Kraj Vysočina

KUJIP01L8KB3

1151/13

SMLOUVA O POSKYTOVÁNÍ SLUŽEB

uzavřená na základě dohody smluvních stran nikoliv na úkor kterékoliv ze smluvních stran podle ustanovení § 1746 odst. 2 zákona č. 89/2012 Sb., občanský zákoník (dále jen „občanský zákoník") ") s přihlédnutím k § § 2371 a násl. občanského zákoníku a k ustanovením zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon), ve znění pozdějších předpisů

I.
Smluvní strany

Kraj Vysočina

se sídlem:	Žižkova 1882/57, 586 01 Jihlava
zastoupený:	Mgr. Vítězslavem Schrekem, MBA, hejtmanem kraje
k podpisu pověřen:	RNDr. Jan Břížďala, radní pro oblast školství, mládež a sport, informatiku a komunikační technologie
IČO:	70890749
DIČ:	CZ70890749
bankovní spojení:	Komerční banka, a.s.
číslo účtu:	123-6403810267/0100

(dále jen „**objednatel**").

a

Spolek pro budování a implementaci sdílených open source nástrojů, z. s.,

se sídlem:	Žižkova 1872/89, 586 01 Jihlava,
spisová značka:	L 22325 vedený u Krajského soudu v Brně
zastoupený:	Ing. Evou Janouškovou, ředitelkou spolku
IČO:	05730732
Bankovní spojení:	Fio Banka, a. s.
Č. účtu:	2401243360/2010
E-mail:	info@spolek-bison.cz

Kontaktní osoba zhotovitele ve věcech technických dle této smlouvy je:
Martin Hadrava, e-mail: hadrava.martin@spolek-bison.cz, tel.: 724 650 289
(dále jen „**zhotovitel**").

II.
Předmět a účel smlouvy

1) Předmětem této smlouvy je poskytnutí kapacit vývojového týmu zhotovitele za účelem výpomoci objednateli při vývoji aplikace **Technet** (dále jen „aplikace").

2) Součástí služeb je:
   - výpomoc při vývoji aplikací dle požadavků zadavatele,
   - zpracování dokumentace k zadaným programátorským pracím týkající se aplikací, včetně předání případného dokumentovaného zdrojového kódu, je-li to relevantní

- vzájemné konzultace a analýzy v průběhu vývoje aplikací.
  (dále jen „služby").

3) Zhotovitel se zavazuje řádně a včas provést služby v dohodnutém termínu, kvalitě a provedení. Objednatel je povinen za řádně a včas zhotovené služby zaplatit cenu uvedenou v čl. V. této smlouvy.

III.
Doba a místo plnění

1) Tato smlouva se uzavírá na dobu neurčitou.

2) Služby budou poskytovány průběžně po celou dobu trvání této smlouvy, a to na výzvu objednatelem pověřené osoby, kterou je Ing. Petr Pavlinec, vedoucí Odboru informatiky Krajského úřadu Kraje Vysočina. Počet odvedených člověkohodin zhotovitel vykáže vždy za každý měsíc trvání této smlouvy, a to protokolem, který odsouhlasí zástupci obou smluvních stran. Za objednatele je k podpisu protokolu pověřen Ing. Petr Pavlinec, Odbor informatiky Krajského úřadu Kraje Vysočina, za zhotovitele je k podpisu protokolu pověřen Bc. Martin Hadrava.

3) Místem poskytování služeb je Česká republika.

4) Pokud nejsou služby provedeny včas, řádně a v souladu s touto smlouvou, není objednatel povinen zaplatit cenu sjednanou v čl. V. této smlouvy.

5) Smluvní strany výslovně sjednávají, že pokud veškeré závazky z této smlouvy vyplývající nebudou zcela splněny či vypořádány do uplynutí doby trvání této smlouvy podle odst. 1 tohoto článku, platnost smlouvy se automaticky prodlužuje do doby úplného vypořádání veškerých závazků z ní vyplývajících.

IV.
Povinnosti smluvních stran

1) Zhotovitel se zavazuje řádně provést služby uvedené v čl. II. smlouvy v termínu sjednaném v čl. III. této smlouvy. Zhotovitel zabezpečí na svůj náklad a své nebezpečí všechny práce, služby a výkony související s poskytováním služeb dle této smlouvy, pokud není v této smlouvě stanoveno jinak.

2) Zhotovitel se zavazuje zachovávat mlčenlivost o všech skutečnostech, se kterými se seznámil při provádění služeb.

3) Objednatel se zavazuje za řádně a v souladu s touto smlouvou provedené služby zaplatit sjednanou cenu.

4) Smluvní strany jsou povinny se vzájemně informovat o všech okolnostech důležitých pro řádné a včasné provedení služeb a poskytovat si součinnost nezbytnou pro řádné a včasné provedení služeb.

5) Zhotovitel je povinen objednatele neprodleně informovat o jakýchkoliv okolnostech, které mohou ohrozit provedení služeb nebo způsobit zpoždění provedení služeb. Objednatel je povinen informovat zhotovitele o všech skutečnostech rozhodných pro řádné a včasné provedení služeb.

6) Zhotovitel se zavazuje nepoužít podklady poskytnuté objednatelem pro poskytování služeb ani výsledné dílo pro svoji činnost, nezveřejnit podkladový materiál nebo služby ani jeho část ani ho neposkytnout třetím osobám bez souhlasu objednatele. Poskytnuté písemné

podklady je zhotovitel povinen objednateli po ukončení poskytování služeb neprodleně vrátit.

V. Cena a platební podmínky

1) Celková a nejvýše přípustná cena za poskytování služeb v rozsahu a v kvalitě dle této smlouvy byla stanovena dohodou smluvních stran v souladu se zákonem č. 526/1990 Sb., o cenách, ve znění pozdějších předpisů, a to takto:
Cena za člověkohodinu **1000,- Kč** bez DPH
(dále jen „cena").

2) Smluvní strany se dohodly, že v případě zákonné změny sazby DPH nebudou uzavírat dodatek k této smlouvě, ale bude fakturovaná cena včetně zákonné sazby DPH.

3) Cenu uhradí objednatel na základě faktury zhotovitele po řádném a včasném dokončení části služeb, které budou specifikované v úvodní analýze a odsouhlasené zhotovitelem i objednatelem a to bezhotovostním převodem na účet zhotovitele na základě faktury vystavené zhotovitelem. Splatnost faktury je dohodou smluvních stran stanovena na 30 dnů ode dne jejího prokazatelného doručení objednateli. Faktura musí obsahovat veškeré náležitosti daňového dokladu podle zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů. Objednatel si vyhrazuje právo před uplynutím lhůty splatnosti vrátit fakturu, pokud neobsahuje požadované náležitosti nebo obsahuje nesprávné cenové údaje. Oprávněným vrácením faktury přestává běžet původní lhůta splatnosti. Opravená nebo přepracovaná faktura bude opatřena novou lhůtou splatnosti.

4) V případě, že dojde k odstoupení od této smlouvy z důvodů na straně objednatele, je zhotovitel oprávněn fakturovat objednateli cenu za v souladu s touto smlouvou zhotovenou část služeb.

5) Úhrada za plnění z této smlouvy bude realizována bezhotovostním převodem na účet zhotovitele, který je správcem daně (finančním úřadem) zveřejněn způsobem umožňujícím dálkový přístup ve smyslu ustanovení § 109 odst. 2 písm. c) zákona č. 235/2004 Sb. o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen "zákon o DPH").

6) Pokud se po dobu účinnosti této smlouvy zhotovitel stane nespolehlivým plátcem ve smyslu ustanovení § 109 odst. 3 zákona o DPH, smluvní strany se dohodly, že kraj uhradí DPH za zdanitelné plnění přímo příslušnému správci daně. Krajem takto provedená úhrada je považována za uhrazení příslušné části smluvní ceny rovnající se výši DPH fakturované zhotovitelem.

7) Za zaplacení se považuje odepsání příslušné částky z účtu objednatele.

VI. Bezpečnost informací

1) Zhotovitel je povinen dodržovat platnou legislativu ČR i EU, která se týká bezpečnosti informací.

2) Zhotovitel se zavazuje dodržovat požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv objednatele uvedené v příloze č. 1 této smlouvy.

3) Zhotovitel je povinen zajistit plnění bezpečnostních opatření a požadavků stanovených touto smlouvou ve stejné míře u všech případných poddodavatelů či jiných osob, které mají přístup k informačním aktivům objednatele prostřednictvím Zhotovitele.

4) Zhotovitel je povinen zachovávat mlčenlivost o všech skutečnostech a informacích, které mu byly v souvislosti s touto smlouvou nebo jejím plněním jakkoliv zpřístupněny, předány či sděleny, nebo o nichž se jakkoliv dozvěděl, vyjma těch, které jsou v okamžiku, kdy se s nimi zhotovitel seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění zhotovitele veřejně přístupnými stanou (dále jen „důvěrné informace"). Zhotovitel nesmí důvěrné informace použít v rozporu s jejich účelem, nesmí je použít ve prospěch svůj nebo třetích osob a nesmí je použít ani v neprospěch objednatele. Povinnosti dle tohoto odstavce je zhotovitel povinen zachovávat i po zániku této smlouvy, vyjma případů, kdy se důvěrné informace stanou prokazatelně veřejně přístupné bez zavinění zhotovitele. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je zhotovitel povinen zveřejnit důvěrnou informaci na základě povinnosti uložené zhotoviteli právním předpisem nebo rozhodnutím orgánu veřejné moci.

5) Za nesplnění kterékoliv povinnosti obsažené v tomto článku, je objednatel oprávněn účtovat zhotoviteli smluvní pokutu ve výši 100 000 Kč, a to za každé jednotlivé porušení povinností obsažených v tomto článku.

VII. Osobní údaje

1) V případě, že bude zhotovitel při plnění služeb dle čl. II této Smlouvy zpracovávat osobní údaje, je povinen zpracovávat a chránit osobní údaje v souladu se zákonem o ochraně osobních údajů, jakožto i v souladu s Nařízením Evropského parlamentu a rady (EU) 2016/679 ze dne 27. dubna 2016, o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů) od dne jeho účinnosti (dále jako „nařízení GDPR), a v souladu s dalšími evropskými i národními předpisy na úseku ochrany osobních údajů, a to zejména takto:

   a) Přístup ke zpracovávaným osobním údajům umožní zhotovitel pouze zaměstnancům zhotovitele a orgánům oprávněným provádět kontrolu, pokud není dále upraveno jinak;
   b) Zaměstnanci zhotovitele, kterým bude umožněn přístup ke zpracovávaným osobním údajům, budou zhotovitelem doložitelně poučeni o povinnosti zachovávat mlčenlivost podle § 15 zákona o ochraně osobních údajů.

2) Zhotovitel se zavazuje, že zavede vhodná technická a organizační opatření, aby byla zajištěna ochrana práv subjektu údajů.

3) Objednatel nepovoluje zhotoviteli umožnit dalšímu subjektu nakládat s osobními údaji zpracovávanými v souvislosti s touto smlouvou.

4) Zhotovitel se zavazuje zachovávat mlčenlivost o všech osobních údajích poskytnutých na základě této smlouvy včetně údajů o smluvních stranách či třetích osobách, majících charakter osobních údajů. Smluvní strany jsou si vzájemně rovněž povinny na žádost druhé smluvní strany prokázat způsob jakým je dodržování povinností stanovených zákonem zajištěno. Zhotovitel se zavazuje zároveň zajistit mlčenlivost všech svých zaměstnanců či jiných osob, jež budou přicházet do styku s osobními údaji.

5) Zhotovitel se zavazuje neuchovávat osobní údaje, s nimiž přijde do styku při poskytování služeb.

6) V případě, že zhotovitel poruší ustanovení této smlouvy, je objednatel oprávněn požadovat po poskytovateli smluvní pokutu ve výši 100.000,- Kč za každé jednotlivé porušení smlouvy ze strany poskytovatele. Poskytovatel je povinen k úhradě takovéto pokuty. Smluvní pokuta je splatná do 14 dnů od doručení oznámení o uplatnění smluvní pokuty.

7) Zároveň se poskytovatel zavazuje k úhradě škody (např. správní či jiné sankce, náhrady škody za neoprávněné nakládání s osobními údaji), která vznikla objednateli v důsledku porušení povinností zhotovitele stanovených právními předpisy či touto smlouvou či v důsledku neposkytnutí příslušné součinnosti.

VIII.
Sankce

1) V případě prodlení objednatele se zaplacením faktury vystavené zhotovitelem v souladu s článkem V. této smlouvy je zhotovitel oprávněn požadovat na objednateli úrok z prodlení ve výši 0,05% z nezaplacené částky, a to za každý i započatý den prodlení.

2) V případě, že zhotovitel neprovede služby části specifikované v termínu daném úvodní analýzou nebo v kvalitě dle této smlouvy, je objednatel oprávněn účtovat zhotoviteli smluvní pokutu ve výši 0,05% z hodnoty příslušné části služeb, a to za každý i započatý den prodlení.

3) Splatnost veškerých smluvních pokut účtovaných podle této smlouvy smluvní strany sjednávají v délce 10 dní od doručení výzvy k úhradě smluvní pokuty stranou oprávněnou straně povinné.

4) Zaplacením úroku z prodlení nebo smluvní pokuty není omezena výše nároku na náhradu škody.

IX. Ukončení smlouvy

1) Platnost smlouvy lze ukončit písemnou dohodou podepsanou oprávněnými zástupci obou smluvních stran.

2) Objednatel může od této smlouvy odstoupit, pokud zhotovitel nedodá služby v termínu stanoveném v čl. III odst. 1 této smlouvy nebo v kvalitě dle této smlouvy. Zhotovitel může od této smlouvy odstoupit, pokud objednatel nezaplatí cenu za řádně a včas splněné služby v termínu uvedeném v čl. V. této smlouvy. Odstoupení nabývá účinnosti dnem následujícím po dni prokazatelného doručení jeho písemného vyhotovení druhé smluvní straně.

3) V případě ukončení smlouvy dle tohoto článku je zhotovitel povinen předat objednateli veškerou dokumentaci k zadaným programátorským pracím týkající se aplikací, včetně předání dokumentovaného zdrojového kódu, a případně dalších podkladů souvisejících se službami objednanými objednatelem dle této Smlouvy.

X.
Ochrana nehmotných statků

1) Tento článek smlouvy se uplatní tehdy, jestliže součástí poskytování služeb bude nehmotný statek, jenž je předmětem úpravy zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon). Majetková práva k dílu náleží objednateli.

XI.
Závěrečná ustanovení

1) Tuto smlouvu lze změnit nebo doplňovat pouze písemnými vzestupně číslovanými dodatky podepsanými oprávněnými zástupci obou smluvních stran.

2) Nastanou-li u některé ze smluvních stran skutečnosti bránící řádnému plnění této smlouvy, je povinna to ihned bez zbytečného odkladu oznámit druhé straně a vyvolat jednání zástupců oprávněných k podpisu smlouvy.

3) Smlouva nabývá platnosti dnem podpisu oprávněnými zástupci obou smluvních stran a účinnosti dnem zveřejnění v informačním systému veřejné správy – Registru smluv.

4) Vzhledem k veřejnoprávnímu charakteru objednatele zhotovitel výslovně prohlašuje, že je s touto skutečností obeznámen a souhlasí se zveřejněním smluvních podmínek obsažených v této smlouvě v rozsahu a za podmínek vyplývajících z příslušných právních předpisů, zejména zák. č. 106/1999 Sb., o svobodném přístupu k informacím, v platném znění. 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.

5) Vztahy smluvních stran touto smlouvou blíže neupravené se řídí příslušnými ustanoveními občanského zákoníku s přihlédnutím k příslušným ustanovením autorského zákona.

6) Zhotovitel výslovně souhlasí se zveřejněním celého textu této smlouvy, včetně podpisů, v registru smluv dle zákona č. 340/2015 Sb., o registru smluv, ve znění pozdějších předpisů a na veřejně přístupných webových stránkách Kraje Vysočina vyjma částí, které podléhají obchodnímu tajemství. Zveřejnění smlouvy v registru smluv zajistí objednatel.

7) Právní vztahy touto smlouvou výslovně neupravené se řídí platnými obecně závaznými právními předpisy, zejména obchodním zákoníkem.

8) Tato smlouva je uzavírána smluvními stranami elektronicky.

9) Smluvní strany této smlouvy prohlašují a stvrzují svými podpisy, že mají plnou způsobilost k právním úkonům, a že tuto smlouvu uzavírají svobodně a vážně, že ji neuzavírají v tísni za nápadně nevýhodných podmínek, že si ji řádně přečetly a jsou srozuměny s jejím obsahem.

10) Nedílnou součástí této smlouvy je příloha č. 1 - Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Objednatele.

11) Smluvní strany se shodly, že podmínky této smlouvy se vztahují i na práce vykonané v období od 1. 1. 2023.

V Jihlavě

za zhotovitele:

Ing. Eva Janoušková
Digitálně podepsal Ing. Eva Janoušková
Datum: 2023.02.13 09:34:54 +01'00'

.....

Ing. Eva Janoušková, ředitelka

V Jihlavě

za objednatele:

RNDr. Jan Bříždala
Digitálně podepsal RNDr. Jan Bříždala
Datum: 2023.02.13 10:18:50 +01'00'

.....

RNDr. Jan Bříždala, radní pro oblast školství, mládež a sport, informatiku a komunikační technologie

Kraj Vysočina

Příloha č. 1

Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv Objednatele

Bezpečnostní požadavky:

- Bezpečnost přístupových oprávnění
  - Poskytovatel je povinen chránit veškeré přístupové údaje k informačním aktivům objednatele včetně přístupů k informačním aktivům poskytovatele, které umožňují přístup k informačním aktivům objednatele či umožnují jejich správu.
  - Poskytovatel je povinen dodržovat tuto bezpečnostní politiku hesel pro výše uvedené přístupové údaje:
    - min. délka hesla 17 znaků
    - složitost hesla musí splňovat minimálně 3 ze 4 kategorií
      - malá písmena
      - velká písmena
      - číslice
      - speciální znaky
    - hesla musí být uchovávána v tajnosti, nesmí být ukládána v nezašifrované podobě (dle bodu kryptografie)
    - hesla nesmí obsahovat žádné informace z přihlašovacího jména (login)
    - platnost hesla musí být maximálně 1,5 roku.
  - Poskytovatel je povinen používat personifikované účty, které jsou nepřenosné na jiné osoby, než kterým byly údaje přiděleny.
  - Přístupová oprávnění lze využívat pouze pro ten účel, pro který byla zřízena.
  - Pokud by Poskytovatel zřizoval přístupová oprávnění třetí straně, je Poskytovatel povinen o této skutečnosti informovat objednatele. Objednatel má v tomto případě právo zřízení přístupu zamítnout.
- Bezpečný vývoj
  - Ochrana před škodlivým kódem musí být zajištěna:
    - na pracovních stanicích vývojářů a programátorů,
    - na serverech/zařízení, kde je uložen zdrojový kód aplikací
  - Ke zdrojovým kódům musí být řízen přístup tak, aby k němu měli přístup pouze oprávnění vývojáři a případně jiné oprávněné osoby Poskytovatele.
  - Přístupy ke zdrojovým kódům a jejich změny musí být monitorovány a logovány. Pro správu zdrojového kódu musí být použit tzv. verzovací systém.
  - Zdrojové kódy systému musí být pravidelně zálohovány a zálohy pravidelně testovány na jejich obnovitelnost.
  -
- Řízení změn
  - Poskytovatel se zavazuje zaznamenávat všechny změny, které v informačním aktivu provedl.
  - Poskytovatel se zavazuje vynucovat zaznamenávání změn i u případných subposkytovatelů.
  - Záznam změny musí obsahovat minimálně tyto informace:
    - Datum a čas změny
    - Jméno osoby, která změnu provedla
    - Název, popis a účel změny
  - Objednatel si vyhrazuje právo na pravidelné informace o záznamech všech změn provedených Zhotovitelem i případnými subzhotoviteli/subposkytovateli.

- Poskytovatel se zavazuje všechny jím provedené změny i změny případných subzhotovitelů poskytnout zadavateli formou (provozního deníku vedeného v SW objednatele/pravidelného měsíčního reportu).

- Řízení rizik
  - Objednatel si vyhrazuje právo na informace o tom, jakým způsobem Zhotovitel řídí rizika v souvislosti s plněním této smlouvy, tedy o tom, jakou metodiku pro řízení rizik používá, jakým způsobem jsou rizika hodnocena a klasifikována, jakým způsobem jsou rizika ošetřována a kdo je za řízení rizik za Zhotovitele zodpovědný.
  - Poskytovatel se zavazuje řídit rizika informační bezpečnosti minimálně v následujícím rozsahu:
    - Identifikace a ohodnocení aktiv souvisejících s plněním této smlouvy,
    - Identifikace, analýza a ohodnocení rizik souvisejících s plněním této smlouvy,
    - Zvládání a monitoring rizik souvisejících s plněním této smlouvy.
- Řízení kybernetických bezpečnostních incidentů:
  - Poskytovatel je povinen objednateli hlásit veškeré kybernetické bezpečnostní incidenty, které by mohli mít nějakou souvislost s:
    - informačními aktivy objednatele,
    - přístupovými údaji k informačním aktivům objednatele,
    - informacím objednatele.
  - Poskytovatel je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy Kraje Vysočina.

- Kryptografie:

Obecně

Pro šifrování, elektronické podepisování a provádění otisků dat (hashování) nesmí být použity proprietární/uzavřené algoritmy, ale ty, které jsou považovány za standardy, jejich funkcionalita je všeobecně známá a popsaná.

Hashovací funkce

Ukládání otisků hesel
- pro ukládání hesel uživatelů mohou být použity pouze tyto tzv. pomalé hashovací funkce:
  - Argon2i
  - bcrypt
  - scrypt
  - PBKDF2
- při hashování hesla musí být použit pseudonáhodně vygenerovaný kryptografický salt
- pro ukládání hesel nesmí být použity tzv. rychlé hashovací funkce typu MD-X, SHA-X, apod.

Elektronické podepisování e-mailů a dokumentů
- SHA-2 a vyšší
- délka otisku 256 bitů a vyšší

Ověřování integrity souborů
- SHA-2 a vyšší
- délka otisku 224 bitů a vyšší

Asymetrická kryptografie

SSL/TLS

- verze protokolu minimálně TLSv1.2 a vyšší
- konfigurace
  - cipher suite musí být vybrána na základě serverem preferovaného pořadí
  - vyšší priority musí mít cipher suites, které obsahují varianty asymetrických algoritmů s eliptickými křivkami, např.:
    - ECDHE musí mít vyšší prioritu než DHE
    - ECDSA musí mít vyšší prioritu než DSA
  - všechny EXPORT cipher suites musí být zakázány
  - algoritmy a funkce pro výměnu klíčů
    - algoritmus pro výměnu klíčů musí podporovat Perfect forward secrecy
      - tzn., že šifrovací klíč je vyměněn mezi klientem a serverem tak, aby jej nebylo možné získat se znalostí privátního klíče serveru, např. musí být použit Diffie-Hellman (DH nebo ECDH) algoritmus
      - a navíc se musí jednat o tzv. ephemeral Diffie-Hellman (DHE, ECDHE), tzn., že pro každou session je generován nový set Diffie-Hellman klíčů
    - délky klíčů:
      - pro Diffie-Hellman (DH) - 2048 bitů a více (postupně přecházet na 3072 bitů, tam kde to bude možné)
      - pro Elliptic Curve Diffie-Hellman (ECDH) – 256 bitů a více
    - nesmí být použita anonymní výměna klíčů
  - algoritmy a funkce pro autentizaci
    - minimální délky klíčů:
      - RSA - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
      - ECDSA - 256 bitů
  - algoritmy a funkce pro symetrické šifrování
    - nesmí být použita hodnota NULL v cipher suites
    - nesmí být použity tyto šifry:
      - DES, 3DES, RC4
    - minimální délka šifrovacího klíče - 128 bitů
    - cipher suites s šiframi s větší délkou klíče musí mít větší prioritu v seznamu ciphersuites než s menší délkou klíče
  - MAC (Message Authentication Code)
    - použití SHA funkce s minimální délkou hashe 256 bitů
    - vyšší délky otisků musí mít vyšší prioritu v cipher suites
- Certifikáty dodá zadavatel

TLS cipher suites

- Doporučené cipher suites (v doporučeném pořadí), které naplňují výše zmíněné požadavky
- TLS1.3:
  TLS_AES_256_GCM_SHA384
  TLS_CHACHA20_POLY1305_SHA256
  TLS_AES_128_GCM_SHA256
  TLS_AES_128_CCM_SHA256

- TLS1.2:
  TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
  TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
  TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
  TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
  TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256

TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256

Šifrování, podepisování a autentizace

- týká se různých technologií PKI, PGP, S/MIME, SSH, apod.
- minimální délka klíče
  - algoritmus DSA – 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
  - algoritmus RSA - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to bude možné)
  - algoritmus ECDSA - 256 bitů
- Ověřování (např. SSH klíče)
  - délka klíče minimálně 2048 bitů u RSA a DSA algoritmů (postupně přecházet na 3072 bitů, tam kde to bude možné)
  - délka klíče minimálně 256 bitů u algoritmů používajících eliptické křivky

Symetrická kryptografie

- nesmí být použity tyto šifry:
  - DES, 3DES, RC4, Blowfish, Kasumi
- minimální délka šifrovacího klíče - 128 bitů
  - pro šifru Chacha20 minimálně 256 bitů a se zatížením klíče menším než 256 GB
- nesmí být použity tyto módy pro ochranu integrity:
  - HMAC-SHA1, CBC-MAC-X9.19