



Ústav aplikované informatiky a kvantitativních metod

Bezpečnostní seminář AFCEA 19. 9. 2012



Perspektivy cloud computingu

doc. Ing. Jaroslav Dočkal, CSc.
Ředitel ÚAIaKM VŠKE
Šéfredaktor DSM

Co je cloud computing především?

Nová technologie?

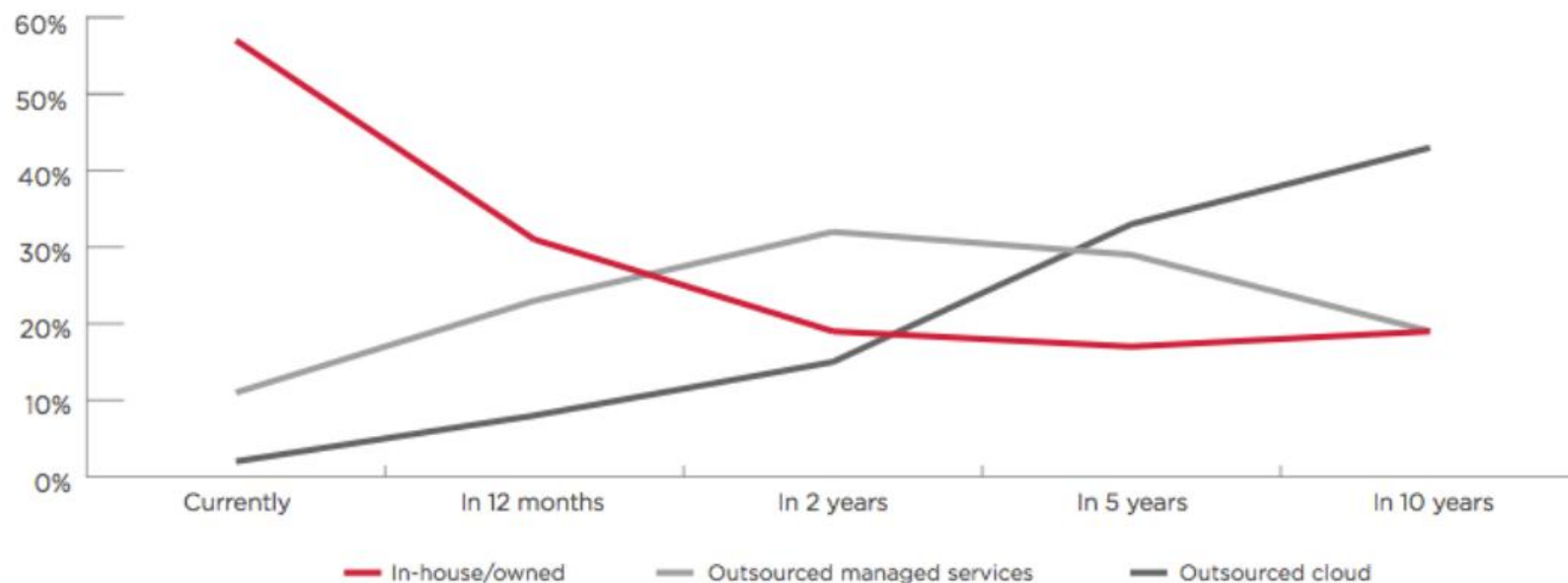
Nová architektura?

Nová metodologie?

Co je cloud computing?

- model poskytování služeb
- Nejde o technologický, ale ekonomický pojem

Desetiletá prognóza



Výzkumná firma Vanson Bourne pro získání podkladů oslovila 550 IT s rozhodovací pravomocí v USA, Velké Británii, Německu, Japonsku, Hong Kongu a Singapuru.

<http://www.businesscloud9.com/content/cloud-edging-out-outsourcing/11820>

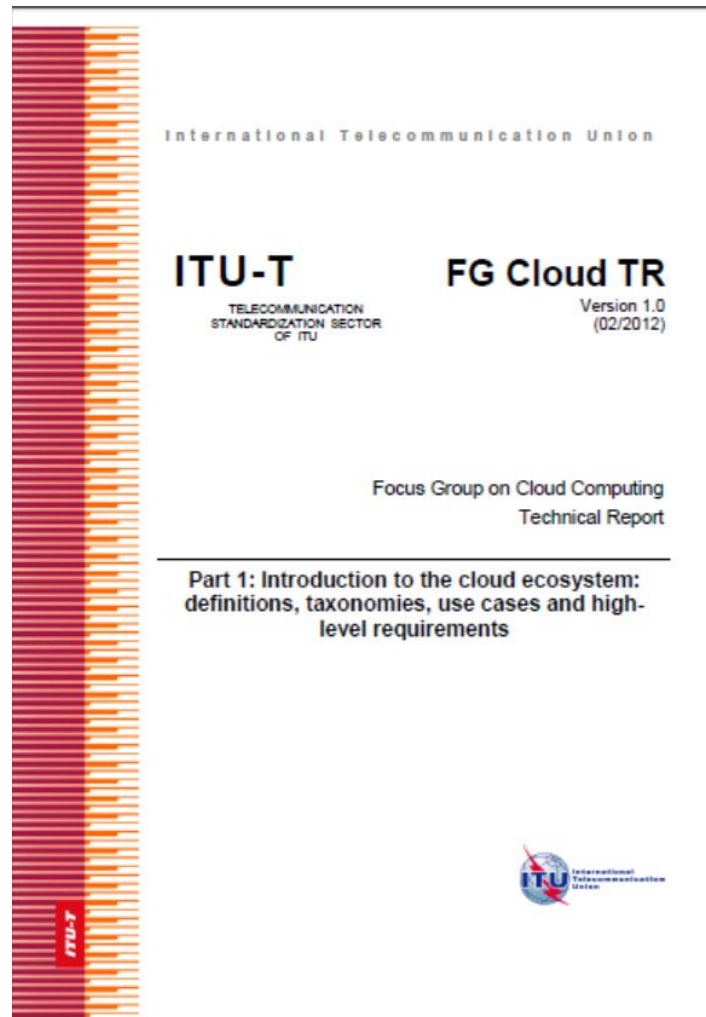
Osnova příspěvku

1. Standardy – jak to s nimi je
2. Je to ekonomický problém

1. Standardy, jak to s nimi je

a) Normy ITU – rok 2012

Joint Coordination Activity on Cloud Computing



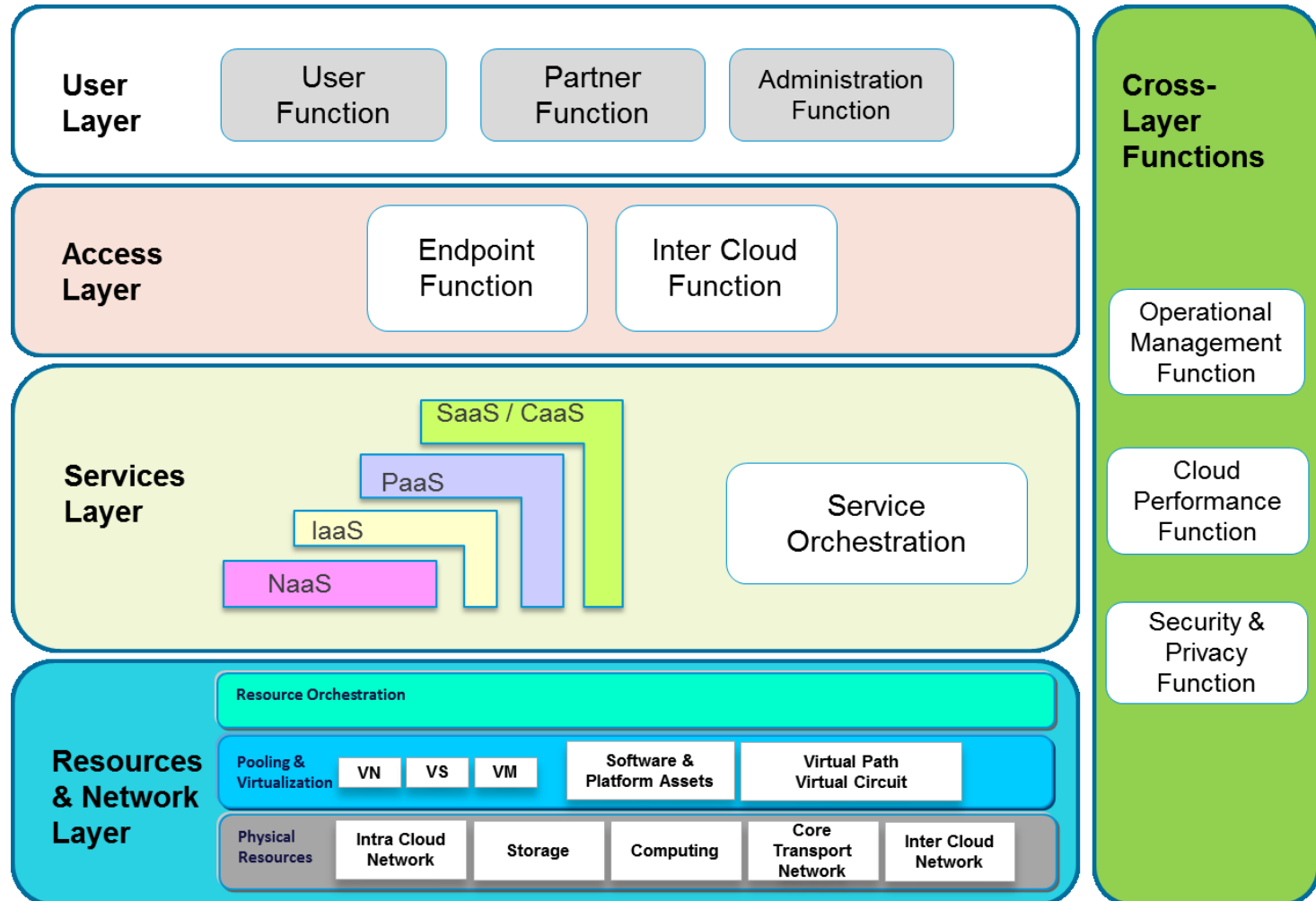
FG Cloud Technical Reports

Organizace ITU-T dokončila svoji předběžnou studii na téma normalizace ekosystému cloudu a vydala své FG Cloud Technical Reports (části 1 až 7). Každá sice vyšla samostatně, ale vzájemně se doplňují:

- 1) Úvod do ekosystému cloudu: definice, taxonomie, případy užití a požadavky
- 2) Funkční požadavky a referenční architektura
- 3) Požadavky a rámec architektury infrastruktury cloudu
- 4) Management zdrojů a analýza děr
- 5) Bezpečnost cloudu
- 6) Přehled SDO (Standards Developing Organizations) zapojených do cloud computingu
- 7) Výhody Cloud computing z hlediska telekomunikací a perspektiv ICT

Tím bylo ukončeno studijního období a jeho výsledky budou pod dohledem *Joint Coordination Activity on Cloud Computing* sloužit pro *Study Group 13* (budoucí síť). Byly identifikovány dva nové typy cloudových služeb, a to **CaaS** a **NaaS** (Communication and Network as a Service). Kromě toho jsou definovány cloud ekosystému a ICT referenční architektura cloudu.

Doplnění CaaS a NaaS do architektury cloudu



Mapování služeb cloudu do jeho typů

	SaaS	PaaS	IaaS	NaaS	CaaS
Desktop as a service				X	
SDPaaS	X	X			X
Komunikační centrum cloudu	X				X
VPN				X	
Pásmo na vyžádání				X	

- Virtuální desktop může snižovat TCO – CAPEX (capital expenditure) i OPEX (operating expenditure)
- SDPaaS (Service Delivery Platform as a Service) – platforma doručení služby jako služba
- Jde o usnadnění přístupu k novým konvergovaným ICT službám (např. IMS, IPTV, M2M/IoT), formátům jako jsou oBIX (Open Building Information Xchange) a schémata XML-oBIX

Klíčová technická řešení DaaS

- **Server-based computing:** Mezi serverem a klientem je přenášena pouze informace z obrazovky klienta. Tato technologie řeší problémy, které se vyskytují při realizaci aplikací na straně klienta.
- **Virtualizace prezentace:** technické řešení, kdy je aplikace uživatelské rozhraní oddělena se od jeho logiky. Aplikace je prezentována na jednom místě a její zpracování, konfigurace a údržba se provádí na jiném místě.
- **Virtualizace desktopu:** technické řešení odděluje prostředí PC desktopu z fyzického počítače pomocí modelu klient-server. Data jsou poskytována zapouzdřená do vzdálené klientské zařízení. Zařízení klienta může používat úplně jinou hardwarovou architekturu, než kterou používá desktopového prostředí, a může být také založena na zcela jiném operačním systému.

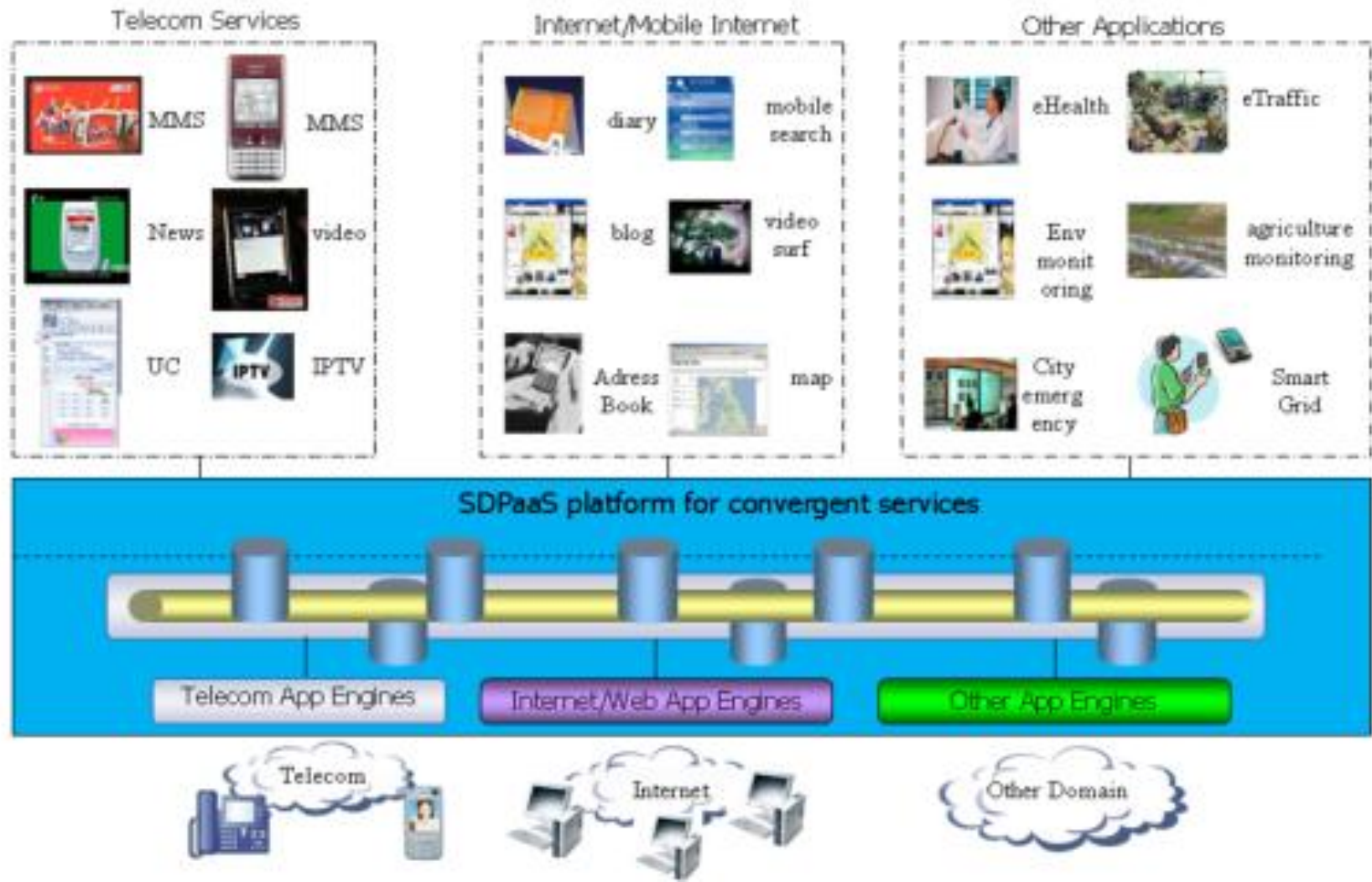
Realizace klienta: dinCloud, Desktonr, Nivie, Applications2U, ICC Global Hosting...

Koncept IoT

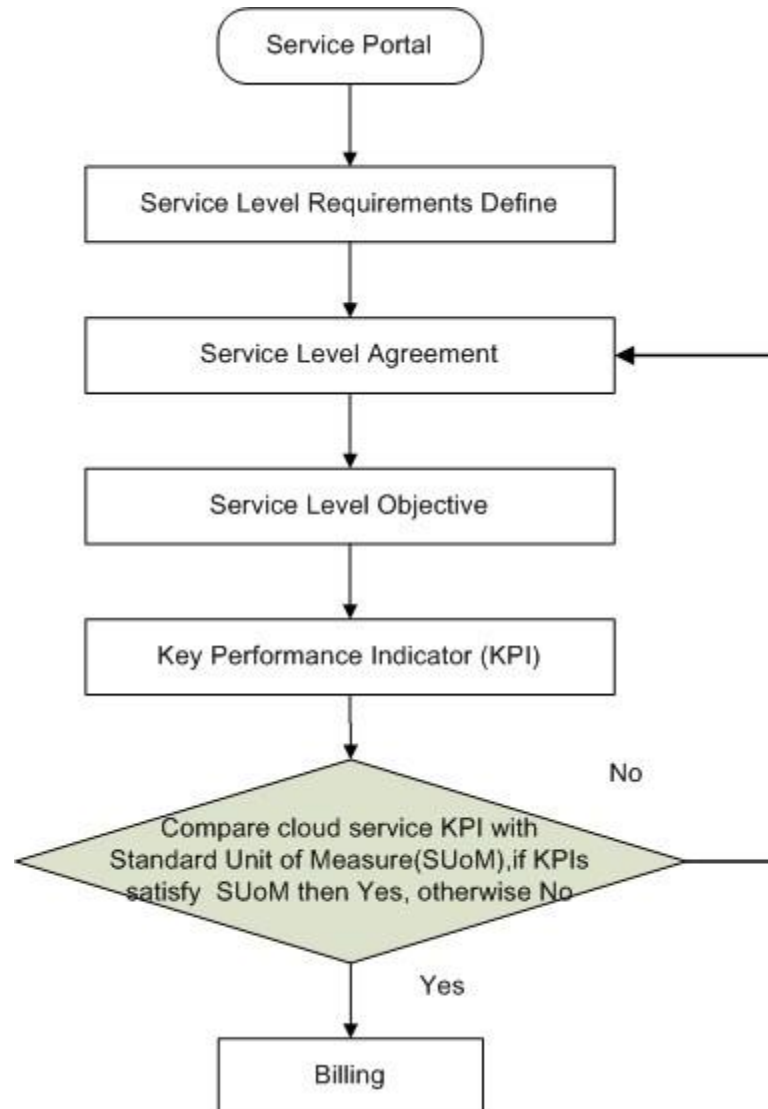
- Internet of Things (IoT) je jeden z nových konceptů, založených na sběru množství informací od velkého množství malých nízkonákladových zařízení (RFID, senzorů, mobilních zařízení atd). Další jsou Internet of Internet of People (IoP), Internet of Energy (IoE), Internet of Media (IoM), Internet of Services (IoS) atd.
- Neboli máme jedno paradigma (úhel pohledu na zkoumanou skutečnost), ale řada scénářů.
- Protokoly rezidenční (např. X10, ZigBee, Z-Wave, Konnex), komerční (např. BACnet, Lonworks), průmyslové (např. Modbus, DeviceNet, ContolNet), automobilní (např. CAN-Bus), měření (M-Bus) a další (Veriticals).



SDPaaS pro konvergované služby (Service Delivery Platform as a Service)



SLA



b) Návrh architektury cloud computingu v publikacích NIST

Special Publication 500-291

NIST Cloud Computing Standards Roadmap – Version 1.0

NIST Cloud Computing Standards Roadmap
Working Group
Michael Hogan
Fang Liu
Annie Sokol
Jin Tong

INTERNETWORK TECHNOLOGIES

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

July 2011



U. S. Department of Commerce

Gary Locke, Secretary

National Institute of Standards and Technology

Patrick D. Gallagher, Director

NIST Special Publication 800-146

Cloud Computing Synopsis and Recommendations

*Recommendations of the National
Institute of Standards and Technology*

Lee Badger
Tim Grance
Robert Patt-Corner
Jeff Voas

COMPUTER SECURITY

Computer Security Division
Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

May 2012



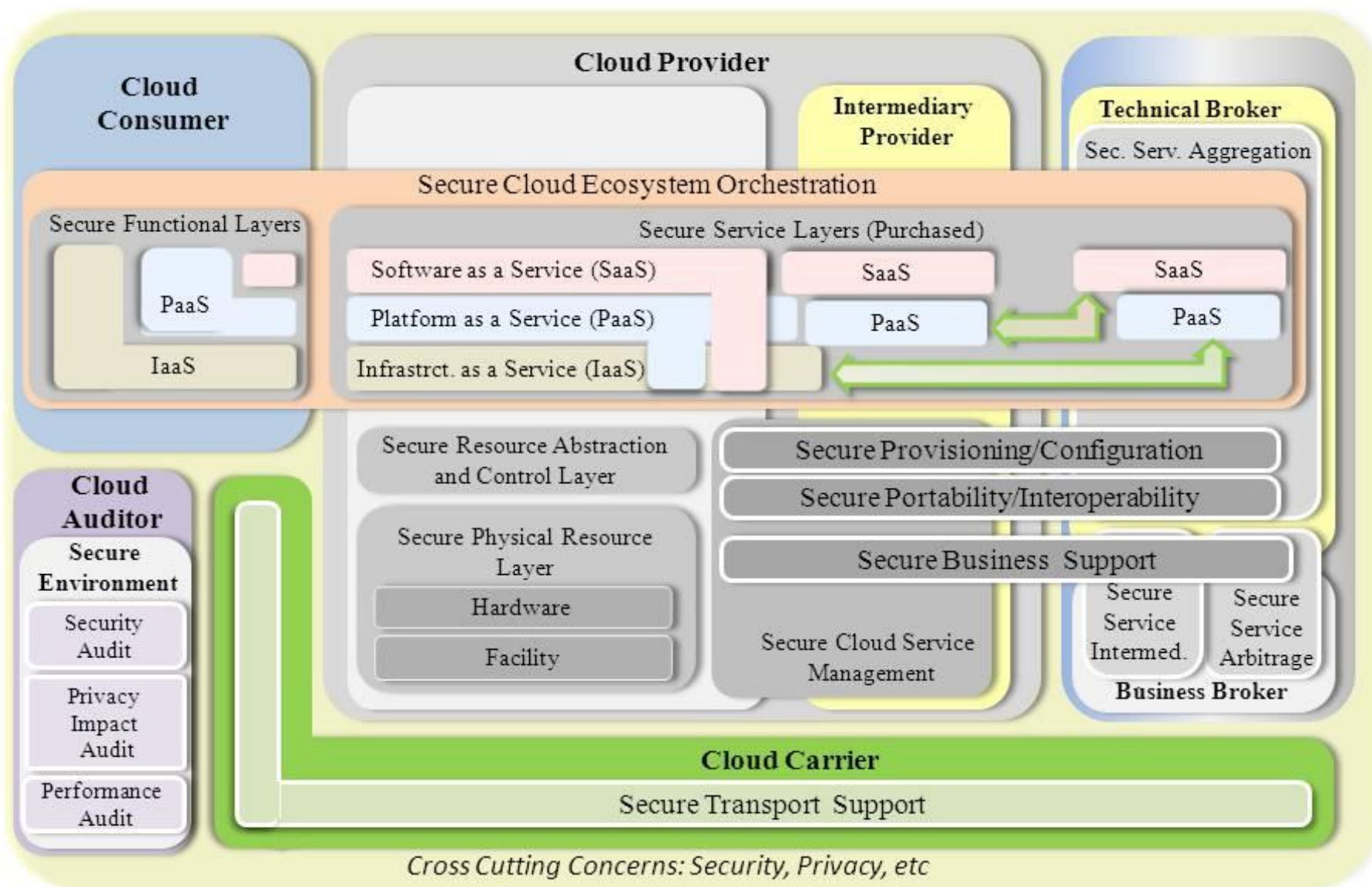
U.S. Department of Commerce

John Bryson, Secretary

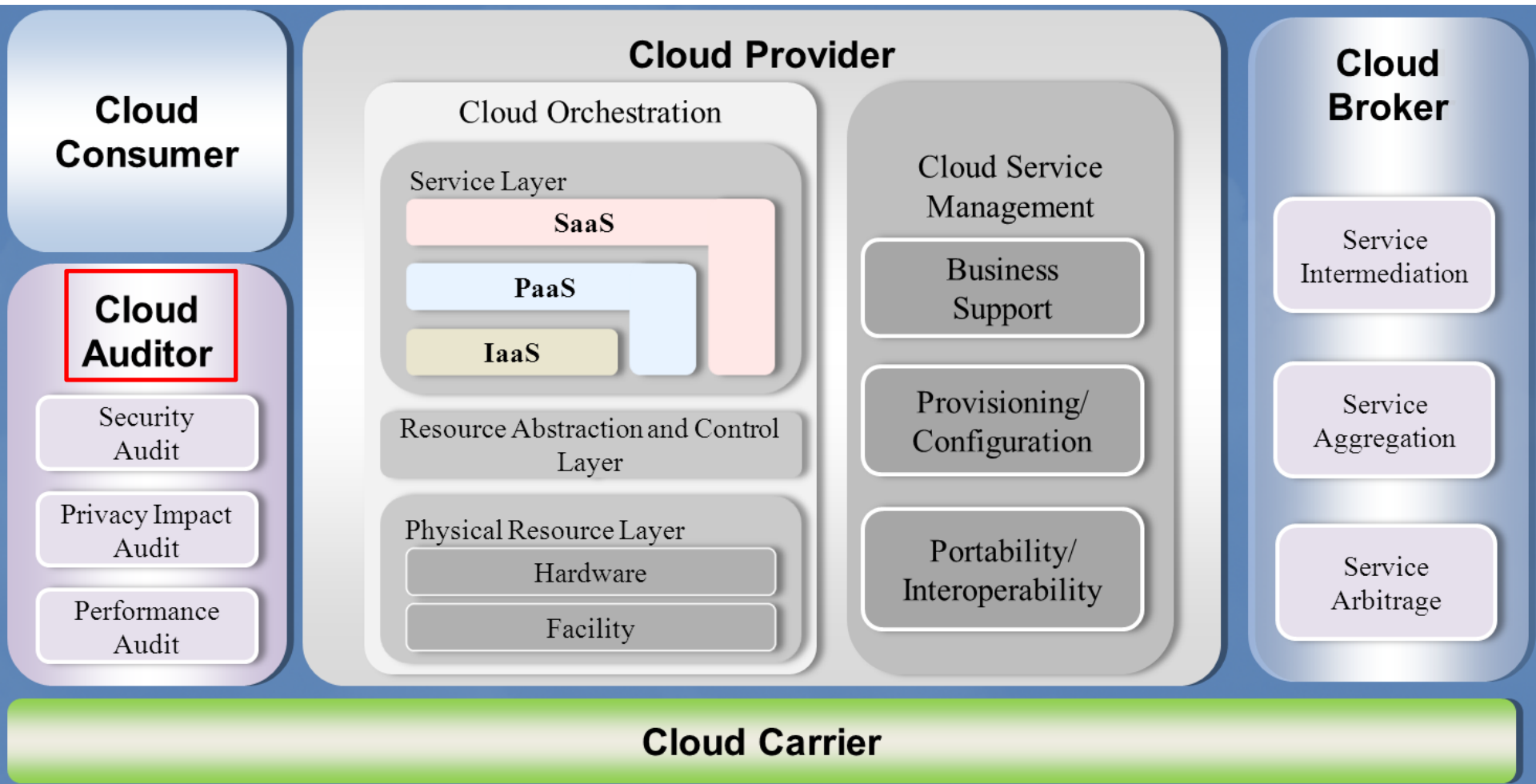
National Institute of Standards and Technology

Patrick D. Gallagher, Under Secretary of Commerce for
Standards and Technology and Director

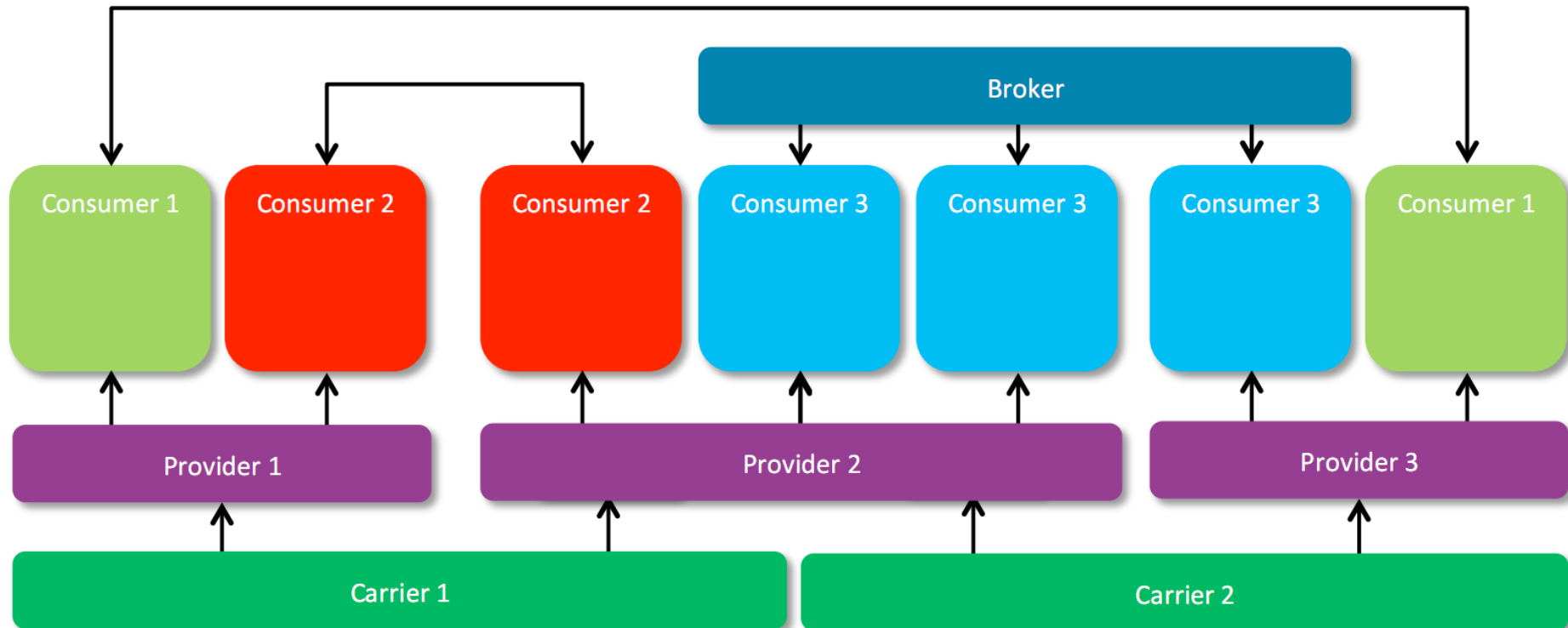
NIST Cloud Computing Security Reference Architecture



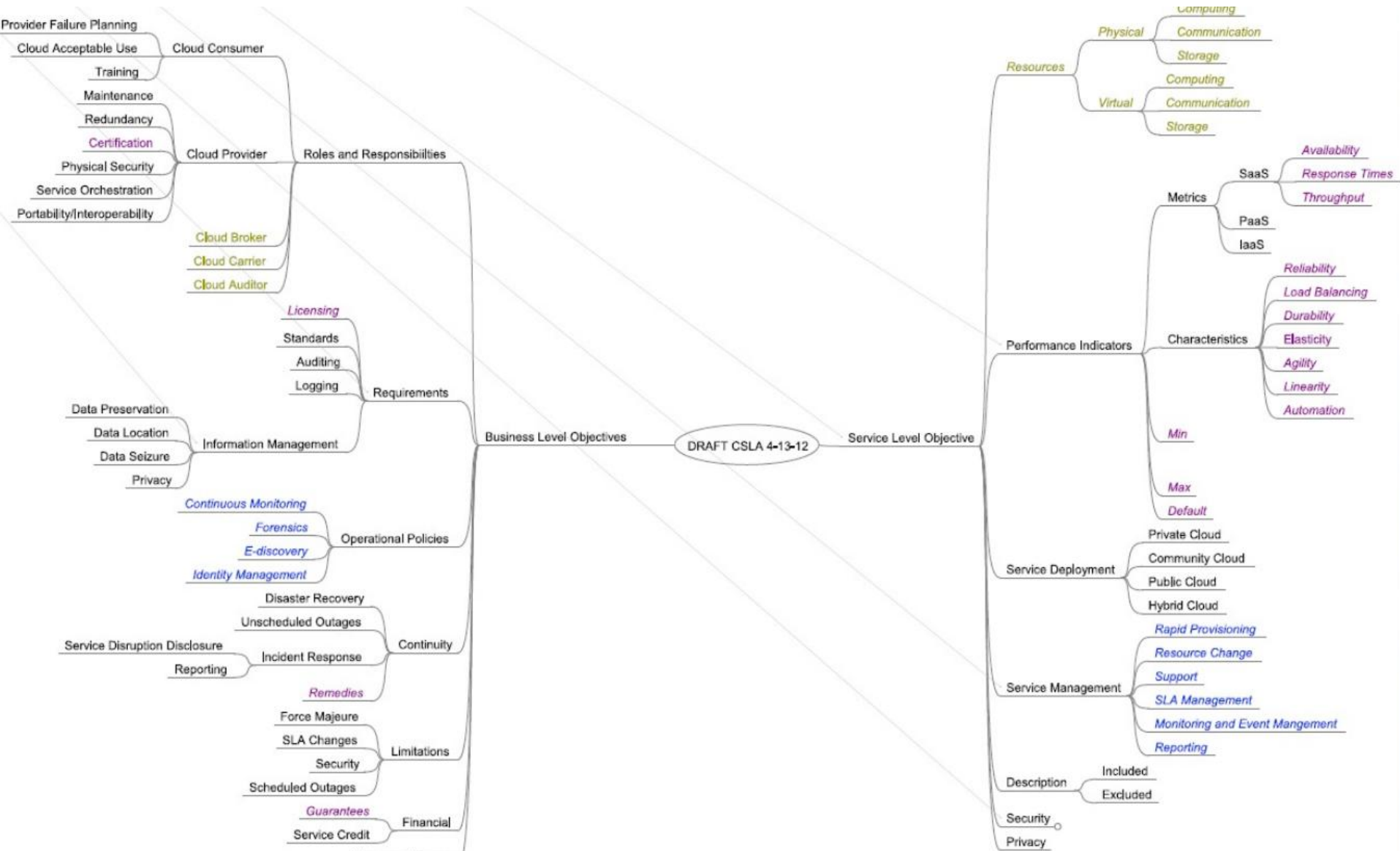
Pět aktérů cloud computingu



Mezi aktéry mohou být složité vztahy



SLA má zde bohatě členěnou strukturu



Součástí SLA je bezpečnostní politika

**UMBC**
AN HONORS UNIVERSITY IN MARYLAND

PROTOTYPE FOR REQUESTING STORAGE SERVICES FROM THE CLOUD

SERVICE ATTRIBUTES [HELP](#)

Expected Start Date (MM-DD-YYYY): [?](#)
Storage size needed (units/month): [?](#)
Service Cost: [?](#)
Service availability: [?](#)
Data Preservation/Backup requirements: [?](#)

REQUEST for Service (RFS)

DATA AND SECURITY POLICIES [HELP](#)

User authentication mechanism: [?](#)
Data Encryption: [?](#)
Data Location: [?](#)
Data Deletion: [?](#)
Virtual Machine (VM) separation: [?](#)
Interface for a storage specification: [?](#)

DISCOVER Services >>

COMPLIANCE POLICIES [HELP](#)

Trusted Internet Connection (TIC) : [?](#)
CC Evaluation Assurance Level (EAL): [?](#)

COMPOSE Services on the CLOUD

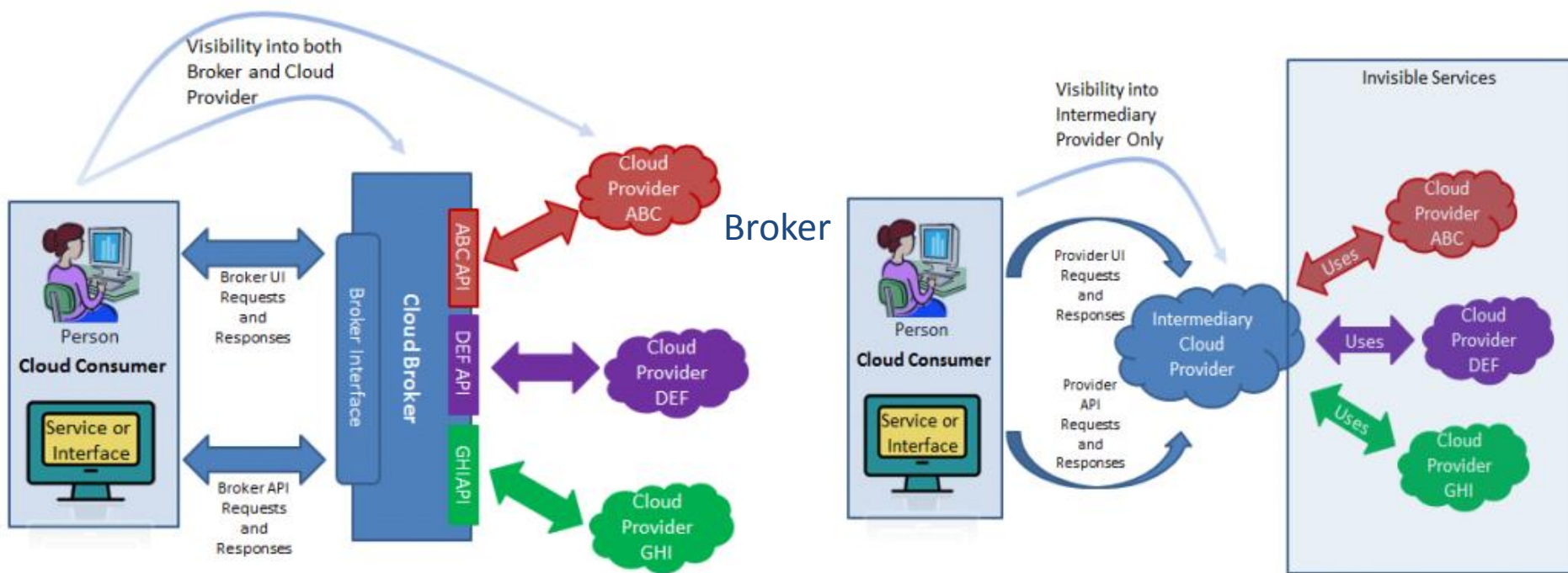
CLOUD INSTANCE [HELP](#)

Size: Speed: Number of cores:

Launch (CONSUME) Service

Výborným cílem útoků je broker

speciální zprostředkovatel (broker) cloud jako mezilehlý poskytovatel služeb dalších cloudů

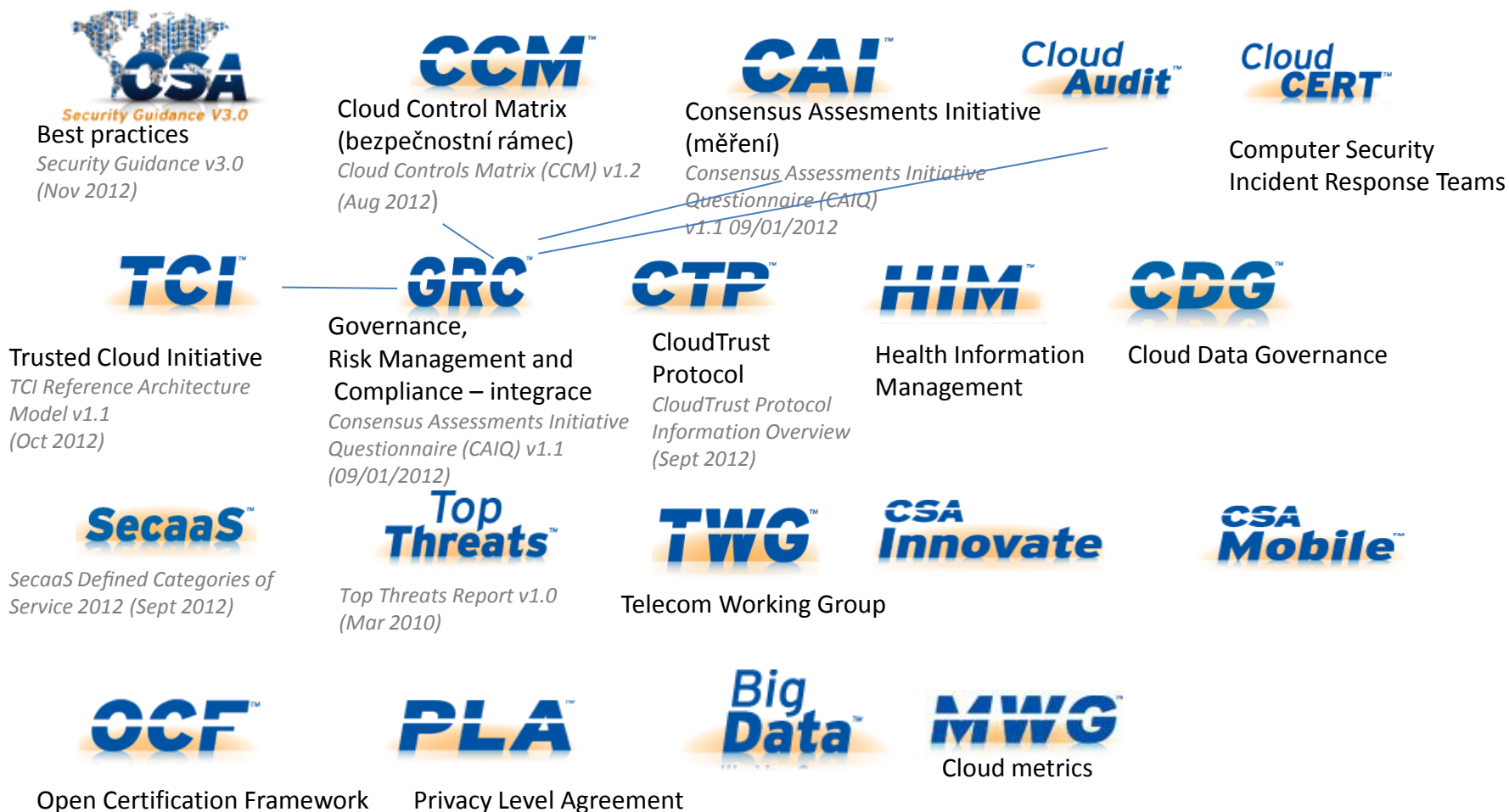


Zprostředkovatel hledá nejlepšího poskytovatele služby (např. cestovní kancelář)

a účtuje si za to příslušné poplatky

Útok: vyberu nejhoršího poskytovatele, navýším poplatky a ty převedu na svůj účet

c) Cloud Security Alliance (cíl: TaaS)



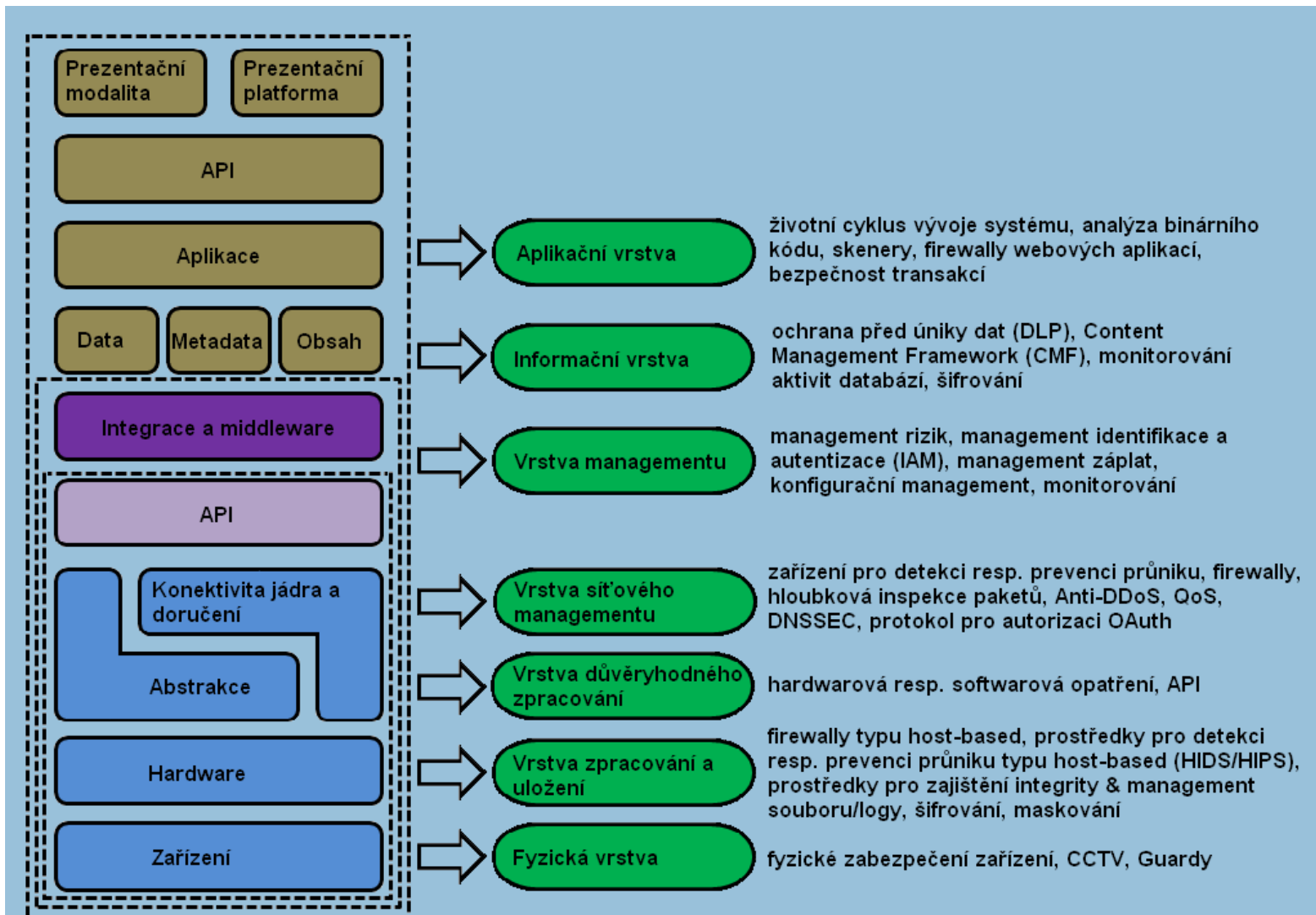
SecaaS Working Group



Table of Contents

Introduction.....	2
Foreword.....	4
Acknowledgments.....	5
Executive Summary	7
Category 1: Identity and Access Management	8
Category 2: Data Loss Prevention.....	10
Category 3: Web Security.....	12
Category 4: Email Security.....	14
Category 5: Security Assessments.....	16
Category 6: Intrusion Management.....	18
Category 7: Security Information and Event Management (SIEM).....	20
Category 8: Encryption.....	22
Category 9: Business Continuity and Disaster Recovery.....	24
Category 10: Network Security.....	26

Mapování modelu cloudu do bezpečnostního modelu



Úkoly Big data WG CSA

- **Analýza big dat z hlediska bezpečnosti** (Fujitsu, HP, SumoLogic) – sběr dat z logů senzorů, M2M, pošty...

Podle McAfee Risk & Compliance Outlook 2012 **60 % respondentů letos instalovalo nástroje pro získání přehledu o svých datech**. Zájem je hlavně o monitorování aktivity databází – aktivity administrátora, neobvyklá čtení/aktualizace, agregace událostí, korelace...

- **Ochrana soukromí** (CipherCloud, DSS)
- **Kryptografické problémy big dat** (Fujitsu)
- **Infrastruktura big dat a útoky proti ní** (Fujitsu, Symantec)
- **Politika a governance** (zatím nikdo)

Podle <http://www-01.ibm.com/software/data/bigdata> 90 % dat vzniklo v posledních dvou letech



d) Open Grid Forum – standardy

(v oblasti bezpečnosti spolupracuje s CSA)

- Bezpečný a rychlý datový přenos (GridFTP, SRM)
- Data Format Description (DFDL)
- Dohody o službách (WS-Agreement, WS-Agreement Negotiation)
- Federated Identity Management (FedSec-CG)
- Řízení důvěryhodného ekosystému (CA operations, AuthN/AuthZ)
- Virtual Organization Management (VOMS)
- Job Submission and Workflow Management (JSDL, BES)
- Management sítě (NSI, NML, NMC, NM)
- Rozhraní pro cloud computing (OCCI)
- Management distribuovaných zdrojů (DRMAA, SAGA, etc.)
- **Firewall Traversal (FiTP)**

Transakční firewall FiTP

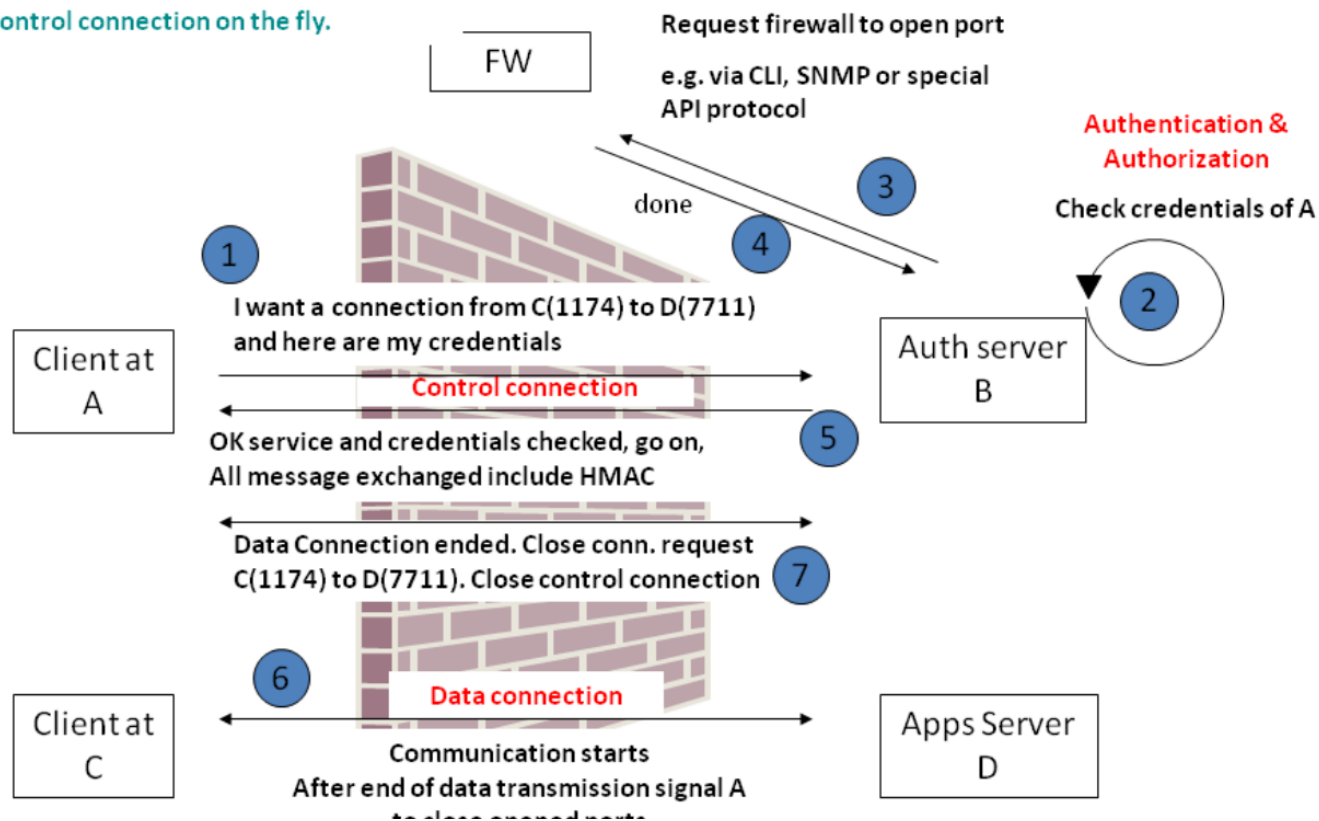
GFD-R-P.196

FVGA-WG May 15, 2012

<http://forge.gridforum.org/sf/projects/fvga-wg>

Ralph Niederberger, Research Center Jülich

3 and 4 are needed only, if
intermediate firewall cannot read
control connection on the fly.



Firewall je transparentní, a to na rozdíl od některých rozšíření iptables (např. Dyna-Fire, který používá Port Knocking) pro Linux. Je určen pro SIP, H.323, FTP atd.



e) Business Application Software Developers Association

10 Special Interest Groups (SIGs)

- Financials SIG
- HR & Payroll SIG
- eBusiness SIG
- Tax and Final Accounts SIG
- Construction SIG
- Marketing SIG
- Green SIG
- Logistics & Supply Chain SIG
- **Cloud Awareness SIG (od roku 2010 pořádá Business Cloud Summit London)**
 Úkol: vzdělávání a komunikace mezi vývojáři, uživateli a výrobci.
- Public Sector SIG

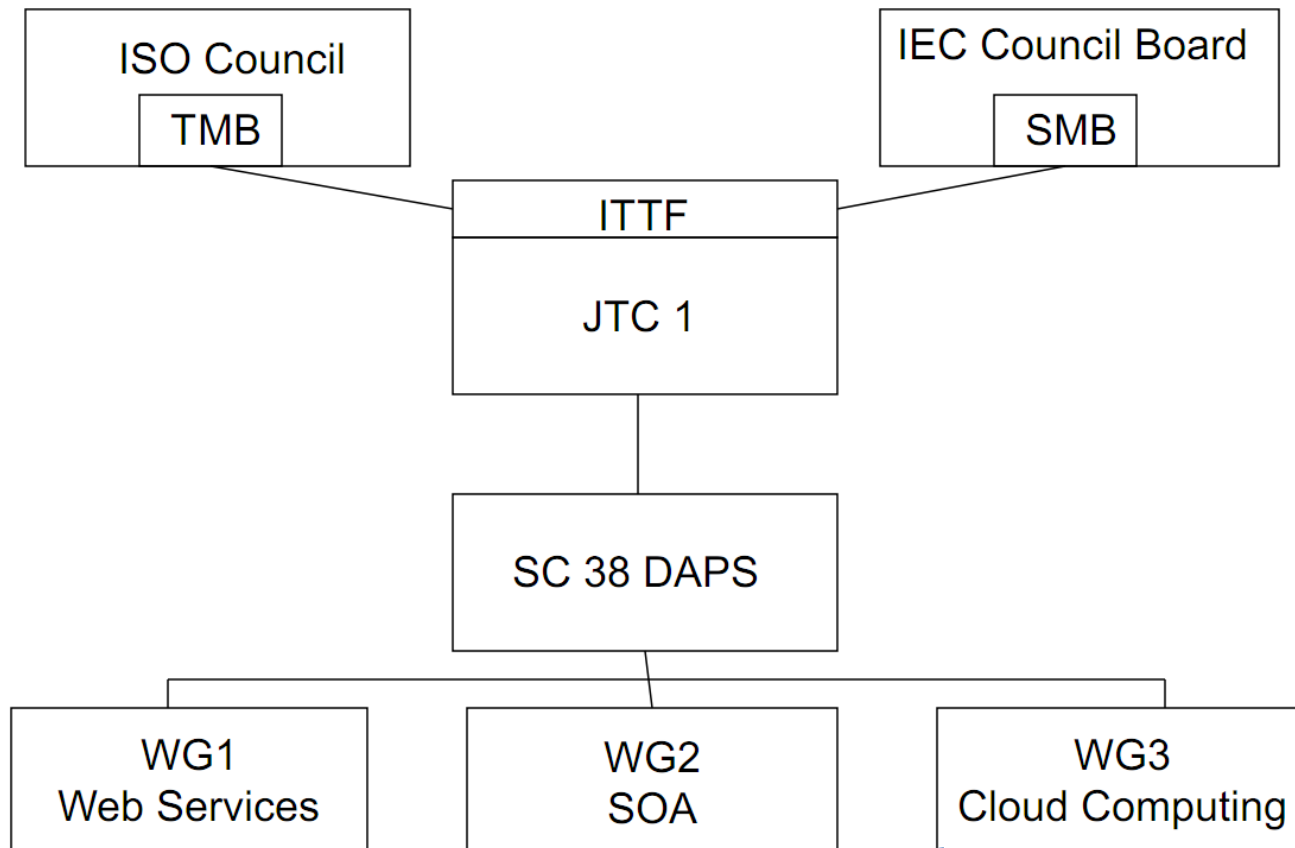


f) EuroCloud

EuroCloud je nezávislá nezisková organizace budovaná na dvou úrovních (koordinátoři, výbory zastupující oficiální členy). Během dvou let má zastoupení koordinátory v 10 zemích a oficiálními členy je 17 evropských zemí. **Česká republika** nemá ani koordinátora. Koordinátor pro **Slovensko** je Juraj Zelenay (juraj.zalanay@itmg.sk) – ze společnosti ITMG, kde má na starost jako konzultant produkty společnosti SAP. Proč člověk ze SAPu?

SAP Business One OnDemand představený letos na CEBITu je vhodný pro **malé firmy a pobočky** velkých podniků, kteří chtějí nasadit svůj první komplexní ERP software. Zákazníci se mohou rozhodnout pro model s využitím cloudového řešení anebo mohou cloudové řešení zkombinovat se softwarem nainstalovaným u sebe, a tak se vyhnout velkým jednorázovým výdajům nebo kapitálovým investicím.

h) ISO SC38 WG3 – probuzení v roce 2012 (obvyklé vyčkávání, až co jiní)



první schůzka únor 2012 – slovník

ČR: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví

g) IEEE bude od roku 2014 vydávat



Standardy pro interoperabilitu

- **IEEE:** CPWG/2301 WG Cloud Profiles WG Working Group
Guide for Cloud Portability and Interoperability Profiles (CPIP)
- **IEEE:** CPWG/2301 WG Cloud Profiles WG Working Group
Standard for Intercloud Interoperability & Federation (SIIF)
- **Open Grid Forum:**
Open Cloud Computing Interface (OCCI)
- **SNIA** (Storage Networking Industry Association):
Cloud Data Management Interface (CDMI)

Standardy pro portabilitu

- **SNIA** (Storage Networking Industry Association):
Cloud Data Management Interface (CDMI)
jde o portabilitu dat
- Distributed Management Task Force (DMTF)
Open Virtualization Format (OVF)
jde o portabilitu systémů
- **IEEE**: CPWG/2301 WG Cloud Profiles WG Working Group
Guide for Cloud Portability and Interoperability Profiles (CPIP)
opět jde o portabilitu systémů

Komunitní cloudy

- Automotive Composites Consortium (DaimlerChrysler, Ford a General Motors)
- HR-XML Consortium (XML pro e-business)
- Web Services Reliable Messaging – pro OASIS (Organization for the Advancement of Structured Information Standards)
- Health Level Seven International (HL7) – ANSI akreditovaná organizace

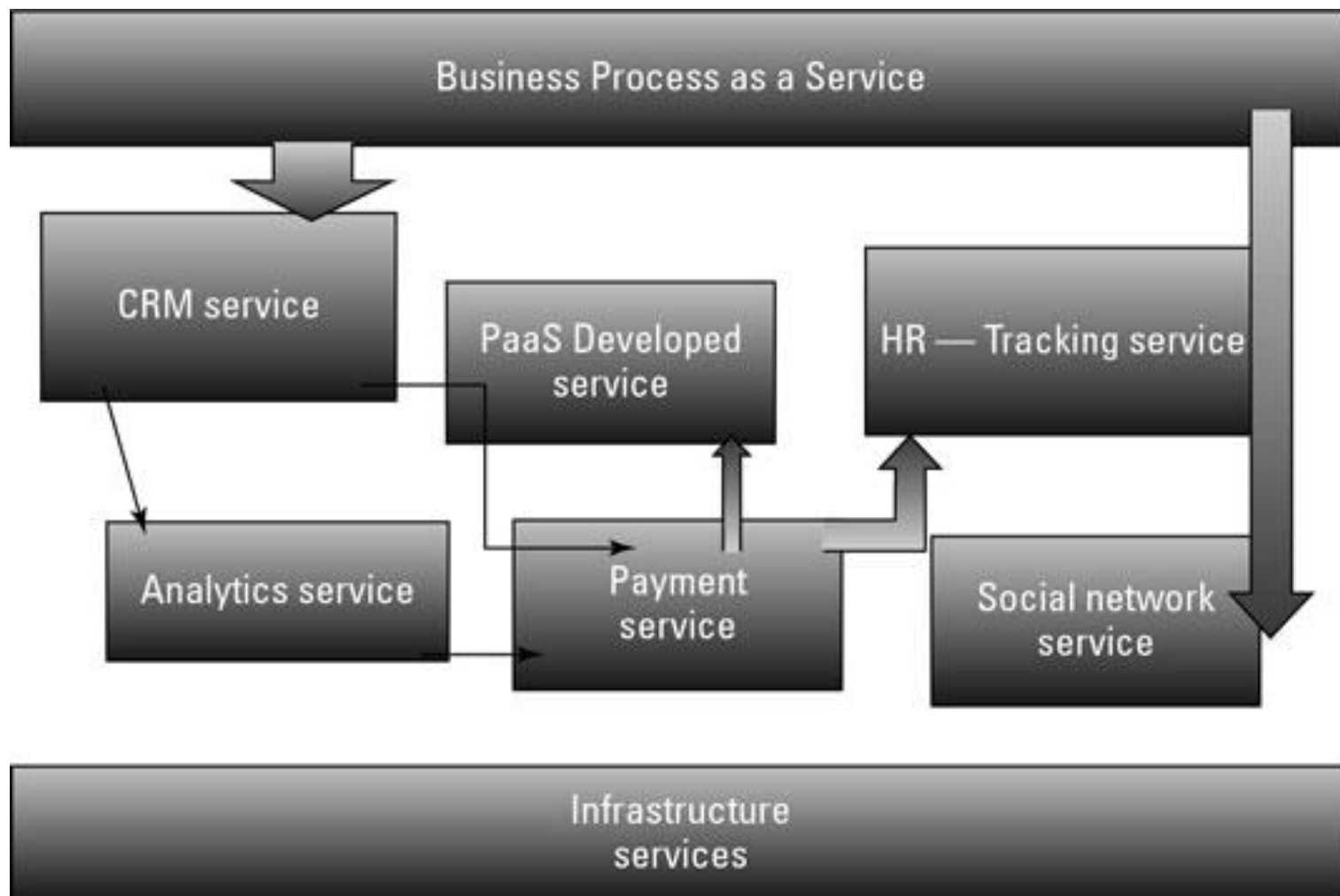
Konsensuální standardy

- Open Virtualization Format (OVF)
- Open Cloud Computing Interface (OCCI)
- Cloud Data Management Interface (CDMI)

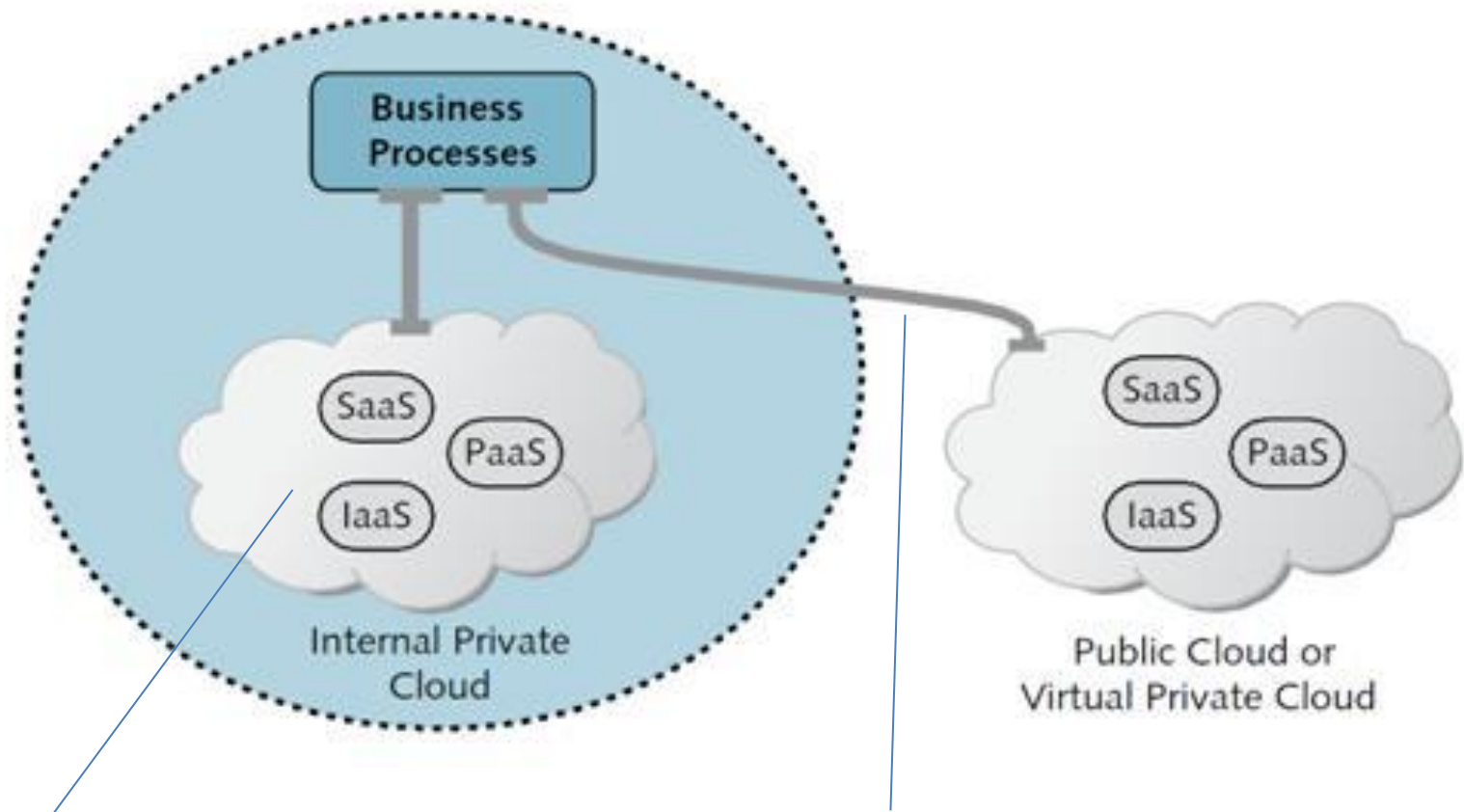
neboli je jich velmi málo!

2. Cloud computing je
především ekonomický
problém

Příklad možného řešení provázanosti služeb v závislosti na business procesech



Business procesy využívají služeb vnitřního privátního a veřejného cloudu



Orchestrace (např. pomocí BPEL –
Business Process Execution Language)

Co mají společné?

Choreografie (např. pomocí WS-CDL –
Web Services Choreography Description Language)

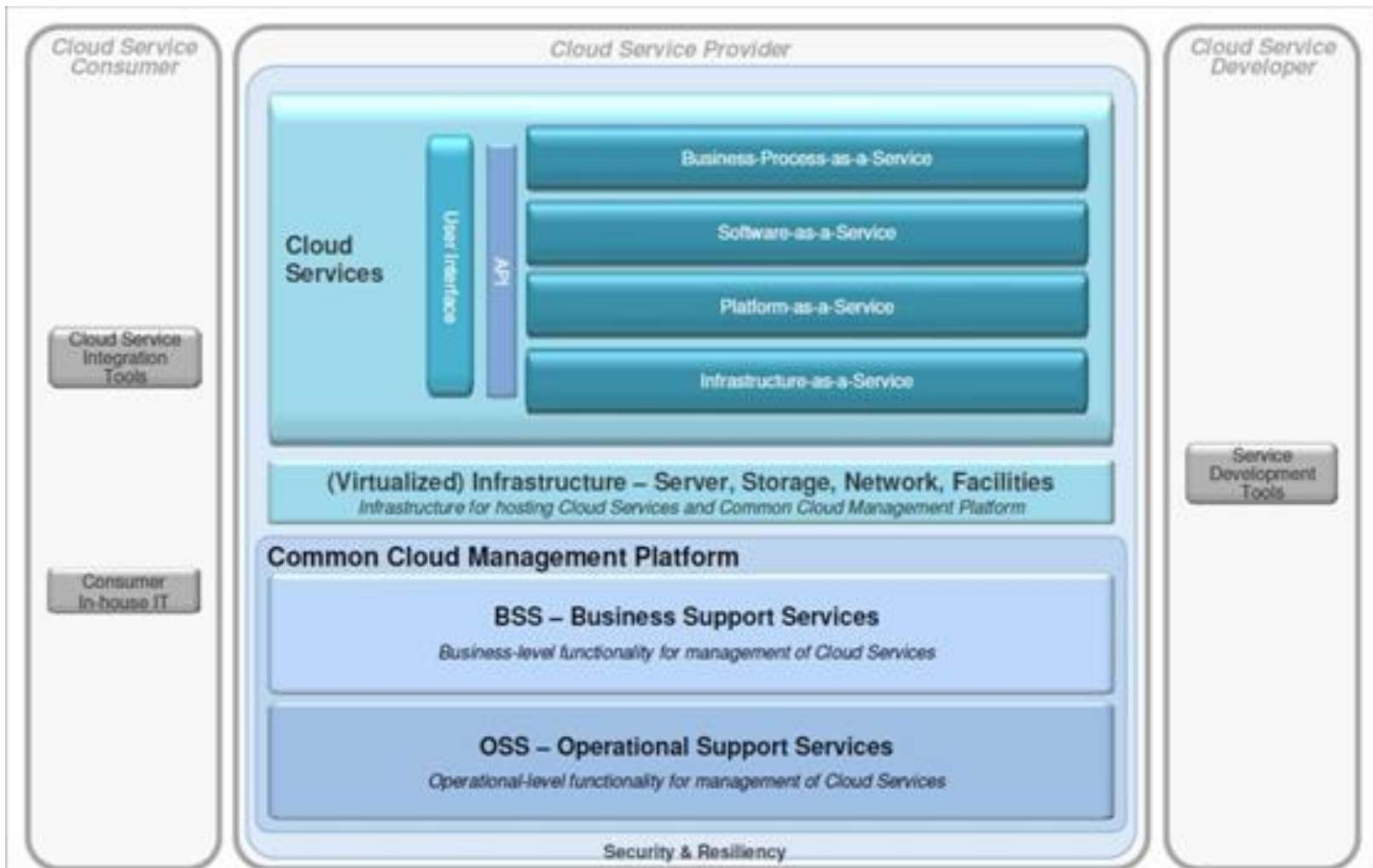
Příklad: Nabídka SaaS společnosti IBM

- sociální spolupráce
- management business procesů
- analýza webu
- management marketingu
- integrace procesů **B2B**
- management zásobovacích procesů
- bezpečnost governance, řízení rizik a dodržování předpisů
- management business

Blíže: <http://thoughtsoncloud.com/index.php/2011/12/business-process-as-a-service-bpaas-delivered-from-the-cloud/>

BPaaS z pohledu IBM

Common Cloud Management Platform Reference Architecture



navrženo IBM proThe Open Group

Ti správní pracovníci jsou okamžitě informováni o příslušných změnách



Porovnání business modelů

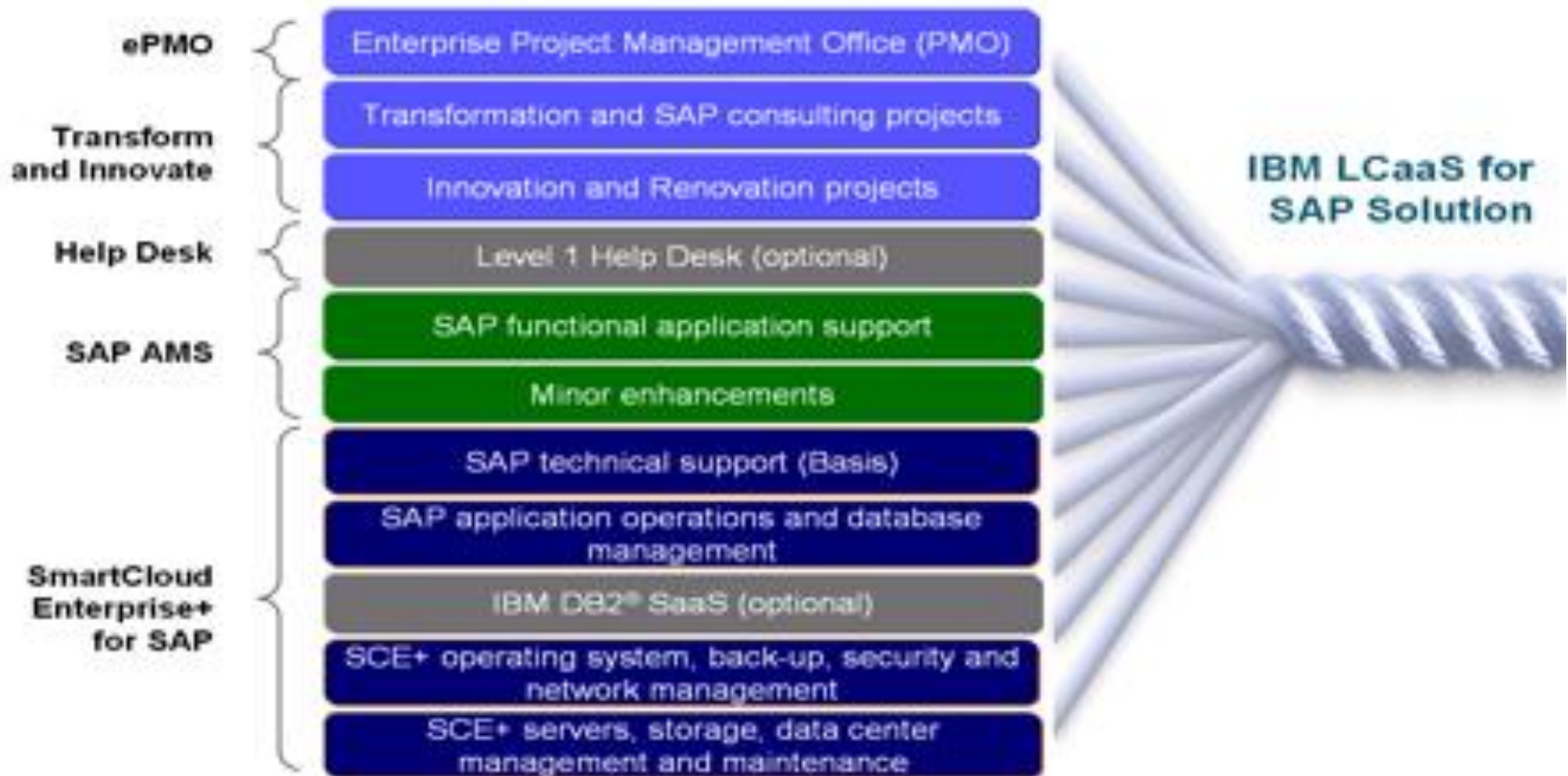
kritérium	Tradiční BPO model	Tradiční IT+BPO model	BPaaS
Vlastnictví aplikace	Zákazník	Zákazník	Poskytovatel služby
Vlastnictví infrastruktury	Zákazník	Zákazník	Poskytovatel služby
Implementace aplikace, podpora a údržba	Zákazník	Poskytovatel služby	Poskytovatel služby
Používání infrastruktury, její podpora a údržba	Zákazník	Poskytovatel služby	Poskytovatel služby
Operace business procesů	Poskytovatel služby	Poskytovatel služby	Poskytovatel služby

TCO je u model BPaaS výrazně menší než u zbývajících modelů!

Úrovně řešení BPaaS

- BP outsourcing v cloudu
- Nové služby (např. *Collaborative Care Solutions* společností IBM a ActiveHealth Management)
- Business Process utility (outsourcing se posune ze vztahu 1:1 na vztah 1:n) pro účetnictví, lidské zdroje, zásobování atd.)

Lifecycle as a Service (LCaaS)



Závěr

- Lze očekávat řadu dalších smysluplných XaaS podporujících business a řešících problém „Big data“ – např. Analytics-as-a-Service (33Across hledá v daném čase vhodné místo pro umístění reklamy na Internetu, Profitero analyzuje ceny konkurence, Sourcefire detekuje malware na korporátní síti a analyzuje, jak se do ní dostal, atd.)
- Standardizační organizace mezi sebou soutěží a konkurují si
- Řada z nich je pod silným vlivem komerčních firem
- Organizací, které vyvíjejí standardy, je přes 200
- Z toho 20 se zabývá vývojem standardů pro cloud computing
- Zde jste byli seznámeni s těmi základními a jejich přínosy pro budoucnost