Ericsson and SK Telecom have signed a Letter of Intent (LoI) to collaborate on the development of a 5G core network that deploys network slicing technology. The development, which leverages Ericsson's Regional Cloud Lab and Ericsson HDS 8000, is planned to be ready by the end of 2015.

Network Functions Virtualization technology allows for easier creation and expansion of separate logical nodes and functions for a specified group of traffic and signaling, often referred to as a network slice. In turn, network slicing opens up a new way of achieving in-service software management at the network level.

With network slicing, a parallel network can be set up with a new software version of network functionality, followed by step-by-step migration of sessions – lowering the risk for the operator and ensuring minimal disruption to subscribers. As a result, it enables more efficient business models for operators while simplifying software architecture requirements, including software upgrades, on network elements such as MME, SGW and PGW.

Under the terms of the agreement, Ericsson and SK Telecom will develop and deploy network slicing technology optimized for 5G services. The two companies will also continue their existing partnership to build a joint 5G test bed. Work on the test bed is starting this year, with the ambition to provide the world’s most advanced end-to-end 5G pilot services.

Projected 5G use cases such as remote machinery, intelligent transportation and virtual reality will place new performance and security demands on networks. To meet these requirements, 5G networks will be built with network slicing technologies that use logical instead of physical resources, and which enable operators to provide networks on an as-a-service basis. The instantiation of the network slicing will use the Ericsson Virtual Evolved Packet Core solution.

A logical instantiation of a network is often called a network slice. Network slices are possible to create with both legacy platforms and network functions, but virtualization technologies substantially lower barriers to using the technology, for example through increased flexibility and decreased costs.

Currently, management of networks is mostly about managing individual network elements. One of the major ideas behind NFV is to automate management for the entire network so that complex network-spanning tasks are easier to perform. Integration of different NFV components will still be a complex task for the operator, but on the other hand NFV allows an entire network to be delivered as a pre-integrated network slice.

Another aspect of management and network slicing is setting up separate management domains for different network slices. This may allow for completely separate management of different parts of the network that are used for different purposes. Examples of use cases include mobile virtual network operators (MVNOs) and enterprise solutions. This kind of network slice would, in current Evolved Packet Core (EPC) networks, only cover the PDN gateway (PGW) and the policy control resource function (PCRF). However, for machine type communication (MTC) and machine-to machine (M2M) solutions, it is likely that it would also cover the Mobile Management Entities (MMEs) and Serving Gateways (SGWs).

Separation of management may also be expanded into security aspects. Separate management per network slice, as described above, is a first step towards this, but by using network slicing it would be possible to deploy virtual network functions (VNFs) in separate networks with separate configuration and network topology. Add to this the potential to run VNFs on dedicated hardware, which provides more predictive characteristics as well, and it is obvious that improved security and improved quality of service assurance are also important aspects of network slicing technology.

When the operator sources a complete network slice from a single vendor, the vendor can deploy a network optimized for a selected set of terminals according to policy and behavior. The network slice may, for example, be resilient to hardware and software failures, or it may be

optimized for signaling intensive behaviors, such as in machine-to-machine terminals.

When a network slice covers only a part of the network topology, it is called a sub-network slice, which indicates that network slicing can also be hierarchical. The most commonly used containment of network slices in EPC is the PGW and PCRF in the same slice. Since the PGW selects the PCRF and the Access Point Name (APN) name is used for PGW selection from the MME, the selection mechanisms employed here are often already in use in legacy networks. But with network slicing in the data center, they are likely to be even more commonly used. It is also likely that there will be dedicated PGWs and PCRFs for many different deployments, both small and large.

Adding a SGW to the previous network slice of a PGW and PCRF and thereby creating another level of network slicing (while still supporting connections from other SGWs to the PGW) is a solution that is of interest when co-located SGWs and PGWs are used. As specified by 3GPP, the SGW selection in the MME can take the selected PGW into account.

5G security will be defined not only by quantitative aspects such as bitrates and latency, but more importantly by qualitative aspects such as new business and trust models, new ways of delivering services, an evolved threat landscape and an increased concern for privacy.

As a result, there is a need for a fundamentally new, multi-actor trust model that allows more flexibility. Security for virtualized networks and services should be considered. Attack-resistance

and data security must represent basic design criteria for new protocols, while security assurance and compliance have to be more verifiable and measurable. Tackling these challenges will require new tools such as network slicing, trusted computing and alternative ways of handling user identities.

“Virtual network architecture, including network slicing, is critical to supporting new services in the era of 5G. We will build an optimal network for a wide array of services from the overall end-to-end standpoint, and pioneer the evolution of innovative networks,” says Alex Jinsung Choi, Chief Technology Officer at SK Telecom.

The collaboration will leverage the capabilities of Ericsson’s Regional Cloud Lab, which is distributed across four sites in North East Asia including Anyang in South Korea, Beijing and Shanghai in China, and Tokyo in Japan. Fully operational since 2014, the Lab supports operators with the development and verification of cloud, Network Functions Virtualization and software-defined networking technologies.

The network infrastructure will be designed and built on Ericsson’s pioneering Hyperscale Datacenter System, Ericsson HDS 8000. Launched at Mobile World Congress in February 2015, this solution represents a new generation of hyperscale datacenter systems that uses Intel® Rack Scale Architecture for a disaggregated hardware approach that dramatically improves efficiency, utilization, automation and total cost of ownership for virtualized environments.

“Network slicing, based on virtual evolved packet core, is an important part of the technology evolution of 5G, supporting operators with a new, broader set of services. It is important that we work together in the industry on this journey”, says Ulf Ewaldsson, CTO, Ericsson.