TLS (Transport Layer Security)

TLS je kryptografický protokol navržený tak, aby poskytoval bezpečnou komunikaci v počítačové síti. Je přímým nástupcem staršího protokolu SSL (Secure Sockets Layer). V naší **digitální architektuře** zajišťuje TLS tři klíčové věci: **soukromí** (šifrování), **integritu** (data nebyla cestou změněna) a **autentizaci** (víme, s kým komunikujeme).

Každé připojení k našemu systému **Jira**, firemnímu webu nebo **VPS** musí být povinně šifrováno pomocí TLS.

Jak TLS funguje? (Handshake)

Předtím, než se začnou přenášet samotná data (např. v kódování **UTF-8**), proběhne tzv. „TLS Handshake“:

```
1. **Pozdrav:** Klient a server si vymění podporované verze protokolu a šifrovací sady.
2. **Certifikát:** Server pošle svůj digitální certifikát. Klient ověří jeho platnost (podpis autority).
3. **Výměna klíčů:** Pomocí asymetrické kryptografie (RSA/ECC) se bezpečně dohodnou na symetrickém klíči.
4. **Šifrovaný kanál:** Od této chvíle jsou všechna data šifrována dohodnutým klíčem.
```

TLS v naší infrastruktuře

1. Webové služby a HTTPS

Všechny naše **WWW** servery používají HTTPS (HTTP přes TLS). Naše brány **UTM** vynucují používání moderní verze **TLS 1.2** nebo **TLS 1.3**. Starší verze (TLS 1.0, 1.1) jsou z důvodu **kybernetické bezpečnosti** zakázány.

2. Zabezpečení e-mailu a [[VPC]]

TLS používáme pro zabezpečení přenosu e-mailů (SMTP over TLS) a pro šifrování vnitřní komunikace mezi mikroslužbami v našem virtuálním cloudu.

3. Identifikace a Certifikáty

Pro správnou funkci TLS využíváme:

- **SSL/TLS Certifikáty:** Vystavené důvěryhodnou autoritou pro naše domény.

- **TPM:** U některých kritických aplikací využíváme hardware pro bezpečné uložení soukromých klíčů k certifikátům.

Rozdíl mezi SSL a TLS

Ačkoliv se v běžné mluvě stále používá termín „SSL certifikát“, technicky se jedná o certifikát pro protokol TLS.

Protokol	Status	Poznámka
SSL 2.0 / 3.0	**Zastaralý**	Nebezpečný, nesmí se používat.
TLS 1.0 / 1.1	**Zastaralý**	Obsahuje známé slabiny (např. BEAST, POODLE).
TLS 1.2	**Standard**	Aktuálně nejrozšířenější v naší síti **WAN**.
TLS 1.3	**Doporučený**	Rychlejší a bezpečnější, náš preferovaný cíl.

Správa certifikátů (IT Podpora)

Naše **IT Podpora** monitoruje expiraci všech certifikátů. Pokud certifikát vyprší, uživatelé uvidí v prohlížeči varování „Vaše připojení není soukromé“, což blokuje přístup k důležitým datům v **VPC**.

> **Upozornění pro vývojáře:** Při testování aplikací nikdy nevypínejte verifikaci TLS certifikátů v kódu. Pokud potřebujete testovat na lokálním stroji, požádejte o vystavení interního certifikátu z naší firemní autority.

— **Související stránky:** ZIF, Kybernetická bezpečnost, WWW, VPS, UTM, IT Podpora, VPC, TPM, UTF