KUPNÍ SMLOUVA

uzavřená níže uvedeného dne, měsíce a roku

dle ustanovení § 2079 a násl. a § 2085 a násl. zákona č. 89/2012 Sb., Občanského zákoníku

Čl. 1 Smluvní strany

Kupující: **Vyšší odborná škola a Střední průmyslová škola elektrotechnická, Plzeň, Koterovská 85**

Sídlo:	Koterovská 828/85, Plzeň
IČ:	49774301
DIČ:	CZ49774301
Zastoupený:	Ing. Naděžda Mauleová, statutární zástupkyně
Kontaktní osoba:	Bc. Pavel Sobotka, vedoucí správy počítačové sítě
	tel. +420 377 418 073
	email: sobotka@spseplzen.cz

jako kupující, na straně jedné

(dále jen kupující)

a

Prodávající: **Továrna na dokonalé programy, s.r.o.**

Sídlo:	Bohúňova 1336/13, Chodov, 149 00 Praha 4
IČ:	45272638
DIČ:	CZ45272638
Zastoupený/Jednající:	Ing. Václav Šamša, jednatel
Kontaktní osoba:	Bc. Jana Dvořáková, Marketing & Account Manager
	tel. +420 724 717 657; e-mail: jdvorakova@tdp.cz
Bankovní spojení:	Komerční banka Praha 4
Číslo účtu:	844 345 041/0100

Zápis v OR: vedený u Městského soudu v Praze, spisová značka C9211

jako prodávající na straně druhé

(dále jen prodávající)

Čl. 2 Úvodní ustanovení

2.1. Tato smlouva je uzavírána v návaznosti na veřejnou zakázku s názvem „Kybernetická bezpečnost na VOŠ a SPŠE Plzeň – dodávka řešení dvoufaktorové autentizace a správy privilegovaných účtů“, zadávanou kupujícím jakožto zadavatelem.

2.2. Technická specifikace kupujícího (zadavatele) k veřejné zakázce a technická specifikace z nabídky prodávajícího tvoří nedílnou součást této smlouvy jako její přílohy.

2.3. Detailní technická specifikace předmětu plnění této smlouvy je obsažena v příloze č. 1 a č. 2 této smlouvy a je její nedílnou součástí. V případě rozporu vzniklého mezi přílohami č. 1 a 2

této smlouvy v podobě technické specifikace platí vždy specifikace kupujícího obsažená v příloze č. 1 této smlouvy.

Čl. 3 Předmět smlouvy

3.1. Předmětem této smlouvy je nehmotný majetek v podobě licencí SW dvoufaktorové autentizace a SW správy privilegovaných účtů a dále hmotný majetek v podobě příslušenství (čtečky karet). Předmět smlouvy je detailně specifikován v příloze č. 1 této smlouvy, včetně příslušenství. Prodávající je tímto povinen odevzdat kupujícímu licence, a umožnit mu ničím nerušené užívání software a současně závazek kupujícího licence převzít a zaplatit za ně prodávajícímu kupní cenu.

3.2. Součástí předmětu plnění jsou dále služby a práce prodávajícího s licencemi přímo související a nezbytné k řádnému uvedení předmětu plnění do provozu, které jsou blíže specifikovány v příloze č. 1 této smlouvy. Jedná se zejména o instalaci, dodávku dokumentace a zaškolení administrátorů kupujícího.

3.3. Prodávající se zavazuje dodat předmět smlouvy kupujícímu s veškerými doklady nutnými k převzetí a zejména k užívání dodaného software.

3.4. Prodávající touto smlouvou prodává kupujícímu do výlučného vlastnictví předmět kupní smlouvy definovaný v bodě 3.1 a to včetně příslušenství.

3.5. Kupující předmět plnění této smlouvy, jímž jsou věci nové a nepoužité, kupuje za dohodnutou kupní cenu a přijímá do svého výlučného vlastnictví.

3.6. Prodávající prohlašuje, že neví ke dni podpisu této kupní smlouvy o žádných vadách prodávaných věcí, na které by kupujícího upozornil.

Čl. 4 Licence

4.1. Prodávající v rámci plnění předmětu této smlouvy dodává software podléhající ochraně podle zákona č. 121/2000 Sb. (autorský zákon) a ustanovení § 2358 a následující zákona č. 89/2012, občanského zákoníku, proto poskytuje kupujícímu licenci (tj. oprávnění k výkonu práva duševního vlastnictví (licenci) v rozsahu obvyklém), a to formou licenčního ujednání v této kupní smlouvě.

4.2. Licence je poskytnutá v maximálním rozsahu povoleném platnými právními předpisy.

4.3. Prodávající prohlašuje, že odměna za poskytnutí licence kupujícímu je již zahrnuta v kupní ceně za poskytnuté plnění dle této kupní smlouvy.

Čl. 5 Kupní cena a platební podmínky

5.1. Kupní cena je nabídkovou cenou předloženou prodávajícím v jeho nabídce na veřejnou zakázku uvedenou v článku 2.1 této smlouvy, přičemž se skládá z ceny dodávky licencí a příslušenství.

5.2. Kupující se zavazuje zaplatit prodávajícímu za předmět spočívající v dodávce plnění uvedený v Čl. 3 této smlouvy kupní cenu ve výši

595 600 Kč bez DPH,

tj. 720 676 Kč včetně DPH,

když DPH ve výši 21% činí 125 076 Kč.

5.3. Kupní cena je stanovena jako cena konečná a úplná, zahrnuje veškeré dodávky a služby s dodávkami související a veškeré jiné náklady nezbytné pro řádnou a úplnou realizaci předmětu plnění této smlouvy včetně všech rizik a vlivů s plněním předmětu této smlouvy souvisejících. Kompletní skladba kupní ceny a její rozklad je obsažen v příloze č. 3 této smlouvy.

5.4. Prodávající není oprávněn požadovat po kupujícím poskytnutí zálohy.

5.5. Prodávající na sebe bere odpovědnost za to, že sazba a výše daně z přidané hodnoty bude stanovena v souladu s platnými právními předpisy. V případě, že dojde mezi dnem podpisu kupní smlouvy a dnem uskutečnění zdanitelného plnění ke změně sazby DPH podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, bude daň z přidané hodnoty připočtena ke kupní ceně ve výši dle právní úpravy platné ke dni uskutečnění zdanitelného plnění.

5.6. Kupní cenu zaplatí kupující prodávajícímu bankovním převodem na bankovní účet prodávajícího uvedený v článku 1 této smlouvy na základě daňového dokladu (faktury) vystaveného prodávajícím ke dni uskutečnění zdanitelného plnění, který je dnem podepsání předávacího protokolu na předmět plnění dle této smlouvy. Daňový doklad je považován za proplacený okamžikem odepsání příslušné částky z účtu kupujícího ve prospěch účtu prodávajícího.

5.7. Na daňovém dokladu (faktuře) bude uveden rozklad fakturované částky za jednotlivé licence a příslušenství, tak aby bylo kupujícímu usnadněno zavedení do majetkové evidence.

5.8. Splatnost daňového dokladu je 30 dnů ode dne jeho doručení kupujícímu.

5.9. Daňový doklad bude obsahovat náležitosti daňového a účetního dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, bude mít náležitosti obchodní listiny dle § 435 zákona č. 89/2012 Sb., občanského zákoníku. V případě, že daňový doklad takové náležitosti nebude splňovat, bude kupujícím vrácen do dne splatnosti daňového dokladu k opravení bez jeho proplacení. V takovém případě lhůta splatnosti počíná běžet znovu ode dne doručení opraveného či nového vyhotovení daňového dokladu.

5.10. Všechny faktury dle této kupní smlouvy musí obsahovat odpovídající název a registrační číslo projektu IROP v10 "Název projektu: Kybernetická bezpečnost na VOŠ a SPŠE Plzeň, registrační číslo projektu: CZ.06.3.05/0.0/0.0/15_011/0006791".

5.11. Pro případ, že prodávající je, nebo se od data uzavření smlouvy do dne uskutečnění zdanitelného plnění stane na základě rozhodnutí správce daně „nespolehlivým plátcem" ve smyslu ustanovení § 106a zákona č. 235/2004 Sb., o DPH, ve znění pozdějších předpisů, souhlasí prodávající s tím, že mu kupující uhradí cenu plnění bez DPH a DPH v příslušné výši odvede za nespolehlivého plátce přímo příslušnému správci daně. V souvislosti s tímto ujednáním nebude prodávající vymáhat od kupujícího část z ceny plnění rovnající se výši odvedeného DPH a souhlasí s tím, že tímto bude uhrazena část jeho pohledávky, kterou má vůči kupujícímu a to ve výši rovnající se výši odvedené DPH.

Čl. 6 Předání a převzetí věci a vlastnické právo

6.1. Prodávající předá kupujícímu předmět plnění této smlouvy do osmy (8) týdnů od uzavření této smlouvy.

6.2. Místem dodání a předání předmětu plnění této smlouvy je adresa sídla kupujícího Koterovská 828/85, Plzeň.

6.3. Vlastnické právo k předmětu plnění přechází na kupujícího v okamžiku jeho předání prodávajícím a převzetí kupujícím potvrzeného na předávacím protokolu.

6.4. Nebezpečí nahodilé zkázy a nahodilého zhoršení vlastností předmětu plnění včetně užitku přechází na kupujícího současně s nabytím vlastnictví.

6.5. Náklady spojené s předáním předmětu plnění nese prodávající a náklady spojené s převzetím nese kupující.

6.6. O předání a převzetí předmětu plnění a souvisejících dokladů bude sepsán předávací protokol podepsaný zástupci obou smluvních stran. Za kupujícího je předávací protokol oprávněn podepsat a předmět plnění převzít kontaktní osoba kupujícího uvedená v článku 1. této smlouvy.

Čl. 7 Další práva a povinnosti smluvních stran

7.1. Prodávající je povinen uchovávat veškerou dokumentaci související s realizací projektu (předmětu plnění této smlouvy) včetně účetních dokladů minimálně do konce roku 2028.

7.2. Prodávající je povinen minimálně do konce roku 2028 poskytovat požadované informace a dokumentaci související s realizací projektu (předmětu plnění této smlouvy) zaměstnancům nebo zmocněncům pověřených orgánů (CRR, MMR ČR, MF ČR, Evropské komise, Evropského účetního dvora, Nejvyššího kontrolního úřadu, příslušného orgánu finanční správy a dalších oprávněných orgánů státní správy) a je povinen vytvořit výše uvedeným osobám podmínky k provedení kontroly vztahující se k realizaci projektu (předmětu plnění této smlouvy) a poskytnout jim při provádění kontroly součinnost.

Čl. 8 Práva z vadného plnění a smluvní záruka

8.1. Záruka na software, který je předmětem plnění této smlouvy, a na příslušenství, počíná svůj běh dnem jejich předání kupujícímu na základě řádně oběma smluvními stranami podepsaného předávacího protokolu.

8.2. Na příslušenství bude prodávajícím poskytována záruka v délce dvou (2) let. V případě vad takového příslušenství se prodávající zavazuje provést opravu nebo věc nahradit novou v sídle kupujícího do 30 kalendářních dnů ode dne nahlášení vady kupujícím.

8.3. Prodávající odpovídá kupujícímu za to, že dodaný předmět smlouvy bude mít vlastnosti zabezpečující jeho řádné užívání, stanovené v minimální konfiguraci v technické specifikaci kupujícího a v konečné konfiguraci ve specifikaci obsažené v nabídce prodávajícího.

8.4. Prodávající odpovídá kupujícímu dále za to, že dodaný předmět smlouvy bude mít vlastnosti zabezpečující jeho řádné užívání a že je bez právních a faktických vad. Dále prodávající zaručuje, že na dodaném předmětu smlouvy neváznou práva třetích osob.

8.5. Vady musí kupující uplatnit u prodávajícího bez zbytečného odkladu poté, co se o nich dozví.

8.6. Uplatněním práv z odpovědnosti za vadné plnění není dotčeno právo kupujícího na náhradu škody.

Čl. 9 Smluvní pokuty

9.1. Pro případ prodlení se zaplacením kupní ceny se kupující zavazuje uhradit prodávajícímu smluvní pokutu ve výši 0,01 % z fakturované ceny za každý den prodlení.

9.2. Pro případ prodlení prodávajícího s dodávkou předmětu plnění této smlouvy v rozsahu a termínech uvedených v této smlouvě se stanovuje smluvní pokuta ve výši 0,1 % z hodnoty dodávky za každý den prodlení.

9.3. V případě prodlení prodávajícího s odstraněním nahlášené závady na příslušenství se stanovuje smluvní pokuta ve výši 200 Kč za každý celý kalendářní týden prodlení.

9.4. Zaplacením smluvní pokuty nezaniká povinnost druhé strany závazek splnit a není tím dotčeno právo poškozené strany na náhradu škody, které nesplněním povinnosti vznikla.

9.5. Výši smluvních pokut shodně považují obě smluvní strany za přiměřené. Smluvní pokuta je splatná do 30 dnů od doručení jejího vyúčtování.

Čl. 10 Odstoupení od smlouvy

10.1. Odstoupení od smlouvy se řídí ustanoveními § 223 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, a dále § 2001 a násl. zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů.

10.2. Nebude-li uhrazena kupní cena do 60 dnů ode dne splatnosti daňového dokladu prodávajícímu v důsledku zavinění kupujícího a ani do dalších 15 dnů po opakovaném vyzvání prodávajícím k takové úhradě, sjednává si prodávající právo odstoupit od této kupní smlouvy.

10.3. Právo odstoupit od této kupní smlouvy má kupující tehdy, jestliže jej prodávající ujistil, že předmět plnění této smlouvy má určité vlastnosti, zejména vlastnosti kupujícím vymíněné, anebo prodávající kupujícího ujistil, že předmět plnění této smlouvy nemá žádné vady, a toto ujištění se ukáže být nepravdivým.

Čl. 11 Registr smluv – doložka

11.1. Prodávající tímto uděluje souhlas kupujícímu k uveřejnění všech podkladů, údajů a informací uvedených v této smlouvě, k jejichž uveřejnění vyplývá pro kupujícího povinnost dle právních předpisů.

11.2. Prodávající je současně srozuměn s tím, že kupující je oprávněn zveřejnit obraz smlouvy a jejich případných změn (dodatků) a dalších dokumentů od této smlouvy odvozených včetně metadata požadovaných k uveřejnění dle zákona č. 340/2015 Sb., o registru smluv.

11.3. Zveřejnění smlouvy a metadata v registru smluv zajistí kupující.

Čl. 12 Závěrečná ustanovení

12.1. Tato smlouva je vyhotovena ve čtyřech (4) výtiscích, každý s platností originálu. Smluvní strany obdrží po dvou vyhotoveních.

12.2. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti uveřejněním v registru smluv.

12.3. Právní vztahy touto smlouvou výslovně neupravené a s ní související nebo z ní vyplývající se řídí ustanoveními zákona č. 89/2012 Sb., občanského zákoníku.

12.4. Přílohami této smlouvy jsou:

- Příloha č. 1 – Technická specifikace zadavatele (kupujícího)
- Příloha č. 2 – Technická specifikace účastníka zadávacího řízení (prodávajícího) z jeho vítězné nabídky, včetně jednotkových cen zařízení
- Příloha č. 3 – Cenová tabulka obsahující skladbu nabídkové ceny z nabídky prodávajícího

12.5. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly a s celým jejím obsahem souhlasí. Dále prohlašují, že tato smlouva vyjadřuje jejich pravou a svobodnou vůli. Na důkaz toho připojují vlastnoruční podpisy na smlouvě.

Za kupujícího

V Plzni dne 29.11.2018

VYŠŠÍ ODBORNÁ ŠKOLA
A STŘEDNÍ PRŮMYSLOVÁ ŠKOLA
ELEKTROTECHNICKÁ

Ing. Naděžda Mauleová, MBA

statutární zástupkyně

Za prodávajícího

V Plzni dne 28/11/2018

Ing. Václav Šamša

jednatel

Příloha č. 2 Výzvy – Technická specifikace (dokumentace) veřejné zakázky
Příloha č. 1 Kupní smlouvy – Technická specifikace (dokumentace) veřejné zakázky

„Kybernetická bezpečnost na VOŠ a SPŠE Plzeň – dodávka řešení dvoufaktorové autentizace a správy privilegovaných účtů“

v rámci projektu „Kybernetická bezpečnost na VOŠ a SPŠE Plzeň“

1 Technická specifikace

Objednatel požaduje dodávku jednotlivých komponent dle této technické dokumentace včetně příslušenství v níže uvedené minimální specifikaci. Předmětem plnění je zejména:

- dodávka řešení dvoufaktorové autentizace,
- řešení správy privilegovaných účtů,
- příslušenství v podobě čteček.

Uvedení konkrétních označení a názvů

Pokud tyto zadávací podmínky obsahují požadavky nebo přímé či nepřímé odkazy na určité dodavatele nebo výrobky, nebo patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu, pak je to z důvodů, že se jedná o stávající zařízení v majetku zadavatele a systémy, se kterými musí být nabízené vybavení kompatibilní. V ostatních případech, pokud by se v některé části ZP takové požadavky nebo přímé či nepřímé odkazy na určité dodavatele nebo výrobky, nebo patenty na vynálezy, užitné vzory, průmyslové vzory, ochranné známky nebo označení původu vyskytly, pak je to z důvodů, že stanovení technických podmínek jiným způsobem nemůže být dostatečně přesné a srozumitelné. V každém takovém případě je v souladu s § 89 odst. 6 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, v platném znění, možné nabídnout i jiné, rovnocenné řešení.

1.1 Řešení dvoufaktorová autentizace

Dodané řešení dvoufaktorová autentizace umožní, aby ověření identity člověka bylo provedeno více na sobě nezávislými faktory – (1) něco vím (heslo), (2) něco mám (karta).

1.1.1 Popis základních požadovaných funkcionalit

Jako obecné základní a minimální požadavky na funkcionalitu řešení lze (mimo výše uvedených) definovat následující:

Dvoufaktorová autentizace
Dodávka řešení dvoufaktorové autentizace pracující s unikátními identifikátory (čísly čipů), kompatibilita řešení se stávajícím řešením (v rámci školy jsou zaměstnanci vybaveni kartami se standardem Mifare / DESFire).
Ovládání zamykání, odemykání, přihlašování a odhlašování pomocí karty.
Odemčení v omezeném časovém úseku musí být možné bez zadávání hesla, pouze kartou.
Odemčení stanice do 1 sec od přiložení karty nebo zadání hesla pokud vyprší doba, po kterou lze odemknout jen kartou.
Integrovaná správa karet, každý uživatel může mít neomezený počet trvale a dočasně přiřazených karet.
Možnost změnit vlastní heslo uživatele pomocí klienta autentizačního systému.
Přístupová práva uživatelů pro správu karet zvlášť pro trvale a pro dočasně přiřazené.
Audit práce s kartami, přiřazování/odebírání.
Neomezený počet zdrojů identit použitý v témže čase.
Podpora práce s více replikami nebo kontrolery v témže čase, tzv. High Availability funkce (ošetření výpadku jednoho nebo více konfigurovaných zdrojů.
Load balancing – vyvažování zátěže replik nebo kontrolerů pro dosažení vyššího výkonu.
Vyhledávání uživatelů podle více atributů (uživatel může jako své jméno zadat například jméno účtu, email adresu, osobní číslo).

Funkce SLO musí pracovat bez prodlevy a spolehlivě i v případe, že uživatel počítač nebo zařízení vypne, uspí nebo odpojí.
Podpora automatické autentizace podle přihlášení uživatele klientem OES for Windows.
Možnost autentizace z Windows, Linux, MacOSX, iOS a Android zařízení.
Podpora SAMLv2 – SP initiated SSO, IdP initiated SSO, IdP initiated SLO, neomezený počet definic pro různé SP.
Přímá podpora SAML pro Google, Office365.
Podpora JWT – SP initiated SSO, IdP initiated SSO, IdP initiated SLO, neomezený počet definic pro různé SP.
Podpora Radius Accounting autentizace v režimu client i server.
Neomezený počet Radius Accountng serverů a klientů.
Podpora NAC protokolu, SLO a SSO notifikace http protokolem.
Dynamické přiřazování a odebírání členství ve skupinách pro účely řízení přístupu na internet bez nutnosti modifikovat LDAP zdroj.
Ověřená funkce SSO a SLO se systémy s FortiOS verze 5 a vyšší.
Funkce inteligentní nástěnky, která umožní omezit viditelnost virtuálně připíchnutých zpráv podle jména uživatele v LDAP zdroji, členství ve skupině, IP adresy nebo IP sítě (pro účely zobrazení zprávy pouze pro uživatele v konkrétním segmentu, např. budově nebo patře).
Řešení bude otevřené pro budoucí integrace se SIEM systémy (prostřednictvím standardního protokolu SYSLOG).
Přímá podpora eDirectory, ActiveDirectory, OpenLDAP.
Podpora výrobce software v délce 5 let spočívající zejména v nárocích na opravné verze software a jeho zabezpečení, která bude uhrazena současně s dodávkou.

1.1.2 Integrační vazby

Objednatel požaduje v rámci plnění realizaci vazby na okolní prostředí a to minimálně v níže uvedeném rozsahu. Objednatel na své náklady zajistí přípravu rozhraní na straně systémů, které budou integrovány a případně také nutnou součinnost jejich aktuálních dodavatelů.

Cílová oblast	Vazba do aplikace / systému
SingleSignOn	Integraci lze provést prostřednictvím 4 standardních rozhraní: (1) SAML2, (2) Radius Accounting a (3) eDirectory Network Address Attribute Management a (4) JWT. Integraci je také možné provést prostřednictvím proprietálního REST API rozhraní. Popisy rozhraní jsou dostupné viz. odkazy: http://www.keyshieldsso.com/documentation/keyshield-sso-server-api/ http://www.keyshieldsso.com/developers-corner/documentation/

1.1.3 Koncová zařízení

Objednatel požaduje v rámci předmětu plnění dodávku a plné zprovoznění následujících koncových zařízení:

Název zařízení	Technická specifikace – minimální požadavky

160× čtečka karet	Stolní RFID čtečka karet, kompatibilní a funkční s dodaným SW řešením, Komunikace dle standardu ISO/IEC 14443 Type A 13,56 MHz (Mifare / DESFire), Provedení bez detekce oddálení karty, Rozhraní USB, délka kabelu minimálně 100 cm, Zvuková a světelná indikace korektního přečtení ID karty, Nové, nerepasované zařízení určené pro provoz v České republice. Záruka 2 roky.

1.1.4 Požadavek na rozsah licenčních oprávnění

Zadavatel požaduje dodávku řešení s trvalou licencí, a to

- pro používání řešení pro min. 1.500 souběžně přihlášených uživatelů,
- pro používání řešení dvoufaktorové autentizace pro min. 660 uživatelů (160 zaměstnanců a 500 žáků).

1.2 Řešení správy privilegovaných účtů

Dodané řešení správy privilegovaných účtů (Privilege Identity Management) umožní zajištění vyšší úrovně zabezpečení citlivých údajů organizace pomocí vícenásobných bezpečnostních konceptů, které jsou uvedeny níže v rámci požadavků.

1.2.1 Popis základních požadovaných funkcionalit

Jako obecné základní a minimální požadavky na funkcionalitu řešení lze (mimo výše uvedených) definovat následující:

Automatické nastavení unikátních hesel pro lokální účty (pro účty administrator, admin, root) pro pracovní stanice, notebooky, servery pod operačními systémy Windows, MacOSX a Linux.
Periodické změny hesel k privilegovaným účtům – nastavení hesel musí být automaticky prováděno denně nebo častěji, nezávisle na tom, zda je/není daný účet používaný a nezávisle na tom, zda má/nemá počítač v okamžiku nastavení síťovou konektivitu do prostředí školy.
Nastavení hesel musí být stejným způsobem možné i pro LDAP účty, požadavek na přímou podporu eDirectory a Active Directory.
Možnost zjištění aktuálního hesla daného účtu na konkrétním počítači pouze pro oprávněné uživatele.
Průběžný a okamžitý přenos auditních informací do SYSLOG.
Bezpečné uložení privilegovaných údajů (hesel, klíčů, certifikátů a souborů) tak, aby uživatelé mohli tyto informace bezpečně sdílet nebo naopak aby nebyly dostupné nikomu kromě uživatele, který je uložil (ani správci systému, zálohování atd.).
Správa uživatelů systému musí umožnit kombinaci převzetí z LDAP zdroje (požadavek na podporu eDirectory a Active Directory) a ručního vytvoření a správy (primárně pro externí uživatele).
Součástí řešení musí být konfigurovatelný generátor hesel. Konfigurace musí umožnit nastavení celkové délky hesla a zastoupení znaků (malá/velká písmena, číslice, speciální znaky).
Systém musí mít roli Auditora, který si může zobrazit všechny akce provedené uživateli i nad daty, ke kterým sám nemá přístup. Toto zobrazení nesmí umožnit přístup k datům, pouze k auditním informacím (ty musí zahrnovat identifikaci uživatele, datum, čas a specifikaci místa přístupu – minimálně zdrojovou IP adresu).
Systém musí umožnit uložit až desítky tisíc záznamů, např. hesel, na uživatele. Požadujeme možnost importu existujících citlivých údajů z formátu CSV (tabulkové kalkulátory) a KeePass (rozšířený jednouživatelský password manager).
Komplexní audit při používání privilegovaných účtů (uloženo pro pozdější vyhodnocení).

Řešení musí být dostupné z Windows, Linux, MacOSX, iOS a Android.
Práce se systémem nesní vyžadovat žádné specifické IT znalosti, je určen i pro běžné uživatele (pedagogické i nepedagogické pracovníky školy).
Centrální řízení přístupu k těmto identitám pouze schváleným uživatelům a aplikacím.
Zajištění identifikace a správa všech správcovských účtů.
Poskytování privilegovaných přístupů a hesel k systémům pouze oprávněným administrátorům na základě pověření.
Automatické změny hesel privilegovaných účtu v definovaných časových intervalech.
Podpora výrobce software v délce 5 let spočívající zejména v nárocích na opravné verze software a jeho zabezpečení, která bude uhrazena současně s dodávkou.

1.2.2 Požadavek na rozsah licenčních oprávnění

Zadavatel požaduje dodávku řešení s trvalou licencí, a to

- pro používání řešení správy privilegovaných účtů pro min. 200 uživatelů.

1.3 Dokumentace

Objednatel požaduje v rámci plnění zpracování dokumentace v rozsahu dle tohoto článku v elektronické podobě v českém jazyce.

Uživatelská dokumentace

Zhotovitel dodá uživatelskou dokumentaci, která bude obsahovat základní popis uložení privilegovaných údajů a práci s nimi.

Administrátorská dokumentace

Zhotovitel dodá administrátorskou dokumentaci pro objednatele, která bude obsahovat detailní popis správy a údržby systému.

1.4 Instalace aplikační části systému

Pro instalaci aplikační části systému ze strany dodavatele řešení budou v prostředí počítačové sítě a technologického prostředí ze strany objednatele vyčleněny potřebné odpovídající systémové prostředky v podobě diskového úložiště, procesorového výkonu, operační paměti a instance linuxového CentOS 7 serveru.

1.5 Další požadavky

Zadavatel požaduje v rámci plnění realizaci následujících služeb:

- doprava koncových zařízení (čtečky karet) na adresu Vyšší odborná škola a Střední průmyslová škola elektrotechnická, Koterovská 828/85, Plzeň,
- oživení 10 kusů „vzorových" koncových zařízení,
- instalace SW části do prostředí zadavatele,
- provedení integrace, nastavení a konfigurace systému, ověření funkčnosti dodaného řešení,
- zpracování a předání dokumentace,
- zaškolení administrátorů a klíčových uživatelů na dodané řešení v rozsahu 6 hodin,
- dodávka požadovaných SW licencí.

TDP s.r.o., Oldřichova 52, 128 00 Praha 2
e-mail: tdp@tdp.cz, http://www.tdp.cz
www.keyshieldsso.com; www.secureanybox.com

Příloha č. 2 – Technická specifikace účastníka zadávacího řízení (prodávajícího) z jeho vítězné nabídky, včetně jednotkových cen zařízení

NÁZEV VEŘEJNÉ ZAKÁZKY:

„Kybernetická bezpečnost na VOŠ a SPŠE Plzeň – dodávka řešení dvoufaktorové autentizace a správy privilegovaných účtů".

Popis nabízeného technického řešení – řešení dvoufaktorové autentizace a specifikace čtečky a podpory

V rámci veřejné zakázky je nabídnuto bezpečnostní řešení KeyShield SSO s následující charakteristikou a s uvedením požadavků, které systém splňuje:

KeyShield SSO je čisté IdP (Identity Provider) řešení, které podporuje SAMLv2, JWT, Radius Accounting, NAC a REST API. Na straně uživatelských zdrojů pracuje s protokolem LDAP s přímou podporou pro Active Directory, eDirectory, OpenLDAP a ApacheDS. Počet a kombinace zdrojů není nijak omezena, je možné mít jak více zdrojů stejného nebo různého typu, tak více konektorů do různých částí stromu (lesa) jediného zdroje. ApacheDS je přímo i součástí serveru a lze ho používat jako další zdroj pokud by to, třeba z licenčních důvodů, bylo vhodné.

Uživatelé se autentizují primárně prostřednictvím nativních klientů, které jsou k dispozici pro Windows, Linux, MacOSX, iOS a Android. Samozřejmě, v případě SAMLv2 integrací je možná i přímá autentizace proti serveru z prostředí browseru.

Jedno přihlášení k autentizačnímu systému KeyShield umožní vstup do více systémů = SSO. Uživatel pak již nezadává znovu přihlašovací jméno a heslo k aplikacím, které jsou zintegrované. Integrace je hotová s aplikacemi od společnosti Micro Focus, GINIS od Gordic, Office 365, Kerio mail i firewall, Moodle a s mnoha dalšími.. KeyShield podporuje jakákoliv zařízení s Radius Accounting, lze ho tedy využít pro autentizaci k těmto aktivním prvkům a řídit tak přístup k Internetu, nebo filtrovat obsah.

Pro vyšší bezpečnost je možné pracovat s dvoufaktorovou autentizací za pomoci vhodného předmětu - podporujeme použití od běžných docházkových tokenů/karet až po nejnovější tokeny/karty standardu eIDAS. Klient umožnuje pomocí tokenů session uživatele i ovládat, abychom dosáhli maximální možné efektivity práce uživatele. Bezpečnost dvoufaktorového přihlášení i s obyčejnou vstupní kartou přesahuje mnohonásobně bezpečnost přihlášení pomocí jména a kvalitního hesla. Vůbec obecně je entropie (míra neurčitosti = bezpečnost) hesla o 10 znacích významně vyšší než PINu o standardní délce 4 číslice. Bezpečnost autentizace zásadně zvyšuje i fakt, že uživatelé pracují ze stanic, které má oddělení IT pod kontrolou, ve vnitřním perimetru síťové ochrany. Autentizace probíhá velmi rychle, přečtení karty trvá desítky milisekund.

Pokud uživatel odejde od počítače, může ho jednoduše zcela uzamknout – odejmutím karty nebo velmi snadnou operací – tzv. Walk Away Security. Návrat k zabezpečenému zamknutému počítači a samotná autentizace probíhá buď pouhým přiložením karty nebo přiložením a zadáním hesla pokud již uplynul tzv. Password timeout (ten umožňuje odskočit a vrátit se jen přiložením karty, a to bez hesla). Délku Password timeout si určujete Vy sami.

V případě odhlášení uživatele/skončení práce, notifikuje autentizační systém KeyShield spuštěné aplikace, které podporují SLO (Secure Log Out – bezpečné odhlášení), o této skutečnosti a aplikace provedou bezpečné odhlášení uživatele.

Systém KeyShield SSO splňuje tyto požadavky zadavatele:

- podpora dvoufaktorové autentizace pracující s unikátními identifikátory (čísly čipů)
- KeyShield SSO je kompatibilní se stávajícím řešením školy - v rámci školy jsou zaměstnanci vybaveni kartami se standardem Mifare / DESFire
- ovládání zamykání, odemykání, přihlašování a odhlašování pomocí karty
- odemčení v omezeném časovém úseku musí být možné bez zadávání hesla, pouze kartou
- odemčení stanice do 1 sec od přiložení karty nebo zadání hesla pokud vyprší doba, po kterou lze odemknout jen kartou
- je integrovaná správa karet, každý uživatel může mít neomezený počet trvale a dočasně přiřazených karet
- možnost změnit vlastní heslo uživatele pomocí klienta autentizačního systému
- přístupová práva uživatelů pro správu karet zvlášť pro trvale a pro dočasně přiřazené
- audit práce s kartami, přiřazování/odebírání
- neomezený počet zdrojů identit použitý v témže čase
- podpora práce s více replikami nebo kontrolery v témže čase, tzv. High Availability funkce (ošetření výpadku jednoho nebo více konfigurovaných zdrojů
- Load balancing – vyvažování zátěže replik nebo kontrolerů pro dosažení vyššího výkonu
- vyhledávání uživatelů podle více atributů (uživatel může jako své jméno zadat například jméno účtu, email adresu, osobní číslo)
- funkce SLO pracuje bez prodlevy a spolehlivě i v případe, že uživatel počítač nebo zařízení vypne, uspí nebo odpojí
- podpora automatické autentizace podle přihlášení uživatele klientem OES for Windows
- možnost autentizace z Windows, Linux, MacOSX, iOS a Android zařízení
- podpora SAMLv2 – SP initiated SSO, IdP initiated SSO, IdP initiated SLO, neomezený počet definic pro různé SP
- přímá podpora SAML pro Google, Office365
- podpora JWT – SP initiated SSO, IdP initiated SSO, IdP initiated SLO, neomezený počet definic pro různé SP
- podpora Radius Accounting autentizace v režimu client i server
- neomezený počet Radius Accountng serverů a klientů
- podpora NAC protokolu, SLO a SSO notifikace http protokolem
- dynamické přiřazování a odebírání členství ve skupinách pro účely řízení přístupu na internet bez nutnosti modifikovat LDAP zdroj
- ověřená funkce SSO a SLO se systémy s FortiOS verze 5 a vyšší
- funkce inteligentní nástěnky, která umožní omezit viditelnost virtuálně připíchnutých zpráv podle jména uživatele v LDAP zdroji, členství ve skupině, IP adresy nebo IP sítě (pro účely zobrazení zprávy pouze pro uživatele v konkrétním segmentu, např. budově nebo patře)
- řešení je otevřené pro budoucí integrace se SIEM systémy (prostřednictvím standardního protokolu SYSLOG)
- přímá podpora eDirectory, ActiveDirectory, OpenLDAP

Specifikace nabídnuté čtečky k dvoufaktorové autentizaci:

- Stolní RFID čtečka karet, kompatibilní a funkční se systémem KeyShield SSO, komunikace probíhá dle standardu ISO/IEC 14443 Type A 13,56 MHz (Mifare / DESFire).
- Čtečka používá USB rozhraní s délkou kabelu 100 cm. Obsahuje zvukovou i světelnou indikaci korektního přečtení ID karty.
- Jedná se o nové zařízení, určené pro provoz v ČR.
- Čtečka nedetekuje oddálení karty.
- Záruka 2 roky.

Jednotková cena čtečky: 1082,50 Kč bez DPH

Specifikace podpory:
Podpora obsahuje nárok na opravné a nové verze systému KeyShield SSO a jeho zabezpečení.

Popis nabízeného technického řešení – řešení správy privilegovaných účtů a specifikace podpory

V rámci veřejné zakázky je nabídnuto bezpečnostní řešení SecureAnyBox s následující charakteristikou a s uvedením požadavků, které řešení splňuje:

Bezpečnostní řešení pro správu privilegovaných účtů SecureAnyBox má dvě části, nabízí agenty pro ochranu lokálních účtů (aktuálně Windows, Linux, MacOSX, LDAP a Raspberian) a pak sdílené kryptované úložiště se zcela unikátní úrovní bezpečnosti, která staví na standardních šifrovacích mechanismech a hlavně na unikátním způsobu správy klíčů. Uživatelé si tak mohou ukládat hesla, klíče, certifikáty i dokumenty (obecné soubory), mohou je bezpečně sdílet a sledovat, kdo je svým přístupem kompromitoval. Sdílení je možné i s uživateli, kteří nejsou zaměstnanci Vaší školy, ale kteří pro Vás pracují či s Vámi spolupracují - externisté, právníci, dodavatelé, odběratelé, jiné školy..

Bezpečnostní řešení SecureAnyBox pro správu privilegovaných účtů splňuje tyto požadavky zadavatele:

- podpora automatického nastavení unikátních hesel pro lokální účty (pro účty administrator, admin, root) pro pracovní stanice, notebooky, servery pod operačními systémy Windows, MacOSX a Linux
- je možné provádět periodické změny hesel k privilegovaným účtům – nastavení hesel musí být automaticky prováděno denně nebo častěji, nezávisle na tom, zda je/není daný účet používaný a nezávisle na tom, zda má/nemá počítač v okamžiku nastavení síťovou konektivitu do prostředí školy
- nastavení hesel je možné stejným způsobem i pro LDAP účty, je zajištěna přímá podpora eDirectory a Active Directory.
- zjištění aktuálního hesla daného účtu na konkrétním počítači je pouze pro oprávněné uživatele
- je průběžný a okamžitý přenos auditních informací do SYSLOG
- bezpečné uložení privilegovaných údajů (hesel, klíčů, certifikátů a souborů) tak, aby uživatelé mohli tyto informace bezpečně sdílet nebo naopak aby nebyly dostupné nikomu kromě uživatele, který je uložil (ani správci systému, zálohování atd.)
- správa uživatelů systému umožňuje kombinaci převzetí z LDAP zdroje (požadavek na podporu eDirectory a Active Directory) a ručního vytvoření a správy (primárně pro externí uživatele)
- součástí řešení je konfigurovatelný generátor hesel. Konfigurace musí umožnit nastavení celkové délky hesla a zastoupení znaků (malá/velká písmena, číslice, speciální znaky)
- řešení má roli Auditora, který si může zobrazit všechny akce provedené uživateli i nad daty, ke kterým sám nemá přístup. Toto zobrazení neumožňuje přístup k datům, pouze k auditním informacím (ty musí zahrnovat identifikaci uživatele, datum, čas a specifikaci místa přístupu – minimálně zdrojovou IP adresu)
- řešení umožňuje uložit až desítky tisíc záznamů, např. hesel, na uživatele. Požadujeme možnost importu existujících citlivých údajů z formátu CSV (tabulkové kalkulátory) a KeePass (rozšířený jednouživatelský password manager)
- obsahuje komplexní audit při používání privilegovaných účtů (uloženo pro pozdější vyhodnocení)
- řešení je dostupné z Windows, Linux, MacOSX, iOS a Android
- práce s řešením nevyžaduje žádné specifické IT znalosti, je určeno i pro běžné uživatele (pedagogické i nepedagogické pracovníky školy)
- centrální řízení přístupu k těmto identitám pouze schváleným uživatelům a aplikacím
- řešení zajišťuje identifikaci a správu všech správcovských účtů
- řešení poskytuje privilegované přístupy a hesla k systémům pouze oprávněným administrátorům na základě pověření
- automatické změny hesel privilegovaných účtu jsou prováděny v definovaných časových intervalech

Specifikace podpory: Podpora obsahuje nárok na opravné a nové verze řešení SecureAnyBox a jeho zabezpečení.

Příloha č. 3 – Cenová tabulka

Položka	**Cena v Kč bez DPH**	**Cena v Kč včetně DPH**
Dvoufaktorová autentizace	266.000,-	321.860,-
Systém správy privilegovaných účtů	80.200,-	97.042,-
Čtečky karet (160 ks)	173.200,-	209.572,-
Dvoufaktorová autentizace – *podpora výrobce software v délce 5 let*	46.000,-	55.660,-
Systém správy privilegovaných účtů – *podpora výrobce software v délce 5 let*	30.200,-	36.542,-
Celková cena	**595.600,-**	**720.676,-**