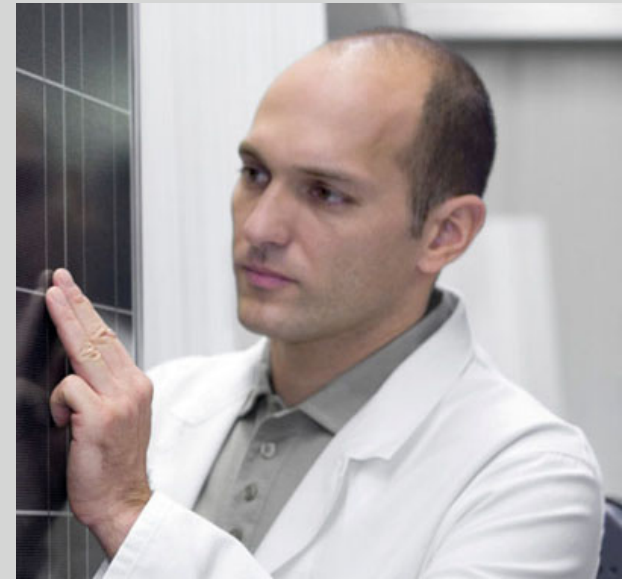


Trusted Architectures / Trust Architectures for the Future Internet Service Offering



Volkmar Lotz
SAP Research

... doesn't mean that nothing can go wrong

- we have to accept that vulnerabilities exist and bad guys are out there

... does mean that service consumers can make informed decisions about the risk that needs to be taken

... does mean that services and infrastructure functionalities are in place that allow to mitigate those risks

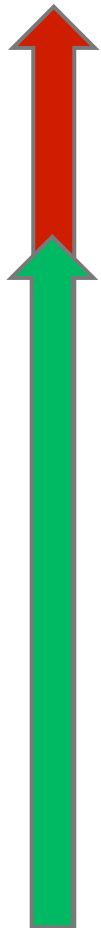
→ risk assessment and management methods and tools are key

→ taking into account the distributed nature of trust

- no single trust anchor, but multiple ones (applications, services, service delivery platform, infrastructure, devices)

How to achieve trust?





asks for a trust and security “toolbox” that can be flexibly adapted to the given business / risk context

- controls
- protocols
- policies
- certificates
- validation

→ many of them are readily available

the “tools” are spread over layers / entities (incl. services) / domains

- management
- composition

methods for assessing the effectiveness of a given selection and composition of tools are key

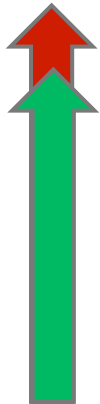
assessing the value of transactions over the FI

- capturing business context
- semantics of (business) processes
- enhanced service descriptions

management methodologies and tools

- ready to be used by the service consumer (services and users)
- taking lifecycle and aggregation aspects into account (→ dynamic risk evaluation)

integration in FI architecture



Essentials of a trusted service architecture and trusted services:

- Context-sensitive risk assessment and management
- Flexible toolbox of controls
- distributed over services, service delivery platforms, and infrastructure
- accessible to services and users
- supporting compositional security and transparency