Enterprise SSO Manager (E-SSOM)

Security Model

TOOLS4EVER
IDENTITY GOVERNANCE & ADMINISTRATION

INHOUD

OVER TOOLS4EVER

Tools4ever biedt sinds 2004 een breed scala van enterprise security gerelateerde oplossingen met een specialisatie op het gebied van Identity Management. Binnen het portfolio van Identity Management biedt Tools4ever naast user provisioning (UMRA) een breed scala van wachtwoord beheer producten aan. Enterprise Single Sign On Manager (E-SSOM) is van deze productlijn het meest prominente product. Andere producten in deze lijn zijn:

- Password Synchronization Manager (PSM): wachtwoord synchronisatie tussen Active Directory, Mainframe, AS/400, Unix, Lotus Notes, SAP, etc.;
- Password Complexity Manager (PCM): Wachtwoord complexity binnen Active Directory, en
- Self Service wachtwoord reset (SSRPM): eindgebruikers kunnen zelfstandig hun wachtwoord resetten.

Duizenden klanten wereldwijd vertrouwen dagelijks op de software van Tools4ever. Tools4ever hecht veel waarde aan betrouwbaarheid en certificatie van haar software. Tools4ever heeft partnerships met partijen waarmee de software samenwerkt, zoals Microsoft, SAP, Citrix, IBM, Novell, IGEL, etc. Ook is de software en E-SSOM in het bijzonder gecertificeerd door Microsoft en Citrix.

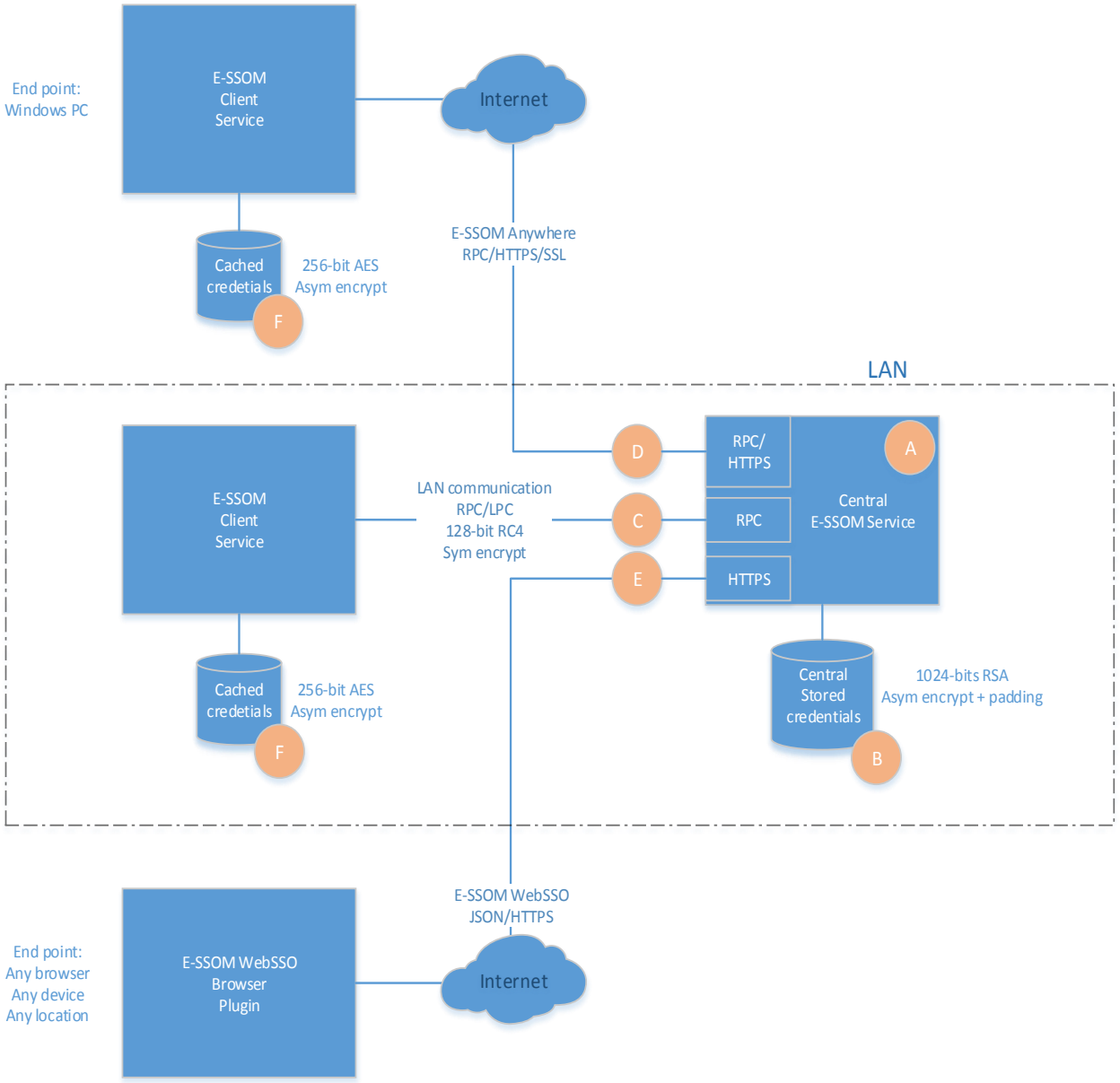
ENTERPRISE SINGLE SIGN ON MANAGER (E-SSOM)

E-SSOM is de Enterprise SSO oplossing van Tools4ever. De primaire functie van de oplossing is het leveren, op een zo'n eenvoudig mogelijke manier, van een laagdrempelige toegang tot bedrijfsinformatie naar de eindgebruikers. Deze functie valt onder te verdelen in het 1) reduceren van het aantal wachtwoorden naar 1 enkel wachtwoord voor de eindgebruiker onafhankelijk van de soort/type applicatie en locatie van de eindgebruiker, 2) het kunnen inloggen met een pasje (2-factor) en 3) het kunnen meenemen van sessies tussen verschillende werkstations (Citrix Sessie roaming).

Om deze functionaliteit te kunnen bieden heeft E-SSOM toegang nodig tot gebruikersnamen en wachtwoorden van de eindgebruikers binnen de organisatie. Deze zogenoemde credentials worden opgeslagen door E-SSOM voor toekomstig gebruik en worden uitgewisseld tussen verschillende onderdelen van E-SSOM. Omdat het hier gaat om kritische bedrijfsgegevens is het van cruciaal belang dat deze gegevens met de grootste zorg worden beheerd binnen E-SSOM. Dit document beschrijft hoe deze beveiliging uitgevoerd is binnen E-SSOM. Let op: er is een bepaald niveau van detaillering gekozen waarbij Tools4ever geen 100% inzicht verschaft om hiermee te voorkomen dat kwaadwillende exact begrijpen hoe het security model van E-SSOM functioneert en ongewenst toegang verkrijgen tot de credentials.

SECURITY ARCHITECTUUR E-SSOM

De E-SSOM oplossing bestaat uit verschillende software componenten. Het onderstaande diagram toont een overzicht van de belangrijkste componenten en de samenhang ertussen. Het architectuur model van E-SSOM is het traditionele drie-lagen model: 1) client laag, 2) server/applicatie-laag en 3) database-laag. Zodra informatie wordt uitgewisseld tussen een laag of (tijdelijk) wordt opgeslagen dan wordt de informatie geëncrypt. In het diagram is aangegeven welke security mechanismes worden toegepast per onderdeel. De mate van security is niet per onderdeel hetzelfde en is afhankelijk van het niveau van de impact, het risico en de technische toepasbaarheid.



In het diagram zijn de volgende onderdelen van belang:

A	Dit is de centrale service van E-SSOM. Dit onderdeel draait op een Windows member server in de LAN-omgeving van de organisatie. De E-SSOM service heeft direct toegang tot de Active Directory en draait in de security context van Windows Active Directory. E-SSOM stelt specifieke eisen aan de permissies van het AD service account waardoor de E-SSOM service de benodigde taken kan uitvoeren. Deze eisen zijn: AD Serviceaccount met admin rechten op SSO Servers en MSSQL omgeving en het beschikbaar hebben van poort 36785. De acties die de centrale E-SSOM service uitvoert zijn: beheer configuratie gegevens applicaties (niet beveiligingsgevoelig), beheer van credentials gegevens van alle medewerkers en alle applicaties (extreem beveiligingsgevoelig), connectie E-SSOM clients (beveiligingsgevoelig), connectie E-SSOM console (redelijk beveiligingsgevoelig). In het diagram is per communicatietype aangegeven wat de encryptiemethode is.
B	De centrale database met alle credentials is beveiligd met een sterk encryptie algoritme. Hiervoor wordt het asymmetrische RSA[1] encryptie algoritme gebruikt. De DPAPI implementatie van RSA maakt gebruik van 'padding'[2] om de bekende problemen met de deterministische[3] aard van RSA te voorkomen.
C	Bij de standaard inrichting van E-SSOM is de scope van de implementatie LAN gebaseerd en vindt er geen uitwisseling van informatie buiten het LAN domein van de organisatie plaats. De E-SSOM clients bevinden zich op Windows gebaseerde clients (al dan niet Citrix gebaseerd). De communicatie tussen de clients en de centrale service is gebaseerd op encrypted RPC/LPC waarbij gebruik wordt gemaakt van 128bit RC4 .
D	Sommige organisaties bieden medewerkers thuis een beheerde Windows werkplek aan. Deze werkplek is geen onderdeel van het domein maar kan via een specifieke setup van de TMG firewall verbonden worden aan het LAN domein van de organisatie. Het communicatie protocol tussen de thuiswerkplek en het LAN is RPC over HTTPS. De beveiligde RPC verbinding wordt in dit geval via een HTTPS tunnel tot stand gebracht. Deze tunnel is zelf met SSL beveiligd. De precieze SSL beveiliging is afhankelijk van de IIS instellingen.

[1] Voor meer informatie over deze algoritme zie http://en.wikipedia.org/wiki/RSA_(cryptosystem)
[2] Voor meer informatie over deze padding zie http://en.wikipedia.org/wiki/Padding_(cryptography)
[3] Deterministisch: Altijd dezelfde output bij dezelfde input.

E	Omdat E-SSOM Anywhere specifieke setup vereist van de externe werkplek en de firewall is deze niet geschikt om breed beschikbaar te maken aan alle medewerkers. Ook beperkt deze setup om SSO aan te bieden alle type devices (tablets, smartphones, laptops, etc.). Om deze reden is native HTTPS communicatie toegevoegd waarbij het niet nodig is om RPC over HTPP toe te passen. De communicatie laag is uitgevoerd op basis van JSON/HTTPS (SSL).
F	Optioneel is het mogelijk om credentials lokaal op te slaan bij de client service. Het lokaal opslaan van de credentials levert de volgende extra functionaliteit: 1) hoge beschikbaarheid van SSO: de eindgebruiker kan doorwerken ook als er geen verbinding is met de centrale service; 2) offline support: indien de eindgebruiker met een laptop werkt is het mogelijk om ook lokaal SSO te gebruiken. Deze lokale gegevens bevatten enkel en alleen de credentials van lokaal ingelogde gebruikers en deze worden opgeslagen bij de roaming profile gegevens van de gebruiker. De security context van de opgeslagen gegevens is het lokale E-SSOM service account. De gegevens in de lokale database zijn beveiligd door middel van AES 256 encryptie[4].

[4] Voor meer informatie over deze algoritme zie http://en.wikipedia.org/wiki/Advanced_Encryption_Standard

TOOLS4EVER BV

Amalialaan 126c
3743 KJ Baarn
Nederland

T +31 (0) 35 54 832 55 F +31 (0) 35 54 327 36

Informatie info@tools4ever.com
Sales sales@tools4ever.com
Support isupport@tools4ever.com