

POŽADAVKY NA SPOLEČNÉ DATOVÉ PROSTŘEDÍ (CDE)

Přeložka silnice II/322 Černá za Bory – Dašice

verze ke dni zahájení řízení

OBSAH

1	Úvod	2
2	API CDE Objednatele	2
3	Systémové požadavky	2
4	Funkční požadavky	2
5	Adresářová struktura	4
6	Bezpečnostní požadavky	4
7	Další požadavky	5

Tento dokument byl zpracován s přihlédnutím k dokumentům vydaným Českou agenturou pro standardizaci v rámci Koncepce BIM, k SFDI Standardům a je v souladu s řadou norem ČSN EN ISO 19650:1-4.

1 ÚVOD

- 1.1.1 **Objednatel má vlastní CDE, v němž provozuje projekty.** Je upřednostňováno, aby si Zhotovitel zajistil přístup do Objednatelem používané aplikace, viz Příloha e.c) BIM Protokol,
- 1.1.2 V tomto dokumentu jsou uvedeny požadavky Objednatele na Společné datové prostředí (dále jen „CDE“), které vchází v platnost v případě, že si Zhotovitel zajistí své vlastní CDE.
- 1.1.3 Zhotovitel zajistí kompatibilitu mezi použitím CDE Zhotovitele a CDE Objednatele. Tato kompatibilita může být zajištěna prostřednictvím otevřeného API. Zhotovitelem zvolené CDE bude splňovat požadavky uvedené v tomto dokumentu.
- 1.1.4 Zhotovitel zajistí přístup osob Zhotovitele do systému CDE a použití systému CDE dle BIM Protokolu a jeho příloh.

2 API CDE OBJEDNATELE

- 2.1.1 API CDE Objednatele je k dispozici na webové adrese:
<https://suspceapi.digitalita.cz/swagger/index.html>

3 SYSTÉMOVÉ POŽADAVKY

- 3.1.1 Zhotovitel musí zajistit technickou podporu formou telefonické „hotline“ pro určené osoby Objednatele v českém jazyce v pracovní dny od 7:00 do 18:00 hodin.
- 3.1.2 Zhotovitel musí zajistit uživatelskou podporu (telefonicky/e-mailem) dostupnou všem uživatelům v pracovní dny od 9:00 do 16:00 hodin.
- 3.1.3 Zhotovitel zajistí nepřetržité propojení systémů skrze API na své náklady. V případě nefunkčnosti/nedostupnosti propojení, garantuje Zhotovitel jeho opětovné zprovoznění do 72 h od telefonického/e-mailového nahlášení nefunkčnosti/nedostupnosti systému Objednatelem.
- 3.1.4 Musí být použity takové technologie/principy, které zajistí požadovanou úroveň důvěrnosti, dostupnosti a integrity uchovávaných dat a informací.

4 FUNKČNÍ POŽADAVKY

- 4.1.1 Požadavky na jednotlivé funkce CDE:
 - (a) Stažení souborů a složek na úložiště mimo CDE.
 - (b) Revize souborů a složek.
 - (c) Integrované prohlížení souborů (formáty .pdf, .doc, .ifc, .xlsx a dalších běžně užívané formáty) a prohlížení nativních formátů.
 - (d) Integrované prohlížení Digitálního informačního modelu stavby (DiMS).

- (e) Systém CDE nesmí být omezen pro ukládání jen na určité formáty, ale musí umožňovat uložit jakýkoli vhodný, resp. relevantní formát souboru dokumentu v digitální podobě.
- (f) Správa jednotlivých verzí souborů, jejich přístupnost v rámci systému.
- (g) Tvorba vlastních pracovních postupů souvisejících se soubory.
- (h) CDE musí podporovat řešení pracovních postupů a procesů prostřednictvím workflow.
- (i) Notifikace na soubory.
- (j) Vyhledávání v datech, full-text u dokumentu ve formátu .doc, .xls a .pdf.
- (k) Filtrování, vhodná zobrazení dat v rámci aplikace filtru.
- (l) Audity souborů.
- (m) Správa uživatelských rolí a oprávnění uživatelů s různými úrovněmi přístupových oprávnění k celému BIM projektu a jeho jednotlivým složkám a pod složkám.
- (n) Práci se skupinami uživatelů a přiřazování oprávnění těmto skupinám uživatelů.
- (o) Definice a správa šablon workflow.
- (p) Vytváření úkolů přímo spojených s určitými místy v dokumentu (2D výkres / IFC model), jejich přiřazení konkrétním řešitelům, notifikace úkolů e-mailem.
- (q) Přístup externím uživatelům do vyhrazeného prostoru a k vyhrazeným složkám, popř. souborům.
- (r) Po ukončení provozu systém umožňuje export dat do adresářové struktury včetně logů, auditů a metadat.

- 4.1.2 Objednatel požaduje, aby CDE umožňovalo vytvoření odkazů na cesty (např. adresářové cesty, url, hypertextový odkaz, ...) směřujících na vybrané dokumenty v digitální podobě a umožňovalo tak propojení dat uložených v CDE s DiMS.

5 ADRESÁŘOVÁ STRUKTURA

- 5.1.1 Adresářová struktura bude předána Objednatelem na základě vyžádání BIM koordinátora Zhotovitele do 10 dní od jejího vyžádání. Adresářovou strukturu je povinen Zhotovitel dodržovat.

6 BEZPEČNOSTNÍ POŽADAVKY

- 6.1.1 Systém zaznamenává auditní logy a umožňuje zástupcům Objednatele přístup k těmto informacím, které musí zahrnovat všechny informace o úpravách všech uložených souborů a jejich metadat včetně informace, kdo se souborem manipuloval.
- 6.1.2 Systém zaznamenává logy obsahující přihlašování uživatelů a umožňuje zástupcům Objednatele přístup k těmto informacím, které musí zahrnovat zejména časové razítko, přihlašovací jméno a popis události.
- 6.1.3 Systém podporuje a vynucuje přístup přes šifrované spojení prostřednictvím webového prohlížeče (HTTPS) pro přístup k veškerým uloženým informacím. Použitý certifikát pro tento účel musí být podepsán důvěryhodnou kořenovou certifikační autoritou.
- 6.1.4 Pokud Zhotovitel Cloud Computingu (služby CDE), který poskytuje tuto službu v České republice, nemá sídlo v Evropské unii a neustavil si svého zástupce v jiném členském státě Evropské unie, musí mít ustanoveného svého zástupce v České republice. Zástupcem

Zhotovitele Cloud Computingu je osoba, která má sídlo v České republice a která je Zhotovitelem Cloud Computingu na základě plné moci zmocněná jej zastupovat.

- 6.1.5 Zhotovitel musí na základě žádosti Objednatele bez zbytečného odkladu zajistit přístup k informacím a datům, které Zhotovitel služby uchovává, včetně možnosti kontroly uchovávaných informací a dat v reálném čase.
- 6.1.6 Zhotovitel musí zajistit řízení kontinuity činností v souvislosti s poskytovanou službou.
- 6.1.7 V případě vyžádání Objednatele podepíše Zhotovitel dohodu o mlčenlivosti (NDA) týkající se prací na projektu.
- 6.1.8 Zhotovitel služby musí informovat o bezpečnostních událostech, které mohou mít vliv na integritu, důvěryhodnost a dostupnost uchovávaných dat a informací.
- 6.1.9 Zhotovitel musí zajistit ochranu před škodlivým kódem nad poskytovatelem služby uchovávanými daty a informacemi.
- 6.1.10 Zhotovitel musí zajistit ochranu webových portálů proti průnikům nasazením vhodné web aplikační ochrany (např. web aplikační firewall).
- 6.1.11 Řešení jako celek (všechny komponenty – OS, aplikace) musí být udržovány aktualizované a v případě zjištění specifické zranitelnosti aplikace musí být tato bezodkladně opravena.
- 6.1.12 Z pohledu důvěrnosti se s informací může seznámit pouze jakýkoliv zaměstnanec Objednatele, nebo jejich konzultanti a pověřené osoby, nebo osoby Zhotovitele. Ostatní osoby musí být schváleny Objednatelem.
- 6.1.13 Po skončení projektu musí Zhotovitel předat Objednateli digitální zálohu, nebo provozuschopnou kopii CDE na paměťovém nosiči (CD, DVD, případně jiném dle dohody ...). V případě digitální zálohy musí tato záloha obsahovat veškerá data CDE exportované do adresářové struktury včetně logů, auditů a metadat.

7 DALŠÍ POŽADAVKY

- 7.1.1 Zhotovitel bude v rámci společného datového prostředí udržovat aktuální dokumenty, digitální informační modely, průzkumy, výkresy, vyjádření, dokumentace dle Smlouvy o dílo tak, aby byly k dispozici Objednateli.
- 7.1.2 Uživatelské rozhraní systému musí být v českém jazyce.
- 7.1.3 Objednatele požaduje, aby systém zohledňoval následující předpisy v jejich aktuálních zněních:
 - (a) zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů;
 - (b) vyhláška č. 259/2012 Sb., o podrobnostech výkonu spisové služby;
 - (c) VMV č. 57/2017 Národní standard pro elektronické systémy spisové služby;
 - (d) zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů;

- (e) vyhláška č. 193/2009 Sb., o stanovení podrobností provádění autorizované konverze dokumentů;
- (f) zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů;
- (g) vyhláška č. 360/2023 Sb., o dlouhodobém řízení informačních systémů veřejné správy;
- (h) zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce;
- (i) zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti);
- (j) vyhláška č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti);
- (k) Nařízení Evropského parlamentu a rady (EU) 2016/679, obecné nařízení o ochraně osobních údajů (např. dodržením ISO 27001).