Browser independent Single Sign On

Manažerské shrnutí

Univerzity a další školy využívají nejčastěji technologie, které jsou závislé na použití browseru. To platí i pro identitní federace jako je například EDUGAIN. Pro SP (Service Provider) systémy, které mají čistě browser rozhraní, je integrace relativně snadná pokud podporují standard SAML nebo JWT. Pro univerzitní jednoúčelové nebo krátkodobé projekty není použití těchto standardů ideální, protože jejich implementace není snadná. Univerzity ale také využívají zejména v oblasti výzkumu mnoho systémů, které browserové rozhraní nemají a v principu ani mít nemohou. Pro ty je pak nutné hledat náhradní řešení nebo je z univerzitního SSO prostředí vyloučit. Specifickou skupinu tvoří aktivní prvky, firewally, web content managery, proxy servery a WiFi řešení. Tyto všechny možnosti ale podporuje univerzální řešení KeyShield.

Osobní karty, čipy, tokeny které nyní uživatelé mají pro otevírání dveří a vjezdů, docházkový systém, objednání a vyzvednutí oběda nebo placení v kantýně jsou využitelné a ve skutečnosti ideální i pro autentizační systém - všichni je znají, mají je pořád s sebou a chrání si je. A například na Slovensku je pro ně definován DESFire standard. Přiložením karty ke čtečce uživatel oznamuje, kdo je a nemusí tedy psát své jméno. Zadáním hesla potvrdí svou identitu a je přihlášen tzv. dvoufaktorově – i kdyby někdo jiný znal jméno a heslo, bez karty/čipu se přihlásit nemůže a vice versa – kartou/čipem bez hesla také ne.

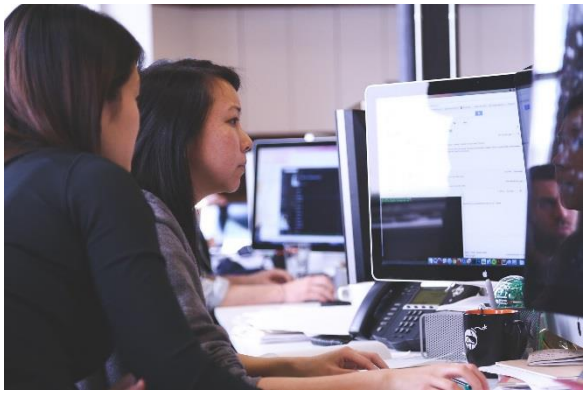
Zabezpečení stanice je nasazením KeyShield významně zvýšeno tím, že pokud uživatel odejde, je automaticky odhlášen a stanice je uzamčena. Pokud se ale vrátí dříve, než vyprší platnost předchozího přihlášení, stačí již jen přiložit kartu a vše je obnoveno – nemusí zadávat heslo znovu..

Efektivitu a bezpečnost Informačních systémů umožňují zvýšit informace, které od KeyShield dostanou – identifikaci uživatele a stanice, na které právě pracuje a změny stavu – uživatel odešel, přišel jiný uživatel, uživatel se vrátil – vždy blesková a bezpečná změna.

Integrace informačních systémů a aplikací je s KeyShield velmi snadná. Potřebný rozsah prací je obvykle 1 až 2 dny programátora a testera. Díky tomu nejde o investici nebo úpravu, na kterou je nutné dlouho čekat. Zejména je to patrné u informačních systémů, které využívá více univerzit.

Stanice mohou být konfigurovány různě, mohou pracovat s 2FA autentizací nebo bez ní. Konfigurace je dynamická ze serveru. Režim práce může být i takový, že se uživatel přihlásí do prostředí Microsoft nebo MicroFocus(Novell) a ke KeyShield je přihlášen automaticky, bez jakéhokoliv dalšího kroku. Podporováno na Windows a MacOSX.

Mobilní zařízení Apple a Android jsou podporována, pouze se s nimi nepoužívají karty.



Pro více informací kontaktujte:

Browser independent Single Sign On

Technické informace

Bezpečný KeyShield je IdP (Identity Provider) – neuchovává hesla ani jiné citlivé informace.

Server KeyShield je implementován v jazyce Java a přímo podporovaná je instalace na Linux a na Windows server. Intuitivní webová konzole pro správu a vestavěný card management.

Klient KeyShield je k dispozici pro všechny hlavní platformy – Windows XP až 10, Linux, MacOSX, iOS (iPhone, iPad), Android. Instalaci klienta na Windows lze zajistit např. jednoduchou politikou, je ve formě .msi. Konfigurace klienta je dynamická ze serveru KeyShield SSO.

LDAP zdroj uživatelů může být libovolná adresářová služba - Active Directory, eDirectory, OpenLDAP, SunOne, Apache DS atd. Lze využít vestavěný Apache DS.

JWT rozhraní je ověřeno s elektronickou poštou Kerio, umožňuje i odhlášení a návrat.

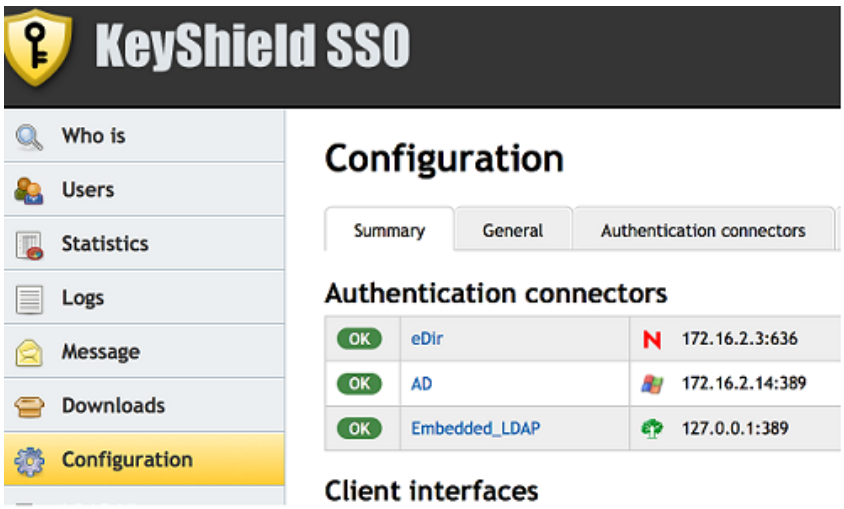
SAML rozhraní je ověřeno s Office365, GoogleApps, SalesForce atd. Lze pracovat s mnoha Service Providery s různými předlohami (assertion template). Podpora pro JWT.

Radius Accounting rozhraní zajišťuje autentizaci uživatelů k libovolnému počtu aktivních prvků v síti (firewall, Web Content Manager, Proxy apod) nebo převzetí identity uživatele VPN od firewallů pro zamezení opakovanému přihlášení.

Integrační API je dostupné na straně serveru (REST) i na straně stanice (DLL) takže nezáleží na tom, zda konkrétní aplikace má tzv. těžkého Windows klienta nebo webové rozhraní nebo obě.

Notifikační rozhraní předává informace všem konfigurovaným integrovaným systémům při každé změně (přihlášení, odhlášení, výměna uživatelů). Rychlost zpracování na straně KeyShield je méně než 1 sekunda.

Prostředí Microsoft a MicroFocus (Novell) jsou plně podporována, klient KeyShield zajistí přihlášení uživatel a připojení jeho domácího adresáře, při odchodu zase odhlášení.



Vašim dodavatelům i vlastním programátorům poskytneme bezplatnou a neomezenou podporu při integraci. Máme zpracované plně funkční příklady pro těžké i webové klienty

Zkušební instalace ve vašem prostředí vyžaduje 1-2 hod