

## FOKUSinnovation

11 – 2009

++ Evolving Toward the Future Internet (FI) ++ Experimental Facilities & Tools ++ Future Internet Security ++

### NGN Evolution toward Future Internet

Fraunhofer FOKUS Pushes Research on NGN Evolution

The Internet is how global businesses and communities communicate. Behind the scenes, however, new demands have collided with old designs, resulting in a complex agglomerate of protocols and patches. These makeshift solutions are hard to manage, protect, or extend. Future Internet (FI) research aims at a fundamental Internet redesign.



At the same time, the world of mobile networks is moving toward all-IP based Next Generation Networks (NGNs) and Next Generation Mobile Networks.

How can the next generations of networks benefit from recent developments in future Internet research? This is the question being investigated by the Fraunhofer Institute FOKUS competence centers NET (Network Research) and NGNI (Next Generation Network Infrastructures), together with the TU Berlin department AV (Architektur der Vermittlungsknoten).

The joint Future Internet Laboratory (FI-Lab) supports rapid prototyping of FI technologies such as application-aware

networks, novel concepts for network security, and flexible network stacks. The Lab is an integral part of all major German and European Future Internet research facilities, including the BMBF (Federal Ministry of Education and Research) sponsored G-Lab. It is also part of the European Union funded Future Internet Research and Experimentation (FIRE) initiative, driven by projects such as OneLab, PII, and VITAL++.

#### Contact

Dr. Tanja Zseby | Prof. Dr. Thomas Magedanz  
tanja.zseby@fokus.fraunhofer.de  
thomas.magedanz@fokus.fraunhofer.de  
[www.fokus.fraunhofer.de/go/fi-lab](http://www.fokus.fraunhofer.de/go/fi-lab)

### G-Lab Deep

2<sup>nd</sup> Wave of Future Internet Projects

On September 1, 2009, Fraunhofer FOKUS and partners launched the G-Lab Deep project with funding from the German Federal Ministry of Education and Research. G-Lab Deep is a second-generation G-Lab project, scheduled to run for two years.

The project will focus on innovative composition approaches for efficient service and network cooperation in the Future Internet, and will place special emphasis on security.

The project team consists of the Fraunhofer competence centers NET and NGNI along with the Technische Universität Kaiserslautern (Professor Paul Müller), the Technische Universität Berlin (Professor Thomas Magedanz), and the Universität Duisburg-Essen (Professor Erwin Rathgeb). Researchers from Fraunhofer FOKUS will focus on network layer functional blocks for surveillance and detection, tools for efficient distributed network control, and cross-domain cross-layer resource federation frameworks.



Contact – Dr. Tanja Zseby  
tanja.zseby@fokus.fraunhofer.de

[www.g-lab-deep.de](http://www.g-lab-deep.de)

# Future Internet Infrastructures for FI Prototyping

## Toward Secure Identity Management in Future Internet Scenarios



Secure Identities for Future Internet Scenarios

In July 2009, the Secure Identities for Future Internet Scenarios project (SCIFIS) began work at its offices in the TU Berlin AV department (Architektur für Vermittlungsknoten). Part of the Fraunhofer innovation cluster "Sichere Identitäten (Secure Identities)" and the TU Berlin research project SI-KUZ (Sichere Identitäten für Kommunikationsszenarien der Zukunft), SCIFIS has the goal of developing methods, concepts, and prototypes for generic identity management in telecommunication and Internet environments. The goal is to develop and integrate a "Future Internet Identity Layer" into Next Generation Network and Future Internet architectures. This will enable a secure identification and authentication of end users, end systems, applications, service enablers, and network components. SI-KUZ is a joint project between the TU Berlin (AV, Entwurf und Testen kommunikationsbasierter Systeme, and Offene Kommunikationssysteme) and FOKUS.

**Contact** – Florian Deinert  
florian.deinert@tu-berlin.de

<http://id.open-ims.org>  
[www.sichere-identitaet.de](http://www.sichere-identitaet.de) (German)  
[www.av.tu-berlin.de](http://www.av.tu-berlin.de)

## The Future of Cyber Security

### Fighting Internet Attacks in the Era of Cloud Computing

The development of the Internet has been accompanied by boundless possibility – as well as severe risk. Malicious Internet activity has already affected many users. Cyber criminals, hackers, and spammers are rapidly adopting new attack vectors. This is why IT security is all about trust. One has to trust hardware, operating system, software vendors, and Internet providers. As the Internet moves toward shared storage and computing resources in clouds, dependencies on network infrastructure and remote services increase. And the more remote entities are used, the more one needs fast and stable access to services.

#### The Eye of the Hurricane

In cloud computing environments protection against attacks on infrastructure and service is essential. Dependence on network connectivity makes the threat of sophisticated DDoS attacks (Distributed Denial of Service) all the more in need of innovative solutions. A DDoS attack on a cloud would not only disrupt a user's Webpage access; it would disconnect him or her from all data and basic services – email, word processing, and so forth. Another growing threat is dedicated worms, which have an ideal breeding ground in cloud environments for spreading from one device to another.

#### Future Internet Security Solutions

In a world where heterogeneous entities under different administrative authorities need to work together, it is essential to protect infrastructures and services. This calls for close cooperation between network entities and applications.

Fraunhofer FOKUS has developed early detection tools to prevent sophisticated DDoS from disturbing service access. With the Distributed Context-aware Firewall

(D-CAF) providers of software, applications, and online services can assess data flows, while collaborative firewalls share valuation matrices that make it easy to distinguish "good" from "bad" user traffic. In this way, D-CAF blocks DDoS attacks while maintaining services for legitimate users.

Cyber security is all about trust. Just because a "friend" sends you something on Facebook or MySpace doesn't mean you should open it – one of the ways new worms are spreading is via social media. Fraunhofer FOKUS is developing technologies to track the perpetrators. The Worm Detection Software developed by the FOKUS NET team is able to distinguish real DNS traffic from a worm requesting access to your address book, and to make sure the latter is denied DNS services.

For more information on future cyber security and related research by Fraunhofer FOKUS, please visit us at [www.fokus.fraunhofer.de/go/net](http://www.fokus.fraunhofer.de/go/net)

**Contact** – Dr. Tanja Zseby  
tanja.zseby@fokus.fraunhofer.de

### TridentCom 2010

6<sup>th</sup> International Conference on Test-beds and Research Infrastructures for the Development of Networks & Communities – [www.tridentcom.org](http://www.tridentcom.org)

May 18-20, 2010, Berlin, Germany – Papers due November 15, 2009

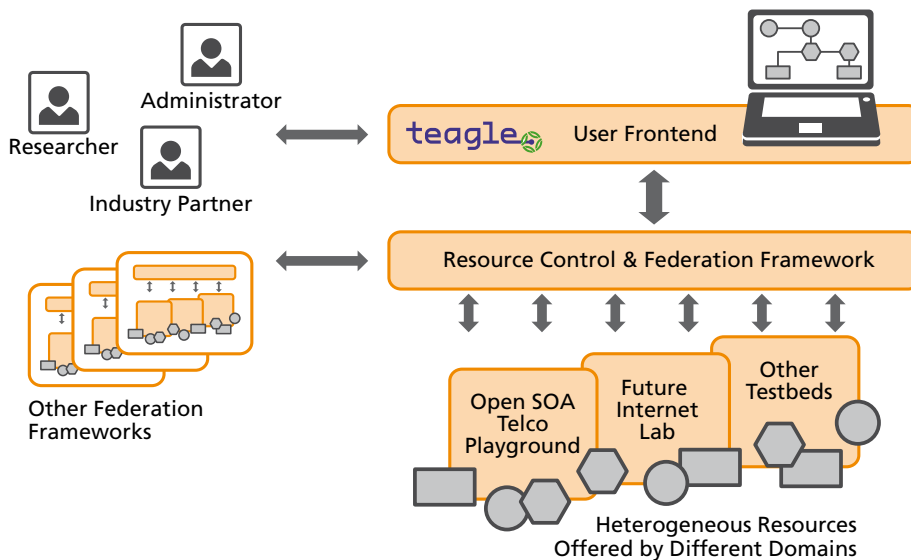


# Future Internet Infrastructures for FI Prototyping

## Future Internet Experimental Facilities

### Infrastructure as a Service and Resource Federation with Teagle

Researchers are working on Future Internet technology, but it is too soon to tell what the future holds in store. The highly complex field spans multiple technology domains and stakeholders along its value chain. Questions regarding large-scale cross-domain networking, distributed cross-layer service architectures, and infrastructure virtualization still need to be investigated, both in theory and practice. A clear understanding of how the Future Internet will work, as well as how existing and Future Internet solutions will operate together, is the key to its commercial deployment, adoption, and success.



The European Commission is addressing these needs by stimulating flexible resource provisioning and federation mechanisms for large-scale Future Internet testing environments.

The federation framework developed by the European FIRE project Panlab (or the Pan-European Laboratory) makes available multi-domain testbeds providing heterogeneous cross-layer infrastructures. Now, a pan-European testbed resource federation framework is available via a central resource-provisioning tool called "Teagle". The first prototype version of Teagle was presented in September 2009 to the European Commission and is now being recommended for use in upcoming Future Internet R&D projects. Resources provided by Panlab partner organizations, such

as Fraunhofer FOKUS or EICT (European Center for Information and Communication Technologies), can be booked on demand via Teagle. Among the resources currently available: general-purpose physical and virtual machines, modular NGN (Next Generation Network) and SDP (Service Delivery Platform) software systems as well as related test tools and services.

Teagle was developed and is maintained by a joint team from Fraunhofer FOKUS and the Technische Universität Berlin (department AV).

**Contact** – Sebastian Wahle  
sebastian.wahle@fokus.fraunhofer.de

[www.panlab.net](http://www.panlab.net)  
[www.fire-teagle.org](http://www.fire-teagle.org)

## Functional Composition

### Experiments in PlanetLab Europe

Since its invention, the Internet has been shaped by the end-to-end paradigm, which has kept networks „application agnostic.“ Over the years, however, pressing demands for quality, security, and mobility have produced a plethora of patchwork solutions that can no longer fulfill the end-to-end doctrine. One of the aims of Future Internet research has been to find new models for making networks “application aware.”

Fraunhofer FOKUS is now working on its own solutions using functional composition technology. It positions flexible functions in network nodes that can be combined on demand for application requirements. The experts at Fraunhofer FOKUS developed a methodology that integrates network providers into service provisioning. Cooperative Service Provisioning (CSP) enables interaction between service provider, network provider, and clients. CSP can be applied at different levels: as supplementary functions in classical networks, in peer-to-peer scenarios, or in disruptive environments that substitute for the network stack by atomic functional blocks (e.g. ANA project).

Creating function chains is a challenging task, especially in large and heterogeneous environments. After theoretical investigations and simulation studies of different algorithms, the Fraunhofer team is now conducting large-scale experiments under real-life Internet conditions at PlanetLab Europe, an open testbed for Future Internet research. Using research tools developed by the EU-funded Project OneLab, the team can control and visualize the function chain establishment process.

**OneLab**   
FUTURE INTERNET TEST BEDS

**Contact** – Dr. Michael Kleis  
michael.kleis@fokus.fraunhofer.de

# Future Internet Infrastructures for FI Prototyping

## Future Internet Tournament 2010 Evolution through Competition



To kick-start research on the Future Internet, Fraunhofer FOKUS officially announced the 2010 Future Internet Tournament at this year's Future Internet Workshop. This contest is designed to foster the development of Future Internet solutions. Networks will compete against each other, putting their cognitive and self-regulatory functions to the test. "We expect this challenge to boost the development of cognitive algorithms," says Dr. Zseby, the Fraunhofer liaison for the project. This first tournament on Future Routers and Networks is open for telecommunication industry professionals, software developers, IT architects as well as other experts representing the Future Internet technology arena. A technical core group of leading Future Internet experts, chaired by Fraunhofer FOKUS, will decide how recently developed assessment criteria for cognitive router and network performance can be enhanced and adjusted to the first challenge.

**Contact** – Dr. Tanja Zseby  
tanja.zseby@fokus.fraunhofer.de

### FIA 2009 4<sup>th</sup> Future Internet Assembly

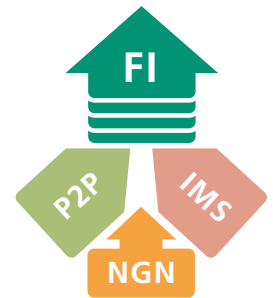
Stockholm, November 23–24, 2009  
www.fi-stockholm.eu

## Next Generation Networks to FI Evolution Prototyping an Innovative Multimedia Delivery Infrastructure

The project VITAL++, a part of the European FIRE initiative, is developing an evolutionary service delivery architecture geared toward operators of Next Generation Networks (NGNs) and the Future Internet (FI). One of the main missions in the FP7 European project VITAL++ is to explore and model synergies of classic infrastructures (IMS/NGN and P2P networks). So far, the project has developed experimental deployments of Peer-to-peer (P2P) authentication and content security architecture.

One of the biggest challenges faced by content distribution is the issue of how to enable efficient user-generated content delivery. P2P networks have proven suitable for large-volume content distribution, as they scale quite well. However, P2P networks lack overall-resource control, resulting in unpredictable throughput behavior at the terminals. NGN technology can exploit the scalability of a P2P network using Quality of Service (QoS) and AAA (Authentication, Authorization and Accounting) characteristics. This capability provides new services and service-models for NGN operators. FOKUS has extended myMONSTER to enable P2P media streaming and P2P authentication by way of a new IMS located P2P assistant. Complete extensions to myMONSTER, along with a fully integrated IMS-P2P assistant, are expected to be released during the third quarter of 2010.

**Contact** – Jens Fiedler: jens.fiedler@fokus.fraunhofer.de  
[www.fokus.fraunhofer.de/go/vitalpp](http://www.fokus.fraunhofer.de/go/vitalpp) | [www.mymonster.org](http://www.mymonster.org)



## FOKUS Future Internet Lab Platform for FI Research

The FOKUS Future Internet Laboratory (FI-Lab) is an open, independent testbed for experimental research and the assessment of new services and technologies. Connected to PlanetLab Europe, PII, VITAL++ and to the Berlin freifunk network, the FI-Lab assembles various wired and wireless network technologies from different vendors. FOKUS plays a leading role in the establishment of federated experimental platforms for FI research, participating in both testbed projects (OneLab, PII) of the European FIRE initiative. Recently, FOKUS also joined the project G-Lab Deep, a part of the G-Lab initiative funded by the Federal Ministry of Education and Research.

The testbed provides overlay and network virtualization technologies as well as research tools to support experiment observation and control. FOKUS also develops novel assessment methods to analyze upcoming cognitive network approaches.

**Contact** – Dr. Tanja Zseby  
tanja.zseby@fokus.fraunhofer.de  
[www.fokus.fraunhofer.de/go/fi-lab](http://www.fokus.fraunhofer.de/go/fi-lab)

