Financováno Evropskou unií
NextGenerationEU

MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY

Národní plán obnovy

Popis procesů bezpečného předávání a dlouhodobého uchovávání studijních dokumentů

Veterinární univerzita Brno

VETUNI pro 21. století: Rozvoj VETUNI v oblasti digitalizace činností, profesionálního vzdělávání a flexibilních forem vzdělávání
Specifický cíl C2. Bezpečnost distančních forem výuky

Projekt NPO registrační číslo NPO_VETUNI_MSMT-16594/2022

Výstup č. 10, vazba na cíl projektu č. 15

Financováno Evropskou unií
NextGenerationEU
MINISTERSTVO ŠKOLSTVÍ, MLÁDEŽE A TĚLOVÝCHOVY
Národní plán obnovy

Popis procesů bezpečného předávání a dlouhodobého uchovávání studijních dokumentů

V rámci tohoto výstupu byly definovány základní pravidla pro předávání informací. Pro bezpečné předání dokumentů je vhodné využívat možnosti šifrovaného přenosu dat. V případě zabezpečené komunikace pomocí protokolu HTTP je doporučeno využívat protokoly TLS 1.2 a vyšší (TLS 1.3), starší protokoly SSL 2.0, SSL 3.0, TLS 1 a TLS 1.1 již nejsou považovány za bezpečné, a nejsou tak již doporučovány pro použití.

Privátní klíč a odpovídající certifikát by měl po celou dobu své životnosti být dostatečně silný, doporučuje se tak využívat velikost klíče minimálně 2048 bitů. Privátní klíč je nutné zabezpečit na úrovni systému souborů pomocí oprávnění, případně jinými technickými a administrativními opatřeními kvůli ochraně proti neoprávněnému získání a potenciálnímu zneužití klíče. Certifikát by měl využívat hashovací algoritmus minimálně SHA-256, starší algoritmy (MD5, SHA-1) již nejsou doporučovány. Certifikát by měl být vydán certifikační autoritou, která je pro všechny klienty důvěryhodná.

Pro úložiště, resp. informační systémy které umožňují přístup ke studijním dokumentům by měly existovat systém řízení přístupu k dokumentům. To zahrnuje definování oprávněných osob, které mají přístup k dokumentům, a nastavení vhodných úrovní oprávnění pro různé role.

Veterinární univerzita Brno se v rámci diskuzí a připomínkování pracovních výstupů přímo zapojila do zpracování výstupu, který předložila koordinující škola. Dílčí výstupy této části projektu byly aplikovány v podmínkách naší univerzity. Jednalo se zejména o ukončení používání starších šifrovacích protokolů.