WIRELESS WORLD
RESEARCH FORUM

ITU-T Workshop on

Addressing security challenges on a global scale

06.+07.12.2010, Geneva

"WWRF – Cloud Implications to Security, Privacy, and Trust"

Mario Hoffmann

Chair WWRF Working Group 7 "Security & Trust"

Fraunhofer Institute for Secure Information Technology

Head of Department "Secure Services & Quality Testing"

Darmstadt/Munich, Germany

WWRF

WIRELESS WORLD
RESEARCH FORUM

http://www.wireless-world-research.org

- Founded 2001, 100 members
- Global pre-standardisation platform to initiate global cooperation towards future wireless world
- Vision from user perspective ➔ requirements for the enabling technologies
- Unique way of active cooperation within and between industry and academia
- Reduce risk for investment in research
- Ease future standardisation by globally harmonising views
- Proven history of creating large scale research cooperation and facilitating funding
- Open to all actors

WG7 – Privacy, Security & Trust

Approach (1/2)

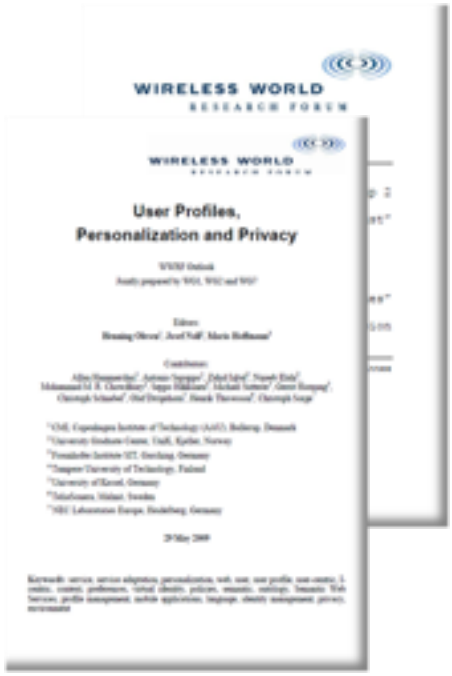
Source: EU-IST Project, 2001

Integration of **Privacy**, **Security** and **Trust** into ...

Integration Layers	Protection Goals
Application Layer	Availability
Platforms/Middleware	Confidentiality
Mobile Devices	Integrity
Infrastructure	Accountability
	Authenticity

WG7 – Privacy, Security & Trust

Approach (2/2)



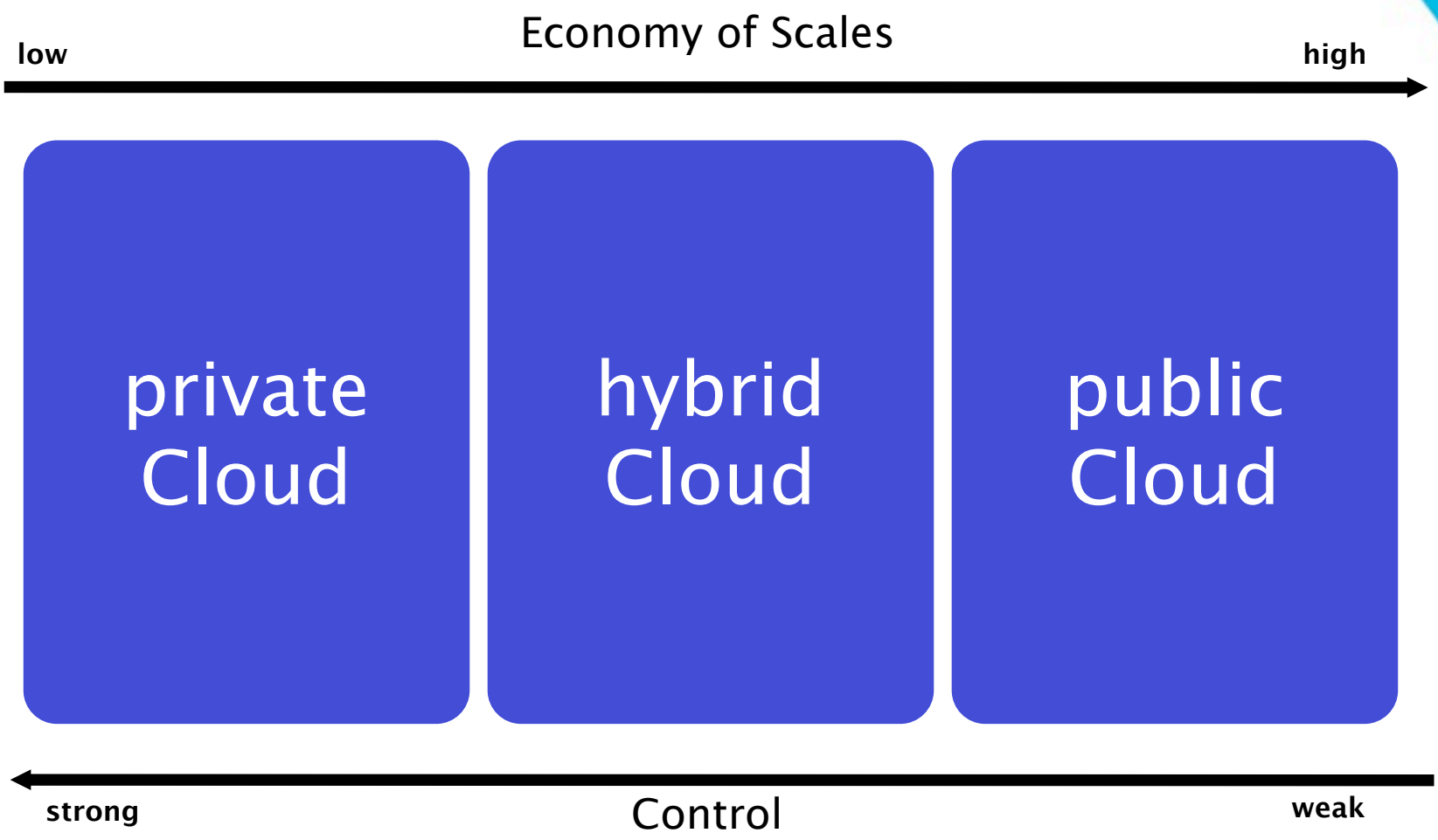
Source: WWRF

How to …

- ... specify, negotiate, enforce and monitor a certain level of Privacy, Security & Trust between cooperation and communication partners in ambient environments?
- ... implement and integrate security enablers by design?
- ... tackle attacking strategies such as spy out, deny, tamper, misuse, misinform?
- ... fulfill user empowerment, user awareness, enforcing security policies, establishing context security?
- ... ensure transparency, usable security?

Cloud Computing
Deployment Models

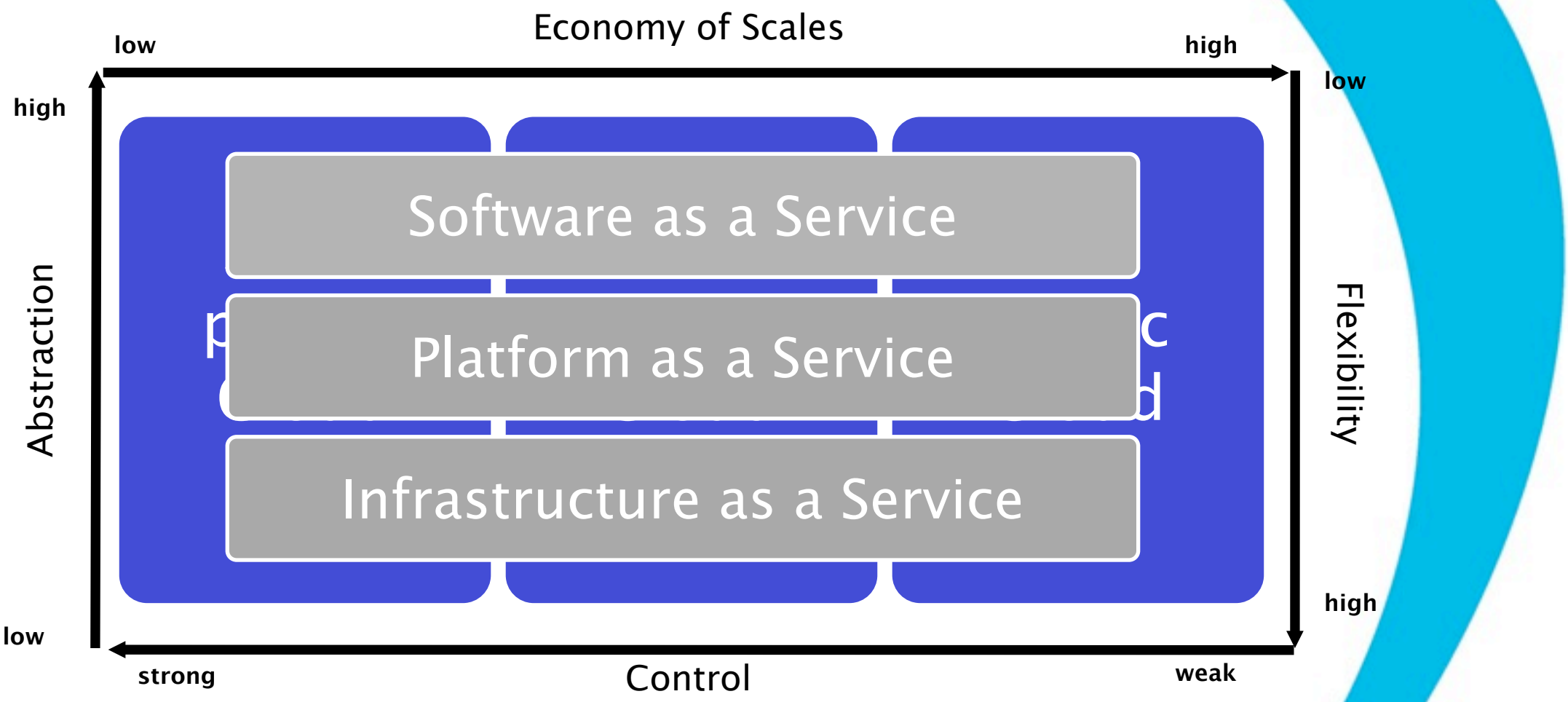
WIRELESS WORLD
RESEARCH FORUM



Cloud Computing

Service Models

WIRELESS WORLD
RESEARCH FORUM



Cloud - Transparency

WIRELESS WORLD
RESEARCH FORUM

Feature

Resources and data are just somewhere in the Cloud and can be accessed on demand from everywhere at any time.

Challenge

- Where is my data?
- Who has access to it?
- How can a Cloud service consumer monitor and control access to his resources?
- How can I guarantee compliance with national law, certified processes, and company's security policies?
- Which jurisdiction is applicable?

Cloud - Identity Management

WIRELESS WORLD
RESEARCH FORUM

- An integral part of Cloud services is identity and access management.
- Identity as a Service: From simple user provisioning to identity federation
- Identification of a unique “object” within an ambiguous environment and its identity lifecycle
- Single-sign-on and usability

Cloud - Interoperability

WIRELESS WORLD
RESEARCH FORUM

- Distinguish Public, Private, Hybrid Clouds (plus Community, Virtual Private Clouds)
- Challenge: Complexity, interoperability, and the ability to change the cloud service provider easily are major issues as standardization is only in an early phase.
- For service providers as well as service consumers it is most important to identify the individual protection goals and risks appropriately following a comprehensive taxonomy

Cloud - Mobility

WIRELESS WORLD
RESEARCH FORUM

- From a research perspective the Cloud approach can be extended to restricted resources which are only temporarily available, such as mobile devices in a meeting room.
- Devices could share single features and dedicated resources for a specific time period taking advantage of additional features from the direct environment.
- Here, the term Cloud has to be re-defined for mobile application scenarios (see [KaFi2010])

Cloud - Encryption

WIRELESS WORLD
RESEARCH FORUM

- A promising candidate to solve the issue that encrypted data in the Cloud has to be decrypted first before it can be processed is full homomorphic encryption.

- Here operations such as multiplication and addition can be realized on encrypted data which would eventually reach a much higher security level (see [SmVe2009])

Cloud - Trustworthy Virtualisation

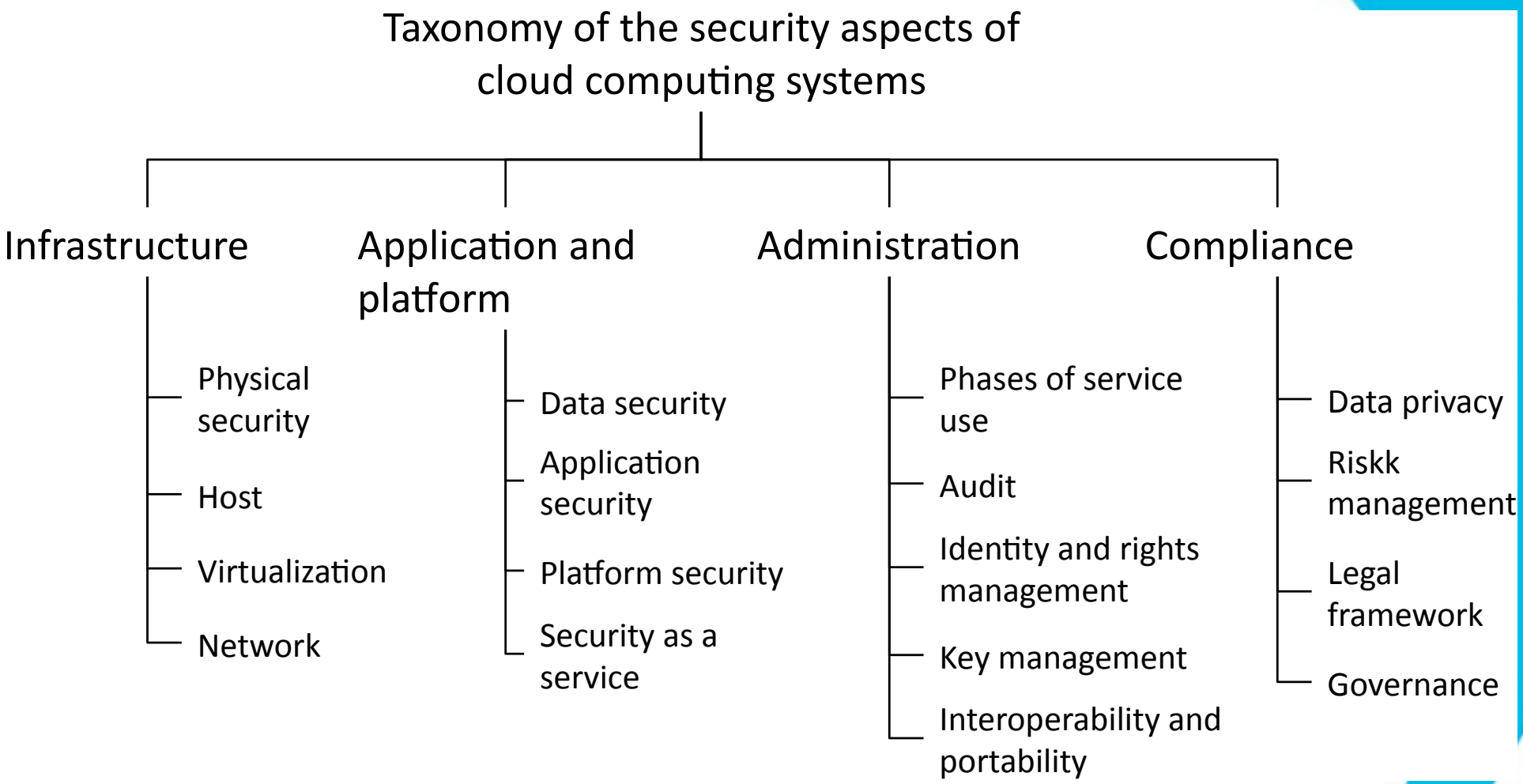
- Next generation Trusted Platform Modules (TPMs) are able to support virtualization on hardware layer.
- Since virtualization is a very important enabler of Cloud Computing this addresses issues related to untrustworthy transactions between Cloud entities on infrastructure, platform as well as software level.
- In environments with high security requirements TPMs might serve as trust anchors (see for example [HKH2009])

Cloud - Top Threats

WIRELESS WORLD
RESEARCH FORUM

- Abuse of Cloud Computing Resources
- Shared Technology Vulnerabilities
- Data Loss or Leakage
- Insecure Application Programmer Interface
- Account, Service & Traffic Hijacking
- Malicious Insiders
- Unknown Risk Profile

Cloud - Security Taxonomy



Cloud - DOs & DONTs

WIRELESS WORLD
RESEARCH FORUM

(1) Use a holistic security concept

(2) Integrate the services in an existing security concept

(3) Build a relationship of trust between the cloud consumer and the cloud vendor

(4) Protect the network infrastructure

(5) Use innovative security solutions for cloud computing systems

(6) Reuse basic services

(7) Pay attention to lock-in effects

(8) Request security certificates

(9) Don’t forgo security concepts for purely financial reasons

(10) Use service level agreements

Cloud - Innovation Areas

WIRELESS WORLD RESEARCH FORUM

Public – Community – Private – Hybrid

Application Areas

- Broadcast/Media
- Collaboration
- ACD, CRM, IAM
- Online-Services
- eGovernment
- eMobility
- Logistics
- Trusted Cloud

Innovation Areas

- Governance, Risk, Compliance
- Monitoring, Risk Analysis
- Identity Lifecycle Management
- Security Services
- Virtualisation & Interoperability

Infrastructure – Platform – Software

Cloud - Funding

WIRELESS WORLD
RESEARCH FORUM

Companies

Cloud-Consumers: What does Cloud Computing mean to my processes, business, and infrastructures?

Cloud-Providers: How will Cloud Computing affect Future Internet and vice versa?

European Union, FP7, Call 8 (Jan 2012)

Germany, “Trusted Cloud” Call (30 M€, Jan 2011)

Cloud - References

[CSA2009] Cloud Security Alliance: Security Guidance for Critical Areas of Focus in Cloud Computing V2.1Dd, http://www.cloudsecurityalliance.org/csaguide.pdf

[CSA2010] Cloud Security Alliance: Guidance for Identity & Access Management V2.1 http://www.cloudsecurityalliance.org/guidance/csaguide-dom12-v2.10.pdf

[ENISA2009] Enisa: Cloud Computing Risk Assessment, http://www.enisa.europa.eu/act/rm/files/deliverables/cloud-computing-risk-assessment/at_download/fullReport

[HKH2009] Kai Hwang, Sameer Kulkareni, Yue Hu, "Cloud Security with Virtualized Defense and Reputation-Based Trust Mangement", Eighth IEEE International Conference on Dependable, Autonomic and Secure Computing, Chengdu, China, 2009

[KaFi2010] M.Katz and F. Fitzek, "Mobile Clouds: Challenges and Potentials", WWRF#24, Penang, Malaysia, April 2010, http://www.wireless-world-research.org

[Kantara2010] Kantara Initiative, Kantara Federation Interoperability Workgroup (FIWG), http://kantarainitiative.org/confluence/display/fiwg/Home

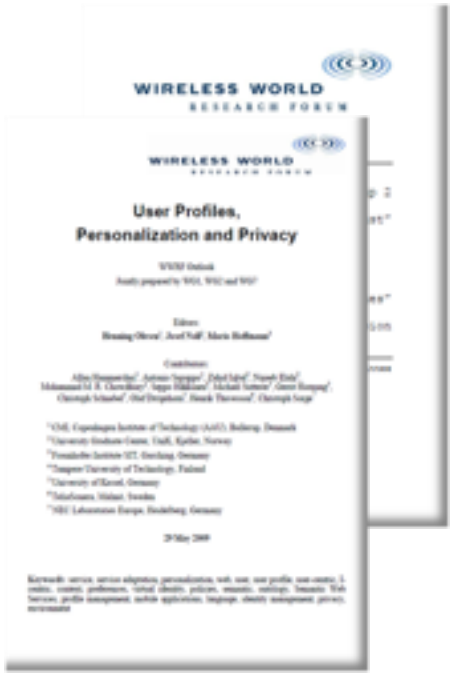
[OASIS2010] OASIS: Identity in the Clouds – Tech. committee, OASIS Identity & Trusted infrastructure, http://xml.coverpages.org/Identity-Clouds-Proposal.html

[StRu2010] Werner Streitberger, Angelika Ruppel, "Cloud Computing Security – Protection Goals, Taxonomy, Market Review", http://www.sit.fraunhofer.de/EN/pressedownloads/artikel/bestellung_ccs.jsp

[SmVe2009] N.P. Smart, F. Vercauteren, "Fully Homomorphic Encryption with Relatively Small Key and Ciphertext Sizes", http://eprint.iacr.org/2009/571.pdf

WG7 – Privacy, Security & Trust

Contact



Source: WWRF

Join WWRF and WG7

Website: **www.wireless-world-research.org/**

Subscribe to our mailing list!

Contact: Mario Hoffmann (Chair)
mario.hoffmann@sit.fraunhofer.de
Marcus Wong (Vice Chair)
wong@huawei.com