

**Návod pro použití bezpečnostního tokenu
SafeNet eToken PASS
s Portálem datových stránek**

Poslední verze ze dne 6. 6. 2011



OBSAH:

Aktivace tokenu eTokenPASS.....	4
Přihlášení k Portálu datových stránek.....	7

Tento návod popisuje proces aktivace (registrace) bezpečnostního tokenu **SafeNet eToken PASS** a zabezpečené přihlášení do Portálu datových schránek. Každý uživatel oprávněný k přístupu do datové schránky může zaregistrovat svůj bezpečnostní token (jeden pro každý uživatelský účet).



Předpoklady:

- Aktivovaná datová schránka
- Bezpečnostní token (bezpečnostní klíč) **SafeNet eToken PASS**
- Tajný klíč (dodaný s eTokenem PASS)

Aktivace tokenu eTokenPASS

Postup aktivace:

1. Přihlašte se do Vaší datové schránky (pověřená osoba nebo administrátor), klikněte na Nastavení. V sekci **Rozšířené zabezpečení přihlašování** klikněte na **Nastavit zabezpečení bezpečnostním klíčem**.

Rozšířené zabezpečení přihlašování

Pro vyšší ochranu Vaší datové schránky je možné přihlašování rozšířit o možnost zabezpečení pomocí SMS kódů nebo pomocí bezpečnostního klíče. [Nápověda](#)

Pozor! Rozšířené zabezpečení přihlašování lze používat pouze na portálu Datových schránek.
Po nastavení rozšířeného zabezpečení nebude možné používat externí aplikace využívající webových služeb Datových schránek, které jsou zpravidla dodávány třetími stranami. Příkladem takových externích aplikací jsou spisové služby nebo e-mailové aplikace (Outlook).

[NASTAVIT ZABEZPEČENÍ SMS KÓDEM](#) [NASTAVIT ZABEZPEČENÍ BEZPEČNOSTNÍM KLÍČEM](#)

2. Klikněte na tlačítko **Aktivovat**.

Nastavení zabezpečení bezpečnostním klíčem

Pro aktivaci tohoto způsobu zabezpečení přihlašování je nutné mít bezpečnostní klíč. [Nápověda](#)

Pozor! Bezúvodně generování kódů bezpečnostním klíčem může vést ke ztrátě synchronizace mezi bezpečnostním klíčem a systémem ISDS. Tento stav je chápán jako ztráta přihlašovacích údajů uživatele a je nutné zažádat o zneplatnění přístupových údajů a vydání nových přístupových údajů.

Pokud bezpečnostní klíč již máte, stiskněte **AKTIVOVAT** bezpečnostní klíč.

Jinak stiskněte **ZPĚT** na Nastavení.

[ZPĚT](#) [AKTIVOVAT](#)


3. V dalším formuláři je potřeba zadat:
 - **Heslo** k datové schránce.
 - **Tajný klíč**¹ získáte od dodavatele bezpečnostních tokenů **SafeNet eToken PASS**. Jedná se zpravidla o 48-znakový řetězec, který

¹ Tajný klíč představuje tzv. sdílené tajemství mezi tokenem a systémem ISDS. Uživatel by měl ve vlastním zájmu nosič obsahující Tajný klíč uložit na bezpečném místě a chránit jej před zneužitím. Současná znalost Tajného klíče a Hesla by potenciálnímu útočníkovi mohla umožnit neoprávněný přístup k datové schránce.

zajišťuje bezpečnost autentizace, a je nutné jej přenést bezchybně.

- **Formát klíče** ponechte **Hexadecimální**.
- Stiskněte tlačítko na bezpečnostním tokenu a vygenerované 6-ti místné heslo opište do pole **Kód z bezpečnostního klíče**.
- Počkejte cca 20 sekund až první heslo zmizí a stiskněte tlačítko na tokenu znovu. Toto vygenerované heslo přepište do pole **Druhý kód z bezpečnostního klíče**.
- Stiskněte **Registrovat**.

Pro dokončení aktivace zabezpečení přihlašování bezpečnostním klíčem zadejte znovu Vaše přihlašovací údaje.

Heslo: 

Tajný klíč:

Formát klíče:

Kód z bezpečnostního klíče:

Druhý kód z bezpečnostního klíče:

ZPĚT **REGISTROVAT**

4. Po úspěšné registraci se objeví potvrzovací okno **Zabezpečení přihlašování bezpečnostním klíčem bylo úspěšně aktivováno**.

V případě, že se registrace nepodaří, zobrazí se červeně příslušná chybová hláška.

- **Chyba přihlášení, znovu zadejte údaje** (chybné heslo do datové schránky)

- **Nepodařilo se dekodovat hexadecimální klíč** (chybně zadaný tajný klíč)
- **Nepodařilo se přihlásit s daným kódem. Buď byl špatně opsán, nebo daný token byl použit vícekrát, než je povoleno** (chybně zadaný 6-ti místný kód)

Důležitá poznámka: V případě, že uživatel omylem vygeneruje bezpečnostním tokenem kódy, které pak nepoužije k přihlášení, bude ještě 48. kód v řadě od posledního úspěšného přihlášení považován za platný a uživateli umožní přihlášení k datové schránce. Překročení uvedeného limitu má stejné důsledky jako ztráta přihlašovacích údajů a je nutné zažádat o zneplatnění přístupových údajů a vydání nových přístupových údajů. Uživatel by měl ve vlastním zájmu zajistit, aby přihlašovací kódy nebyly zbytečně generovány neznalou osobou, dětmi apod.

5. Jestliže je bezpečnostní token registrován pro daného uživatele, musí se tento uživatel nadále přihlašovat do ISDS pouze tímto způsobem. V případě potřeby lze v rámci **Nastavení** datové schránky **Zrušit zabezpečení bezpečnostním klíčem**.

Přihlášení k Portálu datových stránek

Postup autentizace:

1. Zadejte do prohlížeče adresu portálu datových schránek. Vyberte **Přihlášení bezpečnostním klíčem.**

Přihlášení

Uživatelské jméno (ID osoby):

Heslo:
 

Kód

- [Nemůžete se přihlásit?](#)
- [Nápověda](#)

PŘIHLÁSIT

2. Zadejte uživatelské jméno, heslo k datové schránce a 6-ti místný kód, který vygenerujete stisknutím tlačítka na bezpečnostním tokenu.

Pokud je chybně zadané heslo nebo kód z tokenu, objeví se hláška **Chyba přihlášení, znovu zadejte údaje.**

Po zadání správných údajů budete přesměrováni do Vaší datové schránky.

© 2011 ASKON INTERNATIONAL s.r.o., value added reseller společnosti SafeNet, Inc. pro Českou republiku a Slovenskou republiku. Všechna práva vyhrazena.

Tato dokumentace je určena pro zákazníky užívající produkty distribuované společností ASKON INTERNATIONAL s.r.o.

Další šíření této dokumentace nebo jejích částí je možné jen s výslovným písemným souhlasem ASKON INTERNATIONAL s.r.o.

V tomto materiálu uvedené názvy produktů jsou ochranné známky jejich vlastníků.