Independent market research and
competitive analysis of next-generation
business and technology solutions for
service providers and vendors

HEAVY READING

WHITE PAPER

Multi-Vendor 5G Core Networks: The Case for a Disaggregated Control Plane

A Heavy Reading white paper produced for Oracle

ORACLE® Communications

AUTHOR: GABRIEL BROWN, PRINCIPAL ANALYST, HEAVY READING

5G CORE AND STANDALONE OPERATION

5G standalone (SA) operation, using a new core network, is foundational to mobile operators seeking to offer advanced 5G services with a low cost of production. Over the next two to three years, operators in all global regions will design, deploy, and scale 5G core networks on software-defined infrastructure. By April 2021, eight operators had already launched SA, according to the Global Mobile Suppliers Association (GSA), and a further 36 have firm plans to launch in the near term. There is now a good supply of devices that support SA mode, including the iPhone 12 after the latest iOS update.

Decisions about how best to deploy 5G core will have far-reaching and long-term implications for how 5G networks perform and for the operator's service offer. Heavy Reading's white paper makes a case for operators to consider a multi-vendor 5G core deployment. Specifically, it discusses why operators should consider sourcing closely related groups of control plane functions from independent vendors. The paper references the 3GPP service-based architecture (SBA) and cloud-native infrastructure as technology enablers for a "disaggregated control plane" in the 5G core.

This paper makes three main recommendations, as follows:

- **Operators should consider a multi-vendor 5G core** because it enhances service innovation and improves network resiliency. Two to four 5G core suppliers—each providing clusters of related network functions (NFs)—is the optimal number for a multi-vendor strategy. This paper does not advocate large numbers of discrete suppliers that require extensive, custom integration by the operator.
- **Operators should, in most cases, take a phased approach** to 5G core deployment, starting with essential functions for SA operation. They can add more capabilities as requirements become clearer, demand for advanced services increases, and technology matures. Each phase is an opportunity to introduce a best-of-breed vendor to the "5G network platform."
- Specifically, in the control plane, **operators should consider clusters of NF functions** that together create a disaggregated mobile core—for instance, by combining functions in areas such as subscriber data management, signaling/routing & network slicing, and service exposure. A disaggregated control plane also gives operators more choice over user plane solutions to meet diverse service needs.

Multi-vendor 5G core is strategic

The mobile core network is highly strategic. It is involved in virtually every interaction a mobile device has with the network, from authentication, session setup, and mobility to active/idle state changes, applying policies, and routing user traffic. The core is also the locus of service creation and an enabler of the advanced applications that are driving 5G investment. It has a direct impact on the service offer and on the monetization of services.

A multi-vendor 5G core is strategic to operators in two main ways:

- **Supplier diversity and network resiliency**

  High availability is an operator's number one priority. In the mobile core, even small problems can result in widespread outages and brownouts. In 5G, this will become ever more important as more devices and more services—and more critical services—are deployed on the network. By definition, a single-supplier dependency, in the most critical part of the network, is a risk. Very few vendors can provide an entire 5G core network, and those that can often have areas of weakness or can be subject to unforeseen failure.

  A multi-vendor 5G core provides a degree of resiliency because it helps build the operational capability needed to manage a multi-vendor environment and to replace an existing vendor that is not meeting requirements or delivering features as needed. This is particularly important in the current geopolitical climate because operators are typically limited to a choice of one to two end-to-end 5G core suppliers per market. In these cases, a single-vendor failure could be systematically catastrophic.

- **Rapid creation of advanced services**

  Operators are defined by how customers experience their services. The ability to create services that respond to market demand, or that stimulate and enable new applications, is one of the important ways 5G will serve customers. A 5G SA network, with a 5G core, is required for advanced service types such as edge applications, network slicing, and mission-critical Internet of Things (IoT). This makes the 5G core more than a critical connectivity layer; it is also fundamental to service creation in operator networks.

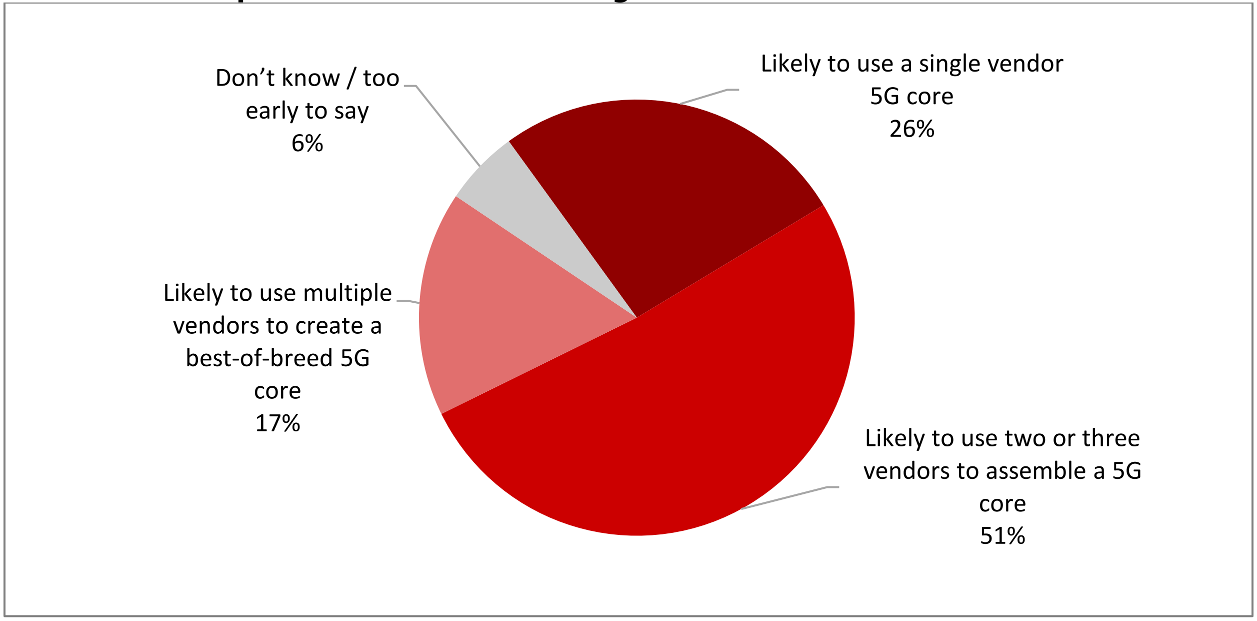
  A multi-vendor core can decouple service creation from connectivity and allow operators to source the best, independent suppliers to support different service types and integrate with external applications using service exposure APIs. 5G core suppliers that are more "cloud-native," with deeper and wider support for open APIs, are better able to integrate with external cloud applications.

Demand for multi-vendor 5G core

The Heavy Reading *5G Core Operator Survey*, published in April 2021, identified a strong appetite among respondents to use a multi-vendor strategy for the 5G core—with some important caveats. **Figure 1** shows 51% of operator respondents say their company is "likely to use two or three vendors to assemble a 5G core." A further 17% are "likely to use multiple vendors to create a best-of-breed 5G core," which means an overall majority is in favor of using diverse 5G core suppliers.

This message is echoed in Heavy Reading's qualitative research where, in practice, it is apparent that most operators of reasonable scale already use multiple core vendors in some form for 4G and expect to continue to do so for 5G. Often, an operator has a "lead" core vendor but also uses specialist best-of-breed suppliers for certain functions.

Figure 1: Does your company plan to assemble the functions that make up the 5G core from multiple vendors or from a single vendor?



n=72
Source: Heavy Reading 5G Core Operator Survey, April 2021

A multi-vendor core strategy is not all plain sailing, however. The difference in this survey result between "two or three vendors" (51%) and "multiple vendors" (17%) highlights an important issue that should be acknowledged: multi-vendor core can be difficult and comes with costs of increased systems integration, interoperability testing, more software updates, extra training, vendor management, and so on. The SBA and cloud-native infrastructure alleviate these challenges, but in many cases, there is nevertheless a practical limit on how many vendors it is optimal for an operator to work with. This paper argues that the use of two to four lead vendors provides significant benefits at a manageable cost.

5G CORE ARCHITECTURE

The 5G system architecture was specified by the 3GPP in Release 15 (TS 23.501) and developed further in Release 16 (the most recent specification), with ongoing enhancements currently underway in Release 17. Further updates, as part of 5G Advanced, from Release 18 onwards should also be expected. The 5G core is an essential part of the 5G system architecture and SA operation.

Software-defined infrastructure

The 3GPP is not prescriptive about how a core network is built and deployed. Nevertheless, the specifications were written in the expectation that operators will use software-defined infrastructure and state-of-the-art cloud networking technologies for the 5G core.

From a multi-vendor perspective, one advantage of decoupling hardware and software is that it makes it easier to source 5G core applications from independent software vendors (ISVs). In effect, by adopting a telco cloud infrastructure platform, operators create a market for ISVs to provide best-in-class 5G core applications.

The choice of virtualized infrastructure using virtual machines (VMs) or cloud-native infrastructure using containers to host applications is important and has far-reaching consequences. Currently, both options are deployed, and, in some cases, operators use VMs and containers in the same core network. In each case, the ability to run multi-vendor applications is widely supported. The trend, over time, is toward cloud-native platforms; this means the ability of the 5G core application vendor to operate in such environments is an advantage, particularly where the 5G core connects to external cloud services and/or offers network service exposure to third parties.

Service-based architecture

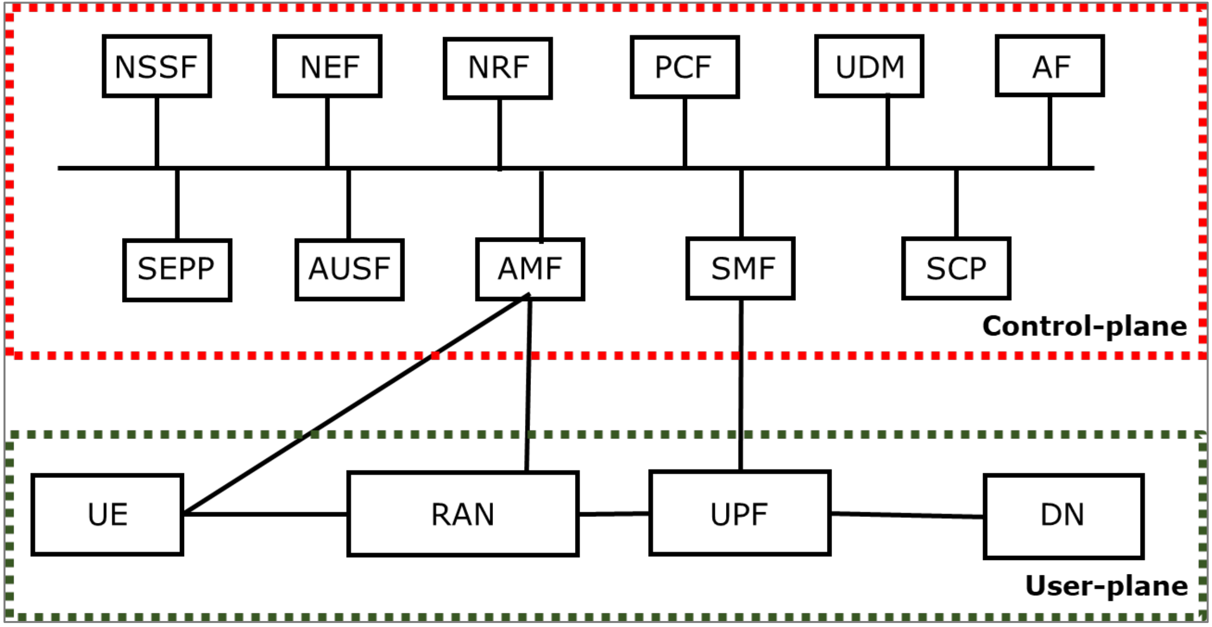
The overall 5G system architecture, shown in **Figure 2**, can be broadly separated into the RAN and the core, which is further divided into the user plane and control plane. The large majority of functions are in the control plane.

The 5G core uses the 3GPP SBA, which adopts service-orientated software design principles, to enable NFs to connect across a service mesh using APIs. This is a major change from the point-to-point architecture used in 4G core and gives operators greater operational flexibility to add, remove, or upgrade functions without impacting live service or requiring wholesale changes to the deployed architecture.

Another important difference is that 5G core incorporates more functional entities in the architecture. In a 4G evolved packet core (EPC), there are typically around 10 discrete node types deployed; in a 5G core, the number of discrete NFs increases to, on the current count, more than 20. The SBA makes it easier to support this wide range of functions and for operators to evolve to more sophisticated 5G core networks over time as they add capabilities and extend their service offer.

Although not part of the 3GPP specification, any 5G core deployment will also include important ancillary functions needed to offer a reliable service, most notably in the areas of routing, security, and traffic/content optimization. These functions should similarly run in the same telco cloud infrastructure and be developed using cloud-native principles.

Figure 2: 5G system architecture



Source: Heavy Reading, 3GPP

The functions that make up the 5G core are listed below. They are not all essential—for example, some are focused on non-3GPP access (e.g., via Wi-Fi) and some may be deployed in a later phase.

• Access and Mobility Management Function (AMF)	• Session Management Function (SMF)
• User Plane Function (UPF)	• Authentication Server Function (AUSF)
• Unstructured Data Storage Function (UDSF)	• Unified Data Management (UDM)
• Unified Data Repository (UDR)	• 5G-Equipment Identity Register (5G-EIR)
• Network Slice Specific Authentication and Authorization Function (NSSAAF)	• Policy Control Function (PCF)
• Charging Function (CHF)	• UE Radio Capability Management Function (UCMF)
• Network Data Analytics Function (NWDAF)	• Network Exposure Function (NEF)
• Network Slice Selection Function (NSSF)	• Network Repository Function (NRF)
• Service Communication Proxy (SCP)	• Security Edge Protection Proxy (SEPP)
• Non-3GPP InterWorking Function (N3IWF)	• Trusted Non-3GPP Gateway Function (TNGF)
• Wireline Access Gateway Function (W-AGF)	• Trusted WLAN Interworking Function (TWIF)

CONTROL PLANE DISAGGREGATION

An attractive multi-vendor 5G core strategy is to think in terms of clusters of related NFs that can be sourced from a single vendor and deployed alongside NF clusters from other suppliers. By using "clusters of related NFs," operators can simplify deployment and gain the advantages of pre-integration yet also realize the benefits of best-of-breed suppliers. This strategy is reasonably familiar in 4G and offers even greater potential in 5G.

The proposal in this paper is to categorize 5G core NFs into subgroups of related functions that can be sourced from ISVs as part of a multi-vendor deployment. These categories are not strictly defined, and operators may frequently move functions between categories or source functions independently according to their network needs and vendor preferences. Heavy Reading believes this is a useful way to think about disaggregating the 5G core that will help operators resist monolithic single-vendor deployments. This model aligns with operator preferences for working with two to four vendors or for working with one lead vendor and one, two, or three specialist suppliers for particular NF groups.

5G core NF categories

The six categories of 5G core functions are as follows: 1) data management, 2) policy & charging, 3) session & mobility management, 4) service automation, orchestration, & analytics, 5) signaling/routing & network slicing, and 6) non-3GPP access. **Figure 3** shows how these categories map to the individual NFs, with a brief description of the category and the reason to place each NF in that category.

Figure 3: 5G core NF categories

Subscriber data management	
AUSF, UDM, UDR,	New subscriber data management for 5G combines frontend applications and backend subscriber databases. There is potential to combine with network data functions such as 5G-EIR and, as/if operators move to an independent network data layer, with the UDSF.
Policy & charging	
PCF, CHF	Policy & charging are traditionally closely related. However, policy control may often be sourced independently or in association with UPFs. Charging is often part of a wider business support system (BSS) solution.
Session & mobility management	
AMF, SMF, UPF	Basic building blocks needed to provide a 5G session. These functions are often provided together, although there is increasing demand to use multiple independent UPF suppliers. Can initially be used in conjunction with 4G subscriber databases.

Automation, orchestration, & analytics	
NWDAF, NSSMF, NSMF	This category includes the Service Based Management Architecture (SBMA) for 5G core and newer analytics functions. Note that the 3GPP SBMA does not define the entirety of the required management architecture, leaving some aspects to other standards organizations.
Signaling/routing & network slicing	
NSSF, NRF, SCP, SEPP, NEF	A major category with particular importance for large-scale 5G cores and where advanced services such as distributed user plane, service exposure, and network slicing are desired by the operator.
Non-3GPP access	
N3IWF, TNGF, W-AGF, TWIF	Non-3GPP access (e.g., Wi-Fi) is often deployed as a solution in one phase. Over time, there may be stronger demand for access gateways (AGFs) as fixed/mobile convergence is adopted.

Source: Heavy Reading

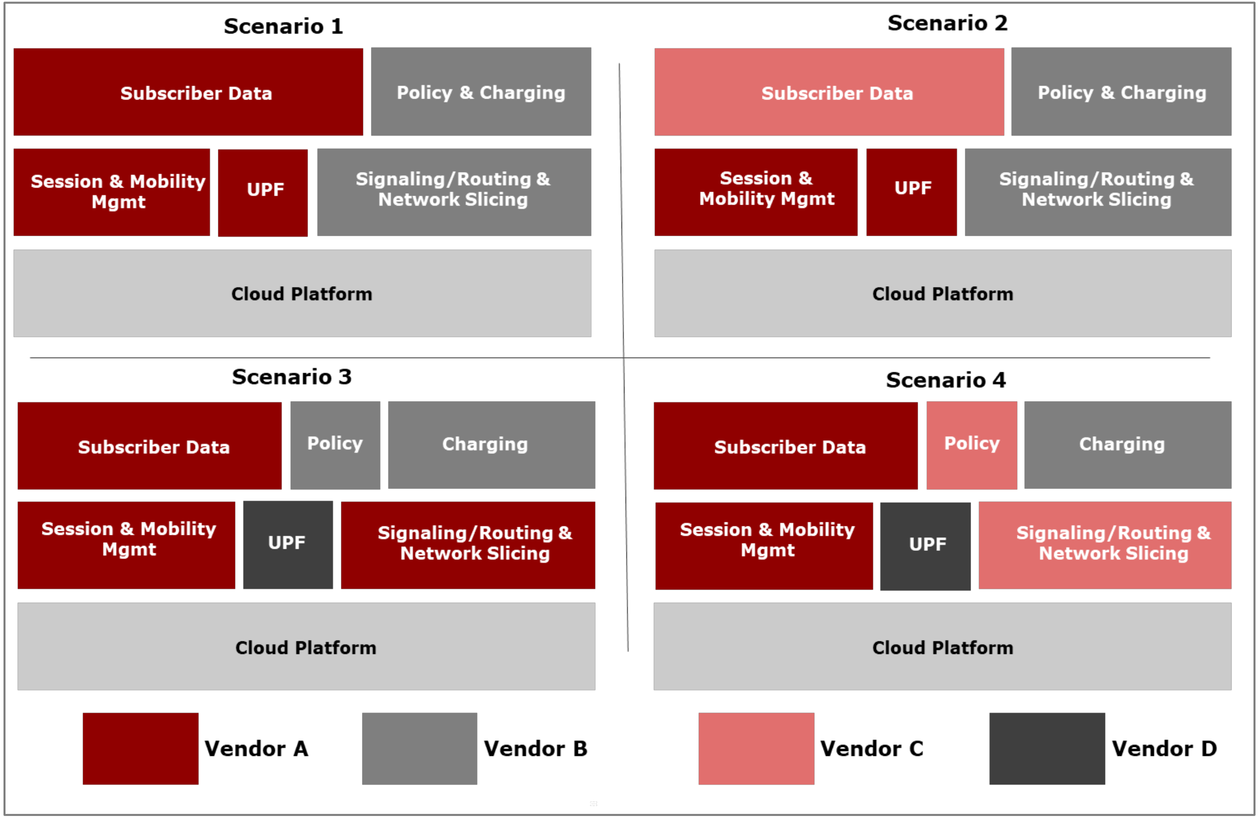
Multi-vendor 5G core scenarios

A multi-vendor strategy will be more effective where the operator selects two to four suppliers to provide the heart of the 5G core deployment. **Figure 4** shows different scenarios that might occur. Variations on these combinations are possible and expected. It is also anticipated that operators will add functionality to the 5G core over time, perhaps introducing new vendors at the start of a new phase.

- **Scenario 1** shows a two-vendor model, with Vendor A supplying session & mobility management, UPF, and subscriber data and Vendor B supplying signaling/routing and policy & charging.
- **Scenario 2** introduces a third vendor (Vendor C) for subscriber data.
- **Scenario 3** shows a lead vendor (Vendor A) providing the majority of the core NF clusters but with a best-of-breed supplier for policy, charging, and UPF.
- **Scenario 4** shows a four-vendor configuration that uses the same vendor for policy and for signaling/routing & network slicing.

These are illustrative multi-vendor scenarios and are representative of the decisions being made by operators as they plan 5G core deployments. It is worth restating an earlier point that 5G core will likely be deployed in phases and that a good time to introduce new vendors is likely to be as each phase is deployed.

Figure 4: 5G multi-vendor 5G selection examples



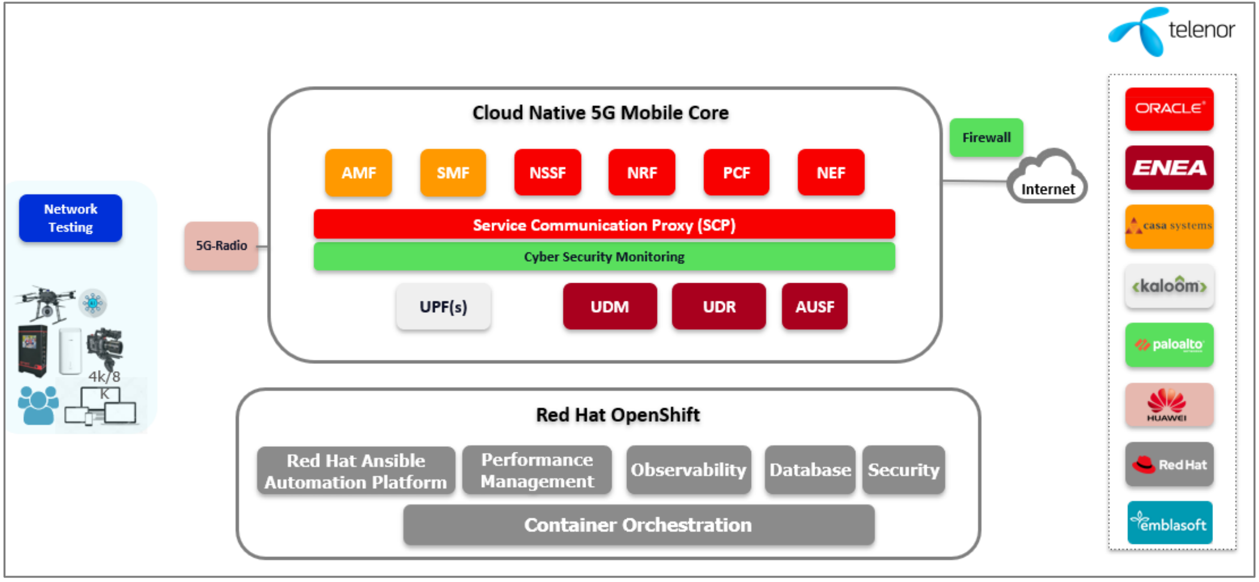
Source: Heavy Reading

Real-world multi-vendor 5G core

A public example of a multi-vendor 5G core is shown in **Figure 5**. In this case, Telenor, an international mobile operator headquartered in Norway with operations across the Nordics and Asia, worked with half a dozen vendors to create a working, deployable 5G core.

The infrastructure platform is built using Red Hat's OpenShift cloud-native technology, with 5G core applications from five different vendors running in containers. The UPF is from Kaloom, the AMF and SMF from Casa Systems, the subscriber data functions are from ENEA, and the SCP, NSSF, NRF, PCF, and NEF from Oracle. Palo Alto provides non-3GPP cloud security monitoring and firewall software on the internet interface (N6).

Figure 5: A multi-vendor cloud-native 5G core example



Source: Telenor, May 2020

Discussing the test bed deployment, Telenor explains that "single-vendor dependency can be a killer for innovation" that "restricts open collaboration from the broader 5G ecosystem of companies developing new technology, use cases, and services."

"We believe that such a multi-vendor environment will stimulate innovation, reduce cost of the infrastructure, increase competition, and accelerate the development of an open 5G-ecosystem, which in turn will enable a range of new services for Telenor's consumers, industry, and government customers," said Patrick Waldemar, vice president and head of Technology at Telenor Research.

INDEPENDENT CONTROL PLANE SIGNALING

One area, among several, where there are clear-cut advantages to selecting a best-of-breed 5G core vendor is signaling and routing. The SCP introduced in Release 16 can be seen, conceptually, as a continuation of the STP/DRA in 3G and 4G networks in that it provides a way to manage core network signaling reliably at scale. There are also significant differences between 4G and 5G signaling—for example, the use of HTTP2 transport in the SBA.

Reliable and scalable signaling is essential. An SCP is used to route and manage signaling, protect against signaling storms, mitigate denial-of-service attacks, increase roaming security, provide centralized monitoring for the 5G core, and more. An independent SCP provides an important way to disaggregate the control plane by acting as a "service mesh" between functions and vendors, making it easier, operationally, to add/remove functions for upgrades, vendor swaps, and so on. Note, however, that an SCP is not a "service mesh" in the classical sense defined by the Cloud Native Computing Foundation (CNCF). The SCP is a designed-for-telecom service mesh and deployed as a discrete set of resilient NFs (centralized or distributed) that support 3GPP enhancement, such as 3GPP-specific headers.

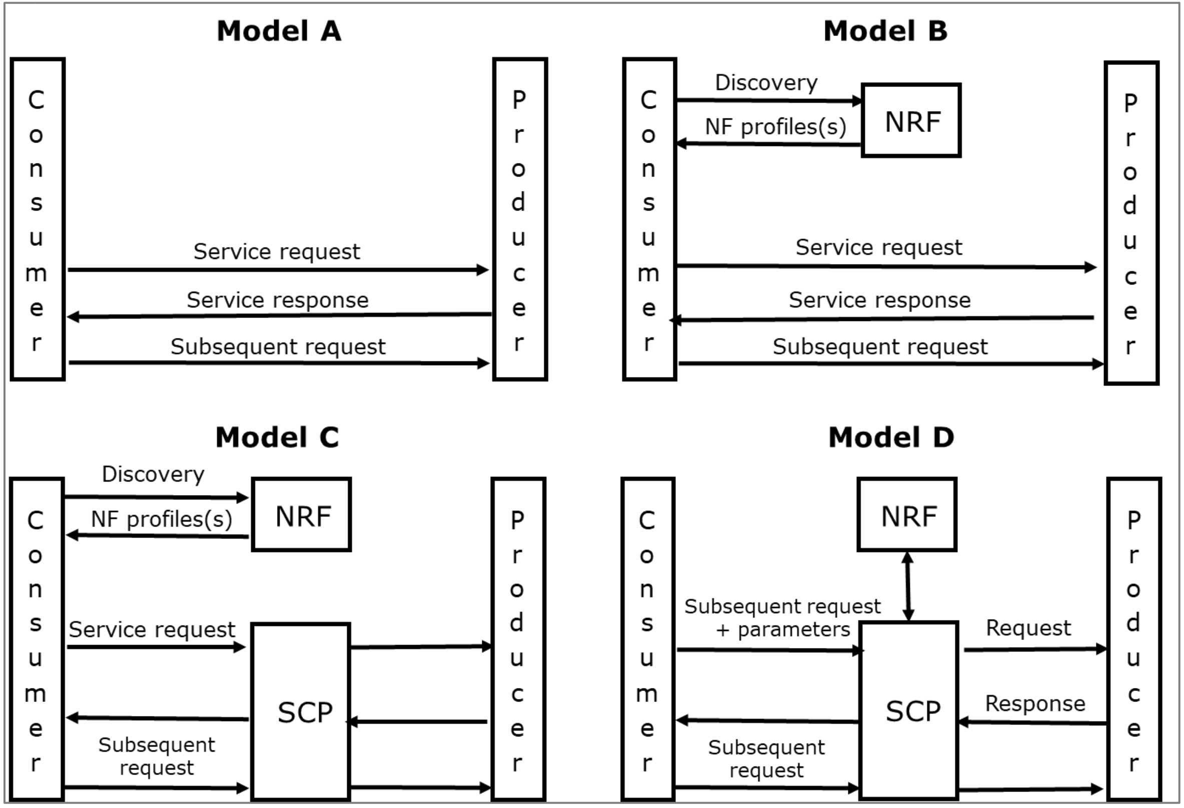
Toward Model D

In the 5G core, NFs are producers and consumers of services provided by other NFs—for example, a policy server consumes information provided by the subscriber database or the AMF consumes information provided by the NSSF. Consumer and producer NFs can "talk" directly to one another. This direct connection model is shown in **Figure 6** below as Model A. This works for smaller-scale deployments with lower numbers of users and transactions. However, it limits operational flexibility and has scaling challenges.

In Model B, consumer NFs, instead of communicating directly with a producer NF to request service, first query the NRF to ask which producer to use before making a direct connection with the producer. The NRF, in this model, can select the appropriate producer NF and provide services such as load balancing. In Models C and D, an SCP is introduced as a proxy between consumers and producers. In Model D, for instance, consumer NFs simply send requests to the SCP, which then identifies the appropriate producer NFs (via the NRF) and returns the requested information. The appeal of this model is that it simplifies the NF, making it easier to add/swap/change NFs and easier to scale the 5G core as service requests increase. In effect, the SCP deployment becomes a 5G core service mesh.

Heavy Reading's qualitative research indicates most operators that have formed a view—many are still in the evaluation phase—intend to deploy Model D. This may be part of the initial design and deployment or earmarked for a later phase investment to be deployed as the technology and requirements mature.

Figure 6: Communication models for NF/NF services interaction



Source: Heavy Reading, 3GPP

Advantages of an independent SCP

An SCP is clearly important and useful. But why should an operator source an independent, best-in-class SCP supplier? There are three main reasons, as follows:

- **Operational agility:** An SCP provides a proxy between functions and can, for example, be used to harmonize protocol implementations between vendors or to reduce the interoperability testing needed to introduce suppliers or update existing functions. This generates ongoing operational efficiency benefits.
- **Rapid technology development:** Specialist suppliers are often faster to develop features (e.g., implementation of 3GPP subscriber ID headers in HTTP2). Specialists are often more familiar with multi-vendor environments and can be faster to complete interop testing when updates or new products are issued by vendors. End-to-end vendors are less incentivized to focus on fast interoperability.
- **Decouples service evolution:** By decoupling vendor roadmaps and through the operational efficiency noted above, an independent SCP deployment allows the operator to be more agile in its service development. For example, if an operator seeks to introduce a new enterprise slice service, it may want to do so with minimal impact on the existing core deployment.

Combining SCP with NRF and network slicing

The logic of sourcing the NRF and SCP from the same vendor is clear from the above diagram (**Figure 6**). These are closely linked functions with little advantage to sourcing them separately. But what other functions could beneficially be combined with an SCP?

This paper posited, in **Figure 3,** a category of related NFs known as "signaling/routing & network slicing" that includes the following: NSSF, NRF, SCP, SEPP, and NEF. It is not required to bundle these functions together, but there are reasons why it may make sense technically and operationally. These are as follows:

- **Security Edge Protection Proxy (SEPP):** Inter-operator security is important for the integrity of user services while roaming—for roaming fraud prevention and for network security. The SEPP handles all inter-network signaling traffic, and it may be logical, from an operational perspective, to purchase it from the same SCP supplier used for internal signaling.
- **Network Slice Selection Function (NSSF):** When requested by the AMF, the NSSF provides configuration information needed to direct the user into the appropriate network slice. This, in some cases, may trigger large numbers of control plane transactions between NFs. For this reason, it may be operationally beneficial to deploy with the SCP. In other cases, the NSSF may be deployed with the policy server (PCF) since it also is a form of policy node.

- **Network Exposure Function (NEF):** In later phases of 5G SA, network exposure will enable customers and other third parties (such as cloud providers, roaming partners, or MVNOs) to create optimized service experiences that make use of internal network capabilities exposed by the operator. It is likely that these services will be tied together in a network slice and will be security and privacy sensitive. In this context, the NEF has an affinity with NSSF, which may make it useful to combine these functions. Further, the security implications of external services interacting with 5G core will require close collaboration with the SCP.

SUMMARY AND CONCLUSION

Operators worldwide are designing and deploying 5G core networks, with large-scale deployment expected from 2022 onwards. This investment will modernize their core infrastructure and be a critical enabler for new 5G applications. Decisions about how to deploy 5G core will have far-reaching and long-term implications for how 5G networks perform, for operator service portfolios, and for the end-user experience.

This white paper makes a case for operators to consider a multi-vendor 5G core deployment. It argues this will enhance network resiliency, increase operational agility, and enable faster service innovation. Specifically, it references the value of a multi-vendor strategy for a disaggregated 5G core control plane.

In this paper, Heavy Reading advocates a multi-vendor strategy that uses between two and four vendors, each supplying closely related groups of NFs from independent suppliers. This gives operators substantial benefits but at a manageable integration cost. The paper does not advocate large numbers of discrete suppliers that require extensive, custom integration.

Underpinning a multi-vendor strategy is the 3GPP-standardized SBA and the use of software-defined, cloud-native infrastructure. These are both vital technology enablers for a disaggregated 5G core because they make it easier and faster for operators to upgrade networks and to introduce new NF vendors without disrupting the deployed architecture.