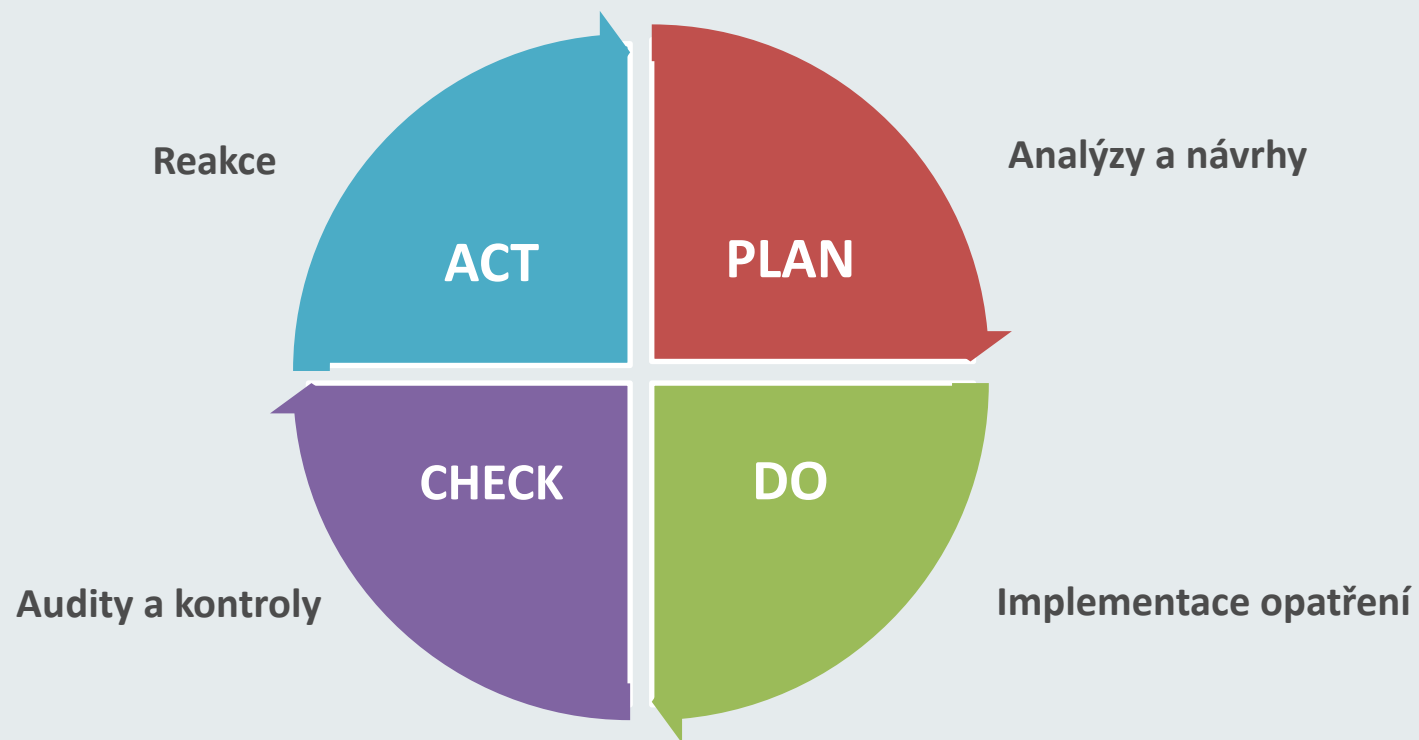


# Budování kybernetické ochrany v Nemocnici Jihlava

Jaroslav Dvořák, AUTOCONT  
David Zažímal, Nemocnice Jihlava

# Budování kybernetické bezpečnosti

**Budování** informační bezpečnosti je **kontinuální** proces plánování, zabezpečování, kontroly a nápravy definovaný jako koloběh činností „Plan-Do-Check-Act“ (PDCA)



**Bezpečnost se nekupuje, bezpečnost se buduje!**

STRATEGIE BEZPEČNOSTI

*Procesní a organizační opatření*

*Technologická opatření*

SOC, NOC - BEZPEČNOSTNÍ A SYSTÉMOVÝ  
DOHLED

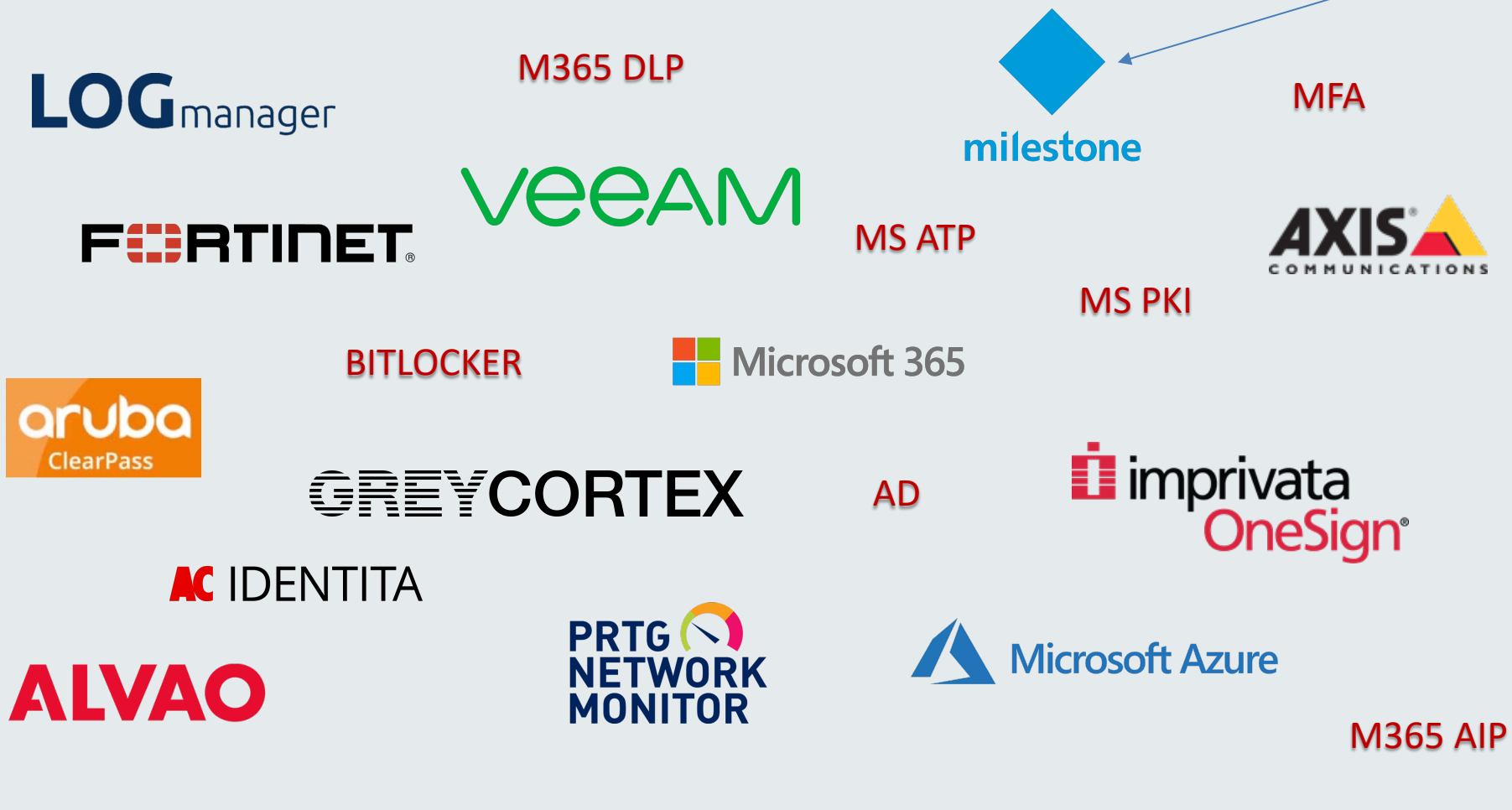
- NemJi je organizací „spadající“ pod zákon o kybernetické bezpečnosti (*únor 2021*)
  - Zákon č.181/2014 Sb.
  - Účinný od 1.1.2015.
  - Určuje způsoby ochrany vůči kybernetickým hrozbám.
  - Definuje dotčené osoby a subjekty.
  - Určuje způsoby řešení bezpečnostních událostí.
  - Navazují na něj prováděcí vyhlášky.
  - Subjektům, které nejsou v souladu se zákonem, hrozí sankce.
  - Z legislativy je 12 měsíců na naplnění podmínek zákona.



- Fyzická bezpečnost.
- Nástroj pro ochranu integrity komunikačních sítí.
- Nástroj pro ověřování identity uživatelů.
- Nástroj pro řízení přístupových oprávnění.
- Nástroj pro ochranu před škodlivým kódem.
- Nástroj pro zaznamenávání činnosti kritické informační infrastruktury a významných informačních systémů jejich uživatelů a administrátorů.
- Nástroj pro detekci kybernetických bezpečnostních událostí.
- Nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí.
- Aplikační bezpečnost.
- Kryptografické prostředky.
- Nástroj pro zajišťování úrovně dostupnosti informací.
- Bezpečnost průmyslových a řídicích systémů.



# Některé technické prostředky v NEMJI



\$17 - Fyzická bezpečnost
\$18 - Bezpečnost komunikačních sítí
\$19 - Správa a ověřování identit
\$20 - Řízení přístupových oprávnění
\$21 - Ochrana před škodlivým kódem
\$22 - Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
\$23 - Detekce kybernetických bezpečnostních událostí
\$24 - Sběr a vyhodnocování kybernetických bezpečnostních událostí
\$25 - Aplikační bezpečnost
\$26 - Kryptografické prostředky
\$27 - Zajišťování úrovně dostupnosti informací
\$28 - Průmyslové, řídicí a obdobné specifické systémy
\$29 - Digitální služby

UŽIVATELÉ      APLIKACE      PROCESY      ISO27000

## A co na to uživatel?

- Uživatel pochopitelně není nadšen.
- Uživatel vnímá zavádění bezpečnostních prvků negativně, protože ho omezují.
- Uživatel často nechápe, proč ho v určitých oblastech omezujeme – je nezbytné systematické školení VŠECH uživatelů.
- Navíc je IT ve zdravotnictví často vnímáno jako „nutné zlo“ ...
- Všechny projekty týkající se kyberbezpečnosti jsou tak zaváděny s jistým odporem uživatelů.

... až na jednu výjimku ...

... „Pípák“ ...



 **imprivata**  
**OneSign<sup>®</sup>**



- Další způsob využití ID karty zaměstnance.
- Zabezpečení druhým faktorem a zároveň zrychlení přihlašování.
- Dvě oblasti zabezpečení přihlašování:
  - k počítači = Multi-factor Authentication (MFA)
  - k aplikacím = Single Sign-On (SSO)
- Alternativa k ID kartě je silikonový náramek – určeno pro pracoviště intenzivní péče a červené zóny.

## Získali jsme:

- zabezpečení koncových stanic pomocí více-faktorové autentizace (**MFA**),
- **zrychlení přihlašování** zdravotnického personálu **k systémům a aplikacím**,
- **zabezpečení a zefektivnění práce na sdílených počítačích s využitím bezkontaktních karet.**



**přihlášení ID kartou**



**přihlášení ID náramkem**

- U každého PC je čtečka. Stávající ID karty + náramky s potiskem.
- Řešení u tabletů – MS Surface – zabudovaná čtečka karet NFC.
- Možnost řešení pomocí USB-C dongle – např. u notebooků.
- Zabezpečení pomocí **FIPS AES 256** šifrování.

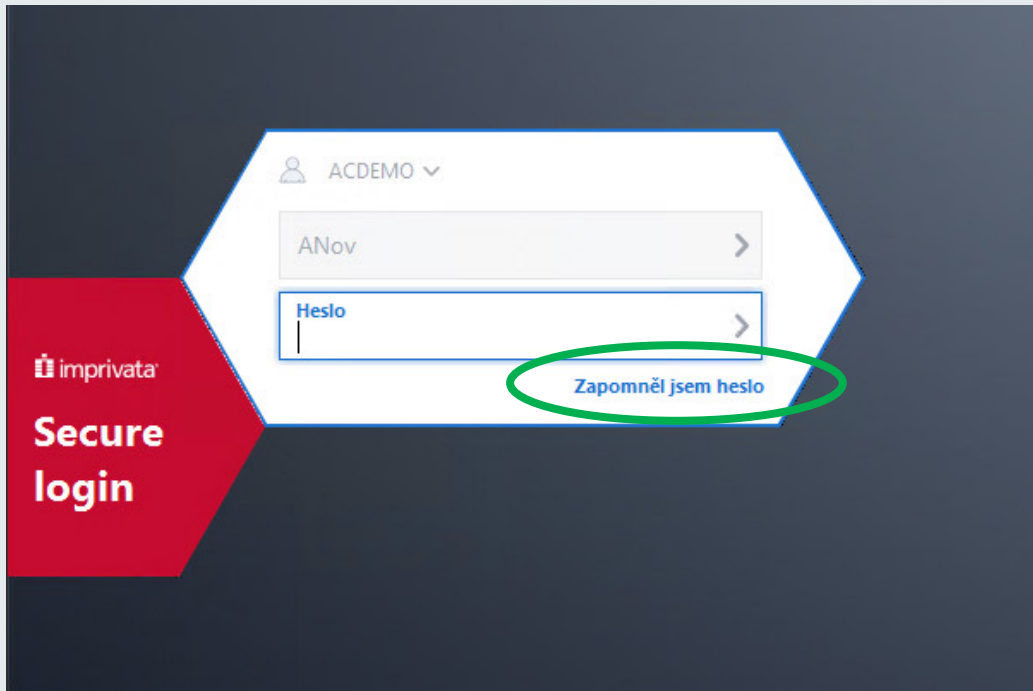
### Systém umožňuje:

- přihlašování uživatelů identitou z Active Directory,
- ukládat hesla v uživatelském správci hesel,
- bezešvé přihlašování do aplikací MS O365 ze sdílených PC,
- univerzálně funkční SSO pro jakékoli webové/desktopové/cloudové/virtualizované aplikace.

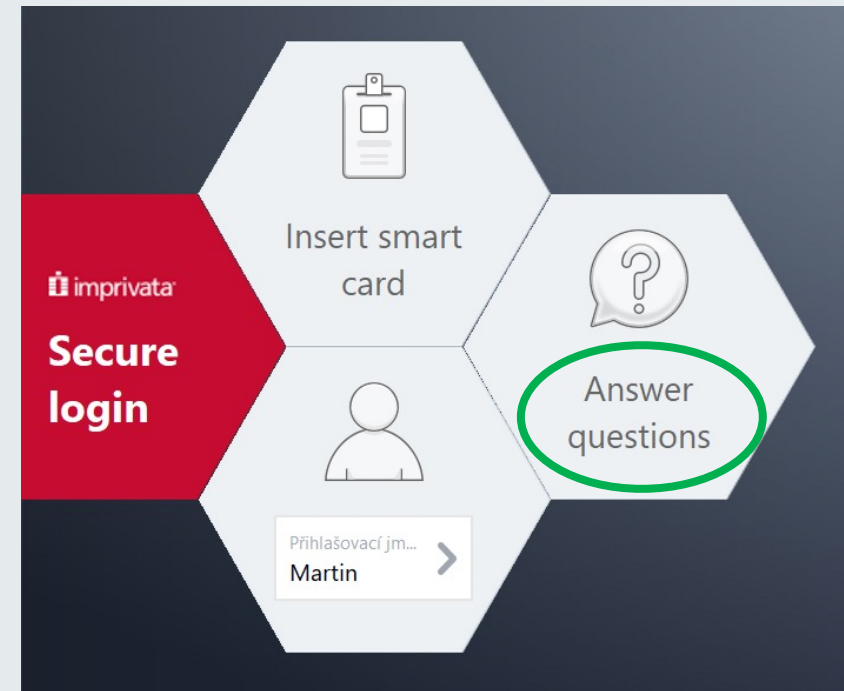
**V tomto způsobu řízení přístupu uživatelů k aplikacím a ostatním ICT prostředkům vidíme budoucnost – certifikovaný Imprivata administrátor přímo v rámci oddělení ICT.**



## Jiné možnosti přihlášení



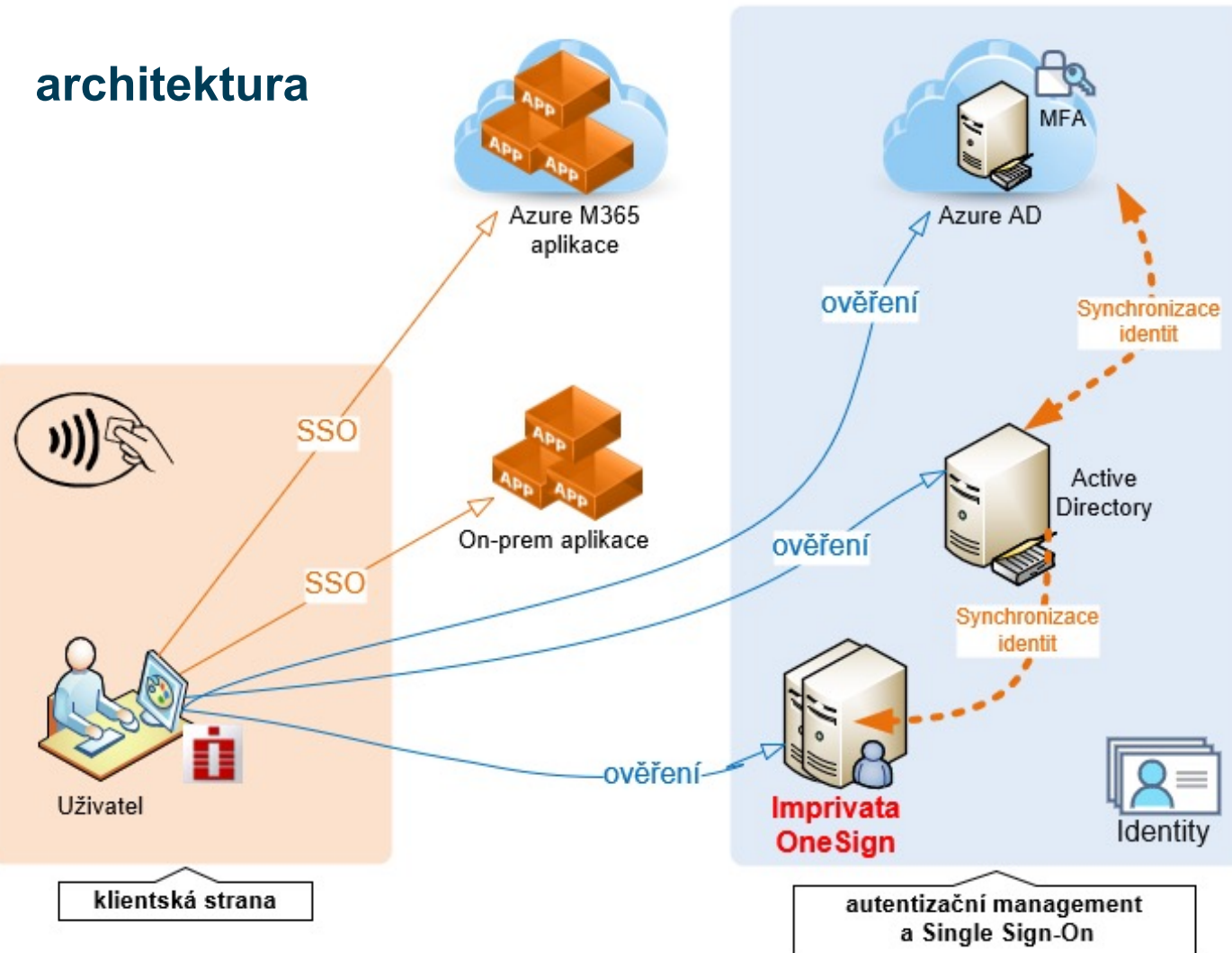
Samoobslužný reset hesla



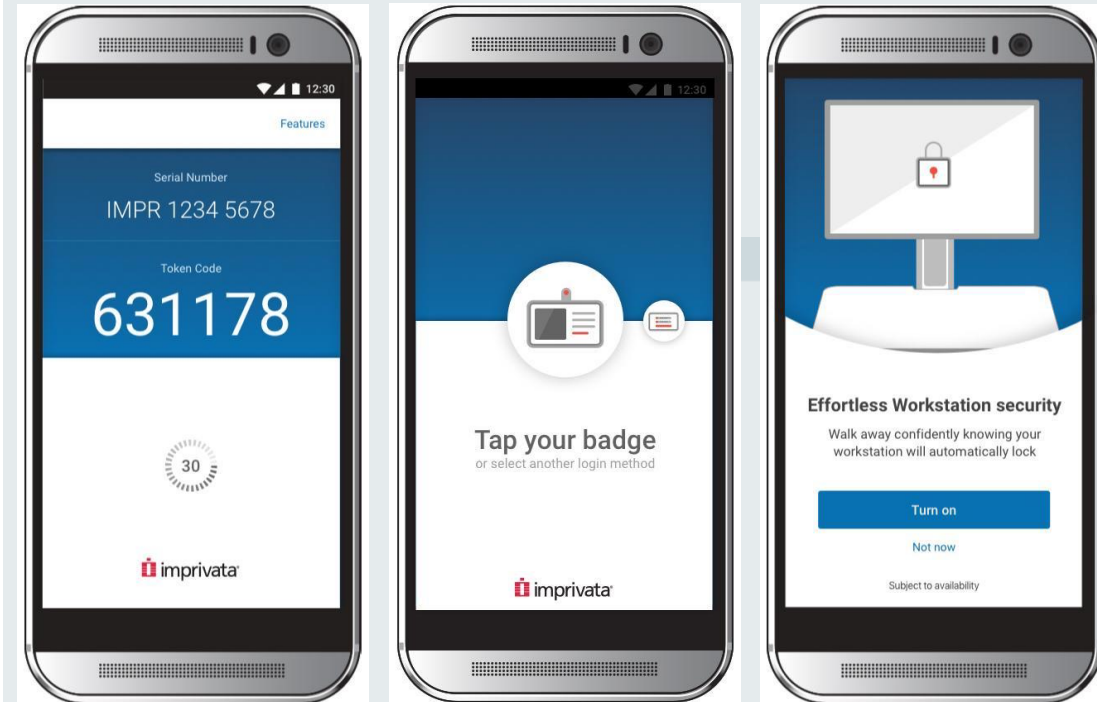
Nouzové přihlášení



## architektura



## další možnosti rozšíření



vzdálený přístup

„pípák“ pro Android

Walk-away security



> 3 700 zákazníků, z toho  
2700 obor zdravotnictví

## OTÁZKY & ODPOVĚDI

 **imprivata<sup>®</sup>**



> 8m uživatelů ve 40 zemích

**Děkujeme za pozornost ...**

David Zažímal  
Jaroslav Dvořák

[www.nemji.cz](http://www.nemji.cz)

