

IRONKEY PERSONAL

UŽIVATELSKÁ PŘÍRUČKA

MODELY S200, S100, D200



Obsah

Co je IronKey?	3
Seznamte se s IronKey	3
Hlavní funkce.....	3
Schémata zařízení	5
<i>Technické a bezpečnostní informace</i>	6
<i>Bezpečnostní služby IronKey</i>	7
Jak to funguje?	9
Rekapitulace produktu.....	9
<i>Inicializace a aktivace vašeho IronKey ve Windows</i>	9
<i>Použití IronKey Unlocker ve Windows</i>	11
<i>Použití IronKey Control Panel (Windows a Mac)</i>	12
<i>Použití virtuální klávesnice IronKey (pouze Windows)</i>	15
<i>Použití Firefox a Secure Sessions Service (Windows)</i>	16
<i>Použití IronKey Identity Manager (pouze Windows)</i>	17
<i>Použití Secure Backup Software (pouze Windows)</i>	19
<i>Import digitálního certifikátu na IronKey (pouze Windows)</i>	20
<i>Použití my.ironkey.com (Windows a Mac)</i>	22
<i>Použití IronKey v režimu čtení (Windows a Mac)</i>	24
Co bude dál?	25
Kde mohu získat další informace?	25
Kdo je IronKey tým?	25

Děkujeme Vám za Váš zájem o IronKey. Společnost IronKey se zavázala k vytváření a rozvoji nejlepších bezpečnostních technologií, vytvářet zařízení jednoduché k použití, cenově dostupné a dostupné pro každého. Roky výzkumu a miliony dolarů na rozvoj Vám přináší tuto technologii v podobě Vášeho IronKey.

Pro rychlý přehled produktů si můžete prohlédnout naše on-line demo na adrese <https://www.ironkey.com/demo>.

Budeme velice rádi za zpětnou vazbu a vážíme si Vašich připomínek, návrhů a zkušeností s IronKey.

- ◆ Standardní připomínky
 - feedback@ironkey.com
- ◆ Anonymní připomínky
 - <https://www.ironkey.com/feedback>
- ◆ IronKey Online
 - <https://my.ironkey.com>
 - <https://forum.ironkey.com>
 - <https://support.ironkey.com>
 - <https://store.ironkey.com>
- ◆ Dotazy na funkce
 - featurerequest@ironkey.com
 - <https://store.ironkey.com>
- ◆ Uživatelské fórum
 - <https://forum.ironkey.com>
- ◆ Podpora IronKey
 - <https://support.ironkey.com>
 - <https://support.ironkey.com>

CO JE IRONKEY?

SEZNAMTE SE S IRONKEY

Bezpečný flash disk IronKey Personal byl navržený pro ještě větší soukromí pomocí dnešních nejvyspělejších bezpečnostních technologií. Pokud váš IronKey ztratíte nebo Vám bude ukraden, zůstanou Vaše data chráněna. Můžou být dokonce obnovena na nový IronKey ze šifrované zálohy. Zatímco základní bezpečnostní technologie jsou složité, IronKey je jednoduchý na používání a stačí si pamatovat heslo k odemknutí.



HLAVNÍ FUNKCE

Hardwarově šifrovaný flash disk

Na Váš IronKey je možné bezpečně uložit 1, 2, 4, 8 nebo 16 GB v podobě dokumentů, aplikací, souborů a dalších dat. IronKey Cryptochip uvnitř chrání Vaše data na stejné úrovni jako vysoce utajované vládní informace a nemůže být ani zakázán ani omylem vypnut.

Autodestrukční funkce

V případě pokusu o násilnou manipulaci nebo napadení hackerem zajistí IronKey Cryptochip autodestrukci. Podobně, po 10 ti po sobě jdoucích nesprávných pokusech o zadání hesla je opět IronKey zničen.

Automatická ochrana proti Malware

IronKey Vás ochrání před mnoha nejnovějšími hrozbami malware napadajících USB flash disky. IronKey detekuje a zabrání autospuštění neschválených programů, a může být odemknut i v režimu Read-Only.

Multiplatformní přenosný přístup k datům

Ironkey Unlocker vám umožní přístup k šifrovaným souborům na platformách Windows 2000, XP, Vista, Mac OS X a Linuxu.

Jednoduchá Správa zařízení

Součástí IronKey je Control Panel pro centrální spouštění aplikací, editaci vašich nastavení a bezpečné zamykání IronKey.

Bezpečná Obnova dat

Bezpečně zálohovat data na Vašem IronKey můžete pomocí zálohovacího software. To Vám umožní obnovit data na nový IronKey v případě, že IronKey ztratíte. Můžete také synchronizovat data mezi více IronKey.

Technologie bezpečného prohlížení

Se službou Secure Sessions Service můžete bezpečně a v soukromí surfovat na webu ve všech sítích, dokonce i přes nezabezpečené bezdrátové hotspots, a to pomocí webového prohlížeče Mozilla Firefox, který je součástí IronKey.

Management hesel

Pomocí Identity Manager můžete bezpečně ukládat a zálohovat všechna Vaše on-line hesla. Umožňuje také automatické přihlášení do online účtu, které brání keyloggingu spyware a phishingu.

Online účet my.ironkey.com

Můžete spravovat všechny Vaše IronKey on-line na adrese my.ironkey.com, zabezpečené webové stránce, která vyžaduje dvoufaktorovou autentizaci přístupu. Zde můžete obnovit zapomenutá hesla, nastavit služby zařízení a další.

Online Security Vault

Pokud Váš IronKey ztratíte nebo Vám ho ukradnou, můžete snadno obnovit hesla z šifrované online zálohy na Váš nový IronKey.



Vodotěsný a odolný proti vlhkosti

IronKey je navržen tak, aby odolal extrémním podmínkám. Má robustní pouzdro s epoxidovou sloučeninou, která zajišťuje nejen odolnost proti vlhkosti, ale i vodotěsnost dle armádní specifikace (MIL-STD-810F).

Přípůsobeno pro osoby se zdravotním postižením

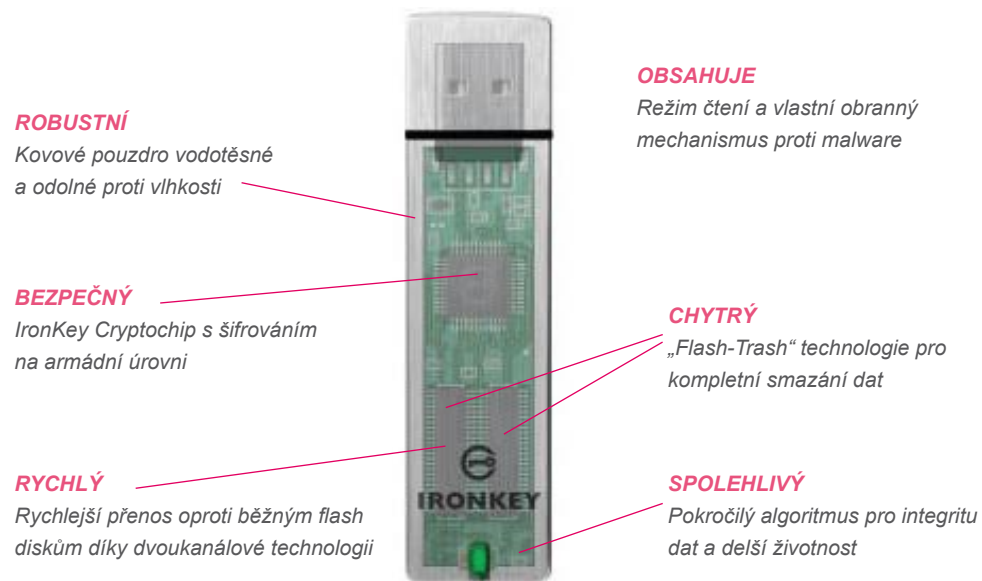
Uživatelé se zdravotním postižením mají podporu klávesnicové navigace a čtení z obrazovky. IronKey Control Panel je navržen v souladu s § 508 (tento zákon byl přijat k odstranění bariér v oblasti IT, poskytnout nové příležitosti pro lidi se zdravotním postižením a podporovat rozvoj technologií).

SCHEMATA ZAŘÍZENÍ

IronKey byl navržen od základu s ohledem na bezpečnost. Kombinace pokročilých bezpečnostních technologií slouží k zajištění maximální ochrany Vašich dat. IronKey je navržen tak, aby byl fyzicky zabezpečený a zabránilo se útokům a manipulaci již na HW úrovni, byl robustní a měl dlouhou životnost. Můžete si být jisti, že když používáte IronKey, jsou Vaše data v bezpečí.



IronKey Cryptochip je odolný proti fyzickým útokům. Je nemožné fyzicky manipulovat s chráněnými daty nebo obnovit počítačové pokusy zadání hesla. Pokud zjistí Cryptochip útok hackera, zničí šifrovací klíče a uložené šifrované soubory budou nepřístupné.



TECHNICKÉ A BEZPEČNOSTNÍ INFORMACE

Společnost IronKey je otevřená v otázce bezpečnostních architektur a technologií, které používá při navrhování a výrobě IronKey zařízení a on-line služeb. Používá osvědčené kryptografické algoritmy, vyvíjí modely hrozeb a provádí bezpečnostní analýzy (interní a třetích stran) svých systémů od návrhu přes vývoj a nasazení.

Bezpečnost IronKey

Klíče šifrovacích dat

- ◆ AES klíče generované pomocí Generátoru náhodných čísel
- ◆ AES klíče generované uživatelem v době inicializace, šifrované
- ◆ AES klíče nikdy neopustí hardware and nejsou uchovávány v paměti NAND

Sebedestrukční ochrana dat

- ◆ Bezpečná část je připojena až po kontrole zadaného hesla v hardware
- ◆ Počítadlo počtu zadaných hesel implementované v hardware odolném proti vlhkosti
- ◆ Jakmile je překročen limit pro nesprávná hesla, jsou všechna data smazána

Dodatečné bezpečnostní prvky

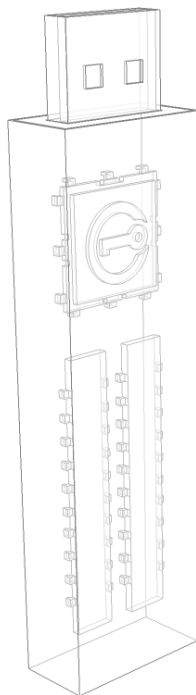
- ◆ Šifrovací kanál USB slouží jako ochrana komunikace zařízení
- ◆ Firmware a software lze bezpečně aktualizovat přes internet
- ◆ Aktualizace se ověřují pomocí digitálních podpisů v hardware

Fyzicky bezpečné

- ◆ Pevné, robustní pouzdro
- ◆ Šifrovací klíče uložené v IronKey Cryptochip, odolném proti vlhkosti
- ◆ Všechny čipy jsou chráněny zalitím epoxidovou sloučeninou
- ◆ Převyšuje armádní normy pro vodotěsnost (MIL-STD-810F)

Ochrana hesla

Heslo zařízení je zakódované pomocí SHA-256 před přenosem do IronKey prostřednictvím zabezpečeného a unikátního kanálu USB. Je uloženo v extrémně nepřístupném místě v chráněném hardware. Heslo je ověřeno v hardware (zde není funkce „Získat heslo“), a pouze po ověření hesla je pomocí šifrování AES klíč odemknut. Čítač nesprávně zadaných hesel je umístěn také v hardware, aby se zabránilo zpětným útokům na paměť. Zadáním nesprávného hesla (10 pokusů) se iniciuje patent „flash-trash“ sekvence, která běží v hardware, a které způsobí smazání dat. Toto zajistí vyšší ochranu pro Vaše data než při SW zabezpečení.



Ochrana Identity Manager

IronKey Identity Manager a *my.ironkey.com* mohou pracovat společně a dávají Vám možnost zálohování hesla do online bezpečnostního trezoru na *my.ironkey.com*. Nejprve musíte odemknout IronKey zařízení, které vyžaduje dvoufaktorovou autentizaci. Vaše hesla jsou bezpečně uložena ve skryté oblasti uvnitř přístroje s hardware šifrováním (ne v souborovém systému), přičemž nejdříve jsou místně šifrována 256 bitovým AES a pomocí náhodně vygenerovanými klíči šifrována pomocí SHA-256. Všechna tato data se pak dvojnásobně šifrují pomocí 128 nebo 256 bitového AES hardwarového šifrování.

Při zálohování vašich hesel online probíhá složitá kryptografie veřejného klíče pomocí RSA 2048 bitového klíče. Po úspěšném ověření je šifrované heslo bezpečně přenášeno přes SSL do Vašeho online bezpečnostního trezoru.

Bezpečnostní služby IronKey

Bezpečné zařízení

IronKey provozuje své online služby ve vyspělém datovém centru třetí strany. Fyzický přístup k IronKey systémům vyžaduje více úrovní autentizace, včetně biometrické čtečky geometrie ruky, „man trap“ vstupu, vládou vydaným ověřováním totožnosti s fotografií a individuálním pověřením k přístupu. Každé datové centrum je vybaveno mnoha bezpečnostními kamerami, detektory pohybu a důmyslnými poplašnými systémy. Infrastruktura IronKey se nachází v zabezpečené „cele“. Celý objekt je sledován bezpečnostním personálem v režimu 24×7.

Bezpečné prostředí a politiky

Logický přístup k prostředí IronKey je řízen několika vrstvami síťových technologií, jako jsou firewally, routery, systémy prevence narušení a zabezpečené aplikace. Pro další ochranu IronKey dělí své online služby a záložní aplikace do různých segmentů sítě s nezávislými bezpečnostními pravidly a politikami.

Bezpečná komunikace a data v klidu

Když uživatelé IronKey přistupují na webové stránky a služby, jsou veškeré informace přenášeny přes šifrovaný kanál. Toto je provedeno přes SSL a s využitím VeriSign Secure Site a VeriSign Secure Site Pro Certificates. Pro zajištění dodatečné bezpečnosti svých služeb je IronKey plně kvalifikovaný a používá rozšířené ověřování SSL. Aplikace IronKey šifrují veškerá citlivá data před přenosem v rámci sítě IronKey a ukládají je do databází.

Bezpečné sekce: TOR dělá rychlejší a bezpečnější

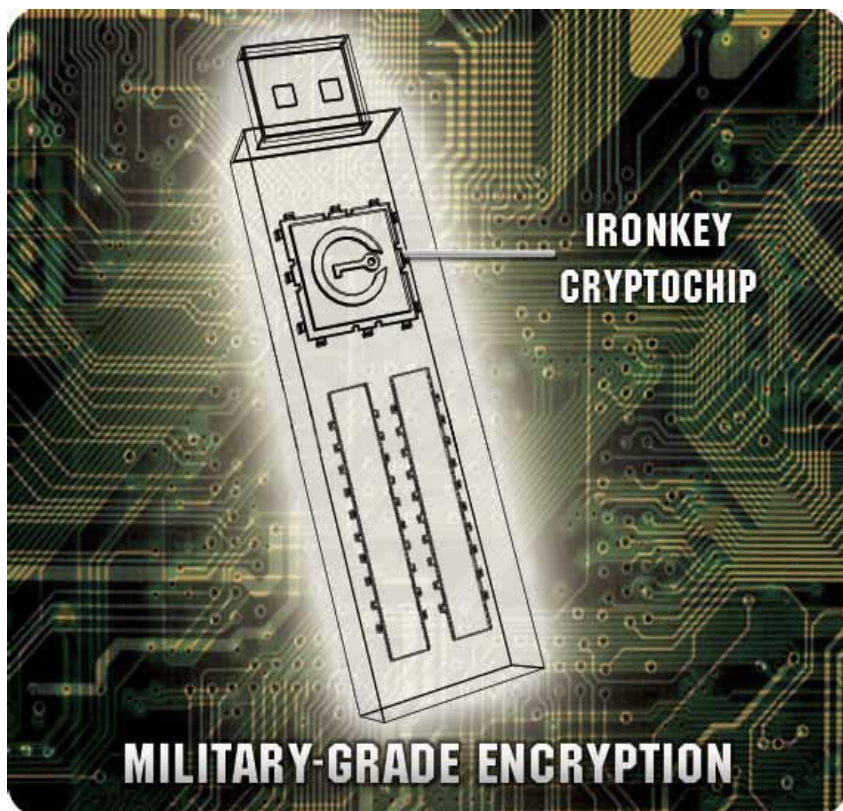
IronKey udržuje bezpečnou, soukromou TOR síť s vlastními, vysoce výkonnými servery (oddělenou od veřejné sítě TOR). To zlepšuje celkovou bezpečnost nejméně dvěma způsoby:

Protože IronKey řídí „exit-node“ ve Vašem šifrovaném okruhu TOR, může zajistit, že nikdo nevpustí do on-line komunikace nechtěný nebo škodlivý obsah, jako jsou reklamy nebo spyware. V jiné veřejně běžící síti si nemůžete být jisti takovouto úrovní zabezpečení.

IronKey může také zajistit, aby žádné exit-node nebylo přeměřované na Vaši web tím, že poskytuje dodatečnou DNS ochranu. Tato anti-pharming opatření můžou také pomoci zmírnit phishingové útoky a jiné online hrozby.

Více technických informací najdete na <https://learn.ironkey.com>.

Pozn.: TOR (The Onion Router) - systém pro vysoce anonymní a šifrovaný přístup k Internetu



JAK TO FUNGUJE?

REKAPITULACE PRODUKTU

Váš IronKey Personal bezpečný flash disk obsahuje následující součásti


- ◆ IronKey Unlocker (Windows, Mac a Linux)
- ◆ IronKey Control Panel (Windows a Mac)
- ◆ IronKey virtuální klávesnice (pouze Windows)
- ◆ Mozilla Firefox a IronKey Secure Sessions Service (pouze Windows)
- ◆ IronKey Identity Manager (pouze Windows)
- ◆ IronKey Secure Backup (pouze Windows)
- ◆ my.ironkey.com (Windows a Mac)


Standardní požadavky

- ◆ Windows 2000 (SP4), XP (SP2+), Vista a 7 Mac OS X (10.4+) nebo Linux (2.6+)
- ◆ USB 2.0 port pro vysokorychlostní přenos dat
- ◆ Emailovou adresu a připojení k internetu pro využití online služeb

INICIALIZACE A AKTIVACE VAŠEHO IRONKEY VE WINDOWS

Když otevřete krabičku, najdete IronKey bezpečný flash disk a Quick Start Guide. Níže je uveden stručný popis standardního způsobu nastavení IronKey:

Krok	Popis
1	<p>Zapojte IronKey do počítače se systémem Windows do USB portu.</p> <p>Váš IronKey může být inicializován ve Windows 2000, XP a Vista. Také může být nastaven na Mac nebo Linuxu.</p> <p>Chcete-li využít plnou rychlost IronKey, zapojte jej do USB 2.0 portu.</p>
2	<p>Objeví se obrazovka "Initialize Your IronKey".</p> <p>IronKey se spustí automaticky jako virtuální CD-ROM.</p> <p>Tato obrazovka se nemusí zobrazit, pokud váš počítač nepovoluje automatické spuštění zařízení. Můžete ji spustit ručně dvojitým kliknutím na IronKey Unlocker ve složce „My computer“ a poklepejte na „IronKey.exe“.</p>
3	<p>Vytvořte heslo zařízení a přezdívku pro Váš IronKey.</p>  <p>Protože můžete mít více IronKey spojených s jedním účtem IronKey, přezdívka Vám pomůže při orientaci mezi různými zařízeními IronKey.</p> <p>Vaše heslo rozlišuje velká a malá písmena a musí mít alespoň 4 znaky. Hrozba útoků hrubou silou je odstraněna sebedestrukční funkcí IronKey.</p>

Krok	Popis
4	<p>Zálohujte heslo do Vašeho online IronKey účtu.</p> <p><input checked="" type="checkbox"/> Backup my password inline in case I forget it</p>
5	<p>Potvrdíte souhlas s Licence Agreement.</p> <p>Objeví se IronKey License Agreement pro konečného uživatele. Lze ji také nalézt na internetové adrese https://www.ironkey.com/terms</p>
6	<p>IronKey se inicializuje.</p>  <p>Během tohoto procesu se generují šifrovací klíče AES, vytvoří se souborový systém pro zabezpečený obsah a kopie bezpečných aplikací a soubory do zabezpečeného obsahu.</p>
7	<p>Aktivujte Váš <i>my.ironkey.com</i> účet.</p> <p><i>my.ironkey.com</i> je zabezpečená stránka, kde můžete spravovat svůj účet IronKey a zařízení. Přístup na <i>my.ironkey.com</i> vyžaduje dvoufaktorovou autentizaci (Váš IronKey a heslo).</p>
8	<p>Postupujte dle instrukcí na obrazovce při nastavení účtu <i>my.ironkey.com</i></p> <p>Vytvořte jedinečné uživatelské jméno a heslo, potvrďte svou e-mailovou adresu pro externí autentizaci a odpovězte na tajné otázky pro doplňující ověření.</p> <p>Vyberte Secret Image, který uvidíte po přihlášení, stejně jako Secret Phrase, která se používá jako opatření proti phishingu při emailové komunikaci s Vámi.</p>
9	<p>Reagujte na potvrzovací e-mail zadáním aktivačního kódu na webových stránkách.</p> <p>IronKey musí ověřit vaši e-mailovou adresu, protože ji používá na obnovení hesla k vašemu účtu, odemyká Váš <i>my.ironkey.com</i> účet a informuje Vás o výstrahách zabezpečení účtu.</p>


Nyní je Váš IronKey připraven chránit Vaše data, identitu a online soukromí.

POUŽITÍ IRONKEY UNLOCKER VE WINDOWS

IronKey Unlocker umožňuje bezpečně přistupovat k souborům na mnoha operačních systémech.

Vyzve Vás k zadání hesla, bezpečně ho ověří a pak jej připojí na zabezpečený svazek, kde jsou všechny soubory uloženy.

Zde je postup, jak odemknout IronKey ve Windows 2000 (SP4), XP (SP2+), Vista a Windows 7:

Krok	Popis
1	<p>Zapojte IronKey a odemkněte Vaším heslem.</p>  <p>Když zapojíte IronKey, objeví se okno „Unlock Your IronKey“.</p> <ul style="list-style-type: none"> • Pokud se tato obrazovka nezobrazí, můžete ji spustit ručně dvojitým kliknutím na IronKey Unlocker ve složce „My Computer“ a kliknutím na „IronKey.exe“ soubor. • Pokud je zadáno heslo správně (což je ověřeno v hardware) připojí se zabezpečený svazek se všemi vašimi aplikacemi a soubory. • Při zadání nesprávného hesla 10x po sobě dojde k trvalému vymazání všech dat. Po každých třech pokusech musíte IronKey odpojit a znovu připojit.
2	<p>Vyberte akci, která se má provést po odemknutí IronKey.</p> <p>Výběrem odpovídajícího zaškrtnutého políčka před odemknutím IronKey si můžete prohlédnout bezpečné soubory, spustit IronKey Control Panel, odemknout IronKey v režimu čtení, kde soubory nelze editovat a bezpečně se přihlásit do svého účtu <i>my.ironkey.com</i>.</p>
3	<p>Stiskněte Unlock.</p>



POUŽITÍ IRONKEY CONTROL PANEL (WINDOWS A MAC)





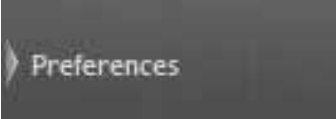
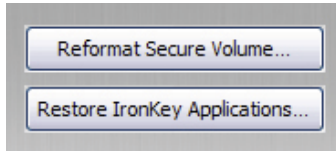
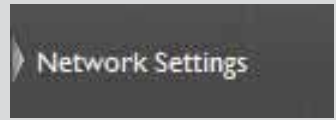

IronKey Control Panel je centrální okno pro:

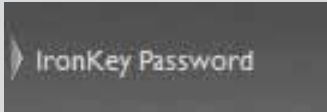



- ◆ Spuštění zabezpečených aplikací
- ◆ Bezpečné přihlášení do *my.ironkey.com*
- ◆ Konfigurace nastavení IronKey
- ◆ Aktualizace přístroje
- ◆ Změna vašeho IronKey hesla
- ◆ Bezpečné zamykání zařízení
- ◆ Získání on-line nápovědy

Většina možností Control Panel je umístěna v menu „Settings“.

Windows verze IronKey Control Panel.

Krok	Popis
1	<p>Vytváření, editace a mazání zabezpečených souborů.</p>  <p>Po klepnutí na tlačítko „Secure Files“ v IronKey Control Panel výchozí prohlížeč na vašem počítači se otevře přímo na váš zabezpečený svazek. Všechny soubory ve vašem IronKey jsou silně šifrovány pomocí AES šifrování na armádní úrovni. Šifrování souborů je pro uživatele stejně jednoduché jako jejich přesunutí do zabezpečeného obsahu. Soubory jsou dešifrovány při jejich přetahování do počítače. IronKey Vám zajistí stejné pohodlí při práci jako u běžného flash disku a zaručí Vám silnou a stálou bezpečnost.</p>
2	<p>Aktualizace firmware / software.</p>  <p>IronKey může bezpečně aktualizovat svůj software a firmware přes podepsané aktualizace, které jsou ověřeny v hardware. Chcete-li zkontrolovat dostupné aktualizace, klepněte na tlačítko „Check for Updates,“ (Windows) nebo „Check Now,“ (Mac). Windows: Dostupnou aktualizaci si můžete stáhnout a nainstalovat kliknutím na „Download Update“. Mac: Dostupnou aktualizaci je třeba stáhnout na počítači s Windows.</p>

Krok	Popis
3	<p>Vaše konfigurace</p>   <p>Klepněte na „Settings“ pro konfiguraci.</p> <ul style="list-style-type: none"> • Můžete povolit Identity Manager • Můžete povolit Secure Sessions • Vyberte výchozí webový prohlížeč pro Váš IronKey • Můžete nastavit automatické zamknutí zařízení po určité době nečinnosti • Můžete nainstalovat Auto-Launch Assistant, který automaticky otevře IronKey Unlocker, když připojíte IronKey. (pouze Mac) <p>Důležité funkce údržby disku:</p> <ul style="list-style-type: none"> • Můžete přeformátovat zabezpečený obsah. • Můžete obnovit IronKey aplikace, jsou-li vymazány nebo poškozeny (pouze Windows).
4	<p>Síťová a proxy konfigurace</p>  <p>Pomocí „Network Settings“ (Windows) nebo „Network“ (Mac) nastavíte konfiguraci připojení k Internetu:</p> <ul style="list-style-type: none"> • Přímé připojení: Nepoužívá proxy. • Použití nastavení systému (výchozí): Používá proxy nastavení počítače. <ul style="list-style-type: none"> ▪ Windows: Ovládací panely > Možnosti Internetu ▪ Mac: System Preferences > Network > Proxy <p>DŮLEŽITÉ: Firefox proxy nastavení musí být stejné jako v System Preferences a IronKey Control Panel. Firefox nepoužívá Systems Preference.</p> <ul style="list-style-type: none"> • Konfigurační skript: Zadejte adresu URL nebo cestu k místu, kde se nachází vaše webové proxy souboru Auto-Detect. • Proxy manuálně: Zadejte adresu URL a číslo portu proxy serveru. <p>Pokud je proxy autentizace požadována, můžete zadat své uživatelské jméno a heslo do příslušných polí.</p>
5	<p>Vytvoření vzkazu pro ztracené a nalezené zařízení</p>  <p>Tato funkce Vám umožní vytvořit zprávu, která se objeví v okně IronKey Unlocker. V případě, že ztratíte IronKey, může Vám nálezce Váš IronKey vrátit na základě této zprávy.</p>

Krok	Popis
6	<p>Změna hesla</p>  <p>Můžete své heslo změnit a zálohovat jej na Váš online bezpečnostní trezor na my.ironkey.com. Požadavkem pro zabezpečení je pravidelná změna hesla. Je důležité si heslo dobře zapamatovat.</p>
7	<p>Informace o zařízení</p>  <p>Můžete si prohlédnout podrobnosti o zařízení - číslo modelu, sériové číslo, verzi software a firmware, disk se zabezpečenými soubory a OS. Můžete také pořídit funkci kopírování (CTRL + C) a zkopírovat details přístroje nebo požadavek na podporu, navštívit webové stránky (CTRL + W) nebo zobrazit právní upozornění (CTRL + N) a certifikáty (CTRL + ?).</p>
8	<p>Přidání, přejmenování a odebrání aplikací na Application List.</p>  <p>Chcete-li spravovat položky v seznamu aplikací z IronKey Control Panel, stačí kliknout pravým tlačítkem kdekoli v seznamu aplikací a zvolit add, rename nebo delete. Můžete také přepínat mezi ikonami a zobrazení seznamu.</p> <p>Poznámky:</p> <ul style="list-style-type: none"> • Mac: Aplikace instalované na zabezpečený svazek jsou automaticky přidány do seznamu (výchozí: prázdný). • Položky v seznamu jsou zkrácenými příkazy na aktuální soubory. Správou položek v seznamu se nezmění aktuální soubor. • Položky jsou automaticky řazeny podle abecedy. • Do seznamu lze přidat libovolný soubor, včetně dokumentů, obrázků a dávkových souborů. • U položek, které nejsou aplikace, Windows otevře položku výchozím programem pro tento typ.
9	<p>Zamknutí a odejmutí zařízení</p>  <p>Kliknutím na „Lock Drive“ (Windows, CTRL + L) nebo „Lock & Quit,“ (Mac) zavřete otevřené aplikace a zamknete zařízení. To pak můžete bezpečně odpojit od počítače. Ujistěte se, že jste zavřeli všechny otevřené aplikace a soubory před zamknutím IronKey, aby jste zabránili poškození dat.</p>



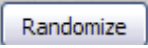

POUŽITÍ VIRTUÁLNÍ KLÁVESNICE IRONKEY (POUZE WINDOWS)

Pokud používáte IronKey na neznámém počítači a máte obavy z keylogging a screenlogging spyware, použijte IronKey virtuální klávesnici, která pomáhá chránit vaše hesla tím, že zadáváte heslo mimo klávesnici. IronKey virtuální klávesnicí obědíte hrozbu trojských koňů, keyloggerů a screenloggerů.

IronKey virtuální klávesnice může být spuštěna:

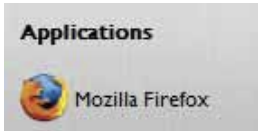

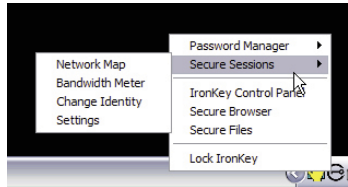
- ♦ V situacích, kde se vaše zadání hesla není z klasické klávesnice bezpečné (např. IronKey Unlocker, změna hesla zařízení, inicializace zařízení).
- ♦ IronKey virtuální klávesnici je možné použít v řadě dalších aplikací, pokud potřebujete bezpečně vytvářet informace (např. e-mail, dokumenty).

Poznámka: Klávesová zkratka CTRL + ALT + V je při práci s IronKey ve Windows vyhrazena pro spuštění virtuální klávesnice a nelze použít pro vložení znaku „@“. Tento znak můžete vkládat ostatními obvyklými způsoby.

Krok	Popis
1	<p>Klikněte na ikonu Virtual Keyboard.</p>  <p>Objeví se IronKey Virtual Keyboard. Můžete také použít CTRL + ALT + V.</p> 
2	<p>Zadejte heslo a Enter.</p> <p>Můžete použít IronKey virtuální klávesnici ve spojení s aktuální klávesnicí tak, že zadáte několik znaků a některé znaky zadáte kliknutím.</p>
3	<p>Můžete také kliknout na „Randomize“ a změnit rozložení klávesnice. To pomáhá chránit proti screenloggerům.</p>  <p>Při klepnutí na klíč na virtuální klávesnici, všechny klávesy zhasnou. Tato funkce zabraňuje Screenloggerům zachytit na co jste klikli. Pokud nechcete používat tuto funkci, můžete ji vypnout v nabídce možností vedle tlačítka Zavřít. V nabídce můžete také nastavit virtuální klávesnici tak, aby se automaticky spustila, když narazí na pole s heslem.</p> 

POUŽITÍ FIREFOX A SLUŽBY SECURE SESSIONS (WINDOWS)

IronKey používá webový prohlížeč Firefox jako součást zařízení a cookies, historie souborů, záložek nebo online hesel se tak neukládá na lokálním počítači. Nyní můžete používat bez obav web na různých počítačích.

Krok	Popis
1	<p>Spustíte webový prohlížeč Firefox.</p>  <p>Kliknutím na ikonu Mozilla Firefox v seznamu aplikací se spustí prohlížeč přímo na IronKey. Lokální verze Firefoxu nemůže běžet ve stejnou dobu, pokud ano, budete vyzváni k jeho ukončení.</p>
2	<p>Přepínejte mezi zabezpečeným a soukromým surfováním v Secure Session.</p>  <p>Kliknutím na tlačítko IronKey v pravém dolním rohu ve Firefoxu bude tiše zapnuta / vypnuta služba Secure Session. Tím se vytvoří šifrovaný tunel přímo z Vašeho IronKey ven na zabezpečený IronKey web server, kde jsou data dešifrována a poslána na cílovou stránku.</p> <p>Toto zabezpečení umožňuje anti-phishing a anti-pharming ochranu (například vlastní DNS kontrola), posílí ochranu soukromí (např. Vaše IP adresa nebude k dispozici jiným webovým stránkách a ISP). Toto můžete zkontrolovat na stránkách <i>whatismyip.com</i> nebo <i>ipchicken.com</i>.</p>
3	<p>Nástroje Secure Sessions: Mapa sítě, měřič šířky pásma a změna identit.</p>  <p>Pomocí Secure Sessions můžete spustit další nástroje tvořící IronKey Menu systémové lišty. Ukáží Vám další informace týkající se vašeho webového provozu a aktuální relace.</p> <p>Mapa sítě zobrazuje veškeré dostupné „okruhy“ a kde na světě je váš provoz aktivní.</p> <p>Bandwidth Meter zobrazuje aktuální šířky pásma metricky.</p> <p>Můžete snadno změnit svoji online „identitu“, která vytvoří nový náhodný okruh a změní cestu k šifrovanému webovému provozu. Pokud přijdete z odlišné IP adresy, budete vypadat, že jste jiný uživatel.</p>

POUŽITÍ IRONKEY IDENTITY MANAGER (POUZE WINDOWS)

IronKey Identity Manager bezpečně ukládá a používá mnoho z Vašich nejdůležitějších informací, včetně přihlašovacích údajů a jednorázových hesel k aplikacím a online účtům. Kliknutím na tlačítko se automaticky spustí specifická aplikace, vyplníte své uživatelské jméno a heslo a přihlásíte se. Můžou se dokonce vytvářet silná hesla, takže si můžete opravdu uzamknout své důležité informace.



IronKey Identity Manager také umožňuje zálohovat šifrovaná data z Identity Manager do zabezpečeného Online trezoru, synchronizovat hesla mezi více IronKey a bezpečně obnovit všechna Vaše hesla do nového IronKey, pokud jste IronKey ztratili nebo Vám byl ukraden. Pouze Vy se můžete přihlásit a dešifrovat Vaše hesla.

IronKey Identity Manager neuchovává hesla v souboru v systému flash disku, takže malware nemůže kopírovat heslo z Vaší databáze. Také to, že nepíšete hesla, poskytuje lepší ochranu před keyloggery a dalším crimeware.



Identity Manager pracuje s VIP službami VeriSign a zamyká mnoho důležitých online účtů, včetně eBay, PayPal, AOL, a Geico účtů. Tato nová technologie generuje jednorázová hesla pro každý login a uzamkne online účet tak, že může být

použit pouze z vašeho IronKey.

Více informací naleznete v souboru Help. Pro jeho zobrazení klikněte na ikonu Help v pravém horním rohu hlavního okna Identity Manager.

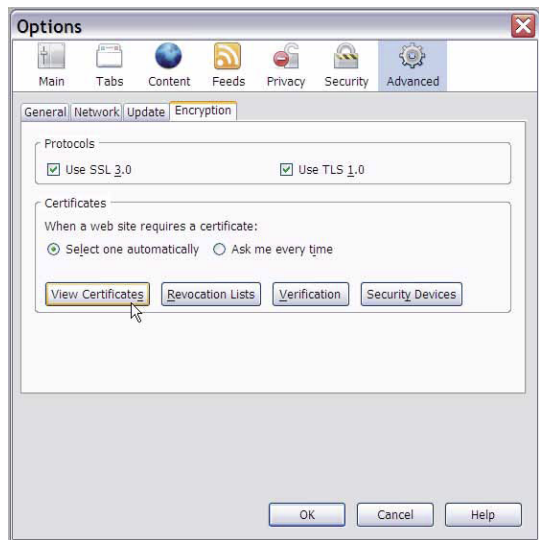
Krok	Popis
1	<p>Přidání účtů a hesel.</p> <p>Přidat účty do Identity Manager můžete několika způsoby:</p> <ul style="list-style-type: none"> • Obnovit je ze svého zabezpečeného online trezoru. • Importovat je z Firefoxu, KeePass, RoboForms nebo Internet Exploreru. • Přidat ručně pomocí tlačítka „Add“ v hlavním okně Identity Manager. • Pokud jsou na určitém webu, zvolte možnost „Add Account“ z Titlebar menu. • Součástí Identity Manager je vestavěná adaptivní funkce, která zachytí Vaše přihlašovací údaje po přihlášení do webu. Identity Manager Vás vyzve k uložení tohoto hesla na vašem IronKey.

IMPORT DIGITÁLNÍHO CERTIFIKÁTU NA IRONKEY (POUZE WINDOWS)

IronKey Cryptochip obsahuje omezené množství extrémně bezpečného hardwarového úložiště, které je možné použít pro uložení soukromého klíče spojeného s digitálním certifikátem. To Vám poskytne další silnou schopnost autentizace.

IronKey používá pro import PKCS#11 rozhraní a vyžaduje prohlížeč Firefox. V IronKey Cryptochip je místo pouze pro jeden další privátní klíč, ale klíč bude chráněn bezpečným hardware šifrováním a sebedestrukčními mechanismy.

Krok	Popis
1	Otevřete instalovaný Firefox.
2	Otevřete Options menu Firefoxu na kartě šifrování.
3	Klikněte na „View Certificates“. Otevře se Certificate Manager Firefox.



Krok	Popis
4	Všimněte si, že je zde k dispozici IronKey certifikát. Můžete přidat vlastní. Klikněte na tlačítko „Import“.
5	Přejděte do souboru s certifikáty formátu PKCS#12 a otevřete jej.
6	Zobrazí se okno s žádostí o potvrzení místa pro uložení certifikátu. Vyberte „IronKey PKCS #11“
7	Zadejte heslo, které bylo použito k ochraně certifikátu. Nebylo-li heslo použito, nechte textové pole prázdné.
8	Certifikát je nyní bezpečně uložen v IronKey Cryptochip a je k dispozici pro použití v instalovaném prohlížeči Firefox.



POUŽITÍ MY.IRONKEY.COM (WINDOWS A MAC)



Váš IronKey podporuje pokročilé šifrovací autentizace pomocí PKI klíčových párů generovaných v IronKey Cryptochip. Když se přihlásíte do *my.ironkey.com* ze zařízení, používají se tyto unikátní klíče jako vaše digitální identity pověření. Váš účet je zamknutý a musíte tedy mít svůj IronKey a heslo pro získání přístupu. Pouze Vy tedy můžete přistupovat ke svému účtu IronKey online.



ke svému účtu IronKey online.

V případě, že ztratíte IronKey, máte stále přístup k webu v nouzovém režimu: v omezeném režimu s omezenou funkcí. Můžete označit IronKey jako ztracený nebo obnovit zapomenuté heslo.

Krok	Popis
1	<p>Bezpečné přihlášení do účtu.</p>  <p>Můžete se bezpečně přihlásit do svého účtu kliknutím na „my.ironkey.com“ v Control Panel. To iniciuje komplexní přihlášení se silnými, multifaktorovými autentizacemi.</p> <p>Pokud ztratíte IronKey, můžete se přihlásit do nouzového režimu na https://my.ironkey.com, pověření pro přihlášení na účet jste vytvořili při aktivaci účtu. To vám umožní označit IronKey jako ztracený nebo obnovit zapomenuté heslo.</p>
2	<p>Označení zařízení jako ztracené.</p>  <p>Pokud ztratíte IronKey, máte jistotu, že nikdo nikdy nezjistí Vaše data. Dalším preventivním opatřením je možnost označení IronKey jako ztracené na <i>my.ironkey.com</i>, to zabrání, aby zařízení bylo zneužito k přístupu k Vašemu účtu. Pokud později IronKey najdete, můžete jej označit jako znovu nalezené.</p>
3	<p>Obnova hesla zařízení.</p>  <p>Pokud zapomenete heslo, IronKey Vám dává možnost zálohovat heslo v online bezpečnostním trezoru na <i>my.ironkey.com</i>. Můžete se přihlásit do nouzového režimu nebo s jiným IronKey a heslo obnovit.</p>
4	<p>Sledování aktivit na účtu.</p>  <p>Account Dashboard zobrazuje poslední aktivity na vašem účtu, jako jsou přihlášení, nezdařené pokusy o zadání hesla a obnovy hesla zařízení.</p>

Krok	Popis
5	<p>Povolení Account Alerts při sledování účtu.</p>  <p>Můžete povolit zaslání zpráv činností na Vašem účtu <i>my.ironkey.com</i>. Bude odeslán Email s podrobnostmi o událostech, jako jsou IP adresa a čas události.</p> <p>Všechny emaily týkající se vašeho účtu budou obsahovat část Secret Phrase v předmětu jako další anti-phishing ochranu.</p>
6	<p>Změna nastavení účtu.</p>  <p>Můžete v rámci <i>my.ironkey.com</i> změnit své heslo, Secret Questions, Secret Image a Phrase, stejně jako váš email tak často, jak chcete. Tím zajistíte ještě větší ochranu pro Váš účet. Můžete také zadat časové pásmo a vybrat formát datumu a času a konfigurovat nastavení časového pásma.</p> <p>Vytvořením sekundární e-mailové adresy předejdete problémům v případě nefunkčnosti primárního emailu.</p>

V případě, že ztratíte IronKey, máte stále přístup k webu v nouzovém režimu: v omezeném režimu s omezenou funkcí. To je užitečné pro označení IronKey jako ztracené nebo obnovení zapomenutého hesla.

Krok	Popis
1	<p>Otevřete https://my.ironkey.com</p> <p>Zde se můžete přihlásit do Safe Mode bez Vašeho IronKey.</p>
2	<p>Zadejte Vaši emailovou adresu (nebo přihlašovací jméno) a heslo Vašeho online účtu.</p> <p>Objeví se Váš Secret Image jako ověření vstupu na správnou stránku.</p> <p>Nezadávejte heslo zařízení na této stránce. Pokud zapomenete heslo Vašeho online účtu, zvolte „Reset Password“.</p>
3	<p>Na Váš email bude odeslána informace s Login Code.</p> <p>Zkopírujte tento Login Code na příslušné místo.</p> <p>V závislosti na konfiguraci Vašeho účtu můžete být požádáni o zodpovězení Secret Questions.</p>
4	<p>Nyní jste přihlášení do Safe Mode.</p> <p>Pokud jste zapomněli heslo zařízení a vytvořili jste zálohu do Online Security Vault, můžete jej nyní obnovit.</p>

POUŽITÍ IRONKEY V REŽIMU ČTENÍ (WINDOWS A MAC)

Můžete odemknout IronKey v režimu čtení. Soubory na Vašem IronKey nebudete moci upravovat. Toto je užitečné, pokud chcete získat přístup k souboru ve Vašem IronKey při používání nedůvěryhodného nebo neznámého počítače. Odemknete-li IronKey v režimu čtení, nemusíte se obávat, že malware na počítači infikuje Váš IronKey nebo upraví soubory.

Po odemknutí IronKey v režimu čtení budete v tomto režimu až do zaknutí IronKey.

Některé funkce nejsou v tomto režimu dostupné, protože vyžadují změnu souborů na IronKey. K dispozici bude Firefox, přeformátování, aktualizace a obnovení aplikací a souborů a použití Application List.

Krok	Popis
1	<p>Při odemknutí IronKey zvolte „Unlock IronKey in Read-Only Mode“.</p> 
2	<p>Na Control Panel se zobrazí potvrzení, že se nacházíte v režimu čtení.</p> 

CO BUDE DÁL?

V mnoha ohledech to je na Vás. Zaměřujeme se nejen na budování nejbezpečnějšího flash disku na světě, ale také na technologie, které jsou jednoduché a jejich použití příjemné. Vaše zpětná vazba je pro nás velice důležitá a my pečlivě přezkoumáváme všechny požadavky na funkce pro stanovení priorit pro naše další produkty.

Máte nápad nebo připomínku? Prosím, dejte nám vědět. Můžete navštívit IronKey fórum (forum.ironkey.com) nebo napsat na feedback@ironkey.com. Dejte nám vědět, pokud byste chtěli být beta tester nových funkcí.

KDE MOHU ZÍSKAT DALŠÍ INFORMACE?

Snažíme se být otevření v otázce bezpečnostních architektur a technologií, které používáme při navrhování a výrobě IronKey zařízení a provozování on-line služeb. Mnoho informací lze nalézt online na webových stránkách:

- ◆ forum.ironkey.com Uživatelské fórum s tisíci "IronKeyologists"
- ◆ www.ironkey.com Základní informace
- ◆ support.ironkey.com Zákaznická podpora a video návody

KDO JE IRONKEY TÝM?

Tým se skládá z expertů v oblastech bezpečnosti a padělání, odborníků s dlouholetými zkušenostmi u společností jako jsou Visa, RSA Security, PayPal, Authenex, Nokia, Cisco, Lexar, Netscape, Tumbleweed, Valicert, Apple a ministerstva vnitřní bezpečnosti. IronKey CEO Dave Jevans je zároveň předsedou Anti-Phishing Working Group (www.antiphishing.org).

SPECIFIKACE PRODUKTU

Kapacita: až 32GB, v závislosti na modelu

Rozměry: 75mm × 19mm × 9mm

Hmotnost: 25 gramů

Vodotěsnost: MIL-STD-810F

Provozní teplota: 0°C - 70°C

Maximální provozní náraz: 16G rms

Šifrování:

- ◆ Hardware: 256-bit AES (Models S200, D200), 128-bit AES (Model S100)
- ◆ Hashing: 256-bit SHA
- ◆ PKI: 2048-bit RSA

FIPS certifikace: www.ironkey.com

Hardware: USB 2.0 (High-Speed) port recommended, USB 1.1

OS Kompatibilita:

- ◆ Windows 2000 (SP4), XP (SP2+), Vista a 7
- ◆ IronKey Unlocker for Linux (2.6+, x86)
- ◆ IronKey Unlocker for Mac (10.4+, Intel)

