Šifrovaný přenos komunikace

a

bezpečné uložení informace na mobilních zařízeních

Mgr. Jan Nožka

13. dubna 2015

OKsystem

Obsah

- Kryptografická ochrana v zákonu o kybernetické bezpečnosti (dále jen ZKB)
- Bezpečnostní rizika mobilních zařízení
- Kryptografická ochrana uložení informací
- Řešení šifrované komunikace
- Principy a využití jednosměrné šifrované komunikace

OKsystem

Kryptografická ochrana jako povinnost ze zákona

Vyhláška č. 316/2014, § 25 stanovuje:

Správci KS a IS KII

Správci VIS

- Určí úroveň ochrany dat.
- Stanoví pravidla kryptografické ochrany informací při přenosu nebo při uložení:
  - na mobilní zařízení,
  - vyměnitelná média.
- Použijí kryptografické prostředky:
  - zajištění ochrany důvěrnost a integrity předávaných nebo ukládaných dat.

Kryptografická ochrana jako povinnost ze zákona

Vyhláška č. 316/2014, § 25 stanovuje:

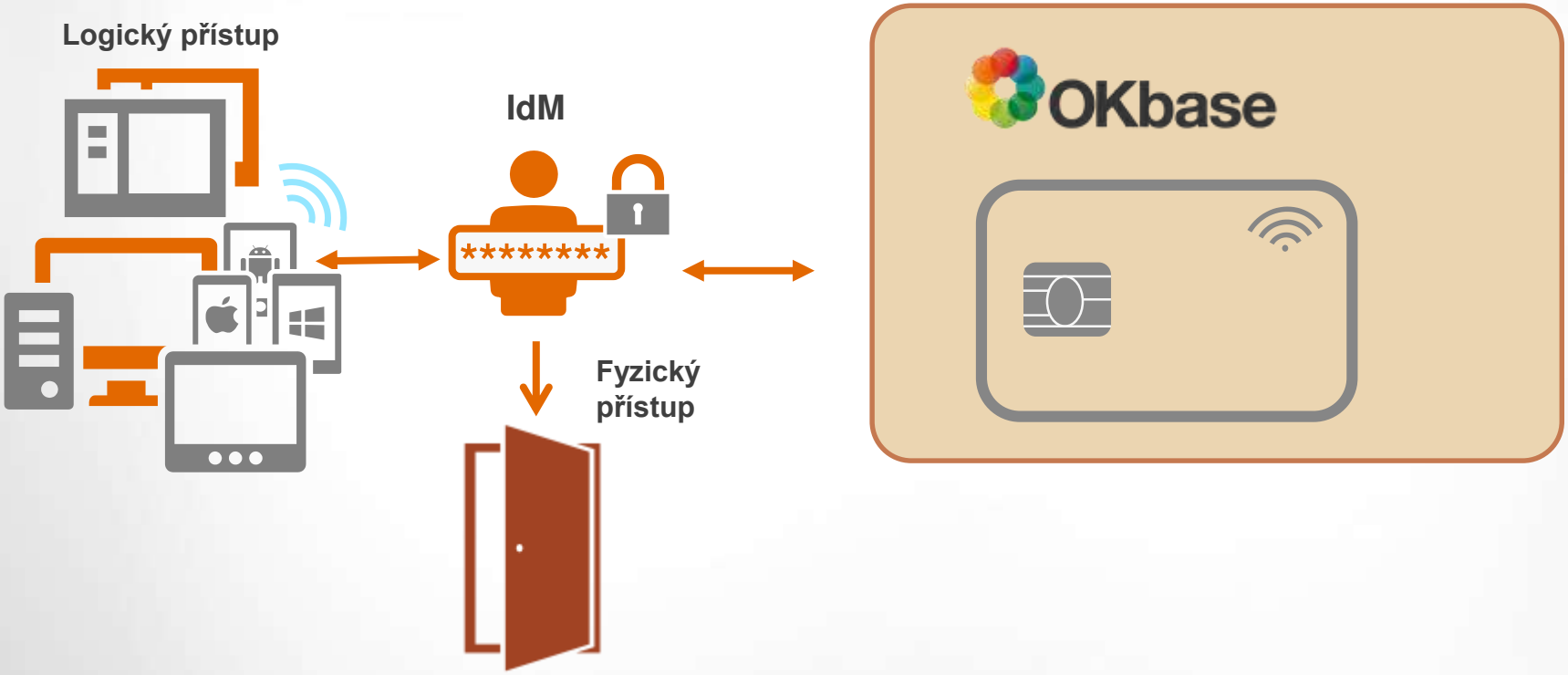
Správci KS a IS KII

Správci VIS

- Zavedou správu klíčů:
  - generování,
  - distribuci,
  - ukládání,
  - archivaci,
  - změny,
  - ničení,
  - kontrolu,
  - audit klíčů.
- Použijí odolné kryptografické algoritmy a kryptografické klíče.

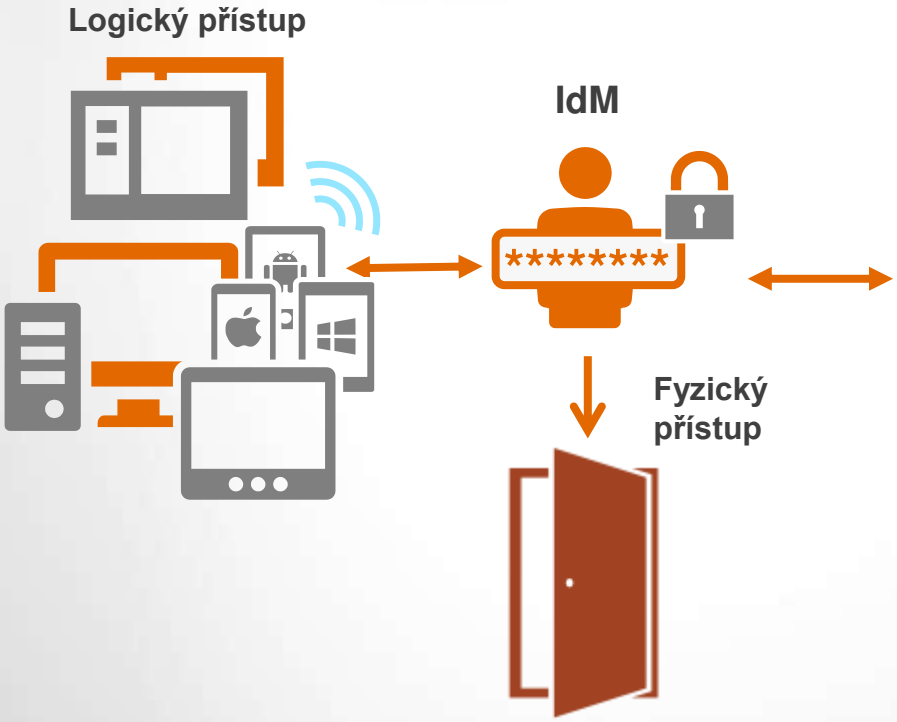
OKsystem

Komplexní správa kryptografických klíčů, certifikátů a čipových karet



OKsystem

Komplexní správa kryptografických klíčů, certifikátů a čipových karet



OKbase

- Systém pro kompletní správu čipových karet
- Evidence vydaných karet a certifikátů
- Průvodce personalizací čipových karet
- Automatizované odvolávání certifikátů
- Obnovení/archivace klíčů

OKsystem

Použití mobilních zařízení přináší rizika

Rizika úniku dat

- více než 50% = lidský faktor
  (uživatelem mobilního zařízení)

Typy ztracených dat

- 2/3 dat jsou pracovní/firemní
  (duševní vlastnictví, finanční, platby, přihlašovací údaje)

Průměrná doba nahlášení ztráty

- v 50% případů po uplynutí 1.- 2. dne od ztráty

Zdroj: Kaspersky LAB
pro rok 2014

OKsystem

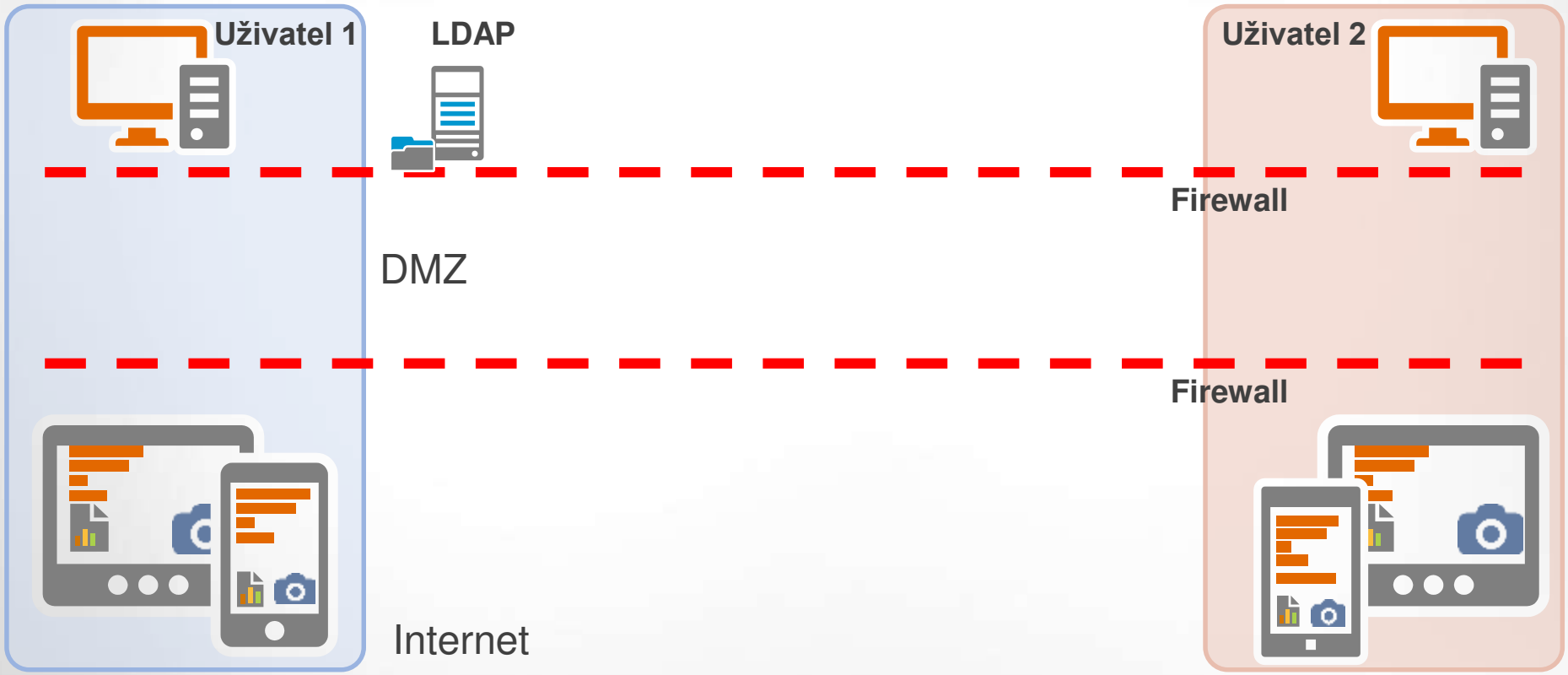
Využití kryptografické ochrany dat

- Při datovém přenosu po internetu

- Při uložení na zařízení
  - mobilní zařízení
  - v rámci DMS

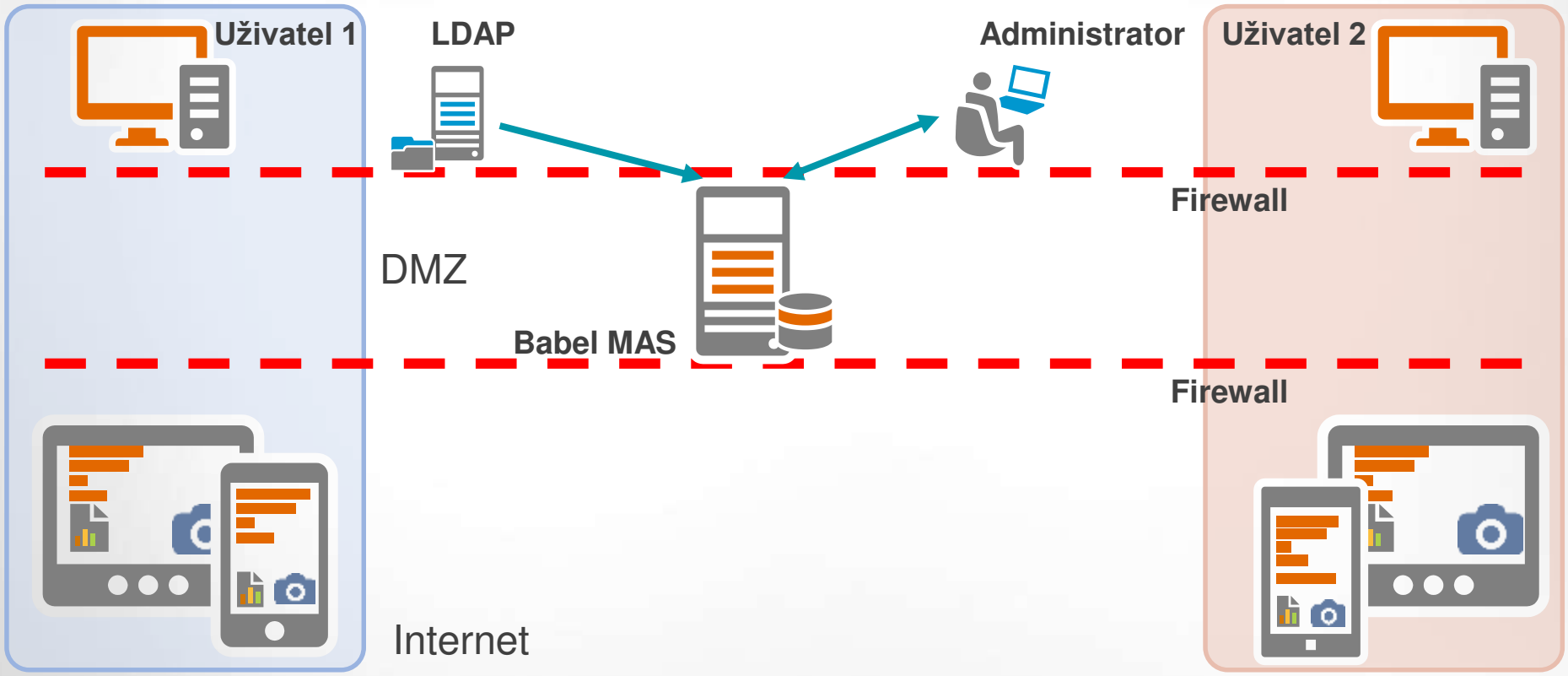
OKsystem

Kryptografická ochrana datového přenosu



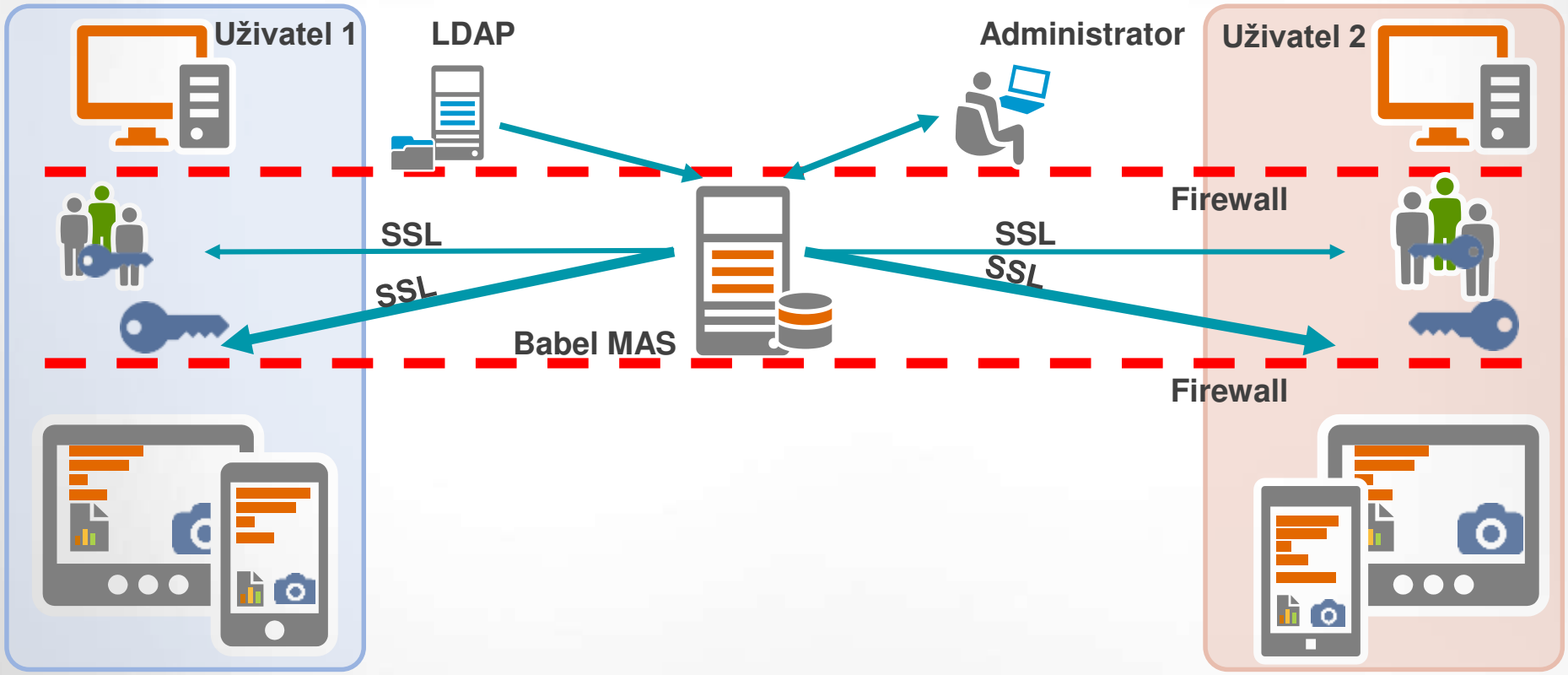
OKsystem

Kryptografická ochrana datového přenosu



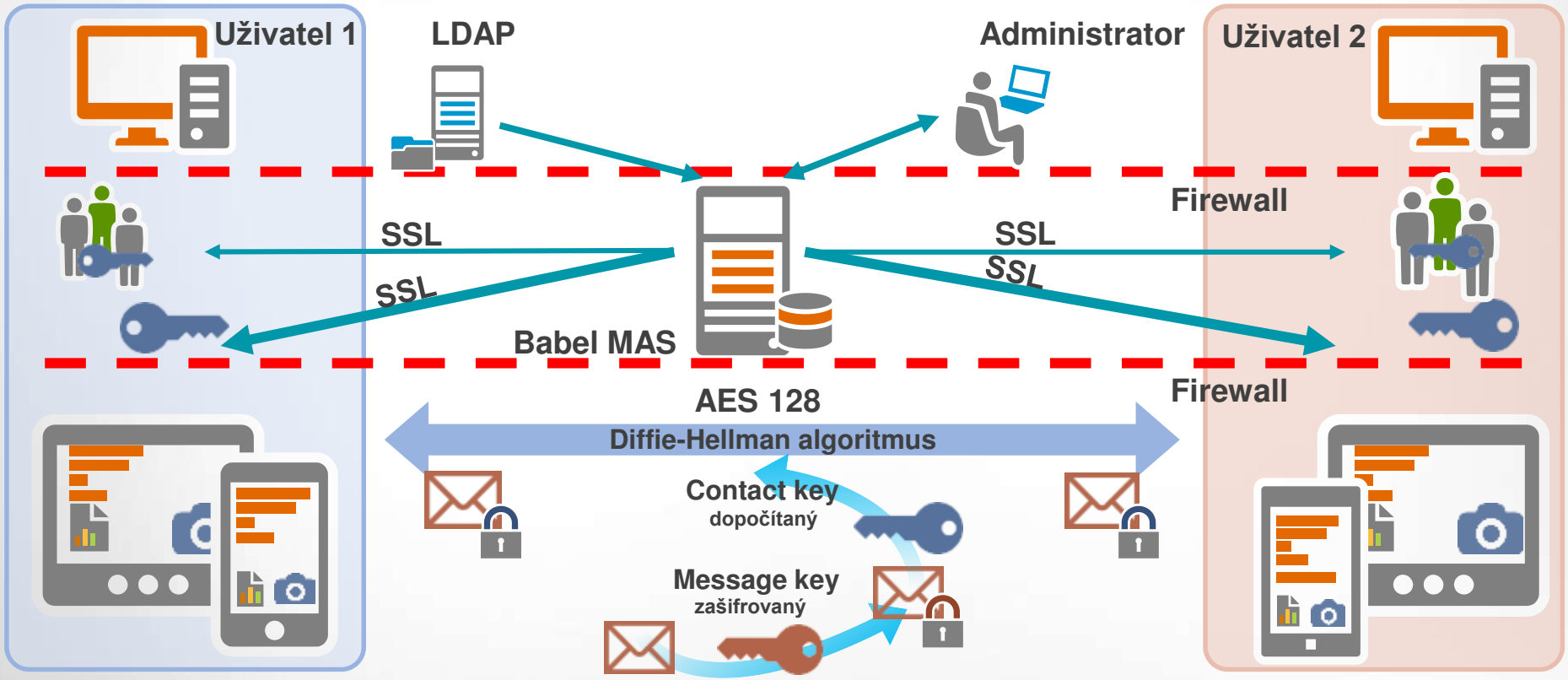
OKsystem

Kryptografická ochrana datového přenosu



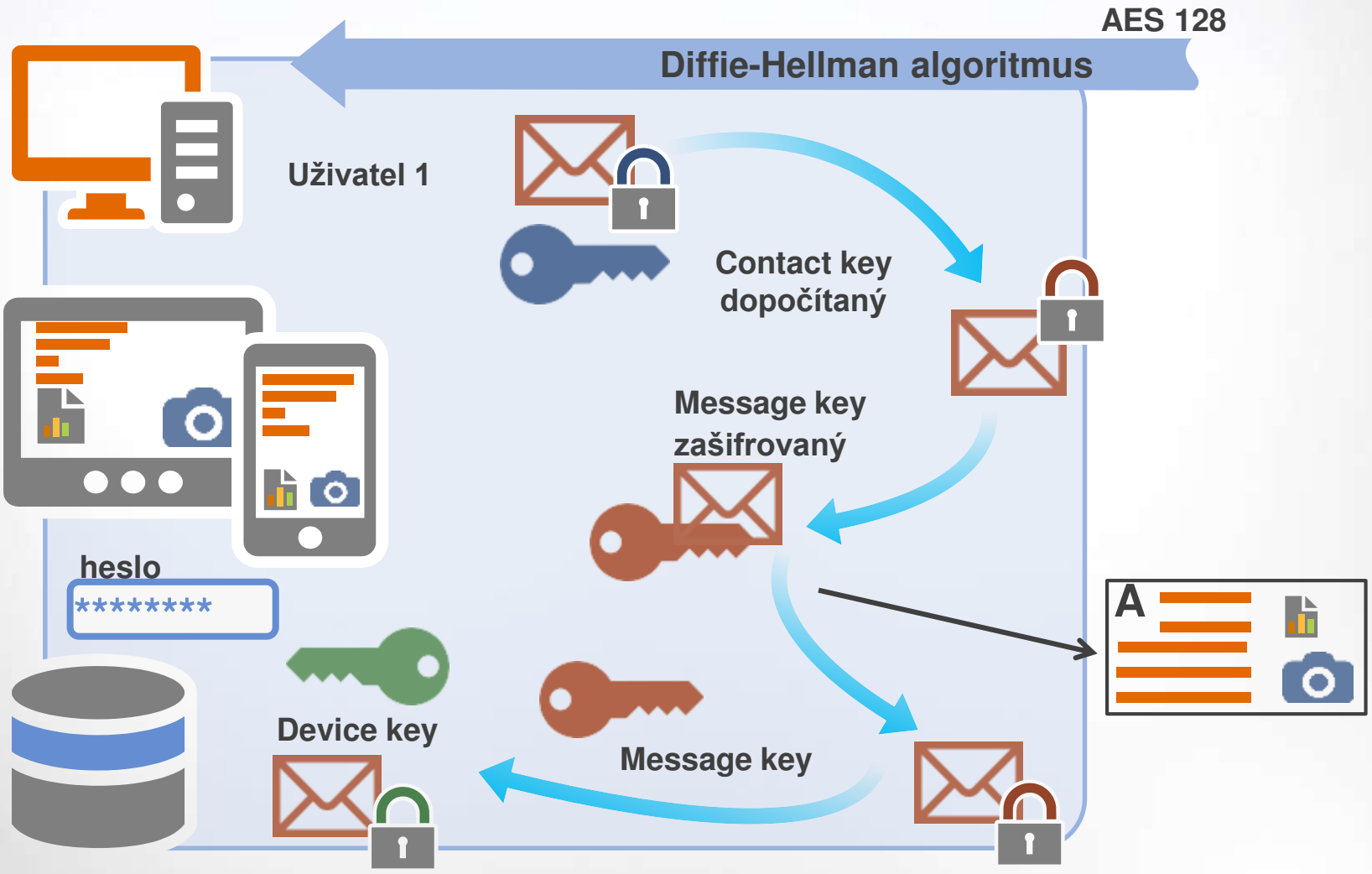
OKsystem

Kryptografická ochrana datového přenosu



OKsystem

Kryptografická ochrana datového přenosu



OKsystem

Význam šifrované komunikace

- **Proč?**
  - Bezpečnost komunikace
  - Produktivita pracovníků (mobilita, flexibilita)

- **Jak?**
  - Enterprise (on-premise) nasazení
  - Integrace na LDAP
  - Mobilní klient: iOS, Android, Win 10
  - Desktop: Windows 7,8.1,10

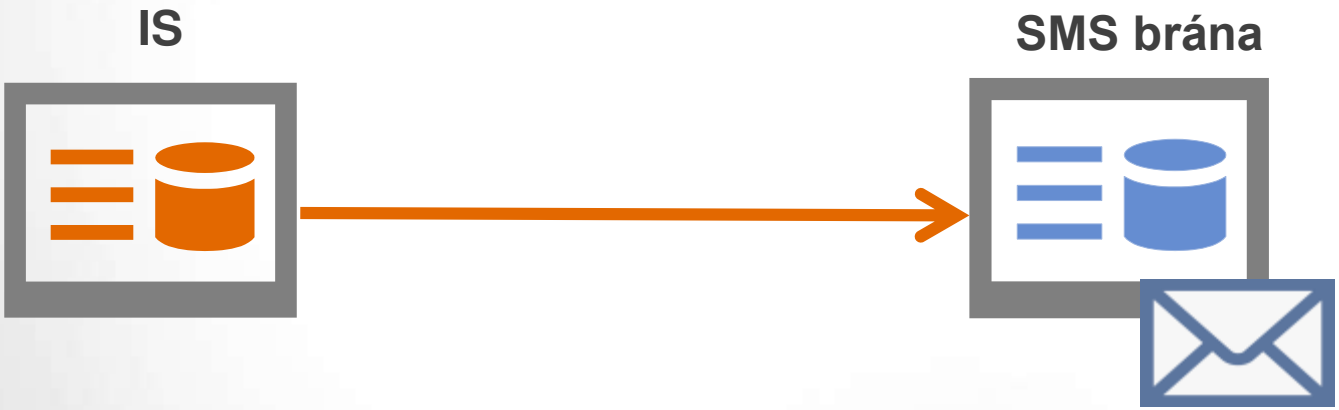
OKsystem

Řešení šifrované komunikace

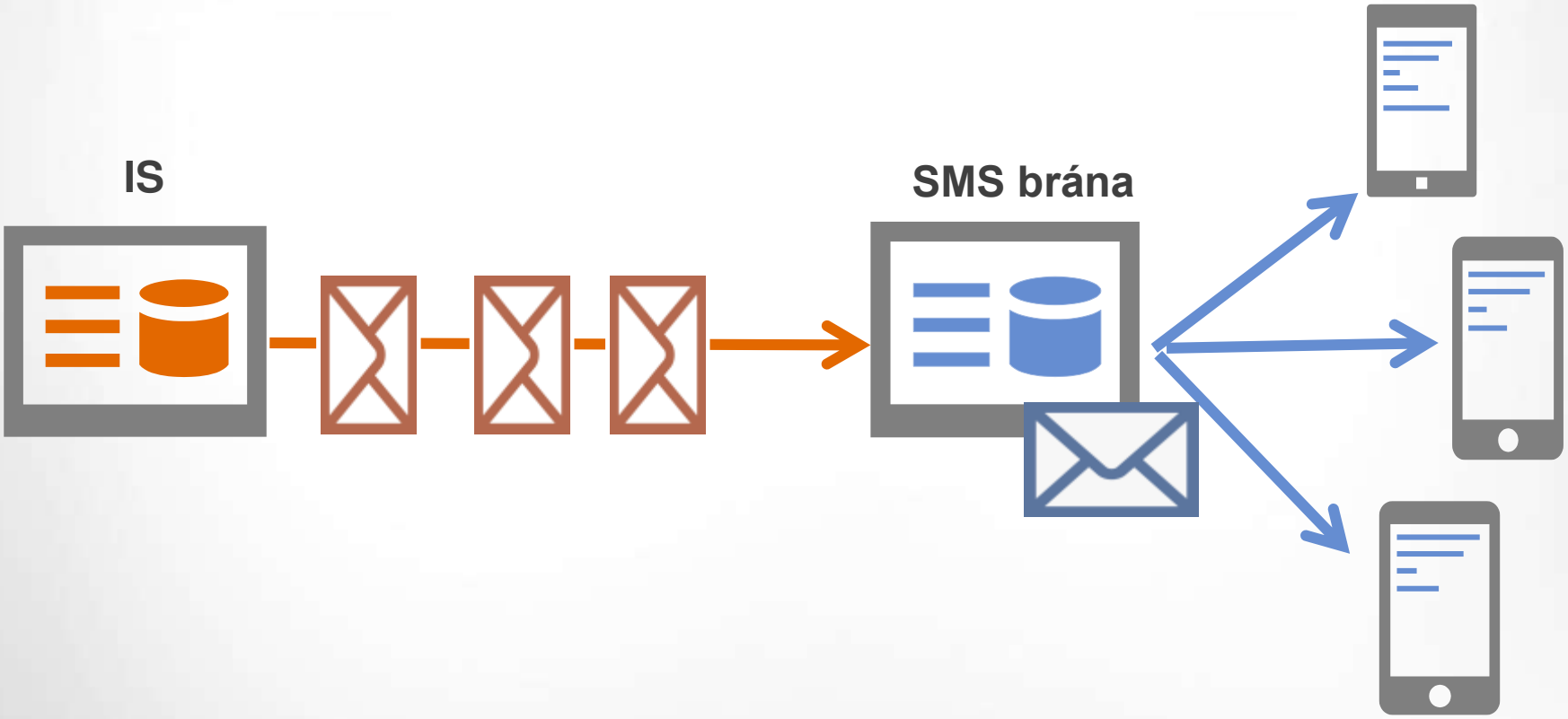
BABEL Business Edition

OKsystem

Jednosměrná komunikace - princip

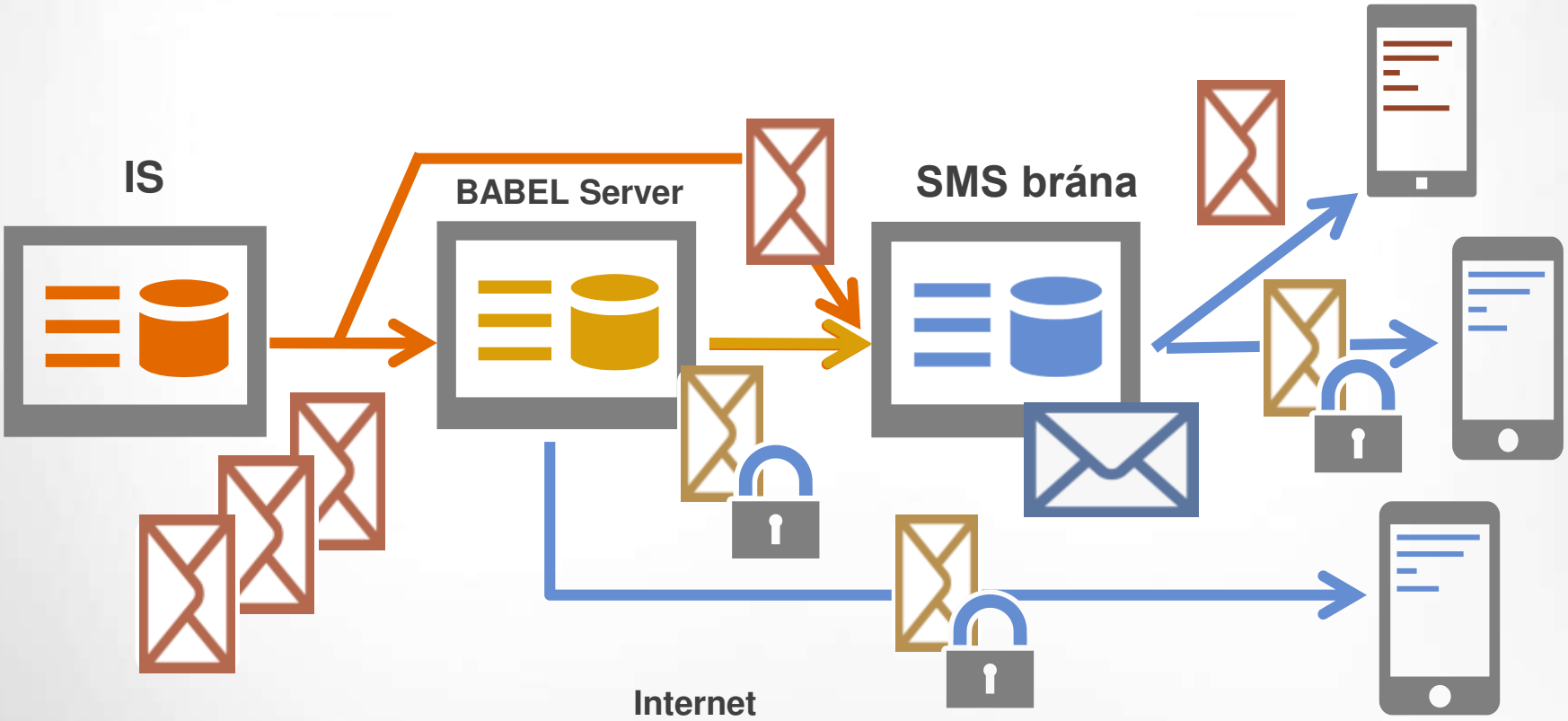


Jednosměrná komunikace - princip



OKsystem

Jednosměrná šifrovaná komunikace - princip



OKsystem

Jednosměrná šifrovaná komunikace - využití

- Zasílání jednorázových přístupových hesel do systému
  - přihlášení do systému v terénu (3Dsecure)
- Zasílání hromadných SMS (datových zpráv) při řešení krizových situací
  - př.: informační kanál o činnostech složek IZS vzhledem k samosprávě
- Zasílání osobních údajů ze systému
  - př.: vlastnictví nemovitostí, finanční informace, přestupky

Děkuji za pozornost