more mature large 5G SA deployments.

Some Chinese operators are experiencing as much as 100x or even more transactions volume on the 5G Control Plane compared to 4G Diameter signaling. Operators need to plan for at least ***two orders of magnitude increase in signaling traffic*** with 5G SA architecture.

SCP plays a critical role in scaling this increased throughput with traffic aggregation and optimized routing to the NRF and intelligent policy based traffic prioritization across the entire Control Plane.

Signaling Storms in 5G SA will impact the Control Plane

Recently a 4G operator in East Asia had a massive failure as a result of network database upgrade and the triggered a *massive signaling storm that led to a 12 hour voice and data service outage.* Even in 5G SA where the failed upgrade could be rolled back systematically with an automated 'Canary' process, and where many live session states are stored and recovered from the Unstructured Data Storage Function (UDSF), the *recovery traffic storm* would likely create an *internal operator Control Plane storm* as massive numbers of NRF discovery requests are made and vast numbers of active instance lookups triggered simultaneously.

SCP therefore plays a critical role here too - to minimize the impact of the Control Plane 'transactions signaling storm'

2. *Multi-Generation Network Service Support*

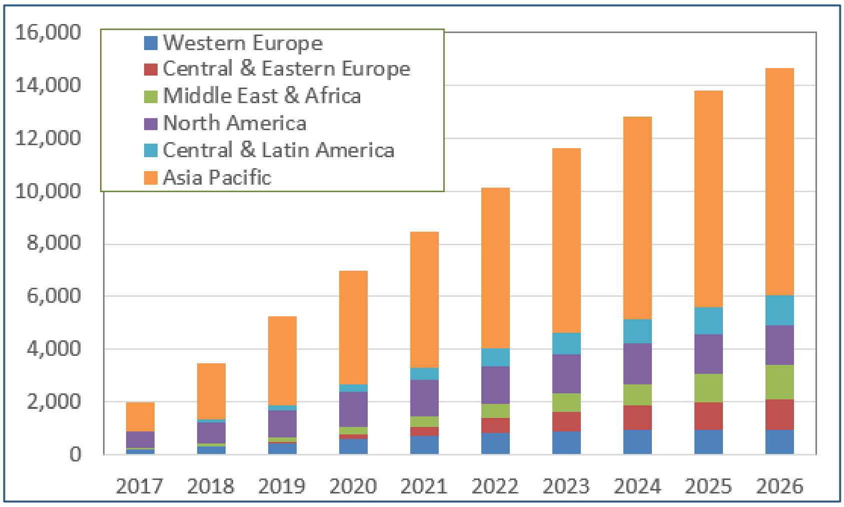
The second area where SCP becomes a major enabler is for multi-generation network interoperability and migration to 5G.

2G,3G, 4G and IP services – SS7 and Diameter will survive for many years

Even as 5G subscribers grow dramatically, many other subscribers continue to operate with earlier generations of network infrastructure. Older subscribers may continue to use legacy 3G phones despite the imminent 3G capacity cutbacks, as the 3G spectrum is refarmed for 5G. Even 2G networks will continue to support several low end or IoT markets for many years. Both 2G and 3G will ***require operators to maintain interworking with the SS7 signaling network for those subscribers.***
Despite the availability of 5G, 4G continues to add new subscribers that require ***Diameter signaling***. On a global basis, through at least 2026, there will still be more 4G than 5G subscribers.

In parallel as the chart below indicates operators are seeing dramatic growth in the need for *interoperability of Voice over IP (VoIP), Voice over LTE (VoLTE), Voice over Wi Fi* to complete voice and video calls - both to terminate IP sessions to 4G/5G NSA networks or to connect to 5G SA. Interoperability with both voice and interactive video over IP as well as voice over Wi Fi will drive ongoing demand for Diameter signaling. As the chart shows billions of calls will continue to originate or terminate with ***Diameter signaling*** for many years.

Chart 6 VoIMS, VoLTE, VoWiFi will continue to Require Diameter Signaling. [Billions of Voice Calls]



Source: Strategy Analytics, Service Provider Strategies

SCP - in conjunction with the Signaling Gateway - can facilitate service interoperabiliy between these networks and ensure low latency call and service completion with appropriate charging and billing.

Seamless Delivery of Converged 4G and 5G Services

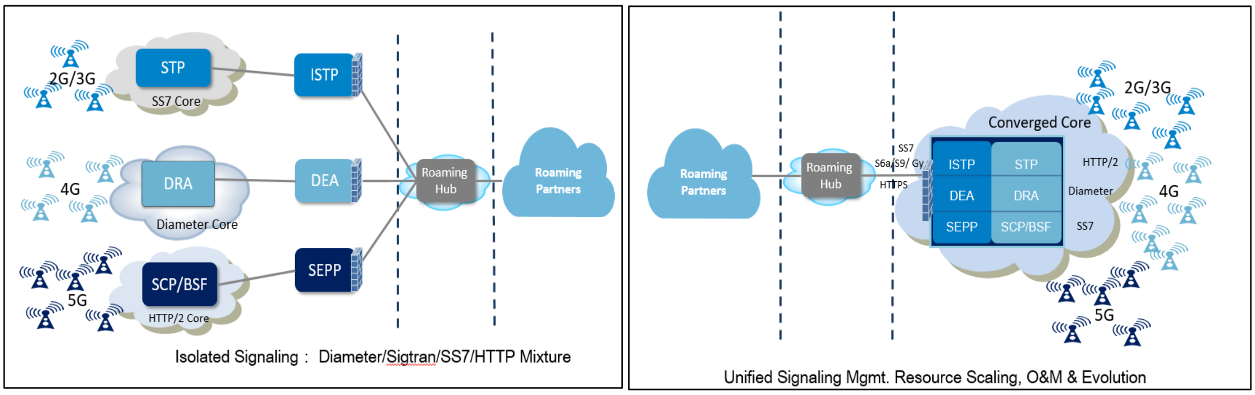
Going forward the SCP therefore becomes *part of a complete Converged Signalling Solution for SS7, Diameter and 5G signaling* that leads to high quality hybrid service continuity and an overall lower cost of operations.

Cost reductions occur as the architecture is fully integrated as shown in the chart below.

The next stage is to evolve from interoperability to a truly converged signaling network.

As the chart below shows on the left, if operators continue to maintain the old SS7 networks and the STPs, as well as Diameter signaling with the Diameter Routing Agents and all the Diameter components alongside the new 5G SCP and support functions, operations get very complicated. Instead as the chart on right indicates it is important to move towards a *converged core model with a converged signaling solution for all types of signaling* that is much simpler and less costly to operate.

Chart 7 Isolated Signaling Network vs. Converged Signaling Network



Source: Webinar '[Signaling - The Critical Nerve Center of 5G Networks]' October 2021

As operators deal with the migration of their networks from 3G and 4G, the converged 5G signaling network can play a key role in making that evolution seamless. A unified signaling solution allows them to leverage dynamic resource allocation across all networks and to assure seamless service for both legacy and 5G end users. So to summarize:

- ***2G, 3G, 4G and 5G will coexist*** over a long period but are already creating serious *End of Life* issues
- ***Converged Signalling*** reduces costs of these hybrid network operations
- ***Interoperability*** and ***Dynamic Resource allocation*** for 2G, 3G, 4G and 5G are needed to protect legacy service revenues and assure return on investment

SCP can play a critical role in facilitating continuous operation of non-5G - 2G, 3G, 4G and VoIP services etc. - as operators migrate to a 5G SA environment and must deliver seamless interoperability.

3. *End to End Service Delivery across Multiple-Domains*

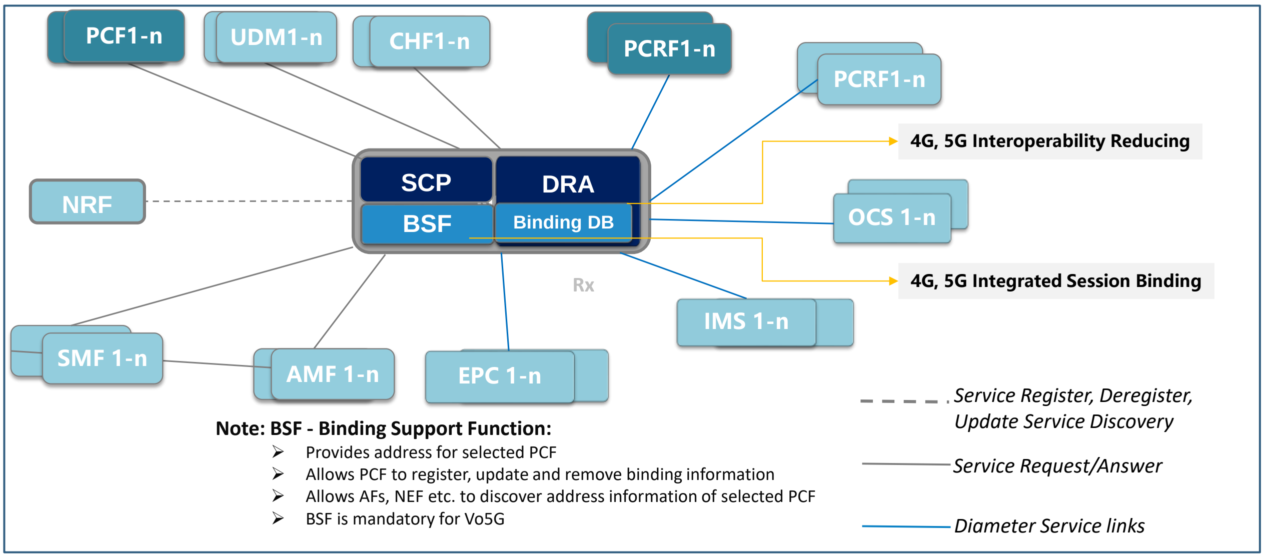
The third area where SCP makes a major contribution to 5G SA service handling is in *operations that must cross multiple domains – wired and wireless, public and private* etc. 5G SA must deal not only with legacy earlier generation networks but also with these diverse Carrier and non-Carrier Network Domains and Signaling systems.

Multi-Carrier Domain Networking

The chart below shows how the SCP works with the Binding Support Function (BSF) and integrates with the Diameter Routing Agent (DRA) and its binding database (DB) to deliver seamless multi-domain services. Note: In the chart functions that operate in ***multiple separate network domains*** are indicated with *1-n* as in the following table.

Function	4G Network	5G Network
Policy Control (Rules)Function	PCRF 1-n	PCF 1-n
(Online) Charging Function	OCS 1-n	CHF 1-n

Chart 8 Multi-Domain Handling with Multi-Domain Policy Control Functions



Note: BSF - Binding Support Function:

- Provides address for selected PCF
- Allows PCF to register, update and remove binding information
- Allows AFs, NEF etc. to discover address information of selected PCF
- BSF is mandatory for Vo5G

*Source: Webinar '**Signaling - The Critical Nerve Center of 5G Networks**' October 2021*

5G as a standard is always specified to be interoperable with 4G. The chart above shows how the SCP can be configured with the DRA - shown in the center. SCP and DRA each continue to manage their own policy domains but operators are now able to complete calls and sessions seamlessly across both 4G and 5G policy domains and function domains within them. With a converged signaling solution, the SCP and the DRA can co-ordinate those policy controls with the appropriate priority for policies in each domain.

One key component shown in the chart above is the Binding Support Function (BSF) that makes sure the networks together deliver End to End (E2E) voice and other services across 4G and 5G. SCP can assure that this happens seamlessly with a common Network Repository Function providing all the 5G discovery information across multiple domains. To summarize - the SCP/BSF and the DRA/Binding DB are essential for multi-domain handling of 4G/5G services with Diverse UDMs, PCFs/PCRFs, CHFs/OCSs etc. They each interface to Policy Rules in their respective domains but together they simplify converged 4G, 5G service operations

Intercarrier Signaling – Multiple Carrier Domains

Similar challenges arise when the diverse domains are operated by different 5G CSPs each with their own UDMs, PCFs, CHFs etc. The Roaming Hub – as shown earlier in Chart 7 – must be accessible to multiple operator domains.

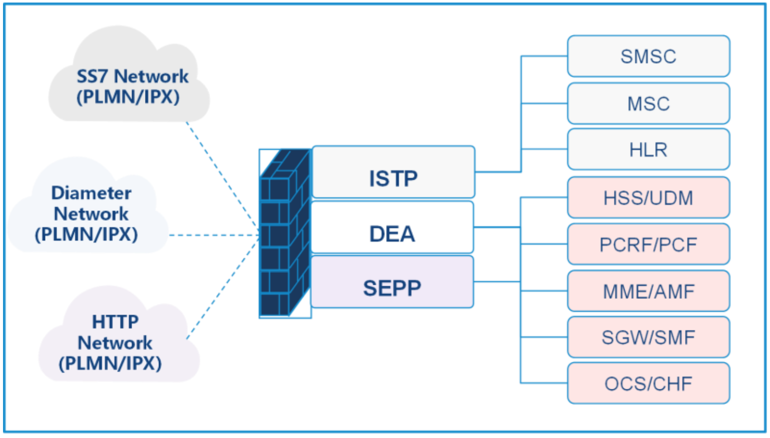
SCP plays an essential role on multi-domain service delivery both different domains at the same operator and between different operators

4. *Security for Signaling Network Itself*

The fourth area where SCP integration with other 5G SA NFs is critical is to ***ensure the security of signaling network itself.***

Securing the 5G signaling network becomes even more critical in 5G SA to protect the shared Control Plane. As the chart below shows 5G Security Edge Protection Proxy (SEPP) therefore needs to work in conjunction with intelligent/Internet Signal Transfer point (ISTP) and Diameter Edge Agent (DEA) as well as the firewall to ***shield all the signaling networks*** – SS7, Diameter and 5G Control Plane over HTTP.

Chart 9 Converged Signalling Firewall Defends Against Roaming Signaling Attacks



In recent years there have been several breaches of security on the signaling network – often by untrustworthy carriers in other countries. One of the most likely targets for attacks is the Signaling Gateway where intercarrier signaling converges. Today many operators have introduced a signaling firewall as shown in Chart 9 above. In a 5G only network – as shown earlier in Chart 7 - a 5G Roaming Hub would mediate roaming signaling securely across multiple peer to peer 5G operators, so that a rogue operator in another country would find it difficult to attack the home operator's 5G signaling system.

Another potential 'attack surface' for control plane attacks e.g. Distributed Denial of Service (DDoS) is at the edge of the network. Today for Multi-Access Edge Compute (MEC) services, operators need to handle potential *security attacks at the edge* prior to reaching any signaling firewall at the nearest data center. In 5G, operators now have ability to embed the Security Edge Protection Proxy (SEPP) and pre-empt attacks before they reach the data center, by providing both pre-session security negotiation, E2E encrypted application security and encapsulation of HTTP/2 core signaling messages as well as operator specific roaming security monitoring. To operate securely the SCP must work with SEPP as part of a secure signaling network that includes:

Interworking Security through:

- Network topology hiding
- Black lists and White lists
- Signaling Screening
- Signaling Firewall
- Transport layer encryption (IPSec, TLS, DTLS)

Multi-network Cross analysis:

- Cross-location, time verification
- Multi-Network security analysis

5G SA therefore has inherent security mechanisms that can be integrated with SCP to protect Control Plane traffic with or without additional Signaling Gateway or Firewall protection.

IV. State of 5G Network Signaling and CSP Adoption

5G SCP Deployment will accelerate alongside 5G Standalone (SA)

State of 5G SA Deployment determines adoption of SCP

Early in 2019 and 2020 operators in China were the first to move to 5G SA directly from 4G. When they began deployment, 3GPP Release 16 was not complete and they adopted Release 15 with Model B and no SCP. As Release 16 and SCP became available, they planned to migrate the original Release 15 networks to Model D, but it has taken some time.

Elsewhere many other operators deployed Release 15 with a Non-Standalone (NSA) core, 4G Diameter signaling and 5G radio technology. *Today, however, in late 2021 operators around the world are rapidly accelerating their commercial deployment of 5G SA*.

As of mid-November 2021, 26 Operators had launched 5G SA Commercial Public service – with 9 of them also providing private network solutions for enterprises, utilities and government entities. Another 7 are in the process of launching commercial 5G SA in the near future. This rapid 5G SA deployment should continue to accelerate in 2022 as the 5G SA Core becomes the network standard in many countries.

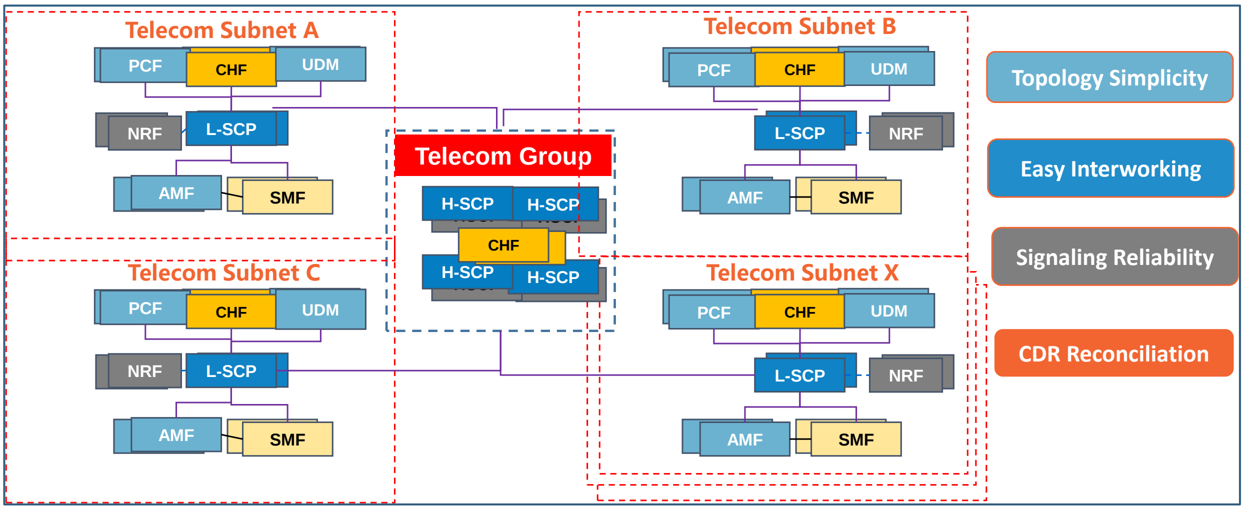
SCP Deployment.

Multiple major operators - Orange, Vodafone, Telefonica, SK Telecom (SKT), Thailand's Advanced Info Service (AIS), Sunrise in Switzerland and the three largest operators in China - are all now planning the full implementation of Release 16 and have started to *consider the SCP as part of their 5G SA deployment plans.* Some have already launched SCP commercially including AIS, China Telecom, Sunrise and SKT. Other new 5G SA operators have discussed their 5G signaling plans and run small scale 5G SA trials. SCP is now viewed as a key component of 5G SA systems as Release 16 rolls out.

China Telecom has launched commercial SCP enabled capabilities

The business case for SCP gets even better when it enables live 5G SA commercial services. China Telecom has leveraged SCP capabilities to manage Call Detail Records (CDRs) for subscriber roaming across multiple subnets as shown in the chart below. SCP dramatically reduced time to set up CDR roaming from weeks to days.

Chart 10 China Telecom Reduced number of links, accelerated Time To Market (TTM) and Leveraged multi-Subnet CDR Roaming with SCP



SK Telecom implementing SCP for 5G SA Control Plane Efficiency in South Korea

In November 2020 SK Telecom (SKT) was the first operator in South Korea to launch 5G SA commercial data service and later the first to complete next-generation 5G Core deployment based on Release 16.

SKT has worked with its vendors to develop a cloud native Service Communication Proxy (SCP) that enables an operator to manage its 5G Control Plane more effectively and efficiently. *SKT adopted the SCP to intelligently control communication of NFs based on traffic status and behavior.* This dramatically increased signaling efficiency, since the SCP now allowed NFs to communicate with each other only as necessary, depending on the network traffic. SKT estimates that *this* ***SCP implementation has improved communication efficiency among NFs by 30%.***

Pre-5G SCP-based software already pre-Deployed for Converged 5G SA signaling on Day Zero

Other operators are already pre-deploying SCP based software to optimize Diameter and SS7 routing for secure converged signaling. Well architected 5G SCP software can generate an *immediate ROI even in pre-5G 'SA ready' networks* to support VoIP, VoWiFi and VoLTE interworking*. SCP is then ready to ensure seamless 4G/5G/VoIMS/VoIP Services on Day Zero as 5G SA Services roll out.*

SCP Is generating Return on Investment (ROI) for Operators

As 5G networks grow the ***SCP Business Case continues to strengthen and SCP becomes the essential mechanism that not only delivers efficient real time 5G performance and scalability, but it also accelerates service delivery, reduces operations cost, optimizes link utilization and leverages End to End (E2E) service revenues.***

V. Service Communications Proxy (SCP) - Leading Vendors

Leading 5G Signaling Vendors

Strategy Analytics used public sources to compare the SCP offerings the four leading vendors:

- Ericsson
- Huawei
- Nokia
- Oracle

Ericsson, Huawei and Nokia all offer versions of the SCP as part of their 5G Core offering.

Huawei

Only Huawei has currently announced a complete SCP offering with its **Unified Signaling Controller (USC)** for *5G core, multi-domain and converged SS7, Diameter* signaling solutions *with integrated 5G SEPP security and optimized signaling routing and load management*. Key capabilities include:

- Intelligent Service and User based Traffic Control
- Robust Load Management for Control Plane/Signaling Storms
- Unified Signaling network for 2G/3G (SS7), 4G (Diameter) and 5G
- Interworking of 4G and 5G and other services with BSF
- Unified Routing Database and Control
- Multi-layer security and integration with 5G SEPP
- Unified Operations and Management for all signaling networks – designed for automation

Both Ericsson and Nokia offer 5G SCP features as summarized below.

Ericsson

Ericsson's **Cloud Signaling Solutions** include the network elements defined by 3GPP in Releases 15 and 16 - SCP, SEPP and BSF as well as its cloud native legacy Diameter Signaling Controller (DSC). Together the solution is referred to as the **Signaling Controller**. It "optimizes the throughput of the network" with support for *static and dynamic overload handling* and *algorithms to take care of signaling peaks*.

Ericsson however, remains very cautious about endorsing the '**Indirect' SCP communications Model D** and notes that "Depending on how SCPs are deployed (including geographical location) and how the signaling is routed from NF consumer to NF producer through the SCPs, the signaling may pass through several SCPs along the way…given a long distance between NFs and the need to pass through several SCPs, some latency-sensitive KPIs may be affected." Strategy Analytics believes that a good, distributed SCP network architecture with high throughput connectivity should obviate this problem.

Nokia

Nokia like Ericsson bundles the three major capabilities as part of its **Cloud Signaling Director (CSD)** i.e. SCP, SEPP and BSF. It handles *signaling plane traffic growth*, controls *topology,* ensures *4G Interoperability on the Control Plane*, *secures the roaming infrastructure* and "boosts operations efficiency, scalability, and performance by defining *behavior in the Control Plane*".

Nokia sees CSD delivering **pre-5G SCP based solution** and eventually 5G SCP for signaling within and between networks including:

- Intelligent routing that increases security and scalability of the Control Plane
- Rules Engine for signaling and Cloud traffic growth

Nokia offers specific modules for signaling storm protection, mediation and interworking, signaling security, intelligent routing and load balancing, overload protection and fraud protection. Nokia also provides interfaces for integration with third-party systems including enhanced capabilities for 'agile' Policy Rules creation and modification.

Oracle.

Oracle Communications cloud native **Service Communication Proxy (SCP)** provides 5G aware load balancing, alternate routing, 5G based traffic prioritization, producer NF discovery and selection, 5G mediation, 'Canary' testing, hybrid deployment, 5G Subscriber Location Function (SLF) and "synergies with NRF beyond standards." Oracle claims the SCP reduces connections to and from NFs, enables congestion control, improves Load Balancing, routing control and resiliency, acts as a 'Circuit Breaker', provides key metrics, KPIs etc. and plays a crucial role in the rollout of new NF releases
 Although Oracle does not have a complete 5G core offering it has recently made significant investments in its signaling division – formerly Tekelec - and has developed a fully cloud native 5G SA signaling solution with this enhanced SCP.

Oracle may in fact be the up and coming player that will challenge the largest players signaling offerings with its new SCP applications.

Potential Threats to Largest Vendors.

In addition there are several small independent signaling software vendors that offer SCP software. They include **Casa Systems**, **NetNumber** and **Tieto**.

This good level of competition bodes well for the *importance of SCP capabilities and the likelihood of innovative enhancements in the future.*

VI. Conclusion

CSPs are just beginning to appreciate the value of Model D as part of Day Zero 5G SA deployment; and to leverage the power of the SCP for dynamic scaling and management of millions of simultaneous service flows and interactions between 5G SA NFs as they move to ensure high performance and service profitability across their 5G and legacy networks.

Summary of the Benefits 5G Service Communications Proxy (SCP) Brings

As CSPs deploy 5G SA and move to Model D with the SCP, they discover the many benefits it brings. The operations benefits of the SCP and of converged signaling with SCP are each summarized below.

- ***Operations Benefits of Model D and SCP include:***
  - **Extensible Service-Based Architecture**
  - **No Changes Required to NFs and NRF**
  - **Simplified End to End (E2E) Service Communications**
  - **Automated Management**
  - **Optimized NF Routing**
  - **Unified Load Balancing and Overload Control**
  - **Service Orchestration** *to assure 5G service latency and reliability requirements.*
  - **Network Robustness** *to counter potential Signalling Storms, DDoS Attacks etc.*
  - **Operations and Maintenance Efficiency Enhancements** *including interoperability, fault isolation, routing management, traffic prediction, embedded security etc.*

- ***Benefits of Converged Signalling with SCP include:***
  - Multi-Network **Operations Simplicity**
  - Improved Resource Utilization and **Reduced Total Cost of Operations (TCO)**
  - **Seamless Evolution** for SS7, Diameter and 5G Signaling
  - **Seamless Interoperability** with 2G, 3G, 4G Services
  - **Multi-Domain Services** (Public and Private Networking, Fixed Wireless Access (FWA), WiFi and Mobile interworking etc.)
  - **Co-ordinated Administrative Services** - Unified Data Management (UDM), Policy Control and Charging Co-ordination

5G SCP based signalling solutions assure Control Plane performance, guarantee seamless E2E delivery and interworking of legacy and 5G Services, secure protection against attacks (including signaling attacks from rogue carriers) and create a ***'Future Proof Architecture' for a myriad of new CSP 5G Services.***

Analyst Contact

The author of this Report Sue Rudd, can be reached at srudd@strategyanalytics.com.

Get help from Strategy Analytics

Working with Strategy Analytics gives you the knowledge you need to succeed.

Understand your customer

Business opportunities abound. But which ones are right for you and your customers? Which will give you the advantage?

Optimize your user experience

Optimize your product to give your users the best experience and you the market advantage.

Analyze the market

Understand the size of the opportunity and where your product fits using our unrivalled knowledge and world class data analysis techniques.

Explore your future

Working with us will focus you. With our insight and forecasting expertise you'll make confident strategic decisions that drive success.

Please contact us at custom@strategyanalytics.com with any questions and for further details and solutions on how we can work with you on creating a custom solution to address your specific needs.