Microsoft

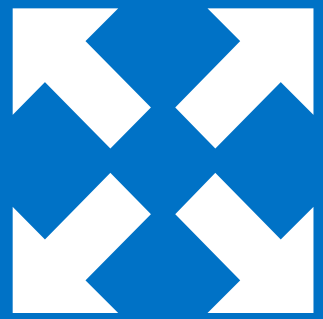
Cloud a povinné osoby ze ZKB

Zdeněk Jiříček, Microsoft s.r.o.
Aleš Špidla, PwC Czech s.r.o.

Přínosy cloudových služeb

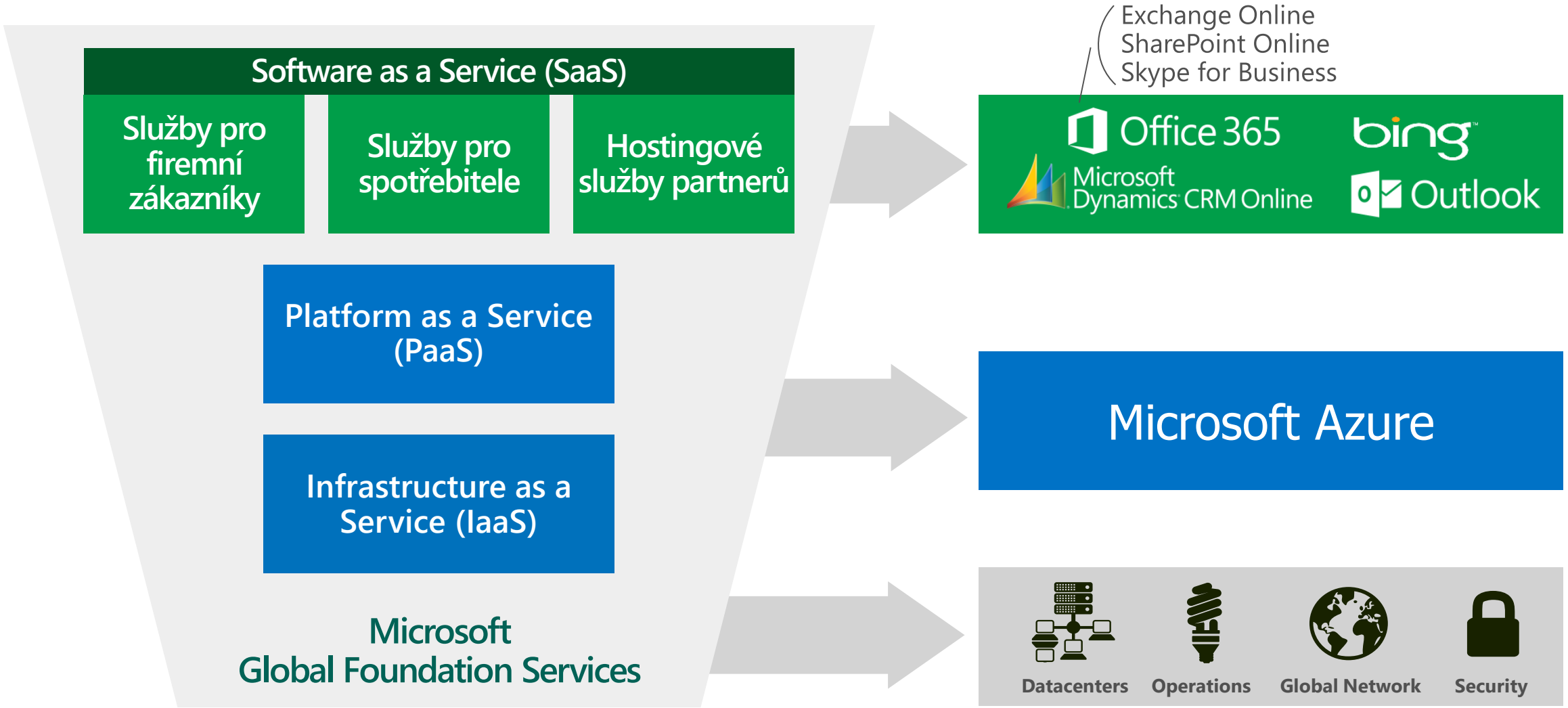
Rychlost nasazení

Škálovatelnost



Cenová výhodnost

Stavba cloudových služeb Microsoftu



Cloud: Online Services Terms (OST) v. 1/8/15

- Podmínky ochrany osobních údajů a zabezpečení (O365 bez Yammer, Azure Core, CRMOL, Intune)
  - Závazek užití dat pouze pro poskytování služeb
  - Závazek neposkytnutí dat třetím stranám kromě vyjmenovaných situací a procesů
  - Oznámení incidentu
  - Použití dodavatelů
  - Umístění pro uchování dat a jurisdikce smlouvy - EU, zpracování dat – možné WW
  - Ochrana osobních údajů – vrácení / smazání dat, pracovníci, subdodavatelé
  - Vyjmenovaná bezpečnostní opatření (v rozsahu ISO 27001)
  - Závazek pokračovat v certifikacích ISO 27001 a auditech SOC 1 & 2
- Příloha 3: Standardní smluvní doložky přesně dle Rozhodnutí Komise 2010/87/EU
  - Povinnosti vývozce, dovozce dat, odpovědnost, spolupráce s regulátorem, dílčí zpracování, povinnosti po ukončení smlouvy

Viz nové Online Services Terms se Stand. smluv. doložkami EU

Soulad s regulatorními požadavky

Horizontální:

Zákon o ochraně osobních údajů č. 101/2000 Sb.

Zákon o kybernetické bezpečnosti č. 181/2014 Sb.

Vertikální:

Veřejná správa:
Zákon o ISVS č. 365/2000 Sb.

Vyhláška o výkonu činnosti bank atd. č. 163/2014 Sb.

Viz nové Online Services Terms se Stand. smluv. doložkami EU

Co když jsou cloudové služby součástí ISMS

Zák. č. 181/2014 Sb. o kybernetické bezpečnosti – povinné osoby:

- KII – Kritická informační infrastruktura dle Nařízení vlády č. 315/2014 Sb.
  - ❖ Např. určité bankovní služby; hlásná povodňová služba, veřejná správa – připravenost na řešení kriz. situací
- Významné IS veřejné správy – (vyhláška o VIS č. 317/2014 Sb.)
  - ❖ **Oblastní** určující kritéria např. **spisová služba**, **el. pošta**, **internetové stránky**. Dopadová kritéria…?
- **Soulad cestou standardizace – ISO 27001 (vyhl. č. 316/2014 Sb.)**
  - ❖ §29: Povinná osoba může splnit certifikací ISO/IEC 27001, pokud tato pokrývá celý rozsah ISMS
  - ❖ §4: Vzít v úvahu min. výčet hrozeb a zranitelností
  - ❖ §7: Požadavky na dodavatele
  - ❖ Metodika řízení rizik minimálně na úrovni vzorové metodiky v Příloze č. 2 (dle ISO 27005)
  - ❖ Zajistit si podklady k dokumentaci dle Přílohy č. 4

Soulad cloudových dodávek dle vyhl. č. 316/2014 Sb.

Dle §7 – Bezpečnostní požadavky pro dodavatele povinných osob

„VIS“ – pouze odst. (1)

Zavedení pravidel pro dodavatele pro potřeby řízení bezpečnosti informací

Dokumentace smlouvou, jejíž součástí je ustanovení o bezpečnosti informací

Microsoft splňuje „Podmínkami pro služby online - OST“:
oddíl „Podmínky ochrany osobních údajů a zabezpečení“ – součást písemné smlouvy

Pozn. OST = Online Services Terms

„KII“ – dále odst (2) b

Smlouva zahrnuje způsoby a úrovně bezp. opatření a vztah odpovědnosti za jejich zavedení a kontrolu

Microsoft: „OST“ obsahuje seznam opatření a závazek cert. ISO 27001

Microsoft dá k dispozici povinné osobě:

1. Svoji „Bezpečnostní politiku“
2. ISO 27001 certifikát (online výpis)
3. ISO 27001 prohlášení o aplikovatelnosti (výčet opatření)
4. ISO 27001 auditní zprávu, a na vyžádání SOC 1 & 2 audit. zprávy

Povinná osoba zapracuje do svojí bezpečnostní politiky

„KII“ – dále odst. (2) a, c

Pravidelné hodnocení rizik služeb (příp. i před uzavřením smlouvy); Kontroly zavedených bezp. opatření

Zhodnocení řízení rizik nezávislým auditorem, podklady dle Přílohy 2):

1. Metodika hodnocení rizik, funkce, definice proměnných a jejich úrovní
2. Min. seznam hrozeb a zranitelností (§4)
3. Pravidelnost hodnocení rizik, způsoby schvalování přijatelných rizik
4. Závazek včasného řešení vyšších úrovní výsledných rizik

Kontrola účinnosti zavedených bezp. opatření auditními zprávami ISO 27001 a SOC 1 & 2 Type 2

Ověření metodik řízení rizik Office 365 a Azure vůči zák. č. 181/2014 Sb. a vyhl. č. 316/2014 Sb.

Report je obecně zaměřen na:

- § 5, odst.2, písm. b zákona - Řízení rizik jako jedno z organizačních opatření
- § 7 vyhlášky- Stanovení bezpečnostních požadavků pro dodavatele
- § 4 vyhlášky - Řízení rizik

Předmětem reportu je zejména:

- Celkový přístup k řízení rizik v cloudu
- Srovnání metodiky Microsoftu se vzorovou metodikou v Příloze č. 2 vyhlášky - hodnocení rizik, funkce, definice proměnných a jejich úrovní
- Minimální seznam hrozeb a zranitelností (§4 odst.4 vyhl.)
- Proces hodnocení rizik - pravidelnost a frekvence , způsoby schvalování přijatelných rizik
- Závazek včasného řešení vyšších úrovní výsledných rizik

Podrobné přezkoumání podkladů a porovnání odpovídajících částí s požadavky zákona a vyhlášky

- Podrobná dokumentace k ISO 27001
- Risk Standard Operating Procedures a další

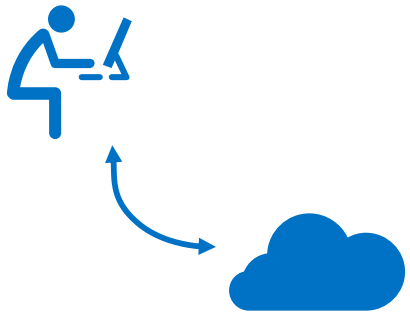
Certifikace MS online služeb – stav 07/2015

Standard - certifikace	Office 365	Dynamics CRM	Microsoft Azure	Windows Intune	Yammer	GFS (Global Foundation Services – infrastruktura datových center)
ISO 27001:2013 (+ ISO 27018)	Ano	Ano	Ano	Ano	Ano	Ano (jen ISO 27001)
Standardní smluvní doložky EU, ověřen „soulad“)	Ano	Ano	Ano	Ano	Ne	Ano
EU Safe Harbor	Ano	Ano	Ano	Ano	Ano	Ano
PCI DSS (Payment Card Industry Data Sec. Standard) Level 1 v3.0	N/A	N/A	Ano	N/A	N/A	Ano
SOC 1 Type 2 (Service Organization Controls - SSAE 16/ISAE 3402)	Ano	Ano	Ano	Ano	Ne	Ano
SOC 2 Type 2 (AT Section 101)	Ano	Ne	Ano	Ano	Ne	Ano
UK G-Cloud v6	Ano	Ano	Ano	Yes	Ne	N/A
FedRAMP (US) (Moderate)	Ano	Ne	Ano	Ne	Ne	Ano
FERPA (US – Education)	Ano	Ano	Ano	N/A	Ano	N/A
HIPAA/BAA (US - Healthcare)	Ano	Ano	Ano	Ano	Ne	Ano
CJIS (US - Criminal Justice)	Ano	Ano	Ano	Ne	Ne	N/A

Ochrana dat v cloudu

Ochrana dat šifrováním

1



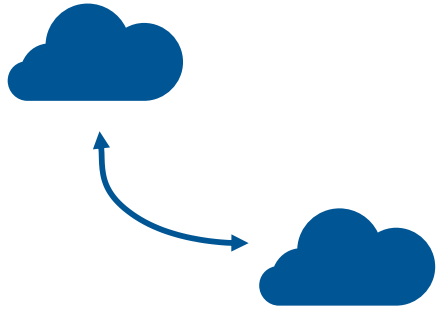
Data v tranzitu uživatel - cloud

Protokol SSL/TLS

Nově: Perfect Forward Secrecy (PFS)

Exchange online podporuje S/MIME, PGP

2



Data v tranzitu mezi datovými centry

Asymetr. šifra 2048 bit

Perfect Forward Secrecy

Exchange Online trunk: TLS by default

3

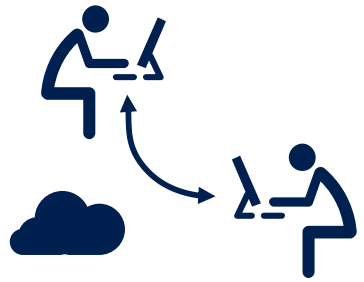
Data v úložišti

Disky: Bitlocker AES 256 likvidace (NIST 800-88)

SP Online, OneDrive Pro: Per-file encryption

Azure Key Vault

4



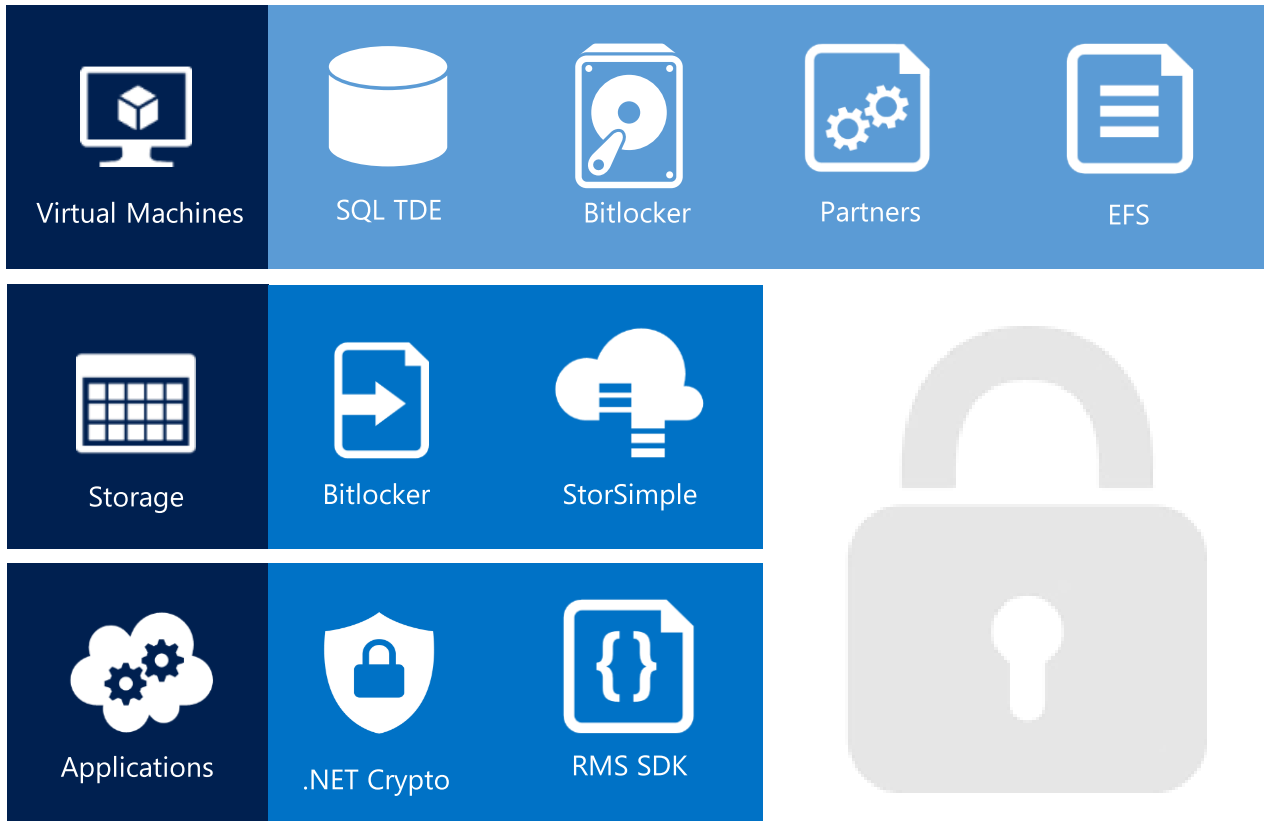
Zabezpečení v rámci organizace

Rights Management Services (RMS)

RMS sharing app / SDK

S/MIME (e-mail)

Azure – možnosti šifrování dat „at rest“



Virtual Machines:

- Data drives – full disk encryption using BitLocker
- Boot drives – BitLocker and partner solutions
- SQL Server – Transparent Data and Column Level Encryption (TDE, CLE)
- Files & folders - EFS in Windows Server

Storage:

- Bitlocker encryption of drives using Azure Import/Export service
- StorSimple with AES-256 encryption

Applications:

- Client Side encryption through .NET Crypto API
- RMS Service and SDK for file encryption by your applications

Azure Key Vault

See http://azure.microsoft.com/en-us/services/key-vault/

Pro zákaznické aplikace

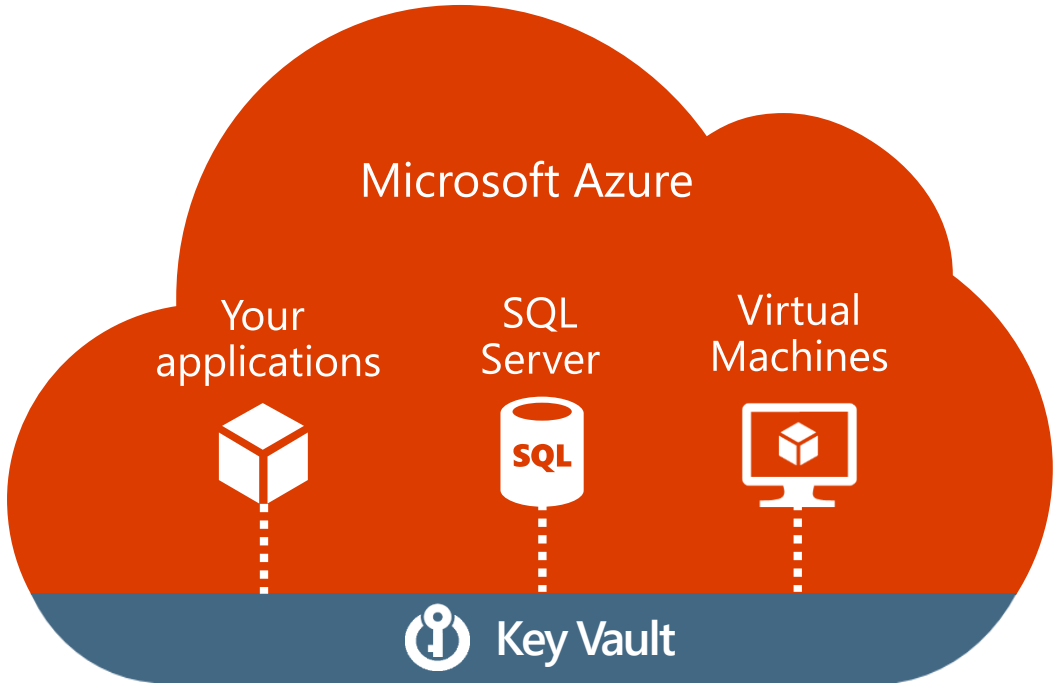
Zabezpečený přístup ke klíčům pro šifrování obsahu a pro el. podpis. Aplikace vyvinuté Azure Storage SDK (poslední verze) mohou šifrovat data automaticky, master key je v Key Vault.

SQL Server

Generování a správa klíčů pro SQL Server TDE, CLE, a Backup
Lze pro Azure Virtual Machines i pro SQL Server on-premises

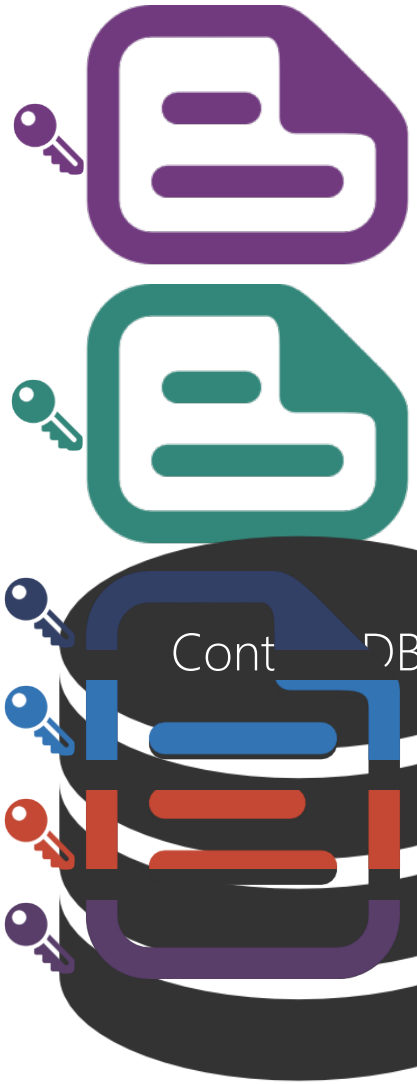
VM's: Azure Disk Encryption

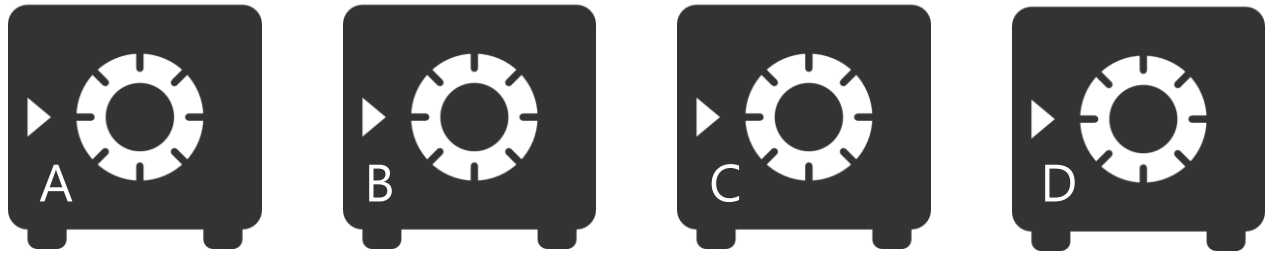
Bitlocker pro Windows Server Virtual Hard Drive (VHD)
Linux DM-Crypt pro Linux VM's
Master key pro CloudLink Secure VM, SafeNet atd.



Office 365 per-file encryption

SharePoint Online;
OneDrive for Biz
(folder level)

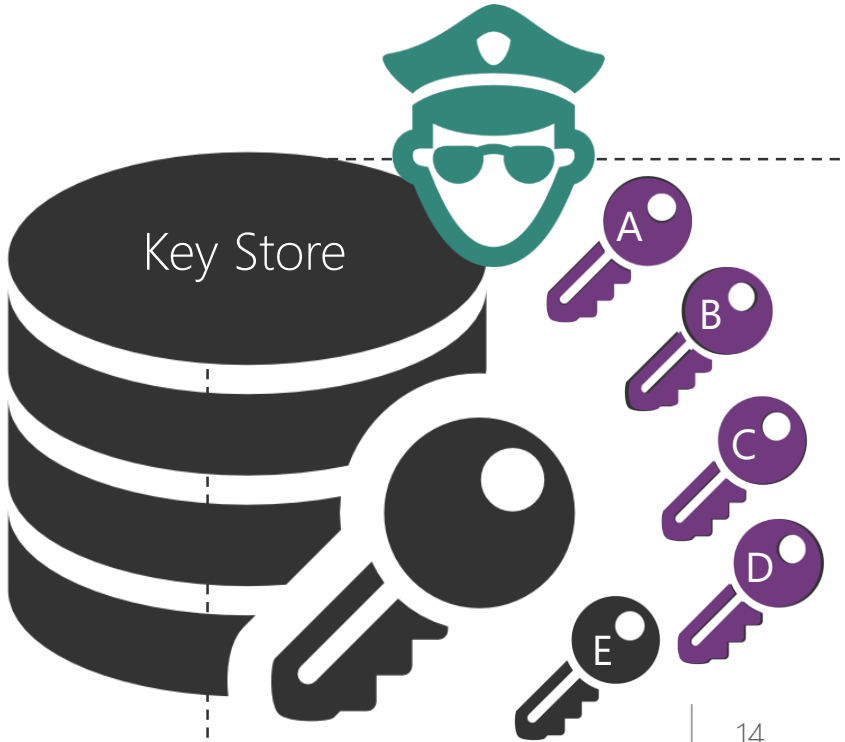




Explanation is here:

[Office 365 Announcement]

[Microsoft Office Blog] (more details)



Shrnutí

- Povinná osoba: vždy provést analýzu rizik a hodnocení informačních aktiv
- Microsoft: bezpečnostní opatření a certifikace jsou součástí smluvních podmínek
- Microsoft: řízení rizik ověřeno PwC (ISAE 3000)
- Využití cloudu dle zajištění informačních aktiv

Děkuji za pozornost!

Microsoft

Zdeněk Jiříček
National Technology Officer
zdenekj@microsoft.com