

ActivIdentity ActivID™ Credential Management System Appliance

...HW řešení bezpečného univerzálního přístupu
– snadné nasazení smart karet a smart USB tokenů

ActivIdentity řešení univerzálního přístupu v podobě CMS Appliance pomáhá organizacím zajistit jejich bezpečnost a dodržování předepsaných politik z pohledu řízení přístupu k systémům a aplikacím. Jedná se o řešení s vysokou mírou efektivity a návratnosti investic. Nabízí uživatelům jednoduché a bezpečné možnosti pro přístup k počítači, síti, aplikacím a potencionálním fyzickým zdrojům - PC, síť, kopírka apod. Využívá silné PIV-C autentizace pro přístup k logickým a fyzickým systémům. ActivIdentity poskytuje nejširší škálu nativně integrovaných enterprise technologií přístupu - rychlá instalace, snazší správa, a velké možnosti rozšíření.

ActivIdentity CMS Appliance

Vlastnosti

K ČEMU SLOUŽÍ?

- ⇒ **Komplexní řešení pro správu autentizačních pověření a přístupů** – obsahuje předinstalovaný CMS software, průvodce nastavením, **HSM (Hardware Security Module)** – pro bezpečné ukládání certifikátů, **integrována databáze, lokální CA (Certificate Authority)**
- ⇒ **Nastavení trvá méně než 30 minut**
- ⇒ **Vystavení bezpečnostních autentizačních pověření pro smart karty a smart USB tokeny**
- ⇒ **Karty podporují standard PIV** – možnost přihlašování do Windows 7 / Windows Server 2008 R2 / MacOS 10.6 bez middlewaru (ActivClient)
- ⇒ **Nahrazuje Windows Uživatelské jméno a heslo** – USB tokenem nebo certifikátem
- ⇒ PIN může být resetován jen přes appliance s pomocí HSM
- ⇒ **Zaznamenává veškeré logy, monitoruje aktivity a reportuje** (pro potřeby auditů – je zde patrná jakákoliv manipulace)
- ⇒ **Automatické šifrované zálohování a nástroje pro jednoduché obnovení systému**
- ⇒ **"Self-Service" pro uživatele prostřednictvím webu**

ActivIdentity CMS Appliance

Výhody řešení

PROČ?

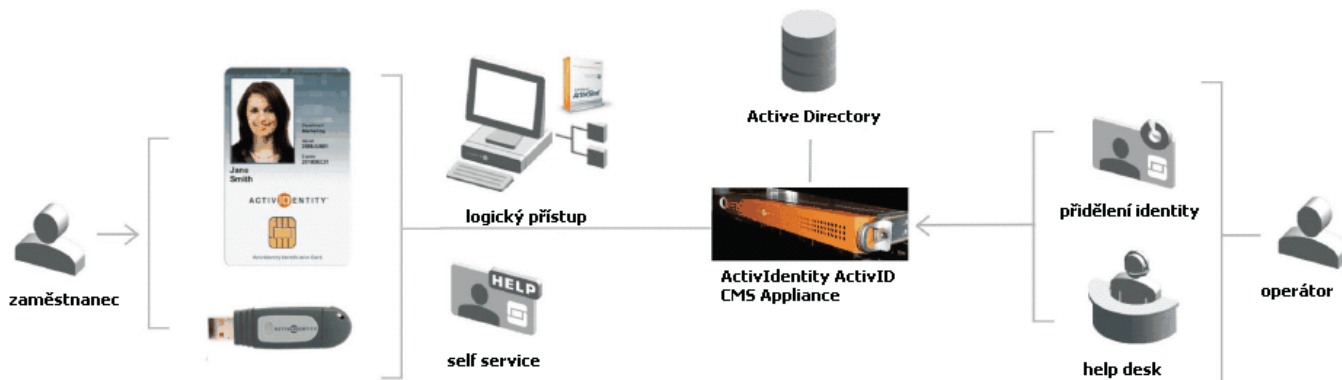
- ⇒ **Snižuje riziko narušení sítě, eliminuje problémy s dodržováním předepsaných politik a zajišťuje dodržování standardů v případě finančních aktivit.**
- ⇒ **Zvyšuje produktivitu** – ze zkušeností uživatelů se jedná o nejjednodušší a na správu pohodlnou silnou autentizaci.
- ⇒ **Zvýšení indexu návratnosti investic (ROI)** – jedno univerzální řešení správy autentizačních pověření – efektivnější správa oprávnění, rychlejší nasazení.
- ⇒ **Využívá osvědčených metod "PKI security" (Public Key Infrastructure)**
- ⇒ **Zvyšuje míru zabezpečení, rychlé osvojení si práce se systémem, zvýšená produktivita**
- ⇒ **Zavedení silné autentizace pro všechny aplikace za pomoci ActivIdentity SecureLogin SSO (Single Sign On)** – volitelně, nutno dokoupit
- ⇒ **Volitelně rozšiřitelné i pro VPN**
- ⇒ Tvoří nejběžnější formu "uzávěry sítě" a kontrolu nad neoprávněným přístupem.

Řešení obsahuje:

- ActivIdentity ActivID CMS Appliance
 - ActivIdentity ActivID CMS-Lite software
 - integrovaná Certification Authority
 - integrovaný HSM
 - integrovaná databáze
 - přednastavený profil "best-practices"
- ActivIdentity ActivID ActivClient
- Smart Card or ActivKey SIM secure USB token
- ActivIdentity SecureLogin SSO (optional)
- Smart Card Reader (optional)



Řešení je určeno pro zákazníky – firmy a společnosti – s počtem zaměstnanců / uživatelů od cca 200 do cca 10.000



Nahrazení statických hesel čipovými kartami – zvýšení bezpečnosti a snížení nákladů na help desk

Statická hesla jsou z pohledu úrovně zabezpečení nedostatečná – jsou příliš zranitelná a často je lze snadno obejít, což je i důvod, proč z hlediska nutnosti dodržování právních norem bývají ve většině případů nevyhovující. Silná autentizace v podobě smart karet nebo smart USB tokenů tato rizika prakticky eliminuje.

CMS Appliance

Jde o centrální prvek řízení vydávání a správy autentizačních prostředků / zařízení, založených na bázi smart-chipu. CMS umožňuje rychlé vydání, změnu a zrušení pověření. Předinstalovaný profil CMS podporuje širokou škálu autentizačních prvků, uživatelé tak mohou mít mnoho možností volby s ohledem na jejich potřeby. CMS zařízení obsahuje integrovanou databázi, plně integrovaný hardware security modul pro tvorbu a správu digitálních certifikátů uložených na čipové katě uživatele. Tyto digitální certifikáty umožňují silnou autentizaci pro uživatele do systému Windows a dalších aplikací.

Autentizační prvky

CMS podporuje širokou škálu autentizačních zařízení včetně různých variant čipových karet a USB tokenů. Tyto prvky uživatelům umožňují změnit si svůj vlastní PIN kód, podporují standardy PKI a PIV-C, a po vyjmutí automaticky zamknou pracovní stanici.

ActivIdentity ActivClient

Jde o přední multiplatformní middleware pro propojení autentizačních prvků, na jedné straně s notebooky nebo desktopy, na straně druhé se systémem CMS. ActivClient je k dispozici pro OS MS Windows a Linux. Karty vydané prostřednictvím ActivID CMS Appliance pracují také s MAC OS x 10.6.

Technické specifikace	
Serverová platforma	1 FIPS 140-2 L2 certified HSM, 2 hot swappable RAID 1 (mirrored) HDD, 2 Gigabit Ethernet LAN port, 1 IPMI 2.0 network management port
Podporované platformy klienta	Operační systémy: Windows 7 32 and 64 bit (všechny edice) Windows Server 2008 R2, Windows Vista 32- and 64-bit (všechny edice), Windows Server 2008 (32- and 64-bit), Windows Server 2003 SP1 / R2 / SP2, Windows XP SP2 / SP3, Windows 2000 SP4, Novell SUSE 10 SP2 (32-bit only), Red Hat® Enterprise Linux® 4, Red Hat Linux 5 (AS, ES, WS, Desktop) (32-bit only), MAC OS® X 10.6
Hlavní funkce	Administrační služby: vydání, řízení životního cyklu karet, PIN management, správa certifikátů, správa uživatelů, konfigurace Služby pro držitele karty: Vydání, řízení životního cyklu karet, PIN management, autentizace
Podporovaná zařízení	Java karty: ActivIdentity ActivKey SIM, ActivIdentity Smart Cards and ActivIdentity Smart Micro SD Cards Čtečky čipových karet: čtečky podporované ActivIdentity ActivClientem
Standardy	U.S. Government: FIPS 201 certified, Smart Card Interoperability Specifications GSC-IS v2.0, GSA Basic Services Interface (BSI), GSC-IS v2.1, Section 508-compliant, FIPS 140-2 certified cards and applications support, FIPS 201 / PIV-certified cards and applications support, FIPS 140-2 certified HSM support Obecné: Secure Sockets Layer (SSL), GlobalPlatform / OpenPlatform, Java Card™ 2.1 and 2.2
Spolupráce se systémy třetích stran	Directories: Microsoft Windows 2003 Active Directory (Enterprise Edition), Microsoft Windows 2008 R2 Active Directory, Microsoft Windows 2008 Active Directory
Kompatibilita s ostatními ActivIdentity SW produkty	ActivIdentity SecureLogin™ Single-Sign On, ActivIdentity ActivClient™, and ActivIdentity ActivClient for Common Access Card