

NAKIT

Národní agentura pro
komunikační a informační
technologie, s. p.

Dvoufázová autentizace a Portál občana

7/2/2019

Jan Vlasák



Hesla dávají smysl

Proto je nutné k heslům přidávat další faktory ověření uživatele

- Příliš složité heslo není možné si pamatovat
 - často visí na papírcích v kanceláři nebo na pracovní ploše v počítači
- Politika hesla na velké písmeno, číslici a min. délku 10 znaků, které je rychle prolomitelné v kombinaci slovníkového a brute force útoku
 - **Lednice159, 123Dovolena**
- Uživatelé nebudou tvořit silná hesla (nelze si je pamatovat)
- Bezpečnější jsou pamatovatelná hesla/PIN společně s dalším faktorem ověření (faktor vlastnictví, faktor biometrie)
- Budoucnost patří ověřování „bez hesla“



Druhý faktor uživatele

V Portálu občana

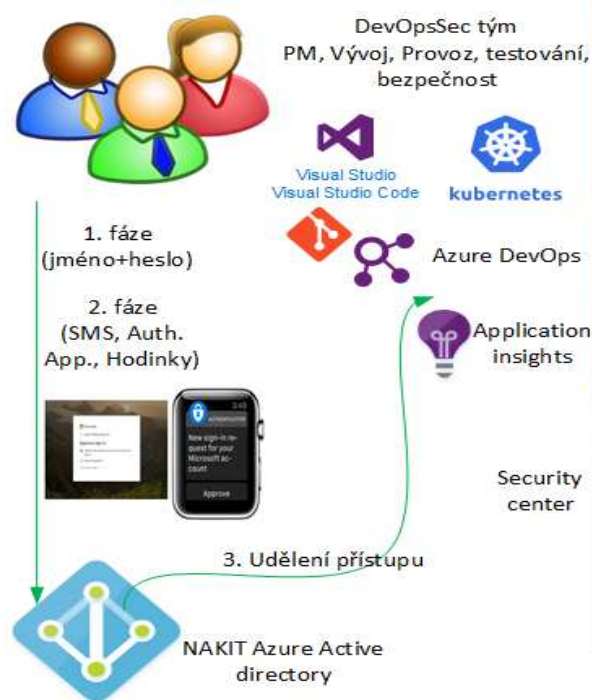
- Portál občana neobsahuje vlastní autentizační modul
 - spoléhá se na externí poskytovatele identit (Národní bod pro identifikaci a autentizaci, Datové schránky)
- Faktorem znalosti je: Jméno + heslo (nebo PIN k eObčance)
- Faktorem vlastnictví je: mobilní telefon pro příjem SMS kódu (nebo eObčanka)
- Faktorem biometrie může být: SMS kód na mobilním telefonu je viditelný až po oskenování prstu nebo obličeje (po odemknutí telefonu)

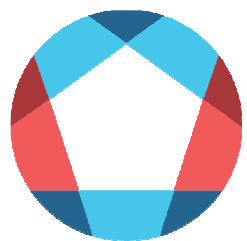
The screenshot shows the login interface of the 'identita.cz' portal. At the top, there are navigation tabs for different login methods: 'PŘIHLÁŠENÍ JMÉNEM A HESLEM', 'PŘIHLÁŠENÍ MOBILNÍM KLÍČEM', 'PŘIHLÁŠENÍ eOBČANKOU', and 'DALŠÍ ZPŮSOBY PŘIHLÁŠENÍ'. The 'PŘIHLÁŠENÍ POMOCÍ SMS' section is active, showing input fields for 'Uživatelské jméno', 'Heslo', and 'SMS kód'. A yellow 'PŘIHLÁŠIT SE' button is visible. To the right, there is explanatory text about the SMS login process. Below the main form, there are links for 'PŘIHLÁŠENÍ CERTIFIKÁTEM' and 'PŘIHLÁŠENÍ BEZPEČNOSTNÍM KÓDEM'. At the bottom, there are links for 'JSTE ZDE POPRVÉ?', 'NEMŮŽETE SE PŘIHLÁŠIT?', and 'NÁPOVĚDA'. A dark blue banner at the bottom of the screenshot contains the text: 'Kvalifikovaný poskytovatel žádá o vaši elektronickou identifikaci. Vyberte si prosím z následujících možností přihlášení:' followed by two options: 'eObčanka od 1. 7. 2018' and 'Jméno, heslo a SMS'. A small disclaimer is visible at the very bottom of the page.

Druhý faktor IT správců a vývojářů

V Portálu občana

- Celý tým dohromady včetně externích partnerů pracuje s 96 aktivy v komerčním cloudu (dohledové nástroje, úložiště zdrojových kódů, DB servery, aplikační clustery, Webové firewall, atd.)
- Použití druhého faktoru je povinné
- Identity správců a vývojářů podléhají bezpečnostní politice a proaktivnímu bezpečnostnímu dohledu
- Cílem pro rychlou efektivní práci: jedna identita na běžnou i privilegovanou činnost (např. just-in-time přístup, dvoufázová autorizace)





NAKIT

Národní agentura pro
komunikační a informační
technologie, s. p.

Děkuji

