Kraj Vysočina

SMLOUVA O DÍLO

uzavřená podle § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů

Kraj Vysočina
se sídlem: Žižkova 1882/57, 58601 Jihlava
zastoupený: Mgr. Vítězslavem Schrekem, MBA, hejtmanem kraje
k podpisu pověřen: RNDr. Jan Bříždala, radní pro oblast školství, mládež a sport, informatiku a komunikační technologie
IČO: 70890749
DIČ: CZ70890749
(dále jen „**Objednatel**")

a

GORDIC spol. s r.o.
se sídlem: Erbenova 4, 586 01 Jihlava
zastoupená: Ing. Jaromírem Řezáčem, jednatelem
IČO: 47903783
DIČ: CZ47903783
bankovní spojení: Komerční banka, a.s.
číslo účtu: 19-4645570287/0100
zapsaná v obchodním rejstříku vedeném Krajským soudem v Brně, oddíl C, vložka č. 9313
(dále jen „**Zhotovitel**")

uzavírají níže uvedeného dne, měsíce a roku

tuto smlouvu:

Čl. I
Účel a předmět smlouvy

1. Účelem této smlouvy je potřeba Objednatele zajistit provazbu mezi systémem GINIS a systémem Vismo – publikace úřední desky, prostřednictvím softwarového modulu (dále jen "modul").
2. Zhotovitel se zavazuje na svůj náklad a nebezpečí provést pro Objednatele dodávku a implementaci modulu, při současném poskytnutí licence – oprávnění k výkonu práva užívat související autorské SW dílo (dále také „dílo").
3. Objednatel se zavazuje dokončené dílo převzít a zaplatit za něj sjednanou cenu.
4. Přesná kalkulace této ceny a struktura jednotlivých cenových položek je uvedena v Příloze č. 2 této Smlouvy.

Čl. II
Práva a povinnosti smluvních stran

1. Zhotovitel se zavazuje provést pro Objednatele dílo specifikované v čl. I této smlouvy za podmínek stanovených touto smlouvou.

2. Smluvní strany se zavazují informovat se navzájem o všech skutečnostech, které mají, nebo by mohly mít vliv na plnění této smlouvy.
3. Smluvní strany jsou povinny poskytovat si nezbytnou součinnost k plnění této smlouvy.

Čl. III
Doba a místo plnění

1. Místem plnění je sídlo Objednatele na adrese Žižkova 1882/57, Jihlava.
2. Zhotovitel je povinen dílo řádně dodat Objednateli v termínu do 31. 12. 2023.
3. Řádné a včasné dodání předmětu této smlouvy bude potvrzeno předávacím protokolem, který bude obsahovat zhodnocení prací a soupis zjištěných vad a nedodělků s termínem pro jejich odstranění. Předávací protokol bude podepsán kontaktními osobami obou smluvních stran.
4. Objednatel je povinen dílo převzít za předpokladu, že je řádně a včas dokončené, odpovídá této smlouvě a je prosté vad a nedodělků s výjimkou drobných ojedinělých vad a nedodělků, které nebrání řádnému užívání díla.

Čl. IV
Cena za dílo

1. Smluvní strany se dohodly, že celková cena za dílo činí **74 950 Kč** bez DPH, 21 % DPH činí 15 739,50 Kč, cena včetně DPH je 90 689,50 Kč (slovy devadesát tisíc šest set osmdesát devět korun českých padesát haléřů).
2. Smluvní strany se dohodly, že v případě změny zákonné sazby DPH uvedené v ceně nebudou uzavírat písemný dodatek na změnu ceny a DPH bude účtována podle předpisů platných v době uskutečnění zdanitelného plnění.

Čl. V
Platební podmínky

1. Cena bude uhrazena na základě faktury - daňového dokladu vystaveného Zhotovitelem. Zhotovitelem předložená faktura bude mít splatnost 14 dnů ode dne prokazatelného doručení Objednateli.
2. Zaplacením se pro účely této smlouvy rozumí odepsání příslušné částky z účtu Objednatele ve prospěch účtu Zhotovitele. Účet Zhotovitele uvedený v záhlaví smlouvy 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"). V případě, že v době platby tento účet nebude zveřejněn u správce daně, zaplatí Objednatel cenu na jiný účet Zhotovitele, který bude zveřejněn v souladu s § 109 odst. 2 písm. c) zákona o DPH.
3. Faktura musí obsahovat náležitosti daňového dokladu podle zákona č. 563/1991 Sb., o účetnictví, ve znění pozdějších předpisů, a zákona č. 235/2004 Sb., o dani z přidané hodnoty, ve znění pozdějších předpisů.
4. Fakturu, která neobsahuje uvedené náležitosti, nebo jsou-li uvedeny nesprávně či neúplně, je Objednatel oprávněn vrátit Zhotoviteli. Při nezaplacení takto vystavené a doručené faktury není Objednatel v prodlení se zaplacením. Po doručení řádně vystavené faktury běží znovu sjednaná lhůta splatnosti.
5. 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 Objednatel

uhradí DPH za zdanitelné plnění přímo příslušnému správci daně. Objednatelem takto provedená úhrada je považována za uhrazení příslušné části smluvní ceny rovnající se výši DPH fakturované Zhotoviteli.

Čl. VI
Kontaktní osoby

1. Kontaktní osobou Zhotovitele je: Ivan Kugler, e-mail: ivan.kugler@gordic.cz , mobil 603 466 382, adresa: KMS software s. r. o., Brněnská 604/22, Jihlava.
2. Kontaktní osoba Kupujícího ve věcech technických je: Ing. Karel Žák, zak.k@kr-vysocina.cz , tel.: 564 602 309.

Čl. VII
Vlastnické právo a nebezpečí škody

1. Vlastnické právo k nosiči softwarových produktů, na kterém bude dílo uloženo, přechází na Objednatele okamžikem jeho převzetí. Předání bude potvrzeno podpisem předávacího protokolu.
2. Nebezpečí vzniku nahodilé škody na nosiči softwarových produktů přechází na Objednatele okamžikem jeho převzetí.

VIII. Licenční ujednání

1. Ke všem částem díla, které mají povahu autorského díla ve smyslu zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů, ve znění pozdějších předpisů („autorský zákon"), a k nimž Zhotovitel má nebo mu vznikne majetkové autorské právo, poskytuje Zhotovitel Objednateli licenci ke všem způsobům užití známým ke dni uzavření této smlouvy, a to s účinností ode dne přechodu vlastnického práva k věci, v níž bylo konkrétní autorské dílo zahrnuto, nejpozději však ode dne dokončení díla.
2. Licenci dle předcházejícího odstavce této smlouvy Zhotovitel uděluje Objednateli jako nevýhradní, přenosnou, na dobu trvání majetkových práv autora, v neomezeném územním rozsahu. Odměna za udělení licence je součástí ceny dle Čl. IV této smlouvy.

Čl. IX
Odpovědnost za škodu

1. Smluvní strany odpovídají za škodu způsobenou porušením povinností vyplývajících z této smlouvy nebo z obecně závazného právního předpisu.
2. Náhrada škody se řídí § 2913 a násl. občanského zákoníku.

Čl. X
Záruční podmínky

1. Zhotovitel poskytuje Objednateli na dílo řádně dodané v souladu s podmínkami této smlouvy záruku za jakost díla v délce 12 měsíců od jeho protokolárního převzetí Objednatelem. V případě, že bylo dílo předáno s drobnými vadami a nedodělky, jež nebrání řádnému užívání díla, počíná záruční době běžet ode dne odstranění těchto vad a nedodělků.

2. Zhotovitel poskytuje záruku na celé dílo a všechny jeho součásti po celou dobu trvání záruční doby, včetně sjednaných technických parametrů.
3. Záruka se vztahuje na všechny vady, s výjimkou vad díla, které jsou způsobeny výlučně objednatelem nebo třetími osobami. Zhotovitel je povinen bez zbytečného odkladu nejpozději do 3 kalendářních dnů po oznámení vady Objednatelem Zhotoviteli, dostavit se po předchozí dohodě na místo stanovené Objednatelem v oznámení vady, a není-li takové místo určeno, pak do sídla Objednatele, za účelem projednání reklamace vad a v téže době Objednateli písemně sdělit, zda jsou oznámené vady záručními vadami nebo jde o vady mimozáruční.
4. Zhotovitel je povinen záruční vady odstranit nejpozději do 10 kalendářních dnů od jejich oznámení Objednatelem Zhotoviteli, nebude-li mezi smluvními stranami písemně dohodnut jiný termín pro odstranění vad.
5. Pokud Zhotovitel neodstraní záruční vady ve sjednané době od jejich oznámení Objednatelem Zhotoviteli, je Objednatel oprávněn podle vlastního uvážení vadu buď sám odstranit, nebo pověřit jejím odstraněním třetí osobu.

Čl. XI
Prodlení, sankce

1. Jestliže je Objednatel v prodlení s plněním povinnosti podle této smlouvy, je Zhotovitel oprávněn vyúčtovat Objednateli smluvní pokutu ve výši 0,05% z celkové ceny díla za každý i započatý den prodlení. Smluvní pokuta je splatná vždy k poslednímu dni příslušného kalendářního měsíce. Uplatněním smluvní pokuty není dotčeno právo Zhotovitele na náhradu újmy.
2. V případě, že je Zhotovitel v prodlení s plněním povinností podle této smlouvy, je Objednatel oprávněn vyúčtovat a Zhotovitel povinen zaplatit smluvní pokutu ve výši 0,05% z celkové ceny díla započatý den prodlení. Smluvní pokuta je splatná vždy k poslednímu dni příslušného kalendářního měsíce.
3. Zhotovitel odpovídá za veškeré škody a nemajetkové újmy, které vzniknou Objednateli v důsledku porušení této smlouvy Zhotovitelem. Zhotovitel je povinen nahradit takto vzniklou škodu a nemajetkovou újmu v plném rozsahu, včetně případných sankcí udělených Objednateli orgány veřejné moci, jejichž příčinou bylo porušení povinností Zhotovitele dle této smlouvy.

Čl. XI
Platnost a změna smlouvy

1. Tato smlouva nabývá platnosti dnem podpisu a účinnosti dnem zveřejnění v informačním systému veřejné správy – Registru smluv. Smluvní strany se dohodly, že smlouvu v Registru smluv zveřejní Objednatel.
2. Platnost smlouvy lze ukončit písemnou dohodou podepsanou oprávněnými zástupci obou smluvních stran.
3. Obsah Smlouvy může být měněn jen dohodou stran smluvních, a to vždy jen vzestupně číslovanými písemnými dodatky podepsanými oprávněnými osobami smluvních stran.
4. Kterákoliv ze smluvních stran je oprávněna tuto smlouvu vypovědět, a to bez udání důvodů. Výpovědní doba činí 2 měsíce a začíná běžet první den měsíce následujícího po prokazatelném doručení výpovědi druhé smluvní straně.

5. Objednatel má právo vypovědět tuto smlouvu v případě, že v souvislosti s plněním účelu této smlouvy dojde ke spáchání trestného činu. Výpovědní doba činí 3 dny a začíná běžet dnem následujícím po dni, kdy bylo písemné vyhotovení výpovědi doručeno Zhotoviteli.

Čl. XII
Bezpečnostní ustanovení

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 subdodavatelů či jiných osob, které mají přístup k informačním aktivům Objednatele prostřednictvím dodavatele.
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 20.000,- Kč, a to za každé jednotlivé porušení povinností obsažených v tomto článku. Celková smluvní pokuta nesmí převýšit celkovou cenu za dílo.

Čl. XIII
Závěrečná ustanovení

1. Výběr Prodávajícího byl proveden v souladu s Pravidly Rady Kraje Vysočina pro zadávání veřejných zakázek ze dne 29. 6. 2021.
2. Zhotovitel prohlašuje, že se před uzavřením smlouvy nedopustil v souvislosti se zadávacím řízením sám nebo prostřednictvím jiné osoby žádného jednání, jež by odporovalo zákonu nebo dobrým mravům nebo by zákon obcházelo, zejména že nenabízel žádné výhody osobám podílejícím se na zadání veřejné zakázky, na kterou s ním kupující uzavřel smlouvu, a že se zejména ve vztahu k ostatním uchazečům nedopustil žádného jednání narušujícího hospodářskou soutěž.
3. 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 zákona č. 106/1999 Sb., o svobodném přístupu k informacím, ve znění pozdějších předpisů.
4. Vztahy smluvních stran touto smlouvou blíže neupravené se řídí příslušnými ustanoveními občanského zákoníku s přihlédnutím k příslušným ustanovením autorského zákona.
5. Smlouva se vyhotovuje ve dvou stejnopisech s platností originálu, z nichž každá smluvní strana obdrží po jednom. V případě, že bude smlouva podepisována elektronicky, každá

smluvní strana obdrží elektronický dokument s kvalifikovanými elektronickými podpisy obou smluvních stran v souladu se zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů.

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, vyjma částí, které jsou označeny jako obchodní tajemství.
7. Nedílnou součástí této smlouvy je:

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

   Příloha č. 2 - Specifikace a kalkulace ceny
8. Smluvní strany prohlašují, že Přílohu č. 2 smlouvy považují za obchodní tajemství dle § 504 zákona č. 89/2012 Sb., občanský zákoník ve znění pozdějších předpisů
9. Smluvní strany prohlašují, že si tuto smlouvu před jejím podpisem přečetly, s jejím obsahem souhlasí, že smlouva je v souladu s jejich svobodnou vůlí a smlouvu nepodepisují v tísni a za nápadně nevýhodných podmínek. Na důkaz toho připojují své podpisy.

V Jihlavě dne .....

Digitálně podepsal Ing. Jaromír Řezáč
Datum: 2023.11.07 20:58:42 +01'00'

Za Zhotovitele
Ing. Jaromír Řezáč

V Jihlavě dne .....

RNDr. Jan Bříždala

Digitálně podepsal RNDr. Jan Bříždala
Datum: 2023.11.13 08:54:47 +01'00'

Za Objednatele
RNDr. Jan Bříždala

Kraj Vysočina

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

- Bezpečnost přístupových oprávnění
  - Zhotovitel je povinen chránit veškeré přístupové údaje k informačním aktivům objednatele včetně přístupů k informačním aktivům Zhotovitele, které umožňují přístup k informačním aktivům objednatele či umožnují jejich správu.
  - Zhotovitel 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.
  - Zhotovitel 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 Zhotovitel zřizoval přístupová oprávnění třetí straně, je Zhotovitel povinen o této skutečnosti informovat objednatele. Objednatel má v tomto případě právo zřízení přístupu zamítnout.

- Řízení rizik
  - Objednatel si vyhrazuje právo na informace o tom, jakým způsobem Zhotovitel řídí rizika informační bezpečnosti, 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.
  - Zhotovitel 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:
  - Zhotovitel 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.
  - Zhotovitel je dále povinen poskytnout adekvátní součinnost při řešení kybernetických bezpečnostních incidentů a při forenzní analýze incidentů souvisejících s informačními aktivy Objednatele.

- Kryptografie:

Pokud budou v souvislosti s plněním této smlouvy použity kryptografické funkce, algoritmy či metody, je Zhotovitel povinen řídit se těmito požadavky:

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:
  - Argon2 s parametry alespoň t=1, m=221, p=4 a funkcí Argon2id
  - scrypt s parametry alespoň N=32768 (215), r=8, a p=1
  - PBKDF2 s počtem iterací alespoň 100 000 a schválenou hašovací funkcí SHA-2 (viz níže)
- 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 (SHA-256, SHA-384, SHA-512, SHA-512/256) a SHA-3 (SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)
- délka otisku 384 bitů a vyšší

Ověřování integrity souborů

- SHA-2 (SHA-256, SHA-384, SHA-512, SHA-512/256) a SHA-3 (SHA3-256, SHA3-384, SHA3-512, SHAKE128, SHAKE256)
- délka otisku 384 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) - 3072 bitů
      - 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 - 3072 bitů
      - DSA – 3072 bitů
      - 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

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 půjde)
  - algoritmus RSA - 2048 bitů (postupně přecházet na 3072 bitů, tam kde to půjde)
  - 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 půjde)
  - 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