

Nasazení vícefaktorového ověřování ve studijním systému

Návrh z 26. října 2019

Vypracoval: Ing. Luboš Pavlíček, Centrum informatiky

Obsah

| | |
|--|---|
| Cíle | 2 |
| Školení | 3 |
| Návod nastavení | 3 |
| Instalace aplikace na jednorázová hesla, doporučené aplikace | 3 |
| Spárování mobilní aplikace s účtem ve studijním systému | 3 |
| Přihlášení pomocí jednorázového hesla | 5 |
| Deaktivování přihlašování pomocí jednorázových hesel | 5 |
| Otázky/problémy | 5 |
| Nemám vhodný mobil, nechci používat soukromý mobil | 5 |
| Mám nový mobil, jak přenesu kód? | 5 |
| Přišel jsem do školy a zapomenu si mobil | 6 |
| Vybil se mi baterka na mobilu | 6 |
| Co je bezpečné zařízení? | 6 |
| Další metody vícefaktorové autentizace | 7 |

Cíle

Ve studijním systému je modul pro vícefaktorovou autentizaci, který využívá jednorázová hesla generovaná pomocí spárované aplikace na mobilním telefonu.

Navrhujeme povinné používání vícefaktorové autentizace u následujících skupin uživatelů:

- uživatelé se superprávem,
- uživatelé se zvýšenými právy, konkrétně:
 - o uživatelé s oprávněním měnit heslo jiným uživatelům,
 - o uživatelé kteří mohou nastavovat přístupový systém (vstupy na karty do místností/prostor) či spravovat identifikační karty,
 - o uživatelé, kteří mohou editovat údaje ve studijní evidenci mimo běžnou činnost vyučujícího. Např. zapisovat studenty do studia, upravovat rozvrh studentům, spravovat přihlášky ke studiu, uznávat předměty z předchozího studia či zahraničních pobytů, upravovat známky mimo období, editovat studijní plány.
 - o uživatelé s možností úprav ve správě osob – např. přiřazování externích rolí či úpravy adres,
 - o uživatelé s přístupem k finančním transakcím ve studijním systému,
 - o uživatelé s právem upravovat budovy či místnosti.

Ostatní zaměstnanci a studenti budou moci vícefaktorovou autentizaci využívat volitelně.

Pro jednotlivé skupiny uživatelů navrhujeme postupné zavedení vícefaktorové autentizaci:

| Skupina uživatelů | Počet osob | Volitelně od | Povinně od |
|-------------------------------------|------------|-------------------|--------------------|
| Uživatelé se superprávem | 33 | 24. října 2019 | 18. listopadu 2019 |
| Uživatelé se zvýšenými právy | 168 | 6. listopadu 2019 | 8. ledna 2020 |
| Zaměstnanci | ≈ 1 600 | 8. ledna 2020 | - |
| Studenti | ≈ 20 000 | 17. února 2020 | - |

Uživatel na začátku spáruje mobilní aplikaci pro jednorázová hesla se svým účtem ve studijním systému. Poté při přihlašování zadá uživatelské jméno a heslo a ve druhém kroku opíše proměnlivý ověřovací kód (jednorázové heslo) z mobilní aplikace. Pokud uživatel označí zařízení jako bezpečné, tak z něho následujících 30 dní nemusí zadávat ověřovací kód (heslo k účtu musí zadávat stále).

Jednorázová hesla budou moci využívat i uživatelé bez mobilního telefonu, ale za výrazného omezení – budou se moci přihlásit pouze z jednoho konkrétního počítače.

Jednorázová hesla chrání účet ve studijním systému ve většině případů, kdy nějakým způsobem unikne heslo uživatele:

- útočník pozoruje klávesnici uživatele při zadávání hesla,
- útočník z uživatele vyláká heslo pomocí podvodného e-mailu či podvodných webových stránek,
- uživatel používá stejné heslo na jiném serveru a z něho jeho heslo unikne,
- útočník odchytí komunikaci mezi počítačem a serverem a z ní získá heslo uživatele (útok Man-in-the-Middle),
- útočník na veřejně dostupném počítači nainstaluje keylogger.

Cenou za toto zvýšení bezpečnosti je mírné zvýšení nepohodlí při přihlašování do studijního systému.

Školení

V následující tabulce jsou termíny školení na Žižkově na používání vícefaktorové autentizace:

| Datum a čas | Čas | Místnost | Cílová skupina |
|-------------------------|---------------|----------|---|
| 6. listopadu 2019 (st) | 14:30 – 15:00 | SB 204 | uživatelé se superprávem |
| 14. listopadu 2019 (čt) | 09:15 – 09:45 | SB 108 | uživatelé se superprávem, pracovníci CI |
| 29. listopadu 2019 (pá) | 09:15 – 10:00 | SB 107 | uživatelé s vyššími právy |
| 19. prosince 2019 (čt) | 12:45 – 14:30 | SB 202 | uživatelé s vyššími právy |
| 7. ledna 2020 (st) | 09:00 – 09:45 | SB 109 | uživatelé s vyššími právy |

S vedoucím Centra informačních technologií Fakulty managementu domlouváme, zda školení zvládnou sami či by byla vhodná naše pomoc.

Návod nastavení

Instalace aplikace na jednorázová hesla, doporučené aplikace

Nejdříve si musíte nainstalovat na svůj mobil aplikaci pro jednorázová hesla. Následuje seznam doporučených bezplatných aplikací, které jsou i bez reklam.

Microsoft Authenticator (Android, iPhone, Windows Phone/Mobile) – jednoduchá aplikace, vedle časového jednorázového hesla podporuje několik metod vícefaktorové autentizace pro Office 365. Tajné heslo lze zálohovat (chráněno dalším heslem) na soukromý účet u společnosti Microsoft (Hotmail, Outlook.com). Na iPhone podporuje Apple Watch.

Google Authenticator (Android, iPhone) – jednoduchá aplikace, neumí zálohovat tajné heslo. Podporuje další metody autentizace pro služby firmy Google.

andOTP (Android) – jednoduchá aplikace s otevřeným kódem a minimem práv. Tajná hesla zálohuje do zašifrovaného souboru, který se následně může zálohovat např. přes DropBox či GDrive.

OTP Auth (iPhone) – jednoduchá aplikace pro iPhone, umí zálohovat do iCloud. Podpora Apple Watch.

Authy 2-Factor Authentication (Android, iPhone) – propracovaná a poměrně velká aplikace, která automaticky zálohuje kódy na síti, popř. je i synchronizuje mezi mobilními telefony. Musíte zadat telefonní číslo. Pro iPhone podpora Apple Watch.

Můžete použít i správce hesel pro mobil s podporou jednorázových hesel (např. 1Password).

Spárování mobilní aplikace s účtem ve studijním systému

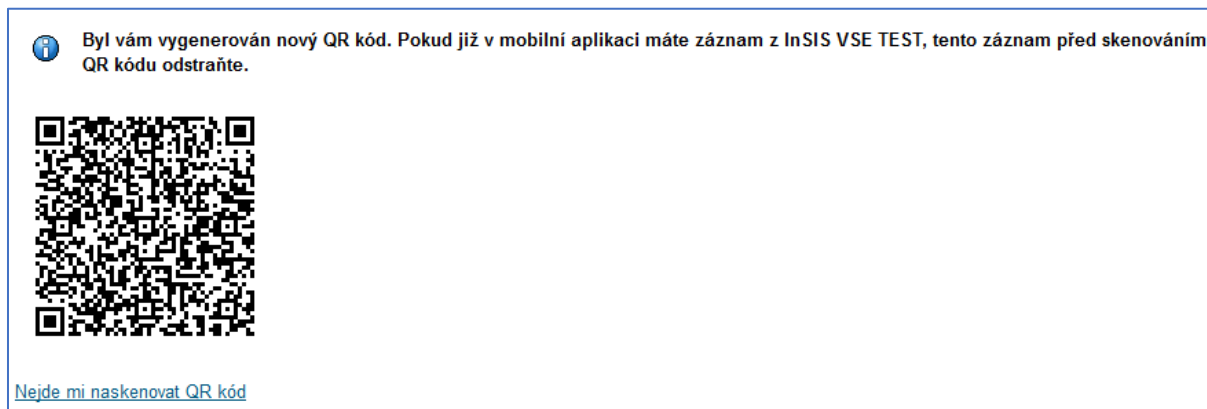
Po přihlášení v sekci „**Nastavení informačního systému**“ je volba „**Nastavení autentizace pomocí jednorázových hesel**“. Pozor – volba může být v této sekci na konci seznamu a tudíž skryta.



V dalším kroku potvrdíte, že máte nainstalovanou aplikaci pro jednorázová hesla:

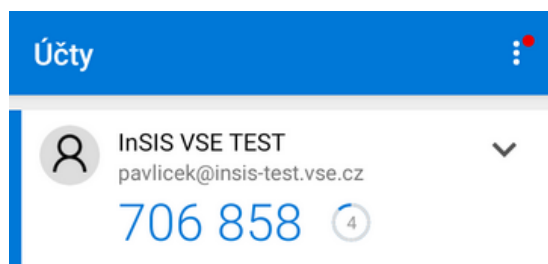
Mám nainstalovanou aplikaci, chci zahájit nastavení

Poté studijní systém vygeneruje tajné heslo (též „zárodek“ či seed) a zobrazí ho ve formě QR kódu (tajné heslo si můžete zobrazit v čitelnějším tvaru přes volbu „Nejde mi naskenovat QR kód“).



V tomto okamžiku si stránku vytiskněte. Bude to Vaše bezpečná záloha pro případ výměny mobilu apod.

V mobilu spusťte aplikaci pro jednorázová hesla, v aplikaci vyfoťte QR na vytištěné záloze. Do aplikace se Vám přidá záznam pro Váš účet v InSIS¹:



Každých 30 vteřin se generuje nové jednorázové heslo. Dolu na stránku opište dvě po sobě následující vygenerovaná čísla:

Dokončení spárování s mobilním zařízením

Pro dokončení spárování do polí **První kód** a **Druhý kód** zadejte dva po sobě jdoucí kódy, které vám aplikace postupně zobrazí. Tlačítkem **Dokončit spárování** dokončíte proces spárování (dojde k uložení do InSIS). Tlačítkem **Dokončit a aktivovat přihlašování** dokončíte spárování a rovnou aktivujete přihlašování pomocí jednorázových hesel.

První kód:
Druhý kód:

Dokončit spárování

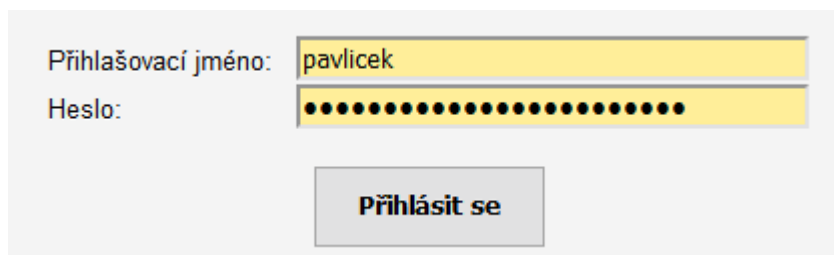
Dokončit a aktivovat přihlašování

Pomocí „**Dokončit a aktivovat přihlašování**“ spárujete mobilní aplikaci se svým účtem ve studijním systému a aktivujete používání jednorázových hesel.

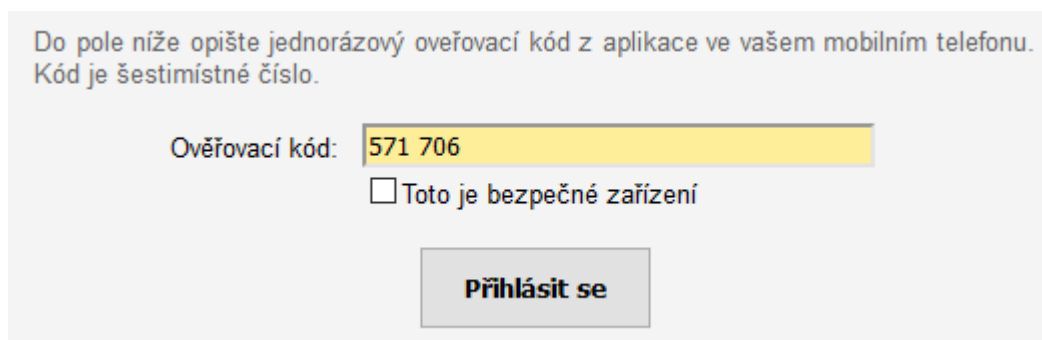
¹ Jak jste si všimli, tak návod vytvářím na insis-test. Nastavte jednorázová hesla na insis.vse.cz, v noci se nastavení přenesou na insis-test. Stejný kód poté budete používat na obou serverech.

Přihlášení pomocí jednorázového hesla

V prvním kroku zadáte své uživatelské jméno a heslo:



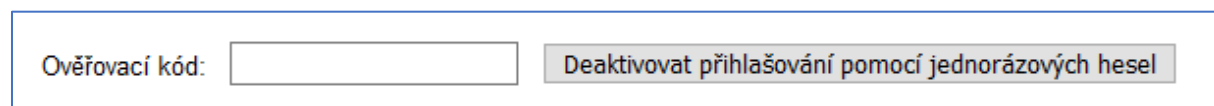
Po odeslání přihlašovacích údajů se objeví dotaz na jednorázové heslo (ověřovací kód):



Z mobilní aplikace opišete ověřovací kód. Pokud je zařízení bezpečné, tak zaškrtněte příslušnou volbu a pokračujte v přihlašování.

Deaktivování přihlašování pomocí jednorázových hesel

Pokud nespadáte do kategorie uživatelů s povinným používáním jednorázových hesel, tak můžete jednorázová hesla deaktivovat ve stejné aplikaci „Nastavení autentizace pomocí jednorázových hesel (OTP)“:



Před deaktivací musíte zadat ověřovací kód.

Otázky/problémy

Nemám vhodný mobil, nechci používat soukromý mobil

Na počítač Vám nainstalujeme aplikaci pro generování jednorázových ověřovacích kódů a spárujeme ji s Vaším účtem ve studijním systému. Má to ale nevýhodu – můžete se přihlašovat jen z tohoto počítače, popř. při přihlášení na jiném počítači se musíte být schopni podívat na ověřovací kód vygenerovaný na primárním počítači.

Mám nový mobil, jak přenesu kód?

Postup závisí na tom, jaký způsob zálohování tajného hesla jste zvolili.

Zálohujete přímo v aplikaci pro generování kódu. Na novém mobilu nainstalujte stejnou aplikaci a vyberte obnovu uložených tajných hesel.

Při spárování mobilu jste si vytiskli QR kód a máte ho k dispozici. Na novém mobilu si nainstalujte nějakou aplikaci pro generování jednorázových hesel a v ní vyfotíte QR kód.

V InSIS spárujete nový mobil se svým účtem. Týká se pouze uživatelů s volitelným použitím jednorázových hesel. Do InSIS se přihlásíte pomocí aplikace na starém mobilu. V aplikaci „Nastavení autentizace pomocí jednorázových hesel (OTP)“ deaktivujte dočasně použití jednorázových hesel a poté zrušíte spárování starého mobilu s účtem. Poté spárujete nový mobil se svým účtem.

Žádnou z předchozích metod nemůžete použít. Požádejte správce o zrušení párování původního mobilu. Při přihlášení spárujete nový mobil se svým účtem ve studijním systému. Přesný postup bude zveřejněn na webu CI.

Přišel jsem do školy a zapomenul si mobil

Pracujete na bezpečném zařízení. Pokud jste si svůj pracovní počítač v kanceláři označili jako bezpečné zařízení, tak je velká pravděpodobnost, že zrovna dnes nebudete muset zadávat ověřovací kód.

Vrátíte se domů pro mobil. Někdy je to nejjednodušší řešení.

Máte v kanceláři papír s vytisknutým QR kódem. Požádáte důvěryhodného kolegu, zda by ofotil Váš QR kód do své aplikace na generování jednorázových hesel a pomohl Vám s přihlášením. Po přihlášení by měl kolega smazat Váš záznam ze své aplikace.

Požádáte o dočasné vypnutí vícefaktorové autentizace. Použití jednorázových hesel lze dočasně vypnout, např. do konce pracovní doby. Je zde ale komplikace – pokud nám někdo zavolá, tak jak poznáme, že se volá konkrétní osoba a ne někdo, kdo se za něho vydává. Přesná pravidla pro ověření uživatele pro dočasné vypnutí jednorázových hesel budou zveřejněna na webu Centra informatiky.

Vybila se mi baterka na mobilu

Nejjednodušší je zapůjčit si nabíječku a mobil nabít. Pokud to není možné, tak použijte některé z řešení pro případ zapomenutého mobilu.

Co je bezpečné zařízení?

Bezpečné zařízení má následující vlastnosti:

- máte na něm svůj účet, který nesdílíte s jinými osobami,
- účet je chráněn heslem, PINem, otiskem prstu či obdobnou metodou,
- k zařízení je omezený přístup,

Podmínky splňují:

- počítače v zamykatelné kanceláři se školními Windows,
- notebooky, na kterých pracujete převážně sami a nosíte je obvykle sebou. Případní další uživatelé mají svůj účet.
- počítače doma, pokud na nich máte samostatný účet,
- mobilní telefon, který nesdílíte s jinými osobami,

Příklady zařízení, které nesplňují podmínky pro bezpečné zařízení:

- počítače na počítačových učebnách,
- cizí počítače, např. Vašich přátel,
- domácí počítač, na kterém sdílíte stejný účet s ostatními členy rodiny,
- mobilní telefon, který půjčujete ke hrám dětem či vnukům,

Informace o bezpečném zařízení se ukládá ve webovém prohlížeči. Pokud používáte více prohlížečů, tak na každém je potřeba samostatně potvrdit bezpečné zařízení. Pokud je prohlížeč v anonymním či soukromém režimu, tak se informace o bezpečném zařízení při jeho ukončení smaže.

Další metody vícefaktorové autentizace

Jednorázová hesla generovaná v mobilní aplikaci jsou jedním ze způsobů vícefaktorové autentizace. Existují další možnosti, se kterými se můžete setkat u jiných serverů (banky, Google, Facebook, ...). Následující seznam je seřazen dle obvyklého hodnocení bezpečnosti metody.

Vytištěný seznam jednorázově použitelných ověřovacích kódů. Tuto nouzovou metodu podporuje např. Google pro případy, kdy uživateli přestane fungovat mobilní telefon a nemá žádné zálohy.

Posílání SMS s ověřovacím kódem, který uživatel opíše při přihlašování. V aplikaci si uživatel zaregistruje telefonní číslo, při přihlašování musí být připojen k telekomunikační síti. Tato metoda již není příliš doporučována.

Jednorázové ověřovací kódy generované pomocí mobilní aplikace. Tuto metodu používá studijní systém.

Speciální aplikace na mobilu, která se spáruje přes internet se serverem. Při každém ověření musí být mobil připojen k internetu a uživatel na mobilu jen potvrdí, že se chce přihlásit (nemusí přepisovat žádný kód).

Hardwarová zařízení jako druhý faktor. Příkladem mohou být „kalkulačky“ k některým bankovním účtům, které generovali kód. Další variantou jsou jednoduché USB tokeny dle standardu UTF či FIDO2.

Čipové karty či USB tokeny s privátním klíčem pro ověření. V tomto případě uživatel nemusí obvykle zadávat heslo k účtu.