M.I.T. Consulting

# Autologin Kerberos

## Návrh řešení

M.I.T. Consulting s.r.o.

**VERZE DOKUMENTU**

| Číslo revize | Datum revize | Sumarizace změn | Provedl |
|---|---|---|---|
| 1.0 | 12. 4. 2021 | Draft | [redacted] |
| | | | |
| | | | |
| | | | |

# 1 Obsah

# 2 Seznam pojmů a zkratek

| Pojem / Zkratka | Definice |
|---|---|
| **AD** | Active Directory – adresářové služby LDAP |
| **Apache** | Softwarový webový server |
| **DC** | Domain Controller |
| **Kerberos** | Síťový autentizační protokol |
| **Liferay** | Portálová platforma |
| **NTLM** | Síťový autentizační protokol |
| **OS** | Operační systém |

*Tabulka 1 Seznam pojmů a zkratek*

# 3 Současný stav

V současnosti je na portálu SŽ implementováno automatické ověření uživatele pomocí protokolu NTLMv2. Tento protokol pro komunikaci využívá vzdálené volání pomocí Netlogon Remote Protocol, který má zranitelnost uvedenou v https://support.microsoft.com/en-us/topic/how-to-manage-the-changes-in-netlogon-secure-channel-connections-associated-with-cve-2020-1472-f7e8cc17-0309-1d6a-304e-5ba73cd1a11e.

Portál Liferay je na SŽ provozován ve verzi 6.2 CE. Pro Liferay je vytvořen autentizační modul, který je vytvořen na míru SŽ, a tento modul implementuje:

- autologin pomocí NTLM,
- manuální přihlášení s ověřením vůči AD,
- manuální přihlášení s ověřením vůči SAP,
- manuální přihlášení s ověřením vůči lokální databázi Liferay,
- podpora pro migraci domén,
- podpora různých způsobů ověření uživatele pro přístup z externí nebo interní sítě,
- podpora IDM a jeho unikátního identifikátoru uživatele.

# 4 Cílový stav

Je požadováno nahrazení protokolu NTLM za síťový autentizační protokol Kerberos.

# 5 Návrh řešení

V této kapitole je popsán návrh řešení.

Návrh řešení vychází z manuálu k řešení modulu Kerberos pro Liferay 7 (viz https://liferaypartneritalia.smc.it/documents/982916/1111493/Guida+Kerberos+EN/b05444fd-0a6d-4959-8598-6de5005bb8e9), na tento dokument je odkazováno z dále uvedeného textu.

## 5.1 Kerberos

Kerberos je síťový autentizační protokol. Princip je uveden k odkazovaném dokumentu v kapitole 2.

### 5.1.1 Spnego

Simple and Protected GSSAPI Negotiation Mechanism (SPNEGO) je mechanismus na vyjednávání o volbě bezpečnostní technologie. Pro vyjednání protokolu Kerberos mezi klientem a serverem, bude využit právě tento mechanismus.

## 5.2 Ověření Kerberos ticketu

Předmětem nabídky je především dodání mechanismu na vyjednání protokolu (jehož jediným úspěšným vyjednáním je protokol Kerberos, NTLM nebude podporováno), a dále mechanismus na ověření Kerberos tickety vůči DC. Po úspěšném ověření bude uživatel přihlášen do portálu.

### 5.2.1 Java knihovny

Java obsahuje knihovny, které slouží pro ověřování ticketu na DC serveru. Tyto knihovny budou využity. Pro získání ticketu od uživatele, který chce být ověřen pomocí SSO, bude využito standardního vyjednávání o autentizačním protokolu (WWW-Authenticate).

## 5.3 Konfigurace na straně AD

### 5.3.1 Servisní účet

Pro ověřování Kerberos ticketu je třeba servisní účet, pomocí kterého aplikační server ověřuje ticket obdržený od klienta. Servisní účet bude vytvořen administrátorem DC, a jeho vytvoření a správa nebude součástí nabídky.

### 5.3.2 Keytab

Předpokladem tohoto řešení je dodání keytab souboruAdministrátor DC dodá keytab soubor, který bude obsahovat definici servisních účtů pro každou portálem poskytovanou službu. Službou je v kontextu protokolu Kerberos myšleno doménové jméno, pod kterým je dostupná stránka portálu, pro niž má být k dispozici SSO pomocí protokolu Kerberos. V odkazovaném dokumentu se jedná o kapitolu 3, jehož řešení nebude součástí nabídky.

## 5.4 Konfigurace klientů

Po přístupu klienta na zabezpečenou stránku portálu bude portálem vrácen status 401 a způsob autentizace „WWW-Authenticate: Negotiate“. Součástí této nabídky není konfigurace klientů tak, aby dokázali získat Kerberos ticket, který předají k validaci na server poskytující službu (různé domény portálu Liferay SŽ). Nastavení klientů je uvedeno v kapitole 6 v odkazovaném dokumentu.

## 5.5 Verze OS AD

Řešení bude otestováno na verzi operačního systému Windows Server 2012 R2 Datacenter, a dále proběhne testování na verzi Windows Server 2019.

## 5.6 Omezení navrženého řešení

Předpokladem je, že autologin pomocí protokolu Kerberos bude dostupný pouze pro doménu UADF.

## 5.7 Testování v prostředí SŽ

Testování bude provedeno v prostředí objednavatele, které bude konfigurováno bezobslužně prostřednictvím doménové politiky objednatele. Výsledkem úspěšného testu je automatické přihlášení do portálu Liferay.

## 5.8 Akceptační kritéria

Uvedený test v předchozí kapitole je zároveň akceptačním testem.

**Ověřovací doložka změny datového formátu dokumentu podle § 69a zákona č. 499/2004 Sb.**

**Doložka číslo:** 1452492

**Původní datový formát:** application/pdf

**UUID původní komponenty:** e5086dee-0fa2-4cbd-b930-920a122205c8

**Jméno a příjmení osoby, která změnu formátu dokumentu provedla:**

Systém ERMS (zpracovatel dokumentu Lenka ANDRÝSOVÁ)

**Subjekt, který změnu formátu provedl:** Správa železnic, státní organizace

**Datum vyhotovení ověřovací doložky:** 15.04.2021 10:52:01

2179cd7d-2811-4af7-8cc2-9c2db91da37e