IT ASOCIÁCIA SLOVENSKA

Hybridný vládny cloud

Peter Weber
Člen prezídia IT Asociácie Slovenska

Medzinárodný kongres ITAPA 2017
Bratislava, 15. 11. 2017

Agenda

- Rámec realizácie Hybridného vládneho cloudu
- Typické prípady využitia Hybridného vládneho cloudu
- Funkcia Sprostredkovateľa v Hybridnom vládnom cloude
- Certifikácia cloudových služieb v Hybridnom vládnom cloude
- Akčný plán a podmienky realizácie Hybridného vládneho cloudu

Rámec realizácie Hybridného vládneho cloudu

- **NKIVS (2016) definovala podoblasť Vládny cloud, ktorá bola detailne rozpracovaná v dokumente Strategická priorita Vládny cloud prijatom v 03/2017.**
- **Strategická priorita predpokladá hybridizáciu Vládneho cloudu: Okrem Dátových centier štátu budú vybrané služby pre zákazníkov verejnej správy (VS) zabezpečovať aj externí poskytovatelia cloudových služieb (CSP) v rámci SR a EÚ.**
- **Hlavným cieľom budovania Hybridného vládneho cloudu je zvýšenie jeho ekonomickej efektívnosti a flexibility.**
  (Cena služieb public cloudu je vždy nižšia ako cena služieb private cloudu.).
- **Cloudové služby (CS) od externých CSP po ich obstaraní a certifikácii z hľadiska bezpečnosti a ochrany osobných údajov budú používané zákazníkmi z VS úplne rovnako ako služby Dátových centier štátu.**

Typické prípady použitia cloudových služieb externých CSP v Hybridnom vládnom cloude

- Pri predpokladanom rýchlom náraste používania cloudových služieb (CS) vo VS bude vhodné používať služby externých CSP v Hybridnom vládnom cloude na základe ekonomickej výhodnosti vždy, keď nepôjde o prácu s citlivými dátami VS.
- Typické príklady z užívateľského hľadiska:
  - **CS na báze Open Data**
  - **CS na báze Big Data**
  - **CS IaaS v prípade Cloud Bursting**
  - **Vybrané CS PaaS**
  - **Vybrané CS SaaS poskytované najmä CSP VS ostatných ČŠ EU**
  - **Kompozitné služby zložené z CS Dátových centier štátu a CS externých CSP**
  - **CS DevOps**
  - **Služby Disaster Recovery**
  - **CS zálohy a archivácie**
  - **Služby Federácie identít**

Funkcia Sprostredkovateľa v Hybridnom vládnom cloude

Funkciu Sprostredkovateľa, Government Cloud Broker (GCB), v Hybridnom vládnom cloude plní ÚPPVII alebo ním poverený subjekt s nasledujúcimi kompetenciami:

- **Prijatie požiadavky na CS od užívateľa z VS formou súboru SLO a SQO.**
- **Priame oslovenie alebo súťaž všetkých akreditovaných CSP v SR a v členských štátoch EÚ (ČŠ EÚ) uvedených v národných repozitároch ako poskytovateľov certifikovaných CS.**
- **Vyhodnotenie odpovedí GCB na publikovanú požiadavku:**
  1. **V prípade splnenia všetkých funkčných požiadaviek GCB overí súlad certifikátu vybranej CS s Národným certifikačným rámcom SR:**
     - Ak **sú splnené** požiadavky Národného certifikačného rámca, GCB zaradí túto CS do zoznamu služieb povolených pre použitie vo VS.
     - Ak **nie sú splnené** požiadavky Národného certifikačného rámca, GCB vyzve CSP, ktorý ponúkol službu, aby zabezpečil doplnenie certifikátu. Po doplnení certifikátu GCB zaradí vybranú službu do zoznamu povolených služieb.

Funkcia Sprostredkovateľa v Hybridnom vládnom cloude (pokr.)

- **Vyhodnotenie odpovedí GCB na publikovanú požiadavku (pokr.):**
  2. **<u>V prípade nesplnenia</u> všetkých funkčných požiadaviek GCB zhodnotí možnosť vytvoriť kompozitnú službu na základe ponúk, alebo informuje zákazníka o možnosti ponúknuť CS spĺňajúcu funkčné požiadavky len čiastočne a zákazník rozhodne o ďalšom postupe.**
     (Napr. zabezpečí vývoj chýbajúcej funkcionality a vytvorí kompozitnú službu s ponúknutou CS, alebo zrealizuje kompletný vývoj služby vlastnými prostriedkami.)

- **GCB po zaradení vybranej CS do zoznamu služieb povolených na použitie vo VS sprostredkuje podpis kontraktu na dodávku CS medzi CSP a zákazníkom.**
  Ak záujem o túto službu majú aj ďalší zákazníci z VS, GCB pre nich sprostredkuje rovnaký kontrakt s CSP bez ďalšieho výberového konania.

- **GCB (v spolupráci s NBÚ) zabezpečí:**
  - **Monitorovanie CS zo zoznamu služieb povolených na použitie vo VS z hľadiska platnosti certifikátu služby a možných bezpečnostných incidentov.**
  - **Notifikáciu všetkých užívateľov tejto CS o pozastavení platnosti certifikátu alebo zistení incidentu v súlade s pripravovaným Zákonom o kybernetickej bezpečnosti.**

Certifikácia cloudových služieb externých CSP z hľadiska bezpečnosti a ochrany osobných údajov

- **Certifikácia CS z hľadiska bezpečnosti a ochrany osobných údajov v prostredí Hybridného vládneho cloudu je jedným z najdôležitejších problémov využívania týchto služieb v prostredí VS.**
  (Pretože užívateľ VS musí mať absolútnu istotu, že sa použitím týchto služieb nevystavuje bezpečnostnému riziku.)

- **Kľúčové na hodnotenie bezpečnosti počítačových systémov vrátane cloudu sú nasledujúce štandardy a smernice:**
  (Okrem toho každý ČŠ EÚ má zvyčajne aj ďalšie regulácie v tejto oblasti.)
  - **Štandardy ISO/IEC série 27 000**
  - **Smernica EK NIS**
  - **Smernica EK GDPR (oblasť ochrany osobných údajov)**

- **Tieto štandardy, zákony a regulácie sú mapované do certifikačných rámcov a detailne popisujú súbor kontrol, ktoré musia byť vykonané, aby bol garantovaný súlad so všetkými mapovanými bezpečnostnými dokumentmi, a spôsob overenia zhody.**

Certifikácia cloudových služieb externých CSP z hľadiska bezpečnosti a ochrany osobných údajov (pokr.)

- Príkladom nadnárodnej cloudovej certifikačnej schémy v Európe je Cloud Security Alliance Open Certification Framework (CSA OCF):
  - **Cloud Controls Matrix: 136 kontrol (+ doplňujúce otázky)**
  - **Spôsob hodnotenia: selfassessment alebo nezávislý audit treťou stranou**
- ÚPPVII musí v nadväznosti na Zákon o kybernetickej bezpečnosti vytvoriť Národný certifikačný rámec ako štandard a metodológiu procesu certifikácie CS. Na urýchlenie tohto procesu je potrebné prevziať existujúci a overený certifikačný rámec, napr. CSA OCF rozvíjaný v rámci projektu Horizon 2020 (projekt EU SEC).
- ÚPPVII v spolupráci s NBÚ musí vytvoriť Národnú certifikačnú autoritu pre CS zodpovednú za:
  - **Aktualizáciu Národného certifikačného rámca**
  - **Notifikácie o zmenách Národného certifikačného rámca pre všetkých akreditovaných CSP**
  - **Akreditáciu audítorov oprávnených vydávať certifikáty CS v súlade s Národným certifikačným rámcom**
  - **Monitorovanie platnosti certifikátov CS**

Akčný plán NKIVS v časti Hybridný vládny cloud

1. **Realizácia NKIVS je rozpracovaná v Akčnom pláne, ktorý bol schválený v RV DVS minulý týždeň.**

2. **Akčný plán je štruktúrovaný v troch úrovniach:**
   (Až do úrovne Nosných aktivít sú stanovené aj časové ciele.)
   - **Podoblasť odpovedajúca strategickej priorite**
   - **Nosné aktivity a činnosti**
   - **Prioritné projekty**

3. **Podoblasť Vládny cloud má v oblasti Hybridného vládneho cloudu dve nosné aktivity:**
   - **Vytvoriť dôveryhodné prostredie**
   - **Realizovať funkcie Sprostredkovateľa Hybridného vládneho cloudu**

4. **Obe aktivity by mali dosiahnuť svoje ciele na operačne využiteľnej úrovni do polovice r. 2018.**
   (Časť Akčného plánu pre Vládny cloud je pre informáciu uvedená v Back-up slidoch.)

5. **Pred ÚPPVII stojí náročná úloha – vytvoriť v priebehu nasledujúcich 6 mesiacov:**
   - **Národný certifikačný rámec CS**
   - **Metodológiu certifikácie CS**
   - **Národnú certifikačnú autoritu**
   - **Funkčného Sprostredkovateľa služieb Hybridného vládneho cloudu**

IT ASOCIÁCIA SLOVENSKA

Ďakujem za pozornosť

Peter Weber

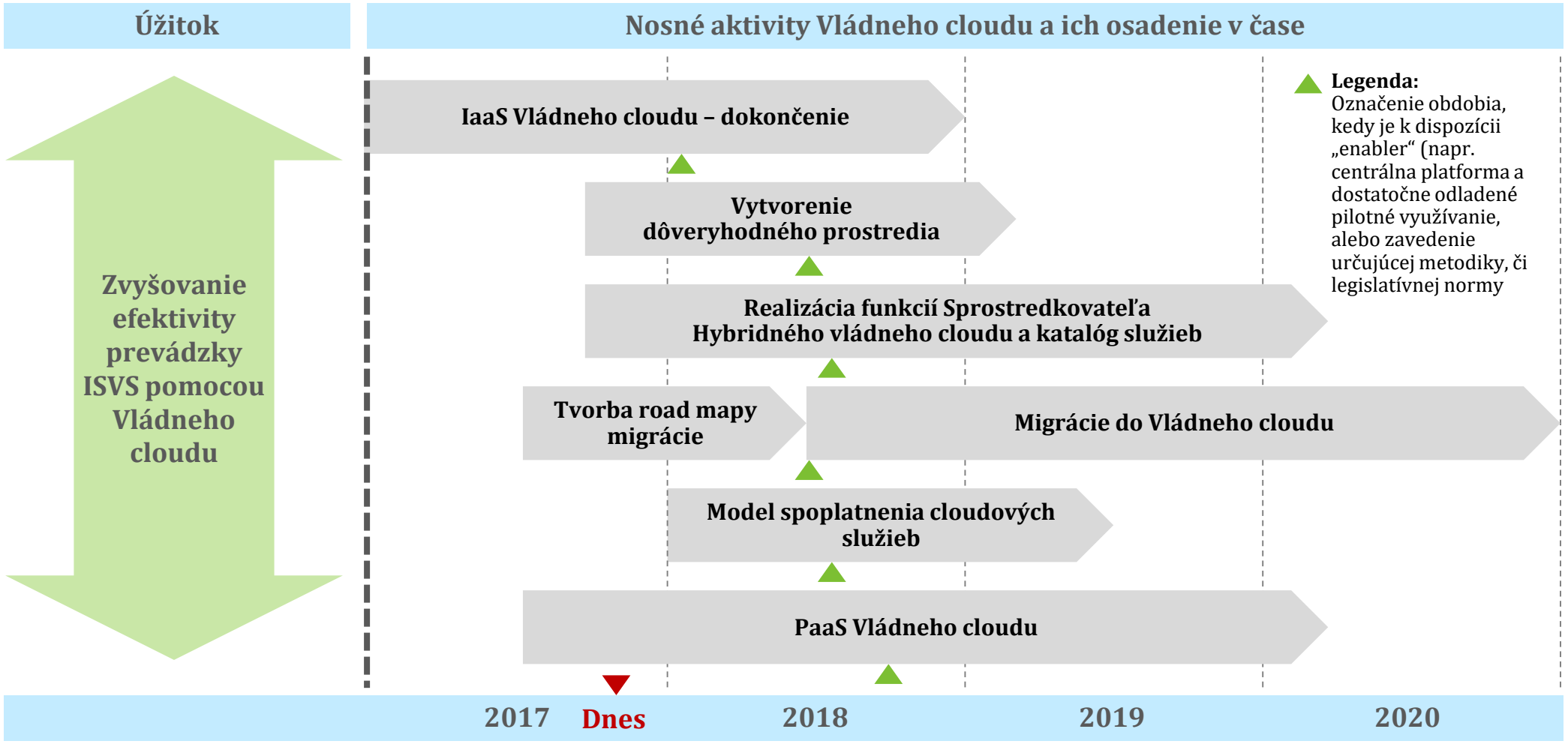
E: weber@itas.sk, **W:** www.itas.sk

IT Asociácia Slovenska

Zdroje:

- http://www.informatizacia.sk/narodna-koncepcia-informatizacie-verejnej-spravy--2016-/22662c
- http://www.informatizacia.sk/strategicke-priority-erf/24190s

Časový harmonogram nosných aktivít Vládneho cloudu



Návrh tém pre prioritné projekty Vládneho cloudu

ID	Projekt	Zdroj financovania	Garant	Indikatívny termín doručenia
1	IaaS vládneho cloudu – rozšírenie portfólia služieb, tak aby migrácia do Vládneho cloudu na tejto úrovni bola jednoduchšia pre čo najväčší počet organizácií (Aktivity: 5.1.1)	OPII	MVSR	2022
2	Vytvorenie dôveryhodného prostredia (certifikácie) a Sprostredkovateľ modelu Hybridného vládneho cloudu. Pre dynamický manažment kapacity Vládneho cloudu bude možné využiť aj overené externé (napr. komerčné) cloudy (Aktivity: 5.1.2, 5.1.3, 5.1.5)	OPII	ÚPPVII	2022
3	PaaS vládneho cloudu. Rozšírenie služieb Vládneho cloudu o služby štandardných stavebných prvkov informačných systémov (napr. databáz, konsolidácie a čistenia údajov, služby prístupovej vrstvy) – pričom správcovia ISVS si tak nebudú musieť tieto prvky stavať v každom projekte a prevádzkovať do najmenšieho detailu. Okrem toho bude PaaS vrstva poskytovať aj špecializované služby na efektívny manažment vývojových, testovacích, integračných a produkčných prostredí tak, aby unikátne SW riešenia mohli pre verejnú správu dodávať aj menšie firmy (úzko špecializované – len na vývoj systému v danej doméne) (Aktivity: 5.1.2, 5.1.3, 5.1.6)	OPII	MVSR	2020

Návrh tém pre prioritné projekty Vládneho cloudu (pokr.)

ID	Projekt	Zdroj financovania	Garant	Indikatívny termín doručenia
4	DCOM migrácia do vládneho cloudu (už prebieha). Centrálne riešenie pokrývajúce veľkú časť samospráv premigruje do prostredia Vládneho cloudu (5.1.4)	ŠR	DEUS	2021
5	Plošné rozšírenie IS DCOM, 2. etapa (DCOM+). Centrálne riešenie bude využívať väčší počet samospráv (5.1.4)	OPII	DEUS	2021
6	Národný projekt migrácie kľúčových ISVS do Vládneho cloudu (centrálny projekt pre rezorty, ktoré sú v rámci informatizácie v súvislosti s migráciou do Vládneho cloudu kľúčové, Aktivity: 5.1.4)	OPII	ÚPPVII v spolupráci s MVSR	2022
7	Dopytové projekty migrácie ISVS do Vládneho cloudu pre ostatné agilné úrady a ich systémy (Aktivity: 5.1.4)	OPII	ÚPPVII v spolupráci s MVSR a príslušné rezorty	2022
8	Centrálny manažment SLA a centralizovaný monitoring výkonu ISVS – zavedenie systematického riadenia a koordinácie SLA medzi rezortmi, ako aj centrálneho monitoringu prevádzky kľúčových ISVS (Aktivity: 5.1.2)	OPII	ÚPPVII	2022