SMLOUVA
NA IMPLEMENTACI BEZPEČNOSTNÍ INFRASTRUKTURY TCK

č. objednatele: D/1773/2014/ŘDP
č. zhotovitele: RCS-2014-Z068

uzavřená na základě ust. § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, v platném znění (dále jen „**občanský zákoník**")

Smluvní strany

Objednatel:	**Zlínský kraj**
Adresa:	třída Tomáše Bati 21, 761 90 Zlín
IČ:	70891320
DIČ:	CZ70891320
Zastoupený:	MVDr. Stanislav Mišák, hejtman
Bankovní spojení:	Česká spořitelna, a.s., č.ú.1827552/0800

a

Zhotovitel:	**AutoCont CZ a.s.**
Adresa sídla:	Hornopolní 3322/34, 702 00 Ostrava, Moravská Ostrava a Přívoz
IČ:	47676795
DIČ:	CZ47676795
Zapsaný v OR:	Krajský soud v Ostravě, oddíl B, vložka 814
Zastoupený:	Jindřich Zimola, ředitel regionálního centra
Bankovní spojení:	Česká spořitelna, a.s., č.ú. 5209452 / 0800

Článek I.
Preambule

1. Tato smlouva je uzavírána v rámci realizace projektu **„Rozvoj e-Governmentu ve Zlínském kraji II"**, reg.č. CZ.1.06/2.1.00/19.09273 (dále jen „projekt"), který objednatel realizuje v rámci Integrovaného operačního programu (dále jen „IOP"). Uzavření této smlouvy předcházelo zadávací řízení dle zákona o veřejných zakázkách. Smluvní strany se proto zavazují respektovat také podmínky uvedené v zadávacím řízení, pokud zajišťují minimálně stejný standard plnění, jako tato smlouva.

Článek II.
Předmět plnění

1. Zhotovitel se touto smlouvou zavazuje provést na svůj náklad a na své nebezpečí pro objednatele dílo a zajistit podporu díla.

   Dílem se rozumí dodávka a implementace jednotlivých částí bezpečnostní infrastruktury.

   Těmito částmi jsou:

   - Rozšíření TCK o LoadBalancer a webaplikační firewall
   - Systém pro ověřování klientů přistupujících do 21NET
   - Systém pro analýzu datových toků
   - Systém pro korelační analýzu událostí – SIEM

   Zhotovitel provede konfiguraci jednotlivých částí tak, aby tyto spolu vzájemně spolupracovaly, zejména pak se systémem SIEM, a v konečném důsledku zvýšily celkovou bezpečnost. To vše za podmínek sjednaných dále v této smlouvě.

2. Objednatel se touto smlouvou zavazuje, že zhotoviteli zaplatí za provedení díla a za poskytnutí služeb uvedených v předchozím odstavci dohodnutou cenu, to vše za podmínek sjednaných dále v této smlouvě.

3. Technické parametry díla a další podrobnosti plnění jsou uvedeny v příloze č. 1, která je nedílnou součástí této smlouvy.

4. Při plnění smlouvy se zhotovitel zavazuje:

   - postupovat v souladu s dokumentem „Studie proveditelnosti pro projekt Rozvoj e-Governmentu ve Zlínském kraji II",. Tento dokument byl součástí zadávací dokumentace veřejné zakázky (P02_P01 ZD_Vymezeni predmetu verejne zakazky), která předcházela uzavření této smlouvy a zhotovitel jej má v době podpisu smlouvy k dispozici; V případě rozporu mezi Studií proveditelnosti a touto Smlouvou má přednost tato smlouva.
   - dodržovat pravidla bezpečnosti ICT objednatele, která jsou uvedena v příloze č. 3, která je nedílnou součástí této smlouvy;
   - postupovat v souladu se svojí nabídkou, kterou podal v rámci zadávacího řízení, které předcházelo uzavření této smlouvy;
   - dodat veškeré komponenty díla dle přílohy č. 2, která je nedílnou součástí této smlouvy.

5. Součástí plnění předmětu smlouvy jsou i práce a dodávky v této smlouvě výslovně nespecifikované, které však jsou k řádnému plnění nezbytné a o kterých zhotovitel vzhledem ke své odbornosti a zkušenostem měl nebo mohl vědět. Provedení těchto prací však v žádném případě nezvyšuje touto smlouvou sjednanou cenu.

6. Podmínky zajištění podpory díla jsou uvedeny v příloze č. 4, která je nedílnou součástí této smlouvy.

Článek III.
Způsob, doba a místo plnění

1. Provádění díla začne ihned po uzavření smlouvy a člení se na následující fáze:

   1.1. Fáze 1: Zpracování předimplementační analýzy a vytvoření prováděcí dokumentace. Do 28 dnů od nabytí účinnosti této smlouvy dodá zhotovitel z jeho strany finální verzi předimplementační analýzy a prováděcí dokumentace k připomínkám objednateli, ten k ní podá připomínky do 5 pracovních dnů; dokumentaci se zapracovanými připomínkami

objednatele zhotovitel předá objednateli do 42 dnů od nabytí účinnosti této smlouvy. O dokončení fáze 1 bude sepsán akceptační protokol č. 1 s pokynem objednatele k zahájení fáze 2 nebo přerušení provádění díla.

1.2. **Fáze 2: Dodávka a instalace HW a SW komponent** díla a celková konfigurace. Fáze 2 bude zahájena po ukončení fáze 1 a bude dokončena do 13 týdnů od nabytí účinnosti této smlouvy. O dokončení fáze 2 bude sepsán akceptační protokol č. 2.

1.3. **Fáze 3: Testovací provoz**

- Zahájení testovacího provozu ihned po dokončení fáze 2. Testovací provoz bude ukončen provedením akceptačních testů.
- Zpracování provozní dokumentace a aktualizace veškeré související dokumentace TCK a 21NET.
- Provedení školení administrátorů.
- Fáze 3 bude ukončena předáním a převzetím řádně dokončeného díla bez vad a nedodělků - vyhotovením protokolu o předání a převzetí díla nejpozději do 28. 2. 2015.

1.4. **Fáze 4: Podpora díla:**

- Záruky a servis ihned na HW komponenty v délce min. 60 měsíců od ukončení fáze 2
- Zajištění následného provozu po dobu 12 měsíců ihned od ukončení fáze 3
- Záruka a servis na SW komponenty v délce 60 měsíců od ukončení fáze 3

2. Podrobný harmonogram provádění díla je zhotovitel povinen uvést v prováděcí dokumentaci.
3. Místem plnění je sídlo Zlínského kraje (tř. Tomáše Bati 21, Zlín) a dále místo druhé lokality TCK, tedy: obec:Zlín, ulice a č.p.: Radiokomunikační objekt Tlustá hora, ul. K Majáku.

Článek IV.
Licenční podmínky

1. Zhotovitel podpisem této smlouvy poskytuje objednateli v souladu s § 2358 a násl. občanského zákoníku a v souladu se zákonem č. 121/2000 Sb., autorský zákon, ve znění pozdějších předpisů (dále jen „autorský zákon"), **výhradní** licenci ke všem způsobům užití všech dokumentům, které je podle této smlouvy povinen vyhotovit a objednateli předat:

- předimplementační analýza
- prováděcí dokumentace,
- provozní dokumentace

Pokud se týká ostatních písemných výstupů, které zhotovitel na základě této smlouvy pro objednatele zhotoví, vztahují se na ně práva a povinnosti, která podle autorského zákona platí pro dílo vytvořené na objednávku.

Objednatel má právo dokumenty dle tohoto odstavce dále upravovat, učinit z nich součást jiného autorského díla, používat z nich výňatky nebo jakkoliv jinak je upravovat.

2. Licence dle předchozího odstavce se poskytují na dobu neurčitou, jako množstevně a územně neomezené a vzhledem k celkové ceně za dílo se sjednávají jako bezúplatné.
3. K veškerému software, který je součástí dodávky zhotovitele, zhotovitel podpisem této smlouvy poskytuje objednateli v ceně díla ve smyslu ustanovení § 2358 a násl. občanského zákoníku také příslušné licence. Tyto licence jsou dodány (poskytnuty) jako územně a časově neomezené nebo, pokud budou časově omezeny, pak musí být účinné minimálně po dobu, po kterou je zhotovitel povinen zajišťovat provoz a podporu díla.
4. Zhotovitel je povinen uspořádat si své právní vztahy se třetími osobami tak, aby plně dostál svým závazkům dle této smlouvy.
5. V případě, že některá z licencí nezbytných pro řádnou funkčnost a provoz díla nebyla zhotovitelem uvedena v jeho nabídce v zadávacím řízení, které předcházelo uzavření této smlouvy, nebo není výslovně uvedena v této smlouvě, pak platí, že zhotovitel je povinen dodat objednateli bez jakýchkoliv finančních nároků všechny potřebné licence tak, aby množstevně, časově a územně zajistily legální a řádnou funkčnost a provoz díla.

Článek V.
Předání a převzetí díla

1. V průběhu realizace díla smluvní strany **akceptačními protokoly** schvalují, že byla provedena určitá dodávka nebo služba. Akceptační protokol č. 1 a č. 2 jsou podkladem pro první fakturaci a musí proto vždy obsahovat konkrétní vymezení poskytnutých dodávek a služeb. Na základě akceptačních protokolů nedochází k přechodu vlastnictví k částem díla ani k přechodu nebezpečí škody. Objednatel není povinen akceptovat dílčí plnění dle tohoto odstavce, pokud není provedeno v souladu s touto smlouvou. Zda je dílo zhotoveno řádně se konstatuje až při předání a převzetí celého díla (po ukončení fáze 3) v protokolu o předání a převzetí díla. Protokol o předání a převzetí díla je podkladem pro druhou fakturaci.
2. Zhotovitel splní svou povinnost zhotovit dílo jeho řádným dokončením a předáním objednateli. Dílo je dokončeno řádně, pokud je provedeno s požadovanými parametry a ve stanovených termínech.
3. Zhotovitel písemnou výzvou učiněnou minimálně 3 týdny před datem plánovaného dokončení díla vyzve objednatele k převzetí díla a současně mu navrhne datum a místo zahájení přejímacího řízení.
4. Datum zahájení přejímacího řízení bude určeno tak, aby smluvní strany měly minimálně 2 týdny k závěrečné kontrole plnění a k odstranění případných vad a nedodělků. Pokud nedojde k prodlení v důsledku odstraňování vad nebo nedodělků v souladu s postupy uvedenými dále v tomto článku, bude přejímací řízení ukončeno a dílo bude předáno a převzato k datu, ke kterému končí fáze 3 díla.
5. Místem předání a převzetí díla je místo, kde je dílo prováděno. Předání a převzetí tak proběhne minimálně v sídle objednatele (primární lokalita); objednatel je oprávněn požadovat prohlídku také na jiných místech, které souvisí s plněním. Pokud se týká dokumentace zpracované zhotovitelem, ta bude objednateli předána v sídle objednatele.
6. Pokud nebudou při přejímacím řízení zjištěny vady ani nedodělky, je objednatel povinen takto řádně provedené dílo převzít.
7. Dílo, které má vady nebo nedodělky, které nebrání zprovoznění a užívání díla, objednatel převezme a o vadách a nedodělcích se v protokolu o předání a převzetí díla učiní záznam s uvedením náhradní lhůty k jejich odstranění. V tomto případě se má za to, že dílo bylo dokončeno řádně a včas a smluvní sankce za prodlení s dokončením díla se neuplatní; v případě prodlení s odstraněním vad a nedodělků v náhradní lhůtě se však uplatní smluvní sankce za prodlení s odstraněním vad a nedodělků. V případě pochybností, zda vady nebo nedodělky

zprovoznění a užívání díla brání, nebo nebrání, se má za to, že zprovoznění a užívání brání. Po odstranění vad a nedodělků dle tohoto odstavce vyzve zhotovitel objednatele ke kontrole jejich odstranění. O kontrole se pořídí protokol. Pokud nebudou vady a nedodělky ve stanovené lhůtě odstraněny, je objednatel oprávněn odstranit je sám nebo prostřednictvím třetí osoby za cenu v místě a čase obvyklou, k čemuž je zhotovitel povinen poskytnout součinnost; náklady objednatele na takové odstranění vad nebo nedodělků, pokud přesáhnou výši zádržného, jsou považovány za škodu, kterou je zhotovitel povinen objednateli nahradit.

8. Dílo, které má vady nebo nedodělky, které brání užívání a zprovoznění díla, není dokončeno. Pokud se při přejímacím řízení prokáže, že dílo není dokončeno, objednatel je nepřevezme a stanoví zhotoviteli náhradní lhůtu k jeho dokončení. Podmínkou pro převzetí díla je také kladný výsledek akceptačních testů. Zhotovitel je povinen dílo dokončit v náhradní lhůtě takto stanovené. Stanovení náhradní lhůty nemá vliv na smluvní sankce, které se stále počítají od termínu plnění určeného smlouvou.
9. Nejpozději k zahájení fáze 3 je zhotovitel povinen objednateli předložit také seznam zařízení, které jsou součástí díla, jejich pasporty, záruční listy, návody k obsluze a údržbě v českém jazyce, neučinil-li tak již dříve. Nedoloží-li zhotovitel tyto doklady, nepovažuje se dílo za dokončené a schopné předání.
10. Přejímací řízení je ukončeno podepsáním **protokolu o předání a převzetí díla** smluvními stranami. Za smluvní strany jsou protokol oprávněni podepsat jejich zástupci ve věcech technických. Stejně tak jsou zástupci ve věcech technických za smluvní strany oprávněni podepsat akceptační protokoly, protokoly o kontrole odstranění vad a nedodělků či jiné dokumenty vztahující se k provádění a kontrole díla.
11. Nedohodnou-li smluvní strany v rámci přejímacího řízení jinak, vyhotoví protokol o předání a převzetí díla zhotovitel.
12. Odmítne-li objednatel řádně a včas zhotovené dílo převzít nebo nedojde-li k dohodě o předání a převzetí díla, sepíší o tom strany (prostřednictvím svých zástupců ve věcech technických) zápis, v němž uvedou svá stanoviska. Zhotovitel není v prodlení, jestliže objednatel odmítl bezdůvodně převzít řádně zhotovené dílo.
13. K přechodu vlastnictví ze zhotovitele na objednatele dochází protokolárním předáním a převzetím díla.
14. Zhotovitel nese nebezpečí škody na díle i jeho jednotlivých komponentách až do doby protokolárního předání a převzetí díla.

Článek VI.
Cena a platební podmínky

1. Celková cena za plnění (tj. cena za dílo a cena za zajištění podpory díla) dle této smlouvy činí:

   Celková cena bez DPH = 7 985 500,- Kč
   DPH = 1 676 955,- Kč
   Celková cena včetně DPH = 9 662 455,- Kč
   (slovy Devětmiliónůšestsetšedesátdvatisícčtyřistapadesátpět korun českých).

2. Z ceny uvedené v odstavci 1. tohoto článku činí **cena za dílo**:

   cena bez DPH = 4 817 500,- Kč
   DPH = 1 011 675,- Kč
   cena včetně DPH = 5 829 175,- Kč
   (slovy Pětmiliónůosmsetdvacetdevěttisícjednostosedmdesátpět korun českých).

3. Cena za dílo bez DPH dle předchozího odstavce je stanovena jako pevná a nejvýše přípustná a zahrnuje veškeré náklady zhotovitele nezbytné k provedení díla dle této smlouvy. Cena za dílo je hrazena z dotace na projekt.

4. Zhotovitel bude cenu za dílo fakturovat v dílčích fakturách takto:

Č. faktury	Doba vystavení	Částka v % z ceny za dílo	Částka v Kč bez DPH
1	Po ukončení fáze 2	60%	**= 2 890 500,- Kč bez DPH**
2	Po dokončení fáze 3 – po předání a převzetí díla protokolem o předání a převzetí díla	40%	**= 1 927 000,- Kč bez DPH**

5. Z celkové ceny uvedené v odstavci 1. tohoto článku činí cena za zajištění podpory díla:

cena bez DPH = 3 168 000,- Kč
DPH = 665 280,- Kč
cena včetně DPH = 3 833 280,- Kč
(slovy třimiliónyosmsettřicettřitisícdvěstěosmdesát korun českých).

6. Cena bez DPH dle předchozího odstavce je stanovena jako pevná a nejvýše přípustná a zahrnuje veškeré náklady zhotovitele nezbytné k splnění jeho povinnosti zajistit podporu díla dle této smlouvy.

7. Zhotovitel fakturuje ročně za zajištění podpory díla, v němž je služba poskytnuta, vždy na začátku roku. U faktury za první rok však platí, že je ji zhotovitel oprávněn vystavit až po předání a převzetí řádně dokončeného díla protokolem o předání a převzetí díla. Každá z faktur bude znít na částku odpovídající jedné pětině ceny dle odstavce 5. tohoto článku. Cena za zajištění podpory díla není objednatelem hrazena z dotace na projekt, ale z jiných zdrojů objednatele.

8. Fakturu č. 1 je zhotovitel oprávněn vystavit po ukončení příslušné části plnění akceptačními protokoly dle čl. V odst. 1 této smlouvy; příslušné akceptační protokoly musí být přílohou faktury. Fakturu č. 2 je zhotovitel oprávněn vystavit po předání a převzetí díla protokolem o předání a převzetí díla, který musí být přílohou faktury č. 2.

9. Pokud byly při předání a převzetí zjištěny vady, které nebrání zprovoznění a užívání díla, částka ve výši 5 % z ceny díla vč. DPH představuje **zádržné**, které bude objednatelem uvolněno po jejich odstranění na základě protokolu o kontrole odstranění vad a nedodělků dle článku V, který zhotovitel doručí objednateli jako přílohu žádosti o uvolnění zádržného. Pokud nebudou vady a nedodělky ve stanovené lhůtě odstraněny, ztrácí zhotovitel nárok na úhradu částky rovnající se zádržnému.

10. Každá faktura bude obsahovat náležitosti podle zákona č. 563/1991 Sb., o účetnictví ve znění pozdějších předpisů, a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Faktura za provedení díla musí obsahovat text: „Výdaje plynoucí z této faktury jsou vynaloženy v rámci projektu Rozvoj e-Governmentu ve Zlínském kraji II, registrační číslo projektu CZ.1.06/2.1.00/19.09273, který je financován z Integrovaného operačního programu". Každá faktura musí obsahovat specifikaci zboží, služeb nebo prací, musí být rozepsána alespoň podle skupin účtovaných položek. Zhotovitel je na každé faktuře povinen výslovně uvést, zda je, či není plátcem DPH.
V případě, že je zhotovitel plátcem DPH, pak součástí každé faktury musí být prohlášení zhotovitele o tom, že:

- nemá v úmyslu nezaplatit daň z přidané hodnoty u zdanitelného plnění podle této smlouvy (dále jen „daň"),
- mu nejsou známy skutečnosti, nasvědčující tomu, že se dostane do postavení, kdy nemůže daň zaplatit a ani se ke dni podpisu této smlouvy v takovém postavení nenachází,
- nezkrátí daň nebo nevyláká daňovou výhodu,
- nebude nespolehlivým plátcem,
- bude mít u správce daně registrován bankovní účet používaný pro ekonomickou činnost,
- souhlasí s tím, že pokud ke dni uskutečnění zdanitelného plnění bude o zhotoviteli zveřejněna správcem daně skutečnost, že zhotovitel je nespolehlivým plátcem, uhradí objednatel daň z přidané hodnoty z přijatého zdanitelného plnění příslušnému správci daně,
- souhlasí s tím, že pokud ke dni uskutečnění zdanitelného plnění bude zjištěna nesrovnalost v registraci bankovního účtu zhotovitele určeného pro ekonomickou činnost správcem daně, uhradí objednatel daň z přidané hodnoty z přijatého zdanitelného plnění příslušnému správci daně.

11. Splatnost faktur je 30 dnů od data jejich doručení objednateli. Daňový doklad bude doručen objednateli ve dvou vyhotoveních. Faktura se považuje za uhrazenou okamžikem odepsání fakturované částky z účtu objednatele ve prospěch účtu zhotovitele. Faktura, která neobsahuje veškeré náležitosti dle zákona o dani z přidané hodnoty nebo dle této smlouvy bude vrácena zhotoviteli k opravě nebo doplnění. Od doručení opravené faktury objednateli běží nová 30 denní lhůta splatnosti. Objednatel se nedostává do prodlení se zaplacením faktury v případě, že zadrží část fakturované částky jako zádržné dle odstavce 9. tohoto článku.
12. V případě změny sazby DPH v průběhu plnění není nutné uzavírat dodatek ke smlouvě, pouze se k příslušnému základu daně uvedenému v této smlouvě přičte sazba DPH účinná v době vzniku zdanitelného plnění.

Článek VII.
Záruka a odpovědnost za vady

1. Zhotovitel poskytuje objednateli záruku na komponenty díla v délce 60 měsíců. Počátek běhu záruční lhůty je uveden v článku III. odst. 1.4. Dokud nepřejde vlastnické právo k dílu na objednatele, uplatňuje práva ze záruky ve prospěch objednatele zhotovitel.
2. Zhotovitel poskytuje objednateli záruku na funkčnost díla v délce 60 měsíců. Běh záruční lhůty počíná dnem následujícím po dni protokolárního předání a převzetí díla.
3. V záruční době má objednatel nárok, při splnění záručních podmínek, na bezplatnou opravu nebo výměnu oprávněně reklamovaných komponent.
4. Odstraňování vad a nedodělků se řídí Podmínkami zajištění podpory díla (příloha č. 4 této smlouvy). Pokud nároky z odpovědnosti za vady díla nelze z jejich povahy řešit v rámci zajištění podpory díla (příloha č. 4 této smlouvy), budou smluvními stranami řešeny v souladu s příslušnými ustanoveními občanského zákoníku.
5. Vady díla a případné nedodělky, které se vyskytnou po záruční době, jakož i vady díla, které se vyskytnou sice v záruční době, ale z jakéhokoliv důvodu je nelze zahrnout pod záruku, se zhotovitel zavazuje odstraňovat způsobem uvedeným v Podmínkách zajištění podpory díla (příloha č. 4 této smlouvy).

Článek VIII.
Sankce

1. Objednatel je oprávněn požadovat a zhotovitel je v takovém případě povinen zaplatit objednateli smluvní pokutu ve výši 10.000,- Kč za každý i započatý kalendářní den prodlení s řádným dokončením díla.
2. Objednatel je oprávněn požadovat a zhotovitel je v takovém případě povinen zaplatit objednateli smluvní pokutu ve výši 10.000,- Kč za každý i započatý kalendářní den prodlení s ukončením fáze 1 a 2 provádění díla.
3. Objednatel je oprávněn požadovat a zhotovitel je v takovém případě povinen zaplatit objednateli smluvní pokutu ve výši 10.000,- Kč za každý i započatý kalendářní den prodlení s odstraněním vad dle článku V. odst. 7 (vady, které nebrání zprovoznění a užívání díla).
4. Pokud zhotovitel na výzvu objednatele neopraví nebo nedoplní údaje na faktuře dle článku VI. odst. 10 této smlouvy je objednatel oprávněn požadovat a zhotovitel je v takovém případě povinen zaplatit objednateli smluvní pokutu ve výši 5.000,- Kč. Pokud se prokáže, že tyto údaje na faktuře požadované dle článku VI. odst. 10 této smlouvy jsou nepravdivé, je objednatel oprávněn požadovat a zhotovitel v takovém případě povinen zaplatit objednateli smluvní pokutu ve výši 5.000,- Kč za každý nepravdivý údaj.
5. Za nedodržení pravidel publicity dle článku XI. odst. 3 této smlouvy je objednatel oprávněn požadovat a zhotovitel je v takovém případě povinen zaplatit objednateli smluvní pokutu ve výši 15.000,- Kč, pokud zhotovitel nesjedná nápravu ani v dodatečné lhůtě, kterou mu ke sjednání nápravy objednatel určí.
6. Za porušení povinností dle článku XII. odst. 1 této smlouvy je objednatel oprávněn požadovat po zhotoviteli a zhotovitel je v takovém případě povinen zaplatit objednateli smluvní pokutu ve výši 10.000,- Kč za jeden dotčený subjekt údajů.
7. Pokud smluvní strana poruší své povinnosti dle článku XII. odst. 2 této smlouvy je povinna druhé smluvní straně, pokud tato to bude požadovat, zaplatit smluvní pokutu ve výši 10.000,- Kč za jeden zjištěný případ úniku informací.
8. Pokud zhotovitel poruší pravidla bezpečnosti ICT (článek II. odst. 4. a příloha č. 3 této smlouvy), je objednatel oprávněn požadovat a zhotovitel je v takovém případě povinen zaplatit objednateli smluvní pokutu ve výši 10.000,- Kč za každý zjištěný případ porušení.
9. V případě nedodržení termínu splatnosti faktury, je zhotovitel oprávněn účtovat objednateli úrok z prodlení ve výši dle obecné úpravy práva občanského (dle nařízení vlády č. 351/2013 Sb.).
10. Zaplacení smluvní pokuty nijak nekrátí nárok objednatele na náhradu škody zhotovitelem, pokud škoda vznikne v příčinné souvislosti s porušením povinností zhotovitele zajištěné smluvní pokutou. Škodou vzniklou objednateli se rozumí i případ, kdy je objednatel v příčinné souvislosti s pochybením zhotovitele sankcionován ze strany poskytovatele dotace, subjektů implementační struktury IOP nebo orgánů veřejné správy.
11. Objednatel je oprávněn požadovat a zhotovitel je v takovém případě povinen zaplatit objednateli smluvní pokutu ve výši 1.000,- Kč za každý den, kdy podpora díla nebyla zajištěna v souladu s parametry stanovenými touto smlouvou.

Článek IX.
Odstoupení od smlouvy, výpověď

1. Případná práva a povinnosti smluvních stran z odstoupení od smlouvy budou řešena podle příslušných ustanovení občanského zákoníku.

2. Za podstatné porušení smlouvy zhotovitelem se považuje zejména to, když:
   - zhotovitel provádí dílo způsobem, který vede nepochybně k vadnému plnění,
   - zhotovitel je v prodlení s ukončením kterékoliv fáze díla delším než 30 kalendářních dnů,
   - zhotovitel i přes písemnou výtku objednatele zajišťuje podporu díla v rozporu s parametry uvedenými v této smlouvě po dobu delší než dva týdny
3. Za podstatné porušení této smlouvy objednatelem se považuje zejména to, jestliže je objednatel i přes urgenci zhotovitele v prodlení s úhradou faktury trvající déle než patnáct dnů od této urgence.
4. Po dokončení fáze 1 provádění díla má objednatel právo s okamžitou účinností ukončit smlouvu výpovědí bez nutnosti uvést důvody výpovědi.

Článek X.

Organizace a komunikace

1. Platformou pro jednání smluvních stran na pracovní úrovni v průběhu plnění smlouvy je Pracovní skupina projektu (PSP). PSP se za objednatele účastní vždy osoba ve věcech technických. Zhotovitel je povinen zajistit, aby se PSP vždy účastnil jeho projektový manažer a jeho specialista odpovědný za oblast, která bude předmětem jednání. V průběhu fáze 1 a fáze 2 provádění díla zhotovitel svolá zasedání PSP tak, aby se PSP konala min. 1x za 14 dnů. PSP se budou konat zpravidla v sídle objednatele, nedohodnou-li se strany jinak. Zhotovitel oznámí objednateli požadavek na rezervaci příslušných místností pro jednání PSP min. s týdenním předstihem. Jednání PSP organizuje zhotovitel, který připravuje podklady pro jednání, zajišťuje zápisy z jednání, prezenční listiny apod. Originál všech zápisů a listin vzešlých z jednání předává objednateli. Na všech dokumentech zhotovitel dodržuje pravidla publicity IOP.

2. Kontaktní údaje smluvních stran

Objednatel:
Kontaktní osoby - zástupci ve věcech technických:
RNDr. Ivo Skrášek, ivo.skrasek@kr-zlinsky.cz, 577 043 260
Bedřich Polák, bedrich.polak@kr-zlinsky.cz, 577 043 256
kontaktní osoby – zástupci ve věcech smluvních:
Ing. Martin Prusenovský, martin.prusenovsky@kr-zlinsky.cz, 577 043 848
Ing. Martin Kobzáň, martin.kobzan@kr-zlinsky.cz, 577 043 820

Zhotovitel:
kontaktní osoby – zástupci ve věcech technických:
Miloslav Eis, miloslav.eis@autocont.cz, 603 587 318
Tomáš Makula, tomas.makula@autocont.cz, 602 717 377
kontaktní osoby – zástupci ve věcech smluvních:
Tomáš Sládek, tomas.sladek@autocont.cz, 602 590 926
Jindřich Zimola, jindrich.zimola@autocont.cz, 910 973 184

Pokud kontaktní osoby - zástupci ve věcech technických nedosáhnou shody ohledně řešení problému při plnění této smlouvy, postoupí se problém k řešení kontaktním osobám – zástupcům ve věcech smluvních. Pokud ani kontaktní osoby – zástupci ve věcech smluvních nedosáhnou shody ohledně řešení takového problému, postoupí se problém k řešení na úroveň vyššího managementu smluvních stran.

3. Pokud dojde ke změně v kontaktních údajích uvedených v předchozím odstavci, jsou smluvní strany oprávněny provést prostřednictvím písemného oznámení druhé smluvní straně, a to předem nebo nejpozději bezodkladně poté, co ke změně dojde. Za dostačující formu oznámení je považováno zaslání emailu kontaktní osobě druhé smluvní strany ve věcech smluvních, která je povinna obdržení e-mailu do 2 pracovních dnů potvrdit. V případě změny v kontaktních údajích uvedených v tomto odstavci není třeba uzavírat dodatek ke smlouvě.
4. Nastanou-li u některé ze smluvních stran skutečnosti bránící řádnému plnění této smlouvy, je povinna to ihned bez zbytečného odkladu oznámit druhé straně.

Článek XI.
Požadavky IOP

1. Zhotovitel je povinen archivovat dokumentaci spojenou s předmětem plnění od podpisu smlouvy oběma stranami do 31. 12. 2025.
2. Zhotovitel je povinen umožnit osobám oprávněným k výkonu kontroly projektu, z něhož je zakázka hrazena (zejm. Ministerstvo vnitra ČR, územní finanční orgány, Ministerstvo financí, Nejvyšší kontrolní úřad, Evropská komise, Evropský účetní dvůr, případně další orgány oprávněné k výkonu kontroly), provést kontrolu všech dokladů vztahujících se k předmětu plnění. Zhotovitel je povinen umožnit kontrolním orgánům vstup do budov a na pozemky dotčené plněním této smlouvy. Tyto povinnosti má zhotovitel ode dne účinnosti smlouvy do 31. 12. 2025.
3. Zhotovitel je povinen provádět publicitu dle požadavků objednatele a poskytovatele dotace (MV ČR), resp. podle požadavků IOP, to znamená, že je zejména povinen na všech dokumentech a písemných výstupech dodržovat pravidla publicity IOP.

Článek XII.
Závěrečná ujednání

1. Zhotovitel se zavazuje zabezpečit ochranu dat a informací získaných v souvislosti s plněním této smlouvy a jakékoliv osobní údaje, se kterými dojde do styku v souvislosti s plněním této smlouvy, chránit v souladu s ustanoveními zákona č.101/2000 Sb., o ochraně osobních údajů a o změně některých zákonů.
2. Obě smluvní strany se zavazují, že obchodní a technické informace, které jim byly svěřeny druhou stranou, nezpřístupní třetím osobám bez písemného souhlasu druhé strany a nepoužijí tyto informace k jiným účelům, než je k plnění podmínek smlouvy. Ustanovení zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, nejsou tímto dotčena.
3. Zhotovitel se zavazuje předložit objednateli seznam subdodavatelů, jimž za plnění subdodávky poskytnuté v souvislosti s plněním dle této smlouvy, uhradil více než 10 % z části ceny, uvedené v odstavci 1 článku VI této smlouvy, uhrazené objednatelem v jednom kalendářním roce. Zhotovitel je povinen předložit seznam subdodavatelů nejpozději do 28. 2. následujícího roku. Má-li subdodavatel formu akciové společnosti, musí být přílohou seznamu subdodavatelů i seznam vlastníků akcií, jejichž souhrnná jmenovitá hodnota přesahuje 10 % základního kapitálu, vyhotovený ve lhůtě 90 dnů před dnem předložení seznamu subdodavatelů.
4. Tuto smlouvu lze změnit nebo doplňovat pouze písemnými vzestupně číslovanými dodatky, které budou podepsány oběma smluvními stranami, není-li v ní uvedeno jinak.
5. Nedílnými součástmi této smlouvy jsou následující přílohy:
    - Příloha č. 1: Podrobné vymezení díla

- Příloha č. 2: Soupis použitých komponent
- Příloha č. 3: Bezpečnostní pravidla ICT
- Příloha č. 4: Podmínky zajištění podpory díla

Pokud se v těchto přílohách hovoří o zadavateli, myslí se jím objednatel. Pokud se v těchto přílohách hovoří o dodavateli nebo uchazeči, myslí se jím zhotovitel. Pokud je v těchto přílohách něco upraveno odlišně než v textu smlouvy samotné, přednost má text smlouvy samotné.

6. V případě, že zhotovitel je plátcem DPH, pak podpisem této smlouvy výslovně prohlašuje, že:
   - nemá v úmyslu nezaplatit daň z přidané hodnoty u zdanitelného plnění podle této faktury (dále jen „daň"),
   - mu nejsou známy skutečnosti, nasvědčující tomu, že se dostane do postavení, kdy nemůže daň zaplatit a ani se ke dni vystavení této faktury v takovém postavení nenachází,
   - nezkrátí daň nebo nevyláká daňovou výhodu,
   - nebude nespolehlivým plátcem,
   - bude mít u správce daně registrován bankovní účet používaný pro ekonomickou činnost,
   - souhlasí s tím, že pokud ke dni uskutečnění zdanitelného plnění bude o zhotoviteli zveřejněna správcem daně skutečnost, že zhotovitel je nespolehlivým plátcem, uhradí objednatel daň z přidané hodnoty z přijatého zdanitelného plnění příslušnému správci daně,
   - souhlasí s tím, že pokud ke dni uskutečnění zdanitelného plnění bude zjištěna nesrovnalost v registraci bankovního účtu zhotovitele určeného pro ekonomickou činnost správcem daně, uhradí zhotovitel daň z přidané hodnoty z přijatého zdanitelného plnění příslušnému správci daně.

7. V souladu s ustanovením § 1801 občanského zákoníku se ve smluvním vztahu založeném touto smlouvou vylučuje použití ustanovení § 1799 a § 1800 občanského zákoníku.

8. Případná neplatnost některého ustanovení této smlouvy nemá za následek neplatnost ostatních ustanovení. V případě, že kterékoliv ustanovení této smlouvy se stane neúčinným nebo neplatným, smluvní strany se zavazují bez zbytečného odkladu nahradit takové ustanovení novým, které svým obsahem a smyslem odpovídá nejlépe obsahu a smyslu ustanovení původního.

9. Práva a povinnosti smluvních stran výslovně v této smlouvě neupravená se řídí příslušnými ustanoveními zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů, zejména ustanoveními upravujícími dílo a licenci.

10. Tato smlouva se vyhotovuje ve čtyřech stejnopisech, z nichž jeden obdrží zhotovitel a tři objednatel. Smlouva nabývá platnosti dnem, kdy bude podepsána oběma stranami, a účinnosti dnem, kdy bude podepsaná smlouva doručena smluvní stranou, která smlouvu podepsala jako poslední, druhé smluvní straně.

Doložka dle § 23 zákona č. 129/2000 Sb., o krajích, ve znění pozdějších předpisů	
Rozhodnuto orgánem kraje:	Rada Zlínského kraje
Datum a číslo jednací:	25. 8. 2014; 0667/R16/14

Za objednatele

Ve Zlíně dne 2. 9. 09. 2014

.....

MVDr. Stanislav Mišák
Hejtman

Za zhotovitele

Ve Zlíně dne 24. 9. 2014

.....

Jindřich Zimola
ředitel regionálního centra

Zlínský kraj se sídlem ve Zlíně 1

Příloha č. 1 Smlouvy: Podrobné vymezení díla

Obecné požadavky na dodávku

- Záměrem Zadavatele je i nadále provozovat infrastrukturu tak, aby v rámci dvou datových center neexistovalo jedno místo, jehož selhání způsobí nefunkčnost celé infrastruktury (tzv. SPOF – single point of failure), a zároveň aby takto vybudovaná infrastruktura byla odolná na výpadek až celé jedné lokality.
- Všechna zařízení síťové a serverové infrastruktury budou v provedení, které umožní montáž do racku 19" (maximální velikosti v jednotkách „U" jsou uvedeny u konkrétních zařízení).
- Všechny v zadání zmíněné technické parametry jsou definovány jako minimální, není-li uvedeno jinak.
- U položek s přepokládaným dodáním více kusů se jejich popis týká parametrů pro jeden kus.
- Případné názvy a popisy v zadávací dokumentaci odkazující na jednotlivá obchodní jména a označení výrobků či obchodních názvů materiálů popisují a specifikují podmínky požadovaného plnění s tím, že zadavatel připouští i jiná kvalitativně a technicky obdobná řešení za podmínky, že nesmí dojít ke zhoršení požadovaných parametrů technického řešení. Musí být zachována plná kompatibilita s používanými zařízeními, která budou v provozu paralelně s novým systémem.
- Zadavatel požaduje dodání zboží, které je určeno pro prodej v České republice.
- Zadavatel vyžaduje, aby uchazeč prokázal, že je oprávněn provádět servis nabízených klíčových zařízení (servery, disková pole, aktivní prvky). Prokázání uchazeč provede předložením certifikátu nebo prohlášením výrobce před ukončením fáze 1.
- Zadavatel nepřipouští variantní řešení.
- Součástí nabídky řešení uchazeče bude podrobný popis použitých prvků řešení uvedených v příloze č. 2 smlouvy. Splnění minimálních požadovaných parametrů uvedených v příloze č. 1 smlouvy (tabulky s názvem požadované technické parametry) uchazeč prokáže doplněním nabízeného řešení a parametrů v této příloze..Zadavatel zdůrazňuje, že předmětem dodávky je komplexní a plně funkční infrastruktura. Pakliže některá ze součástí podmiňujících funkčnost není v této dokumentací zmíněna, je na odborných schopnostech uchazeče, aby takovouto skutečnost odhalil a do svého řešení zahrnul všechny potřebné komponenty.
- Dodavatel provede kompletní implementaci. V průběhu implementace bude prováděno testování jednotlivých komponent.
- Dodavatel bude při implementaci dodržovat zásady projektového řízení.

Požadavky na použité zařízení z hlediska výroby a údržby

Kromě požadavků na funkční a výkonové vlastnosti řešení, vyžaduje Zadavatel, aby konkrétní Uchazečem vybraná zařízení použitá v řešení splňovala z hlediska vývoje, výroby a podpory ze strany výrobce minimálně následující požadavky:

- Zařízení není ve stádiu prototypu či provozního ověřování,
- Výrobce poskytuje podporu pro řešení chyb a nestandardních provozních stavů zařízení po dobu nejméně 5 let (buď sám, nebo prostřednictvím partnerů).

Zadavatel požaduje, aby veškerá konkrétní dodaná zařízení byla nová, nepoužitá. Repasované nebo jinak použité zboží se nepřipouští.

Technické požadavky pro 1. ČÁST VZ - Bezpečnostní infrastruktura TCK

(A) Rozšíření TCK o LoadBalancery a webaplikační firewall

Je požadováno, aby poptávané zařízení poskytovalo následující funkcionality:

- loadbalancer [LB]
- web aplikační firewall [WAF]
- reverzní proxy s pokročilými autentifikačními schopnostmi
- systém vzdáleného přístupu k aplikacím - SSL VPN brána

Koncept řešení
Zadavatel od navrženého zařízení očekává následující přínosy:

- Vyšších aplikačních výkonů
- Vyšší míry vysoké dostupnosti
- Zajištění vyšší operability při správě HW/SW jednotlivých serverů
- Univerzálnost zapojení pro možnost splnění při požadavku na rozklad zátěže pro určitou aplikaci
- snadnou administraci a přehlednost architektury aplikací,
- snadnou škálovatelnost
- aplikaci režimu LB bez rizika na stabilitu síťového prostředí LAN,
- využití LB pro příspěvkové organizace kraje (migrace stávajících veřejných internetových služeb do TCK)
- SSL akcelerace – Serverové certifikáty jsou instalovány již na LB zařízení. LB vykonává funkcí SSL šifrování a odebírá podstatnou část zátěže aplikačního WWW serveru.
- Inteligentní komprese dat– Snížení objemu přenášených dat na základě vlastností typických aplikačních protokolů a klientů. Komprese nevyžaduje instalaci žádných doplňkových produktů na koncové zařízení uživatele.
- Dočasné ukládání dat tzv. caching – LB podporuje ukládání často se opakujících dat do interní paměti a tak zvyšuje výkonnost aplikace.

Konkrétní topologie nasazení LB bude zvolena v rámci prováděcího projektu, který je úvodní fází implementace. V tuto chvíli zadavatel není schopen přesně říci, který z níže uvedených módů bude zvolen. Proto zadavatel požaduje podporu všech následujících módů instalace:

- one-arm mód
- routing mód
- source NAT mód s Client IP Header Insert (XFF)
- destination NAT mód
- L2 bridge mód

Skutečné IP adresy aplikačních serverů, mezi které bude provoz rozkládán, se mohou nacházet v libovolné IP síti v rámci základní routing instance TCK, popřípadě mohou být umístěny kdekoliv v rámci 21NET.

Podobně i klienti aplikací, které budou využívat LB, se mohou nacházet v LAN KÚ, v TCK, v sítích 21NET i v zóně untrust, což je prostor veřejného internetu.

Pro potřeby rozkladu zátěže pro aplikace provozované v různých bezpečnostních zónách je požadováno instalovat LB s podporou virtuálních routovacích instancí a instalovat jej stejným způsobem i v těchto routovacích instancích, tak aby nedošlo k narušení koncepce nezávislých směrovacích instancí a virtuálnímu oddělení na úrovni 3. komunikační vrstvy.

Je vyžadována instalace LB v režimu vysoké dostupnosti (dále jako HA – High Availability), jedna fyzická jednotka bude instalována v části TCK na KÚ a druhá fyzická jednotka v části TCK na Tlusté hoře.
S ohledem na maximální využití výkonových parametrů infrastruktury TCK je požadováno připojení LB pomocí 10G Ethernet rozhraní k přepínačům HP7500, které poskytují dostatečný počet neobsazených 10G portů pomocí SFP+ rozhraní.

Web aplikační firewall
WAF provádí validaci dat, provádí obranu proti útokům jako například XSS (cross site scripting) či SQL injection.
Detekce útoků
Je požadováno dodání zařízení s dvojí detekci útoků využívající jak negativní tak i pozitivní model.

- Negativní model

  Detekce útoků se provádí na základě známých signatur, omezuje se však pouze na známé útoky.

- Pozitivní model

  Detekce útoků je založena na analýze správného chování aplikace. Model pozitivního zabezpečení spočívá v tom, že zařízení má naučen správný vzorec chování aplikace. Blokují se škodlivé akce identifikované jako odchylky od korektní činnosti aplikace. Toto způsob detekce útoků zajišťuje ochranu proti ještě neznámým nepublikovaným rizikům, tzv. zero day attacks.

Rozšířené možnosti zabezpečení
Je požadováno dodání zařízení, které kromě WAF pro http protokol poskytne i funkci aplikačního firewallu pro další protokoly (min. FTP a SMTP).

Detekce anomálií v HTTP provozu, následná ochrana a logování
Je požadováno, aby WAF byls chopen analyzovat na aplikační vrstvě protokol HTTP (záhlaví, tělo dotazů a i odpovědi). Následně musí umožňovat reakci jako standardní firewall – tj. zahození požadavku, zobrazení chybového hlášení, přesměrování na tzv. honeypot nebo prosté logování události (např. do SIEM nástroje).

Just-in-time patching
V případě identifikace nové zranitelnosti tzv. vulnerability aplikačních serverů trvá určitý čas výrobci nebo dodavateli připravit a rozdistribuovat opravu aplikace, tzv. patch. Po dobu než je oprava k dispozici je možné omezit přístup k části aplikace obsahující tuto potencionální hrozbu pouze omezené skupině důvěryhodných uživatelů při zachování stávající funkcionality nebo připravit dočasné zabezpečení na úrovni WAF.

Logování
Doporučujeme, aby systémové i bezpečnostní logy ze zařízení WAF bylo možno exportovat na externí Syslog server, případně zasílat notifikace pomocí emailu, SNMP trapu. Předpokládá se, že tyto události budou následně analyzovány v centrálním SIEM nástroji.

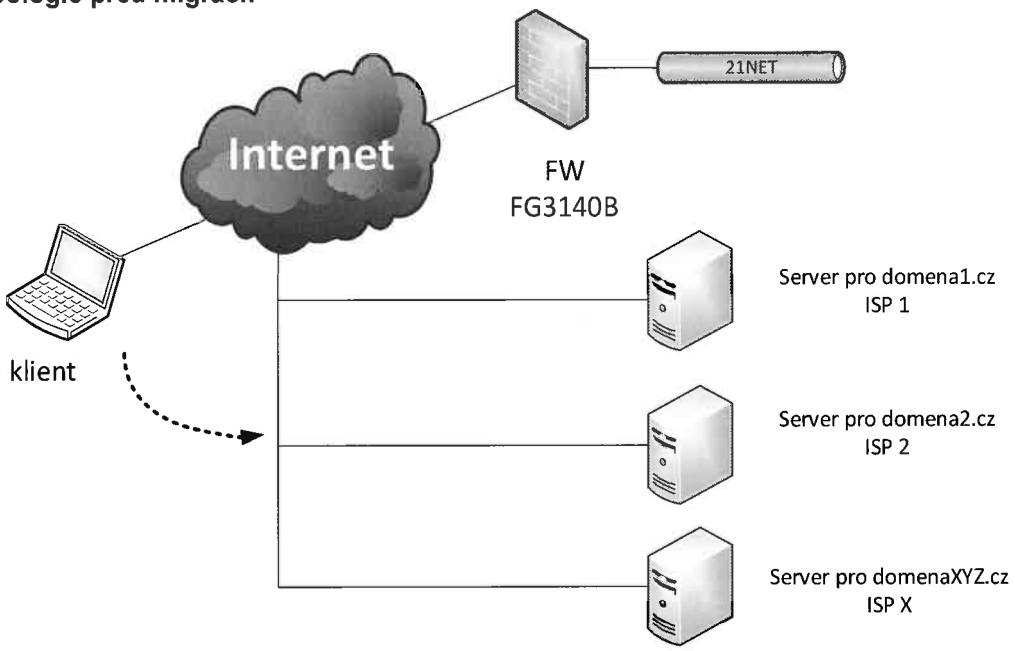
Funkcionalita reverzní proxy
Neoddělitelnou funkcionalitou, která je požadována je reverzní proxy. Díky této vlastnosti je možná publikace služeb a aplikací do různých separátních sítí. Zároveň je požadováno,aby zařízení umožňovalo předávání uživatelských pověření mezi nezávislými aplikacemi (SSO). Předávání je možné na základě protokolu kerberos, NTLM nebo pomocí definovaných http položek. Zdrojem uživatelských identit pak může být jedna nebo více nezávislých databází MS AD, obecný LDAP adresář nebo další běžné protokoly pro ukládání identit. Vzhledem k plánovaným projektů KUZK je požadováno, aby reverzní proxy umožňovala publikací virtuálních desktopů a aplikací (min. technologie VMWare, Microsoft a Citrix, protokol PCoverIP).

Řešení vzdáleného přístupu k aplikacím provozovaným v TCK
V případě instalace LB s funkcí SSL Offload je vyžadováno instalovat řešení, které podporují současně i možnost vzdáleného přístupu k interním aplikacím TCK, které budou dostupné pouze pro omezený okruh uživatelů ze strany např. zaměstnanců Krajského úřadu či organizací spravovaných krajem.
Řešení pro vzdálený přístup musí podporovat tyto služby:

- Autentizace, Autorizace a sdílení identifikačních informací tzv. single sign on (tzv. SSO).
- Podpora pro protokoly Kerberos (MS Active Directory), LDAP, NTLM, Radius, TACAS+, OCSP, CRLDP.
- Možnost zakončení uživatelských SSL spojení - SSL Offload. Snížení procesní zátěže pro aplikační servery.
- Možnost bezpečnostní kontroly koncových zařízení přistupujících k interním aplikacím a službám.
- Podpora pro chytré telefony s operačními systémy iOS, Android, WM atd.
- Plnohodnotný VPN přístup pro klienty OS Windows, Linux mobilní klienty OS Android, Apple iOS, popřípadě další.
- Detailní logování a reporting (integrace se SIEM nástrojem dodávaným v rámci této zakázky).

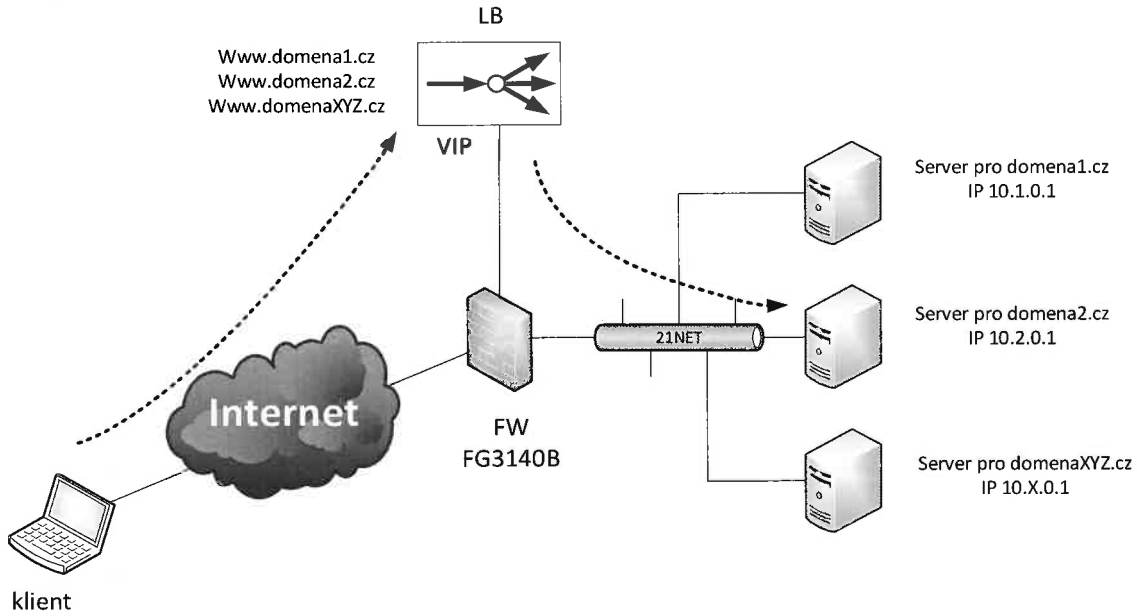
Migrace konektivit PO do TCK
Další klíčovou vlastností požadovaného loadbalanceru je schopnost umožnit postupnou migraci IT zdrojů příspěvkových organizací (PO) do prostředí TCK. Předpokládá se, že budou centrálně nastaveny publikace jednotlivých služeb PO na vnějších rozhraních loadbalanceru. Následně budou přesměrovány DNS záznamy jednotlivých organizací na veřejné IP adresy TCK. Následné směrování provozu na servery bude realizováno buďto pomocí privátní sítě 21NET nebo individuálně dle možností příslušné PO.

Topologie před migrací:



Obrázek 1 - Schématické znázornění topologie před migrací

Topologie po migraci:



Obrázek 2 - Schématické znázornění migrace konektivit PO II

Součinnost zadavatele
Veškeré změny v konfiguracích stávajících aktivních prvků a serverů TCK a 21NET budou provedeny Zadavatelem dle specifikace požadavků Dodavatelem a po jejich vzájemném odsouhlasení.

Požadované technické parametry

Požadovaná hodnota	Splňuje ANO/NE	Uchazečem nabízené řešení či parametr
samostatný box s možností montáže do RACK pro každou lokalitu TCK, maximální výška 2U	ANO	Nabízené řešení, které je plně kompatibilní se zařízeními používanými v současné síti a zároveň v souladu s celkovým záměrem Zadavatele prezentovaným v poskytnuté „Studii proveditelnosti“ je postavené na produktu společnosti F5, konkrétně jde o zařízení BIG-IP 4000s ADC, které je doplněné o moduly Local Traffic Manager, Application Security Manager a Access Policy Manager
min. 8 x 10/100/1000Mbps Ethernet interface a zároveň min. 2 x 10 Gbps interface	ANO	8 x 10/100/1000Mbps Ethernet interface a zároveň 2 x 10 Gbps interface
Plně redundantní zdroj napájení.	ANO	Plně redundantní zdroj napájení.
Port vyhrazený pro lokální management	ANO	Management 10/100/1000 Ethernet port + Console serial port
Dedikovaný management interface pro vzdálený management (GUI, příkazová řádka)	ANO	Dedikovaný management interface pro vzdálený management (GUI, příkazová řádka)
Lights-out management - nezávislý servisní procesor umožňující provádění veškerých administrátorských operací (včetně zastavení bootovacího procesu) vzdáleně po síti ethernet	ANO	Nabízené zařízení má nezávislý servisní procesor, který je přístupný i v případě výpadku vlastního zařízení.
Propustnost min. 10Gbps	ANO	Propustnost 10Gbps
Počet L4 HTTP požadavků za sekundu je min. 1.00M rps	ANO	Zařízení zpracovává až 1,25M rps
Počet L4 Connections per Second je min. 150k cps	ANO	Počet L4 Connections per Second je 150k cps
Počet L7 Connections per Second je min. 50k cps	ANO	Počet L7 Connections per Second je 50k cps
Minimální počet konkurentních spojení - 10 miliónů	ANO	Počet konkurentních spojení - 10 miliónů
Virtualizace - Úplné oddělení síťové komunikace. Možnost vytváření izolovaných a na sobě nezávislých síťových segmentů (IP adresy, routovací tabulky, ...) za účelem úplného oddělení síťového provozu pro různé zóny.	ANO	Virtualizace - Úplné oddělení síťové komunikace. Možnost vytváření izolovaných a na sobě nezávislých síťových segmentů (IP adresy, routovací tabulky, ...) za účelem úplného oddělení síťového provozu pro různé zóny.
Zajištění rozkládání zátěže na interní systémy na základě aktuální dostupnosti služby, zajištění integrity session.	ANO	Zařízení si při rozkládání zátěže kontroluje dostupnost služeb a zároveň si hlídá integritu jednotlivých spojení
Možnost řízení spojení a LB procesu na základě obsahu komunikace na L2 až L7 vrstvě.	ANO	Zařízení pracuje s informacemi z L2-L7
Možnost zpracovat libovolný (i neznámý) síťový protokol (založený na IP).	ANO	Zařízení podporuje libovolný protokol založený na IP
Možnost změny obsahu přenášených dat až na L7	ANO	Zařízení při své činnosti umí manipulovat

vrstvě.		i daty až na L7
Možnost filtrování provozu na úrovni packetů.	ANO	Zařízení může pracovat jako packetový filtr
Možnost filtrování provozu podle obsahu na L7 vrstvě.	ANO	Zařízení umí filtrovat provoz dle obsahu L7
Možnost řízení šířky pásma.	ANO	Zařízení podporuje řízení šířky pásma
Podpora ToS, QoS	ANO	Zařízení podporuje ToS a QoS
Možnost manipulace a přepis URL na základě provozních parametrů spojení (typ klienta, zdrojová adresa, cílová URL apod.)	ANO	Zařízení podporuje požadované typ y manipulace a přepisování URL
Možnost vytvářet uživatelsky přizpůsobitelné statistiky http provozu.	ANO	Zařízení dává operátorům a správcům velké možnosti při vytváření statistik http provozu
Ochrana proti následujícím útokům:	ANO	splňujeme
□ OWASP TOP 10 včetně podpory pro AJAX/JSON/XML	ANO	Zajištěna ochrana proti útokům definovaným jako OWASP TOP 10
□ DoS a DDoS	ANO	Zajištěna ochrana proti útokům typu DoS a DDoS
□ BruteForce	ANO	Zajištěna ochrana proti útokům typu BruteForce
□ Web Scraping	ANO	Zajištěna ochrana proti útokům typu Web Scraping
Integrovaný XML firewall.	ANO	Zařízení má integrovanou funkcionalitu XML FW
Zakončení uživatelských SSL spojení	ANO	Zařízení umožňuje zakončení uživatelských SSL spojení a tím odlehčení zátěže pro App Servery
Podpora prevence úniku citlivých dat.	ANO	Zařízení slouží jako podpora prevence úniku citlivých dat
Možnost provozu v aktivním i pasivním módu.	ANO	Zařízení je možné provozovat jak v aktivním, tak v pasivním módu
Možnost konfigurace za využití učícího se módu.	ANO	Pro konfiguraci je možné využít „učící se mód"
Poskytuje sadu předdefinovaných vzorů pro nastavení bezpečnostní politiky u vybraných aplikací.	ANO	Zařízení nabízí celou řadu předdefinovaných vzorů nastavení bezpečnostních politik – např. pro produkty MS Exchange, Sharepoint atd...
Schopnost testovat nová bezpečnostní pravidla v non-blokovacím režimu při zachování funkčnosti stávající bezpečnostní politiky WAF.	ANO	Nově vytvořená pravidla je možné otestovat v non-blocking režimu a po odladění je přepnout do režimu blokování
Reporting událostí.	ANO	Zařízení nabízí široké možnosti reportingu událostí
Možnost logovat na externí Syslog server.	ANO	K zařízení je možné připojit externí Syslog server
Sdílení identifikačních informací tzv. Single Sign-On (SSO)	ANO	Zařízení podporuje SSO
Spolupráce s více Active directory, podpora protokolu LDAP	ANO	Zařízení podporuje více současných AD i jiných DB založených na LDAP
Podpora pro protokoly Kerberos, NTLM, NTLM2, Radius, TACAS+, OCSP, Basic access authentication/form autentizace, tzn. aby brána dokázala autentizovaného uživatele na těchto protokolech přihlásit na publikované zdroje	ANO	Zařízení podporuje požadované protokoly a funkcionality

(webserver, vzdálená plocha)		
automatické SSO na webové servery IIS/APACHE/TOMCAT umístěné za reverzní proxy na protokolech Kerberos/NTLM/NTLMv2/Basic access authentication, form autentizace	ANO	Zařízení podporuje požadované protokoly a funkcionality
Kontrolovat / řídit úroveň zabezpečení klientských stanic včetně kontroly aktivních (bezpečnostních) programů a jejich stavu (např. lokální antivirus, antimalware, personální firewall apod.), min. požadované verze OS (servis pack) apod.	ANO	Zařízení podporuje požadované funkcionality
Plnohodnotný VPN přístup pro klienty OS Windows, Linux, Android, iOS, popřípadě další	ANO	Zařízení slouží jako VPN koncentrátor a podporuje požadované typy OS.
Vzdálený SSL VPN přístup (client i clientless mód) pro minimálně 500 současně připojených uživatelů - možnost dalšího rozšíření.	ANO	Zařízení v nabízené konfiguraci umožňuje připojení 500 současných SSL VPN uživatelů. Formou licence je možné tento počet navýšit na 5.000. Formou SW upgrade je pak možné dosáhnout až max. kapacity 10.000 SSL VPN
Podpora publikace virtuálních desktopů VMware Horizon View a Workspace/Microsoft RDP	ANO	Zařízení umožňuje publikaci všech bežných VDI řešení, včetně požaovaného VMware
Podpora publikace Microsoft remote apps	ANO	Zařízení umožňuje publikaci MS remote apps.
Podpora uživatelských rolí	ANO	Zařízení podporuje definici různých uživatelských rolí
Přístupový portál pro uživatele konfigurovatelný na základě členství v rolí. Na základě členství poskytne portál publikovanou webovou stránku, virtuální desktop	ANO	Pomocí zařízení je možné vytvářet různé uživatelské skupiny a k nim přiřazovat různé vlastnosti typu různé aplikace na web-top portálu, odpovídající VDI apod.
Zpřístupnění webové aplikace napřímo i mimo portál, např. pokud uživatel zadá aplikace.domena.cz, tak se mu zobrazí frontend brány a po úspěšné autorizaci se zobrazí požadovaná stránka či aplikace	ANO	Zařízení podporuje požadovanou funkcionalitu
Uživatel musí mít možnost si sám bezpečně změnit expirované heslo v MS AD	ANO	Zařízení podporuje požadovanou funkcionalitu
Možnost bezpečného publikování webové stránky na principu reverzní proxy bez nutnosti autentifikace	ANO	Zařízení podporuje požadovanou funkcionalitu
Programovatelný frontend na úrovni HTML, který umožňuje vytvoření vlastní přihlašovací stránky.	ANO	Zařízení umožňuje vytvoření vlastní přihlašovací stránky
Podpora pro publikování MS SharePoint a Exchange OWA včetně SSO	ANO	Zařízení podporuje požadovanou funkcionalitu
Monitorování cílových serverů a na nich provozovaných služeb prostřednictvím: ICMP, HTTP, HTTPS, TCP, UDP, SNMP	ANO	Zařízení umožňuje monitoring cílových serverů pomocí požadovaných protokolů
Možnost zaznamenávat statistiky provozu HTTP a vytvářet exportovatelné výstupy včetně grafu, přes jednotlivé služby.	ANO	Zařízení podporuje požadovanou funkcionalitu
Možnost zachytit uživatelský HTTP provoz (response/request)	ANO	Zařízení podporuje požadovanou funkcionalitu
Možnost posílání logu na externí úložiště minimálně ve formátu syslog	ANO	Ze zařízení je možné posílat logy na externí úložiště v požadovaném formátu

Je vyžadován provoz zajišťující vysokou dostupnost služby spojením dvou a více zařízení, s podporou režimu active/active.	ANO	Součástí dodávky jsou dvě zařízení, která budou provozována v režimu vysoké dostupnosti
Je vyžadována integrace všech poptávaných funkcionalit do jednoho HW zařízení	ANO	Všechny požadované funkcionality pokrývá jedno HW zařízení
Možnost cachování a komprese http provozu (minimálně 4 Gbps) dle standardů http protokolu	ANO	Zařízení umožňuje cáchování a kompresi http provozu s propustnosti 4Gbps
Plná podpora IPv6, IPv6/IPv4 gateway.	ANO	Zařízení podporuje požadovanou funkcionalitu
Je vyžadováno zpracování SSL komunikace na HW úrovni (šifrovací karta).	ANO	Zařízení z důvodů zajištění dostatečné výkonnosti využívá pro zpracování SSL komunikace speciální šifrovací kartu
Min. 4000 SSL transakcí za sekundu (2K klíče)	ANO	Zařízení má kapacitu/výkonnost 4500 SSL tps (pro 2K klíče)
Zařízení garantuje propustnost šifrovaného provozu min. 8 Gbps	ANO	Zařízení podporuje požadovanou propustnost
Podpora standardu SHA-2 , TLS 1.1 i TLS 1.2	ANO	Zařízení podporuje požadovanou funkcionalitu
Podpora SNMP v1, v2, v3	ANO	Zařízení podporuje požadované protokoly
Možnost odeslání elektronické zprávy (e-mail) určené osobě při vzniku sledované události.	ANO	V případě vzniku sledované události lze ze zařízení odeslat e-mail určené osobě

Požadavky na implementaci
V rámci implementace budou Zhotovitelem realizovány minimálně následující kroky:

- zpracování předimplementační analýzy – popis stávajícího stavu, zpřesnění podkladů pro zadání (organizace, uživatelé, aplikace apod.)
- vytvoření prováděcí dokumentace – důsledně vychází z předimplementační analýzy, obsahuje detailní popis cílového stavu a postupy pro jeho dosažení. Vychází z nejlepších praktik a doporučení výrobců implementovaných technologií. Před zahájením implementace musí být schválena Zadavatelem
- vytvoření testovacího prostředí – migrace vydefinovaných aplikací a asistence při testování klíčových uživatelů
- provedení implementace – vytvoření produkčního prostředí a integrace s prostředím TCK, migrace produkčních aplikací.
- testovací provoz – ověření funkčnosti systému, zátěžové testy
- provedení akceptačních testů – ověření shody cílového stavu s prováděcí dokumentací a splnění předepsaných výkonových parametrů
- předání do ostrého provozu;
- zajištění následné provozu je podrobně popsáno v příloze č. 4;
- zpracování provozní dokumentace;
- Provedené školení administrátorů a správců Zadavatele - 2 dny – administrace a správa řešení, provádění údržby apod.;
- aktualizace provozní dokumentace TCK a 21NET– Zhotovitel provede aktualizaci stávající provozní dokumentace TCK a 21NET tak, aby odpovídala stavu po dokončení toho projektu.

(B) Systém pro ověřování klientů přistupujících do 21NET

Koncept řešení
V rámci této zakázky je požadováno nasazení ověřování stanic, které se připojují ke zdrojům uvnitř prostředí 21NET. Uchazečem navržené řešení musí využívat mechanismu 802.1x společně s dynamickým přiřazováním VLAN sítí.
Při tomto nasazení budou všechny porty lokální sítě považovány implicitně jako nedůvěryhodné a budou odpojeny od zbytku sítě. V případě, že stanice a uživatel splní nastavené politiky, bude vpuštěn do počítačové sítě a bude mu přiděleno příslušné oprávnění. Konkrétní scénář nasazení bude zvolen během implementace, již nyní však lze předpokládat jeden z následujících scénářů:

- uživatelé jsou zařazováni do VLAN sítí dle členství ve skupinách MS ActiveDirectory
- uživatelé jsou zařazování do VLAN sítí dle místa, odkud se přihlašují (např. pokud se přihlásí uživatel ve skladu, má jiná oprávnění, než pokud se přihlásí v kanceláři)
- do rozhodovacího procesu mohou být zařazeny také informace o stavu OS, antiviru, personálního FW apod. (neaktualizovaný antivir způsobí, že se uživatel plnohodnotně nepřipojí, dokud antivir neaktualizuje)

Je vyžadováno, aby řešení bylo založeno na standardizovaných komponentách (RADIUS server, 802.1x supplicant atd.).

V rámci dodávky je požadována implementace ověřování uživatelů v síti 21NET (jen na dodaných přepínačích a bezdrátové síti). Je požadováno, aby nasazení zahrnovalo dodávku RADIUS serveru s licencemi pro min. 500 současné připojených uživatelů. Podstatné je, aby uchazeč zajistil, aby bylo řešení vysoce dostupné, aby v případě výpadku jednoho RADIUS serveru bylo zajištěno fungování druhého – redundantního serveru. Dále je požadována integrace se stávajícím systémem pro správu a dohled infrastruktury PRTG. Rovněž je požadováno, aby byl systém integrován se systémem pro korelační analýzu událostí – SIEM (specifikace v kapitole níže).

V budoucnu musí být možné systém rozšířit o kontrolu stavu koncových zařízení (verze OS, stav antiviru, stav personálního firewallu apod.). Rozšíření musí být rovněž možné také s ohledem na počet uživatelů (zapojení několika stovek organizací, zapojení uživatelů KU apod.), maximální počet uživatelů musí být minimálně 2500.

Je požadováno, aby součástí dodávky byly všechny potřebné HW a SW komponenty pro všechny uvažované aktivní prvky a uživatele.

Přístupové aktivní prvky, které slouží k připojování klientů, zahrnují modely HP 5800 a HP 3100 EI. Je požadováno, aby navržené řešení bylo s nimi plně kompatibilní. Nastavení těchto aktivních prvků bude provedena Zadavatelem na základě podkladů dodavatele a po jejich vzájemném odsouhlasení.

Součinnost zadavatele
V případě, že výrobce systému podporuje běh ve virtuálním prostředí, nabízí zadavatel možnost vytvoření virtuálního serveru ve stávající VMware ESX infrastruktuře viz. kapitola Popis souvisejícího současného stavu prostředí KUZK.

Veškeré změny v konfiguracích stávajících aktivních prvků a serverů TCK a 21NET bude provedena Zadavatelem dle specifikace požadavků Dodavatelem a po jejich vzájemném odsouhlasení.

Požadované technické parametry

Požadovaná hodnota	Splňuje ANO/NE	Uchazečem nabízené řešení či parametr
Ověřování pro minimálně 500 souběžných uživatelů (uživatelé, zařízení, hosté, ...)	ANO	Nabízené řešení, které je plně kompatibilní se zařízeními používanými v současné síti a zároveň v souladu s celkovým záměrem Zadavatele prezentovaným v poskytnuté „Studii proveditelnosti" je postavené na produktu společnosti HP, konkrétně jde o zařízení IMC Standard, doplněné o softwarový modul UAM - User Access Manager. Předpokládáme dodávku formou SW, který bude nainstalovaný na VM v rámci stávající VMware ESX infrastruktury. Požadavky (doporučovaný Systém HW) pro Server: • 4 x 3.0 GHz Intel (4 CPU or 2x Dual-Core CPU) • 4 GB RAM memory • 100 GB storage Požadavky (doporučovaný Systém HW) pro Klienta: • 2.0 GHz Intel® Pentium® III or equivalent processor • 2 GB RAM memory 50 GB storage
Samoobslužný portál pro uživatele	ANO	Součástí zařízení je samoobslužný portál pro uživatele
Samoregistrace uživatelů a hostů	ANO	Na samoobslužném portále je možné provádět samoregistraci uživatelů a hostů
Portál pro recepční, generování jednorázových a časově omezených přístupových údajů	ANO	Součástí zařízení je portál pro recepční a umožňuje generování přístových údajů jak je požadováno
Podpora 802.1X autentifikace, MAC autentifikace,webové autentifikace a autentifikace VPN tunelů	ANO	Zařízení podporuje všechny požadované typy autentifikace
Synchronizace s LDAP a Microsoft AD,	ANO	Zařízení je možné synchronizovat s LDAP a MS AD
Podpora multi-tenancy správy systému (možnost operátorských účtů pro skupiny lokalit a služeb),	ANO	Je možné přidělovat role a pravomoci pro různé skupiny a typy operátorů
Možnost přiřazení VLAN uživatelů s výběrem v nástroji z existujících VLAN názvů v síti,	ANO	Zařízení splňuje požadovaný způsob přiřazování VLAN
Možnost přiřazení ACL uživateli s možností toto v nástroji definovat, upravovat a jednoduše vybírat,	ANO	Zařízení splňuje požadovaný způsob přiřazování ACL
Možnost nastavení vendor specific RADIUS atributů s aplikací dle typu a umístění zařízení a politiky,	ANO	Zařízení podporuje vendor specifické RADIUS atributy, kompatibilní s požadavky stávající infrastruktury
Podpora ověřování PAP, CHAP, EAP-PEAP a EAP-TLS,	ANO	Zařízení podporuje požadované typy ověřování

- Určit kritická místa sítě a optimalizovat její infrastrukturu (plánování kapacit sítě, sledování trendů).

Součinnost zadavatele
V případě, že výrobce systému podporuje běh ve virtuálním prostředí, nabízí zadavatel možnost vytvoření virtuálního serveru ve stávající VMware ESX infrastruktuře viz. kapitola Popis souvisejícího současného stavu prostředí KUZK.

Veškeré změny v konfiguracích stávajících aktivních prvků a serverů TCK a 21NET bude provedena Zadavatelem dle specifikace požadavků Dodavatelem a po jejich vzájemném odsouhlasení.

Požadované technické parametry

Požadovaná hodnota	Splňuje ANO/NE	Uchazečem nabízené řešení či parametr
Podpora běhu ve VMWare prostředí, popřípadě variantně dvojice dedikovaných redundantní HW zařízení (v každém datovém centru jedno, podpora A/S konfigurace)	ANO	Nabízené řešení, které je plně kompatibilní se zařízeními používanými v současné síti a zároveň v souladu s celkovým záměrem Zadavatele prezentovaným v poskytnuté „Studii proveditelnosti“ je postavené na produktu společnosti INVEA-TECH. Konkrétně jde o zařízení INVEA, FlowMon, Collector, IFC-3000-VA a INVEA, FlowMon, ADS. Předpokládáme dodávku formou SW, který bude nainstalovaný na VM v rámci stávající VMware ESX infrastruktury. Požadavky (doporučovaný Systém HW) pro FlowMon: 4 CPU jádra, 8GB RAM, 2000 IOPS, úložná kapacita min. 3TB
Schopnost pojmout agregovaná data (disková kapacita alespoň 3TB)	ANO	Navržené zařízení má schopnost pojmout až 3TB dat. Vlastní kapacita záleží na poskytnuté úložné kapacitě.
Kolektor umožňující příjem sFlow, Netflow a Ipfix exportů	ANO	Kolektor umožňující příjem sFlow, Netflow a Ipfix
Tvorba uživatelských statistik a grafů	ANO	Statistiky jsou zobrazovány ve formě grafů a tabulek s možností volby různých perspektiv
Analýza trendů v síti	ANO	Systém sleduje a analyzuje trendy v síti, např. trendy chování uživatelů, dlouhodobé profily chování zařízení na síti z pohledu služeb, objemů provozu a komunikačních partnerů
Automaticky generované a zasílané reporty	ANO	Systém vytváří komplexní grafické reporty rozesílané automaticky nebo generované z aplikace na vyžádání ...
Detekce anomálií včetně konkrétních typů bezpečnostních hrozeb	ANO	Je možné detekovat tyto typy hrozeb: Útoky - skenování portů, slovníkové útoky, denial of service, útoky prostřednictvím telnet protokolu a další, Anomálie datového provozu - DNS, ICMP, DHCP, multicast, nestandardní komunikace, Anomálie v chování zařízení - změna dlouhodobého profilu chování zařízení, změna chování sítě, Nežádoucí aplikace - P2P sítě, Instant messaging, anonymizační služby, TOR, TeamViewer, Bezpečnostní incidenty - viry, spyware, botnety, cizí zařízení v síti, komunikace s IP adresami na blacklistech, Poštovní provoz - odchozí spam, chybná konfigurace, Provozní problémy - zpoždění, nadměrná zátěž,

		reverzní DNS záznamy, nefunkční aktualizace, Potenciální únik dat a informací - upload dat na veřejné servery, webová úložiště, podezřelé destinace
Detekce zero-day útoků na základě chování sítě	ANO	Zařízení detekuje zero-day útoky
Schopnost zpracovat min. 150tis toků za vteřinu	ANO	Zařízení dokáže zpracovat až 150.000 toků za vteřinu...

Požadavky na implementaci
V rámci implementace budou Zhotovitelem realizovány minimálně následující kroky:

- zpracování předimplementační analýzy – popis stávajícího stavu, zpřesnění podkladů pro zadání (organizace, uživatelé, aplikace apod.)
- vytvoření prováděcí dokumentace – důsledně vychází z předimplementační analýzy, obsahuje detailní popis cílového stavu a postupy pro jeho dosažení. Vychází z nejlepších praktik a doporučení výrobců implementovaných technologií. Před zahájením implementace musí být schválena Zadavatelem
- provedení implementace – v integrace s prostředím TCK a 21NET, migrace 15ti lokalit 21NET.
- testovací provoz – ověření funkčnosti systému, zátěžové testy
- provedení akceptačních testů – ověření shody cílového stavu s prováděcí dokumentací a splnění předepsaných výkonových parametrů
- předání do ostrého provozu;
- zajištění následné provozu je podrobně popsáno v příloze č. 4;
- zpracování provozní dokumentace;
- Provedené školení administrátorů a správců Zadavatele – min. 1 den – administrace a správa řešení, provádění údržby;
- aktualizace provozní dokumentace TCK a 21NET– Zhotovitel provede aktualizaci stávající provozní dokumentace TCK a 21NET tak, aby odpovídala stavu po dokončení toho projektu.

(D) Systém pro korelační analýzu událostí – SIEM

Aktuálně je v TCK prováděn provozní monitoring infrastruktury a Windows serverů systémem PRTG. Není zde implementován systém pro sběr a vyhodnocování logů s událostmi bezpečnostní povahy.

Koncept řešení
Zadavatel požaduje dodávku systému SIEM (Security Information and Event Management), který automaticky sbírá, archivuje a analyzuje logy bezpečnostní povahy napříč celou infrastrukturou od síťových prvků přes různé operační systémy až po aplikace. Nad těmito daty pak probíhá pokročilá analýza, korelace a notifikace vyhodnocených bezpečnostních událostí a fenoménů. Díky tomuto systému je možné mít aktuální přehled o potencionálních i skutečných anomáliích, hrozbách a bezpečnostních incidentech sledovaného prostředí. K nim poskytuje zdrojová data pro daný kontext a řešení. SIEM je řízen sadou pravidel vzniklých z předem popsaných modelových situací. Systém obsahuje také předdefinované pohledy a reporty podle mezinárodních standardů jako PCI-DSS, HIPAA, NERC-CIP, FISMA a další pro účely auditu.
Komunikace mezi agentem a SIEM systémem probíhá šifrovaně a pro úsporu přenosové kapacity jsou přenášená data komprimována.

Zdroje dat pro SIEM systém budou minimálně zahrnovat sběr dat z níže uvedených zařízení zadavatele:

- 100 Windows serverů (verze 2008, 2012)

- 30 Linux serverů
- 10 MS SQL serverů
- 2 firewally Fortinet Fortigate 3140B
- 4 přepínače HP 7500
- 20 přepínačů HP 5800
- 50 přepínačů HP 3100
- 20 přepínačů Cisco Catalyst 2950, 3550, 2960, 3560
- bezdrátový kontroler Cisco WLC 5508
- 2 Microsoft doménové kontrolery
- 2 HP Tippingpoint S1400N
- 2 Loadbalancery

Analýza rozsahu a způsobu sběru logů je součástí implementačních prací, jejich rozsah bude přesně definován v prováděcím projektu před samotnou implementací. Nad takto definovaným rozsahem pak budou stanovena bezpečnostní pravidla pro Correlation engine.

Požadované technické parametry

Parametr	Specifikace minimálních požadavků	Splněno Ano/Ne	Uchazečem nabízené řešení či parametr
Platforma	virtuální appliance	ANO	VMware virtuální appliance, model ELU4
Propustnost	1000 EPS	ANO	Doporučený sizing výrobce pro tento model je 1000 EPS
Administrativní rozhraní	Centrální grafická konzole	ANO	Dostupná pomocí webového browseru
	Delegace oprávnění přístupu ke konfiguraci a reportingu	ANO	Delegace podle typů akcí a zařízení na úrovni SIEMu nebo sběr logů, se kterými má uživatel pracovat
Podpora protokolů a přenosu dat	Syslog	ANO	Podpora UDP/TCP a SSL
	SNMP	ANO	Podpora verze 2 i 3
	WMI	ANO	Včetně nejnovějších verzí Windows
	Lokální agentna dohledovaném zařízení	ANO	Podpora Windows i Linux
Podpora sběru dat bez nutnosti instalace agenta z technologii	Wmware	ANO	Typický způsob sběru logů: Syslog
	Linux	ANO	Typický způsob sběru logů: Syslog, SCP
	Windows Server	ANO	Typický způsob sběru logů: WMI, RPC
	Microsoft SQL	ANO	Typický způsob sběru logů: WMI, RPC, CIFS
	Oracle DB	ANO	Typický způsob sběru logů: DB konektor
	Microsoft Exchange	ANO	Typický způsob sběru logů: WMI, RPC, CIFS
	Tipping Point IPS	ANO	Typický způsob sběru logů: Syslog
	Fortigate firewall	ANO	Typický způsob sběru logů: Syslog
	Síťové prvky HP	ANO	Typický způsob sběru logů: Syslog

Práce s daty	Online sledování v reálném čase	ANO	Tail funkce v grafické rozhraní s množstvím filtrů
	Korelace událostí v čase z více zdrojů	ANO	Variabilní možnosti definice korelací
	Tvorba uživatelských šablon reportů	ANO	K dispozici je WYSIWYG editor
Reporting	TBD	ANO	Předpokládáme, že požadavek míří na automatizaci generování reportů, jejich ukládání a zasílání emailem (k tomu se vztahuje i odpověď „Ano")
Archivace dat	Definice retenční doby pro automatický převod dat do archivu	ANO	Definice retenční doby pro automatický převod dat do archivu
	Podpora ukladání archivních dat na uložiště CIFS,NFS, NAS	ANO	Může být více archivních „poolů" připojených přes různé technologie.
	Ochrana archivu před neprávněnou manipulací	ANO	Ochrana integrity po celou dobu zpracování logů, včetně těch archivovaných. Vše je ověřeno certifikacemi FIPS a Common Criteria
Notifikace vyhodnocených incidentů	email, syslog, SNMP trap	ANO	Automatická akce na základě definovaných podmínek. Notifikace mohou být customizovány.
Rozšiřitelnost	Podpora a otevřenost pro rozšíření na distribuovaný model sběru a zpracování dat	ANO	Je možné přidávat další moduly pro sběr a vyhodnocování

Požadavky na implementaci
V rámci implementace budou Zhotovitelem realizovány minimálně následující kroky:

- zpracování předimplementační analýzy – popis stávajícího stavu, zpřesnění podkladů pro zadání
- vytvoření prováděcí dokumentace – důsledně vychází z předimplementační analýzy, obsahuje detailní popis cílového stavu a postupy pro jeho dosažení. Vychází z nejlepších praktik a doporučení výrobců implementovaných technologií. Před zahájením implementace musí být schválena Zadavatelem
- provedení implementace – v integrace s prostředím TCK a 21NET, migrace 15ti lokalit 21NET.
- testovací provoz – ověření funkčnosti systému, zátěžové testy
- provedení akceptačních testů – ověření shody cílového stavu s prováděcí dokumentací a splnění předepsaných výkonových parametrů
- předání do ostrého provozu;
- zajištění následné provozu je podrobně popsáno v příloze č. 4;
- zpracování provozní dokumentace;

- Provedené školení administrátorů a správců Zadavatele – min. 2 dny – administrace a správa řešení, vyhodnocování dat, provádění údržby;
- aktualizace provozní dokumentace TCK a 21NET– Zhotovitel provede aktualizaci stávající provozní dokumentace TCK a 21NET tak, aby odpovídala stavu po dokončení toho projektu.

Příloha č. 2 Smlouvy: Soupis použitých komponent

Souhrnný soupis použitých komponent (prvků). V tabulce budou uvedeny veškeré hw i sw komponenty. Budou uvedeny přesné a celé názvy, tak aby bylo možné jednoznačně identifikovat o jaký produkt (např. o jakou licenci) a v jaké množství se jedná.

Množství	p/n	Název	Specifikace	Jednotková cena v Kč bez DPH
Rozšíření TCK o LoadBalancer a webaplikační firewall				
2	F5-BIG-ADC-4000S-SEC	BIG-IP 4000s Application Delivery Controller Security (16 GB Memory, Local Traffic Manager, Application Security Manager, Access Policy Manager, 500 Concurrent VPN Users, Max SSL, Max Compression)	Základní chassis F5 BIG-IP 4000S; 8 x 10/100/1000Mbps Ethernet interface a zároveň min. 2 x 10 Gbps interface (bez SFP+ modulů); napájecí zdroj. Součástí jsou SW licence LTM (load balancing), APM (SSL VPN + Reverzní proxy + licence pro 500 SSL VPN současných uživatelů) a ASM (web aplikační FW).	1 100 000,- Kč
2	F5-UPG-AC-400W	BIG-IP Single AC Power Supply for 4200v/4000s/2X00s (400 W, Field Upgrade)	Redundantní zdroj napájení	32 000,- Kč
4	F5-UPG-SFP+-R	BIG-IP & VIPRION SFP+ 10GBASE-SR Transceiver (Short Range, Field Upgrade)	SFP+ optický tranceiver 10G, MM	34 000,- Kč
Systém pro ověřování klientů přistupujících do 21NET				
1	JG747AAE	HP IMC Std SW Plat w/ 50 Nodes E-LTU	HP IMC Standard Software Platform - SW	55 000,- Kč
1	JG752AAE	HP IMC UAM SW Mod w/ 50-user E-LTU	HP IMC UAM - rozšiřující SW modul UAM - User Access/Authentication manager - včetně licence pro 50 současně připojených uživatelů	37 000,- Kč
9	JG753AAE	HP IMC UAM SW Mod Add 50-user E-LTU	HP IMC UAM - licence pro rozšíření o 50 současných uživatelů	12 000,- Kč
Systém pro analýzu datových toků				
1	1. IFC-3000-VA	INVEA, FlowMon, Collector, IFC-3000-VA	INVEA FlowMon - FlowMon kolektor ve formě virtuálního zařízení, licencovaná úložná kapacita 3TB. Předpokládáme provoz ve stávající VMware ESX infrastruktuře.	20 000,- Kč
1	FPC-ADS-B	INVEA, FlowMon, ADS, ADS Business (2 uživatel, 2 zdroj dat, 1500 fps)	INVEA FlowMon - ADS, SW nadstavba pro detekci anomálií a nežádoucího chování v datové síti	210 000,- Kč
Systém pro korelační analýzu událostí – SIEM				
1	ELUCKE-AA-AA	McAfee Enterprise Security Manager, Enterprise Log Manager and Event Receiver VM (up to 8 cores) - perpetuální licence s podporou Gold Software Support na 1 rok	McAfee Enterprise Security Manager, Enterprise Log Manager a Event Receiver - SIEM SW, 1x VM (do 8 CPU jader)	390 000,- Kč

Řádky tabulky budou přidány dle skutečného počtu komponent.

Příloha č. 3 Smlouvy: Bezpečnostní pravidla ICT

Bezpečnostní pravidla Informačních a komunikačních technologií (ICT) pro práci v informačním systému (IS) Krajského úřadu Zlínského kraje (KÚZK nebo jen úřad)

Přístup do IS KÚZK

- Přístup jiných subjektů k ICT úřadu (dále jen „druhá smluvní strana") je možný pouze na základě smluvně ošetřeného vztahu s krajem.
- Druhá smluvní strana je povinna dodržovat bezpečnostní pravidla ICT pro práci v IS KÚZK a nese v souladu s platnou legislativou a předpisy svůj díl odpovědnosti za nedodržení či porušení pravidel, případně za škody vzniklé v důsledku bezpečnostních incidentů, které zavinila.
- Všechny povolené způsoby přístupu, povolené časy pro přístup, přístupové údaje a přidělená oprávnění musí být písemně dohodnuty mezi smluvními stranami. Tyto údaje jsou důvěrné a jsou platné jen po dobu platnosti smlouvy.
- Druhá smluvní strana je odpovědná za používání jim přiděleného přístupu do IS KUZK, za svou činnost v IS úřadu a při práci s informacemi.
- Přistupovat k ICT úřadu mohou pouze poučení pracovníci druhé smluvní strany. Druhá smluvní strana zajistí před zahájením poučení a proškolení všech svých pracovníků a subdodavatelů, kteří budou přistupovat k ICT úřadu.
- Přístup a přístupová oprávnění jsou přidělena pouze v rozsahu nezbytně nutném pro výkon smluvních závazků.
- Pracovníci druhé smluvní strany jsou povinni řídit se pokyny oprávněných osob a dalších pracovníků oddělení informatiky KÚZK.
- Činnost druhé smluvní strany v IS úřadu může být monitorována. Pověření pracovníci úřadu mohou evidovat přístupy a ověřovat dodržování stanovených bezpečnostních pravidel.

Vzdálený přístup

- Vzdálený přístup do IS KÚZK je možný pouze dohodnutým způsobem z pracovní stanice která má aktivní a aktuální antivirovou ochranu a nainstalovány všechny bezpečnostní záplaty operačního systému vydané výrobcem.
- Pro zvýšení bezpečnosti je Vzdálený přístup povolen pouze z konkrétních IP adres druhé smluvní strany.

Fyzický přístup k ICT

- Fyzický přístup k prostředkům ICT je možný pouze na základě smluvního vztahu (servisní a dodavatelské organizace, dohody o provedení práce apod.) nebo se souhlasem určené odpovědné osoby, kterou může být vedoucí odboru, vedoucí oddělení informatiky nebo vlastník aktiva.
- Pohyb pracovníků druhých smluvních stran v prostorách serverovny (servisní zásah, revize zařízení apod.) je možný pouze v doprovodu odpovědných pracovníků oddělení informatiky a se souhlasem vedoucího oddělení informatiky.

- Pro práci v IS úřadu smí být použita pouze přidělená technika kraje. Připojování cizí techniky do vnitřní sítě úřadu je bez souhlasu správce systému zakázáno.
- Na přidělenou techniku nesmí být bez souhlasu pověřené osoby instalován nebo z ní odebírán žádný software.
- Při opuštění pracoviště je vždy nutné provést vhodným způsobem jeho zajištění.

Ochrana dat a informačních aktiv

- Druhá smluvní strana odpovídá za všechna převzatá data (elektronická a tištěná), způsob jejich použití a ochranu před neoprávněným přístupem a zneužitím.
  Není-li ve smlouvě stanoveno jinak, před ukončením smluvního vztahu druhá smluvní strana vrátí všechna převzatá data.

- Druhá smluvní strana je do protokolárního předání pracovníkům úřadu odpovědná za všechna zpracovávaná aktiva a je povinna je odpovídajícím způsobem zabezpečit.
- Pracovní data se ukládají pouze na místa, určená pověřenou osobou.
- Pokud druhá smluvní strana při práci v IS úřadu přijde do styku s osobními údaji dle zákona č. 101/2000 Sb. nebo jinými neveřejnými informacemi, je povinna o zjištěných skutečnostech zachovávat mlčenlivost a zajistit jejich utajení.
- Nepotřebná data (elektronická, na mediích i papírová) musí být vždy neprodleně zlikvidována.
- Druhá smluvní strana je povinna dodržovat zásady ochrany proti virům a škodlivým kódům.
- Všechny zásahy na serverech musí být předem odsouhlaseny správcem IS a zaznamenány stanoveným způsobem.

Bezpečnostní incidenty

- Druhá smluvní strana je povinna neprodleně hlásit odpovědným osobám porušení těchto pravidel, všechny zjištěné neobvyklé události, které jsou, nebo mohou být bezpečnostními incidenty a zranitelná místa, a účinně pomáhat při jejich prošetřování a odstraňování.
- Druhá smluvní strana je povinna hlásit všechny zjištěné nedostatky nebo nesoulad se skutečností.
- Druhé smluvní straně není povoleno řešení bezpečnostních incidentů a odstraňování nedostatků či nesouladů vlastními silami bez předchozího schválení bezpečnostním správcem ICT.

Používání internetu

- Druhá smluvní strana může používat při práci v IS KÚZK internet pouze pro pracovní účely při dodržování všech bezpečnostních pravidel, platných pro práci s internetem. Stahování souborů, používání FTP a jiných služeb je možné jen po dohodě se správcem systému KÚZK.
- Pokud není ve smlouvě stanoveno jinak, není povoleno využívat elektronickou korespondenci z prostředí KÚZK.

Tisk

- Pokud bude druhé smluvní straně umožněn tisk na tiskárnách kraje, je povinna šetřit spotřební materiál a tištěné dokumenty zabezpečit proti neoprávněnému přístupu jak během tisku, tak i po jeho vytisknutí až do jejich bezpečné likvidace.

Účty a hesla

- Druhá smluvní strana smí používat pouze jí přidělené přihlašovací účty. Tyto účty jsou chráněny heslem.
- Heslo musí splňovat aktuální požadavky na kvalitu a platnost a musí být uchováno v tajnosti.
- Názvy přihlašovacích účtu a hesla nesmějí být sděleny žádné neoprávněné osobě.
- V případě porušení bezpečnostních pravidel mohou být druhé straně přístupové účty zablokovány nebo zcela odebrány.

Pozn.: Druhé smluvní straně je přísně zakázáno vykonávat jiné než dohodnuté činnosti, přistupovat k jiným než povoleným prostředkům, serverům a datům nebo provádět jakékoli úkony směřující k zjišťování rozsahu přidělených oprávnění, dostupnosti jiných síťových prostředků a služeb a způsobech zabezpečení.

Příloha č. 4 Smlouvy: Podmínky zajištění podpory díla

Podpora díla (záruka a servis) se vztahuje na všechny aktivity (A – D) a je zajišťována ihned po ukončení fáze 2 pro HW komponenty a ihned po ukončení fáze 3 pro SW komponenty:

(A) Rozšíření TCK o LoadBalancer a webaplikační firewall

(B) Systém pro ověřování klientů přistupujících do 21NET

(C) Systém pro analýzu datových toků

(D) Systém pro korelační analýzu událostí – SIEM

Požadovaná podpora je pro výše uvedené aktivity projektu specifikovány takto:

- je požadována záruka na HW komponenty dodávky v délce min. 60 měsíců, oprava následují pracovní den;
- dostupnost bezpečnostních aktualizací pro veškeré použité komponenty minimálně po dobu 60 měsíců
- maintenence (technická podpora výrobce a nárok na nové hlavní verze software) minimálně po dobu 60 měsíců
- registrace (v případě, že je vyžadována) a předání přístupu na portál výrobce, ze kterého lze stahovat aktualizace
- je požadováno, aby záruka byla zajišťována výhradně službami daného výrobce

Podmínky zajištění následného provozu po dobu 12 měsíců ihned po ukončení fáze 3 nad rámec výše uvedeného jsou specifikovány takto:

1. Pro potřeby naplnění této smlouvy Zhotovitel zajistí jednotné kontaktní místo pro hlášení poruch či změnových požadavků. Všechna hlášení (tickety) budou evidována a jejich zadavatel bude informován o aktuálním stavu. Zároveň musí být umožněno měření SLA.
2. Jednotným kontaktním místem je myšleno:
   - systém helpdesk na adrese https://servicedesk.autocont.cz (Zhotovitel je povinen zpřístupnit svůj helpdesk objednateli nejpozději v průběhu fáze 2.)
   - e-mail na adrese servicedesk@autocont.cz, pokud není možno použít helpdesk, objednatel požadavek do helpdesku dodatečně doplní
   - telefon na čísle +420 251 022 564, v případě nefunkčnosti +420 723 465 409, pokud není možno použít helpdesk, objednatel požadavek do helpdesku dodatečně doplní
3. Pro hlášení poruch či změnových požadavků je objednatel oprávněn využít kterýkoli z výše uvedených informačních kanálů.
4. Systém helpdesk musí zajistit:
   - jednoduché a pohodlné vkládání požadavků uživatelem podle jeho oprávnění, např. formou grafického průvodce vložení požadavku
   - aktuální seznam hlášených požadavků s historií a aktuálním stavem řešení a řešitelem
   - e-mailové notifikace zhotoviteli a objednateli při změně stavu řešení požadavku
   - možnost nastavení priority změnových požadavků
   - přístup k aplikaci přes internetový prohlížeč – bez nákladů na software pro objednatele.

Zlínský kraj
krajský úřad
Odbor řízení dotačních programů
nám. Tomáše Bati 21, 761 90 Zlín
IČ: 70891320, třída Tomáše Bati 21, 761 90 Zlín
tel.: +420 577 043 111, fax: +420 577 043 202
podatelna@kr-zlinsky.cz, www.kr-zlinsky.cz

Specifikace požadovaných služeb (SLA), které je zhotovitel povinen zajistit:

5. Zajištění následného provozu v režimu 10x5 zahrnuje zejména:
    - proaktivní řešení poruch a chybových stavů s dobou odstranění problému nejpozději následující pracovní den od jeho vzniku; vznik problému bude detekován buď pomocí monitorovacích nástrojů dodavatele nebo pomocí senzorů stávajícího nástroje pro dohled infrastruktury TCK (PRTG); konfigurace potřebných senzorů proběhne v rámci implementace; potřebnou specifikaci senzorů dodá dodavatel
    - provádění změn konfigurace dle požadavku zadavatele; požadavky budou členěny podle priority, přičemž požadavek s vysokou prioritou musí být vyřešen nejpozději následující pracovní den od jeho podání a požadavek s nízkou prioritou musí být vyřešen do nejpozději do třech následujících pracovních dnů od jeho podání
    - provádění aktualizací
    - konzultace v souhrnné rozsahu 14hodin/měsíc s možností převodu nevyužitých hodin do dalšího období. Hodiny jsou pro jednotlivé oblasti děleny takto:
        - (A) Rozšíření TCK o LoadBalancer a webaplikační firewall 4hodiny/měsíc
        - (B) Systém pro ověřování klientů přistupujících do 21NET 2hodiny/měsíc
        - (C) Systém pro analýzu datových toků 4hodiny/měsíc
        - (D) Systém pro korelační analýzu událostí – SIEM 4hodiny/měsíc
6. Zhotovitel se zavazuje každou zjištěnou poruchu či chybový stav zapsat do systému helpdesk tak, aby měl objednatel možnost kontroly evidence řešených poruch či chybových stavů. Z této evidence musí být zřejmý minimálně datum a čas vzniku, řešitel a popis.
7. Režim 10x5 znamená dostupnost minimálně v pracovní dny od 8:00 do 18:00.

Oprávněné osoby:

8. Oprávněné osoby objednatele:

    Bedřich Polák, e-mail: bedrich.polak@kr-zlinsky.cz, tel. 577 043 256

    Bc. Josef Gottwald, e-mail: Josef.gottwald@kr-zlinsky.cz, tel. 577 043 265

    RNDr. Ivo Skrášek, e-mail: ivo.skrasek@kr-zlinsky.cz, tel. 577 043 260

9. Oprávněné osoby zhotovitele:

    Tomáš Sládek, e-mail: tomas.sladek@autocont.cz, tel. +420 602 590 926

    Jiří Kavan, e-mail: jiri.kavan@autocont.cz, tel. +420 602 734 977

Ověřovací doložka autorizované konverze z moci úřední do PDF dokumentu

Ověřuji pod pořadovým číslem 65390275-49351-141002142810, že tento dokument, který vznikl převedením vstupu v listinné podobě do podoby elektronické, skládající se z 36 listů, se doslovně shoduje s obsahem vstupu.

Autorizovanou konverzí dokumentu se nepotvrzuje správnost a pravdivost údajů obsažených v dokumentu a jejich soulad s právními předpisy.

Zajišťovací prvek:

bez zajišťovacího prvku

Subjekt, který autorizovanou konverzi dokumentu provedl:

Zlínský kraj

Datum vyhotovení ověřovací doložky:

2.10.2014

Jméno, příjmení a podpis osoby, která autorizovanou konverzi dokumentu provedla:

David Neulinger

65390275-49351-141002142810

Poznámka:

Kontrolu této ověřovací doložky lze provést v centrální evidenci ověřovacích doložek přístupné způsobem umožňujícím dálkový přístup na adrese https://www.czechpoint.cz/overovacidolozky.