Česká agentura pro standardizaci, státní příspěvková organizace, IČO: 06578705

se sídlem Biskupský dvůr 1148/5, Praha 1, PSČ 110 00

Bezpečný způsob předání údajů mezi Objednatelem a Atestačním střediskem

Verze: 1.1

Datum vydání: 5. 11. 2024

Datum účinnosti: 5. 11. 2024

Počet stran: 11

Nahrazovaný dokument: Bezpečný způsob předání údajů mezi Objednatelem a Atestačním střediskem, verze 1.0

Seznam změn a revizí

Verze	Datum vydání	Charakter změny / revize	Datum účinnosti	Vypracoval
1.0	30. 6. 2023	Iniciální verze	1. 7. 2023	Petr Stiegler
1.1	5. 11. 2024	Změna aplikace třídy Password Manager z TeamPass na aplikaci Vaultwarden / Bitwarden, doplnění popisu struktury dat v aplikaci.	5. 11. 2024	Petr Stiegler

1 Úvod

Provozní řád Atestačního střediska, především dokument *„Provozní řád Atestačního střediska – Část 1: Metodika přípravy Atestačního prostředí“* vyžaduje bezpečné předávání údajů mezi Objednatelem a Atestačním střediskem, neboť se podle dokumentu *„Provozní řád Atestačního střediska – Část 3: Bezpečnostní politika Atestačního střediska“* jedná o údaje klasifikované stupněm „Důvěrné“.

Účastníky této komunikace jsou Atestační středisko a konkrétní osoby Objednatele v roli Zástupce Objednatele ve věcech technických (dále jen „Zástupce“), které byly nominovány Objednavatelem a jejich kontakty byly Atestačnímu středisku předány prostřednictvím formuláře *„Poskytnutí informací Objednatele k vytvoření Atestačního prostředí“*.

Dokument popisuje způsob předávání důvěrných údajů mezi Atestačním střediskem a Zástupci.

2 Úvod do aplikace Vaultwarden / Bitwarden

Pro předávání důvěrných údajů je použita webová aplikace Vaultwarden / Bitwarden (dále jen „Vaultwarden“). Jedná se o webovou aplikaci třídy Password Manager. Jde o software, který umožňuje řídit a monitorovat distribuci údajů. Více informací o tomto konkrétním produktu lze nalézt na webové stránce https://github.com/dani-garcia/vaultwarden.

Vaultwarden je nainstalován ve výpočetním prostředí Atestačního střediska a je provozován Atestačním střediskem. Jedná se tedy o instalaci lokální pro Atestační středisko; důvěrné údaje jsou ukládány výhradně v prostředí Atestačního střediska a přístup k nim je řízen Atestačním střediskem.

Aby bylo možno předávat důvěrné údaje mezi Atestačním střediskem a Zástupci, musí Zástupci mít zřízen v aplikaci Vaultwarden uživatelský účet.

2.1 Zřízení uživatelského účtu

Uživatelský účet v aplikaci Vaultwarden zřídí Atestační středisko pro všechny Zástupce na základě obdržení správně a úplně vyplněného formuláře *„Poskytnutí informací Objednatele k vytvoření Atestačního prostředí“* od Objednatele. Závazný vzor tohoto formuláře je zveřejněn na Internetových stránkách Atestačního střediska v sekci *Formuláře pro atestace*. Tento formulář obsahuje pole pro zapsání kontaktních údajů Zástupců.

Atestační středisko v aplikaci Vaultwarden pro každého Zástupce vytvoří pozvánku. Aplikace Vaultwarden následně pozvánku odešle formou e-mailové zprávy zaslané z adresy pm@atest-cas.cz na e-mailovou adresu Zástupce uvedenou ve zmíněném formuláři.

E-mailová zpráva má subjekt ve tvaru „Join <přidělené APN> - Atestace eSSL”. Zkontrolujte případně také spamový koš. Váš uživatelský účet vytvoříte kliknutím na tlačítko “Join Organization Now”, následně klikněte na tlačítko “Create account”. E-mailová adresa zadaná do formuláře pro vytvoření uživatelského účtu musí být ta, na kterou byl zaslán pozvánkový e-mail; tato adresa je ve formuláři předvyplněna.

Po vytvoření uživatelského účtu a přihlášení do aplikace Vaultwarden ještě po nějakou dobu nebudete mít dostupné předávané údaje. Důvodem je, že Atestační středisko musí váš přístup potvrdit; jedná se o proces aplikace Vaultwarden a není možné jej na straně Atestačního střediska měnit. Atestační středisko potvrdí váš přístup neprodleně, nejpozději však do druhého pracovního dne. O potvrzení přístupu budete informováni e-mailem zaslaným aplikací Vaultwarden z adresy pm@atest-cas.cz a s předmětem ve tvaru „Invitation to <přidělené APN> - Atestace eSSL confirmed“. Poté vám budou

v aplikaci Vaultwarden dostupné údaje sloužící ke zpřístupnění Atestačního prostředí a konfiguraci testovaného eSSL.

2.2 Zřízení uživatelského účtu v případě více souběžných atestací

Tento bod popisuje případ, kdy konkrétní Zástupce je Zástupcem souběžně pro více Atestačních případů. Pokud vaše společnost nemá otevřeno více Atestačních případů souběžně, je pro vás tento bod irelevantní.

Aplikace Vaultwarden zasílá pozvánku pro každý Atestační případ. Pozvánka má vždy shodný obsah, tj. umožnuje buď vytvoření uživatelského účtu, nebo přihlášení uživatele pod existujícím uživatelským účtem. Uživatelský účet Zástupce je však pouze jeden, přesněji řečeno: uživatelský účet Zástupce je vázán na e-mailovou adresu.

Na první pozvánku do aplikace Vaultwarden je tedy třeba reagovat vytvořením uživatelského účtu, jak je popsáno v bodě 2.1. U druhé pozvánky se uživatelský účet nezřizuje, ale v e-mailové zprávě je potřeba kliknout na tlačítko “Join organization now” a poté na spodní straně formuláře pro vytvoření uživatelského účtu na tlačítko “Log in”, a přihlásit se tak do vašeho již existujícího uživatelského účtu.

Pozn.: druhý pokus o vytvoření uživatelského účtu s se shodným e-mailem přirozeně selže a aplikace Vaultwarden toto selhání oznámí uživateli.

2.3 Přihlášení do aplikace Vaultwarden

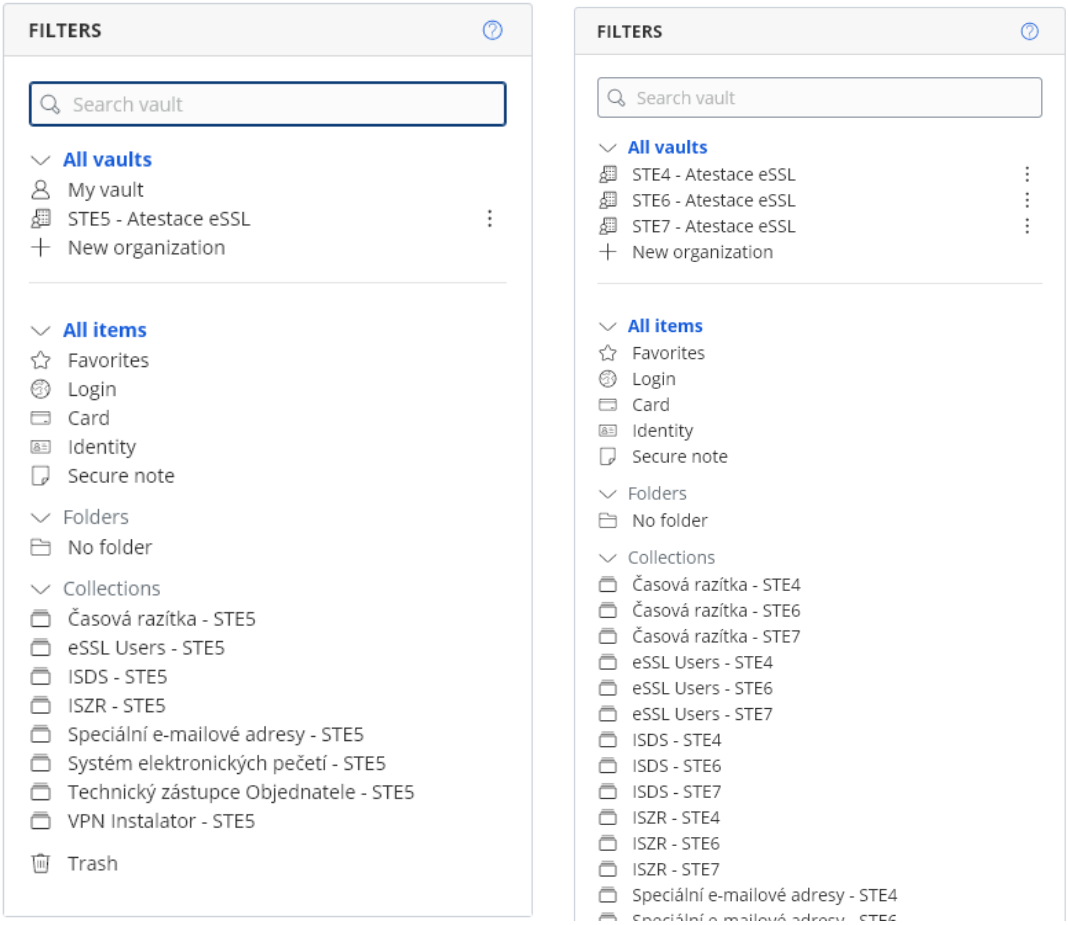
Způsob autentizace do aplikace Vaultwarden je uživatelským jménem a heslem.

Pozn.: Druhý faktor zde není použit. Tento fakt nesnižuje bezpečnost, protože údaje lze využít pouze v Atestačním prostředí, které je dostupné výhradně prostřednictvím VPN; přístup do VPN je chráněn i druhým faktorem.

2.4 Struktura aplikace Vaultwarden

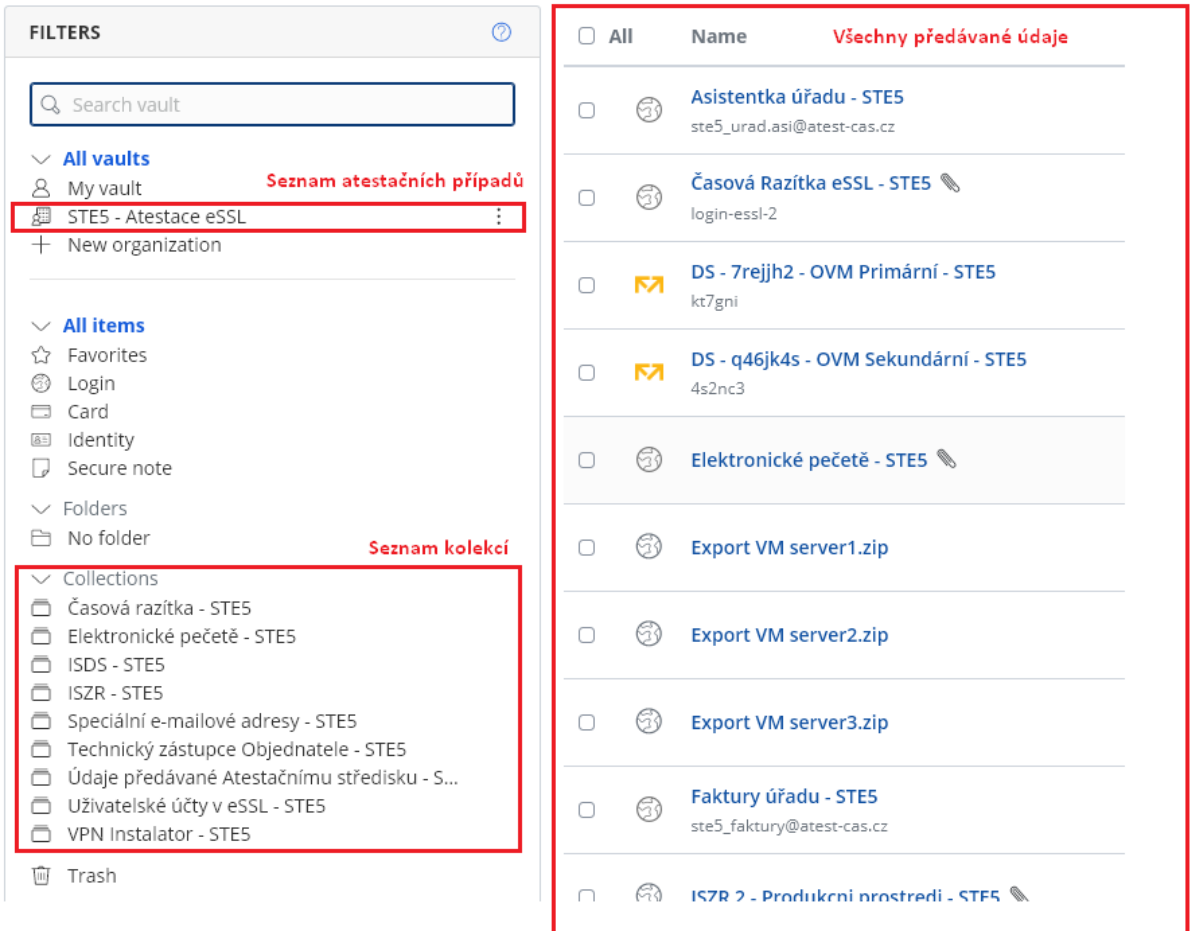
Po přihlášení do aplikace Vaultwarden je v levé horní části obrazovky (vpravo od menu) zobrazen seznam tzv. „organizací“ (trezorů). „Organizace“ je termín aplikace Vaultwarden a je použit pro Atestační případ. Pokud jste souběžně Zástupce pro více Atestačních případů, jste z pohledu aplikace Vaultwarden členem více „organizací“.

Následující obrázek zobrazuje obsah levého menu v případě, že přihlášený uživatel je Zástupcem pro jeden atestační případ (s APN “STE5”, zobrazen v levé polovině obrázku) a v případě, že přihlášený uživatel je Zástupcem pro více atestačních případů (s APN “STE5”, “STE6”a “STE7”, zobrazen v pravé polovině obrázku):



Obr. 1: Příklady zobrazení složek

Předávané údaje jsou v aplikaci zobrazeny v různé struktuře. Následující popis je sestaven pro nejčasnější případ, kdy uživatel je Zástupcem souběžně pouze pro jeden Atestační případ.



Obr. 2: Příklad zobrazení předávaných informací

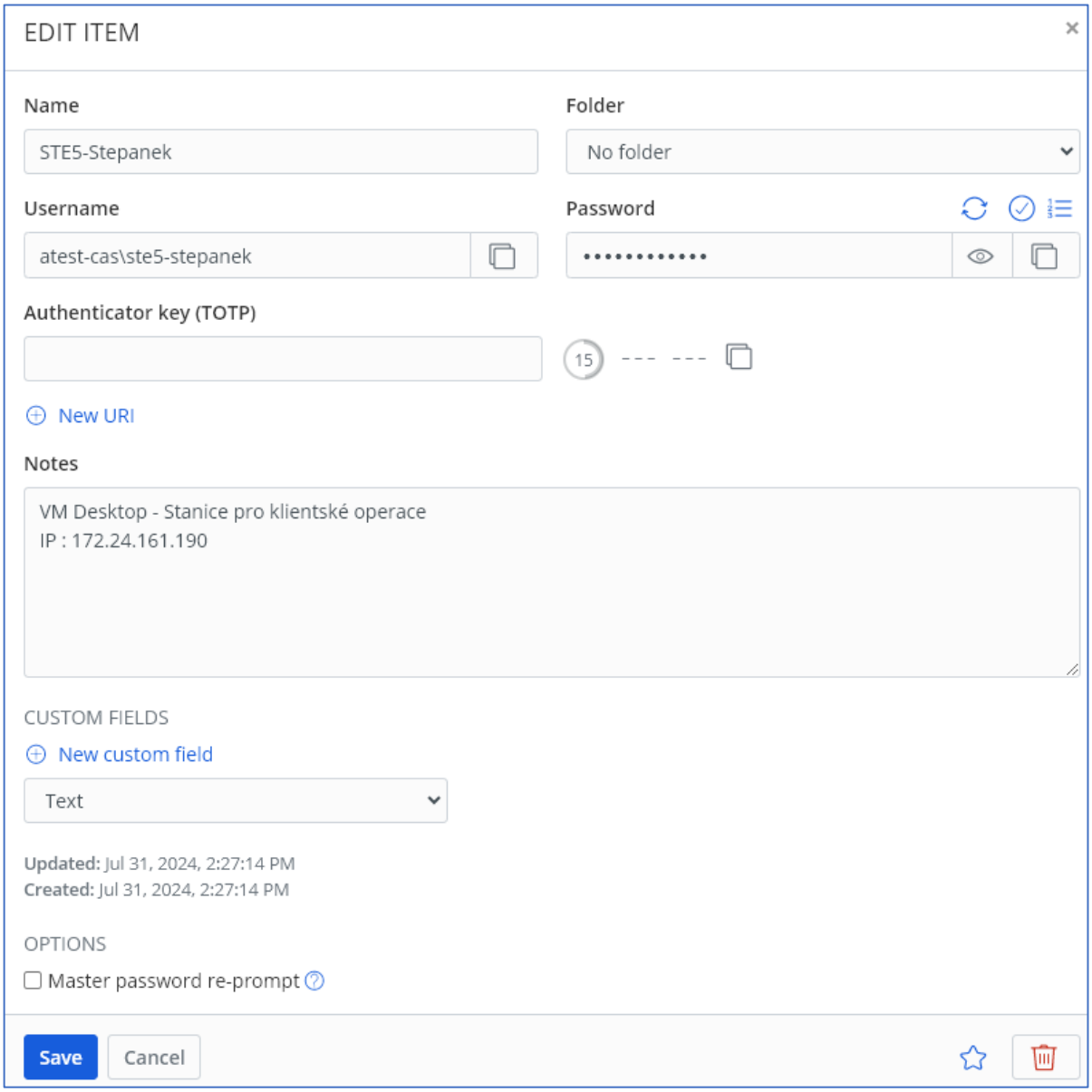
Předávané informace jsou dostupné prostřednictvím neorganizovaného seznamu (na výše uvedeném obrázku v jeho pravé části). Tento seznam doporučujeme filtrovat kliknutím na libovolnou „Collection“ (na výše uvedeném obrázku v jeho levé spodní části, dále v textu jsou označeny jako „kolekce“).

Pokud je přihlášený uživatel Zástupcem pro více Atestačních případů, může seznam kolekcí dále filtrovat kliknutím na název konkrétní „organizace“ (na výše uvedeném obrázku v jeho horní části).

Ostatní položky menu (např. „Card“, „Identity“, „Folders“) nejsou ze strany Atestačního střediska využívány.

2.5 Zobrazení obsahu položky

Obsah položky lze zobrazit kliknutím na její název. Aplikace Vaultwarden poté zobrazí obsah položky takto (příklad je uveden pro položku popisující přístup na Interní atestační prostředí, všechny položky jsou vysvětleny v kap. 3 *„Význam předávaných dat“*):

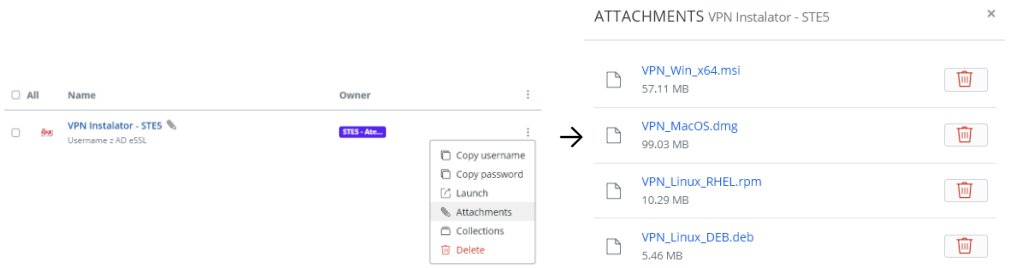


Obr. 3: Příklad zobrazení detailu položky

Tato položka informuje Zástupce o tom, že uživatel „atest-cas\ste5-stepanek“ má přístup na virtualizovanou Stanici pro klientské operace s IP adresou 172.24.161.190 s heslem, které lze zobrazit kliknutím na ikonu nebo zkopírovat do systémové schránky operačního systému kliknutím na ikonu . Pokud byla pro provedení atestace zvolena varianta A) podle čl. 5 dokumentu *„Postup Atestačního střediska“*, budou zde uvedeny i IP adresy vytvořených virtualizovaných serverů. Vzhledem k tomu, že přístup k nim je řízen prostřednictvím Active Directory Atestačního střediska, jsou zde předané autentizační údaje platné pro všechny virtualizované servery i Stanici pro klientské operace.

2.6 Získání předávaného souboru

Některé položky mohou obsahovat také soubory, např. certifikáty, instalační soubory apod. Aplikace Vaultwarden nezobrazuje soubory v detailu položky (viz obr. 3), ale umožní jejich získání prostřednictvím volby „Attachments“ dostupné přes ikonu„⋮“ zobrazenou v seznamu položek, takto:



Obr. 4: Způsob získání vloženého souboru

Soubor lze stáhnout kliknutím na jeho název.

Pozn.:

- pokud má položka přílohu, je v seznamu položek za jejím názvem doplněna ikona .
- přítomnost ikon a Delete případně „ADD NEW ATTACHMENT“ působí dojmem, že každý má oprávnění soubory odstraňovat a přidávat – není tomu tak, aplikace Vaultwarden tyto akce odmítne.

3 Význam předávaných dat

Tato kapitola popisuje obsah a význam dat předávaných v jednotlivých kolekcích aplikace Vaultwarden.
Pozn.: Název kolekce vždy obsahuje i APN – toto je zásadní pro případ, že by uživatel byl Zástupcem pro více souběžných Atestačních případů.

3.1.1 Kolekce „Časová Razítka“

Kolekce „Časová Razítka“ obsahuje jedinou položku „Časová Razítka eSSL“.

Položka „*Časová Razítka eSSL*“ popisuje přístupové údaje na server poskytující službu časových razítek:

- URL
- Záložní (alternativní) URL
- Uživatelské jméno a heslo (platné pro obě URL)
- Dodatečné informace uložené v textové poznámce

Položka též obsahuje i certifikáty certifikačních autorit eIdentity , uložené jako přílohy. Při instalaci eSSL musíte zajistit, aby volající strana (server nebo Stanice pro klientské operace) měla tyto certifikáty importovány.

3.1.2 Kolekce „Uživatelské účty v eSSL“

Kolekce „Uživatelské účty v eSSL“ obsahuje jedinou položku. Tato položka obsahuje přiložené soubory uživatelských jmen a hesel jednotlivých osob podle testovacích scénářů, a to ve formátu CSV a XLSX.

3.1.3 Kolekce „ISDS“

Kolekce „*ISDS*“ obsahuje přístupy do informačního systému datových schránek. Pro atestace je použit testovací systém ISDS. Kolekce obsahuje následující položky:

- „OVM Primární“ – Primární datová schránka Atestační organizace (typ OVM)
- „OVM Sekundární“ – Další datová schránka Atestační organizace (typ OVM)

Poznámky:

- Aby bylo možné do cílové datové schránky posílat zprávy, musí být aktivovaná. K tomu stačí alespoň jedno přihlášení do cílové datové schránky.
- Základním typem přihlášení do datové schránky je jménem a heslem; tyto údaje jsou uvedeny v příslušné položce.

3.1.4 Kolekce „ISZR“

Kolekce „ISZR“ obsahuje přístupy do informačního systému základních registrů. Pro atestace je zpřístupněn jak testovací, tak i produkční systém ISZR. Kolekce obsahuje následující položky:
Pozn.: „n“ je interní označení přístupu do ISZR zřízeného pro účely atestací eSSL; pro Zástupce a Objednatele se jedná o nepodstatný údaj.

- ISZR *n* - Testovací prostředí – Přístup do testovacího systému ISZR je určen pro případné testování Zástupci pro ověření instalace eSSL.
- ISZR *n* - Produkční prostředí – Přístup do produkčního systému ISZR je určen pro provedení testovacích scénářů testery.

U položek jsou zadány:

- Přístupový certifikát – dostupný v příloze („Attachment“) položky
- Heslo k certifikátu – dostupné v detailu položky

3.1.5 Kolekce „Speciální e-mailové adresy“

Kolekce „Speciální e-mailové adresy“ obsahuje adresy e-mailových schránek a k nim příslušná uživatelská jména a hesla pro speciální e-mailové schránky Atestační organizace, které má vybírat testovaný systém eSSL:

- Asistentka úřadu
- Faktury úřadu
- Podatelna úřadu
- Ředitel úřadu

3.1.6 Kolekce „Elektronické pečetě“

Kolekce „Elektronické pečetě“ obsahuje jedinou položku, která popisuje přístupové údaje do nástroje SecuSign společnosti Software 602 použitý pro elektronické pečetě.

Položka obsahuje:

- URL endpointu služby - uvedené v detailu položky
- Autentizační certifikát - v příloze položky
- Heslo k autentizačnímu certifikátu – uvedené v detailu položky.
  Pozn.: heslo je triviální z důvodu toho, je certifikát sám nese informaci, že je vystaven pouze pro účely testování spisových služeb v rámci Atestačního střediska. Pro daný účel je plně dostačující.
- Technickou dokumentaci a příklady volání služby – v příloze
- Popis nastavení parametru volání služeb – v textové poznámce položky

3.1.7 Kolekce „Technický zástupce Objednatele“

Kolekce „Technický zástupce Objednatele“ obsahuje položky s přístupovými údaji do interního atestačního prostředí pro jednotlivé zástupce Objednatele. Pro každého Zástupce je uveden jeho přístup do interního Active Directory Atestačního střediska. Oproti tomuto Active Directory se ověřuje:

- přístup na VPN,
- přihlášení (administrátorský přístup) se k serverům / Stanici pro klientské operace. Hesla zde uvedená jsou generována Atestačním střediskem jako počáteční a Atestační středisko doporučuje si je změnit. Změnu lze provést z libovolného virtualizovaného stroje, který je součástí Interního atestačního prostředí. Nové heslo je zapsáno do Active Directory Atestačního střediska, tedy následně bude třeba se do VPN přihlašovat novým heslem; nedojde však ke změně hesla v aplikaci Vaultwarden.

V textové části pak položky obsahují IP adresy požadovaných virtualizovaných serverů a Stanice pro klientské operace.

3.1.8 Kolekce „VPN Instalátor“

Kolekce „VPN Instalátor“ obsahuje jedinou položku. Tato položka obsahuje:

- URL endpointu VPN (https://vpn.agentura-cas.cz/eSSL) – v poli URL v detailu položky
- Instalační soubory VPN klienta pro jednotlivé operační systémy – v přílohách položky

Přístup prostřednictvím VPN je popsán v následující kapitole.

4 Způsob předání důvěrných údajů Atestačnímu středisku

V předchozích kapitolách je popsán způsob předávání údajů ze strany Atestačního střediska směrem k Zástupcům. Tato kapitola popisuje způsob předávání dat v obráceném směru.

Objednatel prostřednictvím Zástupců za použití aplikace Vaultwarden předává Atestačnímu středisku důvěrné údaje uvedené v kap. 6 *„Předání Atestačního prostředí Atestačnímu středisku po dokončení instalace eSSL“* dokumentu *„Provozní řád Atestačního střediska – Část 1: Metodika přípravy Atestačního prostředí“*.

Způsob předání pro jednotlivé důvěrné údaje uvedené v kap. 6 výše zmíněného dokumentu:

1. Údaje požadované formulářem „Předávací protokol nainstalovaného eSSL“.

   Formulář zašlete Atestačnímu středisku (datovou schránkou)

2. Úplné přístupové údaje pro jednotlivé vytvořené uživatelské účty eSSL, včetně přehledu uživatelských rolí a jejich charakteristiky, a přehledu správcovských rolí – platí v případě, že Objednatel nevyužil možnost autentizace testovacích uživatelských účtů zaměstnanců Atestační organizace prostředky Active Directory Atestačního střediska a z tohoto důvodu vytvořil uživatelské účty zaměstnanců Atestační organizace vlastními prostředky.

   Pokud je pro vás tento požadavek relevantní, vytvořte vhodný soubor (např. CSV, případně Microsoft Excel), nazvěte jej „Přístupové údaje pro uživatelské účty eSSL“ na uložte jej na disk O:\ Stanice pro klientské operace.

3. Uživatelská příručka eSSL, Příručku pro správu eSSL a dokument *„Návod pro realizaci testovacích scénářů pro provedení atestace“*

   Uvedené dokumenty uložte na disk O:\ Stanice pro klientské operace.

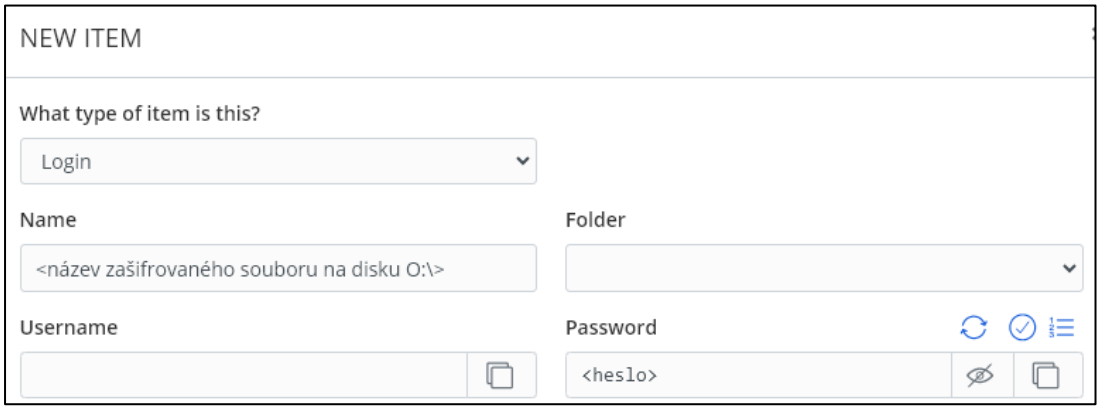
4. Jednorázová záloha (export) Atestačního prostředí a s ní související údaje

   Pozn.: tento požadavek je relevantní pouze v případě, pokud byla pro provedení atestace zvolena varianta B) nebo C) podle čl. 5 dokumentu „Postup Atestačního střediska.“

   Vytvořený export virtualizovaných serverů (případně docker images) zašifrujte, a zašifrované soubory uložte na disk O:\ Stanice pro klientské operace. Heslo k nim předejte prostřednictvím aplikace Vaultwarden takto:

   - V kolekci „*Údaje předávané Atestačnímu středisku*“ založte vhodně pojmenovanou položku
   - Do pole “Name” zadejte název zašifrovaného souboru na disku O:\ Stanice pro klientské operace
   - Vyplňte její heslo

   Příklad vyplnění formuláře nově založené položky:



   Pozn.: ostatní položky nemusíte vyplňovat

5 Upozornění

1. Abyste mohli do Atestačního prostředí instalovat testovaný eSSL, má Váš uživatelský účet práva lokálního administrátora. Přihlašovací údaje jsou přitom vedené centrálně v Active Directory Atestačního střediska. Důsledkem je, že pokud si změníte heslo na libovolném virtualizovaném stroji, uplatní se tato změna pro celý záznam vašeho uživatelského účtu v Active Directory, tedy pro všechny virtualizované stroje i pro přístup prostřednictvím VPN(!). Přitom nedojde k odpojení VPN, avšak při v příštím připojení prostřednictví VPN již musíte zadat nové heslo.
2. Uživatelské účty, které vám jsou přiděleny na virtualizovaných strojích Atestačního střediska, jsou plně ve vaší zprávě, a pracovníci atestačního střediska je nevyužívají. Pokud by však z nějakých důvodů bylo potřeba tyto účty využít, vyhrazuje si atestační středisko právo na změnu hesla u těchto účtů.
3. Testovaný eSSL, instalovaný na Stanici pro klientské operace, musí být instalován pro všechny uživatele operačního systému, nikoliv pouze pro uživatele přihlášeného v době instalace; v opačném případě by tento klient nebyl dostupný pro roli testera.