



V Trutnově 16. srpna 2022

Vážený pane, [REDACTED],

zasíláme Vám nabídku ReadEn zvýšení zabezpečení.

Tuto nabídku předkládáme na základě Vaší výzvy.

V případě potřeby jakéhokoliv upřesnění či dotazů jsme připraveni doplnit potřebné informace a projednat Vaše dotazy a připomínky.

Doba platnosti této nabídky je do **31. října 2022**.

[REDACTED]  
Vedoucí oddělení programování

Tel. [REDACTED]

E-mail: [REDACTED]

Mobil: [REDACTED]

[REDACTED]  
Programátor

Tel. [REDACTED]

E-mail: [REDACTED]

Mobil: [REDACTED]

### Identifikační údaje o dodavateli:

Název společnosti:

**ZPA Smart Energy, a. s.**

se sídlem:

Komenského 821, 541 01 Trutnov

právní forma:

akciová společnost

zastoupená:

[REDACTED]  
členem představenstva a obchodně-technickým ředitelem

IČ:

27445976

DIČ:

CZ [REDACTED]

Bankovní spojení:

Československá obchodní banka, a.s.

pobočka pro korporátní klientelu

Ulrichovo náměstí 735

502 00 Hradec Králové

č.ú.: [REDACTED]

Telefon:

+ [REDACTED]

ID datové schránky:

ez4g6xa

web:

[REDACTED]

E-mail:

[REDACTED]

Společnost je zapsána v obchodním rejstříku vedeném krajským soudem v Hradci Králové oddíl B, vložka číslo 2851.

Kontaktní osoba ve věcech obchodních:

[REDACTED]  
Prodej AMM/AMR systémů

Tel.: [REDACTED]

Mobil: [REDACTED]

E-mail: [REDACTED]

## 1 Úvodem

Měřicí ústředna založená na klient-server-server systému ReadEn je ve společnosti Zadavatele provozována od roku 2013. Systém je provozován na infrastruktuře Zadavatele (On Premise) s aktivní smlouvou o podpoře ze strany Dodavatele.

Databáze ústředny má velikost ~800 GB, obsahuje historii systému od roku 2000, zejména odečty, spotřeby a vstupní údaje – pulsy z napojených odečtových systémů.

Systém obsahuje dvě různé klientské aplikace.

**Tlustý klient** je využíván zejména správci měřicí ústředny, využívá vlastní sadu bezpečnostních rolí, definovaných v aplikaci (konstantní aplikační sada rolí). Využívá doménové uživatelské účty.

Sadu rolí i seznam uživatelů je spravován ve spolupráci s podporou Dodavatele. Změna rolí vyžaduje úpravu zdrojového kódu klienta.

**Tenký klient**, používaný zejména provozními pracovníky, využívá vlastní sadu bezpečnostních rolí, definovaných správcem databáze (dynamická databázová sada rolí). Využívá vlastní sadu uživatelských účtů.

Sadu rolí i seznam uživatelů je spravován zástupci Objednatele.

Požadavky Zadavatele směřují na zvýšení zabezpečení obou klientů.

Je požadováno nasadit v tlustém klientovi obdobný systém rolí, jako v tenkém klientovi, který bude spravován zástupci Zadavatele a v souladu s požadavky interních předpisů Zadavatele (SŽ).

Je požadováno nasadit v tenkém klientovi politiku hesel v souladu s požadavky interních předpisů Zadavatele (SŽ).

Tato nabídka pokrývá také požadavky uvedené v Helpdesk systému ReadEn:

0000007 [REDACTED] ReadEn 2 tenký Klient  
**Kybernetická bezpečnost – zadání pro tenkého klienta**

0000028 [REDACTED] ReadEn 2 tlustý klient  
**Vytvoření nové role se specifickým oprávněním**

### 1.1 Návrh řešení – stručně

Navrhujeme implementovat do tlustého klienta komplexní strategie bezpečnosti včetně správcem (Zadavatel) definovaných pravidel na kybernetickou bezpečnost obecně.

Navrhujeme změnit pro tenkého klienta komplexní strategie bezpečnosti tak, aby politika hesel odpovídala Zadavatelem definovaných pravidel na kybernetickou bezpečnost hesel.

Detailní popis nabízených změn naleznete v kapitole Popis nabízeného řešení.

## 2 Cenová nabídka

Předmětem dodávky je výhradně práce dodavatele na dálku, předmětem dodávky není například školení uživatelů, prezentace řešení a podobně. Předmětem nabídky je účast zástupců dodavatele na nezbytném počtu projektových schůzí v sídle zadavatele. Další služby lze objednat.

Platební podmínky – splatnost faktury 31 dnů od doručení. Veškeré uvedené ceny jsou bez DPH.

Položka	h	Cena/h	Cena
Tlustý klient, implementace komplexní strategie bezpečnosti, role definované správcem v souladu s interními předpisy.	168	1 150 Kč	193 200,00 Kč
Tenký klient, úprava komplexní strategie bezpečnosti, politika hesel dle interních předpisů.	82	1 150 Kč	94 300,00 Kč
Testy a společné ladění řešení.	24	1 150 Kč	27 600,00 Kč
Školení klíčových uživatelů.	16	1 150 Kč	18 400,00 Kč
Školení ostatních uživatelů.	0	1 150 Kč	0,00 Kč
Aktualizace dokumentace SW.	28	1 150 Kč	32 200,00 Kč
	0	1 150 Kč	0,00 Kč
	0	1 150 Kč	0,00 Kč
<b>CELKEM</b>			365 700,00 Kč

## 3 Časový harmonogram

Dodací lhůta 14 týdnů po objednání.

	Týdnů
Implementace	08
Testy, školení, uvedení do produkčního provozu	03
Zvýšený dohled podpory a společné odsouhlasení řešení	03
	00

## 4 Záruka, podpora

Servisní činnost bude zahájena ihned po předání navrhovaného řešení do produktivního provozu.

Servisní činnost bude prováděna na základě stávající servisní smlouvy na systém ReadEn, za podmínek této smlouvy, a to bez navýšení ceny.

## 5 Součinnost

Součinnost vyžaduje standardní spolupráci, jak je nastavená při provozu a podpoře stávající Měřicí ústředny, zejména vzdálený přístup dodavatele do vybrané části sítě zadavatele.

## 6 Popis nabízeného řešení, cílový koncept.

### 6.1 Současný stav

Bezpečnostní systém tlustého klienta, zejména autorizační část (systém rolí) neumožňuje reagovat na měnící se požadavky na oprávnění jednotlivých uživatelů.

Bezpečnostní systém tenkého klienta používá dostatečně rozvinutý komplexní systém zabezpečení, včetně správy rolí a uživatelů, ale politika hesel, požadavky na složitost a změnu hesla je nedostatečná.

### 6.2 Navrhované změny

Implementovat v obou klientech stejný komplexní systém zabezpečení spolu se silnou politikou hesel.

Hesla v bezpečnostním systému

Popis nástrojů pro generování a změnu uživatelských hesel při použití ověřování.

Šifrování hesla

Vestavěné třídy neukládají heslo jako prostý text. Místo toho je odvozený hash vytvořen z hesla pomocí třídy SHA512 (nebo Rfc2898DeriveBytes).

Nové pravidla pro hesla

Minimální délka hesla je 12 znaků (v případě privilegovaných a technologických účtů 19 znaků).

Heslo obsahuje alespoň 3 z následujících skupin znaků:

nejméně jedno velké písmeno (A – Z)

nejméně jedno malé písmeno (a – z)

nejméně jednu číslici (0 – 9)

nejméně jeden speciální nealfanumerický znak (~!@#\$%^&\* \_-+=`|\(){}[];:'"<>,.?/)

Uživatel je povinen měnit svá hesla minimálně každých 365 dní.

Stejně heslo se nesmí opakovat v historii 12-ti posledních hesel.

Zabezpečení (řízení přístupu a ověřování)

Popis typů oprávnění systému zabezpečení. Konfigurace oprávnění se provádí v roli a role přiřazuje oprávnění uživateli. Každý uživatel by měl mít alespoň jednu roli.

Systém zabezpečení kontroluje oprávnění pro každou roli a určuje přístupová práva.

Oprávnění jedné role neovlivňují oprávnění jiné role. Pokud má uživatel několik rolí, bezpečnostní systém důsledně kontroluje oprávnění každé role. Systém zabezpečení sloučí výsledky těchto kontrol dle strategie „Uděleno v jakékoli roli“. To znamená, že uživatel může provést operaci, pokud alespoň jedna z uživatelských rolí tuto operaci umožňuje.

Přehled systému autorizace

Popis typu oprávnění, které jsou k dispozici v systému bezpečnosti implicitně.

Oprávnění nejsou přiřazena uživatelům přímo. Každý uživatel by měl mít alespoň jednu roli s patřičnou sadou přiřazených oprávnění.

#### Role Administrátor

Volba "Je administrativní" má zjednodušovat definici neomezeného přístupu a přiřazuje roli všechna možná oprávnění. Pokud je role administrativní, nelze jí upřít jakákoli práva, dokud administrativní oprávnění není odejmuto.

#### Oprávnění pro typy (entity)

Typ oprávnění specifikuje přístup ke všem objektům specifického typu (ke všem záznamům určité tabulky). Následující typy operací mohou být povolené nebo zamítnuté.

Operace	Popis
Číst	Objekty daného typu jsou ke čtení. Abyste určili objekt pouze ke čtení, zaškrtněte operaci Číst a odškrtněte operaci Psát.
Psát	Objekty daného typu lze upravovat.
Vytvořit	Nové objekty daného typu lze vytvořit. Pozor, umožnit Vytvořit bez umožnění Psát nedovoluje uložit nové objekty.
Vymazat	Objekty daného typu lze mazat.
Navigovat	Pohledy, které zobrazují objekty daného typu mohou být otevřeny Navigačním Systémem. Pokud operace Navigace není povolena, příslušná položka navigace není dostupná.

#### Oprávnění pro členy (položky, sloupce)

Oprávnění pro členy umožňuje přístup k určitým členům objektu (k určitým sloupcům určité tabulky).

Pokud má uživatel přístup Psát pro určitý typ, pak všechny členy lze přepisovat. K povolení přístupu k určitým členům, odstraňte oprávnění psát na úrovni typu a povolte to určeným členům. To samé platí pro operaci Číst. Je možné povolit přístup k více vlastnostem s jediným vstupem – hodnota členů může být seznamem názvů vlastností oddělených středníkem.

Lze také specifikovat kritérium pro přístup oprávnění pro členy. Přístup může být aktivován v případě, že aktuální objekt splní dané kritérium.

Všechna oprávnění pro operace se členy jsou považována jako povolené, pokud je operace povolena pro celý objekt.

Pokud je vytvořen nový objekt (a stále ještě není uložen), oprávnění člena neovlivňuje stav povolení/nepovolení editace. Nicméně při ukládání se oprávnění projeví správně. Můžete použít modul Podmíněné zobrazení, abyste znemožnili editování nového objektu.

#### Oprávnění pro objekty (řádky)

Oprávnění pro objekty povoluje přístup pro instance objektů (k určitým řádkům určité tabulky), které splňují specifické kritérium.

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

**Doložka číslo:** 2963190

**Původní datový formát:** application/pdf

**UUID původní komponenty:** bc708a5c-3bd6-48b4-9afd-d9aac3483beb

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

System ERMS (zpracovatel dokumentu Miriam HEMZOVÁ)

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

**Datum vyhotovení ověřovací doložky:** 31.08.2022 15:44:05



075960a7-1ee0-42b0-b6df-b8f394c304d5