

# ETSI TR 103 126 V1.1.1 (2012-11)



**KLAUD;**  
**Odporúčania pre používateľa klaudu v neverejnom sektore**

**CLOUD;**  
**Cloud private-sector user recommendations**

---

***Európsky inštitút pre telekomunikačné normy***  
***European Telecommunications Standards Institute***

---

**Dôležité upozornenie pre používateľov tejto slovenskej verzie**

ETSI je vlastníkom autorských práv tohto dokumentu ETSI.

V prípade nezrovnalostí medzi anglickou a slovenskou verziou platí anglická verzia tohto dokumentu ETSI.

ETSI neskontroloval preklad a nepreberá žiadnu zodpovednosť za presnosť prekladu tohto dokumentu ETSI.

Anglická verzia tohto dokumentu ETSI sa môže stiahnuť zo stránky:

<http://www.etsi.org/standards-search>

---

**Referenčné číslo**

DTR/CLOUD-0011-UserRec

---

**Kľúčové slová**

CLOUD, Requirements, USER

---

**ETSI**

650 Route des Lucioles  
F-06921 Sophia Antipolis Cedex – France

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C  
Neziskové združenie registrované  
na podprefektúre de Grasse (06) N° 7803/88

---

**Dôležité upozornenie**

Jednotlivé kópie tohto dokumentu možno stiahnuť z

<http://pda.etsi.org>

Tento dokument môže byť dostupný vo viacerých elektronických verziách alebo v tlačenej forme. V prípade existujúceho alebo viditeľného rozdielu v obsahu medzi takýmito verziami je referenčnou verziou verzia v prenosnom dokumentovom formáte (Portable Document Format – PDF).

V prípade sporu je referenčným výtlačok vytlačený na tlačiarni ETSI z verzie PDF uchováanej na určenom sieťovom serveri sekretariátu ETSI.

Používatelia tohto dokumentu by mali brať do úvahy, že dokument môže byť revidovaný alebo sa môže zmeniť jeho postavenie. Informácie o postavení tohto dokumentu a ďalších dokumentov ETSI sú dostupné na

<http://portal.etsi.org/tb/status/status.asp>

Ak nájdete v tomto dokumente chyby, svoje pripomienky zašlite na

[http://portal.etsi.org/chaicor/ETSI\\_support.asp](http://portal.etsi.org/chaicor/ETSI_support.asp)

---

**Oznam o autorských právach**

Nijaká časť sa nesmie reprodukovat' bez písomného povolenia.  
Autorské práva a z toho vyplývajúce obmedzenia sa vzťahujú na reprodukovanie všetkými druhmi médií.

© Európsky inštitút pre telekomunikačné normy 2012.  
Všetky práva vyhradené.

**DECT™**, **PLUGTESTS™**, **UMTS™** sú obchodné značky ETSI registrované na prospech jej členov.  
**3GPP™** a **LTE™** sú obchodné značky ETSI registrované na prospech jej členov a partnerských organizácií 3GPP.  
**GSM®** a logo GSM sú registrované obchodné značky vo vlastníctve asociácie GSM.

---

## Obsah

Práva duševného vlastníctva .....	4
Predhovor .....	4
1 Predmet .....	4
2 Referenčné dokumenty .....	4
2.1 Normatívne referenčné dokumenty .....	4
2.2 Informatívne referenčné dokumenty .....	4
3 Definície a skratky .....	6
3.1 Definície .....	6
3.2 Skratky .....	7
4 Prípady použitia klaudových služieb .....	8
4.1 Podnik-Klaud-Podnik (angl. Enterprise to Cloud to Enterprise) .....	8
4.2 Podnik-Klaud-Koncový užívateľ (angl. Enterprise to Cloud to End User) .....	8
4.3 Podnikový komunitný klaud (angl. Enterprise Community Cloud) .....	8
5 Funkčné odporúčania pre klaudové scenáre .....	9
5.1 Identita a overovanie autenticity .....	9
5.2 Riadenie prístupu .....	9
5.3 Správa údajov a regulačný súlad .....	9
5.4 Meranie a monitorovanie .....	10
5.5 Prístup na sieť .....	10
5.6 Riadenie a správa .....	11
5.7 Bezpečnosť .....	11
5.8 Interoperabilita .....	12
5.9 Prenositeľnosť a zavádzanie .....	13
5.10 Reverzibilita .....	14
5.11 SLA a referenčné úrovne .....	15
5.12 Správa životného cyklu .....	16
6 Mapovanie funkčných odporúčaní pre klaudové scenáre .....	16
História .....	17

---

## Práva duševného vlastníctva

Práva duševného vlastníctva, ktoré majú alebo môžu mať zásadný význam pre daný dokument, sa mohli oznámiť organizácii ETSI. Informácie o týchto zásadných právach duševného vlastníctva, ak existujú, sú pre členov i nečlenov ETSI verejne dostupné a môžu ich nájsť v dokumente ETSI SR 000 314 s názvom: Práva duševného vlastníctva (IPR). Zásadné alebo potenciálne zásadné práva duševného vlastníctva, oznámené organizácii ETSI vo vzťahu k normám ETSI, možno získať na sekretariáte ETSI. Najnovšie znenie je dostupné na serveri ETSI (<http://ipr.etsi.org>).

V súlade so svojou politikou v oblasti práv duševného vlastníctva ETSI neskúma ani nevyhľadáva nijaké práva duševného vlastníctva. Neposkytuje ani záruku na iné práva duševného vlastníctva, ktoré sa neuvádzajú v dokumente SR 000 314 (alebo v jeho aktualizovaných vydaniach na serveri ETSI), ktoré sú alebo môžu byť, alebo by sa mohli stať dôležitými pre predkladaný dokument.

---

## Predhovor

Túto technickú správu (TR) spracovala technická komisia ETSI CLOUD (CLOUD).

---

### 1 Predmet

Dokument poskytuje prehľad odporúčaní pre používateľa kladových služieb v neverejnom sektore, predovšetkým z pohľadu veľkých podnikov v európskom kontexte.

Predkladaný dokument definuje ciele pre budúce požiadavky šandardizácie pri poskytovaní kladových služieb.

---

### 2 Referenčné dokumenty

Referenčné dokumenty sú špecifické (označené dátumom zverejnenia a/alebo číslom vydania, alebo číslom verzie) alebo nešpecifické. Pre špecifické referenčné dokumenty platí len citovaná verzia. Pre nešpecifické referenčné dokumenty platí len posledná verzia referenčného dokumentu (vrátane zmien).

Referenčné dokumenty, ktoré nie sú uznané ako verejne dostupné na očakávanom mieste, je možné nájsť na webovej adrese <http://docbox.etsi.org/Reference>.

POZNÁMKA. – Aj keď všetky hypertextové odkazy obsiahnuté v tomto článku platili v čase publikovania, ETSI nemôže zaručiť ich dlhodobú platnosť.

#### 2.1 Normatívne referenčné dokumenty

Uvedené dokumenty sú nevyhnutné na použitie tohto dokumentu.

Neaplikuje sa.

#### 2.2 Informatívne referenčné dokumenty

Uvedené dokumenty nie sú dôležité pre aplikáciu tohto dokumentu, ale pomáhajú používateľovi v konkrétnej predmetnej oblasti.

[i.1] "Cloud Computing Use Cases White Paper Version 4.0".

POZNÁMKA. – Dostupné na: <http://cloudusecases.org>

[i.2] USERS Recommendations from the European CIO Association for the success of the CLOUD computing in Europe, 30 January 2012.

POZNÁMKA. – Dostupné na:

[http://ec.europa.eu/information\\_society/activities/cloudcomputing/docs/consolidated\\_list\\_of\\_recommendations\\_users\\_%20perspective.pdf%5b1%5d.pdf](http://ec.europa.eu/information_society/activities/cloudcomputing/docs/consolidated_list_of_recommendations_users_%20perspective.pdf%5b1%5d.pdf)

[i.3] "The NIST Definition of Cloud Computing", Special Publication 800-145, September 2011.

POZNÁMKA. – Dostupné na: <http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf>

[i.4] ETSI TR 102 997 (V1.1.1): "CLOUD; Initial analysis of standardization requirements for Cloud services".

---

## 3 Definície a skratky

### 3.1 Definície

Na účely tohto dokumentu platia termíny a definície uvedené v NIST Definition of Cloud Computing [i.3]:

#### Modely služby:

**Softvér ako služba (SaaS)** (angl. Software as a Service): *schopnosť používať aplikácie poskytovateľa prevádzkované v kladovej infraštruktúre, ktorá sa poskytuje spotrebiteľovi. Aplikácie sú dostupné z rôznych klientských zariadení prostredníctvom rozhrania tenkého klienta, napríklad webového prehliadača (napr. webový e-mail) alebo programového rozhrania. Spotrebiteľ nespravuje ani neriadi základnú kladovú infraštruktúru, vrátane siete, serverov, operačných systémov, úložného priestoru, alebo dokonca jednotlivé vlastnosti aplikácií, s možnou výnimkou obmedzeného nastavenia konfigurácie aplikácie špecifickej pre používateľa.*

**Platforma ako služba (PaaS)** (ang. Platform as a Service): *schopnosť, poskytovaná spotrebiteľovi, nasadiť do kladovej infraštruktúry aplikácie, vytvorené spotrebiteľom alebo získané použitím programovacích jazykov, knižníc, služieb a nástrojov podporovaných poskytovateľom. Spotrebiteľ nespravuje ani neriadi základnú kladovú infraštruktúru, vrátane sietí, serverov, operačných systémov alebo úložného priestoru, ale ovláda nasadené aplikácie a prípadné nastavenie konfigurácie v prostredí hostovania aplikácie.*

**Infraštruktúra ako služba (IaaS)** (ang. Infrastructure as a Service): *schopnosť, poskytovaná spotrebiteľovi, poskytovať počítačové spracovanie, úložný priestor, sieť a ďalšie základné výpočtové zdroje, pri ktorej je spotrebiteľ schopný nasadiť a spustiť ľubovoľný softvér, ktorý môže obsahovať operačné systémy a aplikácie. Spotrebiteľ nespravuje ani neriadi základnú kladovú infraštruktúru, ale ovláda operačné systémy, úložný priestor a nasadené aplikácie; a prípadne obmedzene riadi výber sieťových komponentov (napr. hostiteľské firewally).*

#### Modely zavádzania:

**Neverejný klad** (angl. private cloud): *kladová infraštruktúra sa poskytuje na výhradné používanie jednej organizácii, ktorá má viacerých spotrebiteľov (napr. obchodné jednotky). Vlastniť, spravovať a prevádzkovať ho môže organizácia, tretia osoba alebo nejaká ich kombinácia, pričom môže existovať vo vlastných alebo v cudzích priestoroch.*

**Komunitný klad** (angl. community cloud): *kladová infraštruktúra sa poskytuje na výhradné používanie určitej komunity spotrebiteľov v organizáciách, ktoré majú spoločné záujmy (napr. úloha, požiadavky na zabezpečenie, politiku a zhodné dôvody). Vlastniť, spravovať a prevádzkovať ho môže jedna alebo viaceré organizácie v komunite, tretia osoba alebo nejaká ich kombinácia, pričom môže existovať vo vlastných alebo v cudzích priestoroch.*

**Verejný klad** (angl. public cloud): *kladová infraštruktúra sa poskytuje širokej verejnosti na všeobecné použitie. Môže ho vlastniť, spravovať a prevádzkovať podnik, akademická alebo štátna organizácia, alebo nejaká ich kombinácia. Umiestnený je v priestoroch kladového poskytovateľa.*

**Hybridný klad** (angl. hybrid cloud): *kladová infraštruktúra sa skladá z dvoch alebo viacerých odlišných kladových infraštruktúr (neverejná, komunitná alebo verejná), ktoré sú aj naďalej jedinečnými entitami, ale sú navzájom spojené pomocou štandardnej alebo vlastníckej technológie, ktorá umožňuje prenositeľnosť údajov a aplikácií (napr. tzv. cloud bursting na rozdelenie záťaže medzi kladmi).*

Platia aj tieto termíny a definície:

**Zákazník** (angl. customer): subjekt, ktorý nakupuje služby ponúkané iným subjektom.

**Koncový používateľ** (angl. end user): osoba alebo organizácia, ktorá používa kladové služby.

### 3.2 Skratky

CRM	Customer Relationship Management	riadenie vzťahov so zákazníkmi
DMTF	Distributed Management Task Force	pracovná sila pre distribuovanú správu
EC	European Commission	Európska komisia
EU	European Union	Európska únia
IaaS	Infrastructure as a Service	infraštruktúra ako služba
ID	Identity	identita
IT	Information Technology	informačné technológie
NAC	Network Access Control	riadenie prístupu na sieť
PaaS	Platform as a Service	platforma ako služba
PII	Personally Identifying Information	informácia súvisiaca s identifikáciou osoby
QoS	Quality of Service	kvalita služby
SaaS	Software as a Service	softvér ako služba
SLA	Service Level Agreement	zmluva o úrovni služby
VM	Virtual Machine	virtuálny stroj

---

## 4 Prípady použitia klaudových služieb

Nasledujúce ustanovenie predstavuje tri prípady použitia na najvyššej úrovni na základe scenárov pre prípad použitia "Cloud Computing Use Cases White Paper Version 4.0" [i.1] a požiadavky EuroCIO [i.2]. Tieto prípady použitia sú v tomto dokumente základom na zovšeobecnenie dnešných potrieb veľkého podniku. Uvedené odporúčania sa odvádzajú z celkového posúdenia týchto troch scenárov a neskôr sa budú mapovať na tieto scenáre.

### 4.1 Podnik-Klaud-Podnik (angl. Enterprise to Cloud to Enterprise)

Prípad použitia zahŕňa podnik, ktorý používa klaudové služby na podporu svojich interných procesov. V tomto scenári podnik používa klaudové služby na rozšírenie svojich zdrojov, napríklad:

- použitie klaudového úložiska na rozšírenie úložného priestoru pre veľké objemy údajov, na archiváciu zriedkavo používaných údajov, zabezpečenie pružnosti a podporenie spoločného využívania údajov v rámci podniku a s partnermi;
- použitie virtuálnych strojov (VM) v klaude na pridanie ďalšej online procesorovej kapacity na spracovanie špičkovej záťaže služieb a aplikácií (a, samozrejme, zrušenie týchto VM, keď už nie sú potrebné);
- používanie aplikácií v klaude (SaaS) pre určité podnikové funkcie (e-mail, práca s kalendárom, riadenie vzťahov so zákazníkmi CRM, atď.);
- používanie klaudových databáz ako súčasť spracovania aplikácie. To by mohlo byť veľmi užitočné pri spoločnom využívaní databázy s partnermi, vládnymi agentúrami, atď.

### 4.2 Podnik-Klaud-Koncový užívateľ (angl. Enterprise to Cloud to End User)

V tomto scenári podnik používa klaud na dodanie údajov a služieb koncovému používateľovi. Keď koncový užívateľ komunikuje s podnikom, podnik pristupuje na klaud na vyhľadanie údajov a/alebo ich manipuláciu, pričom výsledky zasiela koncovému používateľovi. Koncovým používateľom môže byť niekto z podniku, zákazník alebo niekto z verejnosti.

### 4.3 Podnikový komunitný klaud (angl. Enterprise Community Cloud)

Tento prípad použitia potenciálne zahŕňa verejné aj neverejné klaudy, v ktorých sa infraštruktúra používa spoločne medzi podnikmi majúci spoločný cieľ (napr. integrovaný dodávateľský reťazec). Komunitný klaud môže prevádzkovať jedna z organizácií v komunite alebo klaudový poskytovateľ tretej strany.

Komunitný klaud môže poskytovať sprostredkovateľ tretej strany; rozdiel je v tom, že sprostredkovateľ nemá žiadne vlastné klaudové zdroje. Zdroje v tomto prípade môžu pochádzať od členov komunity alebo externých (napr. verejných) klaudových poskytovateľov. V každom variante prípadu použitia komunitného klaudu sa predpokladá, že správa klaudových zdrojov sa vykonáva v mene zákazníkov a na základe ich podmienok.

Príklad: komunitný klaud má infraštruktúru spoločne využívanú podnikmi so spoločným cieľom.



## 5 Funkčné odporúčania pre klaudové scenáre

Toto ustanovenie poskytuje neúplný zoznam funkčných odporúčaní na základe všeobecných záverov z posudzovania prípadov použitia na vysokej úrovni, ktoré sa už opisovali vyššie. Tieto identifikujú prioritné otázky, pre ktoré by klaudoví poskytovatelia, podniky a koncoví používatelia mali nájsť riešenie, aby znížili prekážky pri osvojovaní klaudových služieb.

Funkčné odporúčania sa neskôr mapujú na tri predošlé scenáre prípadov použitia klaudových služieb na vysokej úrovni.

### 5.1 Identita a overovanie autenticity

Ak koncový používateľ pristupuje ku klaudovej službe, môže sa vyžadovať jeho identifikácia a overenie autenticity.

Podniky zvyčajne majú vlastné politiky na správu identity a riadenie prístupu. Klaudové služby budú musieť s nimi koexistovať v každom z uvažovaných scenárov použitia. Klaudový poskytovateľ by mal stanoviť spôsob spravovania identity a overovania autenticity a v ideálnom prípade ponúkať určitú pružnosť s cieľom zlepšiť súlad s podnikovými systémami. Osobitne treba zvážiť: spôsob spracovania hesiel (šifrovanie, správa kľúčov), obmedzenia na formát hesla (minimálna dĺžka, povolená kombinácia znakov), vyhodnocovanie sily hesla pri písaní, dátumy expirácie hesiel (vynucovanie zmeny), nastavenie začiatkových hesiel a požiadavky na zmeny.

**Federatívna identita:** Okrem základnej identity potrebnej pre od koncového používateľa bude mať používateľ podniku pravdepodobne podnikovú identitu. Ideálne je, ak podnik spravuje jediné ID pomocou infraštruktúry, ktorá zjednocuje iné identity, ktoré by mohli klaudové služby požadovať.

Pre poskytovateľa klaudovej služby je preto žiaduce, aby ponúkol delegovanie overovania autenticity interným systémom riadenia prístupu podniku a pri overovaní autenticity údajov overoval "klientské certifikáty".

Identitu a overovanie identity môže vykonávať podnik pôsobiaci ako poskytovateľ identity v scenári federatívnej identity alebo nezávislá tretia strana a môže viesť k prideleniu pseudonymu používateľovi, aby sa zamaskovala skutočná identita používateľa od poskytovateľa klaudových služieb.

Pre internetové transakcie sú nevyhnutné bezpečné metódy elektronického overovania autenticity. Významným prínosom pre prijatie klaudu by mohli byť spoločné štandardy, ktoré umožňujú bezpečné, ale bezproblémové používanie služieb.

### 5.2 Riadenie prístupu

Prístup podnikového používateľa k údajom a službám hosťovanými klaudovým poskytovateľom by mal zdediť riadenie prístupu k údajom podniku. Predovšetkým, klaudové služby by najmä nemali dovoliť, aby sa privilégiá zvýšili a boli vyššie, ako sú tie, ktoré sa používateľovi povolia, keď sa priamo pripojí k službám podniku.

**Bezpečný prístup klienta:** Okrem základného prístupu koncového používateľa môžu existovať bezpečnostné dôvody a dôvody na dodržanie zhody vyžadujúce overenie bezpečnostného stavu klienta (prostredníctvom riadenia prístupu na sieť NAC) na prístup spoza bezpečnostnej zóny podniku.

### 5.3 Správa údajov a regulačný súlad

Užívatelia podnikových klaudových služieb očakávajú od poskytovateľov klaudových služieb, že stanovia národné a medzinárodné politiky a predpisy, ktoré majú rešpektovať.

Klaudový poskytovateľ by mal zabezpečiť, aby poskytovaná služba bola v súlade s predpismi na ochranu údajov a správy súkromia. Najmä tam, kde sa dáta prenášajú cez medzinárodné hranice, a to najmä v prípade neanonymných osobných údajov (informácia súvisiaca s identifikáciou osoby), by sa mali rešpektovať národné, regionálne a medzinárodné predpisy na ochranu údajov a súkromia.

Regulačné prostredie v jednotlivých krajinách a regiónoch nie je konzistentné. Dokonca aj v rámci Európskej únie (EÚ) existujú rozdiely v národných aplikáciách smerníc EÚ. Podnikoví zákazníci chcú mať jasnosť ohľadom bezpečnosti, súkromia a aplikovateľnej jurisdikcie. Odporúča sa, aby klaudoví poskytovatelia poskytovali priame informácie o spôsobe a mieste spracúvania údajov, aby sa potenciálni zákazníci mohli kvalifikovane rozhodnúť.

Navyše klaudový používateľ a poskytovateľ klaudovej služby by mali zabezpečiť súlad s národnými, regionálnymi a medzinárodnými požiadavkami na prístup k informáciám zo strany orgánov uplatňujúcich právo na podporu národných, regionálnych a medzinárodných právnych sporov.

V závislosti od druhu údajov, ktoré podnik spravuje v záujme koncového používateľa, môžu existovať právne alebo iné obmedzenia týkajúce sa umiestnenia fyzického servera, na ktorom sú uložené údaje. Na PII sa zameriava mnoho aktuálnych zákonov. Podniky by privítali podobnú ochranu rozšírenú na súkromie a bezpečnosť podnikových údajov a odporúča sa, aby klaudoví poskytovatelia spracúvali takéto údaje citlivo a podľa jasne deklarovanej politiky. To sa vzťahuje aj na akúkoľvek službu subdodávateľov. Pri prihlasovaní sa do klaudovej služby by zákazník mal mať možnosť vybrať si krajinu (krajinu), v ktorých je poskytovateľ oprávnený umiestniť, šíriť a/alebo spravovať údaje používateľa klaudovej služby.

Bez predchádzajúceho súhlasu používateľa klaudových služieb nemali by byť žiadne presuny údajov do iného regiónu či krajiny a ani cez ne prechádzať.

Od poskytovateľov klaudových služieb sa očakáva, že poskytnú zoznam krajín, v ktorých sa nachádzajú ich dátové centrá a mapu toku údajov cez krajiny, vrátane krajín, z ktorých môže k údajom pristupovať poskytovateľ (alebo akákoľvek vláda a v akom prípade).

Poskytovatelia by sa mali riadiť podľa miestnych (napr. finančných) aktuálnych predpisov tým, že vhodne prispôsobia svoju klaudovú SaaS.

## 5.4 Meranie a monitorovanie

Všetky klaudové služby treba merať a monitorovať. Týka sa to klaudovej infraštruktúry a prístupu na sieť, ale aj nasadených služieb a aplikácií. Vyžaduje sa to napríklad pri dohľade dohodnutej úrovne kvality služby (QoS) podľa SLA a spustení nápravných opatrení v prípade potreby, ale aj pri riadení nákladov, refundáciách a poskytovaní.

## 5.5 Prístup na sieť

*“Očakávaná konvergencia výpočtovej techniky, dátových úložísk a sietí k jedinej integrovanej infraštruktúre sa stáva realitou. Stráca sa rozdiel medzi sieťovými službami a aplikáciami, ktoré podporujú. Z pohľadu používateľa je podstatná skúsenosť s aplikáciou a tá závisí od všetkých podporných systémov, ktoré fungujú efektívne. Táto užšia integrácia IT a sieťových zdrojov má osobitný význam pre interaktívne aplikácie a aplikácie v reálnom čase (napr. v oblasti telekomunikácií), ktoré majú konkrétne požiadavky na výkon siete. Nasadenie týchto aplikácií do klaudu bude možné, ak sa IT a sieťové zdroje integrujú do jednotnej infraštruktúry” [i.4].*

Navyše, ak sú niektoré údaje alebo služba v klaude, prístup k nim má byť všadeprítomný a v ľubovoľnom čase prostredníctvom vysokorýchlostných sietí, ktoré sú vhodné pre klaudové

aplikácie. Preto poskytovatelia siete a príslušná regulácia sa potrebujú prispôbiť, aby nebránili vývoju trhov závislých od klaudu.

Na vylúčenie akéhokoľvek oneskorenia verejného internetu môže byť potrebné merať metriky, ako sú dostupnosť a výkon (napr. čas reakcie), na vstupnom bode poskytovateľa klaudovej služby. Od SLA sa vo všeobecnosti očakáva, že určí explicitnú metodiku merania pre každú metriku (kvantifikovanú pojmami). Takto sa stanovujú hranice očakávaní, ktoré má zákazník od služby. V prípade, že pre podnik nie je prijateľná nestálosť verejného prístupu k internetu, odporúča sa, aby existovala možnosť použiť medzi zákazníkom a poskytovateľom klaudovej služby neverejnú okruhu alebo spravované virtuálne neverejné siete (VPN).

Pre služby v klaude intenzívne využívajúce médiá a realizované v reálnom čase má kľúčovú úlohu sieť.

*“Tieto aplikácie zahŕňajú niekoľko klaudových zdrojov v prevádzke koniec-koniec, s dôsledkami na výpočtovú techniku, úložný priestor a výkon siete. Spotrebitelia médií, ktoré sú prepojené sieťou, sú geograficky rozdelené a vyžadujú kódovanie a doručenie, ktoré sú vhodné pre ich koncové zariadenie. Prekódovanie z pôvodného základného formátu, aby sa vyhovel požiadavkám rôznych používateľov, je výpočtovo náročné. Rovnako je to aj s dynamickým generovaním spoločne využívaných virtuálnych prostredí. Mnohí spotrebitelia môžu znovu použiť výsledky, ak sa využije ukládanie do vyrovnávacej pamäte alebo logistické prepojenie sietí, a to za cenu prídavného úložného priestoru. Optimalizovaná tvorba médií, úprava, archivácia, distribúcia a dodanie založené na používaní klaudovej infraštruktúry by mohli byť atraktívnou ponukou platformy ako služby (Paas), s cieľom s štandardizovať rozhrania spoločných prvkov [i.4].*

## 5.6 Riadenie a správa

V súčasnosti klaudoví poskytovatelia umožňujú veľmi ľahko vytvoriť účet a začať používať klaudové služby; takéto ľahké používanie vytvára riziko, že jednotlivci v podniku z vlastnej iniciatívy môžu používať klaudové služby so svojimi podnikovými prihlasovacími údajmi. Podniky chcú mať možnosť presadzovať *vlastnú kontrolnú politiku a možnosť požadovať od poskytovateľov klaudových služieb informácie o používaní koncovými používateľmi, pričom sa používanie vzťahuje na podnikový účet.*

*Aktivácia alebo zmena prípadu služby môže požadovať od podniku, aby potvrdil požadovanú službu. Súvisí to s otázkami manažovania identity, spomenuté vyššie. Podnik by mal mať možnosť stanoviť kvóty a byť upozornený v prípade, ak sa služby používajú nad povolené limity.*

## 5.7 Bezpečnosť

Prípady použitia u zákazníka podnikovej klaudovej služby si vyžadujú prísnejšie bezpečnostné požiadavky, ako by očakával bežný koncový používateľ.

Zákazníci podnikových klaudových služieb očakávajú, že poskytovatelia klaudovej služby im ponúknu pre každú službu rôzne úrovne bezpečnosti, z ktorých si budú môcť vybrať.

Poskytovateľ klaudovej služby by mal opísať úrovne zabezpečenia údajov, dôvernosti, integrity, dostupnosti, vrátane zálohovania údajov a prostriedky, ktoré poskytovateľ klaudovej služby používa na splnenie týchto úrovní zabezpečenia údajov (napr. uvedením zoznamu certifikátov). Zaujímavé sú príslušné prevádzkové podrobnosti vrátane akejkoľvek ochrany proti vírusom a škodlivému softvéru, ako aj detekcia a prevencia prieniku do siete.

Od poskytovateľa klaudovej služby sa očakáva, že bude podnikového používateľa okamžite informovať o každom narušení údajov (napr. aby umožnil dodržiavanie všetkých lokálnych oznamovacích povinností o narušení údajov). Podmienky služby by mali uvádzať aj zodpovednosť za oznamovanie narušení. Podniky môžu požadovať možnosť, aby

poskytovateľ klaudivej služby nezverejňoval hlásenia týkajúce sa obsahu každého narušenia. Klaudiví poskytovatelia by mali proaktívne presmerovať aj údaje o akejkoľvek činnosti týkajúcej sa (možných) pokusov narušiť údaje a inej podozrivej činnosti, ktorá môže mať význam pre bezpečnosť dát.

Zákazníci podnikovej klaudivej služby potrebujú bezpečnostné osvedčenie zaručujúce minimálne prevádzkové štandardy, a to bez ohľadu na umiestnenie. Na tomto štandarde by mohli pracovať nezávislé certifikačné a auditorske organizácie. Klaudiví poskytovatelia by mali pre certifikovanú a dôveryhodnú auditorskú organizáciu z tretej strany poskytnúť prostriedky na vykonávanie auditov klaudivých služieb, a to pravidelne alebo na žiadosť zákazníkov. Postupy pre audit by sa mali definovať ako súčasť podmienok služby.

Údaje vo všetkých prípadoch patria používateľovi klaudivej služby. Poskytovateľovi klaudivej služby by sa malo zabrániť, aby k údajom pristupoval s akýmkoľvek iným cieľom, ako mu explicitne povolila organizácia používateľa.

Záznamy o činnosti používateľov (monitorovanie toho, kto a čo kedy urobil vrátane fyzického prístupu, t. j. administrátorov) sú údaje používateľa, ktoré majú byť kedykoľvek prístupné administrátorovi zákazníka.

Poskytovateľ by mal šifrovať údaje vrátane komunikácií, najmä ak sa využíva internet. Zmluva by mala stanovovať dohodnutý šifrovací algoritmus a dĺžku kľúča pre spracúvané údaje a uložené na médiu.

Navyše vyššia/väčšia sila šifrovania údajov v celej EÚ by zvýšila dôveru podniku v klaudivé služby. Konkrétnym problémom je, že niektoré krajiny stanovujú maximálne dĺžky kľúčov na šifrovanie, pričom jednotlivé krajiny majú rôzne obmedzenia. To núti poskytovateľov, aby aplikovali najnižšiu silu, aká je povolená na šírenie cezhraničných údajov, čo oslabuje bezpečnosť. Je preto žiaduce, aby členské štáty EÚ prispôbili svoje predpisy týkajúce sa maximálnej sily šifrovania, prípadne ich nahradili inými povinnosťami organizácie, aby poskytovala prístup orgánom vynucujúcim práva.

## 5.8 Interoperabilita

*Interoperabilita úzko súvisí s prenositeľnosťou. Interoperabilita sa tu interpretuje ako schopnosť združiť viacero klaudiv na podporu jedinej aplikácie. Inými slovami, interoperabilita zahŕňa softvér a údaje, ktoré sú vo viacerých klaudivých infraštruktúrach aktívne súčasne, a vzájomne spolupracujú aby plnili spoločný cieľ.*

V súvislosti s klaudivou interoperabilitou sa vo všeobecnosti začína presadzovať pojem "Intercloud". Ide o analógiu internetu a zakladá sa na podobnej predstave spájanie jednotlivých, v podstate nekoordinovaných klaudivých infraštruktúr a odovzdanie riadenia používateľom. Jedným z poučení z internetu je, že používanie spoločných protokolov (alebo rozhraní) ľahko prístupných pre vývojárov má veľké výhody pri stimulácii inovácií.

Poskytovateľ klaudivej služby alebo zákazník podnikovej klaudivej služby môže mať koordinačnú rolu, pričom využíva služby niekoľkých poskytovateľov z tretej strany, aby koncovému používateľovi zaručil celkový výkon. Jedným z príkladov môže byť počítačový klaudivý poskytovateľ, ktorý na poskytovanie využíva poskytovateľa siete. Tento scenár vyžaduje štandardy na spoločné využívanie informácií o správe, ako sú ciele SLA, medzi poskytovateľmi služieb bez toho, aby sa odhalilo príliš veľa dôverných podrobností o tom, ako sa ciele dosahujú.

Aj tieto umožňujú navrhnúť niekoľko tém na diskusiu o klaudivej interoperabilite:

- aplikácia/služba: štandardy interoperability by mali podporovať distribuované aplikácie s predvídateľným správaním sa a predvídateľným výkonom; napríklad komponenty jednotlivej aplikácie by sa mohli zavádzať vo viacerých klaudivých infraštruktúrach

poskytovateľov a prípadne priebežne prekonfigurovať počas jej činnosti, alebo s obmedzeným prerušením, aby reagovali na zmeny v schémach používania či na zmeny v dostupnosti zdrojov; konfigurácia aplikácie by mala byť odolná vzhľadom na zmeny v konfigurácii v rámci každého klaudu – napríklad úprava, alebo migrácia výpočtových zdrojov;

- **správa:** poskytovatelia klaudovej služby by mali poskytovať štandardizované rozhrania, aby sa jednotlivá aplikácia dala spravovať konzistentným spôsobom koniec-koniec, v podstate nezávisle od detailov jej zavedenia v rôznych klaudových infraštruktúrach; aplikácia pre správu bude môcť riadiť a koordinovať komponenty vo viacerých klaudoch; je potrebná štandardizovaná funkcia správy na zavádzanie a migráciu virtuálnych strojových obrazov medzi rôznymi klaudovými infraštruktúrami. Interoperabilita správy vyžaduje interakciu medzi viacerými nezávislými aktérmi zodpovednými za správu aplikácie a správu infraštruktúry;

- **údaje:** na podporu zavádzania ekvivalentných obrazov virtuálnych strojov a údajov aplikácií do rôznych klaudových infraštruktúr sú potrebné štandardy; základnou požiadavkou na klaudovú interoperabilitu je pripojiteľnosť takej siete medzi klaudovými prostrediami, ktorá je vhodná na prenos prevádzky aplikácie; štandardným spôsobom treba riešiť bezpečnosť a iné otázky týkajúce sa správy údajov vo viacerých doménach;

- **sieťové aspekty:** pre klaudové služby je základom sieťový prístup k výpočtovým zdrojom; sú potrebné štandardy, aby sa podporil jednotný prístup k jednotlivým klaudovým výpočtovým zdrojom a zreťazenie alebo združenie klaudov v rôznych lokalitách; prepojenie medzi klaudmi by malo podporovať požiadavky aplikácií kladené na kvalitu; pripojenie na sieť sa vo všeobecnosti zakladá na používaní spoločných fyzických zdrojov podobne ako vo výpočtovej technike a úložnom priestore; budú potrebné štandardy na rezervovanie a riadenie prístupu [i.4].

## 5.9 Prenositeľnosť a zavádzanie

Klaudová technológia so silnými hnacími silami v priemysle a po úspešnom vstupe na trh má silnú tendenciu vnucovať de facto štandardy (uzamknutie dodávateľom).

Aspekt "Nebyť uzamknutý" vyvoláva potrebu pre štandardy prenositeľnosti, aby sa zabezpečilo, že podnikoví zákazníci budú mať prístup na otvorený trh klaudových služieb a môžu zmeniť a navzájom prepojiť poskytovateľov, keď vynaložia primerané úsilie. Rozsah otvorených štandardov by mal pokrývať formáty údajov, prístupové protokoly a programovacie rozhrania.

*"Prenositeľnosť sa všeobecne týka schopnosti migrovať aplikácie medzi rôznymi klaudmi. To je potrebné, aby sa zákazníci klaudových služieb mohli vyhnúť situácii, že sú viazaní na konkrétneho poskytovateľa klaudovej infraštruktúry potom, ako sa rozhodli aplikáciu prevádzkovať v klaude. Toto prispieva k vnímaným rizikám spojeným s prechodom na klaudovú technológiu. Potenciálny zákazník potrebuje vysoký stupeň dôvery v technické a obchodné schopnosti vybraného poskytovateľa na podporu kritických podnikových aplikácií v dlhodobom horizonte.*

Súčasní poskytovatelia klaudovej infraštruktúry ponúkajú vývojárom aplikácií vlastné rozhrania. Potrebné sú štandardizované rozhrania na správu klaudových infraštruktúr a rôznych druhov zdrojov, ktoré poskytujú. Zníženie nesúladu medzi rôznymi systémami klaudových infraštruktúr by umožnilo nielen konkurenčný trh, ale aj nové obchodné modely, v ktorých sa môže obchodovať s rôznymi klaudovými infraštruktúrami podľa ceny a dopytu.

V extrémnom prípade schopnosť automaticky migrovať kompletnú bežiacu aplikáciu (vrátane akýchkoľvek nevyhnutných prvkov pre správu a monitorovanie) z jednej klaudovej

*infraštruktúry do inej by pre zákazníkov bola nesporne atraktívna (ale oveľa menej pre poskytovateľov klaudovej infraštruktúry, najmä na súčasnom trhu).*

*Prenositeľnosť obrazov virtuálnych strojov rieši DMTF Open Virtualisation Format (OVF). Mala by poskytnúť dobrý základ pre limitovanú prenositeľnosť, ale jej podpora pre komplexnú konfiguráciu a interakcie s akýmikoľvek podpornými systémami je v súčasnosti obmedzená. Tieto otázky sú prirodzene v kompetencii poskytovateľa služby.*

*Prenositeľnosť údajov je dôležitá pre typickú obchodnú aplikáciu. Možnosť zákazníka vyhľadať údaje aplikácie v klaudovej infraštruktúre jedného poskytovateľa a importovať ich do ekvivalentnej aplikácie hostovanej alternatívnym poskytovateľom znižuje riziko vzniku dlhodobej závislosti. To by pravdepodobne vyžadovalo nezanedbateľné úsilie na strane zákazníka (alebo poskytovateľa aplikačnej služby - podrobnosti budú do značnej miery závislé od konkrétnej aplikácie a nebude ich riešiť poskytovateľ klaudovej infraštruktúry). Dosiahnutie prenositeľnosti údajov závisí od účinnej štandardizácie funkcionality importu a exportu údajov medzi poskytovateľmi klaudovej infraštruktúry“ [i.4].*

Licencovanie softvéru bolo vždy zložité. V prípade klaudu je to ešte zložitejšie. Odporúča sa preskúmať spôsob licencovania navrhovaný pre klaudové prostredie. Na zabezpečenie výhodnosti nákladov sa musia starostlivo definovať aspekty prenositeľnosti a opätovného využitia existujúcich licencií vo fáze zavádzania a prenositeľnosti. Osobitnými otázkami sú: kredit na existujúce licencie a trvalé používanie licencie.

## 5.10 Reverzibilita

Veľké podniky už používajú klaudové riešenia na podporu svojich údajov a informačných systémov. Ak už máte má svojho poskytovateľa klaudového riešenia, je nesmierne ťažké zmeniť poskytovateľa, čo predstavuje ozajstný problém. Každý poskytovateľ klaudových riešení používa vlastný súbor rozhraní a formátov údajov. Otvorenie tohto trhu vyžaduje štandardizáciu na úrovni architektúry, stavebných blokov a systémovej úrovne. Z tohto dôvodu je štandardizácia potrebná.

Používatelia podnikovej klaudovej služby by mali dokázať vyhľadať všetky alebo časť svojich údajov na požiadanie a nezávisle (t. j. bez toho, aby poskytovateľ klaudovej služby musel vykonávať špeciálne postupy). Mali by dokázať vyberať údaje a filtrovať osobitné položky, o ktoré majú záujem.

Ak používateľ nemôže údaje vyhľadať samostatne, poskytovateľ by mal byť aspoň zmluvne zaviazaný, aby vrátil údaje v stanovenom časovom období cez internet alebo na fyzické úložné miesto, s výraznými sankciami (uvedenými v SLA).

Rozsah reverzibility presahuje rámec jednoduchých uložených súborov a databázových záznamov, pretože sa týka komplexných údajov, ako je logika obchodných postupov tvoriaca súčasť kódu aplikácie, transakčné, hlavné údaje, agregované údaje, webové denníky (angl. blogs), denníky (angl. logs), definície správ (angl. report definitions), parametrizačné a konfiguračné tabuľky, a tak ďalej.

Štandardne, formát získaných údajov by mal mať rovnaký formát, v ktorom sa poskytli. Ak sa údaje vytvorili v klaude, formát by mal byť štandardný a znovu použiteľný, pričom by sa nemali stratiť žiadne informácie.

Používatelia podnikových klaudových služieb očakávajú, že sa limituje čas vyhľadávania.

Používateľ klaudovej služby očakáva zaručenú minimálnu dobu (t. j. X mesiacov uvedených v SLA) na uchovávanie a dostupnosť údajov po skončení služby poskytovateľom klaudovej služby, skôr ako sa všetky informácie odstránia zo systémov klaudového poskytovateľa natrvalo.

Treba dohodnúť politiku likvidácie údajov (napr. odstrániť údaje na všetkých fyzických zariadeniach, vrátane zálohovacích pásov a akejkolvek inej viacnásobnej off-line duplikácie pre vzdialené kopírovanie).

Ak sa skončí zmluva medzi používateľom a jeho poskytovateľom a vyhľadajú sa úplne všetky údaje používateľa, potom poskytovateľ potvrdí a zabezpečí vymazanie všetkých údajov zo svojich systémov.

Podniky majú obavy z opatrení, ktoré súvisia s bankrotom alebo inými významnými zmenami v podnikaní poskytovateľa kladovej služby. Najmä sa odporúča, aby sa používateľovi kladovej služby zaručil včasný návrat jeho údajov. Malo by byť jasné, že údaje zostávajú majetkom zákazníka. Mechanizmy a postupy na vyhľadávanie údajov by sa mali zaviesť a opísať v zmluvných podmienkach spojených so službou. V týchto otázkach sú vítané regulačné a/alebo priemyselné riešenia.

### 5.11 SLA a referenčné úrovne

*“Zmluva o úrovni služby sa v tejto súvislosti považuje za jednoznačné vyhlásenie o očakávaníach a povinnostiach používateľov a aj poskytovateľov kladových služieb.*

*SLA je zmluva medzi poskytovateľom a zákazníkom služby, ktorá stanovuje funkciu vykonávanú službou, dohodnuté hranice výkonu, povinnosti oboch zmluvných strán a riešenie akýchkoľvek odchýlok. SLA existuje v obchodnom kontexte, a preto bude zahŕňať všetky aspekty interakcie medzi poskytovateľom a zákazníkom, ktoré sú pre službu podstatné“ [i.4].*

Podniky, ktoré podpíšu zmluvu založenú na SLA, budú potrebovať štandardný spôsob na vykonanie referenčného porovnania.

Užívatelia podnikovej kladovej služby očakávajú od poskytovateľa kladovej služby jasné ponuky / jasnú SLA. Ponuky rôznych poskytovateľov kladovej služby by mali používať rovnakú terminológiu, aby sa dali porovnať. Úroveň služby by mala byť garantovaná poskytovateľmi kladových služieb a mala by byť merateľná používateľmi kladových služieb.

Ponuky/SLA poskytovateľov kladovej služby by mali minimálne riešiť:

- informácie o dostupnosti služby pre koncového používateľa vrátane zaručenej dostupnosti, aktivačný čas a akékoľvek prerušenie služby z dôvodu údržby služby;
- informácie o výkone vrátane zaručeného času reakcie;
- informácie pre používateľa kladovej služby a audítorské orgány o dostupnosti štatistiky hodnotiacej kvalitu dodávanej služby. Užívatelia podnikovej kladovej služby očakávajú, že tieto štatistiky budú pre nich a audítorské orgány prístupné nepretržite;
- postup v prípade výskytu incidentu vrátane akéhokoľvek prerušenia prevádzky z dôvodu údržby služby.

Zmluvné ustanovenia, podpísané poskytovateľom kladu, sú v súčasnosti dobrým východiskovým bodom pre všetkých importérov údajov v krajine mimo EÚ. Malo by to platiť aj pre subdodávateľov.

Zmluvné ustanovenia by mali zahŕňať aplikovateľnú jurisdikciu.

SLA by mala stanoviť, čo sa má urobiť v prípade porušenia.

Koncových používateľov môže rušiť pravidelná zmena klaudových služieb, takže je vítaná voľiteľná možnosť statickej služby (pravdepodobne lacnejšia) alebo aspoň možnosť si vybrať, kedy sa má uskutočniť upgrade/vývoj.

Používateľ prístupujúci na klaudovú službu očakáva, že táto služba bude prístupná o krátky čas.

Akékoľvek skončenie služby by sa malo oznámiť aspoň x mesiacov vopred.

SLA by mala obsahovať model oceňovania. Príkladom modelu oceňovania je oceňovanie založené na používaní.

Mal byť sa identifikovať každý subdodávateľ.

## 5.12 Správa životného cyklu

Podniky musia byť schopné spravovať životný cyklus aplikácií a dokumentov. Táto potreba zahŕňa používanie verzií aplikácií, ako aj uchovávanie a likvidáciu údajov. Hlavným problémom pre mnoho organizácií je odhalenie (t. j. v právnom slova zmysle, ak existuje požiadavka na sprístupnenie materiálu dostatočného na to, aby bol prípustným dôkazom v súdnom spore). Ak niektoré údaje už nie sú k dispozícii, predstavuje to podstatné právne riziká. Niektoré z týchto materiálov sa môžu ukladať v klaudových službách, a preto je potrebné jasne stanoviť spôsob spravovania životného cyklu informácií. Týka sa to uchovávanía údajov vrátane odolnosti a dostupnosti. Okrem toho v niektorých prípadoch sa podnik bude chcieť ubezpečiť, že v súlade s príslušným predpisom a podnikovou politikou sa údaje zlikvidovali k určitému dátumu.

## 6 Mapovanie funkčných odporúčaní pre klaudové scenáre

Zoznam funkčných odporúčaní sa mapuje na predchádzajúce tri scenáre prípadov použitia klaudových služieb na vysokej úrovni. Tabuľka 1 ukazuje dôležitosť požiadaviek pre scenáre.

**Tabuľka č. 1 – Mapovanie funkčných odporúčaní pre scenáre**

	Podnik- Klaud- Podnik	Podnik- Klaud- Koncový užívateľ	Podnikový komunitný klaud
1. Identita a overenie autenticity		✓	✓
2. Riadenie prístupu		✓	✓
3. Regulačný súlad	✓	✓	✓
4. Meranie a monitorovanie		✓	✓
5. Prístup na sieť			
6. Riadenie a správa		✓	✓
7. Bezpečnosť	✓	✓	✓
8. Interoperabilita		✓	✓
9. Zavádzanie a prenositeľnosť	✓	✓	✓
10. Reverzibilita		✓	✓
11. SLA a referenčné úrovne		✓	✓
12. Správa životného cyklu	✓		✓



---

**História**

<b>História dokumentu</b>		
V1.1.1	November 2012	Zverejnenie