Technická specifikace Digitální regulatorní pískoviště (sandbox)

Název dokumentu	Technická specifikace Digitální regulatorní pískoviště (sandbox)
Název souboru	Příloha č. 1 - Technická specifikace
Počet stran	31
Verze	1.0
Stupeň důvěrnosti	Veřejné

Obsah

1 Umístnění a ochrana dokumentu

Součástí obsahu tohoto dokumentu jsou informace, které jsou veřejné pro účel přípravy nabídky Digitálního regulatorního pískoviště (sandbox) – FinTech platformy (dále jen „platforma / sandbox“). Dokument je uchováván, přenášen a distribuován v souladu s pravidly ochrany informací. Informace, které tento dokument obsahuje, nemůžou být bez předchozího svolení firmou CzechInvest postoupeny třetí straně a nesmí být používány, či jakkoliv jinak rozmnožovány pro jiné účely než za účelem posouzení obsahu dokumentu. Dokument je klasifikován stupněm důvěrnosti: veřejné informace. V případě zhotovení tištěné verze z elektronické podoby se jedná o neřízený dokument.

2 Účel dokumentu

Dokument je součást poptávané zakázky od firmy CzechInvest pro tvorbu platformy jako příloha zakázky a je určen pro technický popis řešení platformy.

3 Legislativní rámec a strategické dokumenty

Poskytované služby sandboxu musí být v souladu s:

- zákonem č. 181/2014 Sb., o kybernetické bezpečnosti,
- nařízením Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES,
- zákonem č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce,
- zákonem č. 12/2020 Sb., o právu na digitální službu,
- zákonem č. 250/2017 Sb., o elektronické identifikaci,
- zákonem č. 110/2000 Sb., o ochraně osobních údajů,
- zákonem č. 106/1999 Sb., o svobodném přístupu k informacím,
- zákonem č. 634/1992 Sb., o ochraně spotřebitele,
- nařízením Evropského parlamentu a Rady (EU) č. 2016/679 ze dne 27. dubna 2016 ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES,
- zákonem č. 99/2019 Sb., o přístupnosti internetových stránek a mobilních aplikací,
- dokumentací sloužící k poskytování a provozu služeb definované firmou CzechInvest.

4 Motivace a cílový stav

Dokument vznikl na základě Výzvy Ministerstva průmyslu a obchodu ČR „Digitální regulatorní pískoviště: v rámci komponenty 1.4 Národního plánu obnovy. Tato výzva, která je součástí Investice č. 11, má za cíl podpořit rozvoj digitální ekonomiky, inovativních start-upů a nových technologií prostřednictvím vytvoření regulovaného prostředí pro testování nových fintech a AI produktů. Cílem je posílit podporu pro FinTech a DLT ekosystémy v ČR a zajistit, aby testování nových služeb a obchodních modelů bylo v souladu s evropskou strategií pro digitální finance a doporučeními Rady týkajícími se regulačních pískovišť.

Sandbox poskytne uživatelům platformy přístup k datovým sadám, testování a vývoji řešení v rámci celého programu FinTech platformy. Návrh a řešení sandboxu musí dodržovat architektonický přístup

modulárního řešení, přičemž moduly jsou implementovány jako samostatné sdílené služby anebo interní mikroslužby s jasně definovaným rozhraním.

Sandbox bude poskytován Zadavateli formou služby, která bude mít rozhraní vystaveno pro Zadavatele. Sandbox bude vytvořen jako 3 vrstvá aplikace zahrnující front-end vrstvu, back-end vrstvu, aplikační logiku a datovou vrstvu. Datová vrstva pro vrstvu businessové logiky definuje jednoznačné unifikované rozhraní umožňující v případě nutnosti nahradit poskytovatele služeb sandboxu. Úložiště dat musí být navrženo v souladu s pravidly pro relační anebo NoSQL databáze. Databáze nesmí obsahovat implementovanou aplikační ani jinou logiku, která by znemožňovala případnou výměnu databázové technologie.

Poskytované služby sandboxu by měli:

- být schopny poskytnout datové sady k tématu FinTech v souladu s transakcemi finančních služeb a podpory mandátu ochrany spotřebitele,
- umožnit uživateli vyvíjet / testovat data v testovacím a produkčním prostředí v rámci sandboxu,
- poskytnout možnost přidání dalších datových sad do platformy pro testování bez nutnosti navýšení pracnosti na straně zákazníka,
- být založeny na cloudu,
- zajišťovat přístup k cca. 50 uživatelů včetně poskytnutí administrátorského přístupu pro 28 uživatelů,
- poskytovat přístup k živým, přesným a historickým záznamům operací koncových uživatelů a dat,
- být uživatelsky přívětivé s jasnými grafickými pokyny.

5 Definice sandboxu

Sandbox je framework / technologická platforma, která je vytvořena za účelem urychlení testování FinTech aplikací z pohledu bezpečnosti, optimalizace zdrojového kódu, funkcí a plnění uživatelských procesů, dat, uplatnění regulátorů ovlivňujících plnění funkcí FinTech aplikace, přenosu / příjmu dat přes API rozhraní, konfigurace a napojení IoT zařízení. Sandbox je implementován v perimetru dodavatele sandboxu (cloudové prostředí), který nese odpovědnost za plnění rutinního provozu platformy včetně dodržování legislativních povinností plynoucí ze zákonů a nařízeních uvedených v části Legislativní rámec a strategické dokumenty tohoto dokumentu.

Testování bude probíhat v modulech sandboxu, které bude používat jak zákazník CzechInvest, tak také dodavatel start-up FinTech aplikace:

- **IT Security** – testování zátěže, penetrace, simulace útoků (minimálně DoS / DDOS – Denial-of-service, Distributed denail-of-service, MITM – Man in the middle, Phishing a Pharming, Drive-by, Cross-site scripting – XSS, SQL injection, Malware, Eavesdropping),
- **Backoffice** – poskytování součinnosti a řešení provozu průběhu testování na pozadí, dokumentace sandboxu,
- **Datové tržiště** – testování splnění 3NF, duplicita dat, integrita dat, zabezpečení dat – hashe, anonymizace dat,
- **API** – testování použitých webových služeb, poskytování katalogu služeb,
- **IDE** – testování a práce se zdrojovým kódem, včetně spuštění aplikace a provedení uživatelsky akceptačních testů – simulace procesů / funkčních požadavků FinTech aplikace, spuštění a provedení automatizovaných testů – ověření, zdali odpovídají funkčním požadavkům, dokumentace FinTech aplikace, podpora automatizovaného refaktoringu a optimalizaci zdrojového kódu,
- **Pravidla / Regulátory** – testování definovaných regulátorů ve FinTech aplikaci,
- **CRM** – komunikační kanál pro technickou podporu zákazníka (komunikace dodavatel sandboxu – zákazník CzechInvest), pro technickou podporu start-upu (komunikace CzechInvest – start-up), dokumentace sandboxu a FinTech aplikace,
- **IoT** – testování integrace IoT zařízení včetně operací a instrukcí spojených se životním cyklem IoT zařízení,
- **Přehledy a analýzy** – hlavní přehledový dashboard pro zobrazení testů start-upů a zákazníka CzechInvest, vyhodnocování testů, monitoring a reporting testů.

Testy poskytované sandboxem se budou lišit v závislosti dle testovaného případu užití. Cílem testů bude prokázat vysokou míru úspešnosti v případě ověření pravdivých výsledků, nízkou míru falešně pozitivních výsledků a nízkou míru chybné identifikace v případě ověření pravdivých výsledků.
V případě testování API budou testy zaměřeny na prokázání nízké latence API a správnost vrácených dat.

Dodavatel sandboxu poskytne zákazníkovi testovací a produkční prostředí sandboxu přes vytvoření požadovaných přístupů, rolí a oprávnění uvedených požadovaných dle tohoto dokumentu. Testovací prostředí bude určeno pro ověření funkcí a školení sandboxu pro zákazníka, případně ho zákazník dokáže využít pro školení dodavatelů FinTech aplikací. Produkční prostředí bude určeno pro

provádění testování FinTech aplikací dodavateli FinTech aplikací (start-up firmy) a ověřování plnění testování zákazníkem CzechInvest. Vytvořená prostředí budou škálovatelné pro potřeby vykonávání požadovaných testů bez omezení snížení odezvy systému vzhledem k navýšení přihlášených uživatelů, spuštěných instancí testování, navýšení kapacity datového tržiště, ověřování služeb přes volání API rozhraní, navýšení integrovaných zařízení nebo modulů plynoucích z upgradeu zdrojových kódů dodavatele FinTech aplikace.

Uživatelská podpora sandboxu je rozdělena do těchto streamů:

- Podpora do akceptace projektu
    - dodavatel sandboxu poskytne podporu při zprovoznění testovacího a produkčního prostředí sandboxu pro zákazníka CzechInvest, dodavatel sandboxu poskytne jak konzultace, tak také požadovanou dokumentaci (blíže popsáno v části Požadavky na dokumentaci tohoto dokumentu),
- Podpora v rutinním provozu
    - Dodavatel sandboxu poskytne zákazníkovi CzechInvest školení, školící materiály a dokumentaci v požadovaném rozsahu popsaném v části Požadavky na dokumentaci tohoto dokumentu),
    - Dodavatel sandboxu poskytne zákazníkovi CzechInvest zákaznickou podporu (HelpDesk) přes modul CRM, případně doplněno o chatbot / nápovědu pro řešení běžných Q&A,
    - Zákazník CzechInvest poskytne dodavateli FinTech aplikace (start-upu) zákaznickou podporu přes modul CRM.

6 Architektura požadovaného řešení

6.1 Složení řešitelského týmu

Dle stanovených očekávaných výstupů projektu jsou definovány role řešitelského týmu s požadavky na:

- jejich odpovědnost a činnosti, které prováděli v rámci plnění referenčního projektu,
- jejich odpovědnost a činnosti, které budou provádět v rámci plnění této zakázky.

Funkce člena řešitelského týmu	Aktivity v době realizace referenčního projektu	Předpokládané aktivity v době řešení projektu pro CzechInvest
Architekt	Návrh architektury řešení, Návrh technologií, Dohled nad dodržování konceptu řešení	Návrh rozšíření aplikace (bude-li plynout z technické specifikace zakázky), Dohled nad funkčním celkem sandboxu, Detekce a vyhodnocení nových technologických možností v případě nutnosti provozu
IT Teamleader	Implementace návrhu, Dohled nad implementací včetně refaktoringu a optimalizace zdrojových kódů, Dohled nad nasazování, Dohled nad dodržováním verzování a pravidel ITILu	Provádění a dohled refaktoringu a optimalizace zdrojových kódů, Dohled nad dopadem změny technologie (bude-li plynout z nutnosti provozu), Dohled nad dodržováním verzování (bude-li plynout z nutnosti provozu)
Vývojář	Realizace fullstack projektu, Dokumentace zdrojového kódu	Realizace fullstack rozšíření projektu (bude-li plynout z nutnosti provozu), Dokumentace zdrojového kódu
Systémový inženýr / Databázový specialista	Návrh konfigurace systémových zařízení a rozhraní, Nasazování aplikace, Dohled nad infrastrukturou, Dohled nad databázovým systémem	Změny v konfiguraci systémových zařízení a rozhraní, Nasazení rozšíření projektu, Dohled nad infrastrukturou, Dohled nad databázovým systémem

Systémový inženýr	L2 servis, Návrh refaktoringu a optimalizace zdrojových kódů, Nasazování aplikace, Správa infrastruktury, Správa rozhraní, Správa služeb	Správa infrastruktury, Správa rozhraní, Správa služeb
Tester manažer / Tester	Návrh a provedení testovací analýzy, Vyhodnocování kvality, Návrh změn	Návrh a provedení testovací analýzy (bude-li plynout z nutnosti provozu), Úpravy a rozšíření testovacích scénářů (bude-li plynout z nutnosti provozu), Provedení testování rozšíření a změn (bude-li plynout z nutnosti provozu), Dokumentace výsledků testování (bude-li plynout z nutnosti provozu)
Bezpečnostní specialista	Návrh ochrany sandboxu a dat před kybernetickými hrozbami, Návrh opatření bezpečnostních kolizí, bezpečnostní politiky a mitigace rizik, Monitoring síťového provozu, Bezpečnostní audity sandboxu, Řešení bezpečnostních incidentů	Dokumentace bezpečnostních incidentů, audit, Monitoring síťového provozu, Řešení bezpečnostních incidentů
Analytik	Analytický návrh řešení, Dokumentace návrhu	Identifikace nových vylepšení (bude-li plynout z nutnosti provozu), Návrh řešení nových vylepšení (bude-li plynout z nutnosti provozu), Dokumentace návrhu
Projektový manažer	Vedení týmu, Projektová dokumentace, Kontrola dodržování milníků a časového harmonogramu	Vedení týmu, Projektová dokumentace

6.2 Role v sandboxu

V rámci sandbox platformy jsou očekávaný role, které budou pracovat s moduly sandboxu:

- **Orchestrátor** – řídí a dohlíží nad plněním businessových požadavků na sandbox, jakožto i na plnění businessových požadavků dodavatele start-upu FinTech aplikace, komunikuje s dodavatelem sandboxu a s manažerem start-upu, deleguje vzniklé úkoly na ostatní účastníky realizované session,
- **Administrátor** – spravuje, řídí a dohlíží nad plynulým během rutinního provozu testovacího a produkčního prostředí sandboxu, realizuje provozní požadavky vzniklé při testování jak zákazníkem CzechInvest, tak také start-upem, monitoruje a reportuje vzniklé incidenty dodavateli sandboxu, podílí se na nutných úpravách sandboxu pro spuštění a provoz testování FinTech aplikace start-upu, pracuje se zákaznickou podporou, administrátorská role je určena pro CzechInvest, ale také i pro administrátora FinTech aplikace start-upu,
- **Uživatel / Účastník** – uživatel zákazníka CzechInvest nebo FinTech aplikace start-upu, účastní a realizuje testování v souladu s funkčními možnostmi sandboxu, vyhodnocuje analýzu testování, komunikuje s dalšími účastníky při testování, pracuje se zákaznickou podporou,
- **Interní uživatel** – řídí, spravuje a deleguje úkony vzniklé při testování, ověřuje výsledky testování, sleduje provoz a dokáže poskytnout návrh řešení vzniklých kolizích, ovládá procesy sandboxu a dokáže poskytnout základní podporu při testování,
- **Systém** – realizuje automatizované požadavky sandboxu a testování FinTech aplikací.

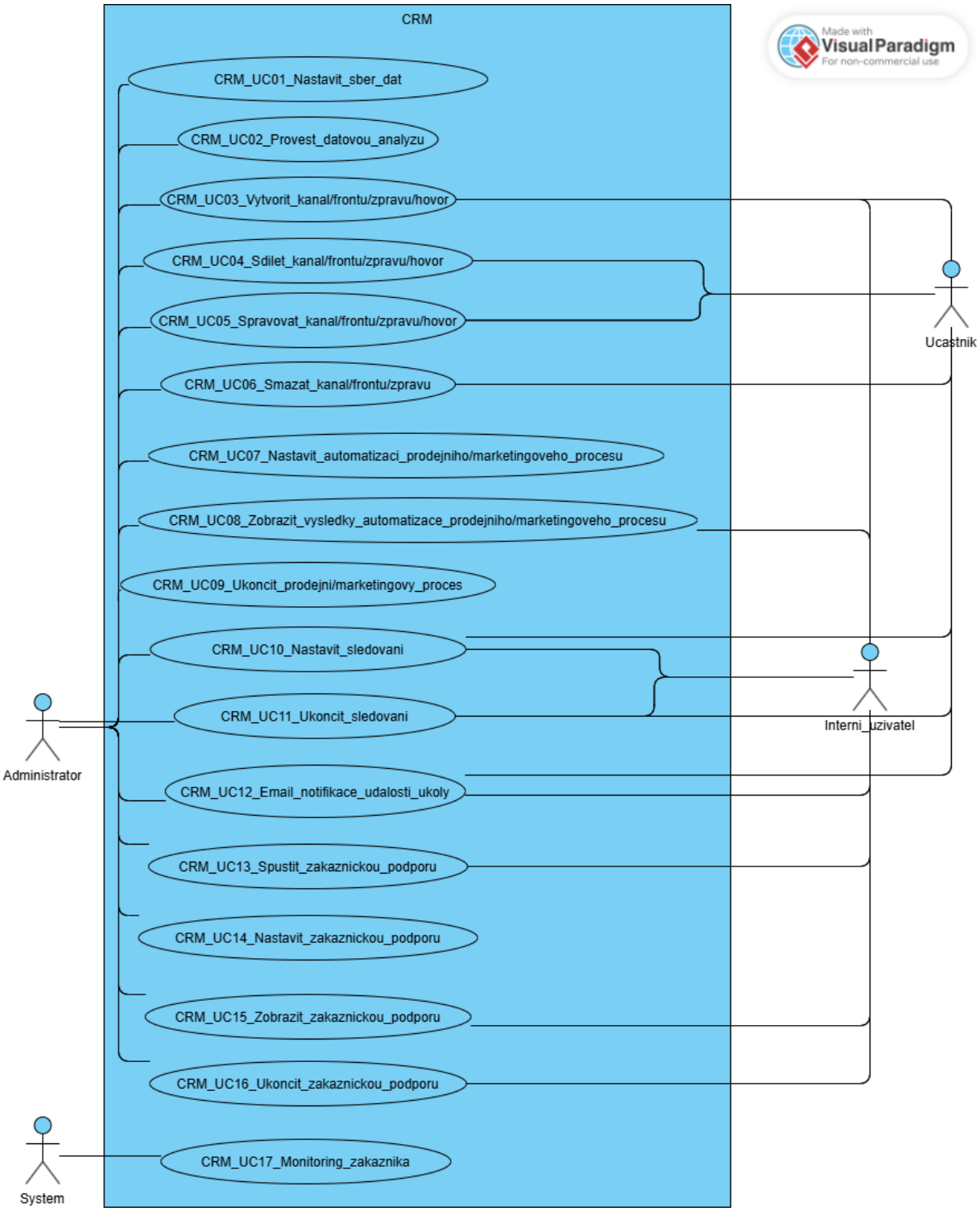
6.3 Funkční požadavky

6.3.1 Modul CRM

Modul CRM je zákaznicky orientovaný modul pod správou administrátora. Funkční požadavky modulu jsou rozděleny do pěti kategorií: zákaznická data, segmentace zákazníku, prodejní a marketingové procesy, operace zákazníka, zákaznická podpora. Administrátor dle definovaných pravidel, klíčových událostí, stanovené strategie neustálého zlepšování konfiguruje sběr zákaznických dat, ze kterých dokáže pomoci integrované business inteligence provést datovou analýzu. Nastavení konfigurace ovlivňuje definice segmentů zákazníků určených Orchestrátorem vzhledem k očekávaným automatizovaným prodejním nebo marketingovým procesům. Kromě konsolidace chování zákazníků modul poskytuje také zaměření sledování na jednotlivce za účelem ověřování chování vybraných klíčových klientů. Kategorie zákaznické podpory je určena pro komunikaci jak s interními uživateli, tak také pro komunikaci s veřejností.

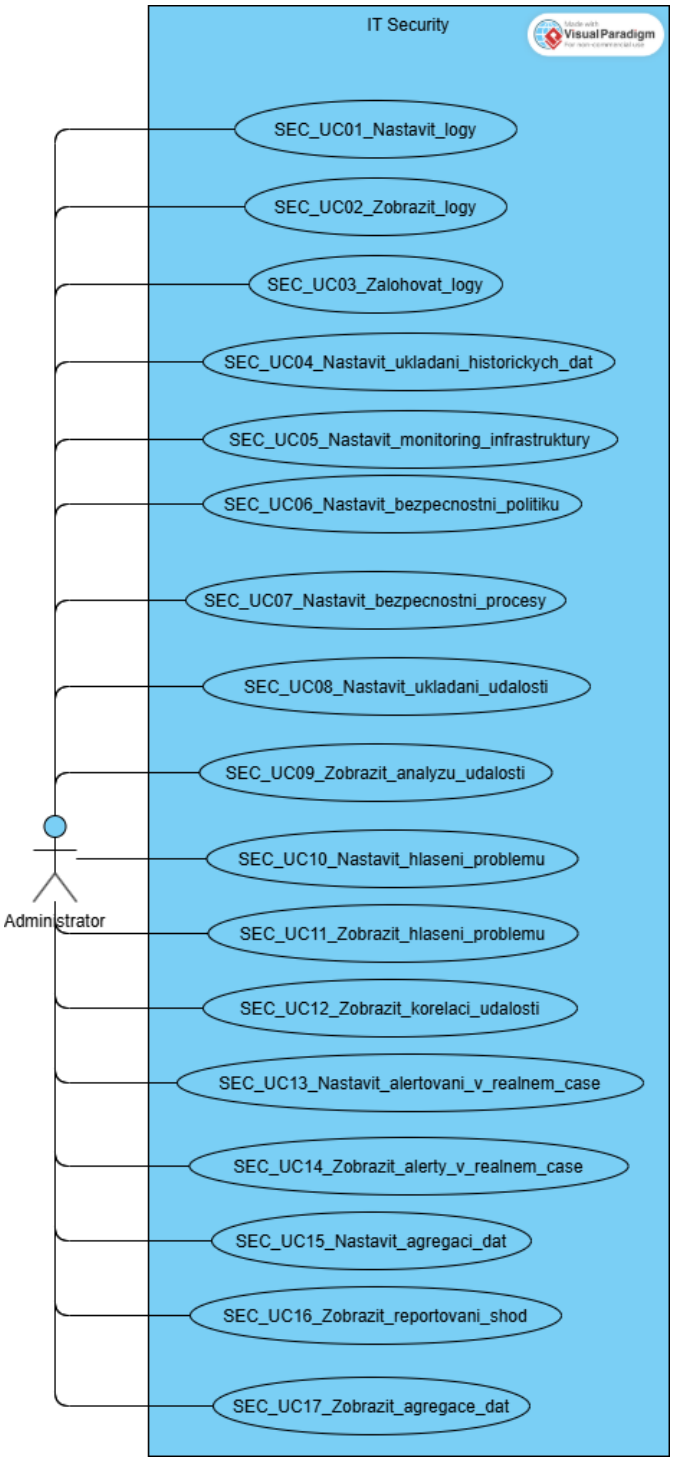
Komunikace mezi uživateli (účastníky), interními uživateli včetně Orchestrátora a Administrátora je vedena přes CRM. Zprávy je možno zasílat na konkrétního uživatele, kde odesláním první zprávy systém vytváří kanál, do kterého v budoucnu je možno doplnit dalšího uživatele s nastavením zobrazení / skrytí předešlé historické komunikace. Další možnosti je vytvoření kanálu za účelem konkrétního tématu, kde uživatel předem zvolí účastníky komunikace. Každému účastníkovi komunikace je povoleno / zamítnuto sdílet kanál, připojit / odpojit se z kanálu kdykoliv během životního běhu komunikačního kanálu s možností nastavení zobrazení / skrytí historické komunikace, přičemž veškeré záznamy jsou logovány a operace zaznamenávány pro auditní stopu. Modul umožňuje také řešení front, kde jsou ukládány pracovní úkoly, události, případně zprávy, hovory. Fronty jsou vytvářeny dle strategických a provozních požadavků Orchestrátora a jsou určeny k efektivnímu sledování a zpracování platformou / uživateli vytvářených úkolů, události a zprávy (obsahuje-li zpráva definici úkolu). V rámci fronty je umožněno nastavení priorit zpracování úkolů,

události a zpráv / hovorů, a tím zajištěna podpora řízení zpracování dle definovaných vlastností fronty.



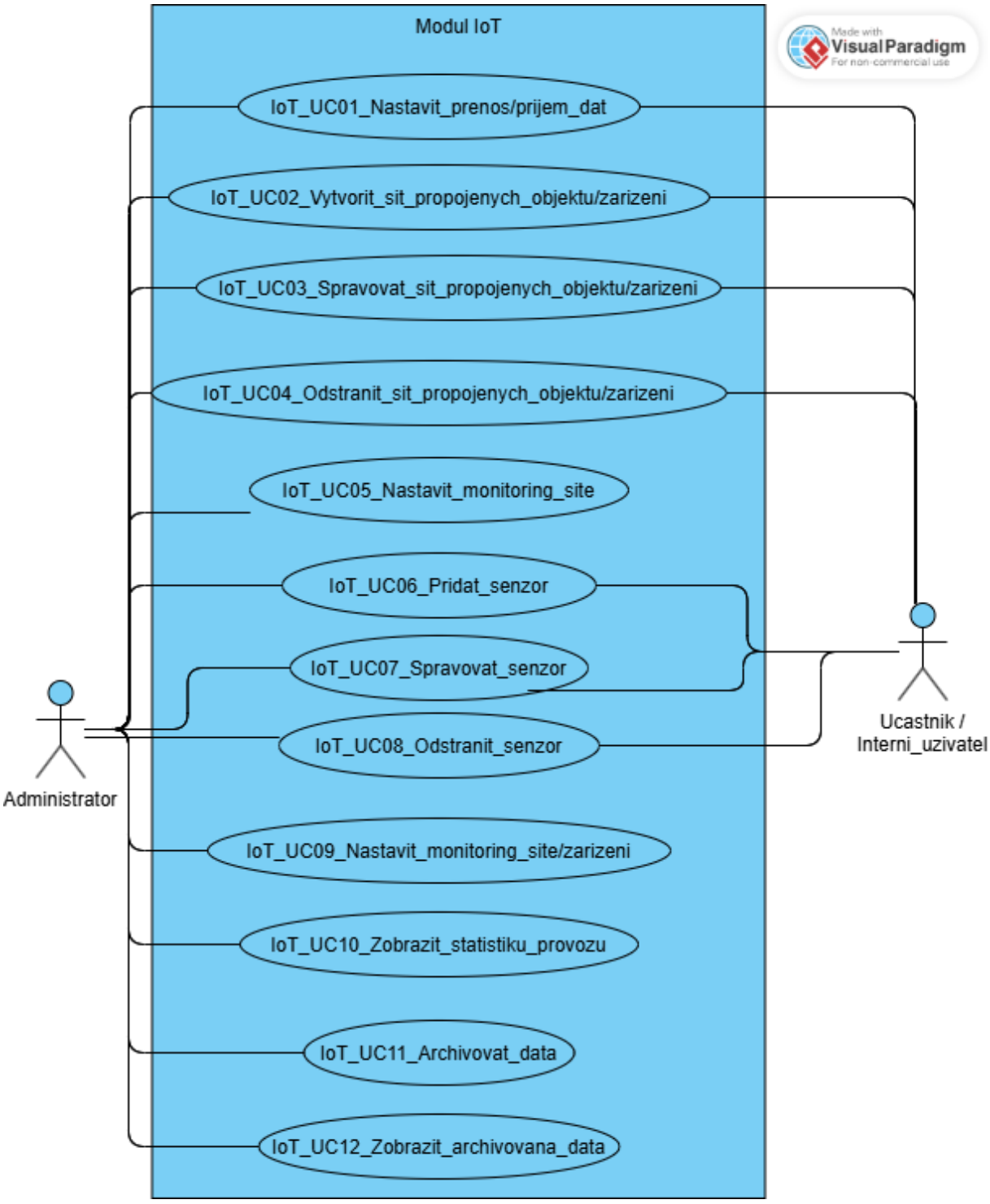
6.3.2 Modul IT Security

Pro řízení a dohled nad bezpečností dat a chováním uživatelů, nebo IoT zařízení včetně podpory auditování je určen modul IT Security. Modul zpracovává data v reálním čase, a také dokáže poskytnout komplexní historii z důvodu zachování auditních stop prováděných v platformě. Základní funkcí je logování, jak transakční, tak také auditní s dodržením vlastností transakčního zpracování: atomicity, konzistence, izolace, durability. Modul se řídí nastavením bezpečnostní politiky definované Orchestrátorem. Její součástí je určení řídících a podpůrných bezpečnostních procesů a událostí. Výsledkem bezpečnostního monitoringu je reporting incidentů, chyb, útoků, rizik a identifikovaných kolizí. Pro detailnější monitoring je poskytnuta funkce nastavení alertování.



6.3.3 Modul IoT

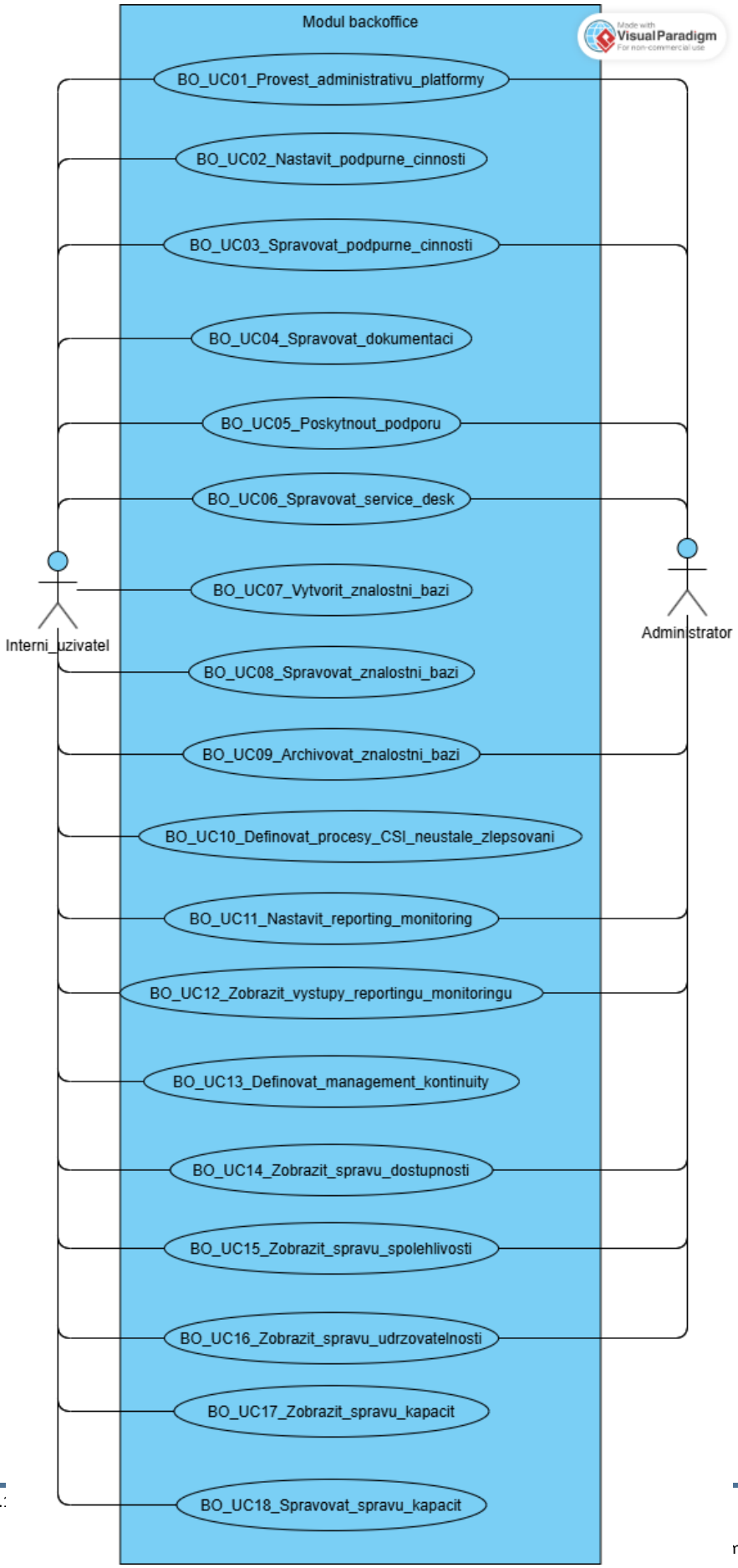
Platforma podporuje také integraci s chytrými zařízeními, a pro jejich správu je určen modul IoT. Základní připojení zařízení a definici přenosu / příjmu dat provádí účastník, interní uživatel, a rozšiřující připojení s možností konfigurace zabezpečení provádí Administrátor. Zařízení jsou konsolidována do sítě z důvodu monitoringu a reportování chování jako i provozu a kolizních situací. Některé typy zařízení umožňují také práci se senzorem, čímž se zvýší efektivita využíván IoT zařízení. Data přenášena přes IoT zařízení je možno archivovat, a poté zpětně zobrazit pro případ rekonstrukce chybového zásahu, nebo narušení bezpečnosti.



6.3.4 Modul backoffice

Pro řízení procesů na pozadí včetně podpůrných činností platformy je stanoven modul backoffice. Modul je primárně určen pro práci Interního uživatele a Administrátora. Kromě práci s procesy a jejich činnostmi, je backoffice zaměřen i na dokumentaci, která vzniká a řídí se funkcemi platformy. Součástí modulu je také práce se znalostní bází, která je jednotným místem pro pomoc service desku

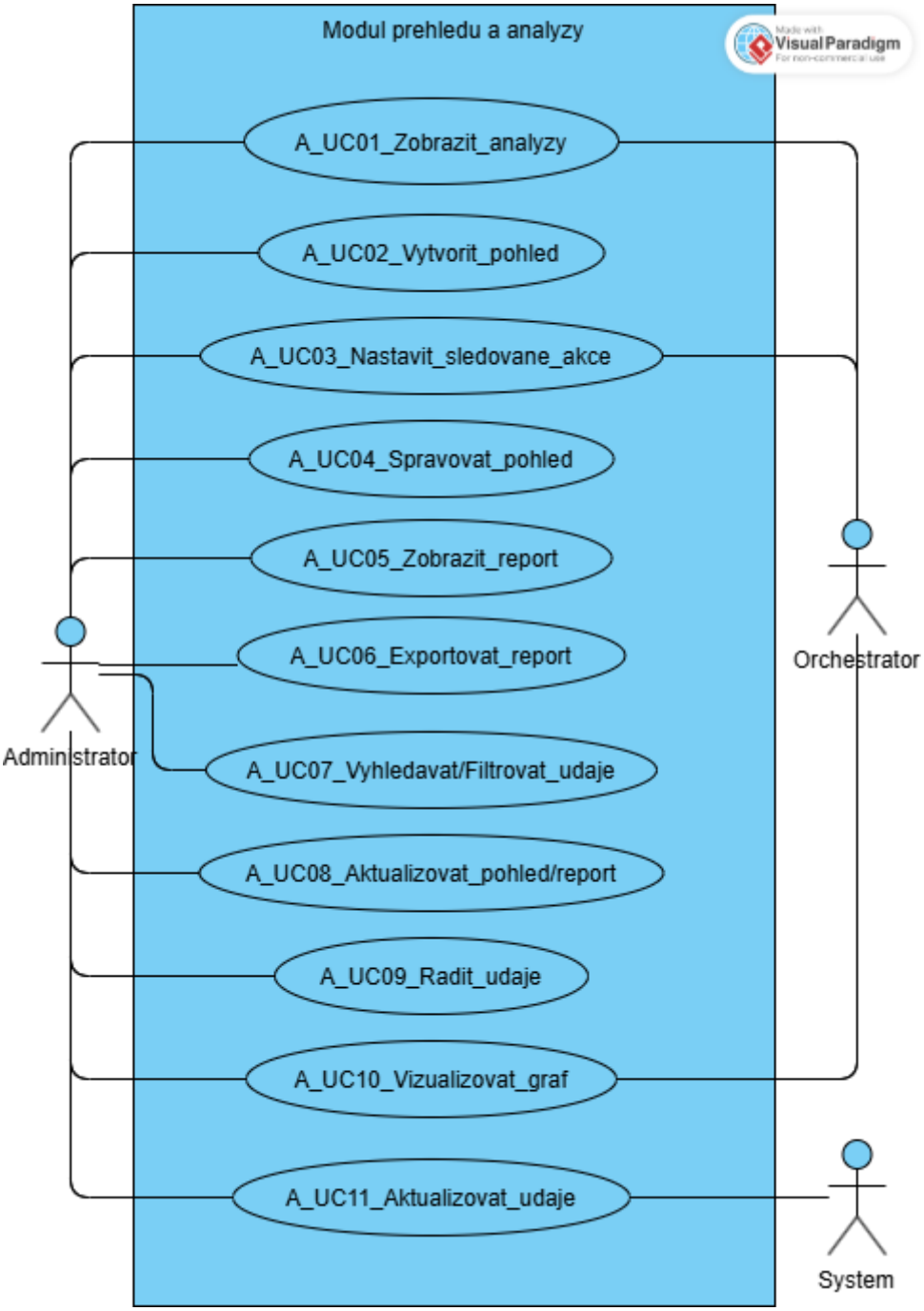
platformy, a pomocí zachycení kolizí a jejich řešení, je vstupním podkladem pro definici CSI procesů – procesů neustálého zlepšování. Tyto procesy jsou důležité z hlediska vylepšování platformy a plnění harmonogramu change a release managementu, jako i pravidel bezpečnostních i businessových. Řešení backofficu je v souladu s pravidly ITILu, a tedy poskytují i monitoring kontinuity všech modulů platformy. Pro monitoring provozu jsou poskytovány funkce správy dostupnosti (hlídání vysoké dostupnosti, vytíženosti sítě, CPU, paměti, kapacita disku), správy spolehlivosti (hlídání vysoké dostupnosti na základě automatizovaného propočtu, dle identifikovaných výpadků, kolizí, incidentů, a tím způsobených odstávek platformy, doby rekonvalescence platformy, případně jiných typů bezpečnostních útoků), správu udržovatelnosti (soulad s plánem change a release managementu) a správu kapacit (identifikace lidských i materiálních kapacit – hardwarové a softwarové kapacity dle konfigurace infrastruktury, na které je platforma nasazena).


Modul backoffice
Made with Visual Paradigm For non-commercial use
BO_UC01_Provest_administrativu_platformy
BO_UC02_Nastavit_podpurne_cinnosti
BO_UC03_Spravovat_podpurne_cinnosti
BO_UC04_Spravovat_dokumentaci
BO_UC05_Poskytnout_podporu
BO_UC06_Spravovat_service_desk
BO_UC07_Vytvorit_znalostni_bazi
BO_UC08_Spravovat_znalostni_bazi
BO_UC09_Archivovat_znalostni_bazi
BO_UC10_Definovat_procesy_CSI_neustale_zlepsovani
BO_UC11_Nastavit_reporting_monitoring
BO_UC12_Zobrazit_vystupy_reportingu_monitoringu
BO_UC13_Definovat_management_kontinuity
BO_UC14_Zobrazit_spravu_dostupnosti
BO_UC15_Zobrazit_spravu_spolehlivosti
BO_UC16_Zobrazit_spravu_udrzovatelnosti
BO_UC17_Zobrazit_spravu_kapacit
BO_UC18_Spravovat_spravu_kapacit
Interni_uzivatel
Administrator

nent!

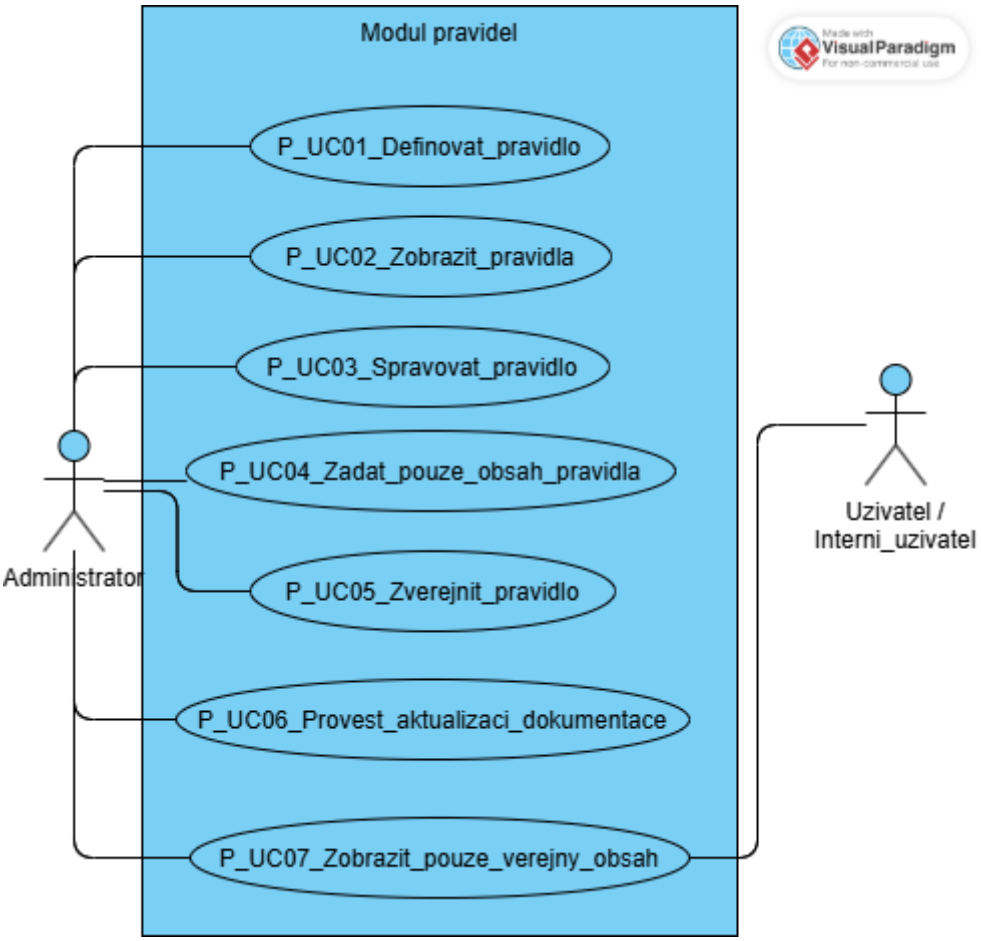
6.3.5 Modul přehledu a analýzy

Přehledový modul je určen pro high level pohled provozu platformy. Pohled je umožněno spravovat, a tak přidávat nové dlaždice sledování provozu z pohledu všech modulů platformy. Součástí přehledu je prezentace analýzy běhu modulů. Přes modul přehledu a analýz je umožněno nastavení sledování akcí, které jsou různě defragmentovány dle nastavení typu zobrazovaných údajů a typu zdroje dat. Přehled je také reportován vizuálně graficky a digitálně zpracovatelný pomocí integrované business inteligence. Údaje v pohledech jsou aktualizovány real-time.



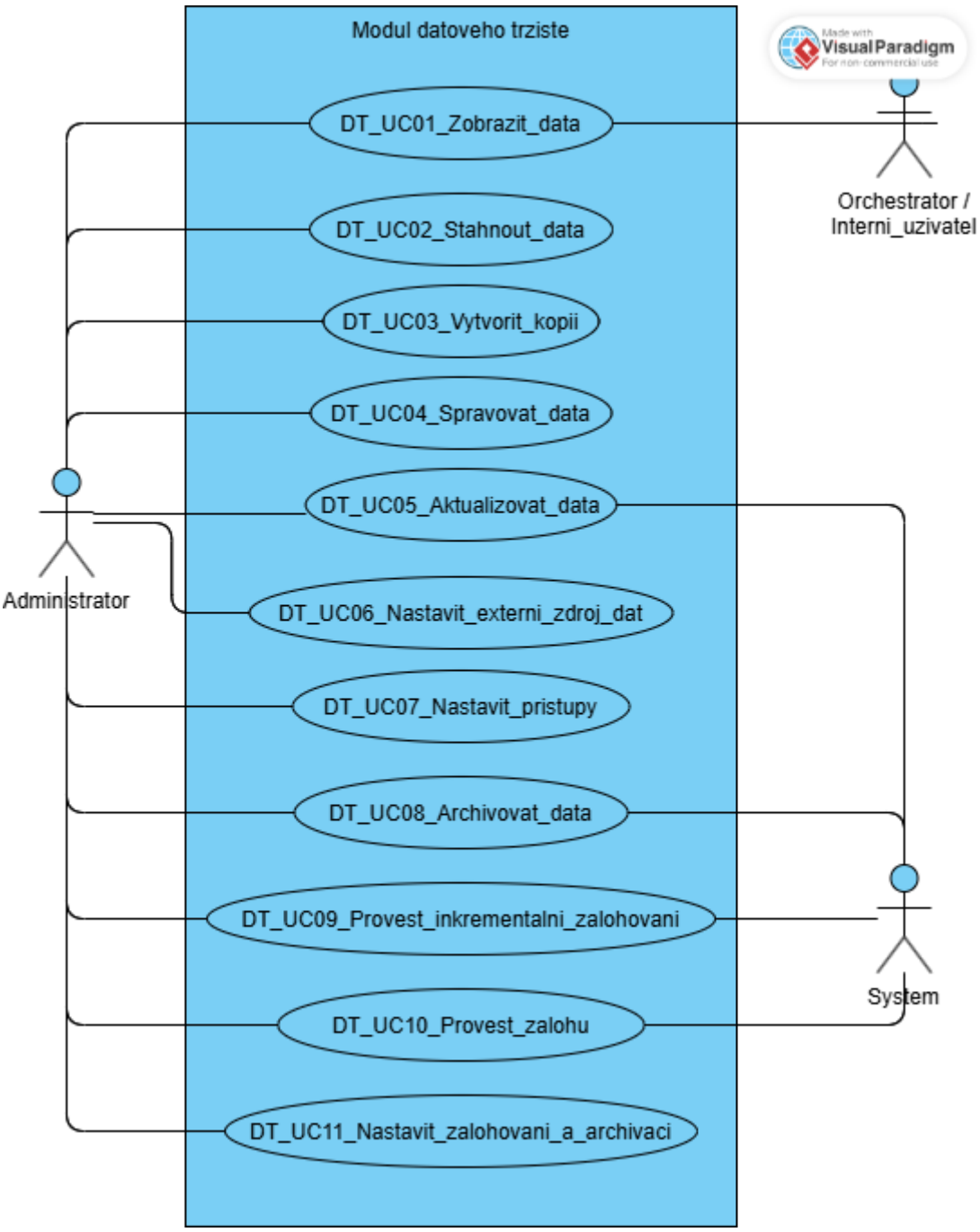
6.3.6 Modul pravidel

Komplexní chování modulů platformy je řízení regulacemi, pravidly, které je nutno definovat a správně nastavit vzhledem ke všem modulům platformy. Pravidlo může být interní a externí, a také je možno u pravidla nastavit pouze obsah, nebo komplexní metadata a kontinuitu vůči životnímu cyklu dat používaných v platformě. Aktualizace pravidel probíhá manuálně z důvodu identifikace kolizních pravidel a jejich ověření souladu s nastavením stávajících běžících instancí platformy. Některá pravidla jsou veřejná, kdy je povoleno pouze zobrazení veřejného obsahu, nikoliv metadat a pozadí akcí včetně auditní stopy instancí, které jsou řízeny pravidly. Veřejné obsahy jsou definovány také vládními reguli, zákony, normy, vyhláškami, ale někdy můžou být ovlivněny i interními regulacemi, které mají dopad na obecného uživatele, účastníka.



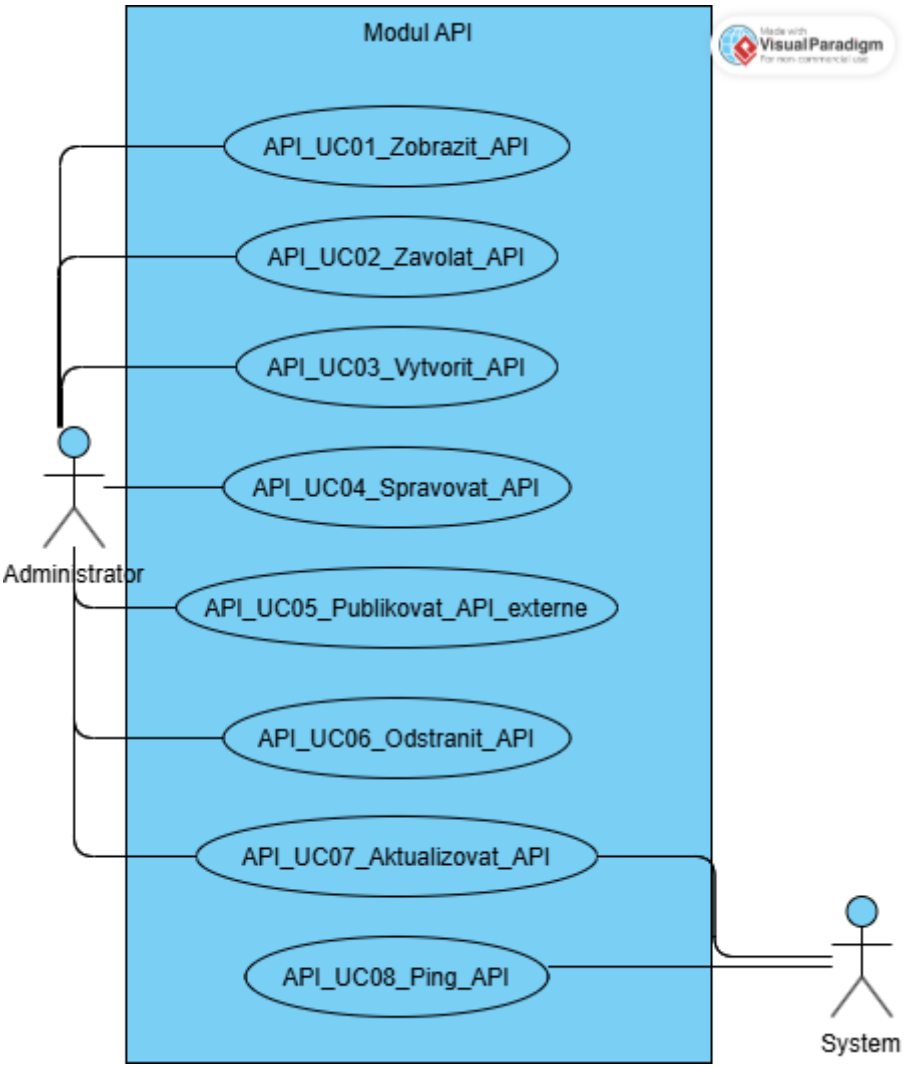
6.3.7 Modul datového tržiště

Pro komplexní zprávu dat je vytvořen modul datového tržiště. Cílem modulu je korigovat práci s daty a operace vykonávané nad daty. Veškerá technická správa podléhá Administrátoru, který nastavuje systémové funkce pro automatizované procesy s daty v platformě. Kromě CRUD operací modul umožnuje práci s nastavením zdroje dat, archivací dat a zálohováním dat. Data jsou zpracovávána také v kooperaci s modulem IoT a modulem I/O aplikace.



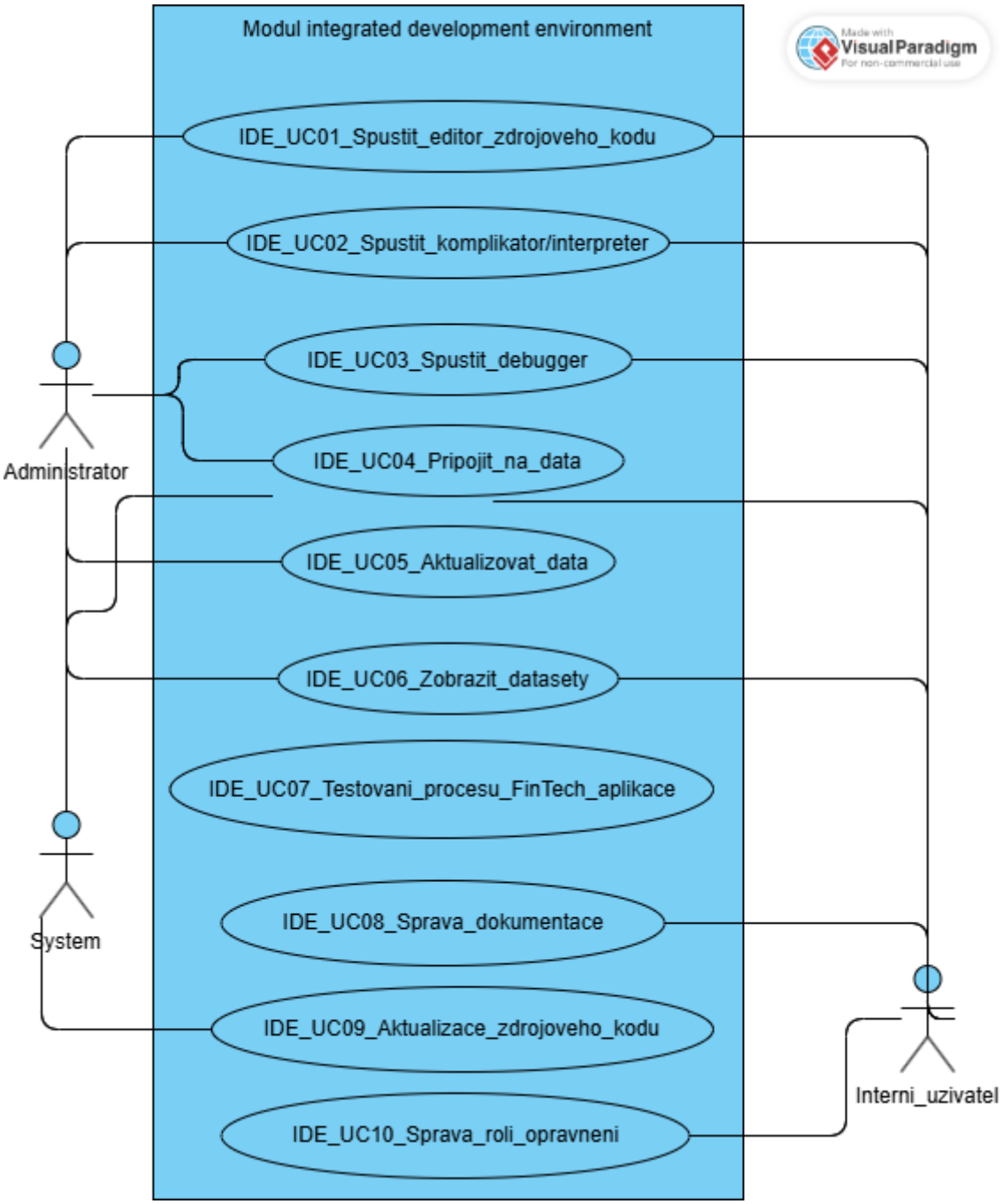
6.3.8 Modul API

Komunikace interní mezi moduly jako i komunikace veřejná je řešena přes jednotné místo reprezentováno API rozhraním, kde jsou přijímány služby (SOAP, REST) přes integrované unifikované jednotné rozhraní (ESB, WSO2), a také data z externích zdrojů (zdroje může být zařízení IoT, nebo externí datové tržiště přes integraci na server, nebo vystavené rozhraní), přes vystavené komunikační brány, které podléhají nastavení IT security. Vzniklá komunikační rozhraní je možno publikovat v souladu s pravidly a regulátory platformy. Pro ověření nastavené komunikace je definováno automatizované ověření konektivity a provedení aktualizace, která je zaznamenána v harmonogramu change a release managementu. Součástí testování volání API bude také prokázání nízké latence API a správnost vrácených dat.



6.3.9 Modul integrated development environment

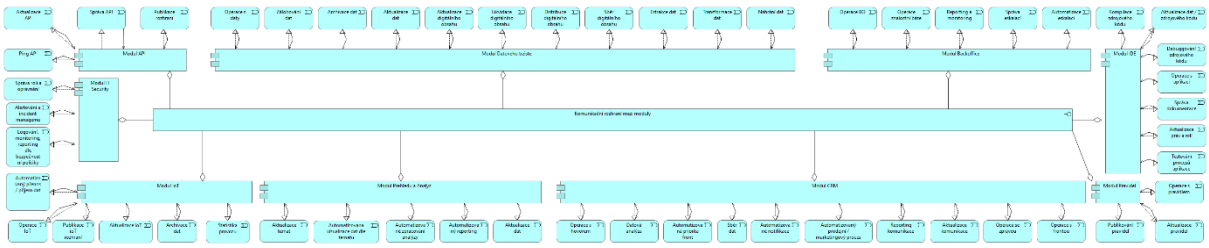
Pro urychlení vývojářské práce je součástí platformy integrované vývojové prostředí, které obsahuje editor zdrojového kódu, kompilátor, případně interpreter a také debugger. Integrovanou součástí modulu je RAD systém, tedy systém pro rychlý vývoj aplikací, který je určen pro vizuální návrh grafického uživatelského rozhraní, objet browser. Modul plně podporuje použité programovací paradigma daného programovacího jazyka. Součástí modulu je také umožnění práce s vizuálním programováním, kde jsou využity nové aplikace přemístěním programovacích stavebních bloků a vytvořením vývojových diagramů nebo blokových schémat, které jsou reprezentovány diagramy definovanými jazykem UML. Důležitým aspektem modulu je funkce pro šifrování a propojení s různými typy databází. Modul také podporuje automatizovaný refaktoring a optimalizaci zdrojového kódu.



6.4 Aplikační vrstva FinTech Platformy

Identifikované moduly aplikační vrstvy FinTech platformy odpovídají realizaci funkčních požadavků definovaných v businessové vrstvě. Moduly jsou řízeny událostmi, které vznikají v průběhu běhu procesů platformy, tedy při zpracování operací a instrukcí vedených ze vzniklých instancí a akcí systémů, jakožto i uživatel. Vzájemné propojení je tvořeno unifikovaným jednotným rozhraní, které je realizované v souladu s požadavky přenosu a příjmu jak událostí, tak také dat, ale není omezováno typem technologie. Jediné omezení komunikačního rozhraní je bezpečnostní politika, regulátory a infrastrukturní konfigurace prostředí, ve kterém je platforma nasazena. Jednotlivé moduly jsou unifikované pro provedení realizace bez závislosti na omezení technologie s možností obnovení / zneplatnění modulu bez nutnosti vážnějšího dopadu na běh platformy, ale také i s podporou vysoké škálovatelnosti, která umožní napojení nového modulu přes komunikační rozhraní na hlavní komunikační bránu platformy bez nutnosti delšího výpadku platformy. Události platformy lze obecně rozdělit na:

- události aktualizační (zde se jedná jak o aktualizaci dat, tak také kontextu – obsahu),
- události přenosu / příjmu jak dat, tak také i kontextu,
- operační události určené pro vykonání funkčních požadavků vzniklých z businessové vrstvy a instancí vzniklých z podpůrných procesů, procesů běžících na pozadí, nutných pro realizaci životního cyklu platformy v daném prostředí,
- monitorovací a reportovací události za účelem přehledu a analýz, ale také za účelem zpětné auditní stopy na základě získaných logů a akcí,
- události provozních jako jsou publikování, likvidace, distribuce, sběr, skartace, archivace, zálohování dat, událostí i obsahu,
- události určených pro obnovu pro případy ztráty dat, událostí, obsahu,
- bezpečnostních událostí dle nastavených dle bezpečnostní směrnice a regulátorů platformy.



6.4.1 Modul API

Modul API reprezentuje vystavené rozhraní, přes které je možno komunikovat se sandboxem. Součástí modulu jsou události řídící správu definovaného rozhraní, jeho publikace, jako i ověření správného napojení a komunikace.

6.4.2 Modul IT Security

Pro dodržení bezpečnosti řízení využití platformy a monitorování všech akcí a operací vykonávaných jak s daty, tak s kontextem sandboxu je vytvořen modul IT Security. Součástí modulu je i reprezentace rolí a nastavení oprávnění včetně možnosti správy uživatelů, rolí a skupin, které jsou zaváděny do sandboxu jako interní uživatelé i účastníci testování FinTech aplikace. Modul je konfigurován tak, ať poskytuje alertování a plnou podporu pro incident management, včetně

rutinních provozních akcí, jakými je logování jak transakcí, tak obsahu, monitoring a reporting dle bezpečnostní politiky.

6.4.3 Modul IoT

V případě využívání IoT zařízení je navržen modul pro vytvoření a konfiguraci komunikace s IoT zařízením nebo senzorem. Dle nastavené konfigurace je prováděn přenos / příjem dat, který je monitorován dle identifikace prováděných operací. Aktualizace komunikačního rozhraní včetně aktualizace operací s daty je ve správě nastavení modulu a rozsahu plnění publikovaného rozhraní.

6.4.4 Modul Přehledu a analýz

Pro sledování provozu, zobrazení výsledků statistik a hodnocení testování je určen Modul Přehledu a analýz. Požadované výstupy jsou systematizovány dle výběru tématu, který poskytuje správu s určením konkrétních hlídaných funkcí, dat, operací, případně uživatelů. Granularita výstupů a zpracování analýz je uživatelsky přívětivé dle požadavků na vizualizaci a možnosti hodnocení testování.

6.4.5 Modul Datového tržiště

Modul Datového tržiště je určen pro operace s daty včetně zálohování, archivace, extrakce, transformace, sběru, likvidace, nahrávání / exportování dat i digitálního obsahu. Datové tržiště umožňuje také náhled databáze včetně datové struktury a možnosti práce s daty pomocí zadávání dotazů a jejich zpracování na pozadí. Je-li použita datová struktura vizualizována také obecnějším pohledem, umožňuje zobrazování datových view, se kterými testovaná aplikace pracuje. Datové tržiště automatizovaně kontroluje jak plnění normálních forem, tak také duplicity dat, nedodržení integrity dat, nedodržení datových typů, duplicity primárních klíčů.

6.4.6 Modul Backoffice

Správa sandboxu je řízena přes Modul backoffice. Jeho cílem je hlídání operací na pozadí, práce se znalostní bází, která je vytvářena na základě zjišťovaných chyb, učení se interních uživatelů při testování FinTech aplikace. Součástí modulu je také práce s eskalací a vytvářením eskalačních pravidel, které jsou poté sandboxem zpracovávány automatizovaně a řídí průběhu testování. Modul Backoffice poskytuje také reporting a monitoring provozu.

6.4.7 Modul IDE

Pro zobrazení, vývoj, úpravy a testování zdrojového kódu FinTech aplikace je navržen Modul IDE. Kromě kompilace kódu a jeho vizualizace, poskytuje také správu nad dokumentací, která je součástí dodávky testované FinTech aplikace. Modul poskytuje rozhraní, které umožňuje aplikaci spustit a vizualizovat také pro možnost testování GUI dle testovacích scénářů. Pro správu rolí a oprávnění je zde doplněna událost aktualizace práv a rolí, a to z důvodu ověření všech možných rolí, které v testované aplikaci byly zaneseny.

6.4.8 Modul Pravidel

Každá testovaná FinTech aplikace uplatňuje regulátory, pravidla, která omezují funkční požadavky a jejich plnění. Pravidla jsou současně realizována i jako interní pravidla – například bezpečnostní směrnice. Definovaná pravidla ovlivňují také možnost práce s daty, s eskalacemi, s frontami, se zprávami, nebo se vzniklými dokumenty.

6.4.9 Modul CRM

Pro komunikaci mezi interním uživatelem, který testuje FinTech aplikaci a dodavatelem FinTech aplikace je určen Modul CRM, který poskytuje veškeré CRUD operace vykonávány při hovoru nebo zprávě. Komunikace jsou definovány procesem, který může mít zaměření na plnění prodejního / marketingového procesu. Modul poskytuje také odesílání a správu notifikací, které jsou ovlivněny eskalacemi a definovanými pravidly. Veškerá data získána z komunikace podléhají datové analýze a reportingu.

6.5 Technologická a infrastrukturní vrstva sandboxu

Sanbox není technologicky omezen z pohledu vývojové platformy nebo řešení IDE. Základním požadavkem je naplnění požadavku na řešení cloudové aplikace, která je implementována v perimetru dodavatele sandboxu a současně její správa a zabezpečení je v plné kompetenci dodavatele, přičemž dodavatel pravidelně provádí release, hotfixy, service patch, uploady a upgrade sandboxu. O provedení zásahu je informován zákazník předem včetně identifikace technologické a infrastrukturní změny a dopadu do architektury sandboxu.

7 Požadavky na bezpečnost

7.1.1 Prostředí

Sandbox je poskytován v testovacím a produkčním prostředí. Testovací prostředí je určeno pro účel provádění školení, ověření realizace provedených zásahů z důvodu rutinních prací dle technologické a infrastrukturní vrstvy, testování nových rozšíření sandboxu. Produkční prostředí je určeno pouze pro provádění ostrých testů FinTech aplikace, kde je důležité zaznamenání všech výsledků testování aplikace za účelem rozhodnutí vhodnosti / nevhodnosti aplikace, určení intervenčních oblastí FinTech aplikace, identifikace kolizních situací, alertů, incidentů a provozních chyb zachycených jak v datovém tržišti, tak také v modulu IT Security.

7.1.2 Vývoj a dokumentace

Je předpokládán vývoj sandboxu v průběhu poskytování služby a s tím související verzování sandboxu a aktualizace uživatelské, administrátořské a vývojářské dokumentace. Každá vzniklá dokumentace bude verzována včetně identifikace změny a určení dopadu změny. Změny vzniklé při nasazování nové verze aplikace budou předem obeznámeny zákazníkovi s dopadem na možnosti budoucího využití sandboxu. Změny nemůžou být prováděny, pokud aktuálně probíhá testování FinTech aplikace, a bez schválení zákazníka. Budou-li identifikovány změnové požadavky na sandbox ze strany zákazníka, budou se řídit metodikou ITIL.

7.1.3 AAA bezpečnost

Aplikační a programové vybavení sandboxu musí umožňovat logování protokolem Syslog nebo jiným obdobným způsobem. Systém ukládá údaje o všech uživatelských operacích, včetně identifikace uživatele, který operaci provedl. Jedná se jak o změny údajů, tak i informace o náhled na informace.

Funkcionalita auditování a logování zaznamenává informace o bezpečnostních a provozních událostech. Logy musí být jednořádkové. Sběr informací zajišťuje zejména:

- datum a čas včetně specifikace časového pásma,
- typ činnosti,
- identifikaci technického aktiva, které činnost zaznamenalo,
- jednoznačnou identifikaci účtu, pod kterým byla činnost provedena,
- jednoznačnou síťovou identifikaci zařízení původce
- úspěšnost nebo neúspěšnost činnosti.

Nad rámec výše uvedeného bude součástí logování také:

• přihlašování a odhlašování ke všem účtům (i neexistujícím účtům), a to včetně zaznamenání o úspěšném či neúspěšném pokusu,

• činnosti provedené administrátory (privilegovanými účty),

• úspěšné i neúspěšné manipulace s účty, oprávněními a právy,

• neprovedení činností v důsledku nedostatku přístupových práv a oprávnění,

• činnosti uživatelů, které mohou mít vliv na bezpečnost informačního a komunikačního systému,

• úspěšné a neúspěšné zahájení a ukončení činností technických aktiv,

• kritická i chybová hlášení technických aktiv,

• přístupy k záznamům o událostech (žurnálům), pokusy o manipulaci se záznamy o událostech a změny nastavení nástrojů a komponent vykonávající činnosti a funkce určené pro zaznamenávání událostí.

Sandbox nemusí být provozován v režimu vysoké dostupnsoti (High Availability, HA).

Autorizace a autentizace uživatelů bude probíhat ověřováním uživatele a jeho oprávnění. Systém bude podporovat SSO v rámci všech komponent sandboxu, tzn. Uživatel se nemusí hlásit do různých částí systému znovu (vícekrát).

Předpokladem je, že systém bude ukládat data do dvou umístění, v nichž budou data chráněna před neoprávněným přístupem standardními prostředky samotného systému.

7.2 Požadavky na dokumentaci

Vzniklá dokumentace k sandboxu bude obsahovat:

- provozní dokumentaci / administrátorská dokumentace,
- technickou dokumentaci,
- bezpečnostní dokumentaci,
- vývojářskou a testovací dokumentaci,
- uživatelskou dokumentaci,
- architektonickou dokumentaci a dokumentaci designu,
- testovací scénáře včetně ověření požadovaných funkcionalit a integrací,
- školící materiály.

Finální dokumentace bude předána v digitální podobě při spuštění služby v produkčním prostředí.

7.3 Požadavky na školení

Součástí školení budou školící materiály v digitální podobě. Školící materiály budou průběžně aktualizovány dle aktualizace provozních zásahů a nových rozšíření funkcí sandboxu plynoucích se změn vázaných k aktualizaci vývoje. Školení bude provedeno on-line formou, zde možnost odevzdání školících videí (manuálů), nebo on-line schůzek.

7.4 Harmonogram projektu

Fáze projektu	Milníky a jejich obsah	Doba trvání fáze	Požadovaný výstup
T1 Analýza a návrh Sandboxu	M1.1 Kick-off a potvrzení obsahu a rozsahu zakázky Zadavatelem i Dodavatelem	T0 + 1 týden	Draft analytických dokumentů – architektonická dokumentace, dokumentace designu, bezpečnostní dokumentace, provozní dokumentace

	M1.2 Předání dokumentace v českém i anglickém jazyku		
T2 Příprava testovacího a produkčního prostředí Sandboxu	M 2.1Vytvoření rolí a oprávnění pro Zadavatele M 2.2 Potvrzení zprovoznění testovacího a produkčního prostředí služby sandboxu pro Zadavatele	T1 + 1 týden	Draft dokumentace – Vývojářská a testovací dokumentace včetně testovacích scénářů, příprava testovacích / produkčních rolí, Administrátorská dokumentace
T3 Nasazení a testování Sandboxu	M 3.1 Zpřístupnění testovacího prostředí Zadavateli včetně testovacích rolí, dokumentace a scénářů M 3.2 Předání připomínek Zadavatele v testovacím prostředí Dodavateli M 3.3 Akceptace zapracování připomínek z testovacího prostředí Zadavatele Dodavatelem M 3.4 Zpřístupnění produkčního prostředí Zadavateli včetně produkčních rolí, dokumentace a scénářů M 3.5 Předání připomínek Zadavatele v produkčním prostředí Dodavateli M 3.6 Akceptace zapracování připomínek z produkčního prostředí Zadavatele Dodavatelem	T2 + 4 týdny	Sandbox nasazen na testovací prostředí Připomínkování a vyřešení připomínek k testovacímu prostředí Sandbox nasazen na produkční prostředí Aktualizace draftů dokumentace a předání finální verze Připomínkování a vyřešení připomínek k produkčnímu prostředí
T4 Akceptace Sandboxu	M 4.1 Předání aktualizované dokumentace Zadavateli M 4.2 Akceptace testovacího a produkčního prostředí	T3 + 1 týden	Seznam realizovaných výstupů Akceptace testovacího a produkčního prostředí

T5 Provoz Sandboxu	*Definováno plněním požadavků technické podpory služby*	T4 + 1 týden	Průběžná aktualizace požadované dokumentace Průběžná kooperace při provozu dle ITILu