Český rozhlas

ICZ 966641 / 1

DÍLČÍ SMLOUVA O DÍLO č. 1

k rámcové dohodě o dílo s jedním účastníkem ze dne **17.10.2024**

Český rozhlas
zřízený zákonem č. 484/1991 Sb., o Českém rozhlasu
nezapisuje se do obchodního rejstříku
se sídlem Vinohradská 12, 120 99 Praha 2
zastoupený: Mgr. Renémem Zavoralem, generálním ředitelem
IČO 45245053, DIČ CZ45245053
bankovní spojení: Raiffeisenbank a.s., číslo účtu: 1001040797/5500
zástupce pro věcná jednání [redacted]

(dále jen jako „**objednatel**“)

a

ICZ a.s.
zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, oddíl B, vložka 4840
se sídlem Na hřebenech II 1718/10, Nusle, 140 00 Praha 4
zastoupená: [redacted] na základě plné moci
IČO 25145444, DIC CZ699000372
bankovní spojení: UniCredit Bank Czech Republic and Slovakia, a.s., číslo účtu: 2109164825/2700
zástupce pro věcná jednání [redacted]

(dále jen jako „**zhotovitel**“)

uzavírají v souladu s ustanovením § 2586 a násl. zákona č. 89/2012 Sb., občanský zákoník, ve znění pozdějších předpisů (dále jen „**OZ**“) a v souladu s článkem II. rámcové dohody o dílo s jedním účastníkem ze dne **17.10.2024** (dále jen „**rámcová dohoda**“) tuto dílčí smlouvu o dílo (dále jen jako „**smlouva**“)

I. Předmět smlouvy

1. Předmětem této smlouvy je povinnost zhotovitele na svůj náklad a nebezpečí pro objednatele následující dílo: **zajištění implementace systému pro vícefaktorové ověřování včetně poskytování služeb s tím souvisejících**, blíže specifikované v příloze smlouvy, to vše dle podmínek stanovených v této smlouvě (dále také jen „**dílo**“), umožnit objednateli nabýt vlastnické právo k dílu na straně jedné a povinnost objednatele dílo převzít a zaplatit zhotoviteli cenu na straně druhé.

2. V případě, že je zhotovitel dle specifikace díla povinen, v rámci své povinnosti provádět dílo, dodat objednateli jakékoliv zboží považováno za součást díla, bez jehož dodání není možné

dílo považovat za řádně dokončené. Hodnota takového zboží, jakož i náklady na jeho dodání, jsou zahrnuty v ceně díla.

3. Zhotovitel je povinen objednateli dílo odevzdat včetně veškeré dokumentace, která je nezbytná k tomu, aby dílo mohlo sloužit svému účelu.

II. Místo a doba plnění

1. Pokud se smluvní strany nedohodly písemně jinak, místem provádění a odevzdání díla je **Český rozhlas, Vinohradská 12, 120 99 Praha 2**.

2. Zhotovitel se zavazuje odevzdat dílo v místě odevzdání díla na vlastní náklad a nebezpečí nejpozději do **3 měsíců ode dne účinnosti této smlouvy**. Na přesném datu započetí provádění díla a jeho způsobu je zhotovitel povinen se předem písemně dohodnout s objednatelem.

III. Cena služeb

1. Cena díla je určena v souladu s rámcovou dohodou a činí **5.653.184,- Kč bez DPH**. Cena s DPH činí 6.840.352,64 Kč. Platební podmínky jsou sjednány v souladu s rámcovou dohodou. Způsob výpočtu ceny díla je uveden v příloze této smlouvy.

2. Celková cena dle předchozího odstavce je konečná a zahrnuje veškeré náklady zhotovitele související s prováděním díla dle této smlouvy (např. doprava materiálu a zboží nutných k provedení díla, navrácení místa provádění díla do původního stavu, náklady na likvidaci vzniklých odpadů, cla a jiné poplatky, a další náklady nezbytné k řádnému provedení díla).

IV. Závěrečná ustanovení

1. Tato smlouva nabývá platnosti dnem jejího podpisu oběma smluvními stranami a účinnosti dnem jejího uveřejnění v registru smluv v souladu se zákonem č. 340/2015 Sb., o zvláštních podmínkách účinnosti některých smluv, uveřejňování těchto smluv a o registru smluv (zákon o registru smluv), ve znění pozdějších předpisů. Uveřejnění smlouvy v registru smluv zajistí objednatel.

2. Smluvní strany výslovně sjednávají, že právem rozhodným pro tuto smlouvu je právo České republiky. Práva a povinnosti smluvních stran touto smlouvou neupravená se řídí zejm. rámcovou dohodou a příslušnými ustanoveními OZ.

3. Bude-li v této smlouvě použit jakýkoli pojem, aniž by byl smlouvou zvlášť definován, potom bude mít význam, který mu dává rámcová dohoda.

4. Tato smlouva je vyhotovena ve třech stejnopisech s platností originálu, z nichž objednatel obdrží dva a zhotovitel jeden. V případě, že bude smlouva uzavřena na dálku za využití elektronických prostředků, zašle smluvní strana, jenž smlouvu podepisuje jako poslední, jeden originál smlouvy spolu s jejími přílohami druhé smluvní straně.

5. Nedílnou součástí této smlouvy je její:

   Příloha č. 1 - Specifikace díla a ceny.

V Praze dne elektronického podpisu	V Praze dne elektronického podpisu
[redacted]	[redacted]

PŘÍLOHA Č. 1 – SPECIFIKACE SLUŽEB A CENY

A. SPECIFIKACE SLUŽEB

Objednatel požaduje navýšení zabezpečení služeb MS Exchange následujícím způsobem:

Implementace systému pro vícefaktorové ověřování a dodávka hardware:

a. Hardwarového řešení systému, který bude zajišťovat funkce reverzní proxy, load balanceru a aplikační proxy pro řízení přístupu k aplikacím a službám – dále jen systém ADC (Application Delivery Controller). Tento systém ADC bude umístěn před vlastními servery MS Exchange a bude zajišťovat terminaci HTTPS provozu, autentizaci uživatelů a balancování provozu na cílové servery MS Exchange. Objednatel požaduje řešení, které bude provozované v režimu vysoké dostupnosti.

   V rámci dodávky objednatel požaduje, s ohledem na vysokou dostupnost systému ADC, dodat 2 kusy hardware zařízení ADC a to včetně 4 kusů SFP+ 10GBASE-SR Transceiverů.

   Pro zařízení požadujeme služby typu:

   - Podpora pro výměnu hardware v režimu Next-Business-Day minimálně 8x5,
   - Produktovou podporu od výrobce v režimu minimálně 8x5.

   Součástí dodávky předpokládáme dodání licence, pokud to je relevantní.
   Detailní popis požadavků na systém je uveden v kapitole č. 2.

   V tomto bodě dodávky **objednatel nepřipouští licenční model typu subskripce.**

b. systému poskytujícího funkci dalšího faktoru pro autentizaci uživatelů k současnému způsobu ověření uživatele jménem a heslem – dále jen systém MFA (Multi-Factor Authentication). Detailní popis je uveden v kapitole č. 3 této přílohy.
   Součástí dodávku předpokládáme dodání licence a produktové podpory, pokud to je relevantní.

   V tomto bodě dodávky **objednatel připouští licenční model typu subskripce.**

c. Rozšíření stávajícího webového samoobslužného systému ČRo (interní certifikační autorita ČRo) o vydávání konfiguračních profilů s certifikáty pro klientská zařízení Apple iOS

1. Požadavky na systém ADC

Objednatel požaduje vytvořit návrh, dodání a implementaci systému ADC ve formě hardwarové appliance (zařízení). Objednatel nepřipouští řešení provozované na virtualizační platformě nebo v cloudu. Systém ADC bude provozován v režimu vysoké dostupnosti – **dvojice hardware zařízení**. Systém ADC bude publikovat definované služby a oddělovat cílové on-premise MS Exchange servery od přistupujících uživatelů. Systém ADC bude realizovat funkci řízení aplikačního provozu a musí splňovat požadavky uvedené v tabulce č. 1 (Tabulka technických parametrů systému ADC.) této přílohy .

1.1 Reverzní proxy a load balancer

Systém ADC bude koncipován jako redundantní a vysoce dostupný cluster, který může fungovat v režimu Active-Active nebo Active-Standby. Systém ADC bude odpovědný za monitoring, řízení a distribuci zátěže na cílové servery MS Exchange. Systém ADC bude také zajišťovat optimalizaci aplikačního provozu s cílem efektivně využívat zdroje aplikace. Systém ADC bude také zodpovědný za optimalizaci TCP provozu, HTTP kompresi a související optimalizaci aplikačního provozu. Systém bude umožňovat provoz alespoň dvou virtuálních ADC na jednom fyzickém zařízení, kdy jeden virtuální ADC bude sloužit pro odbavování provozu v externí DMZ a druhý ADC bude sloužit pro provoz ve vnitřní síti.
Implementaci politik a pravidel pro řízení aplikačního provozu předpokládáme minimálně v rozsahu:

— Zapojení a integrace v prostředí objednatele
— Vytvoření HA clusteru
— Monitoring zdraví aplikací a služeb

- TLS terminace, management TLS certifikátů
- Napojení na monitorovací a logovací nástroje
- Reverzní proxy s funkcí NAT44, případně NAT 46, NAT 64
- Optimalizace HTTP provozu (HTTP komprese)
- Zabezpečení HTTP provozu (cookies, manipulace s HTTP záhlavím apod.)

1.2 Aplikační proxy pro řízení přístupu k aplikacím

Pro každý přístup k poštovní schránce ČRo z intranetu nebo prostřednictvím VPN bude vyžadováno pouze ověření uživatelským jménem a heslem. Naopak z internetu bude vyžadována jedna ze dvou doplňkových metod ověření a autorizace uživatelů využívající další faktor – MFA.
Popis požadovaného způsobu řízení přístupu k jednotlivým službám MS Exchange je uveden dále.

1.2.1 Řízení přístupu ke službě OWA

Při přihlášení uživatele z internetu webovým protokolem OWA proběhne v první fázi ověření uživatele jménem a heslem proti on-premise Active Directory objednatele, které zprostředkuje systém ADC. Jakmile uživatel projde úspěšně touto první kontrolou, systém ADC zprostředkuje ověření dalším faktorem (MFA autentizaci), kdy kontaktuje příslušnou službu MFA systému, která pro ověřovaného uživatele zašle push notifikaci na příslušné registrované mobilní zařízení s nainstalovanou autorizační aplikací MFA systému. Po schválení přihlášení prostřednictvím autorizační aplikace MFA systému na obrazovce mobilního zařízení uživatele, zajistí ADC balancování a šifrování provozu na cílové servery MS Exchange a předání přihlašovacích údajů prostřednictvím SSO (Single Sign On).
Pokud uživatel projde úspěšně celým ověřovacím procesem na ADC, bude provoz následně balancován na cílové MS Exchange servery, které uživateli zobrazí obsah poštovní schránky. Pokud ale v libovolné fázi ověřovacího procesu dojde k chybě nebo zadání nesprávných údajů, provoz nebude propuštěn na cílové Exchange servery a zobrazí se text s důvodem selhání a stručným popisem příčiny.

1.2.2 Řízení přístupu k ostatním službám MS Exchange

Pro přihlášení z internetu prostřednictvím zbývajících protokolů MS Exchange (EWS, EAS, MAPI) z internetu bude v rámci TLS handshake výměny vyžadována autentizace osobním klientským certifikátem přihlašovaného uživatele, která v tomto případě představuje další faktor ověření koncového uživatele/zařízení a bude zprostředkováno ADC systémem. V případě úspěšného sestavení TLS spojení bude následovat ověření jménem a heslem proti on-premise Active Directory objednatele, opět zprostředkované ADC systémem. V případě úspěšné autentizace bude uživateli povoleno spojení protokolem EWS, EAS nebo MAPI s poštovními servery MS Exchange Českého rozhlasu. ADC systém opět zajistí balancování a šifrování provozu na cílové servery MS Exchange a předání přihlašovacích údajů prostřednictvím SSO (Single Sign On)
V opačném případě ke spojení klientské poštovní aplikace s poštovními servery MS Exchange Českého rozhlasu nedojde.

1.3 Další požadavky na dodávané ADC řešení

Požadované řešení musí poskytovat služby reverzní proxy, load balanceru a aplikační proxy s dostatečným výkonem pro zajištění provozu stávajících i budoucích služeb a aplikací objednatele. Kromě toho musí systém ADC podporovat rozšíření o další funkce na základě dokoupení příslušné licence. Zejména se jedná o funkce webového aplikačního firewallu.

2. Systém MFA

Objednatel požaduje návrh, dodání a implementaci systému MFA, který musí podporovat přímou integraci se systémem ADC prostřednictvím protokolů SAML nebo OAUTH.

Dále musí kromě jiného umožňovat distribuci a instalaci autorizační aplikace MFA systému na mobilní zařízení ověřovaných uživatelů a jejich propojení (registraci) se službou MFA systému. Je požadováno, aby průvodci zajišťující distribuci, instalaci a registraci používali jazykovou lokalizaci dle jazykového nastavení webového prohlížeče. MFA systém musí podporovat správu jednotlivých

uživatelských účtů a k nim přiřazených mobilních zařízení a synchronizaci uživatelských účtů s on-premise službou Active Directory objednatele.

V případě využití cloudového prostředí pro zajištění MFA je pro zajištění funkcionality ověřovacího mechanismu povoleno v cloudovém prostředí poskytovatele služby MFA systému využívat z on-premise Active Directory objednatele pouze tyto položky: přihlašovací jméno a email uživatele, jméno a příjmení uživatele a telefonní číslo mobilního zařízení uživatele. Jiné položky z Active Directory objednatele ani samotný obsah poštovní komunikace nebude povoleno zpracovávat na zařízeních poskytovatele mimo prostor budov Českého rozhlasu.

Webová aplikace pro správu i autorizační aplikace pro mobilní zařízení, které budou součástí MFA systému, musí splňovat požadavky na standardizované unifikované řešení již ověřené a užívané v celosvětovém měřítku. Objednatel nepřipouští softwarové či aplikační řešení šité na míru.

Pokud u uživatele dojde k výměně mobilního zařízení za jiné, bude mít možnost samoobslužně takovou záměnu bezpečně provádět výhradně prostřednictvím zaslání SMS s údaji pro instalaci autorizační aplikace MFA systému a její propojení s autorizačními servery MFA systému na nové mobilní zařízení.

Dodaný systém MFA bude licencován na počet uživatelských účtů. Požadujeme licence pro 2000 ks uživatelů.

Systém MFA bude realizovat funkci vícenásobného ověření uživatele pomocí dalších faktorů a musí splňovat požadavky uvedené v kapitole 3 a tabulce č. 2 (Tabulka technických parametrů systému MFA) v této přílohy.

2.1 Další požadavky na dodávané MFA řešení

Objednatel v současné době provozuje intranetovou webovou aplikaci pki.rozhlas.cz, která je používána k automatizovanému vydávání klientských certifikátů interní certifikační autority, založené na Microsoft Active Directory Certificate Services. Po ověření uživatelského jména a hesla zajistí tato Samoobsluha vydání klientského certifikátu podle předem schválené šablony certifikátu. Objednatel požaduje rozšíření stávající aplikace o funkcionalitu, která vedle klientských certifikátů umožní přihlášenému uživateli také dynamické vytvoření a stažení jeho osobního konfiguračního profilu pro zařízení s Apple iOS. Tento profil bude obsahovat konfiguraci pro zpřístupnění systému Microsoft Exchange v síti objednatele, upravenou přesně pro potřeby příslušného koncového uživatele (předem vyplněné uživatelské jméno, adresy server MS Exchange a kompletní sadu certifikátů, včetně osobního certifikátu).

3. Specifikace implementačního procesu a požadovaných produktů a výstupů

1. Zhotovitel zpracuje na základě analytických schůzek dokument Analýza nasazení systémů ADC a MFA, jehož obsah bude následující:
   - Návrh a obecný popis architektury (High Level Design) dodávaného řešení,
   - popis terminologie, použité v dokumentu,
   - informace o stávajícím prostředí objednatele,
   - seznam aplikací, které budou ADC využívat,
   - popis změn v infrastruktuře.
2. Zhotovitel zpracuje na základě analytických schůzek dokument Funkční specifikace, jehož obsah bude následující:
   - Vymezení rozsahu řešení,
   - popis funkčních vlastností požadovaného řízení přístupu k aplikacím pomocí systémů ADC a MFA,
   - popis úprav existujícího IT prostředí objednatele,
   - schéma řešení včetně integrace do prostředí objednatele,
   - popis cílové úpravy vnitřních procesů.
3. Zhotovitel zpracuje dokument Low Level Design s následujícím obsahem:

- Celkový návrh řešení ADC.
- Typizované konfigurační šablony (soubor pravidel) pro řízení aplikačního provozu.
- Jmennou konvenci pro ADC řešení.
- Konfigurace ADC clusteru.
- Konfigurace politik řízení aplikačního provozu pro aplikace.
- Vytvoření a implementace standardů (soubor pravidel) pro SSL terminaci.
- Vytvoření a implementace standardů (soubor pravidel) pro monitoring aplikací.
- Vytvoření a implementace standardů (soubor pravidel) pro manipulaci s HTTP provozem (vkládání/odebíraní HTTP záhlaví apod.).
- Vytvoření a implementace standardů pro optimalizaci TCP a HTTP provozu.
- Konfigurace ostatních aspektů bezpečnostní politiky dle funkční specifikace.
- Konfigurace MFA služby a integrace s řešením ADC.
- Konfigurace politik pro řízení přístupu k aplikacím.
- Konfigurace politik MFA služby.
- Konfigurace synchronizace uživatelských účtů mezi MFA službou a on-premise Active Directory objednatele.
- Customizace autentizačního procesu.
- Konfigurace spolupracujících systémů (Active Directory, logovací systém, monitoring a další).
- Doplnění funkcionality aplikace pki.rozhlas.cz.

4. Zhotovitel připraví podrobné akceptační testy ADC a MFA systému včetně scénářů pro otestování vysoké dostupnosti.
5. Zhotovitel provede pod dohledem objednatele akceptační testy ADC a MFA systému.
6. Zhotovitel zpracuje Dokumentaci skutečného provedení, která bude obsahovat popis finálního nastavení jednotlivých komponent řešení a procesů.

1. Tabulka technických parametrů systému ADC

Požadovaná funkcionalita/vlastnost	**Detailní popis naplnění pro nabízené řešení, případně odkaz na dokumentaci**
Platforma	
Nasazení redundantních HW zařízení ve funkci load-balancer s podporou autentizace uživatelů, SSL akcelerátoru a webového aplikačního firewallu.	2x fyzická appliance F5 BigIP R4600
Každé zařízení podporuje připojení minimálně 4 x 25/10 Gbps optickými SFP+ a 4x 10/1 Gbps metalickými porty.	4x 25G/10G/1G SFP+/SFP28/SFP, 4 x 10G/1G RJ45
Datová propustnost zařízení alespoň 40 Gbps či více na L4 a 28 Gbps či více na L7	40 Gbps na L4, 30 Gbps na L7
Minimální propustnost HTTP požadavků: 2.3 mil.za sekundu	2.5 mil. L4 HTTP requestů za sekundu
Minimální propustnost L7 požadavků: 1.1 mil. za sekundu	1.3 mil. L7 HTTP requestů za sekundu
Počet současných L4 spojení: 36 mil.	38 mil.
Offload – SW komprese – propustnost min. 18 Gbps	20 Gbps
SSL akcelerace v HW	ANO
Počet SSL transakcí za sekundu min. 28000 (při použití 2K klíče)	30K TPS (2K SSL TPS)

Počet SSL transakcí za sekundu min. 12000 (při použití ECDSA P-256 klíče)	14K TPS (ECDHE-ECDSA P-256 TPS), 14K TPS (ECDHE P-256-RSA 2k TPS)
Celkový šifrovací výkon 18 Gbps	20 Gbps bulk encryption
Virtualizace HW zdrojů	ANO, až 2 tenanty
Nezávislé rozhraní pro management	ANO
HW podpora následujících funkcí: - SYN Cookie ochrana pro každou virtualizovanou službu - Základní DoS vektory, s možností nastavení každou virtualizovanou službu - SIP a DNS DoS vektory	ANO
Redundantní napájení	ANO
K dispozici jako autonomní box nebo ve formě šasi	ANO
Management: sériový port, GUI, příkazový řádek, iLO	Sériový port, GUI, CLI, dedikovaný management port
Operační systém	
Full-Proxy architektura (plné oddělení klientského a serverového spojení)	ANO
Podpora IPv4	ANO
Plná podpora IPv6, IPv4/IPv6 gateway (Podpora Ipv4 a Ipv6 na straně klienta i na straně serveru včetně všech možných kombinací)	ANO
Podpora externích šifrovacích karet pro SSL (HSM)	Podpora nCipher/Entrust, Safenet, Atos, Equinix, Amazon
Podpora ověření certifikátů vydaných podřízenou CA (intermediate CA)	ANO
Podpora Spanning Tree Protokolu (STP)	ANO
Možnost přidat vlastní funkce pomocí skriptování – umožnění plnohodnotné manipulace a správy veškerého IP aplikačního provozu s cílem zachytit, zkontrolovat, transformovat a nasměrovat příchozí nebo odchozí provoz pomocí skriptovacího jazyka/syntaxe.	ANO
Podpora HTTP/2	ANO
Podpora IPSec IKEv2	ANO
Podpora konfigurace a správu zařízení přes REST API	ANO
Podpora SNMP (v1/v2c/v3)	ANO
Možnost aktivovat následující funkce na jedné HW platformě: - L4-7 loadbalancing - ICSA certifikovaný Web aplikační firewall - ICSA certifikovaný síťový firewall - Autorizace a autentizace aplikací, SSL VPN - DNS služby a DNS firewall	ANO
Možnost používat knihovny JavaScript třetích stran k úpravě a správě provozu	ANO
Podpora Active-Active a Active-Pasive módu	ANO

Režim HA, cluster: - Active/active, active/passive, transparentní přepínání bez přerušení session, včetně terminovaného SSL spojení. - Možnost zařadit do HA clusteru min. 3 zařízení. Jednotlivá zařízení mohou být různých HW typů, nebo jako virtuální appliance. - Pokud jsou vyžadovány dodatečné licence, tak musí být součástí nabídky.	ANO
Řízení provozu (load balancing)	
Možnost připojení k monitorovacím nástrojům třetích stran prostřednictvím otevřeného API	ANO
Podpora REST API	ANO
Autentizace klientů přes LDAP/Radius	ANO
Povolení/zakázání ICMP pro VIP	ANO
Podpora vysokorychlostního granulárního logování / logování per aplikace / bez omezení výkonnosti zařízení	ANO
Podpora alespoň pro 19 metod rozvažování zátěže	ANO - Round Robin, Ratio (member), Least Connections (member), Observed (member), Predictive (member), Ratio (node), Least Connections (node), Fastest (node), Observed (node), Predictive (node), Dynamic Ratio (node), Fastest (application), Least Sessions, Dynamic Ratio (member), Weighted Least Connections (member), Weighted Least Connections (node), Ratio (session), Ratio Least Connections (member), Ratio Least Connections (node)
Podpora filtrace paketů	ANO
Podpora ToS, QoS (marking/preservation/mimic)	ANO
Podpora SNMP (v1/v2c/v3)	ANO
Podpora rozvažování zátěže založené na poměrech (ratio) s CARP perzistencí	ANO
Podpora SSL certifikátů podepsaných SHA-2 algoritmem	ANO
Podpora práce s 4096-bit klíči	ANO
Současná podpora ECC a RSA certifikátu	ANO
Podpora pro TLS 1.2 a TLS 1.3	ANO
Podpora ECC a DH šifer v HW	ANO
Podpora SSL Forward proxy	ANO
Stavové filtrovaní paketů (ACL)	ANO
Podpora vlastních skriptů pro monitorování zdraví a dostupnosti služeb	ANO

Podpora monitorování služeb na základě výkonu konkrétních hostů	ANO
TCP optimalizace síťových toků	ANO
Komprese a cachování specifických služeb	ANO
Zrcadlení SSL spojení (“connection”) a relací (“session”) napříč vícero uzly loadbalancerů – v případě výpadku jednoho zařízení si SSL spojení/relaci přebírá druhý uzel a SSL komunikace je zachována.	ANO
Podpora optimalizace dynamické velikosti TLS bloků (TLS record size)	ANO
Řízení uživatelských přístupů	
Podpora těchto autentizačních protokolů: - HTTTP basic - HTML form - Certificate - OCSP - CRLDP - Radius - LDAP - Active Directory - NTLM v1/v2 - Kerberos - SAML - SecurID - OAM - Tacacs+ - Local DB	ANO
Podpora Zero Trust konceptu	ANO
Import uživatelských identit IF-MAP	ANO
Podpora pro External logon page	ANO
AAA-server autentizace a vysoká dostupnost	ANO
OTP (generování a ověření)	ANO
Podpora CAPTCHA	ANO
Podpora Google recaptcha v2	ANO
Autorizace: - Radius - LDAP - Active Directory	ANO
SAML: - SP - IdP	ANO
Modifikace SAML atributů	ANO
Podpora SAML 2.0	ANO
SSO: - HTTP basic	ANO

- HTML form - NTLM v1/v2 - Kerberos - SAML	
Cachování uživatelských identit a SSO proxy	ANO
Podpora federace (SSO napříč různými doménami, např. on-prem a SaaS)	ANO
Podpora for Kerberos ticketingu	ANO
PCoIP proxy	ANO
RDP proxy	ANO
Patching: - HTML - JavaScript - CSS - Flash - Java	ANO
Jednotný URL portál	ANO
Uživatelský portál, kde se zobrazují aplikace podle přístupových práv	ANO
Podpora L7 ACL	ANO
Dynamický import ACL	ANO
Dynamická kontrola přístupů	ANO
Podpora ochrany a enkrypce „pracovniho“ prostoru („workspace“)	ANO
Network SSL VPN DTLS	ANO
Separátní SSL VPN tunel pro každou přístupnou aplikaci	ANO
Přístup pomocí Client-less	ANO
OS support: - Windows - MAC - Linux - iOS - Android	ANO
Podpora nativní MDM	ANO
Podpora Oauth 2.0	ANO
Podpora OpenID Connect	ANO
Podpora IPSEC IKE v2	ANO
Kontrola zabezpečení koncových bodů a posture kontrol	ANO
Podpora L7 ACL pro uživatelský přístup	ANO
Grafický editor pro správu řízení uživatelských přístupů	ANO
Podpora Microsoft ActiveSync a Outlook Anywhere s client-side NTLM	ANO
Zjednodušené řízení uživatelských přístupů pro Citrix XenApp a XenDesktop	ANO

Step-up autentizace	ANO
Podpora Ping Identity's Policy Agent protocol	ANO
Podpora forward proxy chaining	ANO
Schopnost integrace se systémy AAA třetích stran pomocí volání API	ANO
Podpora ADFS proxy a ADFS-PIP protokolu	ANO

2. Tabulka technických parametrů systému MFA

Požadovaná funkcionalita/vlastnost	Popis naplnění pro nabízené řešení, případně odkaz na dokumentaci
Autentizace a enrollment	
Podpora registrace více mobilních zařízení pro ověření uživatele	ANO
Podpora výběru preferovaného mobilního zařízení pro ověření uživatele	ANO
Podpora výběru alternativního mobilního zařízení (registrovaného danému uživateli), pokud není k dispozici jeho primární mobilní zařízení	ANO
Podpora ověření pomocí push notikace zaslané na mobilní zařízení	ANO
Push notifikace používají asymetrické klíče	ANO
Podpora ověření pomocí SMS zaslané na mobilní zařízení	ANO
Podpora mobilní zařízení těchto platforem: - iOS - Android	ANO
Podpor ověření pomocí hardwarových tokenů - tokeny Yubikeys - tokeny třetích stran kompatibilní se SAML / OAUTH	ANO
Podpora ověření pomocí jednorázového hesla (OTP) generovaného z mobilní aplikace	ANO
Podpora ověření pomocí bypass kódu poskytnutého administrátorem pro nouzové případy, kdy uživatel nemůže pro ověření použít své registrované mobilní zařízení	ANO
Podpora provisioning mobilní aplikace pomocí - SMS - QR kódu	ANO
Podpora IP whitelistingu pro jednotlivé uživatele, uživatelské skupiny nebo chráněné aplikace	ANO
Podpora IP whitelistingu v definovaných časových oknech	ANO
Podpora těchto autentizačních metod: - platform authenticator (Touch ID, Face ID, Android biometric) - roaming authenticator (FIDO security klíče – USB, Bluetooth, NFC) - push notifikace s verifikačním kódem - OTP v mobilní aplikaci - OTP přes SMS - phone callback - SAML / OAUTH hardwarové tokeny	ANO
Možnost vytváření vlastních konfigurovatelných politik pro blokování/upozornění na neaktuální software webového prohlížeče a poskytují možnost self-remediace	ANO

Možnost vytváření vlastních konfigurovatelných politik pro blokování nebo vyžadování vyšší úroveň ověření podle geolokace uživatele	ANO
Možnost vytváření vlastních konfigurovatelných politik pro blokování uživatelů s jailbroken/rooted mobilními zařízeními	ANO
Možnost vytváření vlastních konfigurovatelných politik pro zabránění pokusů o přístup z anonymních IP adres (TOR a I2P, HTTP/HTTPS proxy nebo anonymní VPN)	ANO
Možnost vytváření vlastních konfigurovatelných politik, které vyžadují aktivní zámek obrazovky na mobilních zařízeních při schvalování ověřování na těchto zařízeních	ANO
Možnost vytváření vlastních konfigurovatelných politik, které vyžadují použití otisku prstu/TouchID ověření na mobilních zařízeních při schvalování ověřování na těchto zařízeních	ANO
Možnost vytváření vlastních konfigurovatelných politik, které vyžadují plné šifrování disku na mobilních zařízeních při schvalování ověřování na těchto zařízeních	ANO
Možnost vytváření vlastních konfigurovatelných politik, které vyžadují aplikované aktuální bezpečnostní záplaty ověřovací aplikace na mobilních zařízeních při schvalování ověřování na těchto zařízeních	ANO
Možnost vytváření vlastních konfigurovatelných politik, které omezují dostupné metody ověřování	ANO
Administrace	
Výrobce garantuje SLA pro nabízené řešení	ANO
Zabezpečení a architektura řešení má audit od nezávislých třetích stran	ANO
Řešení založené na SaaS	ANO
Řešení je hostováno u poskytovatele služeb s certifikací PCI DSS, ISO 27001 a auditovaného podle SSAE 16	ANO
Škálovatelné řešení z pohledu integrace s dalšími výrobci a počtu uživatelů	ANO
Řešení navržené s vysokou dostupností (HA) v rámci několika geografických lokalit a poskytovatelů služeb	ANO
Řešení používá asymetrickou kryptografii pro ověřování	ANO
Řešení neshromažďuje jakékoliv informace o uživatelích využitelné pro jejich identifikaci.	ANO
Řešení je nezávislé na primárním způsobu ověření	ANO
Pro vlastní ověření řešení nevyžaduje jakékoli dedikované on-premise servery	ANO
Podpora přímé integrace se systémy ADC pomocí protokolů SAML / OAUTH	ANO
Podpora synchronizace kontaktů s Microsoft Active Directory prostřednictvím LDAP protokolu	ANO

B. SPECIFIKACE CENY

1. Specifikace ceny dodávek, implementačních činností je uvedena v následující tabulce:

Dodání hardware systému ADC (Application Delivery Controller)	**Počet**	**Cena za položku bez DPH**	**Cena celkem bez DPH**
Dodávka 2 kusů hardware komponentního systému ADC F5 BIG-IP r4600 + APM module	2	932.467,- Kč	1.864.934,- Kč
Produktová podpora výrobce dodávaného řešení min. v režimu Next-Business-Day HW replacement	1	931.650,- Kč	931.650,- Kč
Celková cena v Kč bez DPH			**2.796.584,- Kč**

Dodání systému MFA	**Počet [kusů /počet]**	**Cena za položku bez DPH**	**Cena celkem bez DPH**
Systém MFA Cisco DUO pro 2000 uživatelských licencí na dobu 36 měsíců	2000	1.176,- Kč	2.352.000,- Kč
Celková cena v Kč bez DPH			**2.352.000,- Kč**

Implementační činnosti	**Cena celkem bez DPH**
Implementace systému ADC	174.000,- Kč
Implementace systému MFA	69.600,- Kč
Programové rozšíření stávajícího webového samoobslužného systému ČRo (interní certifikační autorita ČRo) o vydávání konfiguračních profilů s certifikáty pro klientská zařízení Apple iOS	261.000,- Kč
Celková cena v Kč bez DPH	**504.600,- Kč**

2. Harmonogram

Deteailní harmonogram jednotlivých plnění tj.dodávky a implementační činnosti budou upřesněny v rámci projektového týmu, který bude ustanovené po účinnosti této dílči smlouvy. Předání jednotlivých plnění podléhá protokolárnímu převzetí.

PLNÁ MOC

ICZ a.s., IČ: 25145444, se sídlem Na hřebenech II 1718/10, Nusle, 140 00 Praha 4, zapsaná v obchodním rejstříku vedeném Městským soudem v Praze, sp. zn. B 4840 (dále jen „**Zmocnitel**“)

tímto uděluje plnou moc

[redacted] (dále jen „**Zmocněnec**“),

aby za Zmocnitele činil veškerá právní jednání a jiné úkony **v obchodních vztazích** (včetně vztahů týkajících se veřejných zakázek ve smyslu ustanovení zákona č. 134/2016 Sb., zákon o zadávání veřejných zakázek, ve znění pozdějších předpisů), v nichž cena předmětu plnění vyjádřená peněžní částkou nepřesáhne částku **13.000.000,-Kč** (slovy třináct miliónů korun českých) s tím, že půjde-li o opakující se plnění, je základem pro výpočet tohoto limitu součet ceny všech opakujících se plnění bez DPH.

Tato plná moc nezahrnuje oprávnění Zmocněnce nakupovat a zcizovat cenné papíry, obchodní podíly, uzavírat smlouvy o prodeji části nebo celého podniku, zprostředkovatelské smlouvy, smlouvy o sdružení, smlouvy příkazní či mandátní, smlouvy nájemní, podnájemní či leasingové, přijímat a poskytovat úvěry, sjednávat odstupné, podepisovat směnky, zcizovat nemovitosti a zatěžovat je právními závazky. Zmocněnec dále není na základě této plné moci oprávněn zavazovat Zmocnitele jakýmikoli ručitelskými závazky.

Tato plná moc nahrazuje jakoukoli plnou moc dříve udělenou Zmocněnci Zmocnitelem ohledně výše uvedeného předmětu plné moci.

Tato plná moc se uděluje na dobu neurčitou.

V Praze dne 4 / 12 /2023

[redacted]

předseda představenstva
ICZ a.s.

PROHLÁŠENÍ O PRAVOSTI PODPISU

[redacted]

Zmocnění přijímám v plném rozsahu.

[redacted]

Doložka z konverze dokumentu do elektronické podoby – na žádost