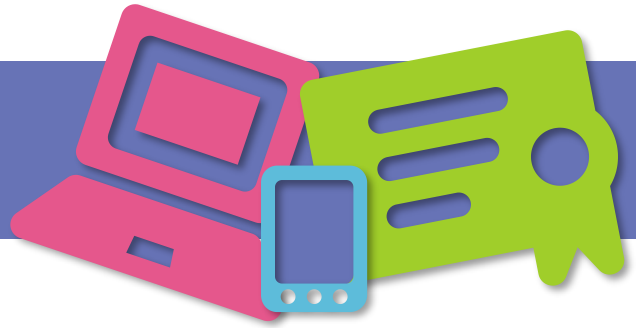
SECURITY 2015

23. ročník konference o bezpečnosti v ICT



Mobilní zařízení jako autentizační nástroj a jeho integrace do systémů

Milan Hrdlička

MONET+, a.s.

Osnova

- Buzzword „mobilní token“
- Není integrace jako integrace
- Mobilní token ≠ SW token
- Co lze očekávat v budoucnosti?

Mobile token…

mobile token

Internet | Obrázky | Mapy | Nákupy | Videa | Více | Vyhledávací nástroje

Přibližný počet výsledků: 55 000 000 (0,38 s)

One Time Password (OTP) | Mobile Soft Token | Entrust
www.entrust.com/products/**mobile**-otp/ ▾ Přeložit tuto stránku
Leverage **mobile** devices for improved security including one time passwords (otp) authentication, transaction verification, and embedded **mobile** app security.

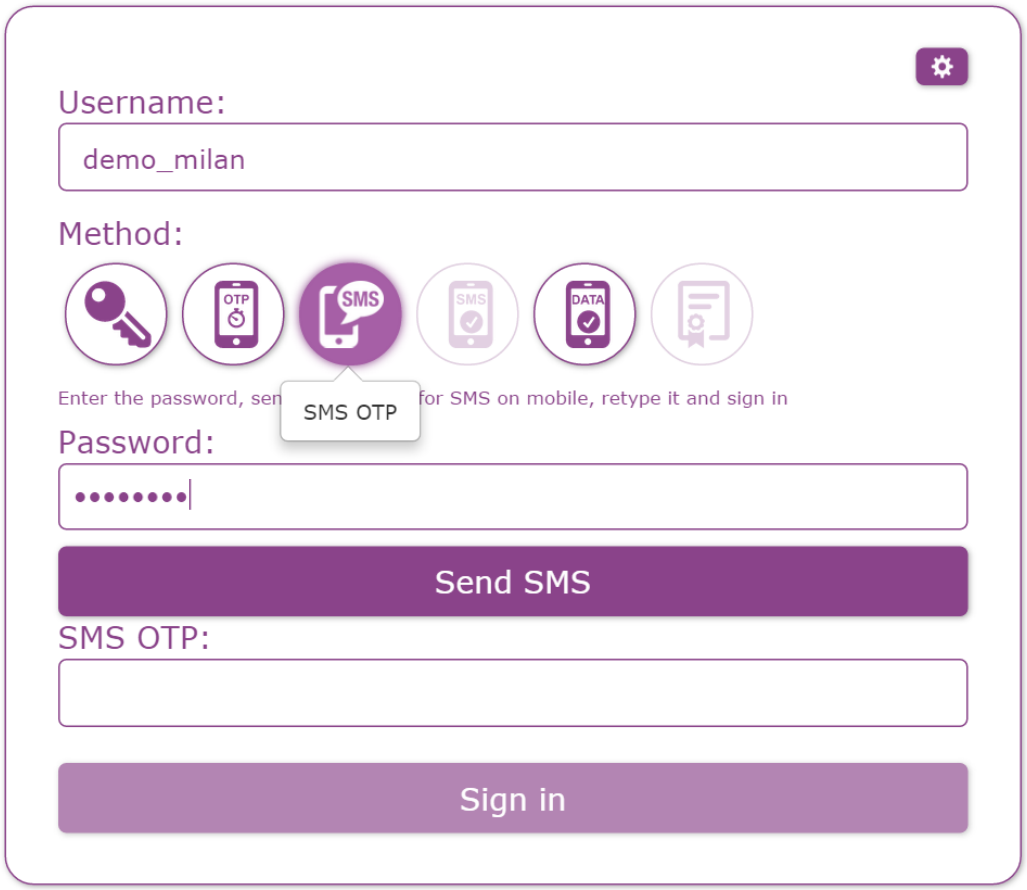
Mobile Token: Generatore Password nel Cellulare ...
www.unicredit.it › ... › app per smartphone ▾ Přeložit tuto stránku
Infatti, l'applicazione UniCredit per cellulare contiene il **Mobile Token** uno strumento che consente, nella massima sicurezza, di generare password dispositive.

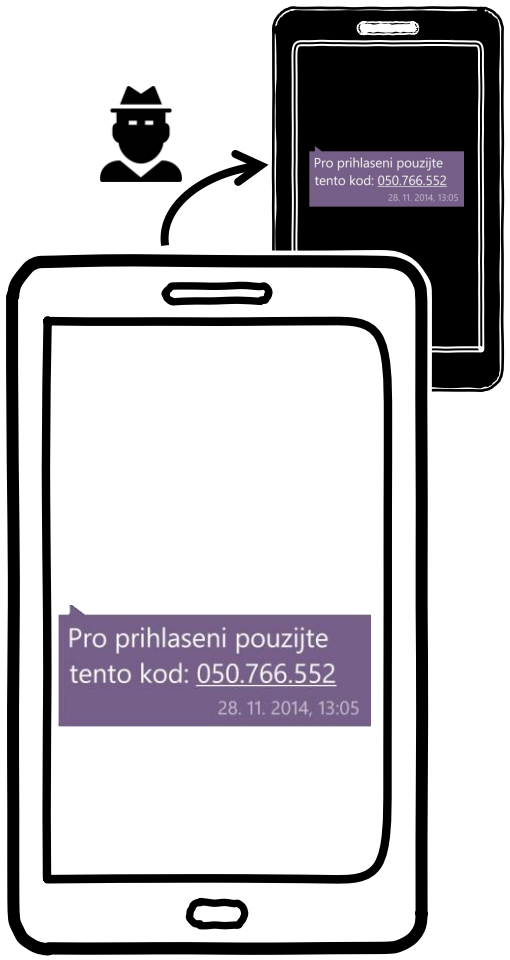
Obrázky pro dotaz mobile token — Nahlásit obrázky

Další obrázky pro dotaz mobile token

SMS zaslaná poskytovatelem služby

```
Uri uriSMSURI = Uri.parse("content://sms/inbox");
```





Android poskytuje API pro přístup na SMS (aplikace musí mít povolení android.permission.READ_SMS – kontrolují jej uživatelé?)

Proč mobilní token?

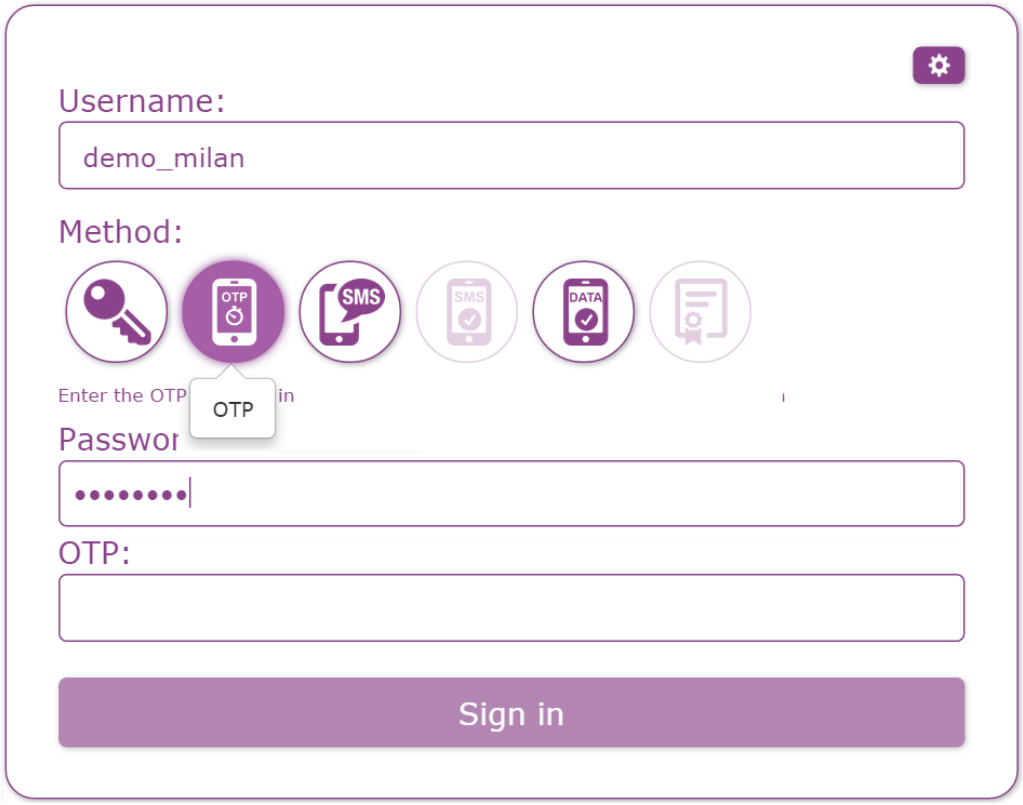
TOP 20 mobile threats of 2014

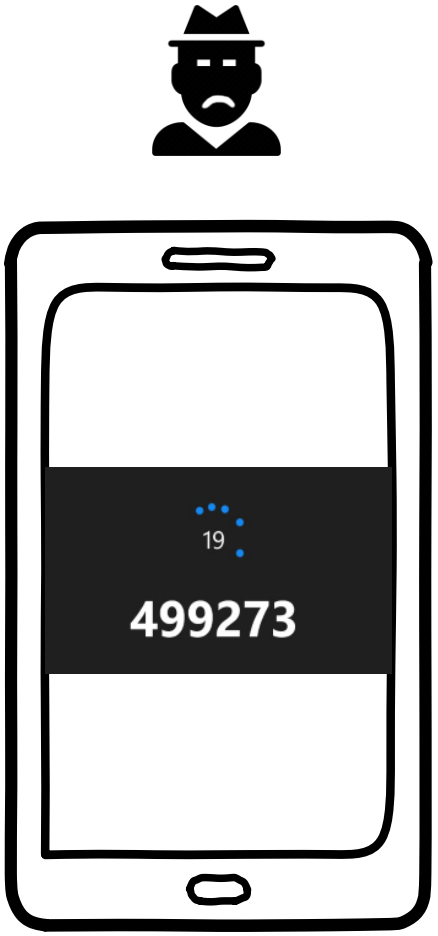
	Name	% of attacks
1	Trojan-SMS.AndroidOS.Stealer.a	18.0%
2	RiskTool.AndroidOS.MimobSMS.a	7.1%
3	DangerousObject.Multi.Generic	6.9%
4	RiskTool.AndroidOS.SMSreg.gc	6.7%
5	Trojan-SMS.AndroidOS.OpFake.bo	6.4%
6	AdWare.AndroidOS.Viser.a	5.9%
7	Trojan-SMS.AndroidOS.FakeInst.a	5.4%
8	Trojan-SMS.AndroidOS.OpFake.a	5.1%
9	Trojan-SMS.AndroidOS.FakeInst.fb	4.6%
10	Trojan-SMS.AndroidOS.Erop.a	4.0%
11	AdWare.AndroidOS.Ganlet.a	3.8%
12	Trojan-SMS.AndroidOS.Agent.u	3.4%
13	Trojan-SMS.AndroidOS.FakeInst.ff	3.0%
14	RiskTool.AndroidOS.Mobogen.a	3.0%
15	RiskTool.AndroidOS.CallPay.a	2.9%
16	Trojan-SMS.AndroidOS.Agent.ao	2.5%
17	Exploit.AndroidOS.Lotoor.be	2.5%
18	Trojan-SMS.AndroidOS.FakeInst.ei	2.4%
19	Backdoor.AndroidOS.Fobus.a	1.9%
20	Trojan-Banker.AndroidOS.Faketoken.a	1.7%

KASPERSKY SECURITY BULLETIN 2014

10 z 20-ti hrozeb jsou typu SMS trojan

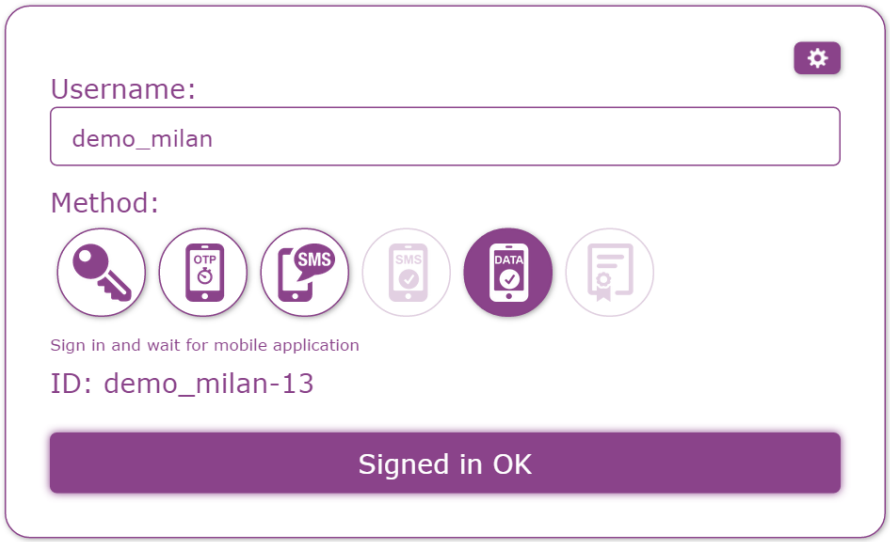
OTP generované aplikací v mobilu



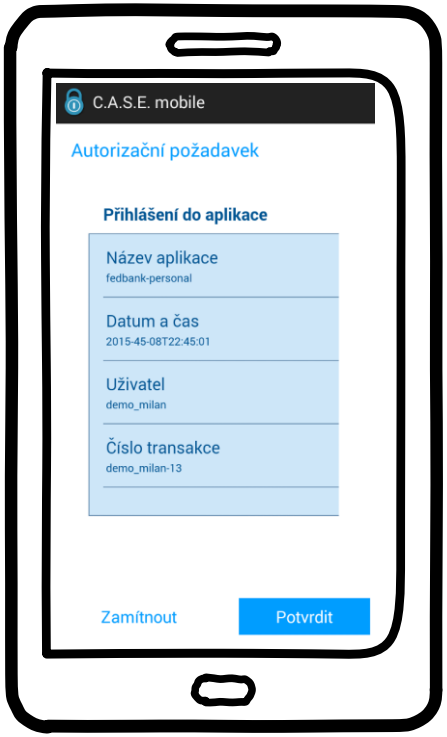


OTP = One Time Password
Heslo, které lze použít pouze jednou. Platí jen omezený čas.
Nelze jej snadno z aplikace získat.

Push notifikace



Push notifikace



Online potvrzení

Potvrzení uživatelem

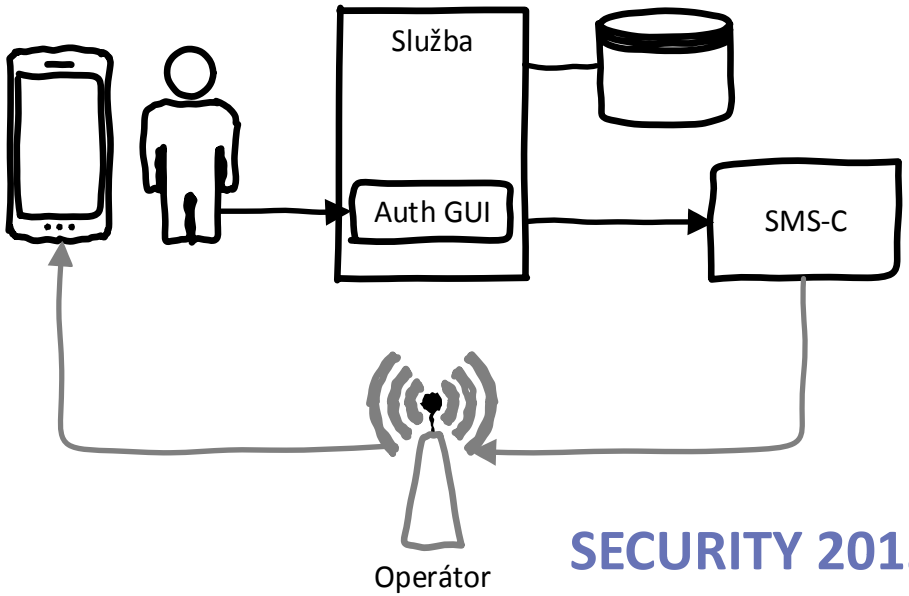
Potenciál mobilního tokenu

- Ideální náhrada za SMS
  - Vyšší bezpečnost
  - Nižší provozní náklady
  - Vysoký komfort s použitím datového spojení a push notifikací
- Pozor na provisioning!
  - SMS těží z HW bezpečnosti SIM
  - Typicky SW řešení je nutné správně inicializovat
  - Vytvoření tajemství, vazba na identitu uživatele
  - Řeší se kompromis pohodlí vs bezpečnost

Není integrace jako integrace…

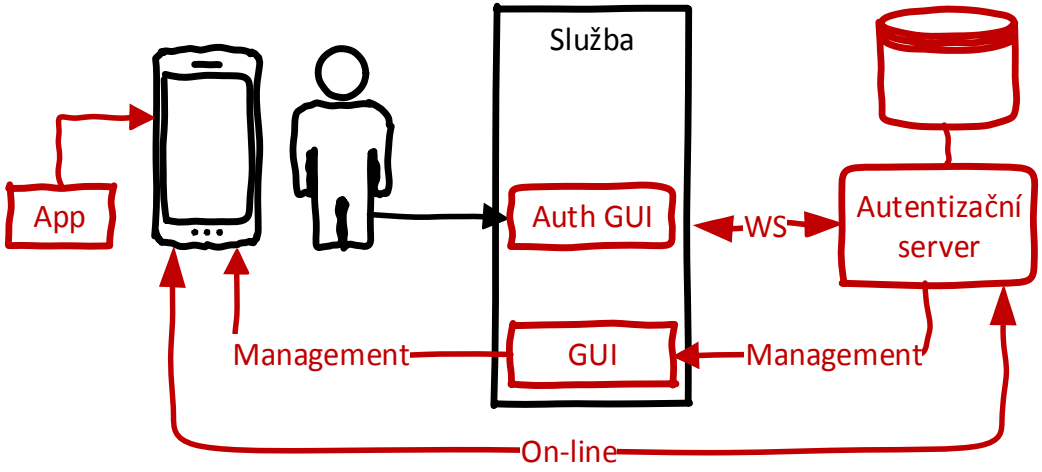
Běžný způsob integrace SMS auth

- Do služby (např. internetbankingu) je přímo integrována autentizační metoda
  - Přímé napojení na SMS centrum (SMS-C)
  - DB s generovanými OTP
  - Jednoduchá funkce pro porovnání zadaného SMS OTP kódu proti DB



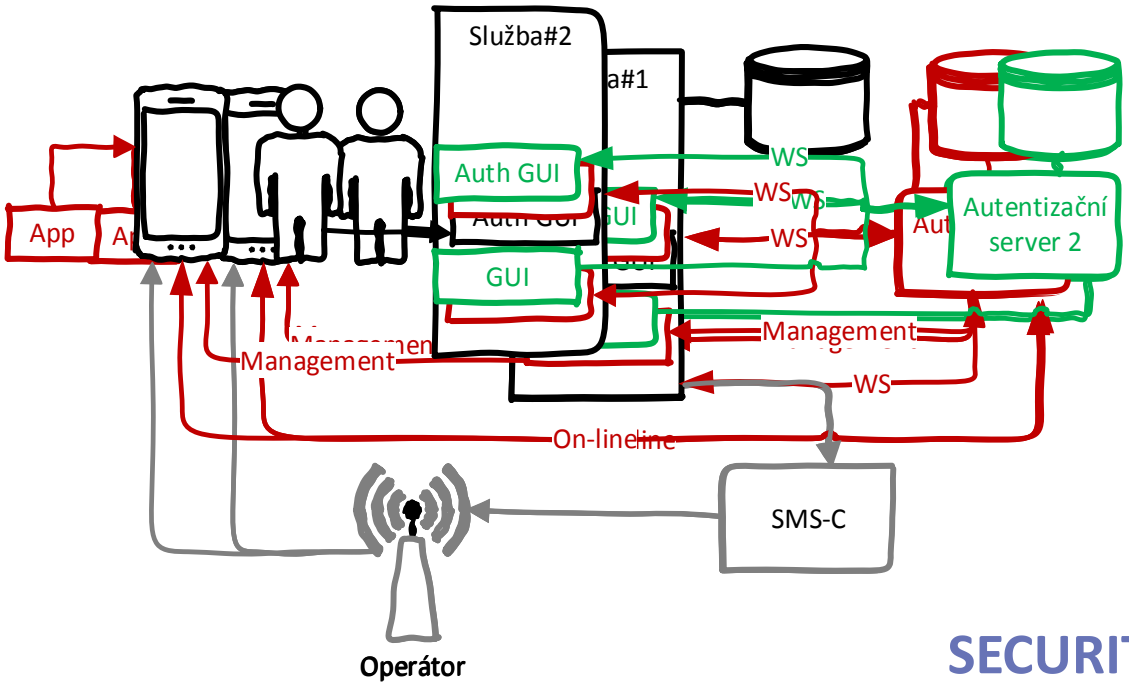
„Legacy“ integrace nové metody

- Služba je integrována s autentizačním serverem technologickým rozhraním (SOAP, …)
  - Provisioning tajemství, synchronizace
  - Verifikace
- Nové procesy, podpora
- Nové GUI
  - Autentizační
  - Autorizační
  - Správa



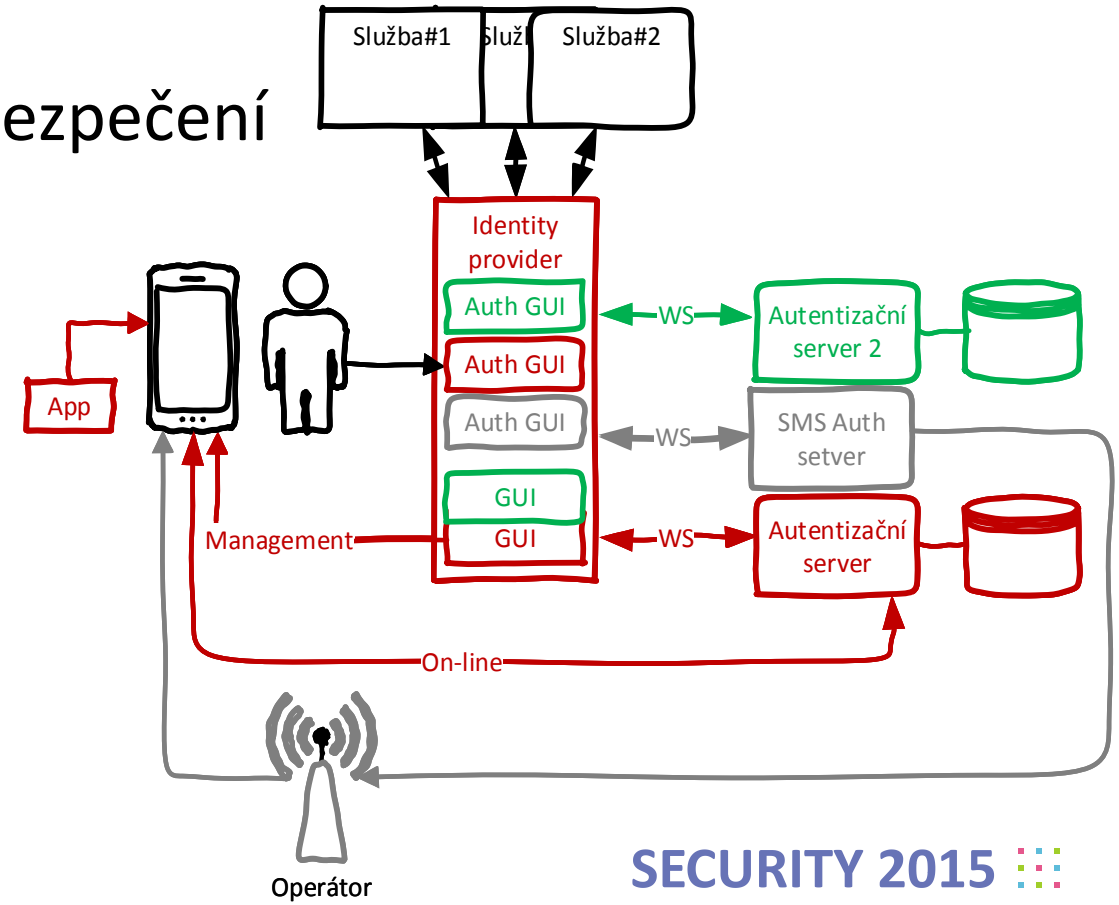
Podpora starých a nových metod

- Služba integruje
  - API obou (všech) metod
  - GUI rozhraní obou (všech) metod
- Více služeb i více metod komplikuje integraci

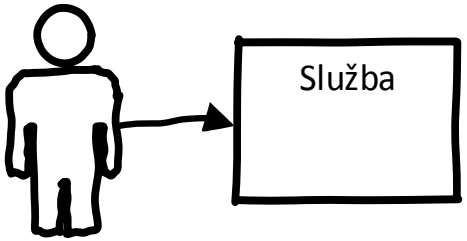


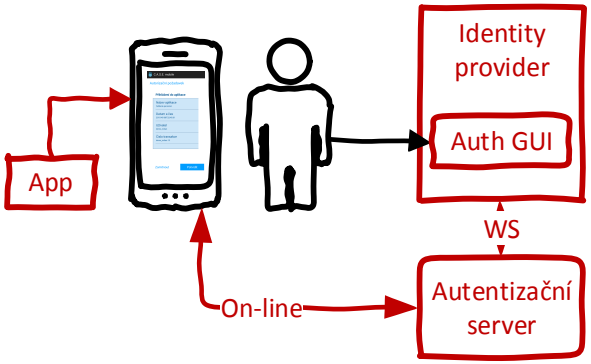
Oddělení služeb a bezpečnosti

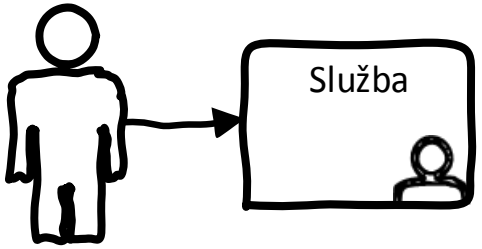
- Služby mají jen jedno integrační rozhraní na identity providera
- Identity provider
  - Externalizuje zabezpečení
  - GUI pro použití
  - GUI pro správu
  - Procesy, funkce
- Standardy
  - SAML, OAuth, …

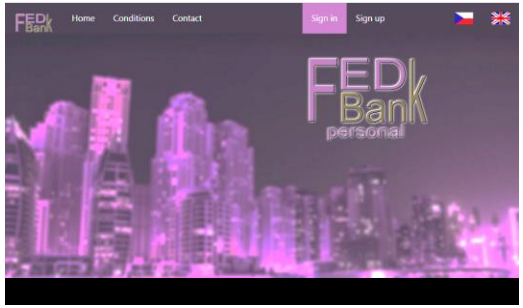


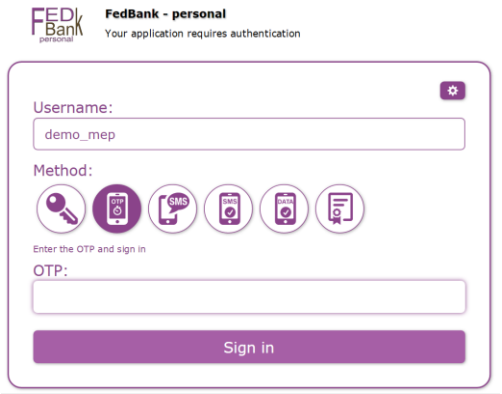
Flow přihlášení

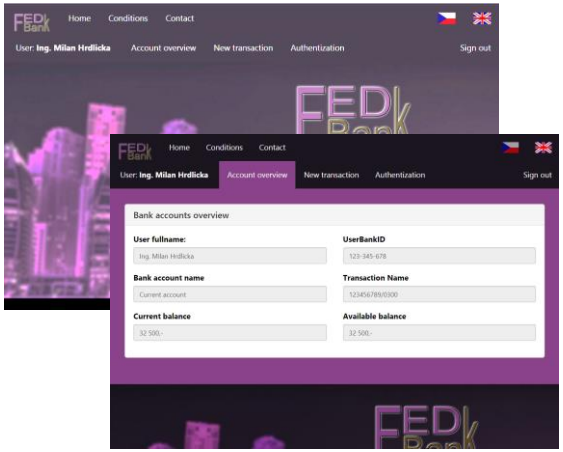




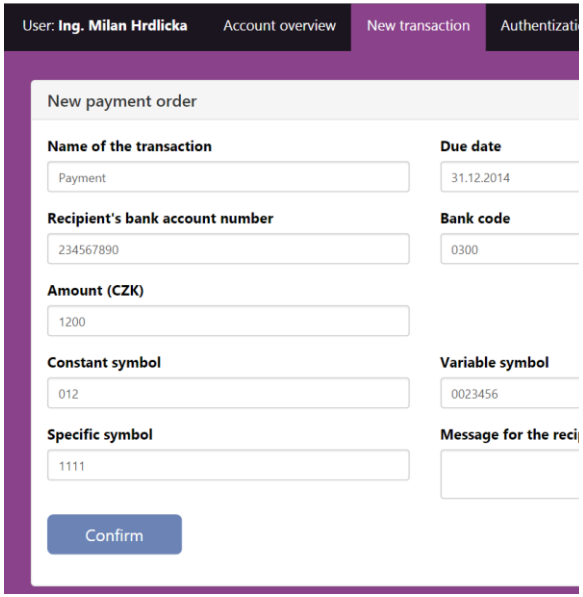


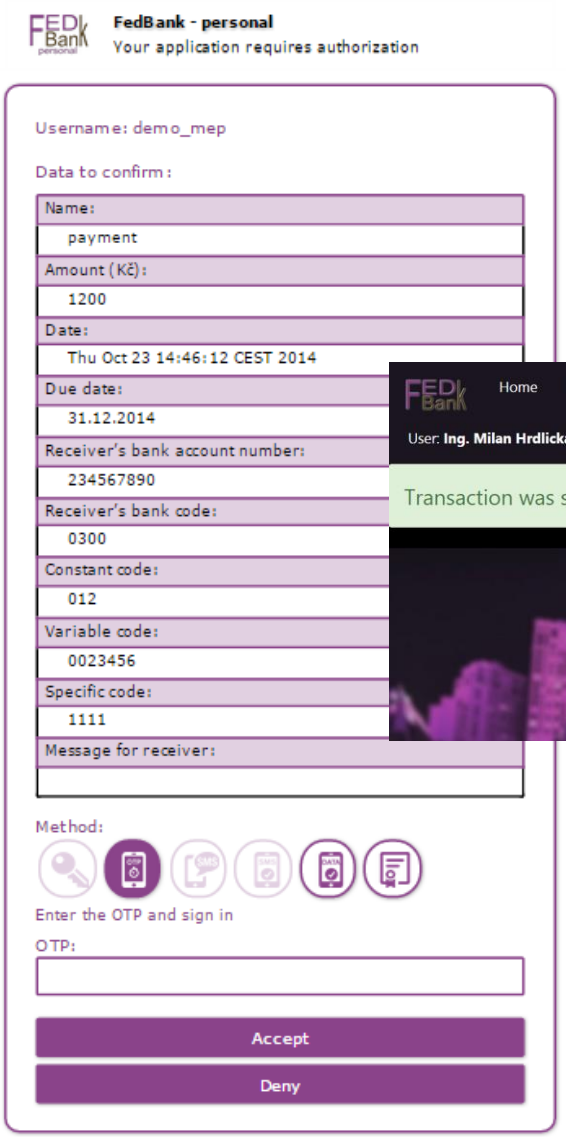


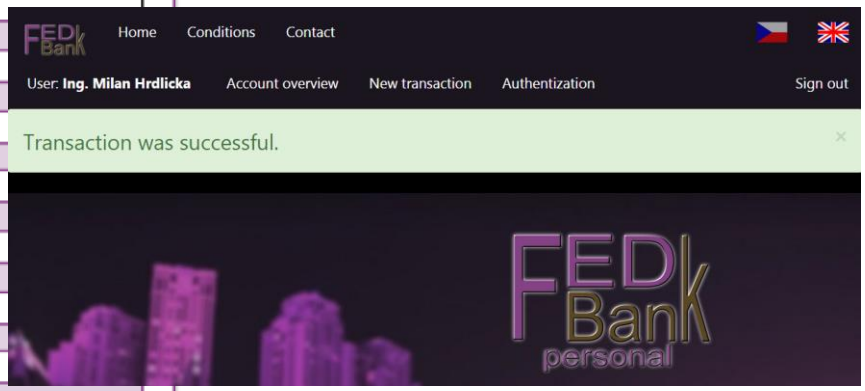




Flow autorizace transakcí

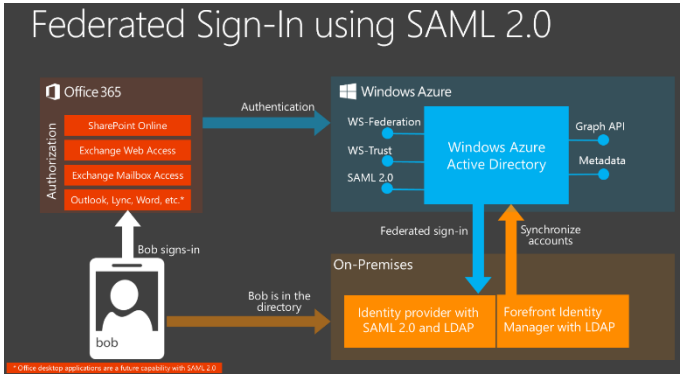




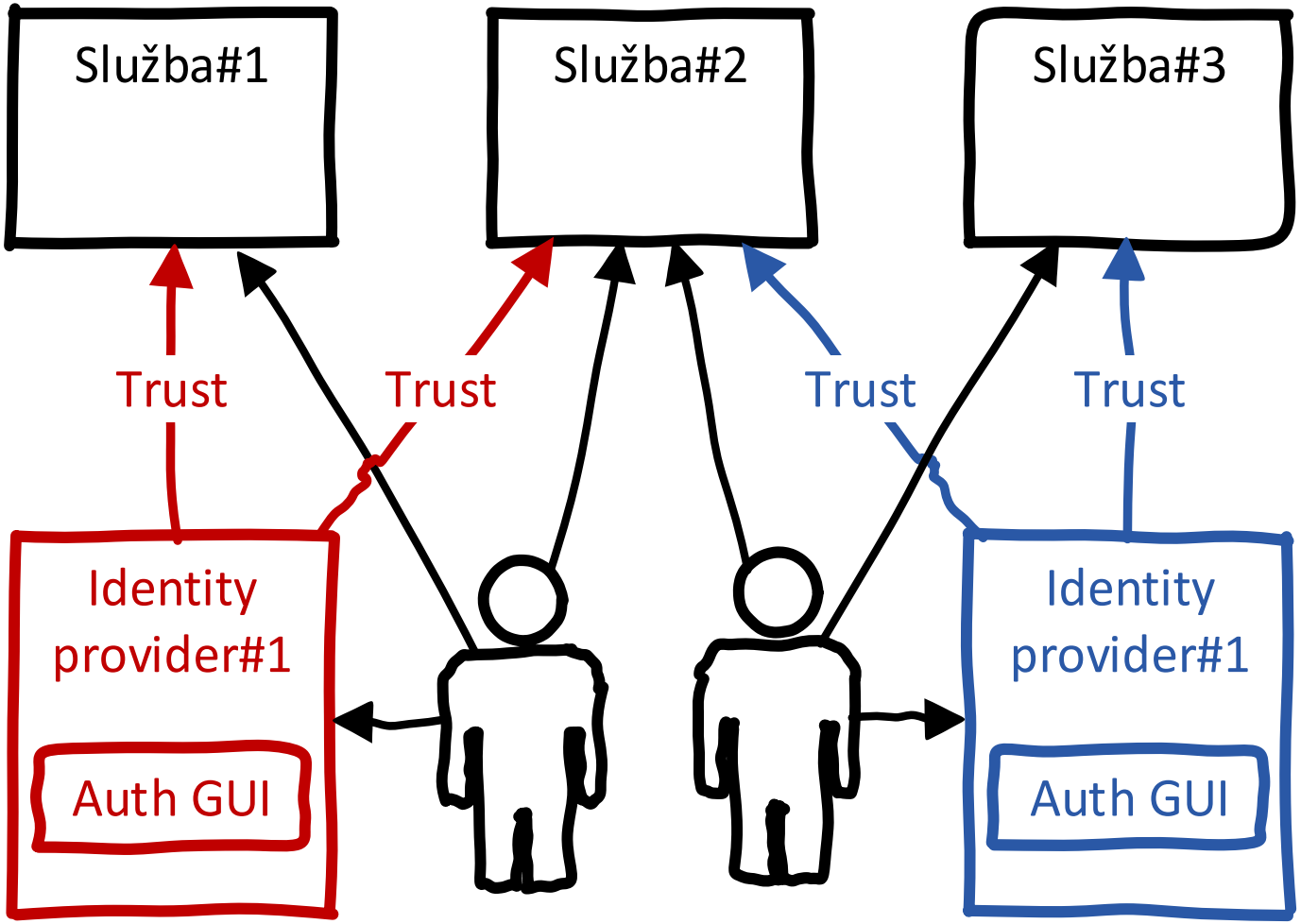


SAML 2.0 vs OAuth 2.0

- SAML – Security Assertion Markup Language
  - Robustní standard pro výměnu autentizačních a autorizačních dat na bázi XML (+podpis a šifrování)
  - Heterogenní systémy
    - Více Service providerů, více Identity providerů
  - Používá jej mnoho cloudových služeb pro externalizaci přihlášení uživatele
    - Office 365, Google Apps, Salesforce, WebEx, Workday, AtTask, LotusLive, OpenAir, Yammer, Zendesk, …



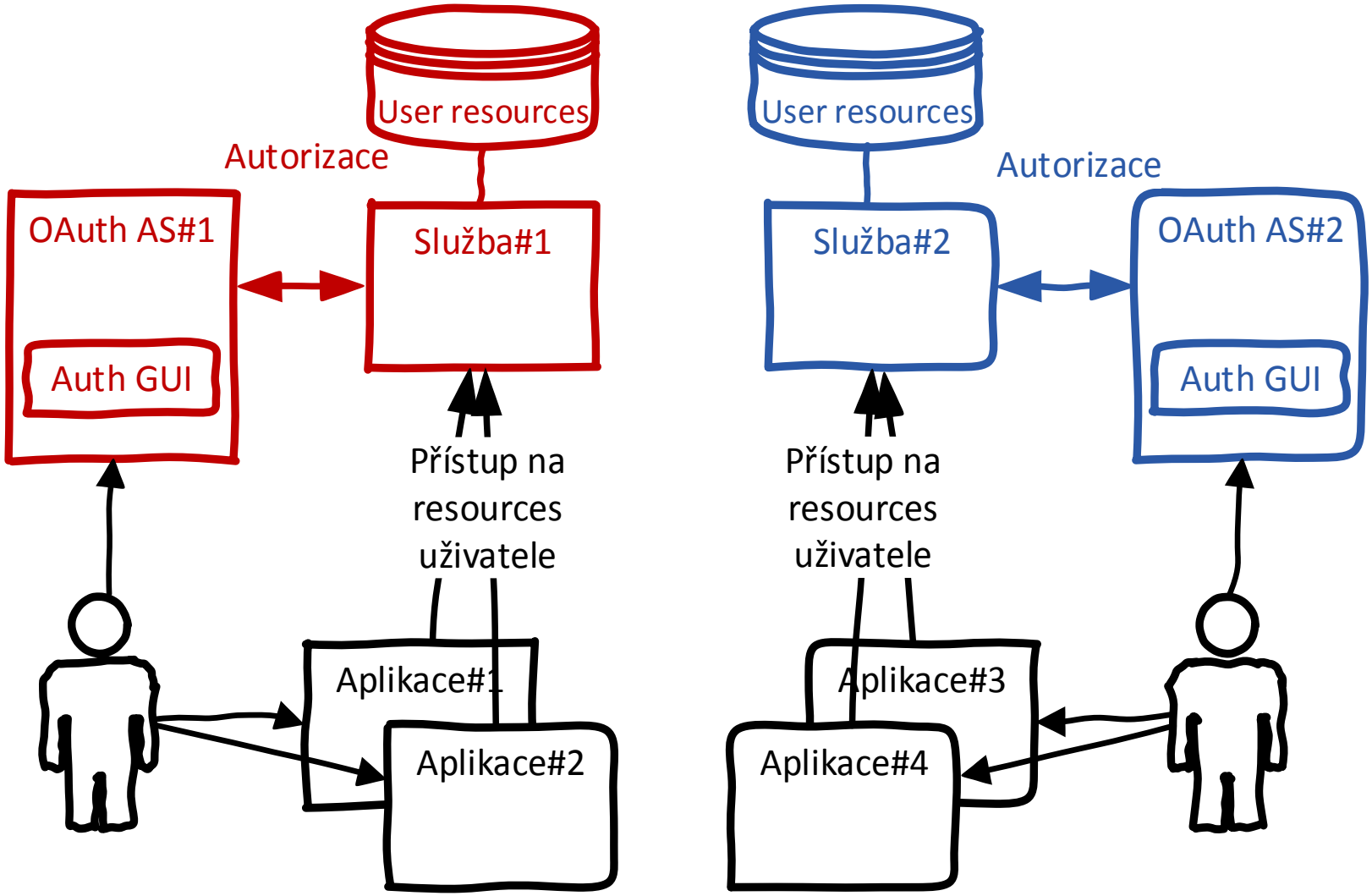
SAML ekosystém



SAML 2.0 vs OAuth 2.0

- OAuth 2.0 – Autorizační Framework
  - RFC 6749, RFC 6750, RFC 6819
  - OAuth autorizační server externalizuje proces autentizace uživatele a autorizace přístupu aplikace třetí strany na resources pod jménem uživatele
  - Resources mohou být nejen data, ale i API
    - Populární pro ochranu přístupu na WebAPI
  - Přístup chráněn pomocí „access tokenů“
  - **Proprietární vazba mezi OAuth AS a službou poskytující resource! → Nízká interoperabilita!**

OAuth ekosystém



Mobilní token ≠ SW token

SW mobilní OTP token

- Založen na sdíleném tajemství
- On-line i off-line
- Algoritmy HOTP, OCRA (RFC 4226, 6287)
  - Existuje mnoho HW HOTP, OCRA kalkulátorů
  - Koexistence standalone HW OTP a smart SW řešení
- Data uložena tak, aby útočník nemohl offline ověřit jejich správnost
  - Autentizační metoda se blokuje online na serveru
  - Možné volit méně komplexní PIN
- On-line provisioning nutný pro podporu push notifikací

SW mobilní PKI token

- Založen na asymetrické kryptografii a certifikátech
  - Lepší princip neodmítnutelnosti odpovědnosti
  - Mírně snazší provisioning (nedochází k výměně sdíleného tajemství)
- Pouze on-line režim
- Pár veřejný a privátní klíč dává útočníkovi možnost zkontrolovat správnost hesla
  - Použití složitého hesla snižuje ergonomii

SIMToolkit

- SIM karta řídí mobilní telefon
  - Zobrazení
  - Čtení klávesnice
  - SIM = bezpečný HW → **velmi bezpečné**
  - Podpora drtivé většiny handsetů
- Se SIM lze komunikovat Over The Air (OTA)
  - Snadný provisioning
  - Cena za SMS
- Nutná dohoda s operátorem
- Bez použití OTA problematická ergonomie

NFC – UICC

- UICC – multiaplikační („NFC“) SIM
  - Vzdálená OTA správa pomocí TSM infrastruktury
  - Prakticky libovolná aplikace
    - Symetrická/Asymetrická kryptografie
    - Online i offline režim
    - Plně grafické GUI mobilní aplikace
  - Klíče bezpečně uloženy v SIM kartě
  - Řízení přístupu na SIM
- Nutná dohoda s operátorem
- Nízká penetrace technologie
  - WP8.1 a vybrané Android
- Pouze pilotní projekty
  - Piloty technologie i business modelů

NFC – reader/writer mode

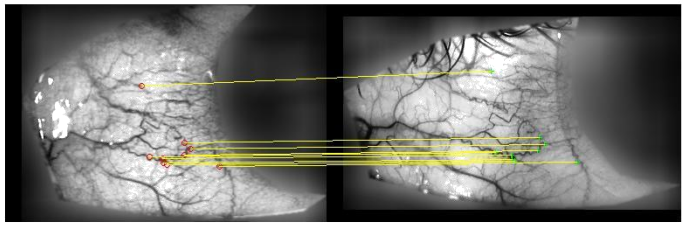
- Mobilní telefon pracuje jako čtečka bezkontaktních karet
  - PKI, ale i „klasické“ bezkontaktní platební karty
- Nízká penetrace a interoperabilita technologie
- Vyzkoušejte si svůj NFC telefon a bezkontaktní platební kartu ;)

cardme

Touch ID, Eyeprint ID™, …

- Uživatelsky atraktivní
- Tak (ne)bezpečné, jak (ne)bezpečné jsou současné biometrické technologie
- Touch ID – *„Your fingerprint is the perfect password“*

- Eyeprint ID™ – *„Highly accurate and secure biometric for mobile devices“*
  - „image and pattern match the blood vessels in the whites of the eye“

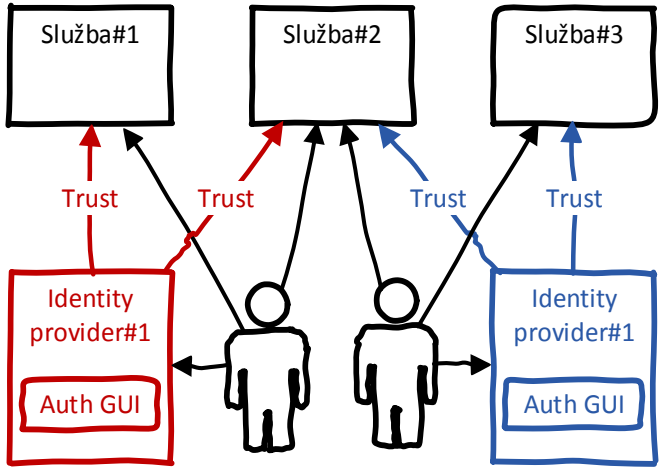


Bluetooth Low Energy tokeny

- Atraktivní v kombinaci se smart watches popř. jinými „wearables“
- Uživatel odsouhlasí transakci stiskem tlačítka, popř. gestem
- BLE zařízení přidává další faktor
  - Ovšem čím chytřejší, tím více se problém bezpečnosti přesouvá do BLE zařízení

Budoucnost

- Budoucnost přinese velké množství zajímavých technologií
  - Rozvoj biometrických metod
  - Wearables s monitoringem životních funkcí
  - NFC, TEE, …
  - eIDAS
- Správnou integrací bezpečnostních technologií můžete už dnes být připraveni na zítřek ☺



SECURITY 2015

23. ročník konference o bezpečnosti v ICT

Děkujeme za pozornost.

Milan Hrdlička

MONET+, a.s.

mhrdlicka@monetplus.cz