



SENDATE-TANDEM

Project ID: C2015/3-2

Start Date: 1 April 2016

Closure date: 31 September 2019

Partners:

Astellia, France
 atesio GmbH, Germany
 B<>com Fondation, France
 CityPassenger SA, France
 Creonic GmbH, Germany
 Fraunhofer FOKUS, Germany
 Gemalto SA, France
 ID Photonics GmbH, Germany
 INRIA (Institut National de Recherche en Informatique et en Automatique), France
 Institut Mines Télécom, France
 itWatch, Germany
 Montimage, France
 Nokia Deutschland AG, Germany
 Nokia Bell Labs, France
 Orange SA, France
 Prove & Run S.A.S., France
 TAGES SolidShield, France
 Technical University Berlin, Germany
 Thales SIX GTS France SAS, France
 University of Erlangen, Germany
 University of Stuttgart – IKR, Germany
 University Rennes 1, France
 VectraWave, France
 VirtuOR SARL, France

Co-ordinator:

Dr. Yvan Pointurier

Nokia Bell Labs, France

E-Mail: yvan.pointurier@nokia.com

Project Website

www.celticplus.eu/project-sendate-tandem

www.sendate.eu

Tailored Network for Data cEnters in the Metro

“SENDATE-TANDEM” addresses the challenge for a new network infrastructure with reference to high volatile data traffic of mobile linked objects. A dynamic switching and a reliable transport of huge amounts of data as well as a handover of sensible, time critical application data without any interruptions must be provided between data centers with security guarantees.

Main focus

Data centers: Current centralized DCs offer high processing power, huge storage capacities and performance but due to the big distance to end users they show long response times and furthermore use the network as static transport medium only. SENDATE-TANDEM focuses on distributed data centers for enhanced flexibility and lower latency experienced by end-users.

Networks: Today’s networks lack automation, require specific, separate processes and operations for the telecom resources on the one hand and IT resources on the other hand, and generally lack flexibility to operate these resources. Time-to-market for new services is also too long. Optical transport networks are too static and also lack flexibility. SENDATE-TANDEM focuses on automated, flexible, dynamic, pro-active networks that can reconfigure themselves even before a security breach is detected.

Security: distinct contributions do not help to achieve a continuous end-to-end security path between multiple tenants but merely offer a toolkit of available security functions that may or may not combine smoothly. The fusion of telecommunication networks and IT Infrastructure, already observed for many years, progresses further. Meanwhile the most important

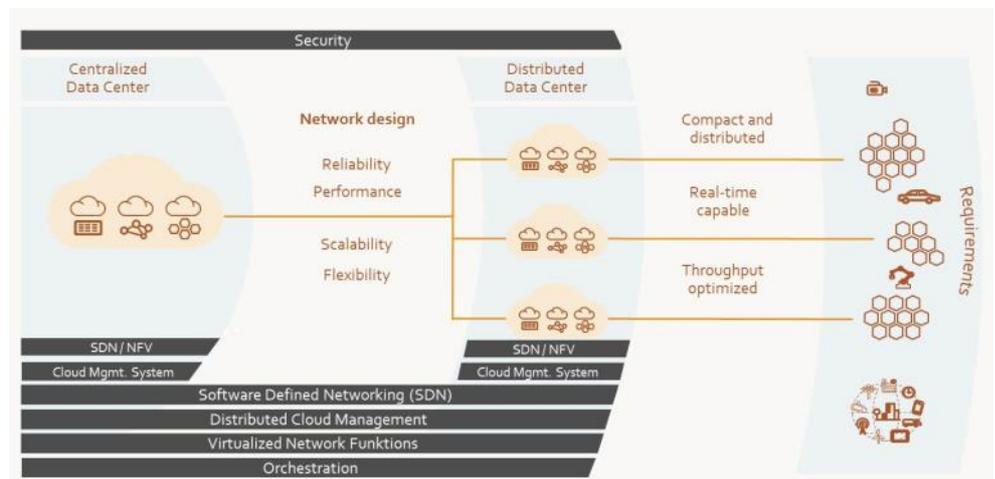
control centers of the Internet are data centers. There both business and private data are stored, operated, forwarded and analyzed. SENDATE-TANDEM will focus on guaranteeing network security, including for instance control plane securization and virtualization of the security functions.

Approach

Within the metro network, essential elements are virtualized: integrated nodes consisting of traditional DCs (RAM, processor) but also e.g. virtualized DSL- and radio access (vRAN) network elements or IP-router and optical network elements like cross-connects. Virtualization shall lead to a flexible arrangement of single modules and to a dynamic provision of resources according to application demands. Here latency and bandwidth but also QoS classes and findings from simulative traffic investigations will be considered.

Furthermore a common control plane is needed for an optimized control of network elements across levels. The first underlying assumption is based upon a flexible control plane and develops an application, which is able to adapt the network from one load status to another. The second assumption goes for full flexibility from scratch within definition of control plane architecture, intending to turn today’s networks into a flexible platform for future services and applications.

The convergence of IT (Information Technology) and OT (Operational Technology) networks, as well as the extended connectivity provided to new endpoints (e.g., connected objects) will require the provision of metamorphic networks, able to adapt and accommodate various endpoints and communication protocols or media. In SENDATE, we aim to provide a secure



networking infrastructure as well as security services to enable end-to-end connectivity for multi-tenant/multidomain clouds.

Achieved results

An orchestrator has been developed and is called the SENDATE MANO. It allows automatic deployment of SDN controller modules and VNF as applications.

An SDN controller has been developed and integrates new data models for high speed reconfiguration. An end-to-end optical light path over multi domains and multi equipment has been established in Orange Labs to show the interoperability between two SDN controllers over two domains (with equipment by different makers) without optical regeneration. This provides a new way to established easily on heterogeneous domains with multiple sources of equipment's an end-to-end optical light path.

A real-time testbed with a flexible optical transmitter was built to interconnect data centers, where wavelength and, resp. the baudrate, can be changed in less than 500 ns, resp. 12 μ s, for next-generation highly dynamic optical networks.

A proof-of-concept on advanced monitoring and machine learning concepts has been demonstrated. The use case shown was the classification of different types of mechanical stress on optical fiber, which can buy time to anticipate a fiber break and hence reroute traffic at lower cost before any performance degradation is visible.

An algorithm was implemented to enable secure path computing and enforcement by solving the multi-provider security-aware virtual network embedding problem and implementation of a resilient security function chaining solution as well as various. In addition to that various software defined security functions were defined, such as the Software Defined Firewall.

Implementation of the IAMaaS, the SSLaaS (formal verification + monitoring) solution and the SPaaS (Software Protection as a Service) solution.

Polar Codes as a class of forward error correction codes archive the theoretical limit for error correction performance. Creonic and Nokia developed a hardware Polar codec for FPGA and ASIC applications. Due to the target system-level knowledge of Nokia, Creonic was able to develop the best hardware design (in sense of performance and energy consumption). The resulting products were the world-first multi-gigabit per second Polar decoders for FPGA. The ASIC design reaches 100Gbit per second which is a world record.

A solution was developed to store and execute critical, verified system code in a trustworthy runtime environment so it cannot be altered by an attacker. This was achieved by virtually dividing processors and their periphery into an unsecure and a secure part. The secure part runs a security-oriented operating system, the Trusted Execution Environment. The existing network element's operating system runs in the non-

secure part of the processor.

Concepts have been developed that allow data streams from various sources to be aggregated on sub-port rates without explicit packet processing (OIF FlexE). These data streams are then adapted to the available, dynamic transport channels using standard Optical Transport Network (OTN) mappings (ITU-T FlexO), which ensures carrier grade implementation. Both implementations were evaluated on the NOKIA 1830 PSS system that provides OTN transport & aggregation.

- ◆ 82 technical articles, including 1 keynote speech (Design of Reliable Communication Networks, 2019)

- ◆ 12 patents

Contributions to standardization bodies:

- ◆ CyberSecurity PPP (ECSO)

- ◆ OASIS XACML

- ◆ ETSI / NFV

- ◆ 3GPP SA#3

- ◆ OIF PLL:

- ◆ oif2018.202.00: When the road gets rough - Surface Impact on Signal Propagation

- ◆ oif2018.124.00: CEI-112G: PAM-4 FEC requirements

- ◆ oif2016.026.00: Need to cover higher insertion loss in CEI-56G-LR-PAM4

- ◆ OIF 400ZR Project:

- ◆ OIF2017.325.00; Proposal for HD-FEC for 400ZR project

- ◆ OIF2017.326.00; 400ZR link engineering options with HD-FEC

- ◆ ITU-T Q6/15

- ◆ Contributions to open source

- ◆ C0699 on parameter values for 100G DP-DQPSK application code

- ◆ OpenROADM

- ◆ Linux Foundation OpenDayLight Transport-PCE

- ◆ Open Networking Foundation

- ◆ (i) ONOS/Open & Disaggregated Transport Networks

- ◆ (ii)T-API

Impact

The white paper on Security pushed by SENDATE (including a well-defined slicing concept) has the ambition to be used as a reference within the security community. Numerous products and product features, some of them world's first, were developed thanks to SENDATE, in particular, the first EAL7-certified SSL Network filter.

About Celtic-Plus

Celtic-Plus is an industry-driven European research initiative to define, perform and finance through public and private funding common research projects in the area of telecommunications, new media, future Internet, and applications & services focusing on a new „Smart Connected World“ paradigm. Celtic-Plus is a EUREKA ICT cluster and belongs to the inter-governmental EUREKA network. Celtic-Plus is open to any type of company covering the Celtic-Plus research areas, large industry as well as small companies

or universities and research organizations. Even companies outside the EUREKA countries may get some possibilities to join a Celtic-Plus project under certain conditions.

Celtic Office

c/o Eurescom, Wieblingen Weg 19/4

69123 Heidelberg, Germany

Phone: +49 6221 989 381

E-mail: office@celticplus.eu

www.celticplus.eu

