Security Management interoperability challenges for Collaborative Clouds

4th International DMTF Academic Alliance Workshop on Systems and Virtualization Management: Standards and the Cloud (SVM 2010) - 29/10/2010

[Michael.Kretzschmar, Sebastian Hanigk]@unibw.de

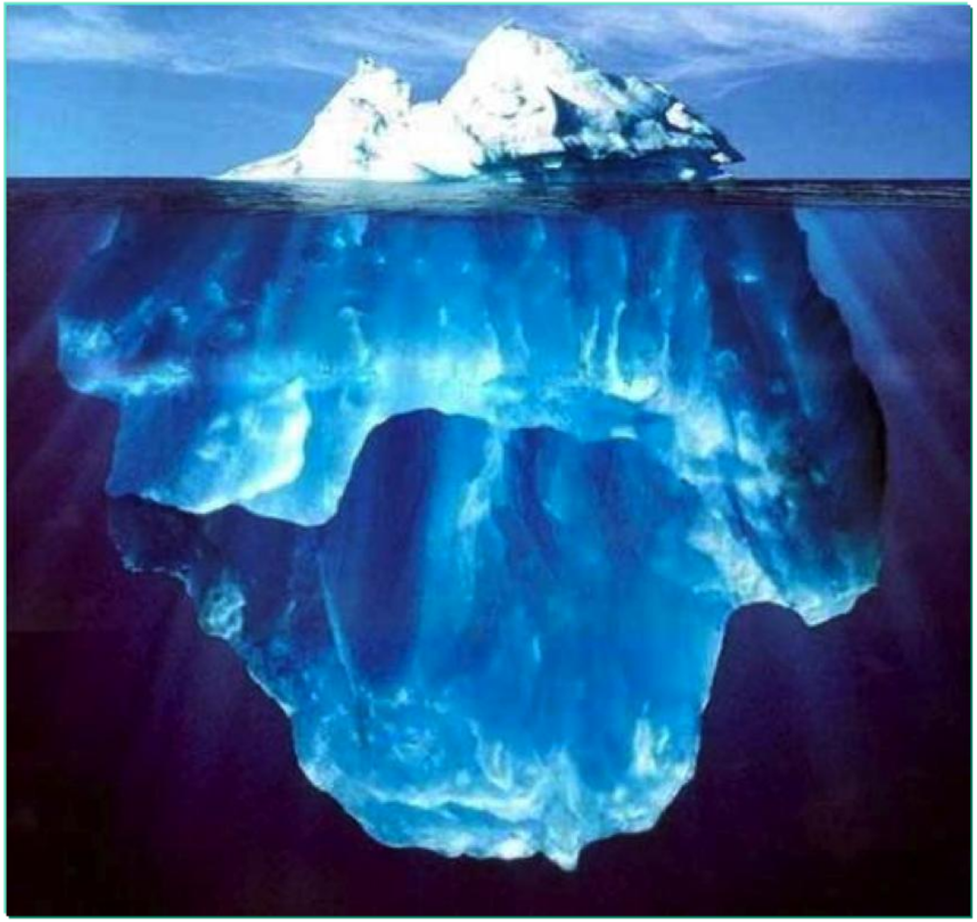
About me

- IT-officer in the German Army
- Research assistant at the Universität der Bundeswehr München (UniBwM)
- Topics of research:
  - IT-security
  - Security management
  - Cloud Computing
- Member of:
  - NATO SC/4 SMI and TIAS
  - EDA PT CIS
  - NMN-Team

Journey in the Cloud

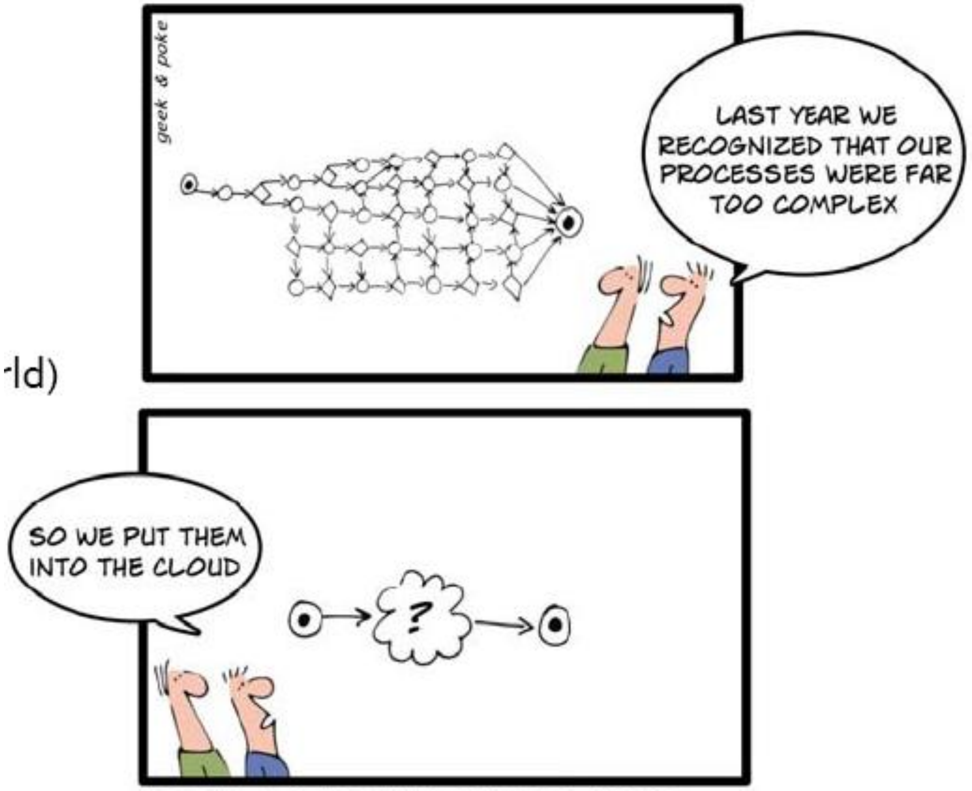
What we see

What is there



Agenda

1. Setting the scene
2. Cloud environment
3. SM domains
4. Status quo
5. Security management objects


geek & poke
LAST YEAR WE RECOGNIZED THAT OUR PROCESSES WERE FAR TOO COMPLEX
SO WE PUT THEM INTO THE CLOUD
?

ld)

LET THE CLOUDS MAKE YOUR LIFE EASIER

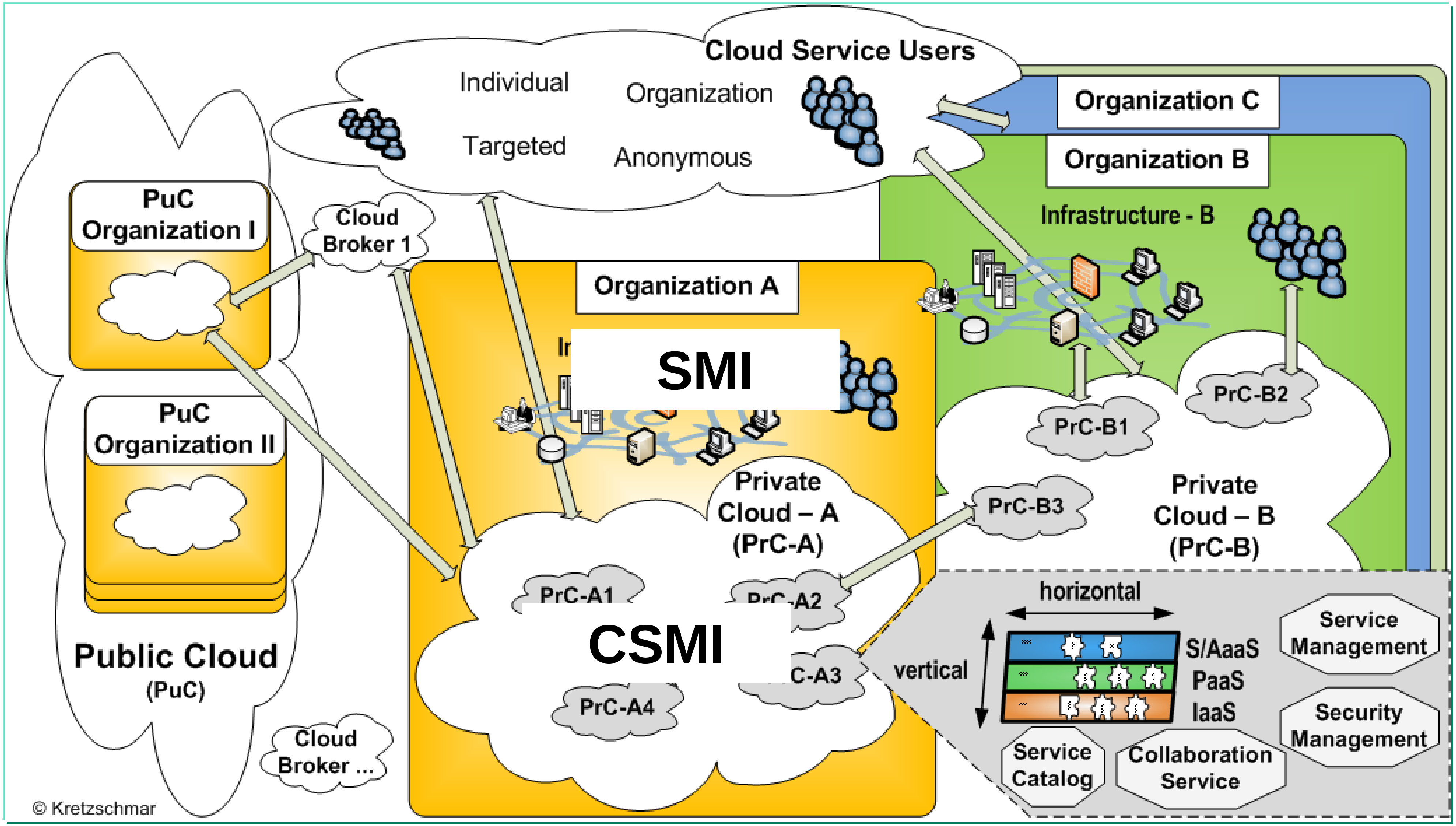
Setting the scene

- Provide trust and security over multi-provider Cloud Computing environments (dedicated communication infrastructures, security mechanisms, processes and policies)
- “Cloud Computing usage, as Cloud Computing services will multiply and expand faster than the ability of Cloud Computing consumers to manage or govern their usage”
- Vision: global, consistent, accountable and integrated security management – “air traffic control system”

Setting the scene – RSA 3 layer

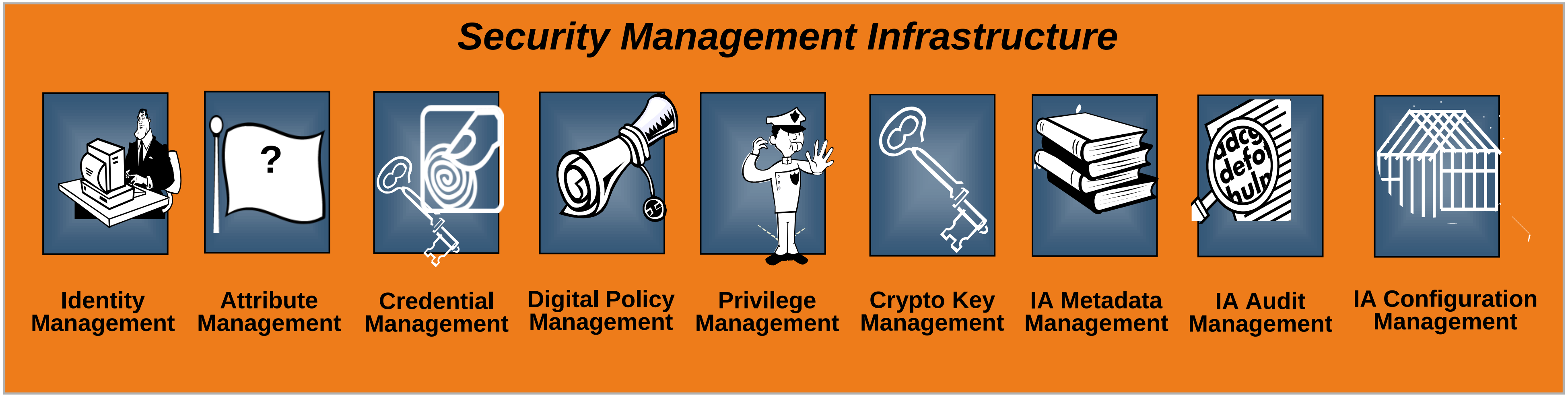
- 1 enforcement of control:
  - Enforcement of security regulations
  - Reporting
- 2 control management:
  - Providing and monitoring controls
- 3 security management:
  - Policies for all security management functional areas
  - Collection/aggregation/integration of events and alerts from controls or the regular infrastructure
  - → merging technology/platforms within a framework = air traffic control system

Cloud environment



SM domains (1)

- **Security management functions**
  - Data
    - Policy enforcement at all points
    - Encrypt all data - in motion or at rest
    - Key management
  - Identity nightmare - AAA



Security Management Infrastructure

Identity Management · **Attribute Management** · **Credential Management** · **Digital Policy Management** · **Privilege Management** · **Crypto Key Management** · **IA Metadata Management** · **IA Audit Management** · **IA Configuration Management**

SM domains (2)

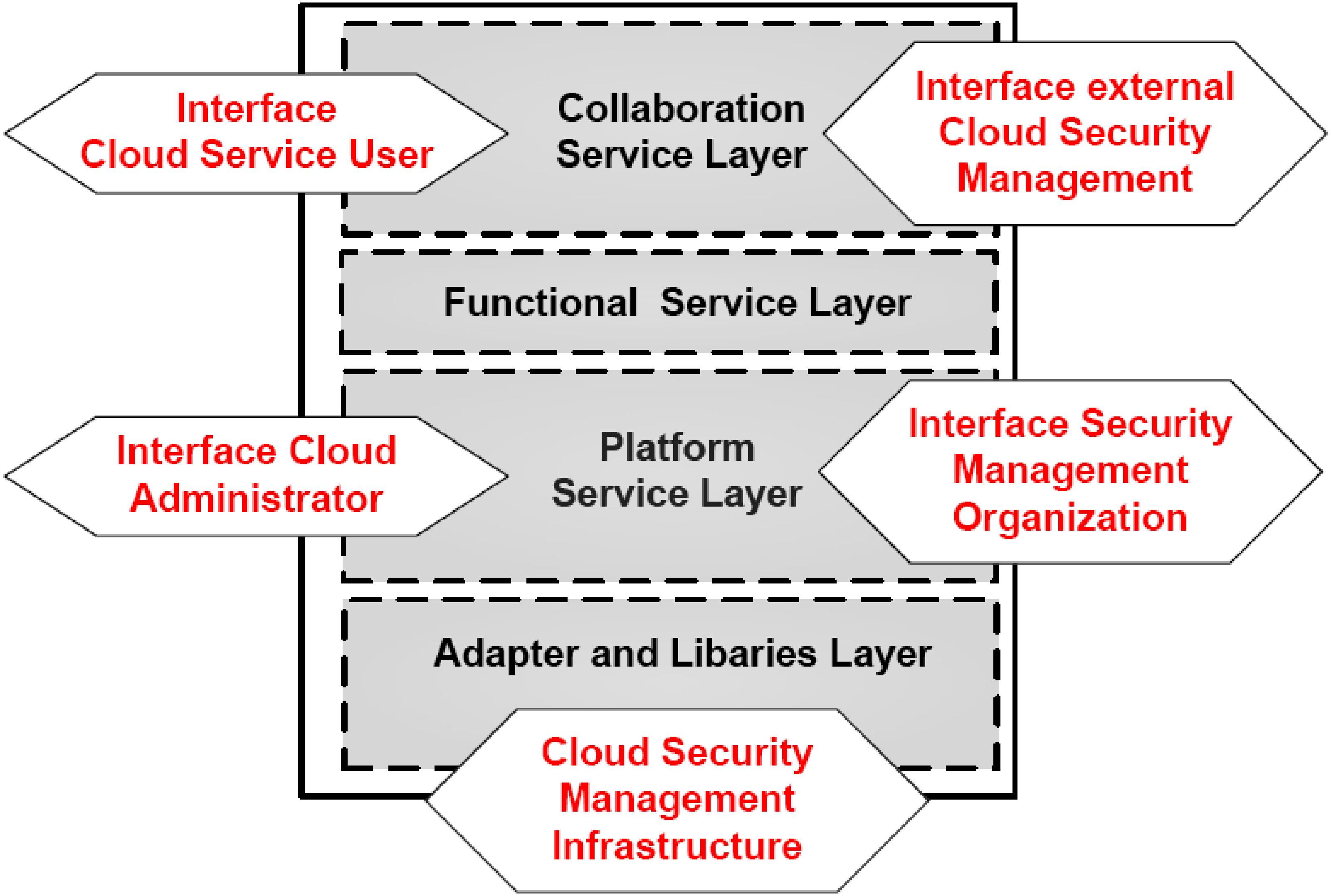
- **Collaboration**
  - Shared environment:
    - Integration of inter-security management information exchange
    - Standardised and non-proprietary protocols
  - Distributed time zones
    - sufficient timestamps
    - Schedules
  - Management information exchange between Cloud security management system - overarching security management system of whole organization

SM domains (3)

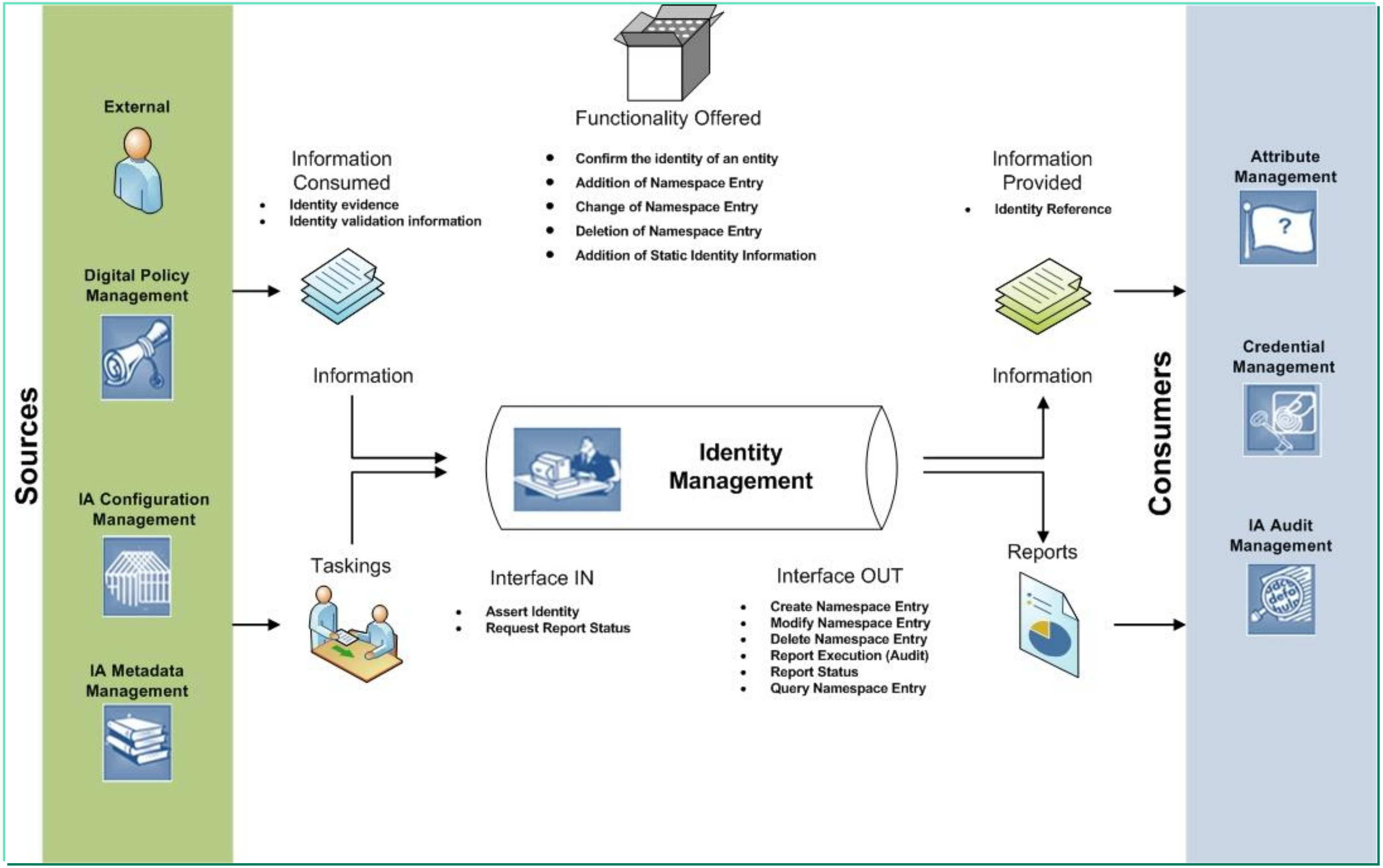
- **Integration of Security Management Objects**
  - Interfaces and API’s
  - Support of standards
  - Responsibility SaaS, PaaS, IaaS

- **General Requirements**
  - Scalability and flexibility
  - Geographic and linguistic

Cloud security management model



Status quo – security management services



Sources

External

Digital Policy Management

IA Configuration Management

IA Metadata Management

Information Consumed

- Identity evidence
- Identity validation information

Functionality Offered

- Confirm the identity of an entity
- Addition of Namespace Entry
- Change of Namespace Entry
- Deletion of Namespace Entry
- Addition of Static Identity Information

Information Provided

- Identity Reference

Information

Taskings

Identity Management

Information

Reports

Interface IN

- Assert Identity
- Request Report Status

Interface OUT

- Create Namespace Entry
- Modify Namespace Entry
- Delete Namespace Entry
- Report Execution (Audit)
- Report Status
- Query Namespace Entry

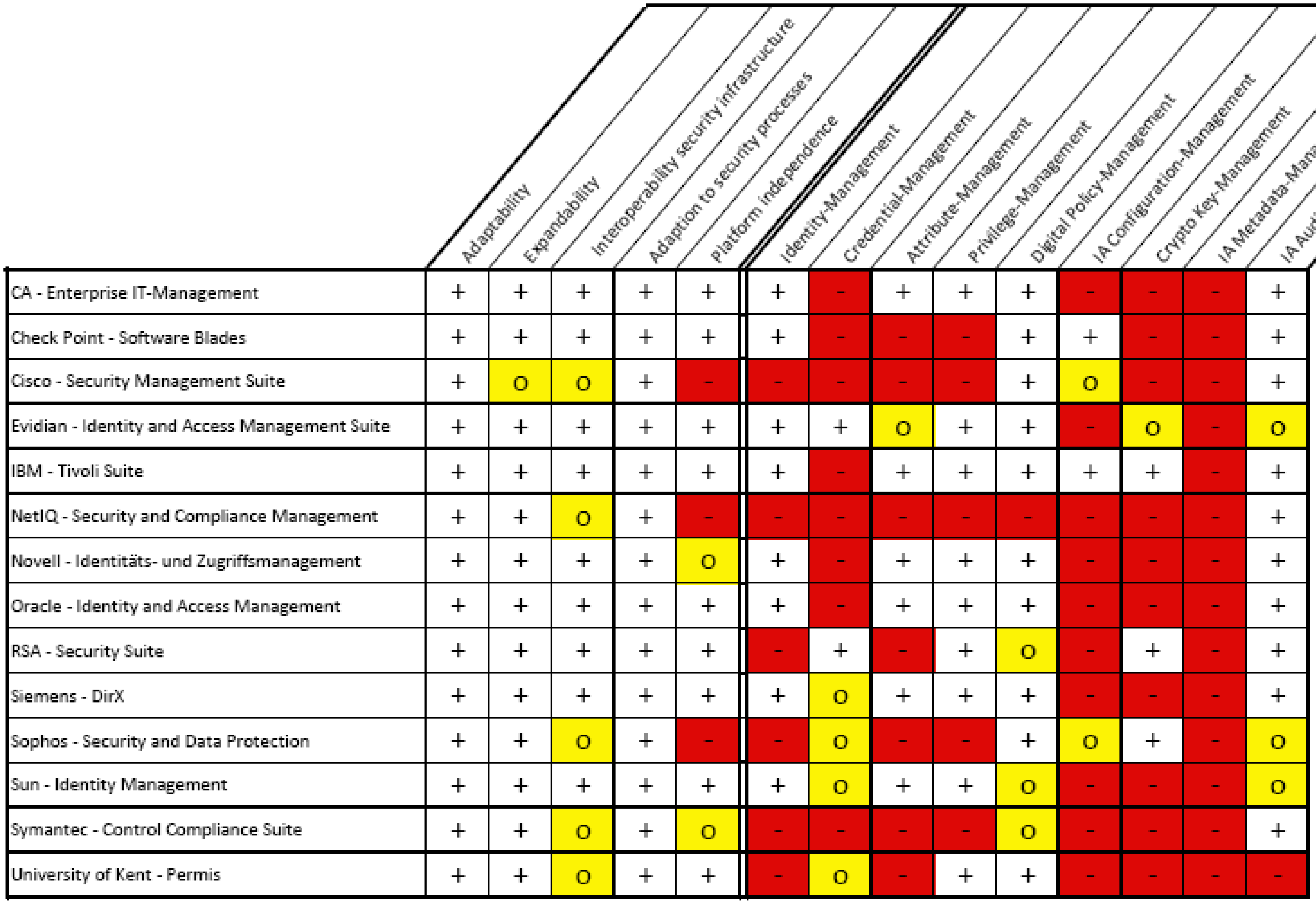
Consumers

Attribute Management

Credential Management

IA Audit Management

Status quo – security management



	Adaptability	Expandability	Interoperability security infrastructure	Adaption to security processes	Platform independence	Identity-Management	Credential-Management	Attribute-Management	Privilege-Management	Digital Policy-Management	IA Configuration-Management	Crypto Key-Management	IA Metadata-Management	IA Audit-Management
CA - Enterprise IT-Management	+	+	+	+	+	+	-	+	+	+	-	-	-	+
Check Point - Software Blades	+	+	+	+	+	+	-	-	-	+	+	-	-	+
Cisco - Security Management Suite	+	O	O	+	-	-	-	-	-	+	O	-	-	+
Evidian - Identity and Access Management Suite	+	+	+	+	+	+	+	O	+	+	-	O	-	O
IBM - Tivoli Suite	+	+	+	+	+	+	-	+	+	+	+	+	-	+
NetIQ - Security and Compliance Management	+	+	O	+	-	-	-	-	-	-	-	-	-	+
Novell - Identitäts- und Zugriffsmanagement	+	+	+	+	O	+	-	+	+	+	-	-	-	+
Oracle - Identity and Access Management	+	+	+	+	+	+	-	+	+	+	-	-	-	+
RSA - Security Suite	+	+	+	+	+	-	+	-	+	O	-	+	-	+
Siemens - DirX	+	+	+	+	+	+	O	+	+	+	-	-	-	+
Sophos - Security and Data Protection	+	+	O	+	-	-	O	-	-	+	O	+	-	O
Sun - Identity Management	+	+	+	+	+	+	O	+	+	O	-	-	-	O
Symantec - Control Compliance Suite	+	+	O	+	O	-	-	-	-	O	-	-	-	+
University of Kent - Permis	+	+	O	+	+	-	O	-	+	+	-	-	-	-

Legend:

+	fulfilled
O	partial fulfilled
-	not fulfilled

Status quo - standards

- General:
  - Open Cloud Computing Interface (OCCI)
  - Amazon EC2 API
  - VMware’s DMTF-submitted vCloud API
  - Rackspace API
  - Cloud Data Management Interface (CDMI)
- Security:
  - OASIS SAML
  - Key Management Interoperability Protocol(KMIP)
  - Generic Security Services Application Program Interface (GSS-API)

SM objects (1)

- **Security functions provided by Cloud service providers**
  - Example: Amazon Elastic Compute Cloud (Amazon EC2) Security
  - Multifactor authentication (knowledge and ownership)
  - Control privileges + supporting of credentials like X.509 Certificate/proprietary Amazon Secret Access Key (e.g. to sign API calls)
  - Key management
  - Access is logged + audited
  - Multiple geographic regions as well as across multiple availability zones

SM objects (2)

- **Cloud security management services**
  - Example: PingFederate
  - Identity-as-a-Service
  - federating identity management
- **Security management objects within interfaces**
  - Example: Cloud Data Management Interface (CDMI)
  - User + entity authentication, authorisation and access controls
  - Data integrity + data at-rest encryption + crypto key management
  - Audit and meta-data management

Q&A and Discussion

Michael Kretzschmar
Universität der Bundeswehr München
Werner-Heisenberg-Weg 39
85579 Neubiberg
Germany
Phone +49 (0)89 6004 4764

This research activity has been performed partially in cooperation with the Bundesamt für Sicherheit in der Informationstechnik (German NSA).