

## SMLOUVA O POSKYTOVÁNÍ SLUŽEB

Číslo smlouvy zhotovitele: č. 10/1/2020

Smluvní strany:

a) Objednatel

**Koordinátor Integrovaného dopravního systému Olomouckého kraje, příspěvková organizace**

IČ: 72556064

DIČ: CZ72556064

se sídlem: Jeremenkova 1211/40b, Hodolany, 779 00 Olomouc

zapsaný v Obchodním rejstříku vedeném Krajským soudem v Ostravě, spisová značka Pr 5064

zastoupený Ing. Kateřina Suchánková, MBA - ředitelka

Bankovní spojení: [REDACTED]

Číslo účtu (CZK): [REDACTED]

(dále jen jako „objednatel“)

a

b) Poskytovatel

**ABIRAIL CZ s.r.o.**

IČ: 01732544

DIČ: CZ01732544

se sídlem Peroutková 290/5, 60200 Brno

zapsaný v Obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka 79219

zastoupený: Ing. Jiří Janšta, jednatel společnosti

Ing. Ondřej Kovář, jednatel společnosti

Bankovní spojení: [REDACTED]

Číslo účtu (CZK): [REDACTED]

(dále jen jako „poskytovatel“ a společně s objednatel dále jen „strany“ a každá z nich samostatně „strana“)

mezi sebou uzavírají

dle § 1746 odst. 2 zákona č. 89/2012 Sb., občanského zákoníku

následující smlouvu o poskytování služeb (dále jen „smlouva“):

I.

Předmět smlouvy

Poskytovatel se touto smlouvou zavazuje poskytovat pro objednatel ve sjednané době produkční prostředí pro aplikaci ABIRUN APC a datové SIM karty do vozidel na dobu určitou, a to nejméně do 31. 12. 2027.

Poskytovatel bude poskytovat službu v kvalitě a rozsahu stanoveném touto smlouvou ode dne podpisu této smlouvy dle části V. Předání a poskytování služeb (dále jen „služby“). Objednatel se zavazuje zaplatit poskytovateli za poskytování služeb níže stanovenou cenu.

1. Podrobný popis poskytovaných služeb:
  - a) Produkční prostředí pro aplikaci ABIRUN APC
    1. Hostingové služby pro dedikovaný server
      - a. Operační systém Windows Server 2019
      - b. 6 GB RAM
      - c. 150 GB SSD
      - d. Zálohování dat
      - e. FTP server
      - f. Pevná veřejná IP adresa (IPv4)
      - g. Internetová konektivita
      - h. Zálohování dat v geograficky oddělené lokalitě
      - i. Součinnost pro aktualizaci DNS záznamů s objednatelem
      - j. Databázový systém MS SQL server 2016 standard edition
    2. SMTP server pro distribuci e-mailů
  - b) Datové SIM karty pro 20 ks autobusů vybavených systémem pro automatické počítání cestujících:
    1. 150 MB data za měsíc – přenos naměřených dat z vozidel

## II.

### Podklady pro poskytování služeb

1. Základním podkladem pro zpracování předmětu plnění jsou tyto dokumenty:
  - Smlouva o dílo.
2. Objednatel se zavazuje, že na vyzvání poskytovatele mu bez zbytečného odkladu poskytne další vyjádření, stanoviska, případně doplnění podkladů, jejichž potřeba vznikne v průběhu poskytování služeb.

## III.

### Cena za poskytované služby a platební podmínky

1. Objednatel je povinen poskytovateli zaplatit za poskytované služby v rozsahu definovaném dle části I. Předmět smlouvy  
Cenu ve výši 1450,- Kč (slovy: jedentisícčtyřistapadesát korun českých) bez DPH za měsíc, pokud je poskytovatel plátcem DPH, bude daňový doklad vystaven v souladu se zákonem o DPH.
2. Poskytované služby budou fakturovány vždy k poslednímu dni v měsíci, za který byly poskytnuty.
3. Platba ceny za služby dle této smlouvy bude objednatelem provedena na základě faktur vystavených zhotovitelem. Objednatel nebude poskytovat žádné zálohy. Splatnost faktur se stanovuje na dvacetjedna (21) kalendářních dnů ode dne doručení daňového dokladu objednateli. Cena za poskytované služby nemůže být navýšena. Platby budou probíhat výhradně v Kč, rovněž cenové údaje budou v této měně. Faktura musí být doručena objednateli nejdéle do 5 kalendářních dnů od data vystavení faktury.
4. Faktury budou mít náležitosti účetního dokladu podle zákona č. 563/1991 Sb. ve znění pozdějších předpisů a náležitosti daňového dokladu podle §28, odst. 2, zákona č. 235/2004 Sb. ve znění pozdějších předpisů.

5. V případě, že faktury nebudou mít odpovídající náležitosti, je objednatel oprávněn je vrátit ve lhůtě splatnosti zpět poskytovateli k doplnění, aniž se tak dostane do prodlení se splatností. Lhůta splatnosti počíná běžet znovu od opětovného zaslání náležitě doplněného či opraveného daňového dokladu.
6. Závazek objednatele zaplatit fakturu je splněn připsáním fakturované částky na účet poskytovatele.
7. Faktura bude obsahovat výkaz poskytovaných služeb za období, za které bude příslušná faktura vystavena. Součástí výkazu bude uvedené procento dostupnosti poskytovaných služeb.
8. Poskytovatel bude objednateli posílat faktury v elektronické podobě na e-mail: kidsok@kidsok.cz.
9. Úhrada za plnění z této smlouvy bude realizována bezhotovostním převodem na účet poskytovatele, který je správcem daně (finančním úřadem) zveřejněn způsobem umožňujícím dálkový přístup ve smyslu ustanovení § 98 zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů (dále jen „zákon o DPH“).
10. Pokud se po dobu účinnosti této smlouvy poskytovatel stane nespolehlivým plátcem ve smyslu ustanovení § 106a zákona o DPH, smluvní strany se dohodly, že objednatel uhradí DPH za zdanitelné plnění přímo příslušnému správci daně. Objednatel takto provedená úhrada je považována za uhrazení příslušné části smluvní ceny rovnající se výši DPH fakturované poskytovatelem.

#### IV. Termín plnění

1. Poskytovatel se zavazuje k poskytování služeb dle předmětu této smlouvy v následujících termínech:
  - poskytování služeb od podpisu smlouvy do 31. 12. 2027 smlouvy.

#### V. Předání a poskytování služeb

1. Poskytovatel splní svou povinnost poskytovat služby jejich řádným zpřístupněním dle části IV. této smlouvy takto:
  - a. zpřístupněním aplikace ABIRUN APC na veřejně dostupné internetové adrese dostupná aplikace ABIRUN APC a předáním přístupových údajů pro přihlášení,
  - b. přenosem dat ze systému automatického počítání cestujících z 20 vozidel vybavených tímto systémem za každý den provozu takového vozidla,
  - c. ukládáním a zálohováním dat ze systému automatického počítání cestujících,
  - d. publikováním dat ze systému automatického počítání cestujících prostřednictvím aplikace ABIRUN APC.
2. Poskytovatel zahájí poskytování služeb dnem podpisu této smlouvy. Funkčnost poskytovaných služeb potvrdí poskytovateli za objednatele osoba odpovědná za smluvní vztah v předávacím protokolu.
3. Poskytované služby se považují za splněné, pokud dostupnost služeb je 99 % časovém intervalu od 0:00 do 23:59 v jednotlivých dnech za daný kalendářní měsíc.

#### VI. Práva a povinnosti poskytovatele

1. Poskytovatel je povinen poskytovat služby v kvalitě a rozsahu, jež je určena charakterem této smlouvy.
2. Poskytovatel prohlašuje, že disponuje potřebnými odbornými znalostmi a schopnostmi pro poskytování služeb podle této smlouvy.

3. Poskytovatel se zavazuje, že data, která obdrží pro účely plnění této smlouvy od objednatele a výsledky služeb z těchto dat podle této smlouvy neposkytne bez písemného souhlasu objednatele dalším subjektům.
4. Poskytovatel zpřístupní službu pouze osobám určeným objednatelem.
5. Poskytovatel je povinen zachovat mlčenlivost o všech skutečnostech, o kterých se při plnění této smlouvy dozvěděl. Povinnosti mlčenlivosti může poskytovatele zprostit jen objednatel svým písemným prohlášením či zmocněním a dále v případech stanovaných zákonnými předpisy.
6. Poskytovatel se zavazuje, že při své činnosti bude postupovat nanejvýš diskrétně a bude dbát, aby nebyla poškozena dobrá pověst objednatele.
7. Poskytovatel je povinen chránit zájmy objednatele, zejména je povinen upozornit objednatele na veškerá nebezpečí škod, která jsou mu známa a která souvisejí s poskytováním služeb.
8. Poskytovatel se zavazuje zajistit ochranu dat objednatele, nesoucích informace o osobních údajích objednatele nebo jeho zaměstnanců, s nimiž přijde poskytovatel či jeho zaměstnanci, do styku při plnění dle této smlouvy, a to v souladu s právními předpisy o zpracování a ochraně osobních údajů.

## VII.

### Práva a povinnosti objednatele

1. Objednatel se zavazuje poskytnout poskytovateli maximální součinnost a veškeré potřebné informace k funkcionalitám poskytovaných služeb.
2. Objednatel se povinen informovat poskytovatele o všech důležitých skutečnostech, které by mohly mít vliv na realizaci předmětu smlouvy.
3. Objednatel je povinen předávat a aktualizovat seznam svých zaměstnanců, kteří mají přístup k poskytovaným službám. Aktualizovaný seznam zaměstnanců bude odeslán na e-mail poskytovatele: [podpora@abirail.cz](mailto:podpora@abirail.cz)
4. Objednatel je povinen zpřístupnit poskytované služby pouze svým zaměstnancům. Objednatel není oprávněn zpřístupnit službu třetím osobám nebo požadovat nastavení přístupových oprávnění ke službám pro třetí osoby.

## VIII.

### Zajištění závazků poskytovatele a objednatele

1. V případě nedodržení doby plnění dohodnuté ve smlouvě o poskytování služeb je poskytovatel povinen uhradit objednateli smluvní pokutu ve výši 500,- Kč (pět set korun českých) za každý započatý den prodlení.
2. Z důvodu nedodržení termínu odstranění vad poskytované služby je poskytovatel povinen objednateli uhradit smluvní pokutu 500,- Kč (pět set korun českých) za každý započatý den prodlení.
3. V případě nedodržení parametru dostupnosti poskytovaných služeb dle části V. odstavce 3 v daném kalendářním měsíci, je objednatel oprávněn požadovat po poskytovateli zaplacení smluvní pokuty ve výši 1 % z ceny poskytovaných služeb v daném měsíci za každé započaté procento nedostupnosti služeb nad dohodnutou povolenou nedostupnost služeb.
4. Při prodlení úhrady peněžitého plnění zaplatí objednatel poskytovateli smluvní pokutu ve výši 0,05 % z dlužné částky za každý započatý den prodlení.
5. Smluvní pokutu je příslušná smluvní strana povinna uhradit do jednoho měsíce po obdržení výzvy k zaplacení smluvní pokuty.
6. Těmito ujednáními není dotčeno právo objednatele a poskytovatele na náhradu způsobené škody, která by vznikla objednateli nebo poskytovateli v příčinné souvislosti s porušením této smlouvy druhou stranou.

7. Strany jsou oprávněny, v případě neuhrazení vyúčtované smluvní pokuty, tuto smluvní pokutu započíst vůči jakémukoli finančnímu plnění poskytovanému druhé straně, a to i v rámci jiného obchodního případu.

#### IX.

##### Odpovědnost za vady

1. Poskytované služby mají vady, jestliže jejich výsledek neodpovídá předmětu smlouvy, účelu jeho využití, případně pokud nemá vlastnosti výslovně stanovené touto smlouvou, technickými normami nebo jinou dokumentací poskytnutou poskytovateli v písemné podobě před započítáním poskytování služeb. Za vadu poskytovaných služeb se považuje i jejich neúplnost.
2. Odstranění případných vad bude poskytovatelem provedeno bezodkladně, nejpozději však ve lhůtách sjednaných mezi smluvními stranami po uplatnění reklamace objednatelem.
3. Objednatel je oprávněn uplatňovat svá případná práva z odpovědnosti poskytovatele za vady plnění podle této smlouvy, níže uvedeným způsobem:
  - v případě neodstranitelných vad má objednatel právo požadovat odstranění vady bezplatným dodáním nové služby nebo jeho části, nebo právo na přiměřenou slevu z ceny za službu,
  - v případě odstranitelných vad požadovat odstranění vady bezplatnou opravou služby nebo jeho části, nebo právo na přiměřenou slevu z ceny za službu.

#### X.

##### Bezpečnost informací

- Poskytovatel je povinen dodržovat platnou legislativu ČR i EU, která se týká bezpečnosti informací.
- Poskytovatel se zavazuje dodržovat požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv objednatele uvedené v příloze č. 1 této smlouvy.
- Poskytovatel je povinen zajistit plnění bezpečnostních opatření a požadavků stanovených touto smlouvou ve stejné míře u všech případných subdodavatelů či jiných osob, které mají přístup k informačním aktivům objednatele prostřednictvím poskytovatele.
- Poskytovatel 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 poskytovatel seznámil, prokazatelně veřejně přístupné nebo těch, které se bez zavinění poskytovatele veřejně přístupnými stanou (dále jen „důvěrné informace“). Poskytovatel 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 poskytovatel povinen zachovávat i po zániku této smlouvy, vyjma případů, kdy se důvěrné informace stanou prokazatelně veřejně přístupné bez zavinění poskytovatele. Povinnosti dle tohoto odstavce se nevztahují na případy, kdy je poskytovatel povinen zveřejnit důvěrnou informaci na základě povinnosti uložené poskytovateli právním předpisem nebo rozhodnutím orgánu veřejné moci.
- Za nesplnění kterékoliv povinnosti obsažené v tomto článku, je objednatel oprávněn účtovat poskytovateli smluvní pokutu ve výši 2.000 Kč, a to za každé jednotlivé porušení povinností obsažených v tomto článku.

#### XI.

##### Záruka za jakost

1. Objednatel je povinen zjištěnou vadu písemně oznámit poskytovateli (uplatnění reklamace) bez zbytečného odkladu. Za písemnou formu se považuje též doručení emailu s nárokem na



adresu: [podpora@abirail.cz](mailto:podpora@abirail.cz). Poskytovatel je povinen na základě oznámení vady objednatelem bezplatně odstranit vady reklamované v průběhu záruční doby.

2. Pokud se prokáže reklamace jako neoprávněná, objednatel je povinen uhradit poskytovateli přiměřené náklady spojené s posouzením reklamace, technickými pracemi a ověřováním funkčnosti.

## XII.

### Odstoupení od smlouvy

1. Kterákoliv ze stran je oprávněna od této smlouvy odstoupit, poruší-li druhá strana podstatným způsobem své smluvní povinnosti, přestože byla na tuto skutečnost prokazatelným způsobem upozorněna.

Za podstatné porušení smlouvy se považuje:

- prodlení objednatele se zaplacením ceny po dobu delší než třicet (30) dnů,
  - prodlení poskytovatele s poskytováním služeb po dobu delší než dvacet (20) dnů,
  - zjištění, že parametry poskytovaných služeb neodpovídají požadavkům stanoveným smlouvou,
  - opakované porušení povinností poskytovatele vyplývajících z této smlouvy, přičemž za opakované porušení se považuje takové porušení, na které objednatel poskytovatele již v minulosti výslovně upozornil,
  - prodlení poskytovatele s odstraněním vady delším než třicet (30) dnů.
2. Stanoví-li oprávněná strana druhé straně pro splnění jejího závazku náhradní (dodatečnou) lhůtu, vzniká jí právo odstoupit od smlouvy až po marném uplynutí této lhůty, to neplatí, jestliže druhá strana v průběhu této lhůty prohlásí, že svůj závazek nesplní. V takovém případě může dotčená strana odstoupit od smlouvy i před uplynutím lhůty dodatečného plnění, poté, co prohlášení druhé strany obdržela.
  3. Objednatel je oprávněn od této smlouvy odstoupit bez udání důvodu s výpovědní lhůtou 3 měsíce

## XIII.

### Důvěrné informace

1. Strany se dohodly, že za důvěrné informace dle této smlouvy jsou považovány nejen veškeré údaje uvedené v dokladech, na které smlouva odkazuje, a dále i jakékoli informace vyměněné mezi stranami, či stranami jinak získané v souvislosti s plněním této smlouvy (dále jen „důvěrné informace“).
2. Za důvěrné informace nebudou považovány informace, které jsou veřejně přístupné nebo známé v době jejich užití nebo zpřístupnění, pokud jejich veřejná přístupnost či známost nenastala v důsledku porušení zákonné či smluvní povinnosti, nebo byly prokazatelně k dispozici jedné ze stran ještě předtím, než druhá strana projevila zájem uzavřít tuto smlouvu. Strany se zavazují, že bez předchozího písemného souhlasu druhé strany:
  - neužijí důvěrné informace pro jiné účely než pro účely poskytovaných služeb a splnění povinností podle této smlouvy, a nebo
  - nezveřejní ani jinak neposkytnou důvěrné informace žádné třetí osobě, vyjma svých pověřených zaměstnanců, členů svých vnitřních orgánů, odborných poradců a právních zástupců.
3. Pokud bude jakýkoli orgán státní správy a samosprávy, soud či jiný veřejný orgán vyžadovat poskytnutí jakékoli důvěrné informace, oznámí strana takovou skutečnost bez zbytečného odkladu písemně druhé straně a bude s ní spolupracovat při uplatnění všech zákonných prostředků, které mohou odhalení důvěrné informace zabránit.

XIV.  
Závěrečná ustanovení

1. Pokud se jakékoliv ustanovení této smlouvy stane nebo bude shledáno příslušným soudem nebo jiným orgánem neplatným, neúčinným nebo nevymahatelným, bude takové ustanovení považováno za vypuštěné ze smlouvy a ostatní ustanovení této smlouvy budou nadále trvat, pokud z povahy takového ustanovení nebo z jeho obsahu anebo z okolností, za nichž bylo uzavřeno, nevyplývá, že je nelze oddělit od ostatního obsahu této smlouvy. Strany v takovém případě bez zbytečného odkladu uzavřou takové dodatky k této smlouvě, které umožní dosažení výsledku stejného, a pokud to není možné, pak co nejbližšího tomu, jakého mělo být dosaženo neplatným, neúčinným nebo nevymahatelným ustanovením.
2. Tato smlouva může být měněna a doplňována pouze prostřednictvím písemných průběžně číslovaných dodatků podepsaných oběma stranami. Za písemnou formu nebude pro tento účel považována výměna emailových či jiných elektronických zpráv.
3. Smlouva je vyhotovena ve dvou rovnocenných vyhotoveních, z nichž každé má platnost originálu. Každá strana obdrží po jednom vyhotovení.
4. Smlouva nabývá platnosti dnem podpisu a účinnosti dnem uveřejnění v informačním systému veřejné správy – Registru smluv. Poskytovatel výslovně souhlasí se zveřejněním celého textu této smlouvy včetně podpisů v informačním systému veřejné správy – Registru smluv. Zákonnou povinnost dle § 5 odst. 2 zákona č. 340/2015 Sb., o registru smluv splní objednatel a splnění této povinnosti písemně potvrdí poskytovateli.
5. Obě strany prohlašují, že si smlouvu pečlivě přečetly a na důkaz souhlasu s výše uvedenými ustanoveními připojují své podpisy.

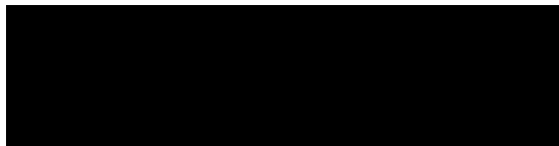
Příloha č. 1 Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv

V Olomouci dne

1.2.2021

V Brně dne

Objednatel

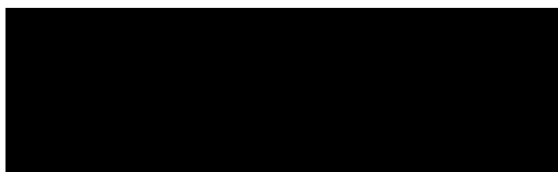


Ing. Kateřina Suchánková, MBA

Poskytovatel



Ing. Jiří Janšta, jednatel společnosti



Ing. Ondřej Kovář, jednatel společnosti

## Příloha č. 1 - Požadavky a opatření pro zajištění bezpečnosti informací a informačních aktiv

- **Bezpečnost přístupových oprávnění**
  - Poskytovatele je povinen chránit veškeré přístupové údaje k informačním aktivům objednatele včetně přístupů k informačním aktivům poskytovatele, které umožňují přístup k informačním aktivům objednatele či umožňují jejich správu.
  - Poskytovatel je povinen dodržovat tuto bezpečnostní politiku hesel pro výše uvedené přístupové údaje:
    - min. délka hesla 12 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 rok.
  - Poskytovatel je povinen používat personifikované účty, které jsou nepřenositelné 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.
- **Řízení kybernetických bezpečnostních incidentů:**
  - Poskytovatel je povinen objednateli hlásit veškeré kybernetické bezpečnostní incidenty, které se týkají informačních aktiv objednatele nebo informačních aktiv poskytovatele, pokud se kybernetický bezpečnostní incident týká informací či informačních aktiv objednatele.
  - Poskytovatel je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy objednatele.
- **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
  - **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
        - výměna 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 algoritmus
            - a navíc se musí jednat o tzv. ephemeral Diffie-Hellman (DHE), tzn. že pro každou session je generován nový set Diffie-Hellman klíčů
          - v případě použití Diffie-Hellman algoritmu musí mít modulo délku minimálně 2048b (2048-bit group)
          - nesmí být použita anonymní výměna klíčů
      - autentizace
        - minimální délky klíčů:
          - RSA - 2048 bitů
          - ECDSA - 256 bitů
      - 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 1024b
        - vyšší délky otisků musí mít vyšší prioritu v cipher suites
      - Způsob naplnění:
        - Diffie-Hellman implementace: <https://weakdh.org/sysadmin.html>
    - certifikáty
      - minimální délka privátního klíče
        - RSA 2048 bitů
        - ECDSA - 256 bitů
      - hash funkce pro podpis
        - SHA-2 s minimální délkou 224 bitů

- v případě veřejně publikované webové aplikace (pokud VKB neurčí jinak)
  - certifikát musí být vydán důvěryhodnou certifikační autoritou
  - musí se jednat o EV certifikát
  - je možné použít multi-domain certifikát
  - EV certifikát nesmí mít platnost delší než 3 roky
- ověřování (např. SSH klíče)
  - délka klíče minimálně 2048 b u RSA a DSA algoritmů
  - délka klíče minimálně 256 bitů u algoritmů používajících eliptické křivky
- Symetrická kryptografie
  - nesmí být použity tyto šifry:
    - DES, 3DES, RC4
    - minimální délka šifrovacího klíče - 128 bitů