

## Výhody

### Výhody pro administrátory

#### SafeNet Rapid Deploy Technology™

automatizuje management pravidel a pověření PC stanic pomocí jediného Management Centra.

SSO zjednodušuje konfiguraci a nasazení smart karet a tokenů zajišťujících přístup ke všem prostředkům společnosti.

#### Další výhody zahrnují:

- Aplikace a infrastruktura zůstávají nedotčené
- Silná autentizace a bezpečný email založené na PKI
- Klientský SW, který propaguje pravidla, je transparentně posouván na každou pracovní stanici
- Automatická aktualizace SW a pověřovacích dokladů
- Automatická podpora silných hesel a přístupových pravidel
- Podpora Microsoft a Citrix terminal services
- Bezpečnost organizace je zvýšena pomocí zabezpečeného SSO do Windows, aplikací společnosti, vzdáleného přístupu prostřednictvím VPN/RAS, aplikací Microsoftu a kontrolních systémů fyzického přístupu

#### Výhody pro uživatele

Díky jednotnému PIN, který odemkává přístup k pověřením uloženým na smart kartě anebo tokenu a automatizovanému přístupu ke všem prostředkům společnosti, odpadá pro uživatele nutnost pamatovat si velké množství hesel.

Díky tomu se výrazně zvyšuje produktivita práce.

#### Výhody pro společnost

Rychlá návratnost investice do SSO pro větší i střední organizace spočívá zejména ve:

- Výrazném snížení administrativy, které umožňuje IT administrátorům koncentrovat se na další důležité úkoly
- Zjednodušení přístupu koncových uživatelů a zvýšení jejich produktivity
- Silnější bezpečnosti a přehledu všech přístupů

## SafeNet Borderless Security

# SingleSign-On

### Silná autentizace a Single Sign-On

SafeNet Borderless Security SSO (Single Sign-On) poskytuje zásadní výhody. Snadnou integraci. Velmi rychlé nasazení.

Jednoduchou správu a provoz. Vysokou investiční návratnost.

Nejsilnější možnou bezpečnost přístupu. To vše z jednoho místa.

### SafeNet Borderless Security Single Sign-On Administrative Management Center

Single Sign-On Administrativní Management Centrum (AMC) je robustní řešení správy identifikace, které zjednodušuje správu a konfiguraci smart karet/tokenů a také správu logického a fyzického přístupu v rámci organizace. Administrátor používá Single Sign-On AMC k:

- Natavení kontroly pravidel pro hesla pro korporátní aplikace.
- Konfiguraci pravidel pro smart karty a tokeny a výběr, jak budou karty/tokeny používány.
- Konfiguraci a nasazení klienta pravidel SSO na všech uživatelských stanicích.
- Automatické aktualizaci pokaždé, kdy je k dispozici upgrade softwaru.
- Nastavení bezpečného zálohování a znovuoobnovení pověřovacích dokladů.

### Rapid Deploy Technology™

Skutečná síla, která pohání SingleSignOn AMC spočívá v implementaci Rapid Deploy Technology™ (Technologie rychlého nasazení). Pomocí této technologie se Single Sign-On učí stávající obchodní aplikace a přihlašovací postupy. Učí „Client Policy“ (klient pravidel), aby používal smart karty a tokeny k automatickému bezpečnému přístupu, aniž by byly vyžadovány jakékoliv změny v aplikacích nebo infrastruktuře. Rapid Deploy Technology™ podporuje „push“ instalaci „Client Policy“ z centrálního úložiště na PC stanice uživatelů. Po instalaci Rapid Deploy Technology™ umožňuje automatické aktualizace softwaru a pověřovacích dokladů.



### Automated Desktop Management

Pomocí Single Sign-On AMC administrátoři mohou definovat, sestavovat a nasazovat konsistentní prostředí pro PC stanice, které jsou vybaveny smart kartami/tokeny, které umožňují uživatelům přistupovat ke všem prostředkům společnosti. Klientský software je aktualizován automaticky bez zásahu uživatele tak, jak je definováno administrátorem.

### Automated Credential Management

SafeNet Borderless Security Single Sign-On umožňuje administrátorům kompletní kontrolu nad definováním, prosazením a povolením toho, jaký přístup k aplikacím a dalším zdrojům dostane každý uživatel pomocí hesel uložených na uživatelově smart kartě/tokenu. Administrátoři si nyní mohou zajistit používání silných hesel (automaticky generovaných pomocí Single Sign-On).



Hesla jsou měněna tak, jak je vyžadováno aplikacemi společnosti a po té jsou zaslána na kartu uživatele. Toto zaslání („push“) je prováděno na pozadí v okamžiku, kdy se uživatel přihlašuje do systému. A protože uživatel toto heslo nezná (pouze si musí pamatovat PIN ke své kartě), bezpečnost systému se tímto způsobem výrazně zvyšuje. Kromě definování přístupu k aplikacím mohou administrátoři pomocí AMC definovat pravidla pro samotné karty/tokeny (minimální délka PIN, maximální počet chybných pokusů při zadávání PIN, atd.). Toto dohromady dovoluje administrátorům nastavení konsistentní bezpečnosti z jednoho místa pro celou organizaci.

### SafeNet Borderless Security Single Sign-on Policy Client

Single Sign-On Policy Client (klient pravidel) běží na PC stanici uživatele a spojuje tak uživatele a všechny prostředky společnosti a prosazuje pravidla pro smart karty/tokeny pro řízení přístupu. Poskytuje zejména:

- Kontrolu toho, jak je smart karta/token používána a pro jaké aplikace.
- Automatizuje Single Sign-On k aplikacím. Vždy, když se uživatel přihlásí, „Policy Client“ automaticky předloží pověření všem aplikacím bez dalšího zásahu uživatele.
- Software „push“ instalaci a aktualizaci bez zásahu uživatele, která probíhá rychle a jednoduše.
- Zabudované přihlašovací aplikace pro smart karty/tokeny, včetně přihlašování do Windows® (pomocí certifikátu anebo username/hesla) a přihlašování pomocí biometrie.

### Smart karta (USB token)/Čtečka

Pro uživatele je přístup pomocí SafeNet Borderless Security Single Sign-On zjednodušen na pouhé užívání smart karty nebo tokenu. BSec SSO ukládá všechna hesla a pověření, což může začínat kontrolou vstupu do budovy a končit přihlašování do sítě a zabezpečeným přístupem chráněných webových aplikací a jiných aplikací. Single Sign-On nabízí zejména:

- **Pohodlí.** Pokaždé, když se uživatel přihlašuje, vsune svou kartu a zadá PIN. Po té má okamžitě bezpečný přístup ke svému PC, k síti, VPN, e-mailu, chráněným webovým stránkám a obchodním aplikacím.
- **Jednoduchost.** Mohou být využívána komplexní hesla, která jsou uložena na smart kartě/tokenu, takže si je uživatel nemusí pamatovat. Tato hesla jsou instalována na uživatelskou kartu pomocí Single Sign-ON AMC.
- **Flexibilita.** Uživatel může na své kartě ukládat i svá osobní hesla k přístupu do aplikací, která nejsou chráněná organizací. Pokud si uživatel ukládá na kartu svá osobní hesla, je tím více motivován k tomu, aby kartu ochraňoval před zničením nebo ztrátou. Single Sign-On propaguje důvěru a harmonii.

### Technická specifikace

#### Požadavky na HW pro administrátory

- Procesor Pentium a vyšší
- Minimálně 16 MB RAM (doporučeno 32MB)

#### Požadavky na SW pro administrátory

- Windows 2000 Server, Windows 2000 Professional, Windows 2003 Server nebo Windows XP Professional
- Active Directory (Pokud se „Policy Client“ implementuje přes Group Policy nebo SMS)
- Síťové připojení ke stanicím koncových uživatelů (Pokud se „Policy Client“ implementuje přes Group Policy nebo SMS)
- RRAS (pro vzdálený přístup)
- Microsoft CA (pro použití s PKI)

#### Požadavky na HW uživatele

- Procesor Pentium a vyšší
- Minimálně 16 MB RAM (doporučeno 32MB)
- PCMCIA slot nebo USB port pro USB čtečku smart karty anebo tokenu

#### Požadavky na SW uživatele

- Procesor Pentium a vyšší
- Minimálně 16 MB RAM (doporučeno 32 MB)

#### Požadavky na smart karty & tokeny

- SafeNet smart karta model 330(m), 400(m)
- SafeNet USB token iKey 2032, iKey 4000
- PS/SC kompatibilní čtečka smart karet

