

Číslo Smlouvy MF

17-909-0066

Toto číslo uvádějte při fakturaci

SMLOUVA

na dodávku a implementaci systémů pro centralizovanou správu logů, událostí a strojových dat (systém SEM)

uzavřená ve smyslu ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku, ve znění pozdějších předpisů (dále jen „Občanský zákoník“) v souladu se zákonem č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů (dále jen „ZZVZ“) na základě výzvy k podání nabídky ve věci veřejné zakázky malého rozsahu zadané prostřednictvím Národního elektronického nástroje (NEN) pod č.j.: MF-33769/2017/9003-1

Evidenční číslo: 9009/096/2017

(dále jen „Smlouva“)

Smluvní strany

Česká republika - Ministerstvo financí

Sídlo: Letenská 15, 118 10 Praha 1

jejímž jménem jedná: Viktor Janáček, pověřen řízením odboru 70

IČO: 00006947

DIČ: CZ 00006947

bankovní spojení:

ID datové schránky: xzeaauv

(dále jen „Objednatel“)

a

Caleum a.s.

Sídlo: Na Pankráci 1724/129, 140 00 Praha - Nusle

zapsaná v obchodním rejstříku pod spisovou značkou B 18559 vedenou u Městského soudu v Praze

zastoupená: Josefem Ladrou, předsedou představenstva

IČO: 28351363

DIČ: CZ28351363

bankovní spojení:

ID datové schránky: ecfi232

(dále jen „Zhotovitel“)

(Objednatel a Zhotovitel společně dále též jen jako „Smluvní strany“ a jednotlivě jako „Smluvní strana“).

PREAMBULE

Tato Smlouva se uzavírá na základě výsledků zadávacího řízení veřejné zakázky na dodávku a implementaci „Systémů pro centralizovanou správu logů, událostí a strojových dat (systém SEM)“ (dále též „Zadávací řízení“), kdy nabídka Zhotovitele byla vybrána jako nejvhodnější. Pokud se v této Smlouvě odkazuje na zadávací podmínky, zadávací dokumentaci či nabídku Zhotovitele, míní se tím dokumenty související se Zadávacím řízením (dále jen „Dokumenty Zadávacího řízení“).

I. Účel Smlouvy

Účelem této Smlouvy je plnění požadavků Zákona o kybernetické bezpečnosti č. 181/2014 Sb., ve znění pozdějších předpisů, v informačním prostředí Ministerstva financí ČR (dále jen „IS MF“) zajištěním Systémů pro centralizovanou správu logů, událostí a strojových dat (dále jen „Systém SEM“).

II. Předmět Smlouvy

1) Předmětem plnění této Smlouvy je závazek Zhotovitele zajistit:

1.1. Hardware (dále jen „HW“) a **software** (dále jen „SW“) pro dva Systémy SEM do IS MF v rozsahu a funkcích:

- a) sběr logů z infrastrukturních prvků, databázových strojů a aplikačního programového vybavení IS MF (tj. networking, firewally, DB, OS serverů a stanic),
- b) aplikační podpora pro tvorbu jednotného formátu ukládaných logů (parser),
- c) jednotné centrální dlouhodobé úložiště logů,
- d) u každého Systému pro centralizovanou správu logů, bude kapacita úložiště pro logy o velikosti min. 40 TB (minimální ochrana proti ztrátě dat RAID 5, nebo 6).
- e) generování výstrah (alerting a reporting),
- f) plnění požadavků Zákona o kybernetické bezpečnosti č. 181/2014 Sb. ve znění pozdějších předpisů, ve smyslu prováděcí §21 vyhlášky č. 316/2014 Sb. §21,
- g) ověřování přijetí, integrity a zdroje záznamu,
- h) uživatelské GUI pro sledování aktuálních stavů, generování reportů a sestav pro kontrolní a analytickou činnost,
- i) podpora vysoké dostupnosti formou geografická redundance mezi nástroji pro centralizovanou správu logů a jejich úložištěm (forma – master-slave),
- j) aplikační vybavení pro sběr logů, událostí a strojových dat ze dvou vzdálených lokalit Objednatele (z lokality Vápenka a Voctářova do lokality Letenská),
- k) Instalační, provozní a uživatelská dokumentace,
- l) instalační média k dodanému SW a operačnímu systému.

1.2. Implementaci a zprovoznění Systému SEM do IS MF, které spočívá v :

- a) instalaci dodaného HW a SW vybavení do prostředí IS MF,
- b) konfiguraci řešení o vysoké dostupnosti ,
- c) výrobě, implementaci a zprovoznění log parserů pro:
 - 17 aplikačních agend (systémů),
 - systém SAP,
 - Symantec messaging gateway
- d) instalaci a zprovoznění sběru logů nástroji podporovaných formátů do oblastí infrastruktury IS MF:
 - networking, firewally a systémů pro řízení protokolů 802.,
 - servery a stanice s OS Windows, Linux, Solaris, HP Unix,
 - VMware,
 - Antiviry Symantec,
 - Adresářové služby MS Active Directory,
 - Databáze Oracle, Informix, MS SQL, My SQL,

- e) dokumentaci obsahující popis struktury prostředí a mapu toku logů z jednotlivých zdrojů do centrálního úložiště, specifikaci nastavení alertů reportů a transformace logů do požadované formy.

1.3. Zaškolení zaměstnanců Objednatele v provozování Systému SEM v celkovém rozsahu 48 hod., které se týká:

- a) instalace, konfigurace a správy systému včetně log databáze,
- b) ovládaní GUI, definice alertů, reportingu, analýzy logů,
- c) tvorby vlastních parserů pomocí vizuálního programovacího jazyka a konzultace.

1.4. Technickou podporu pro Systém SEM (dále jen „**Produkt**“) 12 měsíců ode dne instalace SW spočívající v:

- a) možnosti bezplatného přístupu a oprávnění k používání aktuální verze Produktu a opravné verze Produktu, včetně jejich aktualizace, budou-li nějaké dostupné;
- b) asistenci v případě otázek týkajících se rutinního provozu, krátkodobé instalace a použití (otázky typu "jak na to") a dále otázek týkajících se kódu (chybové či nestandardní stavy, chování v rozporu s Dokumentací Produktu);
- c) řešení závad Produktu;
- d) právu užívat podporované verze Produktů na libovolném Podporovaném operačním systému.
- e) bezplatném elektronickém on-line přístupu k posledním Aktuálním verzím Produktu s možností čerpání Podpory.

- 2) Zhotovitel bude při plnění této Smlouvy postupovat dle Přílohy č. 1 této Smlouvy „Požadavky na systém pro centralizovanou správu logů, událostí a strojových dat“.
- 3) Předmětem plnění této Smlouvy je zároveň závazek Objednatele za řádně a včas dodaný Předmět plnění uhradit Zhotoviteli za řádně a včas poskytnuté plnění Cenu dle čl. IV. této Smlouvy.
- 4) Zhotovitel závazně prohlašuje, že Předmět plnění odpovídá požadavku uvedenému v zadávací dokumentaci k veřejné zakázce č.j. MF-33769/2017/9003-1.

III. Způsob plnění – místo plnění, termín plnění, předávací řízení

- 1) Předmět plnění je Zhotovitel povinen předat (umožnit jeho užití) Objednateli v místě plnění, kterým je sídlo Objednatele: Letenská 525/15, 118 10 Praha 1, není-li Smluvními stranami dohodnuto jinak (dále jen „Místo plnění“).
- 2) Zhotovitel se zavazuje, že bude Předmět plnění vykonávat prostřednictvím jedné nebo více fyzických osob, jejichž kvalifikace bude prokázána ve výběrovém řízení. Předmět plnění bude vykonán řádně a s odbornou péčí.
- 3) Předmětu plnění bude Objednateli předložen formou níže uvedených Dílčích výstupů k akceptaci.

Dílčí výstup:

- 1. Předmět plnění v čl. II. odst. 1.1. Smlouvy
- 2. Předmět plnění v čl. II. odst. 1.2. Smlouvy
- 3. Předmět plnění v čl. II. odst. 1.3. Smlouvy
- 4. Předmět plnění v čl. II. odst. 1.4. Smlouvy

Zahájení plnění:

- den podpisu Smlouvy
- den podpisu Smlouvy
- den podpisu Smlouvy
- ode dne instalace SW

Termín dokončení: (hodnotící kritérium)

- 07.04.2018
- 27.06.2018
- 29.06.2018
- 29.06.2019

- 4) Smluvní strany sjednávají, že každý jednotlivý Dílčí výstup Předmětu plnění uvedený v čl. II. odst. 1.1. -1.3. bude podroben akceptačnímu řízení (vyjma Předmětu plnění uvedeného v čl. II. odst. 1.4.). Výstupem akceptačního řízení je Akceptační protokol podepsaný oběma Smluvními stranami, jehož vzor tvoří Přílohu č. 2 této Smlouvy.
- 5) Zhotovitel je povinen upozornit Objednatele 2 pracovní dny předem o termínu předání Předmětu plnění k akceptaci. Objednatel provede akceptaci každého Dílčího výstupu nejpozději do 10 pracovních dní od jeho předání k akceptaci. Pro odstranění nejasností se uvádí, že termín předání uvedený v odst. 3) tohoto článku je termínem pro předání Dílčího výstupu již po proběhlé akceptaci.
- 6) V případě, že nedojde k podpisu Akceptačního protokolu ze strany Objednatele, není Dílčí výstup Předmětu plnění ze strany Zhotovitele považován za řádně předaný a ze strany Objednatele za řádně převzatý a schválený.
- 7) Okamžikem podpisu Akceptačního protokolu a jeho schválením bez výhrad se považuje Předmět plnění ze strany Zhotovitele za řádně předaný a ze strany Objednatele za převzatý a schválený.
- 8) Nebude-li mezi Smluvními stranami dohodnuto v rámci akceptačního řízení jinak, je Zhotovitel povinen odstranit vady Předmětu plnění, zjištěné v rámci akceptačního řízení, do 5 pracovních dnů od okamžiku podpisu Akceptačního protokolu se soupisem zjištěných vad ze strany Objednatele.
- 9) Akceptační protokol zpracuje Zhotovitel ve dvou vyhotoveních, z nichž každá Smluvní strana obdrží po jednom vyhotovení.
- 10) Předmět plnění musí vyhovovat bezpečnostním standardům, jejichž použití je obvyklé u obdobných produktů, a musí svou technickou úroveň odpovídat zadávacím podmínkám Objednatele v oblasti bezpečnosti a provozu informačních a komunikačních technologií a závazným i doporučujícím technickým a bezpečnostním normám platným v České republice.

IV. Platební podmínky – cena, platební podmínky a fakturace

- 1) Za řádné a včasné poskytnutí Předmětu plnění se Objednatel zavazuje zaplatit Zhotoviteli celkovou maximální Smluvní cenu uvedenou bez DPH, která byla sjednána dohodou smluvních stran podle zákona č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů, která je nepřekročitelná, a která zahrnuje veškeré náklady Zhotovitele spojené s Předmětem plnění Smlouvy (tj. např. náklady na dopravu, na zprovoznění atd.) (dále jen „Smluvní cena“). Smluvní cena byla dohodou Smluvních stran stanovena ve výši:
 - bez DPH **1 931 000 Kč**, (slovy: jedenmilionděvsetřicetjednatisíc korun českých)
 - DPH 21% 405 510 Kč, (slovy: čtyřistapěttisícpětsetdeset korun českých)
 - včetně DPH **2 336 510 Kč**, (slovy: dvěmilionytristatřicetšesttisícpětsetdeset korun českých).
- 2) Smluvní cena za Předmět plnění uvedená v odst. 1. tohoto článku se člení na dílčí Smluvní ceny:
 - a) dílčí Smluvní cenu za Předmět plnění uvedený čl. II. odst. 1.1. (**Dodávka HW a SW**) :
 - bez DPH 1 084 000 Kč , (slovy: jedenmilionosmdesátčtyřtisíc korun českých)
 - DPH 21% 227 640 Kč, (slovy: dvěstědvacetsedmtisícšestsetčtyřicet korun českých)
 - včetně DPH 1 311 640 Kč,(slovy: jedenmiliontřístajedenácttisícšestsetčtyřicet korun českých)

b) dílčí Smluvní cenu za Předmět plnění uvedený čl. II. odst. 1.2. (**Implementace**) :
bez DPH 637 000 Kč, (slovy: šestsetčtyřicetstisíc korun českých)
DPH 21% 133 770 Kč, (slovy: stočtyřicetstisíc sedmsetšedesát korun českých),
včetně DPH 770 770 Kč, (slovy: sedmsetšedesátstisíc sedmsetšedesát)

c) dílčí Smluvní cenu za Předmět plnění uvedený čl. II. odst. 1.3. (**Zaškolení**) :
bez DPH 54 000 Kč, (slovy: padesátčtyřtisíc korun českých)
DPH 21% 11 340 Kč, (slovy: jedenácttisíc tři sta čtyřicet korun českých)
včetně DPH 65 340 Kč, (slovy: šedesát pět tisíc tři sta čtyřicet korun českých)

d) dílčí Smluvní cenu za Předmět plnění uvedený čl. II. odst. 1.4. (**Podpora**) :
bez DPH 156 000 Kč, (slovy: stopadesátšesttisíc korun českých)
DPH 21% 32 760 Kč, (slovy: třicetdvatisíc sedmsetšedesát korun českých)
včetně DPH 188 760 Kč, (slovy: stoosmdesátstisíc sedmsetšedesát korun českých)

3) Smluvní cena za Předmět plnění uvedená v odstavci 1) tohoto článku bude uhrazena jednorázově na základě jedné vystavené faktury s příloženým Akceptačním protokolem podepsaným oběma Smluvními stranami.

4) Zhotovitel vystaví fakturu Objednateli až po předání všech Dílčích výstupů Předmětu plnění (vyjma Předmětu plnění uvedeného v čl. II. odst. 1.4.), resp. po podpisu Akceptačního protokolu Objednatel **bez výhrad**. Akceptační protokol bude tvořit přílohu faktury.

5) Zhotovitel doručí fakturu na adresu Objednatele:

Ministerstvo financí
Podatelna
Letenská 15, 118 10 Praha 1

6) Faktura bude obsahovat náležitosti obchodní listiny dle § 435 Občanského zákoníku a v případě, že jde o daňový doklad, také náležitosti dle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Faktura musí dále obsahovat:

- a) identifikaci Předmětu plnění podle Smlouvy a Dokumentů Zadávacího řízení;
- b) číslo Smlouvy, uvedené v záhlaví Smlouvy v rámečku, které slouží jako identifikátor platby;
- c) úplné bankovní spojení Zhotovitele;
- d) kopii Akceptačního protokolu.

7) Zhotovitel prohlašuje, že je plátcem DPH. Ke každé dílčí Smluvní ceně bude připočtena DPH dle sazby daně platné ke dni uskutečnění zdanitelného plnění.

8) Smluvní strany se dohodly, že je-li Zhotovitel plátcem DPH a je v okamžiku uskutečnění zdanitelného plnění veden v rejstříku nespolehlivých plátců DPH, anebo nastane některá z jiných skutečností rozhodných pro ručení Objednatele, je Objednatel oprávněn zaplatit Zhotoviteli pouze dohodnutou cenu bez DPH a DPH odvést příslušnému správci daně dle platných právních předpisů, nedohodnou-li se smluvní strany jinak. O provedené úhradě DPH správci daně bude Objednatel Zhotovitele informovat kopií oznámení pro správce daně dle §109a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů, bez zbytečného odkladu.

9) Splatnost řádně vystavené faktury činí 30 kalendářních dnů ode dne doručení Objednateli.

10) Objednatel má právo fakturu Zhotoviteli před uplynutím lhůty splatnosti vrátit, aniž by došlo

k prodlení s její úhradou, obsahuje-li nesprávné náležitosti nebo údaje, chybí-li na faktuře některá z náležitostí nebo údajů nebo chybí-li kopie Akceptačního protokolu. Ode dne doručení opravené faktury běží Objednateli nová lhůta splatnosti.

- 11) Platby budou probíhat výhradně v korunách českých a rovněž veškeré cenové údaje budou uvedeny v této měně. K platbě dojde bezhotovostně převodem na účet uvedený v záhlaví Smlouvy a podle údajů na vystavené faktuře. Odlišné bankovní údaje uvedené na faktuře mají přednost před údaji uvedenými v záhlaví této Smlouvy.

V. Práva a povinnosti smluvních stran

Povinnosti Objednatele

- 1) Objednatel se zavazuje zkontrolovat soulad Akceptačního protokolu se skutečně dodaným Předmětem plnění a v případě jakýchkoliv nesrovnalostí uvést všechny výhrady ohledně předávaného Předmětu plnění do Akceptačního protokolu. Nejsou-li na Akceptačním protokolu uvedeny žádné výhrady, má se za to, že Objednatel Předmět plnění přejímá bez výhrad.
- 2) Objednatel se zavazuje zaplatit včas Smluvní cenu za řádně provedený a předaný Předmět plnění.
- 3) Objednatel se zavazuje poskytnout potřebnou součinnost, kterou lze po něm spravedlivě požadovat při řešení všech záležitostí souvisejících s poskytováním plnění dle této Smlouvy.

Povinnosti Zhotovitele

- 4) Zhotovitel se zavazuje včas předat Objednateli Předmět plnění a převést vlastnické právo k Předmětu plnění na Objednatele ke dni podepsání Akceptačního protokolu.
- 5) Zhotovitel je povinen do 10 pracovních dní od vyžádání Objednatele předložit rozpracovaný Předmět plnění k nahlédnutí a případným připomínkám Objednatele.

VI. Práva duševního vlastnictví

- 1) Smluvní cena zahrnuje i případnou odměnu za poskytnutí licence k užití Předmětu plnění.
- 2) Zhotovitel je povinen zajistit, aby Předmět plnění byl bez právních vad, zejména, aby nebyl zatížen žádnými právy či nároky třetích osob, z nichž by pro Objednatele vyplynul jakýkoliv finanční nebo jiný závazek ve prospěch třetí strany nebo která by jakkoliv omezovala užívání Předmětu plnění.
- 3) V případě porušení tohoto závazku je Zhotovitel v plném rozsahu odpovědný za případné následky takového porušení, přičemž právo Objednatele na případnou náhradu škody a smluvní pokutu zůstává nedotčeno.
- 4) Zhotovitel se zavazuje, že při poskytování Předmětu plnění bude postupovat tak, aby nedošlo k neoprávněnému zásahu do práv třetích osob.
- 5) Zhotovitel zajistí pro Objednatele Licenci k užívání Předmětu plnění všemi způsoby užití, a to ode dne jeho předání a převzetí ze strany Objednatele Akceptačním protokolem na dobu neurčitou. Objednatel není povinen Licenci využít. Licence je udělena jako licence nevýhradní ve smyslu § 2360 Občanského zákoníku.

VII. Odpovědnost za vady – záruční podmínky

- 1) Zhotovitel prohlašuje, že Předmět plnění nebude mít při předání žádné vady.

- 2) Smluvní strany si ujednaly záruku za vady pro Předmět plnění uvedený v čl. II. odst. 1.1. Smlouvy v délce **5 let**. Záruční doba počíná běžet od data podpisu Akceptačního protokolu bez výhrad.
- 3) Smluvní strany si ujednaly záruku za vady pro Předmět plnění uvedený v čl. II. odst. 1.2. Smlouvy v délce **12 měsíců**. Záruční doba počíná běžet od data podpisu Akceptačního protokolu bez výhrad.
- 4) Zhotovitel se zavazuje v záruční době podle předcházejících ustanovení bezplatně odstranit vady Předmětu plnění, které se vyskytly po jeho předání (vyjma HW viz odst. 5 tohoto článku), a to do **15 kalendářních dnů** od prokazatelného nahlášení vady. Zhotovitel je povinen vady odstranit opravou, úpravou nebo přepracováním Předmětu plnění nebo jiným způsobem podle volby Objednatele.
- 5) Zhotovitel se zavazuje v záruční době zajistit bezplatnou servisní podporu na dodaný HW s opravou v místě instalace do **2 pracovních dnů** od nahlášení poruchy oprávněnou osobou na kontaktní místo Zhotovitele (helpdesk Caleum a.s., helpdesk@caleum.cz, +420 225 992 271) v pracovních dnech od 7:00 do 19:00 hod.
- 5) Pokud Zhotovitel neodstraní vady ve lhůtě uvedené v odst. 4 a 5 tohoto článku, je Objednatel oprávněn odstranit vady nebo zajistit odstranění vad prostřednictvím třetích osob a požadovat po Zhotoviteli úhradu nákladů účelně vynaložených v souvislosti s odstraňováním těchto vad. Uplatněním práva podle tohoto článku není dotčeno právo Objednatele na odstoupení od Smlouvy.
- 6) V případě prodloužení Zhotovitele s plněním práv Objednatele z vad Předmětu plnění je Zhotovitel povinen uhradit Objednateli smluvní pokutu uvedenou v odst. 1 článku X. Sankce.
- 7) Zhotovitel v rámci záruky odpovídá za to, že Předmět plnění bude v souladu s touto Smlouvou a podmínkami stanovenými právními předpisy. Zhotovitel zejména odpovídá za shodu Předmětu plnění s požadavky Objednatele uvedenými v Příloze č. 1 této Smlouvy a s požadavky Objednatele uplatněnými formou připomínek v průběhu rozpracovanosti Předmětu plnění.
- 8) Pro uplatnění vad Předmětu plnění neplatí § 2618 Občanského zákoníku. Objednatel je oprávněn uplatnit vady Předmětu plnění u Zhotovitele kdykoliv během záruční doby bez ohledu na to, kdy Objednatel takové vady zjistil nebo mohl zjistit. Pro vyloučení pochybností se sjednává, že převzetím Předmětu plnění není dotčeno právo Objednatele uplatňovat práva z vad Předmětu plnění, které byly zjistitelné, ale zjištěny nebyly, v průběhu předání Předmětu plnění.
- 9) Pokud Objednatel nemůže Předmět plnění užívat, prodlužuje se záruční doba o dobu od oznámení vad Zhotoviteli do jejich úplného odstranění Zhotovitelem.

VIII. Odpovědnost za škodu

- 1) Smluvní strany odpovídají za každé zaviněné porušení smluvní povinnosti v plné výši.
- 2) Škodu hradí škůdce v penězích a v plné výši, nežádá-li poškozený uvedení do předešlého stavu.
- 3) Náhrada škody je splatná ve lhůtě sedmi dnů od doručení písemné výzvy oprávněné Smluvní strany Smluvní straně povinné z náhrady škody.

IX. Mlčenlivost

- 1) Smluvní strany souhlasí s tím, že podepsaná Smlouva, jakož i její text, může být v elektronické podobě zveřejněn v registru smluv, na internetových stránkách Ministerstva financí ČR, na profilu

Zhotovitele ve smyslu ZZVZ a dále v souladu s povinnostmi vyplývajícími z právních předpisů, a to bez časového omezení. Objednatel se zavazuje, že Smlouvu v souladu se zákonem č. 340/2015 Sb., zákona o registru smluv, uveřejní v registru smluv.

- 2) Smluvní strany se zavazují udržovat v tajnosti, podniknout všechny nezbytné kroky k zabezpečení a nezpřístupnit třetím osobám diskrétní informace (dále jen „Diskrétní informace“). Povinnost poskytovat informace podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů, není tímto ustanovením dotčena. Za Diskrétní informace se považují veškeré následující informace:
 - a) veškeré informace poskytnuté Zhotovitelem Objednateli v souvislosti s plněním této Smlouvy (pokud nejsou výslovně obsaženy ve znění Smlouvy zveřejňovaném dle odst. 1 tohoto článku);
 - b) informace, na která se vztahuje zákonem uložená povinnost mlčenlivosti;
 - c) veškeré další informace, které budou Zhotovitelem označeny jako diskrétní ve smyslu ustanovení § 218 ZZVZ.
- 3) Povinnost zachovávat mlčenlivost uvedená v tomto článku se nevztahuje na informace:
 - a) které je Objednatel povinen poskytnout třetím osobám podle zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů
 - b) jejichž sdělení vyžaduje jiný právní předpis
 - c) které jsou nebo se stanou všeobecně a veřejně přístupnými jinak, než porušením právních povinností ze strany některé ze Smluvních stran;
 - d) u nichž je Zhotovitel schopen prokázat, že mu byly známy ještě před přijetím těchto informací od Objednatele, avšak pouze za podmínky, že se na tyto informace nevztahuje povinnost mlčenlivosti z jiných důvodů;
 - e) které budou Zhotovitelem po uzavření této Smlouvy sděleny bez závazku mlčenlivosti třetí stranou, jež rovněž není ve vztahu k nim nijak vázána.
- 4) Jako s Diskrétními informacemi musí být nakládáno také s informacemi, které splňují podmínky uvedené v odst. 2 tohoto článku, i když byly získané náhodně nebo bez vědomí Objednatele, a dále s veškerými informacemi získanými od jakékoliv třetí strany, pokud se týkají Objednatele či plnění této Smlouvy.
- 5) Zhotovitel se zavazuje, že Diskrétní informace užije pouze za účelem plnění této Smlouvy. K jinému použití je třeba předchozí písemné svolení Objednatele.
- 6) Zhotovitel je povinen svého případného poddodavatele zavázat povinností mlčenlivosti a respektováním práv Objednatele nejméně ve stejném rozsahu, v jakém je v tomto smluvním vztahu zavázán sám.
- 7) Povinnost zachování mlčenlivosti trvá i po dobu 5 let od skončení záruční doby bez ohledu na zánik ostatních závazků ze Smlouvy.
- 8) Závazky vyplývající z tohoto článku včetně závazů vyplývajících z odst. 1) není Zhotovitel oprávněn vypovědět ani jiným způsobem jednostranně ukončit.

X. Sankce

- 1) V případě prodlení Zhotovitele s plněním jakékoliv povinnosti vyplývající z této Smlouvy a plněním jakéhokoliv termínu této Smlouvy, má Objednatel právo uplatnit vůči Zhotoviteli

smluvní pokutu ve výši 2 % (slovy: dvě procenta) ze Smluvní ceny za každý i započatý den prodlení.

- 2) Při prodlení Objednatele se zaplacením řádně vystavené faktury je Zhotovitel oprávněn požadovat zaplacení úroku z prodlení ve výši stanovené právními předpisy.
- 3) V případě, že některá ze Smluvních stran poruší některou z povinností mlčenlivosti dle čl. IX., je druhá Smluvní strana oprávněna požadovat smluvní pokutu ve výši 100 000,- Kč (slovy: jedno sto tisíc korun Českých), a to za každý jednotlivý případ porušení.
- 4) Smluvní pokuta je splatná ve lhůtě sedmi dnů od doručení písemné výzvy oprávněné Smluvní strany Smluvní straně povinné ze smluvní pokuty.
- 5) Ujednáním o smluvní pokutě není dotčeno právo poškozené smluvní strany domáhat se náhrady škody v plné výši.

XI. Rozhodné právo

- 1) Tato Smlouva se řídí právním řádem České republiky. V záležitostech touto Smlouvou neupravených se právní vztah mezi Smluvními stranami řídí Občanským zákoníkem.
- 2) Veškeré spory mezi Smluvními stranami vyplývající z této Smlouvy nebo z jejího porušení, ukončení nebo neplatnosti budou rozhodovány obecnými soudy České republiky.

XII. Oprávněné osoby

- 1) Každá ze Smluvních stran jmenuje svoji oprávněnou osobu (dále jen „Oprávněné osoby“). Oprávněné osoby jsou oprávněny jménem stran provádět veškeré úkony v rámci akceptačních procedur dle Smlouvy a připravovat dodatky ke Smlouvě pro jejich písemné schválení osobám oprávněným zavazovat strany (statutárním orgánům), nebo jejich zplnomocněným zástupcům.
- 2) Smluvní strany jsou oprávněny změnit Oprávněné osoby i bez nutnosti uzavření dodatku ke Smlouvě, jsou však povinny na takovou změnu druhou smluvní stranu písemně upozornit.
- 3) Oprávněné osoby nejsou zmocněny k jednání, jež by mělo za přímý následek změnu Smlouvy nebo jejího předmětu.
- 4) Smluvní strany se dohodly na dále uvedených Oprávněných osobách, kteří budou za Smluvní strany jednat ve věcech obchodních, technických, ekonomických:

Za Objednatele:

Ve věcech smluvních a technických:

Jméno: Pavel Kříž
Adresa: Letenská 15, Praha 1
E-mail:

Jméno: Ing. Petr Šedivý
Adresa: Letenská 15, Praha 1
E-mail:

Jméno: Jiří Skořepa
Adresa: Letenská 15, Praha 1
E-mail:

Ve věcech ekonomických:
Jméno: Ing. Alena Mecová
Adresa: Letenská 15, Praha 1
E-mail:

Za Zhotovitele: Caleum a.s.

Ve věcech smluvních a ekonomických:
Jméno:
Adresa: Italská 438/36, 130 00 Praha 3
E-mail:
Datová schránka: ecfi232

Ve věcech technických (certifikovaný projekt manager):
Jméno:
Adresa: Italská 438/36, 130 00 Praha 3
E-mail:
Datová schránka: ecfi232

XIII. Ukončení Smlouvy

- 1) Smlouva může být ukončena dohodou Smluvních stran.
- 2) Objednatel je oprávněn vypovědět Smlouvu bez výpovědní doby v následujících případech:
 - a. bude rozhodnuto o likvidaci Zhotovitele;
 - b. Zhotovitel podá insolvenční návrh ohledně své osoby, bude rozhodnuto o úpadku Zhotovitele nebo bude ve vztahu k Zhotoviteli vydáno jiné rozhodnutí s obdobnými účinky;
 - c. Zhotovitel bude pravomocně odsouzen za úmyslný majetkový nebo hospodářský trestný čin.
- 3) Smluvní strany jsou vždy oprávněny od této Smlouvy odstoupit, nastanou-li okolnosti předvídané ustanovením § 2002 Občanského zákoníku.
- 4) Za podstatné porušení smlouvy Zhotovitelem ve smyslu § 2002 Občanského zákoníku se považuje zejména:
 - a. prodlení Zhotovitele s dodáním Předmětu plnění o více než 30 kalendářních dní po termínu plnění;
 - b. porušení povinnosti Zhotovitele odstranit vady Předmětu plnění ve lhůtě 15 kalendářních dní od jejich oznámení Objednatelem;
 - c. vícečetné porušování smluvních či jiných právních povinností v souvislosti s plněním smlouvy;
 - d. jakékoliv porušení povinností Zhotovitelem, které nebude odstraněno či napraveno ani do 30 kalendářních dní od porušení povinnosti, je-li náprava možná.
- 5) Za podstatné porušení Smlouvy Objednatelem ve smyslu § 2002 Občanského zákoníku se považuje zejména prodlení Objednatele s úhradou faktury o více než 30 kalendářních dní.
- 6) Odstoupením od této Smlouvy se závazek touto Smlouvou založený zrušuje od počátku a Smluvní

strany si jsou povinny vrátit vše, co si plnily, a to bez zbytečného odkladu, nejpozději však do 30 dnů od doručení oznámení Smluvní strany o odstoupení od této Smlouvy. Ustanovení odstavce 4 tohoto článku není dotčeno.

- 7) Odstoupení od Smlouvy se nedotýká práva na zaplacení smluvní pokuty nebo úroku z prodlení, pokud už dospěl, práva na náhradu škody vzniklé z porušení smluvní povinnosti ani ujednání, které má vzhledem ke své povaze zavazovat Smluvní strany i po odstoupení od této Smlouvy.
- 8) Zhotovitel je oprávněn od této Smlouvy odstoupit v případě, že Objednatel neuhradí Cenu ani v dodatečně poskytnuté přiměřené lhůtě.

XIV. Závěrečná ustanovení

- 1) Oznámení nebo jiná sdělení podle této Smlouvy musí být učiněna písemně v českém jazyce. Jakékoliv úkony směřující ke skončení této Smlouvy musí být oznámeny druhé Smluvní straně datovou schránkou nebo formou doporučeného dopisu. Oznámení nebo jiná sdělení podle této Smlouvy se budou považovat za řádně učiněná, pokud budou doručena osobně, poštou, emailem či kurýrem na adresy uvedené v tomto odstavci nebo na jinou adresu, kterou příslušná Smluvní strana v předstihu písemně oznámí druhé Smluvní straně.
- 2) Účinnost oznámení nastává v pracovní den následující po dni doručení tohoto oznámení druhé Smluvní straně.
- 3) Ke změně Smlouvy nebo ukončení Smlouvy je oprávněn vedoucí samostatného oddělení 9003 za Objednatele, a dále ministr a osoby pověřené ministrem financí. Ke změně Smlouvy nebo ukončení Smlouvy je oprávněn za Zhotovitele sám Zhotovitel (pokud je fyzickou osobou – podnikatelem) nebo statutární orgán Zhotovitele, a to dle způsobu jednání uvedeném v obchodním rejstříku (dále jen „Odpovědné osoby pro věci smluvní“). Odpovědné osoby pro věci smluvní mají současně všechna oprávnění Kontaktních osob.
- 4) Tato Smlouva se řídí právními předpisy České republiky. Smluvní strany pro vyloučení pochybností sjednávají, že tato Smlouva se řídí subsidiárně ustanoveními Občanského zákoníku o smlouvě o Předmět plnění.
- 5) Stane-li se kterékoli ustanovení této Smlouvy neplatným, neúčinným nebo nevykonatelným, zůstává platnost, účinnost a vykonatelnost ostatních ustanovení této Smlouvy neovlivněna a nedotčena, nevyplývá-li z povahy daného ustanovení, obsahu Smlouvy nebo okolností, za nichž bylo toto ustanovení vytvořeno, že toto ustanovení nelze oddělit od ostatního obsahu Smlouvy.
- 6) Jestliže kterákoli ze Smluvních stran neuplatní nárok nebo nevykoná právo podle této Smlouvy, nebo je vykoná se zpožděním či pouze částečně, nebude to znamenat vzdání se těchto nároků nebo práv. Vzdání se práva z titulu porušení této Smlouvy nebo práva na nápravu anebo jakéhokoliv jiného práva podle této Smlouvy musí být vyhotoveno písemně a podepsáno Smluvní stranou, která takové vzdání se činí.
- 7) Žádná ze Smluvních stran není oprávněna bez souhlasu druhé Smluvní strany postoupit Smlouvu, jednotlivý závazek ze Smlouvy ani pohledávky vzniklé v souvislosti s touto Smlouvou na třetí osoby ani učinit jakékoliv právní jednání, v jehož důsledku by došlo k převodu či přechodu práv či povinností vyplývajících z této Smlouvy.
- 8) Tato Smlouva je vyhotovena ve dvou (2) vyhotoveních v českém jazyce, přičemž každá ze Smluvních stran obdrží po jednom (1) vyhotovení.

- 9) Změny nebo doplňky této Smlouvy včetně jejích příloh musejí být vyhotoveny písemně a podepsány oběma Smluvními stranami s podpisy Smluvních stran na jedné listině.
- 10) Tato Smlouva nabývá platnosti okamžikem podpisu oběma Smluvními stranami.
- 11) Tato Smlouva nabývá účinnosti okamžikem jejího zveřejnění v registru smluv.
- 12) Součástí této Smlouvy jsou i následující přílohy:
 Příloha č. 1 - Požadavky na systém pro centralizovanou správu logů, událostí a strojových dat
 Příloha č. 2 - Akceptační protokol – vzor

V Praze dne _____	V _____ dne _____
_____	_____
Objednatel Česká republika- Ministerstvo financí Viktor Janáček Pověřen řízením odboru 70	Zhotovitel Caleum a.s. Josef Ladra Předseda představenstva

Příloha č. 1 Smlouvy - Požadavky na systém pro centralizovanou správu logů, událostí a strojových dat

a) Seznam aplikačních agend, ke kterým je nutné realizovat a implementovat parsery logů.

č.	Název aplikační agendy
1	ARES – administrativní registr ekonomických subjektů
2	AUDIT
3	Centrální evidence dotací z rozpočtu na Ministerstvu financí
4	FKVS 1 – VSK veřejnoprávní kontrola
5	FKVS 2 – MRZ
6	MPP – IS pro přezkoumávání hospodaření územně správních celků
7	ISPSP – IS o platu a služebním příjmu
8	KSP – kontrola státní podpory stavebního spoření
9	SDPF – státní dozor nad penzijními fondy
10	WSS TREMA – ŘÍZENÍ STÁTNÍHO DLUHU
11	VIOLA – IS pro administraci prostředků z rozpočtu EU a finančních mechanismů EHP / Norsko, EHP / Norsko 2 a Švýcarsko
12	IS AO – Informační systém Auditního orgánu
13	Evidenční dotační systém / Správa majetku ve vlastnictví státu
14	Státní dozor nad loteriemi a sázkami
15	REGOZ – Registr oznámení
16	Integrovaný informační systém státní pokladny + MONITOR pro zveřejňování dat IISSP
17	VIOLA Fund Management

b) Technické požadavky na systém pro centralizovanou správu logů, událostí a strojových dat

Popis
Technické požadavky na systém pro centralizovanou správu logů, událostí a strojových dat
System provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware
System umožňuje dopsání parseru pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na psaní zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů bez vlivu na jeho ostatní funkce.
System přijímá a zpracovává logy, události a další strojově generovaná data na prostřednictvím minimálně následujících protokolů: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). System musí umožňovat přijímat logy i na uživatelsky definovaných UDP a TCP portech. Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv.
System zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se systém defaultně řídí.

Všechny normalizované položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.
Možnost sběru událostí minimálně ve formátech RAW, Syslog, CEF, LEEF, JSON RFC7159.
Systém nesmí umožnit mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.
Systém provádí konsolidaci logů na centrálním místě.
Systém umožňuje snadné vyhledávání událostí (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce.
Systém provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí).
Systém umožňuje snadno vytvářet grafické znázornění TOP událostí nad všemi daty za určité časové období.
Systém provádí automatické doplňování GeolIP informací k událostem a jejich grafické znázornění na mapě.
Systém provádí automatické doplňování reverzních DNS záznamů k IP adresám.
V případě přetížení systému nesmí dojít ke ztrátě logů. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. Při výraznějším plnění vyrovnávací paměti musí být administrátor systému automaticky informován. Velikost vyrovnávací paměti nesmí být nižší než 50 GB.
Systém musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízení.
Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ISO 27001:2014 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit ani čestným prohlášením.
Systém musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování.
Systém obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů.
Systém obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.
Systém podporuje i automatizuje průběžné aktualizace reportů a pohledů výrobcem.
Konfigurační a Systémové rozhraní a On-line dokumentace musí být identické anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce.
Systém nabízí kapacitní i výkonovou škálovatelnost.
Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 40TB.
Požadujeme, aby ze systému bylo možné vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.
Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.
Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňoval autorizovaný přístup ke strukturované databázi logů.

Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 316 / 2014 ze dne 15. prosince 2014 „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)“ k Zákonu 181 / 2014 „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) bezpečnosti“ ze dne 23. července 2014.
Jednotná centrální webová konzole pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Není přípustné, aby dodaný systém měl více konzolí pro jednotlivé části systému.
Požadujeme, aby systém umožňoval snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému.
Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření z lokální databáze.
Minimální HW parametry požadovaného systému
Dvě HW appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely. Dvě HW appliance jsou z důvodů vysoké dostupnosti.
HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislá na dalších systémech.
2 procesory (min. 10 jader každý), podpora HyperThreadingu.
Min. 64GB DDR-4.
Minimálně 40TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache min. 2GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.
Z výkonových důvodů požadujeme, aby v systému bylo minimálně 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček.
Minimálně 2x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW.
Větráky v systému musí být vyměnitelné za provozu a redundantní.
2x napájecí zdroje s redundancí napájení 1+1.
Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.
Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdoba HP iLO, Dell iDRAC apod).
Výkonnostní a SW parametry systému
Systém funguje formou appliance (všechny části systémů je možné nastavit v centrální správčovské konzoli - viz bod 29, není nutné editovat žádné konfigurační soubory včetně IP adresace systému).
Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální správčovskou konzoli (viz bod 29).
Průměrný trvalý příjem min. 6 tis událostí / s. s možností navýšení na minimálně 12 tis. událostí /s. prostřednictvím licence nebo rozšíření hardware.
Špičkový příjem 12 tis událostí / s po dobu nejméně 10 minut, v případě vyššího počtu událostí je systém uloží do bufferu a zpracuje je později. Po volitelném licenčním nebo hardware zvýšení výkonu pak 24 tis událostí po dobu nejméně 10 minut.

Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den, nebo licence na minimálně 200GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 40 TB a nad to musí podporovat kompresi ukládaných dat.
Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli (viz bod 29). Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.
Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeolIP informace a identifikace výrobce zařízení podle MAC adresy.
Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat.
V centrální správcovské konzoli (viz bod 29) je možné přidávat k jednotlivým zdrojům dat, aplikaci, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod.
V centrální správcovské konzoli (viz bod 29) je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.).
Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.
Podpora zrcadlení a clusteru – 2 a více zařízení v režimu active / active.
Vícenodový systém se chová jako 1 celek.
V případě využití více zařízení v systému se zrychluje vyhledávání, a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru.
Rozšiřování kapacity i navýšování výkonu pomocí přidávání dalších zařízení do clusteru.
V případě rozšíření na cluster (přidání dalšího node) musejí zařízení odesílající události odesílat pouze na jednu virtuální adresu a zároveň cluster musí zajišťovat synchronizaci událostí mezi jednotlivými nody.
Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém.
Alerty
Systém je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert.
Text alertu může být uživatelsky definovaný s proměnnými z přijaté rozparsované události.
Předpřipravené sety/vzory alertů výrobcem.
Konfigurace alertů pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.
V alertech je možné využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru, který běží v lokalitě Praha).
Sběr událostí z Microsoft prostředí
Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring souborových logů.
Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací.
Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správcovské konzole z bodu 29.

Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správcovské konzole z bodu 29. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.
Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzole systému (viz bod 29). Správa a aktualizace Windows agenta se neprovádí z Group Policy.
Agent automaticky překládá zástupné kódy ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.).
Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů.
Komunikace Windows agenta a centrálního systému musí být šifrovaná.
Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole (viz bod 29) nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb.
Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.
Počet instalací Windows agenta nesmí být licenčně omezen. (případně požadujeme licenci na 2000 systémů.)
Podpora pro sběr událostí z poboček
Systém musí obsahovat řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat.
Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášená data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.
Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.
Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.
Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí /s. a to i v trvalé zátěži.
Řešení musí poskytnout podporu pro UDP i TCP zdroje a pro aktivní sběr z Windows agentů.
Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.
Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).
SW Podpora
SW - Podpora výrobce na aktualizaci systému a parserů na 1 rok . Podpora musí obsahovat aktualizaci SW minimálně 2x ročně, opravy chyb a telefonická a emailová podpora s diagnostikou vzdáleným přístupem.

Příloha č. 2 – Akceptační protokol – vzor

AKCEPTAČNÍ PROTOKOL č.1

Akceptace výstupů, které realizoval Zhotovitel podle Smlouvy 17-909-0066

Výstup	
Specifikace dílčí části Předmětu plnění	Bod 1.1.,1.2. a 1.3. předmětu smlouvy
Období realizace	
Skutečný termín zahájení realizace plnění	
Skutečný termín ukončení realizace plnění	
Předmět plnění dle Předmětu Smlouvy 17-909-0066	
Akceptační kritérium	Akceptační Výrok
<p>1) Hardware (dále jen „HW“) a software (dále jen “SW“) pro dva kusy Systém SEM s vysokou dostupností do IS MF v rozsahu a funkcích:</p> <ol style="list-style-type: none"> a. sběr logů z infrastrukturních prvků, databázových strojů a aplikačního programového vybavení IS MF (tj. networking, firewally, DB, OS serverů a stanic), b. aplikační podpora pro tvorbu jednotného formátu ukládaných logů (parser), c. jednotné centrální dlouhodobé úložiště logů, d. u každého Systému pro centralizovanou správu logů, bude kapacita úložiště pro logy o velikosti min. 40 TB (ochrana proti ztrátě dat RAID 5, nebo 6). e. generování výstrah (alerting a reporting), f. plnění požadavků Zákona o kybernetické bezpečnosti č. 181/2014 Sb. ve znění pozdějších předpisů, ve smyslu prováděcí §21 vyhlášky č. 316/2014 Sb. §21, g. ověřování přijetí, integrity a zdroje záznamu, h. uživatelské GUI pro sledování aktuálních stavů, generování reportů a sestav pro kontrolní a analytickou činnost, i. Podpora vysoké dostupnosti formou geografická redundance mezi nástroji pro centralizovanou správu logů a jejich úložištěm (forma – master-slave), j. aplikační vybavení pro sběr logů, událostí a strojových dat ze dvou vzdálených lokalit MF (z lokality Vápenka a Voctářova do lokality Letenská), k. Záruka na dodaný systém je 5let, SW renewal HA min. 1 rok [doplní účastník řízení] l. Instalační, provozní a uživatelská dokumentace, m. instalační média k dodanému SW a OS. 	
<p>2) Poskytnutí služeb k implementaci a zprovoznění Systému pro centralizovanou správu logů, událostí a strojových dat (systém SEM) do prostředí IS MF:</p> <ol style="list-style-type: none"> a. instalace dodaného HW a SW vybavení do prostředí IS MF, b. konfigurace HA řešení, c. výroba, implementace a zprovoznění log parserů pro: <ul style="list-style-type: none"> • 17 aplikačních agend (systémů), • systém SAP, • Symantec messaging gateway d. instalace a zprovoznění sběru logů nástroji podporovaných formátů do oblastí infrastruktury IS MF: <ul style="list-style-type: none"> • networking, firewally a systémů pro řízení protokolů 802., • servery a stanice s OS Windows, Linux, Solaris (Unix) s, • VMware, • Antiviry, • Adresářové služby MS Active directory, • Databáze Oracle, Informix, MS SQL, My SQL, e. dokumentace obsahující popis struktury prostředí a mapu toku logů z jednotlivých zdrojů do centrálního úložiště, specifikaci nastavení alertů reportů a transformace logů do požadované formy. 	

3) Školení zaměstnanců objednatele v provozování Systému pro centralizovanou správu logů, událostí a strojových dat (systém SEM) v rozsahu 48 hod:		
a. instalace, konfigurace a správa systému včetně log databáze, b. ovládaní GUI, definice alertů, reporting, analýza logů, c. tvorba vlastních parserů pomocí vizuálního programovacího jazyka, konzultace		
Rozhodnutí o rozsahu akceptace		
<i>Zástupce Objednatele dle čl. XII. Smlouvy 17-909-0066 odpovědný za kontrolu kvality a schválení plnění dle Předmětu smlouvy potvrzuje převzetí a akceptaci dílčího výstupu Předmětu plnění zakroužkováním varianty akceptačního výroku A, B nebo C.</i>		
A) Akceptováno – v plném rozsahu bez výhrad. B) Akceptováno s výhradou – poskytnuté výstupy jsou akceptovány s výhradou viz <i>Zdůvodnění</i> . C) Neakceptováno – poskytnuté výstupy nejsou akceptovány viz <i>Zdůvodnění</i> .		
Název role		Akceptovaný počet MD
Zdůvodnění rozhodnutí o rozsahu akceptace:		
Cena za Předmět plnění:		
Za objednatele	Cena v Kč bez DPH	Cena v Kč s DPH
1) Dodávka 2 kusů HW a SW „Systém pro centralizovanou správu logů, událostí a strojových dat (systém SEM)“ s vysokou dostupností (HA řešení).		
2) Poskytnutí služeb k implementaci a zprovoznění Systému pro centralizovanou správu logů, událostí a strojových dat (systém SEM).		
3) Školení zaměstnanců objednatele v provozování Systému pro centralizovanou správu logů, událostí a strojových dat (systém SEM)		
4) Technická podpora pro Systém SEM		
Celkem		
Schválení akceptačního protokolu zástupci zodpovědnými za kontrolu kvality Předmětu plnění (<i>datum, jméno, podpis</i>).		
Za Objednatele		
Za Zhotovitele		
Schválení akceptačního protokolu osobami odpovědnými za jednání a realizaci plnění Předmětu Smlouvy (<i>datum, jméno, podpis</i>).		
Za Objednatele		
Za Zhotovitele		

1) Akceptace splnění požadavků na systém pro centralizovanou správu logů, událostí a strojových dat

a) **Seznam aplikačních agend, ke kterým je nutné realizovat a implementovat parsery logů.**

č.	Název aplikační agendy	Splněno	Nesplněno
1	ARES – administrativní registr ekonomických subjektů		
2	AUDIT		
3	Centrální evidence dotací z rozpočtu na Ministerstvu financí		
4	FKVS 1 – VSK veřejnoprávní kontrola		
5	FKVS 2 – MRZ		
6	MPP – IS pro přezkoumávání hospodaření územně správních celků		
7	ISPSP – IS o platu a služebním příjmu		
8	KSP – kontrola státní podpory stavebního spoření		
9	SDPF – státní dozor nad penzijními fondy		
10	WSS TREMA – ŘÍZENÍ STÁTNÍHO DLUHU		
11	VIOLA – IS pro administraci prostředků z rozpočtu EU a finančních mechanismů EHP / Norsko, EHP / Norsko 2 a Švýcarsko		
12	IS AO – Informační systém Auditního orgánu		
13	Evidenční dotační systém / Správa majetku ve vlastnictví státu		
14	Státní dozor nad loteriemi a sázkami		
15	REGOZ – Registr oznámení		
16	Integrovaný informační systém státní pokladny + MONITOR pro zveřejňování dat IISSP		
17	VIOLA Fund Management		

b) **Technické požadavky na systém pro centralizovanou správu logů, událostí a strojových dat**

Popis	Splněno	Nesplněno
Technické požadavky na systém pro centralizovanou správu logů, událostí a strojových dat		
Systém provádí zpracování událostí z předdefinovaných zdrojů logů napříč výrobci aplikací, operačních systémů a síťového hardware		
Systém umožňuje dopsání parseru pro výše neuvedená zařízení uživatelem bez nutnosti spolupráce s výrobcem nebo dodavatelem (vč. subdodavatelů) nabízeného systému - Uživatelsky definované parsery. Dokumentace musí obsahovat přehledný návod na psaní zákaznických parserů a systém musí obsahovat možnost testování a ladění zákaznických parserů bez vlivu na jeho ostatní funkce.		
Systém přijímá a zpracovává logy, události a další strojově generovaná data na prostřednictvím minimálně následujících protokolů: UDP/TCP 514 (SYSLOG), TCP 20514 (RELP, nešifrovaně) a TCP 20515 (RELP, šifrovaně). Systém musí umožňovat přijímat logy i na uživatelsky definovaných UDP a TPC portech. Přijaté logy systém standardizuje do jednotného formátu a logy jsou normalizovány (rozdělovány) do příslušných polí dle jejich typu. Zároveň systém uchovává i originální verzi zpráv.		

System zachovává původní informaci ze zdroje logu o časové značce události, ale nedůvěřuje jí a vytváří vlastní důvěryhodné časové razítko ke každému logu, kterým se systém defaultně řídí.		
Všechny normalizované položky přijaté systémem jsou automaticky indexovány. Nad všemi položkami je možné ihned provádět vyhledávání bez nutnosti dodatečného ručního indexování administrátorem.		
Možnost sběru událostí minimálně ve formátech RAW, Syslog, CEF, LEEF, JSON RFC7159.		
System nesmí umožnit mazání nebo modifikování již uložených logů. Každý log musí mít unikátní identifikátor, který umožní jeho jednoznačnou identifikaci.		
System provádí konsolidaci logů na centrálním místě.		
System umožňuje snadné vyhledávání událostí (ad hoc) bez nutnosti dodatečného programování nebo aplikování dotazů v SQL jazyce.		
System provádí ucelenou vizualizaci logů, událostí a strojových dat (grafy událostí).		
System umožňuje snadno vytvářet grafické znázornění TOP událostí nad všemi daty za určité časové období.		
System provádí automatické doplňování GeoIP informací k událostem a jejich grafické znázornění na mapě.		
System provádí automatické doplňování reverzních DNS záznamů k IP adresám.		
V případě přetížení systému nesmí dojít ke ztrátě logů. Všechny přijaté nezpracované logy/události musí být ukládány do vyrovnávací paměti. Při výraznějším plnění vyrovnávací paměti musí být administrátor systému automaticky informován. Velikost vyrovnávací paměti nesmí být nižší než 50 GB.		
System musí umožňovat unifikované vyhledávání napříč všemi typy dat a zařízení.		
Dodavatel musí předložit potvrzení vystavené autorizovanou osobou o shodě, že nabízený systém splňuje požadavky normy ISO 27001:2014 na pořizování auditních záznamů. Toto potvrzení není možné nahradit certifikátem na společnost dodavatele (subdodavatele) nebo výrobce nabízeného systému. Nelze nahradit ani čestným prohlášením.		
System musí mít možnost uložení uživatelem vytvořených pohledů na data (dashboardů) pro budoucí zpracování.		
System obsahuje reportovací nástroj s přednastavenými nejběžnějšími reporty a možností vlastních úprav a vytvoření nových pohledů.		
System obsahuje předpřipravené pohledy na uložená data dle jednotlivých kategorií zdrojových zařízení i dle logického členění.		
System podporuje i automatizuje průběžné aktualizace reportů a pohledů výrobcem.		
Konfigurační a Systémové rozhraní a On-line dokumentace musí být identické anglickém i v českém jazyce. Nepřipouští se omezená dokumentace v českém jazyce.		
System nabízí kapacitní i výkonovou škálovatelnost.		
Čistá kapacita úložného prostoru (kapacita diskového pole) dostupná pro uložená data nabízeného systému musí být minimálně 40TB.		
Požadujeme, aby ze systému bylo možné vytáhnout libovolné dva disky, bez ztráty dat a vlivu na funkčnost řešení. Redundance disků nesmí ovlivňovat požadovanou kapacitu úložiště.		
Monitoring stavu systému - alertování při překročení prahových hodnot nebo chybě systému, přeposlání upozornění pomocí SMTP nebo Syslog.		

Požadujeme, aby systém obsahoval REST-API pro integraci s externím monitorovacím systémem (Zabbix, Nagios, MRTG a další) a umožňoval autorizovaný přístup ke strukturované databázi logů.		
Dodavatel doloží prohlášení výrobce o shodě s požadavky Vyhlášky 316 / 2014 ze dne 15. prosince 2014 „o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)“ k Zákonu 181 / 2014 „o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti) bezpečnosti“ ze dne 23. července 2014.		
Jednotná centrální webová konzole pro přístup k logům, alertům, reportům a pro správu systému. Z této konzole se provádí veškerá konfigurace, správa a analýza logů. Není přípustné, aby dodaný systém měl více konzolí pro jednotlivé části systému.		
Požadujeme, aby systém umožňoval snadné vytváření uživatelských rolí definujících přístupová práva k uloženým událostem a jednotlivým ovládacím komponentům systému.		
Systém musí podporovat ověřování uživatele systému na externím LDAP serveru. V případě výpadku externího LDAP systému musí podporovat ověření z lokální databáze.		
Minimální HW parametry požadovaného systému		
Dvě HW appliance o velikosti max. 2U, včetně ramena pro kabelový management umožňujícího vysunutí zapnutého systému z racku pro servisní účely. Dvě HW appliance jsou z důvodů vysoké dostupnosti.		
HW appliance obsahuje veškeré potřebné komponenty (CPU, RAM, diskový prostor) a je nezávislá na dalších systémech.		
2 procesory (min. 10 jader každý), podpora HyperThreadingu.		
Min. 64GB DDR-4.		
Minimálně 40TB pro integrovanou databázi podporovanou HW akcelerovaným SAS RAID řadičem s read-write cache min. 2GB. Řadič diskového pole musí obsahovat zálohovací baterii nebo být vybaven flash pamětí.		
Z výkonových důvodů požadujeme, aby v systému bylo minimálně 12 ks stejných RAID edition disků určených pro použití v datacentrech, o rychlosti minimálně 7200 otáček.		
Minimálně 2x 1Gbit LAN porty + 1x dedikovaný 1Gbit port pro management HW.		
Větráky v systému musí být vyměnitelné za provozu a redundantní.		
2x napájecí zdroje s redundancí napájení 1+1.		
Virtuální KVM (tj. převzetí textové i grafické konzole serveru a zajištění přenosu povelů z klávesnice a myši vzdáleného počítače.		
Systém pro vzdálenou správu serveru včetně potřebné licence, pokud je třeba (obdobu HP iLO, Dell iDRAC apod).		
Výkonnostní a SW parametry systému		
Systém funguje formou appliance (všechny části systémů je možné nastavit v centrální správčovské konzoli - viz bod 29, není nutné editovat žádné konfigurační soubory včetně IP adresace systému).		
Aktualizace systému jsou distribuovány v jednotném balíku a jejich instalace je prováděna přes centrální správčovskou konzoli (viz bod 29).		
Průměrný trvalý příjem min. 6 tis událostí / s. s možností navýšení na minimálně 12 tis. událostí /s. prostřednictvím licence nebo rozšíření hardware.		

Špičkový příjem 12 tis událostí / s po dobu nejméně 10 minut, v případě vyššího počtu událostí je systém uloží do bufferu a zpracuje je později. Po volitelném licenčním nebo hardware zvýšení výkonu pak 24 tis událostí po dobu nejméně 10 minut.		
Licenčně neomezený počet zařízení pro příjem zasílaných událostí. Licenčně neomezený počet událostí v GB za den, nebo licence na minimálně 200GB uložených událostí za den. Integrovaná databáze musí mít čistou velikost nejméně 40 TB a nad to musí podporovat kompresi ukládaných dat.		
Uživatelská konfigurace vlastních parserů pomocí vizuálního programovacího jazyka v centrální správcovské webové konzoli (viz bod 29). Vizuální programovací jazyk musí uživateli umožnit psát vlastní parsery bez nutnosti znalosti programování (např. Node-RED, Microsoft VPL, Blockly apod). Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.		
Konfigurace uživatelských parserů musí umožňovat automatické doplňování DNS reverzních záznamů, GeoIP informace a identifikace výrobce zařízení podle MAC adresy.		
Možnost on-line ladění uživatelsky definovaných parserů - při jejich vytváření je možné vložit vlastní testovací zprávy, při změně je okamžitě zobrazena výsledná podoba rozparsovaných dat.		
V centrální správcovské konzoli (viz bod 29) je možné přidávat k jednotlivým zdrojům dat, aplikaci, zařízením nebo IP subnetům tzv. značky, označující například umístění zařízení, typ zařízení, kritičnost zařízení apod.		
V centrální správcovské konzoli (viz bod 29) je při definici vlastního parseru možno přidávat značky pro typy událostí (login, logout apod.).		
Všechny přidávané značky jsou ukládány s každou přijatou událostí, na základě značky je možné filtrovat data nebo omezovat oprávnění uživatelů systému k jednotlivým událostem.		
Podpora zrcadlení a clusteru – 2 a více zařízení v režimu active / active.		
Vícenodový systém se chová jako 1 celek.		
V případě využití více zařízení v systému se zrychluje vyhledávání, a jsou automaticky prohledávána všechna data na všech zařízeních v clusteru.		
Rozšiřování kapacity i navyšování výkonu pomocí přidávání dalších zařízení do clusteru.		
V případě rozšíření na cluster (přidání dalšího node) musejí zařízení odesílající události odesílat pouze na jednu virtuální adresu a zároveň cluster musí zajišťovat synchronizaci událostí mezi jednotlivými nody.		
Podpora zálohování nebo obnovení konfigurace v jednom kroku a jednom souboru pro celý systém.		
Alerty		
Systém je schopen na základě zadaných podmínek splněných v přijatých datech vygenerovat alert.		
Text alertu může být uživatelsky definovaný s proměnnými z přijaté rozpársované události.		
Předpřipravené sety/vzory alertů výrobcem.		
Konfigurace alertů pomocí vizuálního programovacího jazyka. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.		

V alertech je možné využít značky (příklad: pošli alert jen v případě, že se událost stala na kritickém serveru, který běží v lokalitě Praha).		
Sběr událostí z Microsoft prostředí		
Události z Microsoft prostředí jsou vyčítány pomocí agenta instalovaného přímo v koncových systémech. Windows agent musí současně podporovat jak monitoring interních windows logů, tak monitoring souborových logů.		
Agent zajišťuje sběr nemodifikovaných událostí a detailní zpracování auditních informací.		
Agent podporuje nastavení filtrace odesílaných událostí pomocí centrální správčovské konzole z bodu 29.		
Filtrace odesílaných událostí agentem se konfiguruje pomocí vizuálního programovacího jazyka z centrální správčovské konzole z bodu 29. Vizuální programovací jazyk není prezentován textově, ale graficky formou obrázků, které obsahují aplikační logiku.		
Windows agent nevyžaduje administrátorské zásahy na koncovém systému – je centrálně spravovaný a automaticky aktualizovatelný přímo z centrální konzole systému (viz bod 29). Správa a aktualizace Windows agenta se neprovádí z Group Policy.		
Agent automaticky překládá zástupné kódy ve zprávách na text (např. Logon Type 2 = Interactive, Logon Type 3 = Network, atd.).		
Windows agent má buffer pro případ ztráty spojení mezi koncovým systémem a centrálním úložištěm logů.		
Komunikace Windows agenta a centrálního systému musí být šifrovaná.		
Windows agent podporuje sběr nejen ze základních systémových logů (Aplikace, Zabezpečení, Instalace, Systém), ale je možné z centrální konzole (viz bod 29) nastavit i sběr všech ostatních logů ve složce Protokoly aplikací a služeb.		
Windows agent automaticky doplňuje ke všem odesílaným událostem jejich textový popis tak, jak je zobrazen v Prohlížeči událostí (Event Viewer) na koncovém systému.		
Počet instalací Windows agenta nesmí být licenčně omezen. (případně požadujeme licenci na 2000 systémů.)		
Podpora pro sběr událostí z poboček		
Systém musí obsahovat řešení, které sbírá události na pobočkách a umožní jejich odeslání po saturované lince bez ztráty dat.		
Řešení musí být schopno automaticky navázat spojení s centrálním úložištěm dat a přenášena data šifrovat. V případě výpadku spojení mezi pobočkou a centrálou musí spojení automaticky obnovit.		
Řešení musí komunikovat po definovaném IP protokolu, aby mohla být centrálně nastavena kvalita služby (QoS) pro přenos událostí.		
Řešení musí poskytovat kapacitu vyrovnávací paměti pro minimálně 100GB událostí, které na pobočce mohou vzniknout během výpadku spojení mezi pobočkou a datovým centrem.		
Řešení pro sběr dat z poboček musí mít výkon minimálně 5 tisíc událostí /s. a to i v trvalé zátěži.		
Řešení musí poskytnout podporu pro UDP i TCP zdroje a pro aktivní sběr z Windows agentů.		
Řešení musí být k dispozici jako fyzický systém nebo jako virtuální systém pro VMware ESXi a Hyper-V.		

Řešení musí být schopno komunikovat z pobočky na centrálu i přes vícenásobný překlad adres (NAT).		
SW Podpora		
SW - Podpora výrobce na aktualizaci systému a parserů na 1 rok . Podpora musí obsahovat aktualizaci SW minimálně 2x ročně, opravy chyb a telefonická a emailová podpora s diagnostikou vzdáleným přístupem.		