SOLUTION BRIEF

# NFV Security Gateway for Communications Service Providers

Table of Contents

Revision 1.0 October 2016

## Executive Overview

Intel is accelerating Network Functions Virtualization (NFV) with unique capabilities that enable optimal use of data center resources to deliver communications services. Virtualized Network Functions (VNFs) provide the communications Service Provider (Comms SP) with the ability to introduce new services more rapidly and to scale current and future services more seamlessly. More than ever, traditional operators must keep pace in a world where application developers bring to market new services and capabilities that currently take Comms SPs years to launch. To remain relevant and competitive, Comms SPs are investing in the development of virtualized networks to enable new services to retain and grow the customer base.

The 3rd Generation Partnership Project* (3GPP*) specification 3GPP 33.310 mandates security on the S1 interface to the packet core. Intel has a number of technologies that can be utilized to accelerate cryptographic operations. This document details the critical technologies and capabilities, and describes Intel's role in the ecosystem that will be required to participate fully in Comms SP production deployments.

## Introduction

Increasing market pressures, such as skyrocketing mobile traffic, demand for enhanced services in a more agile environment, and the search for more cost-effective solutions are driving Communications Service Providers (Comms SPs) to adopt network functions virtualization (NFV). Virtualizing services onto standard, off-the-shelf hardware and taking advantage of Software-Defined Networking (SDN) can increase network flexibility and reduce costs, as well as enable operators to quickly launch new revenue-generating services in a more efficient manner.

The key benefit of virtualizing network functions, such as the Security Gateway, is that a Comms SP can host multiple workloads on the same rack of Intel® architecture-based servers and can dynamically scale services up or down depending on the hours of heavy use and real-time requirements. In addition, there is a drive toward locating packet core functions closer to the edge of the network. In a European Telecommunications Standards Institute (ETSI) Mobile Edge Computing (MEC) whitepaper,[1] the benefits are summarized as follows: "For application developers and content providers, the Radio Access Network (RAN) edge offers a service environment with ultra-low latency and high-bandwidth as well as direct access to real-time radio network information (such as subscriber location, cell load, etc.) that can be used by applications and services to offer context-related services; these services are capable of differentiating the mobile broadband experience." As services become distributed or moved toward the edge of the network, collocating the Security Gateway functionality on an Intel architecture-based server with workloads like those under the MEC initiative could offer benefits to a Comms SP.

Mobile traffic is expected to grow at a compound annual growth rate (CAGR) of at least 45 percent,[2] and analysts predict the current USD 2.3 billion NFV market to reach USD 11.6 billion in 2019.[3] Comms SPs and the ecosystem that supports the industry are evaluating approaches to efficiently scale to meet these traffic requirements.

Many system integrators, software vendors, and platform providers rely on Intel® technologies to deliver the performance and scalability required for Security Gateway solutions. The Security Gateway described in this document implements Internet Protocol Security (IPsec) functionality recommended by the 3GPP on the S1 and X2 interface. Using a Security Gateway solution based on Intel technologies, Comms SPs can offer a full range of services without having to use multiple purpose-built systems.

This paper describes the technologies required to enable Security Gateway technologies to support Comms SP production deployments.

## Market Opportunity

A Security Gateway implements IPsec functionality on the S1 interface between the eNodeB and mobile core and also on the X2 interface between eNodeBs. The main drivers for implementing Security Gateway on Intel architecture are:

- **Equipment refresh**. Security Gateways have been implemented on fixed-function boxes which may be nearing end of life. Implementing this function on common off-the-shelf servers (COTS) may provide capital expense (CapEx) savings.
- **Distributed packet core**. There are a number of compelling reasons why mobile core functions are being pushed to the RAN. MEC allows content, services, and applications to be accelerated, increasing responsiveness from the network's edge. The mobile subscriber's experience will be enriched through efficient network and service operations based on insight into the radio and network conditions. This could require that Evolved Packet Core (EPC) functions be located closer to the RAN, where they could coexist with the Security Gateway on COTS hardware. 5G low latency use cases, such as autonomous driving, could also push Comms SPs to adopt a more distributed model for Packet Core functions.
- **Distributed Central Office**. Many operators are looking at re-architecting the Central Office and leveraging Cloud technologies to accelerate time to market for new services. They are looking to move to commodity infrastructure. Initiatives like CORD (Central Office Re-architected as a Data Center)[4] are looking to a distributed architecture to provide "Everything as a Service."

3GPP 33.310 recommends using IPsec for authentication and encryption of IP traffic on the S1 interface to the Packet Core and on the X2 interface between eNodeBs. Today, however, this is not mandatory. The IKEv2 authentication feature of IPsec is recommended in the specification.

In a recent report, IHS[5] provides a good snapshot of the market opportunity for mobile backhaul equipment, which is expected to show steady growth through 2020. Security Gateway elements would be a percentage of the IP Router subsegment. Table 1 shows worldwide backhaul revenue for the 2014 to 2020 period.

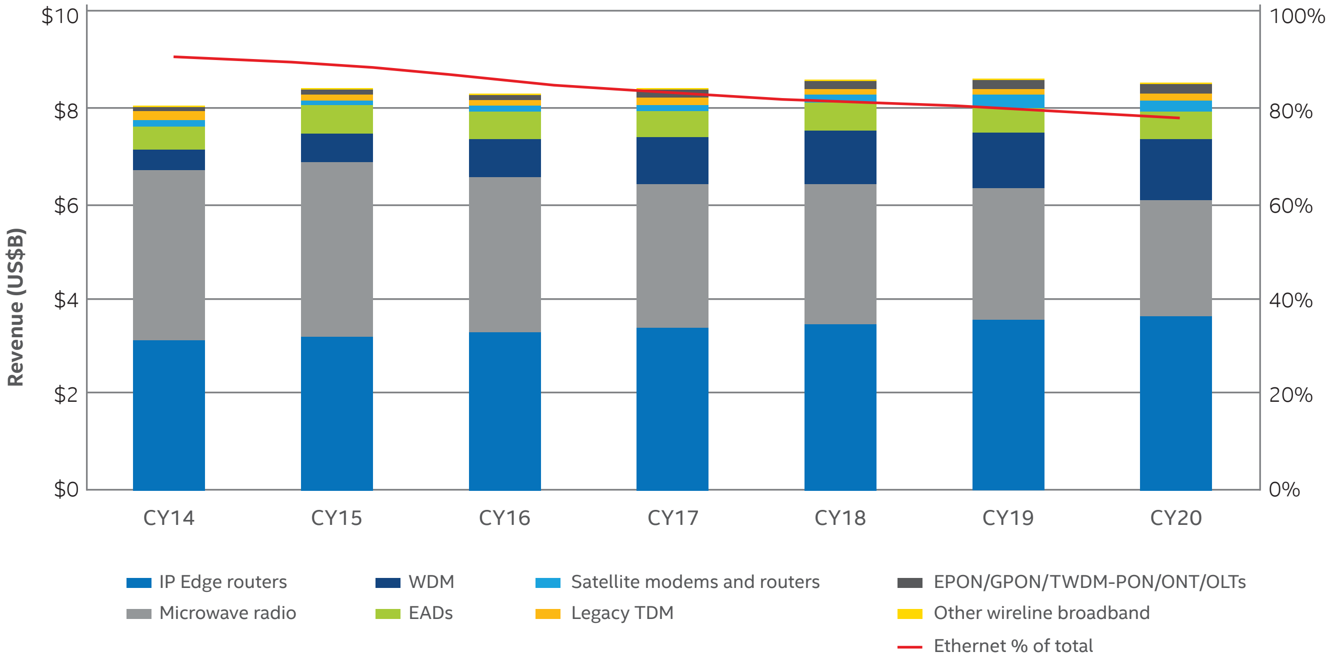


**Table 1.** Projected worldwide macrocell mobile backhaul equipment revenue

The IHS report indicates that Long-Term Evolution (LTE) acts as the final trigger for transitioning to an all-IP/Ethernet backhaul. It goes on to state that operators trust that all-Ethernet is the means to provide LTE/LTE-A and future 5G networks with backhaul bandwidth and are making deployments based on these plans.[6]

## Industry Challenges

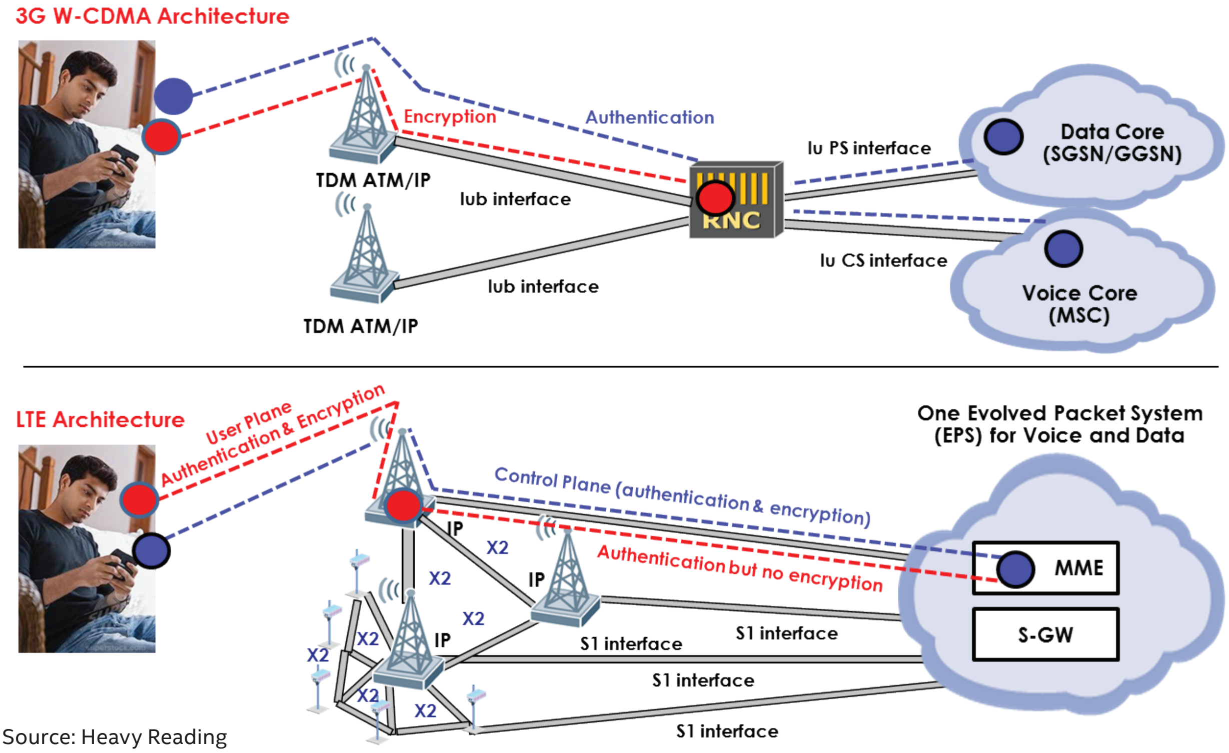
Security remains a key impediment to implementing virtualized mobile edge technologies. When operators rolled out 3rd Generation (3G) mobile networks, security was built into the network from the base station to the Radio Network Controller (RNC). The connection between the base station and the core network was often over E1 or DS1 interfaces, which are secure technologies. With the advent of General Packet Radio Services (GPRS), and continuing toward LTE, user demand stimulated Internet traffic tremendously, causing Comms SPs to tackle the challenge of blocking malicious traffic. An example of this evolution is shown in Figure 1, which provides a comparison between encryption in 3G and LTE networks.

Current mobile network deployments may not have implemented IPsec on the mobile backhaul. Per a Heavy Reading whitepaper,[7] only 15 percent of the world's LTE cell sites supported IPsec at the end of 2013. Heavy Reading predicts that has grown to 35 percent at the end of 2015 and will reach 53 percent by the end of 2017. In the cases where Comms SPs did implement IPsec, they may have implemented the function using an IP edge router, which is typically a fixed-function appliance. In general, fixed-function appliances can take a long time to deploy, are expensive to operate, and do not easily allow an operator to introduce services quickly. These fixed-function appliances often use network processors to handle the routing and security processing.

The IPsec functionality could also be implemented as part of the EPC solution. IPsec is a compute-intensive algorithm, which could be offloaded to hardware accelerator add-in cards or on the network interface card (NIC).

Two security concerns according to the report from Heavy Reading are:

- An attacker that is able to intervene in the network at the cell site or at any other point on the S1 or X2 interface might gain access to the clear text stream leading potentially to access to the network.
- Traffic is unencrypted across the backhaul in LTE, whereas it is encrypted in 3G, and the distributed architecture of the LTE network means the number of network elements that can potentially be impacted by an attacker is substantially larger than in 3G.



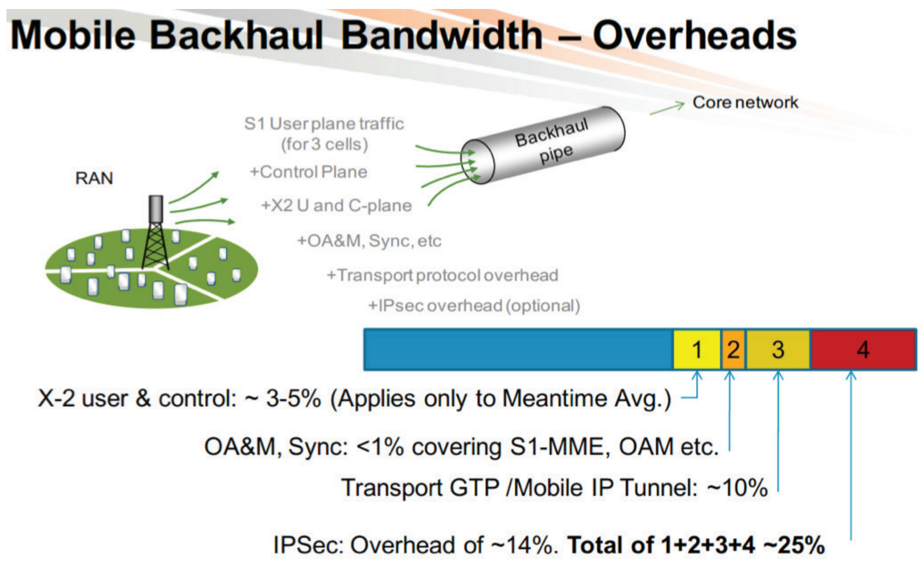
Source: Heavy Reading

**Figure 1.** Encryption comparison between 3G and LTE networks

There are also concerns around how IPsec deployment might affect overall network performance. IPsec causes an overhead of approximately 14 to 17 percent.[8] Figure 2 below shows the overhead impact of implementing IPsec without MPLS. In those cases where a 2 label MPLS stack (8bytes) is present, an additional three percent overhead would be added to the figures shown.

In a distributed architecture, the implementation of the Security Gateway may create X2 latency.[9] The X2 interface, which is new in LTE, was developed to assist with handover and to coordinate radio resource utilization. Many carriers do not implement encryption on the X2 interface as the cost of distributing the Security Gateway is high and the additional latency it introduces affects the user equipment (UE) performance.

The impact of X2 latency on user throughput has been investigated in connection with the dynamic coordination of resources using LTE-A and may also require evaluation when implementing IPsec. Figure 3 shows the impact of X2 delay on user throughput and assumes 3km/h users.



Mobile Backhaul Bandwidth – Overheads

X-2 user & control: ~ 3-5% (Applies only to Meantime Avg.)

OA&M, Sync: <1% covering S1-MME, OAM etc.

Transport GTP /Mobile IP Tunnel: ~10%

IPSec: Overhead of ~14%. **Total of 1+2+3+4 ~25%**

**Figure 2.** IpSec overhead on S1 and X2 interfaces

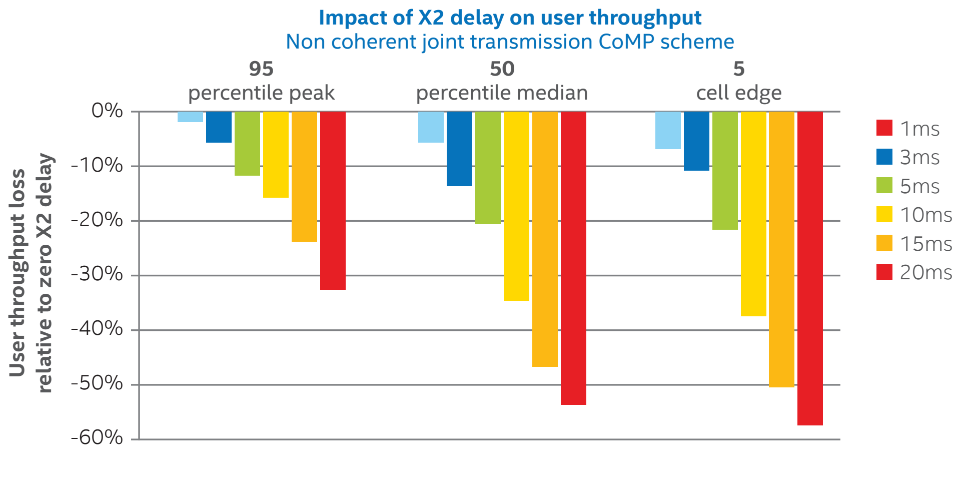


**Figure 3.** Impact of X2 delay on user throughput with CoMP scheme

Source: http://www.cisco.com/web/ME/expo2011/saudiarabia/pdfs/LTE_Design_and_Deployment_Strategies-Zeljko_Savic.pdf

Source: http://cbnl.com/sites/all/files/userfiles/files/Backhauling-X2.pdf

## State of the Industry

There are virtualized network solutions for Security Gateways available today; however, adoption is not widespread. Comparisons of Security Gateway elements, between physical functions and those running virtualized, do not focus on the flexibility benefits of virtualization. There is some evidence that Comms SPs are considering virtualized network elements, especially with the advent of distributed architectures supported by MEC and 5G. As stated above, many carriers do not implement encryption on the X2 interface for reasons of cost, performance and latency.  It is expected, however, that you will see distributed Security Gateway for X1 when the carriers distribute the EPC.

There are a range of vendors providing a virtualized solution on COTS, including offerings from Clavister,[10] 6Wind,[11] RadiSys,[12] and F5.[13]

By adopting industry-standard servers, Comms SPs can also take advantage of Moore's Law and realize ongoing improvements in server performance currently seen in IT data centers. This addresses the growing demand for processing while minimizing the impact on their operations.

Intel is contributing to several open source communities, including Open vSwitch*,[14] OpenDaylight*,[15] and OpenStack*[16] in order to drive open source integration efforts, such as the Intel® Open Network Platform (Intel® ONP) Server and the Open Platform for NFV* (OPNFV*),[17] and to support the growth of the key technologies. Intel is also working with ecosystem partners and suppliers on proofs of concept to validate end-to-end solutions that demonstrate the capabilities and maturity of the technologies. These end-to-end solutions will provide the industry with visibility into the gaps impeding broader adoption of virtualized solutions using SDN/NFV technologies for mobile Comms SPs' services.

## Intel's Role in Addressing Market Pain Points

For market adoption of new technologies, the business drivers for the technology are problem resolution, cost savings, or new service innovation. Intel is driving the ecosystem that will make NFV a reality. Intel is providing significant technology innovation and contributing to the ecosystem that will enable virtualized network functions and routing applications to scale more efficiently to deliver end-to-end services. A common software approach to programming virtualized functions and facilitating the routing between these functions will provide the ability to scale traffic in a more efficient manner.

Service agility and flexibility are key benefits for deploying a virtualized solution. A distributed network architecture on a bank of COTS servers would allow the Comms SP to scale up and down different services depending on traffic utilization. The current deployments are not flexible in coping with traffic changes.

For network elements, such as Security Gateways, current challenges include throughput, latency, and jitter performance. With respect to IPSec throughput, Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) or Intel® QuickAssist Technology performance can also be improved by data acceleration methods such as:[18]

- Core Pinning
- PCIe* Pass through
- Single Root I/O Virtualization (SR-IOV)
- Accelerated Virtual Switches (vSwitches)

Intel is making it easier to scale compression and cryptography capacity through Intel QuickAssist Technology, which has built-in acceleration for common workloads, including packet forwarding, bulk cryptography, and compression. These capabilities, available on COTS servers, are a more flexible alternative to purpose-built hardware. Performance throughput of approximately 255 million packets per second (MPPS) of L3 forwarding and 80 gigabits per second (Gbps) of IPsec acceleration have been demonstrated on servers with dual Intel® Xeon® processor E5-2600 v2 product family and Intel® Communications Chipset 89xx Series. Please review this whitepaper for more information.

http://www.intel.ie/content/dam/www/public/us/en/documents/solution-briefs/scaling-acceleration-capacity-brief.pdf

Intel continues to expose features, such as Core Pinning, which come under the Enhanced Platform Awareness (EPA)[19] feature set, in OpenStack. Core Pinning can be specified as a CPU policy. Intel is also ensuring instruction extensions (for example, Intel AES-NI) are exposed using the OpenStack Nova libvirt driver. PCIe Pass through and SR-IOV can also be configured using the OpenStack Nova configuration file.

Review this whitepaper for more details on these features: https://networkbuilders.intel.com/docs/openStack_Kilo_wp_v2.pdf

Intel has also been involved in developing a number of preferred methods for real-time processing to minimize jitter and latency.

More details on these methods can be found at: http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/real-time-virtualization-on-xeon-server-white-paper.pdf

Intel continues to be an active participant in communications-focused, industry-wide open standards and open source projects. As part of these NFV-related efforts, Intel is involved in a real-time KVM project within the OPNFV community.

KVM work can be found at: https://wiki.opnfv.org/display/kvm/Nfv-kvm.

KVM best-known methods are summarized here: https://wiki.opnfv.org/display/kvm/Nfv-kvm-tuning.

### SDN/NFV for Security Gateway Network Functions

SDN and NFV promise to revolutionize the industry by driving reduced cost and increased service revenue. However, the transition to NFV will require a number of new, disparate technologies to work collaboratively. The maturity of these technologies is captured in Intel's Network Maturity Model for Comms SPs.[20]

## Technology Overview

The following sections describe the relevant Intel technology contributions in more detail.

### Traditional Solution

3GPP requirements are implemented using an IPsec tunnel initiated at the eNodeB carrying the bearer and signaling traffic, which can be decrypted by a Security Gateway. This function could be implemented using an IP edge router, which typically uses physical cabling and preconfigured static routing mechanisms. Lead times are long for these dedicated appliances, and deployment can be complex. In addition, proprietary platforms are not interchangeable among applications from different vendors.

## Intel Technologies and Ecosystem Enablers

For network Comms SPs that intend to deploy Security Gateway solutions, the benefits provided by Intel architecture and related ecosystem contributions are significant. Intel's product performance, unique platform awareness capabilities, software portability from network edge to core, and contributions to open source communities and standards bodies all support the realization of a Security Gateway solution.

Intel's chipset and platform capabilities enable network functions to facilitate efficient resource utilization via optimal performance and programmability. Intel continues to work with the ecosystem to enable optimal use of these capabilities with seamless integration by the NFV/SDN architecture.

Virtualized network functions benefit from the ongoing efforts to enable and enhance the horizontal platform. Platform capabilities, based on Intel's chipsets supporting open source ingredients (including Data Plane Development Kit (DPDK)[21] and Open vSwitch[22]), are leveraged by Comms SPs to achieve the benefits of NFV. The horizontal platform provides the foundation for a virtualized infrastructure. Capabilities such as CPU/Memory virtualization, I/O virtualization, workload isolation, and acceleration are the foundation of NFV.[23]

Intel has also worked closely with ecosystem participants to develop Reference Architectures that maximize the value of NFV. These architectures capitalize on open, industry-standard technologies to help Comms SPs reduce vendor costs, more easily produce scalable solutions, and accelerate time to market for new solutions. Purpose-built devices require Comms SPs and their hardware partners to qualify each version of a device, whether it is produced to offer a distinct service or to accommodate a different number of users. With Security Gateways based on industry-standard technologies, Comms SPs can produce, and qualify, fewer variations for their solutions. The virtualized environment allows them to support different services and to scale more easily.

### Intel's Chipset and Architecture Capabilities

Specific Intel capabilities that drive optimal performance and security for these functions are identified below. Some of these capabilities include Enhanced Platform Awareness, Intel QuickAssist Technology, Intel® Trusted Execution Technology (Intel® TXT),[24] Intel AES-NI, Intel® Resource Director Technology (Intel® RDT),[25] among others.

Specifically for accelerating IPsec on Intel architecture, Intel has developed two options:

- Intel AES-NI instructions
- Hardware offload using Intel QuickAssist Technology

#### Intel Advanced Encryption Standard New Instructions

Intel AES-NI was developed specifically to accelerate the AES algorithm utilized by IpSec. Intel has developed a plug-in for the Linux* kernel crypto framework, which is the module within the Linux kernel that manages cryptographic operations. This kernel-enabling work has enabled applications (for example, Openswan*) to take advantage of Intel AES-NI more easily. For more information around implementing IpSec using Intel AES-NI, please see this whitepaper:

http://www.intel.ie/content/dam/www/public/us/en/documents/white-papers/aes-ipsec-performance-linux-paper.pdf

Also Intel has developed a Multi-Buffer Crypto for IPsec Library, a set of functions that implement the computationally intensive authentication and encryption algorithms for IPsec. For more information, please see:

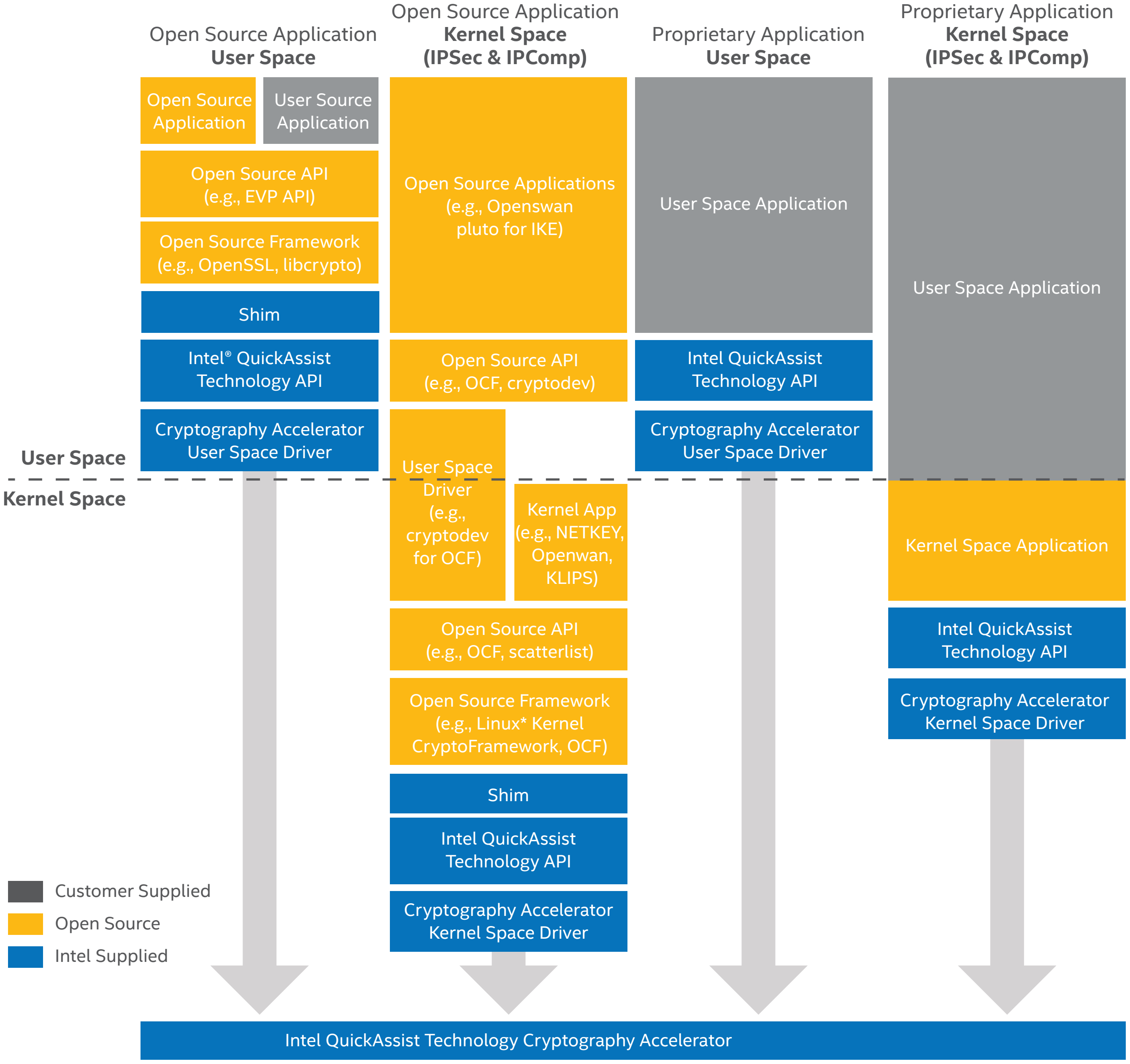
http://www.intel.ie/content/dam/www/public/us/en/documents/white-papers/fast-multi-buffer-ipsec-implementations-ia-processors-paper.pdf

#### Intel QuickAssist Technology

Intel is making it easier to scale cryptography capacity using Intel QuickAssist Technology. Performance throughput of approximately 255 million packets per second of L3 forwarding and 80 gigabits per second of IPsec acceleration have been demonstrated on servers with dual Intel Xeon processor E5-2600 v2 product family and Intel Communications Chipset 89xx Series.

The Intel Communications Chipset 89xx Series has built-in cryptographic acceleration to speed up SSL/TLS workloads. It encrypts/decrypts SSL/TLS records, helps establish SSL/TLS connections by generating random numbers, and accelerates public key cryptographic algorithms, such as RSA, DSA, Diffie-Hellman, ECDH, and ECDSA. There are a number of mechanisms for leveraging Intel QuickAssist Technology. Utilizing open source frameworks like IPsec Netkey (IP stack built into the kernel). Intel QuickAssist Technology provides high flexibility because it supports diverse workloads, embraces open source software and runs in both kernel and user space to best accommodate the implementation provided by the open source community. This is illustrated in Figure 4.

Intel QuickAssist Technology implementation examples are shown below:



Open Source Application User Space
Open Source Application Kernel Space (IPSec & IPComp)
Proprietary Application User Space
Proprietary Application Kernel Space (IPSec & IPComp)
Open Source Application
User Source Application
Open Source API (e.g., EVP API)
Open Source Framework (e.g., OpenSSL, libcrypto)
Shim
Intel® QuickAssist Technology API
Cryptography Accelerator User Space Driver
Open Source Applications (e.g., Openswan pluto for IKE)
Open Source API (e.g., OCF, cryptodev)
User Space Driver (e.g., cryptodev for OCF)
Kernel App (e.g., NETKEY, Openwan, KLIPS)
Open Source API (e.g., OCF, scatterlist)
Open Source Framework (e.g., Linux* Kernel CryptoFramework, OCF)
Shim
Intel QuickAssist Technology API
Cryptography Accelerator Kernel Space Driver
User Space Application
Intel QuickAssist Technology API
Cryptography Accelerator User Space Driver
User Space Application
Kernel Space Application
Intel QuickAssist Technology API
Cryptography Accelerator Kernel Space Driver
User Space
Kernel Space
Customer Supplied
Open Source
Intel Supplied
Intel QuickAssist Technology Cryptography Accelerator

**Figure 4.** Intel® QuickAssist Technology implementation examples (SSL)

## DPDK and IpSec

An IpSec Security Gateway application is now available as part of the DPDK set of libraries[26] (developed to accelerate packet processing on Intel architecture). It utilizes a cryptodev API, which was developed to consolidate all crypto functions. This application can leverage Intel AES-NI or Intel QuickAssist Technology.

Table 2 provides some additional links to the features described in the previous sections.

| | |
|---|---|
| Intel® Resource Director Technology | http://www.intel.com/content/www/us/en/architecture-and-technology/resource-director-technology.html |
| Intel® QuickAssist Technology | http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/communications-quick-assist-paper.pdf<br>https://01.org/packet-processing/intel®-quickassist-technology-drivers-and-patches |
| Intel® Trusted Execution Technology | http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/malware-reduction-general-technology.html<br>http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/trusted-execution-technology-security-paper.html<br>http://www.intel.com/content/dam/www/public/us/en/documents/guides/intel-txt-software-development-guide.pdf |
| Intel® Advanced Encryption Standards New Instructions | https://software.intel.com/en-us/articles/intel-advanced-encryption-standard-instructions-aes-ni<br>http://www.intel.com/content/dam/www/public/us/en/documents/white-papers/aes-ipsec-performance-linux-paper.pdf |
| Enhanced Platform Awareness | https://software.intel.com/sites/default/files/managed/8e/63/OpenStack_Enhanced_Platform_Awareness.pdf<br>https://networkbuilders.intel.com/docs/openStack_Kilo_wp_v2.pdf |
| Open vSwitch* | https://networkbuilders.intel.com/docs/open-vswitch-enables-sdn-and-nfv-transformation-paper.pdf |
| Data Plane Development Kit | http://www.intel.com/content/www/us/en/intelligent-systems/intel-technology/dpdk-packet-processing-ia-overview-presentation.html<br>https://networkbuilders.intel.com/docs/aug_17/Future_Enhancements_to_DPDK_Framework.pdf |
| Hardware Offload | http://www.intel.com/content/www/us/en/ethernet-products/controllers/overview.html |

**Table 2.** Links to specific capabilities.

## Open Source and Standards

Intel is driving software contributions and broad market capabilities through open source communities.

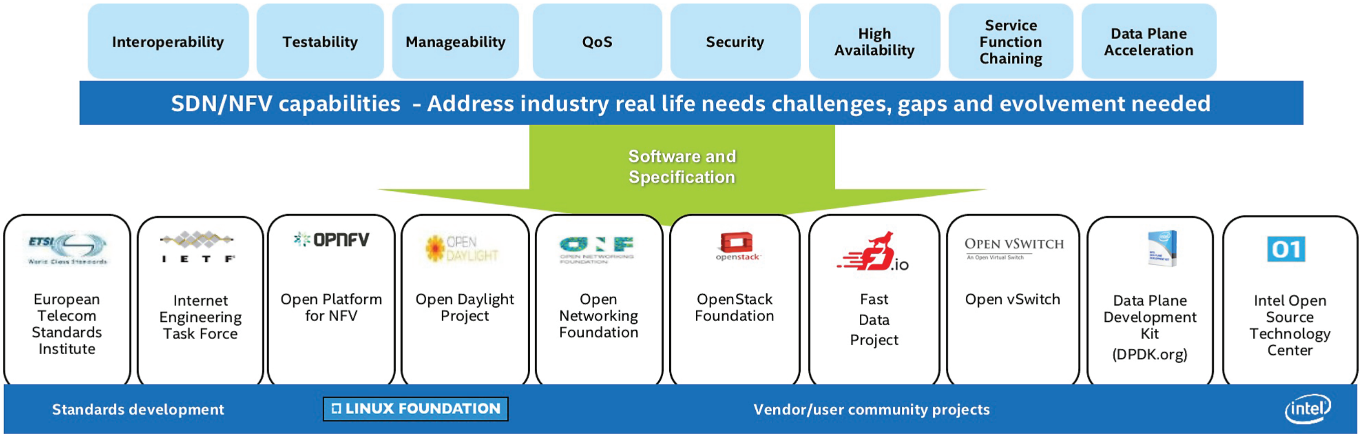

Interoperability
Testability
Manageability
QoS
Security
High Availability
Service Function Chaining
Data Plane Acceleration
SDN/NFV capabilities - Address industry real life needs challenges, gaps and evolvement needed
Software and Specification
ETSI
European Telecom Standards Institute
IETF
Internet Engineering Task Force
OPNFV
Open Platform for NFV
OPEN DAYLIGHT
Open Daylight Project
ONF
Open Networking Foundation
openstack
OpenStack Foundation
fd.io
Fast Data Project
OPEN VSWITCH
Open vSwitch
Data Plane Development Kit (DPDK.org)
01
Intel Open Source Technology Center
Standards development
LINUX FOUNDATION
Vendor/user community projects
intel

**Figure 6.** Intel's involvement in open source and standards.

Intel invests in 10 Open Source and standards initiatives shown on Figure 6, from the ETSI-NFV group to Intel's own packet processing project on 01.org.

Contributions are driven both by the market and by specific customer requirements. This includes providing real-life deployment and business needs, targeting performance metrics, closing development gaps, and enabling the management tools needed to ensure service levels.

Intel's contribution is across the entire spectrum, including technical specifications, code development, testing and benchmark tools and reference platforms.

## Intel® Open Network Platform Reference Architecture

Intel ONP Server is an enablement program with a Reference Architecture integrating Intel's hardware and open source software ingredients for easier ecosystem adoption. One of the key objectives of Intel ONP Server is to align and optimize key Open Community software ingredients for architects and engineers targeting high-performing SDN and NFV solutions. Intel ONP provides a convenient reference platform to evaluate the latest performance contributions for OpenStack,[26] DPDK,[28] and accelerated OVS.[29]

## Intel® Network Builders

Intel recognizes that enabling network transformation will require a strong ecosystem of partners. The Intel® Network Builders community (www.networkbuilders.intel.com) has more than 180+ partners developing SDN/NFV solutions on Intel architecture (see Figure 7). Within this community, there are more than 30 software vendors for critical SDN/NFV use cases. The work of the community extends to proofs of concept, reference architectures, and trials. With the help of its ecosystem partners, Intel remains committed to the development of technology solutions and capabilities that will improve the performance of virtualized network functions for Comms SPs.

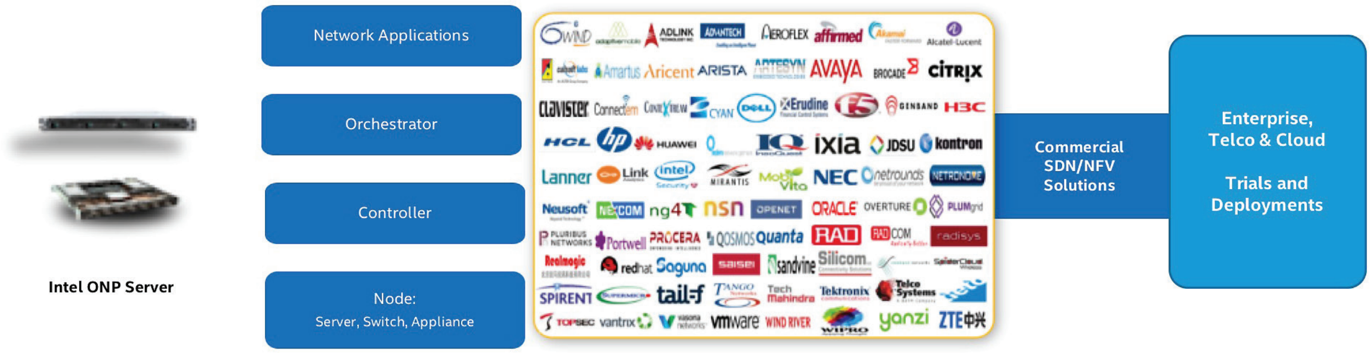


**Figure 7.** Intel® Network Builders

## Additional Information

### Related efforts in Intel:

- OpenDaylight contribution and IETF efforts on NSH
  https://tools.ietf.org/pdf/draft-ietf-sfc-nsh-00.pdf
  https://wiki.opendaylight.org/view/Project_Proposals:Service_function_chaining
- Openstack EPA contributions:
  https://01.org/sites/default/files/page/openstack-epa_wp_fin.pdf
  https://networkbuilders.intel.com/docs/openStack_Kilo_wp_v2.pdf
- Intel Open Network Platform
  https://01.org/packet-processing/intel-onp-servers

### Intel Network Builders:

- https://networkbuilders.intel.com/docs/Intel-Virtual-VOIP-Orch-RA.pdf
- https://networkbuilders.intel.com/solutionscatalog/session-border-controller-74
- https://www.brighttalk.com/webcast/12229/181563

### MEC Whitepaper

https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/Mobile-edge_Computing_-_Introductory_Technical_White_Paper_V1%2018-09-14.pdf

[1] https://portal.etsi.org/Portals/0/TBpages/MEC/Docs/Mobile-edge_Computing_-_Introductory_Technical_White_Paper_V1%2018-09-14.pdf

[2] Ericsson Mobility Report, June 2015. http://www.ericsson.com/res/docs/2015/ericsson-mobility-report-june-2015.pdf

[3] http://www.fiercewireless.com/tech/story/study-nfv-market-will-hit-116b-2019/2015-07-20

[4] http://onrc.stanford.edu/protected%20files/PDF/ONRC-CORD-Larry.pdf

[5] https://technology.ihs.com/576751/macrocell-mobile-backhaul-equipment-market-tracker-regional-h1-2016

[6] https://technology.ihs.com/576751/macrocell-mobile-backhaul-equipment-market-tracker-regional-h1-2016

[7] https://forums.juniper.net/jnet/attachments/jnet/IndustrySolutionsEMEA/286/1/The%20Security%20Vulnerabilities%20of%20LTE%20Opportunity%20and%20Risks%20for%20Operators.pdf

[8] http://www.cisco.com/web/ME/expo2011/saudiarabia/pdfs/LTE_Design_and_Deployment_Strategies-Zeljko_Savic.pdf

[9] http://cbnl.com/sites/all/files/userfiles/files/Backhauling-X2.pdf

[10] https://www.clavister.com/telecom/core-security/

[11] http://www.6wind.com/solutions/network-security/

[12] http://investor.radisys.com/phoenix.zhtml?c=90237&p=irol-newsArticle&ID=1482843

[13] https://f5.com/resources/white-papers/ten-essentials-for-securing-lte-networks

[14] http://www.openvswitch.org

[15] http://www.opendaylight.org

[16] http://www.openstack.org

[17] http://www.opnfv.org

[18] http://www.intel.com/content/www/us/en/embedded/technology/quickassist/overview.html

[19] https://software.intel.com/en-us/articles/openstack-enhanced-platform-awareness

[20] http://www.intel.com/content/www/us/en/communications/service-provider-network-maturity-paper.html

[21] http://dpdk.org/

[22] http://openvswitch.org/

[23] http://www.intel.com/content/www/us/en/virtualization/virtualization-technology/intel-virtualization-technology.html

[24] http://www.intel.com/content/www/us/en/architecture-and-technology/trusted-execution-technology/trusted-execution-technology-security-paper.html

[25] http://www.intel.com/content/www/us/en/architecture-and-technology/resource-director-technology.html

[26] http://www.dpdk.org/doc/guides/sample_app_ug/ipsec_secgw.html

[27] http://www.openstack.org

[28] http://www.dpdk.org

[29] http://openvswitch.org

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL® PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER, AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked "reserved" or "undefined." Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request. Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order. Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or by visiting Intel's Web site at www.intel.com.