Token Based Firewalls

GGF-16 Firewall Issues Research Group

Athens, Feb 14th 2006

LAMBDAGRID

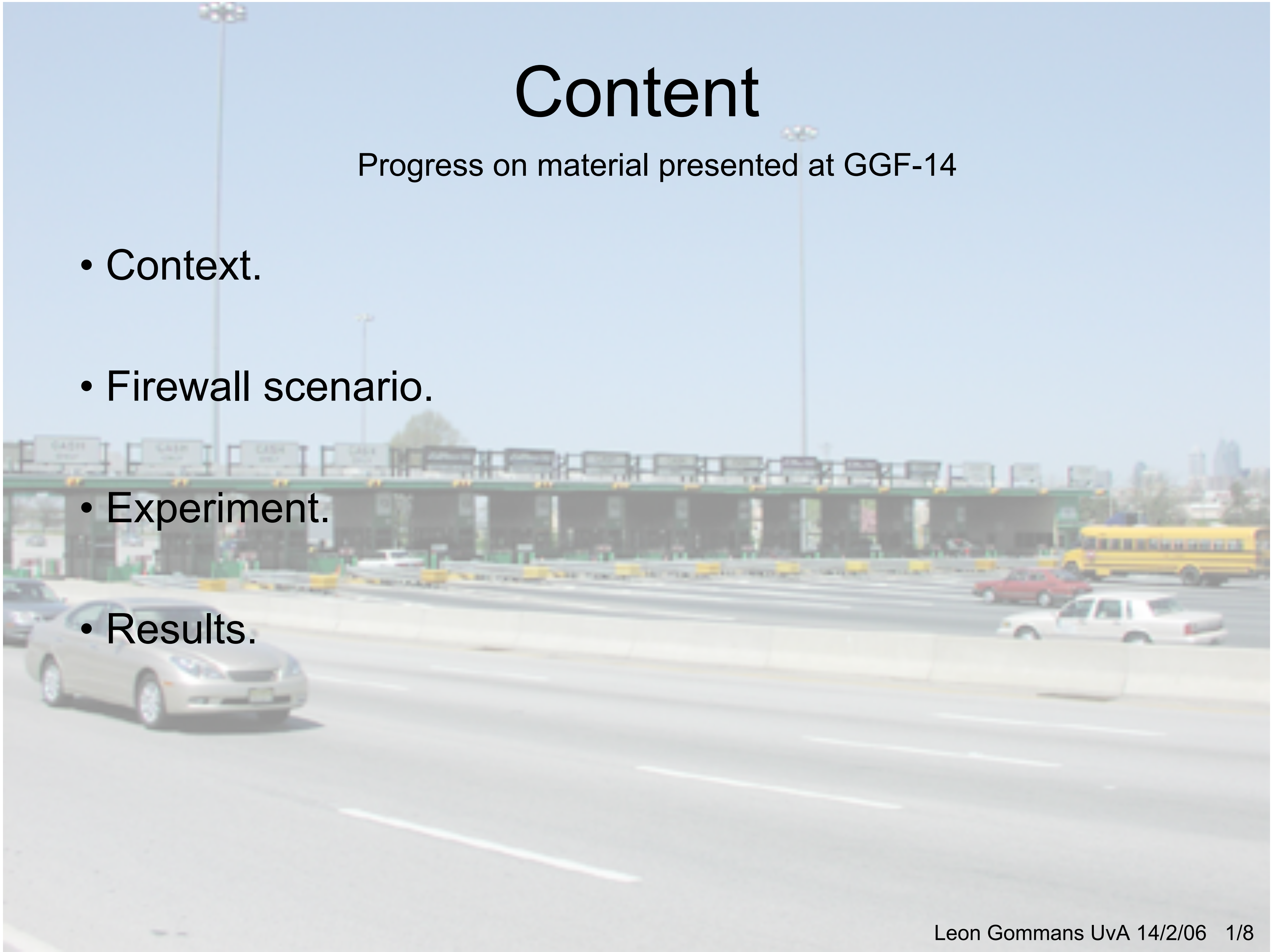
Welcome

Leon Gommans - University of Amsterdam

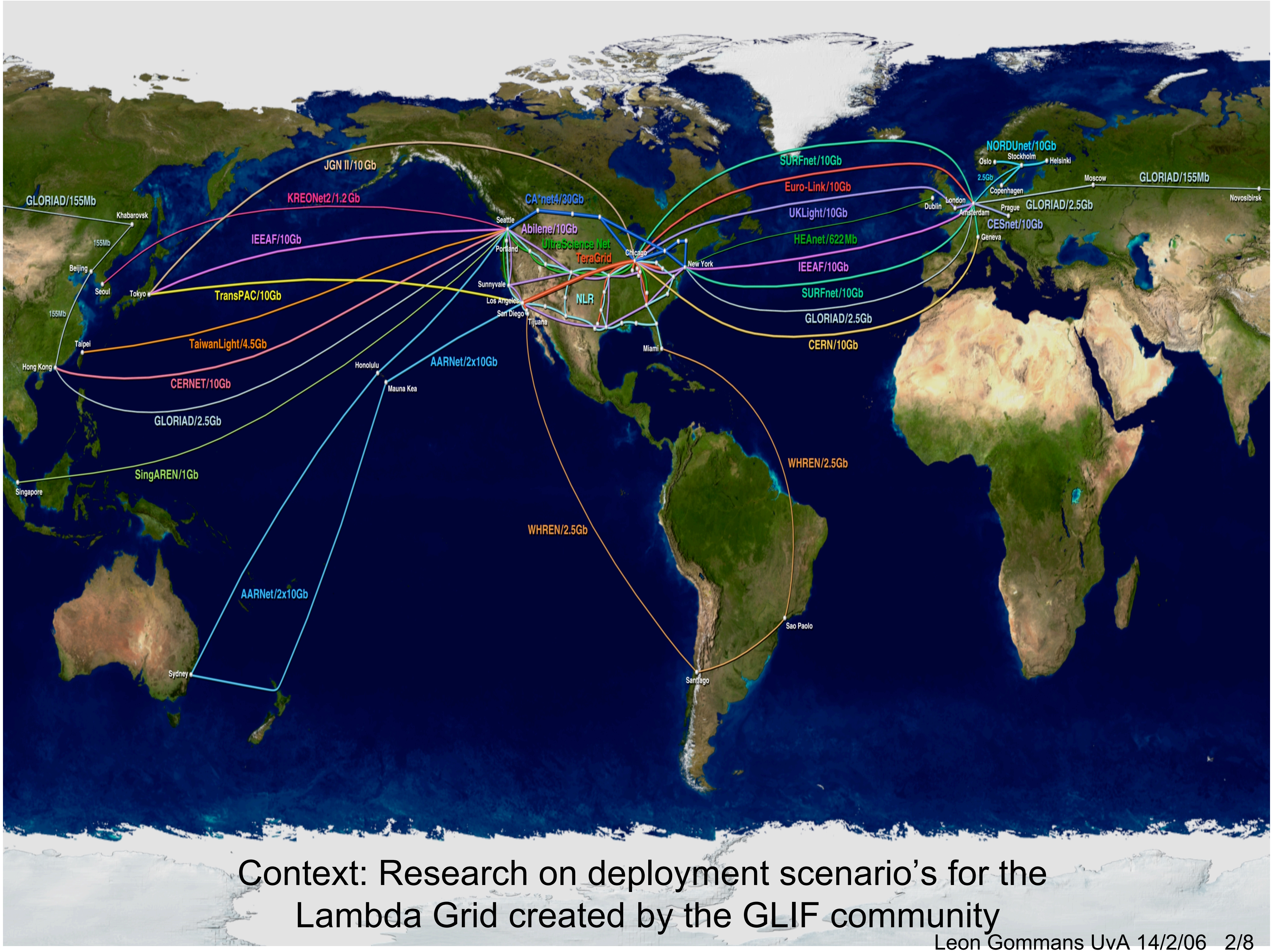
leon.gommans@science.uva.nl

Content

Progress on material presented at GGF-14

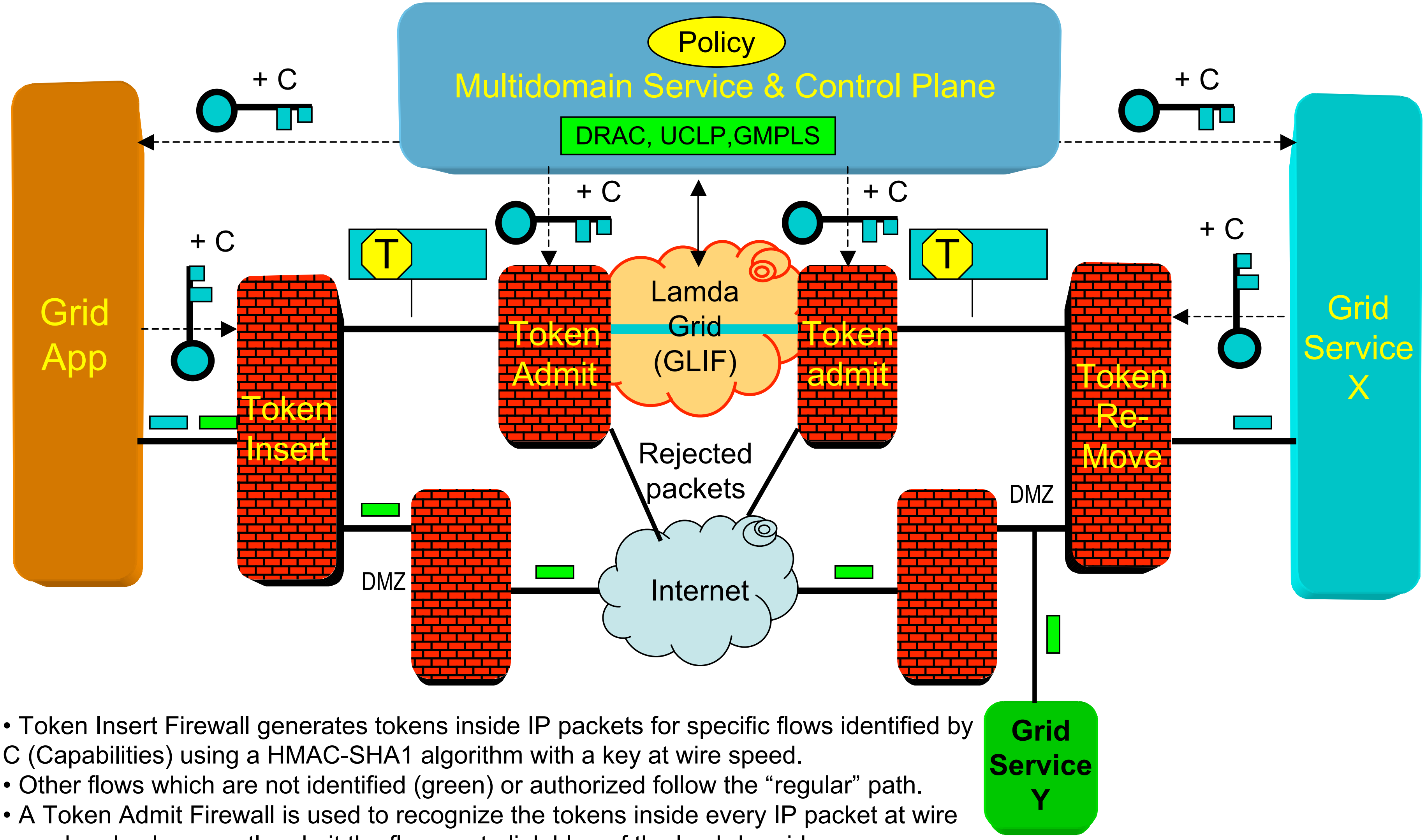


- Context.
- Firewall scenario.
- Experiment.
- Results.



Context: Research on deployment scenario's for the Lambda Grid created by the GLIF community

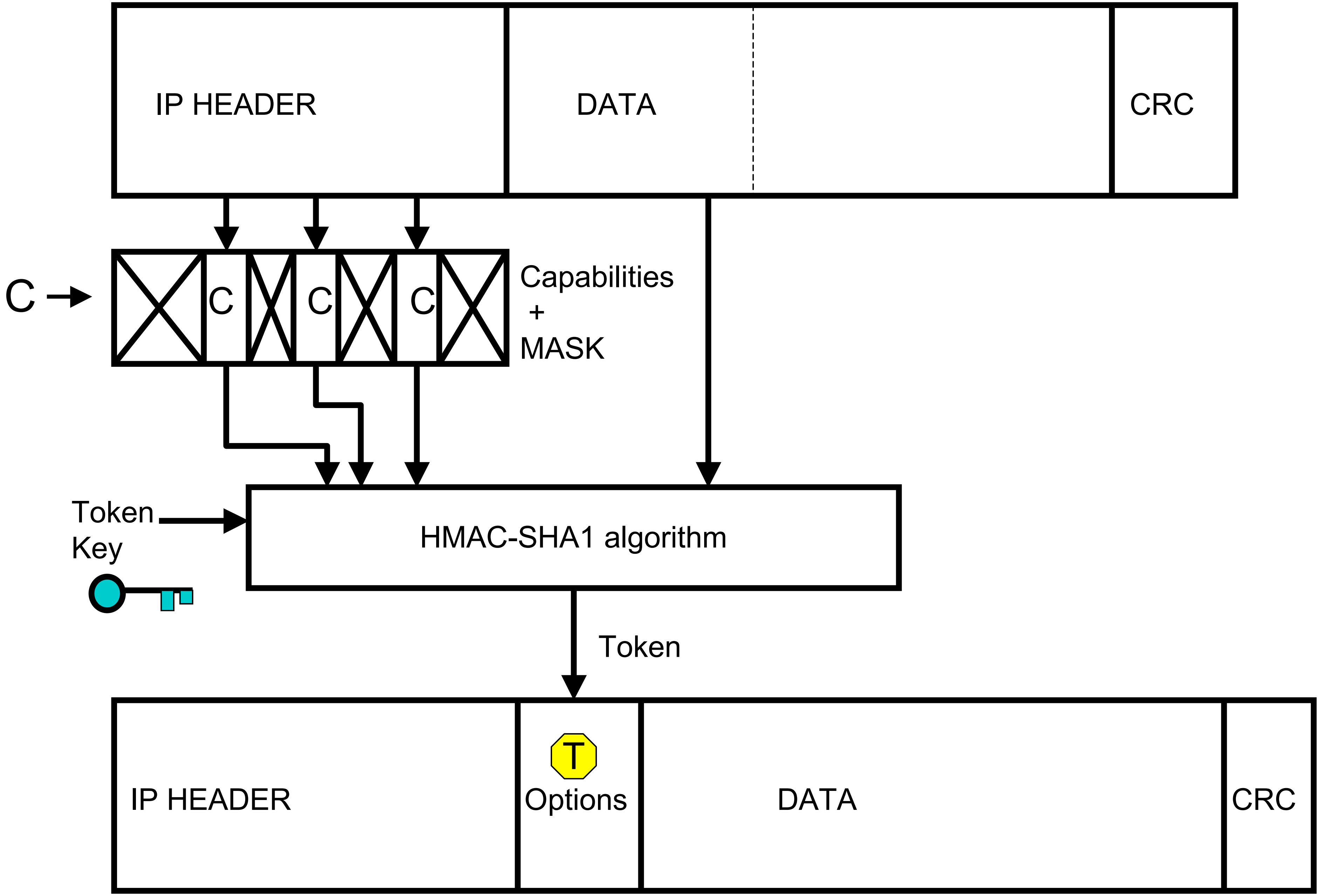
Token Based Firewall scenario admitting flows to a Lambda Grid



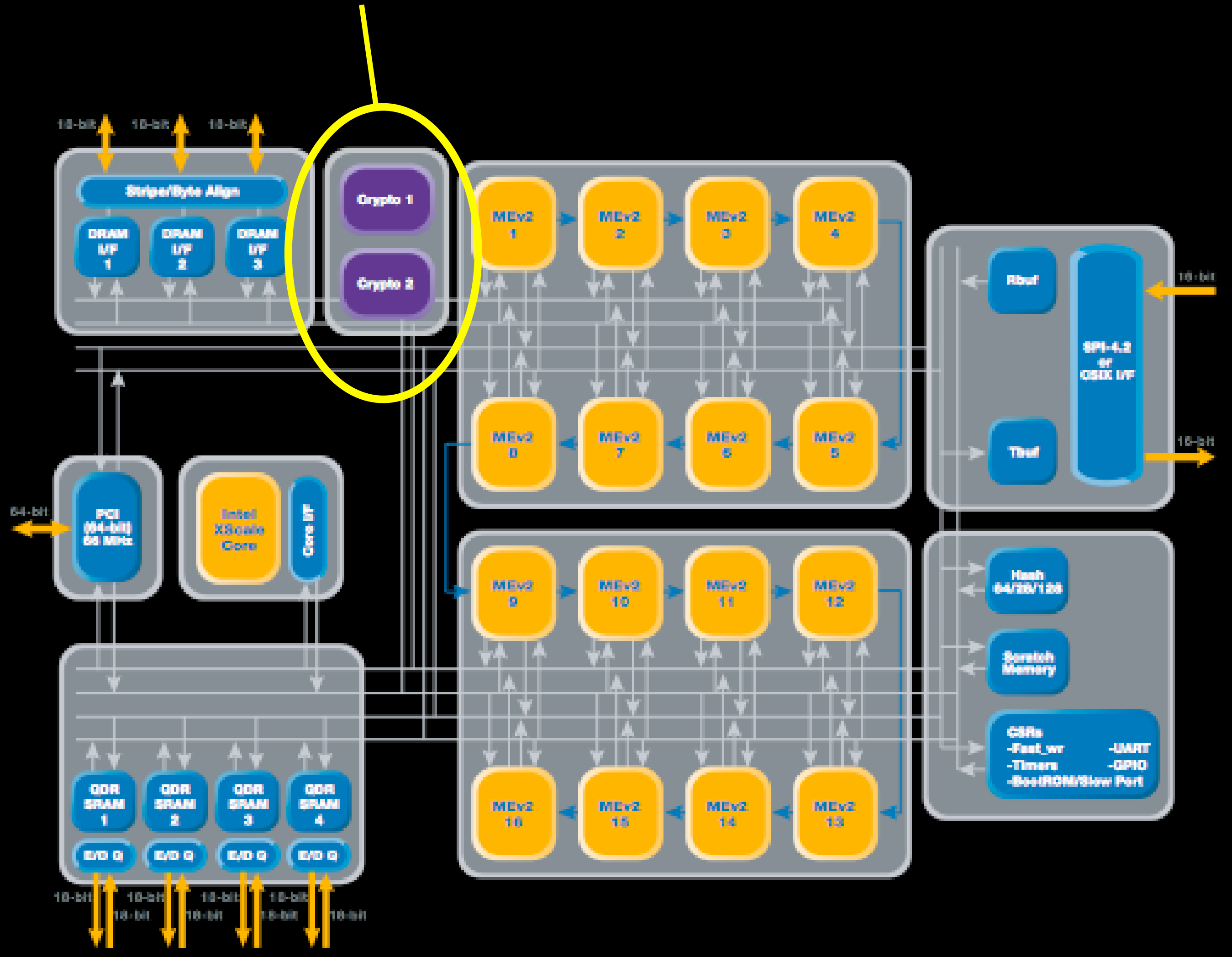
- Token Insert Firewall generates tokens inside IP packets for specific flows identified by C (Capabilities) using a HMAC-SHA1 algorithm with a key at wire speed.
- Other flows which are not identified (green) or authorized follow the “regular” path.
- A Token Admit Firewall is used to recognize the tokens inside every IP packet at wire speed and subsequently admit the flows onto link blue of the lambda grid.
- Keys are issued on behalf of the owner of Lambda Grid link blue by the service & control plane. The service plane hereto deploys AAA mechanisms.
- Service plane provisions the corresponding path configurations.

------ Secure and Trusted control Channel

Prototype implementation on Intel NPU development platform

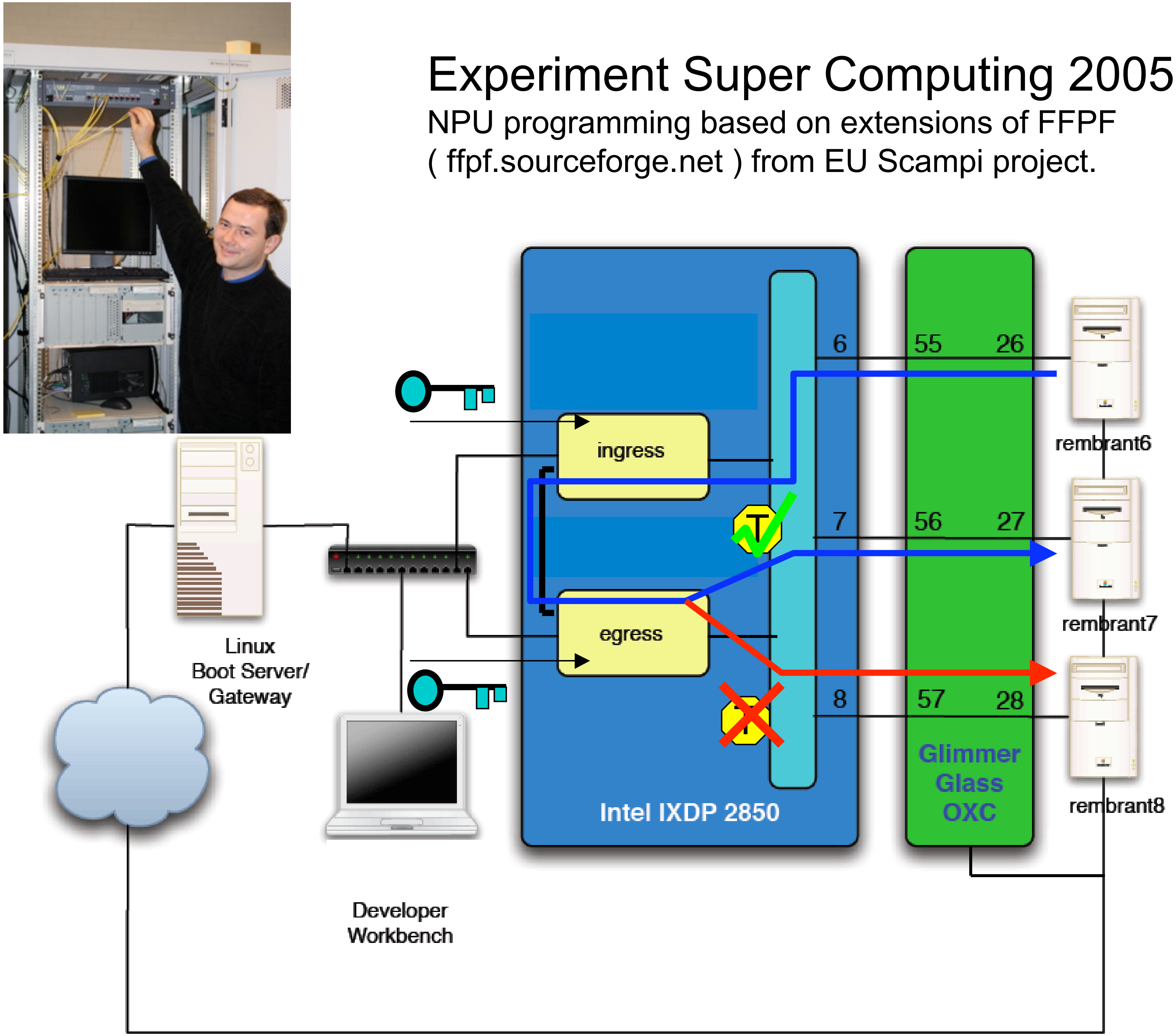


Intel IXP 2855: 11M HMAC-SHA1 operations/sec @ 1.5 GHz



Experiment Super Computing 2005

NPU programming based on extensions of FFPF
(ffpf.sourceforge.net) from EU Scampi project.

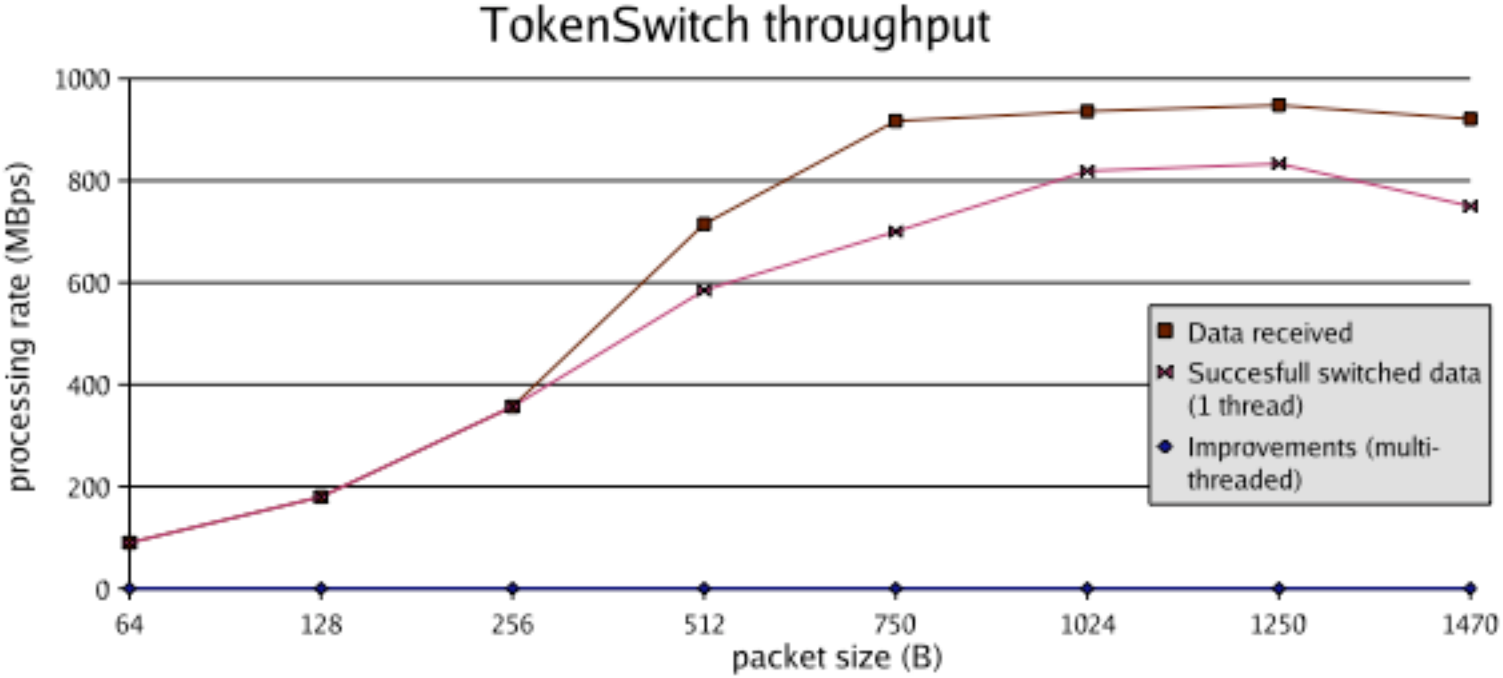


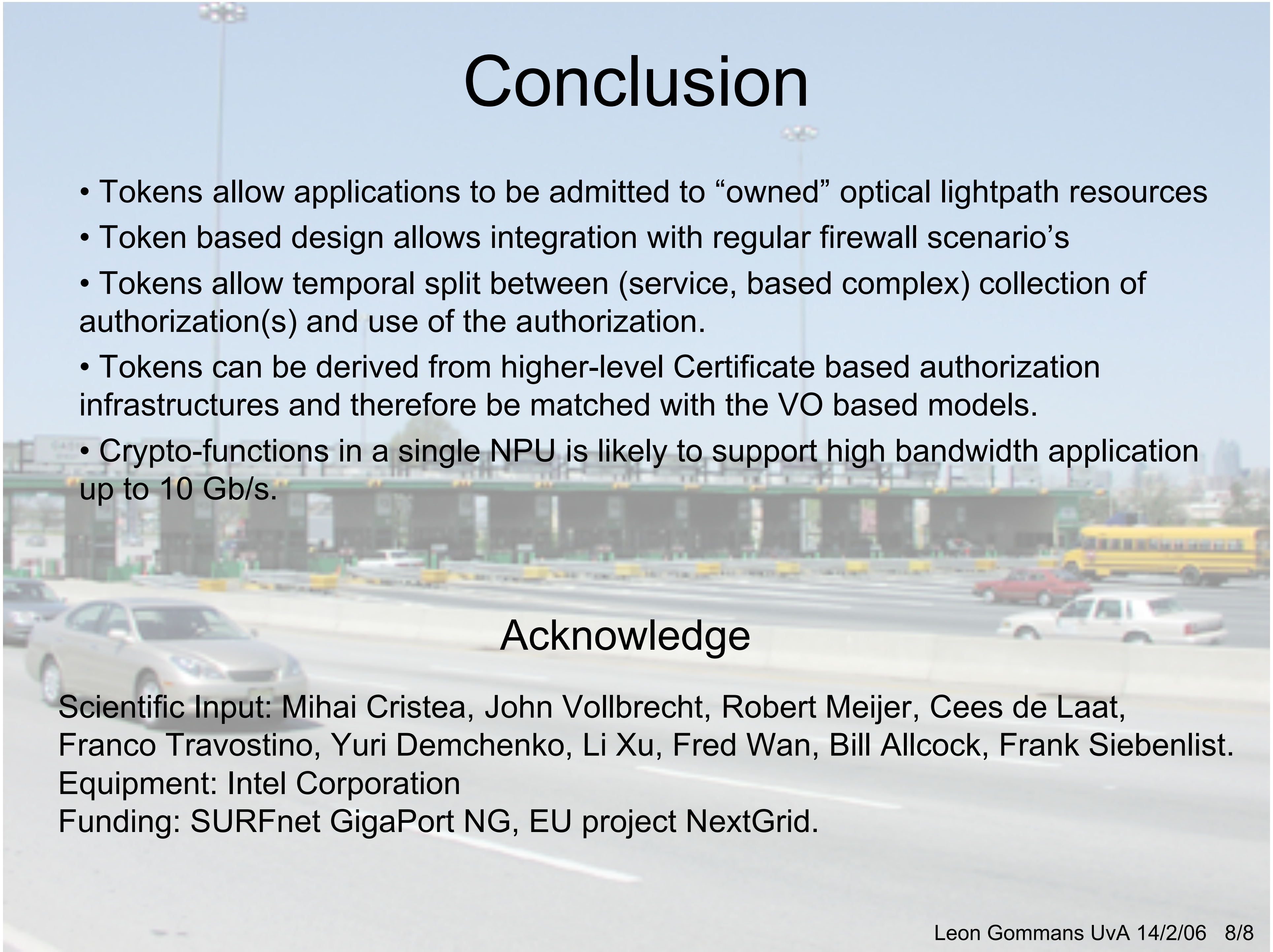
First results: Single Thread / Single Micro-Engine implementation

using single 1 gb/s input port using UDP iperf.

Working now on multi-thread implementation and later

put it on multiple Micro-Engines (up to 16 available)





Conclusion

- Tokens allow applications to be admitted to “owned” optical lightpath resources
- Token based design allows integration with regular firewall scenario’s
- Tokens allow temporal split between (service, based complex) collection of authorization(s) and use of the authorization.
- Tokens can be derived from higher-level Certificate based authorization infrastructures and therefore be matched with the VO based models.
- Crypto-functions in a single NPU is likely to support high bandwidth application up to 10 Gb/s.

Acknowledge

Scientific Input: Mihai Cristea, John Vollbrecht, Robert Meijer, Cees de Laat, Franco Travostino, Yuri Demchenko, Li Xu, Fred Wan, Bill Allcock, Frank Siebenlist.
Equipment: Intel Corporation
Funding: SURFnet GigaPort NG, EU project NextGrid.