Popis Fraud Protection

1 Popis Služby

Služba Fraud Protection je doplňkovou službou k veřejně dostupným telefonním službám (včetně části veřejně dostupných telefonních služeb, které jsou zahrnuty společně v jedné službě s jiným druhem veřejně dostupných služeb elektronických komunikací) poskytovaným poskytovatelem účastníkovi dle příslušné smlouvy a Specifikací služeb (dále také jen „telefonní služby“ nebo „služby“). Služba Fraud Protection zahrnuje soubor nástrojů a procesů poskytovatele, které umožňují účastníkovi identifikovat rizika spojená s neočekávaným telefonním provozem, který může být způsoben technickou závadou telekomunikační infrastruktury na straně účastníka, napadením a/nebo zneužitím telekomunikační infrastruktury účastníka třetí stranou nebo jejím neautorizovaným využíváním. Taková identifikace rizik umožňuje následně účastníkovi přijmout účinná opatření k minimalizaci případných škod a finančních ztrát vzniklých v souvislosti se zjištěným neočekávaným telefonním provozem.

Služba Fraud Protection (popř. její jednotlivé moduly) je poskytována pouze na základě a v souladu s tímto platným Popisem služby Fraud Protection a na základě a v souladu s příslušnou Specifikací služby Fraud Protection uzavřenou mezi poskytovatelem a účastníkem, není-li dále v tomto dokumentu uvedeno, že určitý modul služby Fraud Protection lze sjednat i v příslušné Specifikaci služby definující konkrétní veřejně dostupnou telefonní službu.

1.1 Moduly služby Fraud Protection

Služba Fraud Protection zahrnuje následující dílčí moduly ochrany účastníka, které lze aktivovat samostatně nebo v kombinacích podle typu a charakteru užívaní telefonní služby:

- Monitoring provozu
- ECD – detekce extrémně dlouhých hovorů
- Blacklist rizikových destinací

Konkrétní rozsah aktivovaných modulů služby Fraud Protection a jejich nastavení je uvedeno v příslušné Specifikaci služby Fraud Protection a/nebo v příslušné Specifikaci služby definující konkrétní veřejně dostupnou telefonní službu.

1.2 Monitoring provozu

Princip ochrany účastníka v rámci modulu monitoringu provozu je založen na vytvoření statistického profilu provozu účastníka a jeho automatickém porovnávání s aktuálním denním provozem účastníka. V rámci modulu monitoringu provozu jsou poskytovatelem zpracovávána pouze data, která se standardně užívají pro vyúčtování veřejně dostupných telefonních služeb účastníkům. Tento modul lze poskytovat pouze na základě podepsané Specifikace služby Fraud Protection.

1.2.1 Definice statistického profilu provozu

Statistický profil provozu je sestaven buď automaticky na základě historických dat o provozu účastníka s následnou pravidelnou aktualizací 1x měsíčně (tzv. dynamický profil), nebo ručně dle konkrétních požadavků účastníka (tzv. statický profil).
Do statistického profilu provozu lze zahrnout služby v jednom z následujících rozsahů:

- veškeré telefonní služby účastníka poskytované na základě příslušné smlouvy
- veškeré telefonní služby účastníka poskytované na základě smlouvy pod jedním zákaznickým číslem
- vybrané konkrétní telefonní služby účastníka

Dynamický profil provozu je definován v detailu na skupiny směrů volání:

- ČR pevné a mobilní sítě
- ČR Audiotex
- Mezinárodní 1
- Mezinárodní 2
- Mezinárodní 3
- Mezinárodní 4
- Mezinárodní rizikové

Hodnoty ve výše uvedeném členění jsou nastaveny samostatně pro pracovní a nepracovní dny.
Skupiny směrů zahrnují dílčí směry volání. Konkrétní zařazení dílčích směrů volání do skupin je uvedeno v dokumentu „FP – definice skupin směrů volání“, který je přílohou tohoto Popisu služby. Tento dokument „FP – definice skupin směrů volání“ je poskytovatel oprávněn kdykoliv jednostranně aktualizovat.

1.2.2 Statický profil provozu

Účastníkem ručně definovaný statický profil provozu lze definovat v detailu na skupiny směrů volání jako u dynamického profilu provozu. Ruční definice se uvádí na příslušném formuláři, který je přílohou Specifikace služby Fraud Protection. Statický profil provozu není systémem pravidelně aktualizován. Případné změny statického profilu provozu je účastník oprávněn objednat prostřednictvím změnové Specifikace služby Fraud Protection. Takto požadované změny statického profilu provozu se uplatní od prvního dne kalendářního měsíce následujícího po doručení platné změnové Specifikace služby Fraud Protection poskytovateli, pokud je ovšem Specifikace služby Fraud Protection doručena poskytovateli nejpozději 10 pracovních dní před koncem kalendářního měsíce, jinak vstupuje v účinnost až od 1. dne druhého kalendářního měsíce následujícího po doručení takové Specifikace služby Fraud Protection poskytovateli.

1.2.3 Algoritmus vyhodnocení rizika

Vyhodnocení rizika probíhá na denní bázi, kdy jsou systémem automaticky zpracovávána data o aktuálním provozu účastníka a porovnávána s definovaným statistickým profilem provozu (dynamickým nebo statickým) účastníka. Práh rizika je odvozen z profilu provozu s přihlédnutím k rozptylu hodnot denního objemu provozu a se zahrnutím minimálních hodnot pro skupiny směrů volání. Pro dynamický profil jsou tyto hodnoty nastaveny systémem na základě historie provozu účastníka a pro statický profil jsou definovány účastníkem v rámci definice profilu dle příslušné Specifikace služby Fraud Protection. Detailní algoritmus vytvoření prahu rizika je z důvodu bezpečnosti systému obchodním tajemstvím poskytovatele. Účastník má však možnost ověřit aktuální hodnotu nastavení prahu rizika prostřednictvím on-line reportingu (viz článek 1.2.6 tohoto Popisu služby).

Popis Fraud Protection

1.2.4 Notifikace alarmů

Pokud systém poprvé v daném zúčtovacím období vyhodnotí překročení prahu rizika, je automaticky vytvořen alarm, který je v dále definované garantované době, odeslán na kontakty účastníka definované v příslušné Specifikaci služby Fraud Protection prostřednictvím e-mailu a/nebo SMS zprávy, popř. i jinak, např. telefonicky. Záznam o alarmu je také zaznamenán do databáze alarmů u poskytovatele.
Pokud již v daném zúčtovacím období došlo k alespoň jednomu případu překročení prahu rizika s následnou notifikací alarmu, je po zbytek daného zúčtovacího období odesílána notifikace alarmů pouze v případě, že aktuální výše provozu způsobí překročení prahu rizika o více jak 30 procent ve srovnání s maximální hodnotou překročení prahu rizika v daném zúčtovacím období.
Notifikační SMS obsahuje upozornění na zjištění neočekávaného nárůstu telefonního provozu účastníka (zjištění rizika).
Notifikační e-mail obsahuje:

- upozornění na zjištění neočekávaného nárůstu telefonního provozu účastníka (zjištění rizika)
- skupinu směrů, kde došlo k detekci rizika
- aktuální objem provozu na dané skupině směrů (v Kč v okamžiku vyhodnocení překročení prahu rizika s uvedením dne a času)
- Za řádné odeslání alarmu účastníkovi je též považováno i jakékoliv jiné doručení informace o překročení prahu rizika ú častníkovi (např. telefonicky).

1.2.5 Postup řešení rizikového stavu

Pokud účastník obdrží notifikaci (alarm), případně jiným způsobem zjistí vznik podezřelého telefonního provozu, a vyhodnotí takový provoz jako nežádoucí, je povinen přijmout taková opatření, která účinně zabrání vzniku škod způsobených nežádoucím provozem nebo které vzniklé škody minimalizují. Pokud účastník nemá možnost omezit takový telefonní provoz okamžitým zásahem na své straně (např. zablokováním provozu na pobočkové telefonní ústředně, odpojením telefonního zařízení apod.) kontaktuje neprodleně Zákaznickou linku poskytovatele s žádostí o součinnost při řešení rizikového stavu. Po vzájemné dohodě mezi účastníkem a poskytovatelem přikročí poskytovatel k zablokování podezřelého telefonního provozu svými technickými prostředky, případně přijme jiná opatření výslovně dohodnutá mezi poskytovatelem a účastníka.

1.2.6 Reporting

Reporting k modulu monitoringu provozu je dostupný prostřednictvím zabezpečené on-line aplikace Webcare. Aplikace nabízí:

- aktuální report modulu monitoringu provozu
- detailní výpisy volání jednotlivých telefonních služeb
- aktuální data a základní statistiky provozu vč. grafického zobrazení

1.3 ECD – detekce extrémně dlouhých hovorů

Modul ECD sleduje délku jednotlivých souvislých hovorů a porovnává ji s maximální délkou, která je definována pro daný typ hovoru poskytovatelem. V případě překročení maximální délky hovoru, je hovor automaticky v následujících 60 minutách přerušen veřejnou telefonní ústřednou poskytovatele.

1.3.1 Definice povolené délky hovoru

Modul ECD je standardně aktivován pro každou nově zřízenou veřejně dostupnou telefonní službu v síti poskytovatele. Pro jednotlivé typy hovorů jsou nastaveny defaultní hodnoty maximální délky hovoru. Konkrétní hodnoty nejsou z důvodu bezpečnosti systému zveřejňovány, ale poskytovatel je sdělí účastníkovi na vyžádání.
Účastník má možnost prostřednictvím Specifikace služby Fraud Protection nebo Specifikace služby definující konkrétní veřejně dostupnou telefonní službu individuálně:

- zkrátit nebo prodloužit maximální délku hovoru pro jednotlivé typy hovorů, přičemž minimální hodnota je 120 minut.
- deaktivovat modul ECD pro konkrétní telefonní službu účastníka.

1.4 Blacklist rizikových destinací

Modul Blacklist rizikových destinací je realizován prostřednictvím funkce veřejné ústředny poskytovatele OCB-NC (blokování odchozích hovorů řízené sítí).

1.4.1 Definice rizikových destinací

Rizikové destinace jsou definovány v rámci speciálních profilů OCB-NC v těchto volitelných variantách:

- rizikové zahraniční destinace
- rizikové zahraniční destinace + národní audiotex (90x, 976)

Seznam rizikových destinací je poskytovatelem průběžně aktualizován na základě aktuálních informací poskytovatele o pokusech podvodných volání a zneužití infrastruktury účastníků v síti poskytovatele nebo z jiných dostupných zdrojů a s přihlédnutím k charakteru obvyklého provozu do dané destinace. Aktuální seznam destinací zařazených mezi rizikové je účastníkovi k dispozici na vyžádání.
Blacklist rizikových destinací lze aktivovat pro jednotlivou veřejně dostupnou telefonní službu účastníka poskytovanou dle příslušné Specifikace služby, a to buď vyznačením požadavku v příslušné Specifikaci služby Fraud Protection, nebo vyznačením požadavku v příslušné Specifikaci služby definující konkrétní veřejně dostupnou telefonní službu.

1.4.2 Omezení provozu

V případě aktivního blacklistu rizikových destinací jsou v síti poskytovatele blokována veškerá volání z veřejně dostupné telefonní služby účastníka do destinací zařazených mezi rizikové destinace u takové služby.
U služeb založených na volbě a předvolbě operátora (CS, CPS) je omezení provozu účinné pouze na hovory realizované prostřednictvím veřejné telefonní sítě poskytovatele. Poskytovatel nemůže ovlivnit telefonní provoz účastníka realizovaný prostřednictvím jiných veřejných telefonních sítí.

Popis Fraud Protection

2 Odpovědnosti poskytovatele a účastníka související s poskytováním/užíváním služby Fraud Protection

2.1 Zabezpečení telekomunikační infrastruktury účastníka

Služba Fraud Protection umožňuje účastníkovi identifikovat rizika spojená s neočekávaným telefonním provozem, který může být způsoben technickou závadou telekomunikační infrastruktury na straně účastníka, napadením a/nebo zneužitím telekomunikační infrastruktury účastníka třetí stranou nebo jejím neautorizovaným využíváním. Taková identifikace rizik umožňuje následně účastníkovi přijmout účinná opatření k minimalizaci případných škod a finančních ztrát vzniklých v souvislosti se zjištěným neočekávaným provozem.
Zodpovědnost za provoz a řádné zabezpečení komunikační infrastruktury a/nebo telekomunikačních zařízení účastníka je však vždy plně na straně účastníka, poskytovatel nenese žádnou odpovědnost za provoz a řádné zabezpečení telekomunikačních zařízení účastníka.
Účastník je vždy povinen přijmout na své straně taková opatření, která zabrání zneužití jeho komunikační infrastruktury a/nebo telekomunikačních zařízení. Mezi taková opatření patří zejména:

- zabezpečení přístupu k pobočkové telefonní ústředně
- dle možností účastníka nastavení povolených/zakázaných směrů volání s využitím funkcí pobočkové telefonní ústředny účastníka a/nebo prostřednictvím doplňkových služeb poskytovatele dle Popisu služby příslušné telefonní služby poskytovatele
- dle možností účastníka omezit přístup uživatelů k funkcím jako je přesměrování mimo pobočkovou ústřednu, přidržení hovoru (HOLD), vzdálený přístup k ústředně apod.
- neustálé aktivní sledování objemu a charakteru telefonního provozu (např. prostřednictvím aplikace Webcare a/nebo prostřednictvím nástrojů pobočkové ústředny účastníka)

2.1.1 Ochrana IP pobočkových ústředen

Každé zařízení, připojené k veřejnému internetu, se nachází pod hrozbou jeho zneužití. Z hlediska telefonních služeb se toto riziko týká především VoIP hlasových bran a pobočkových ústředen. Poskytovatel nedoporučuje připojování těchto zařízení k veřejnému internetu, nicméně pokud je to z hlediska komunikačních potřeb účastníka nezbytné, je nutné provést účinná zabezpečení těchto zařízení na straně účastníka. Poskytovatel nemůže zabránit napadení těchto zařízení, které jsou ve správě účastníka, přičemž za případné zneužití těchto zařízení nenese poskytovatel žádnou odpovědnost.
Poskytovatel doporučuje zejména tyto způsoby zabezpečení VoIP zařízení účastníka:

- připojení do sítě přes privátní IP adresy
- zakázat nepoužívané služby a protokoly
- omezit přístup z internetu k VoIP bránám
- definovat přísný dial plan brány (dle podmínek účastníka)
- sledovat notifikace typu “security issues” od výrobce zařízení, plnit doporučené pokyny a pravidelně upgradovat firmware

2.1.2 Vyloučení odpovědnosti poskytovatele

Poskytovatel nenese žádnou odpovědnost za provoz či řádné zabezpečení telekomunikačních zařízení a sítí (včetně IP pobočkových ústředen) účastníka, resp. za zneužití těchto telekomunikačních zařízení a sítí účastníka. Poskytovatel nenese žádnou odpovědnost za případně vzniklý neočekávaný provoz. Poskytovatel nenese žádnou odpovědnou za škody a finanční ztráty vzniklé v souvislosti s tím, že účastník řádně nezabezpečil svá telekomunikační zařízení. Poskytovatel rovněž nenese žádnou odpovědnost za případné škody a/nebo finanční ztráty vzniklé v souvislosti s neočekávaným provozem, zejména však nenese odpovědnost za případné škody a/nebo finanční ztráty vzniklé tím, že účastník nepřijal účinná a/nebo včasná opatření k minimalizaci těchto škod a/nebo finančních ztrát.

2.2 Garantované parametry monitoringu provozu a s tím související smluvní sankce

Účastníkovi užívajícímu službu Fraud Protection na základě příslušné platné smlouvy a specifikace služby Fraud Protection garantuje poskytovatel v rámci modulu monitoringu provozu odeslání informace (alarmu) o vzniku rizikového provozu do 24 hodin od okamžiku překročení prahu rizika, a toza podmínek dle článku 1.2.4 tohoto Popisu služby Fraud Protection (dále jen „garantovaná doba alarmu“).
Pokud dojde k prodlení s odesláním alarmu v garantované době alarmu, je účastník oprávněn uplatnit vůči poskytovateli smluvní sankci ve výši dle následující tabulky:

Skutečná doba odeslání alarmu (od okamžiku překročení aktuálního prahu rizika)	Smluvní sankce
Do 24 hodin (tzn. bez prodlení s odesláním alarmu, resp. alarm je odeslán v garantované době alarmu)	Bez smluvní sankce
Nad 24 hodin - do 48 hodin	Smluvní sankce (ve formě slevy) ve výši **50 %** vyúčtované ceny za fraudulentní provoz [1] vyúčtovaný za časový úsek mezi garantovanou dobou odeslání alarmu (tzn. do 24 hodin) a skutečnou dobou odeslání alarmu.
Více než 48 hodin	Smluvní sankce (ve formě slevy) ve výši **80 %** vyúčtované ceny za fraudulentní provoz [1] vyúčtovaný za časový úsek mezi garantovanou dobou odeslání alarmu (tzn. do 24 hodin) a skutečnou dobou odeslání alarmu.

Popis Fraud Protection

1) Fraudulentním provozem se pro účely výpočtu sankce dle předchozí tabulky rozumí poskytovatelem a účastníkem vzájemně odsouhlasený typ telefonního provozu definovaný vazbou číslo volajícího (A-číslo) a číslo volaného (B-číslo), který byl identifikován jako jednoznačný zdroj neočekávaného zvýšení provozu účastníka v příslušném časovém úseku.
V případě nesplnění garantované doby alarmu ze strany poskytovatele má účastník právo uplatnit vůči poskytovateli smluvní sankce stanovené ve výše uvedené tabulce. Účastník v takovém případě požádá poskytovatele písemně o uplatnění smluvní sankce prostřednictvím reklamačního řízení v souladu s článkem 4 tohoto Popisu služby Fraud Protection, přičemž tento nárok je účastník oprávněn uplatnit nejpozději do dne uplynutí reklamační lhůty stanovené pro uplatnění reklamace vůči vyúčtování příslušné služby za dané zúčtovací období, u které v daném zúčtovacím období nebyla splněna garantovaná doba alarmu dle tohoto článku. Pokud účastník nárok na příslušnou smluvní sankci neuplatní ve lhůtě uvedené v předchozí větě, tak jeho nárok na smluvní sankci dle tohoto článku navždy zanikne.

3 Zřízení a změny služby

3.1 Zřízení služby

Služba Fraud Protection se zřizuje jako doplňková služba k existujícím veřejně dostupným telefonním službám poskytovaným poskytovatelem účastníkovi na základě smlouvy a příslušné Specifikace služby definující konkrétní veřejně dostupnou telefonní službu. Modul monitoringu provozu je zřízen od prvního dne následujícího kalendářního měsíce po doručení platné Specifikace služby Fraud Protection poskytovateli, pokud je ovšem Specifikace služby Fraud Protection doručena poskytovateli nejpozději 10 pracovních dní před koncem kalendářního měsíce, jinak vstupuje v účinnost až od 1. dne druhého kalendářního měsíce následujícího po doručení takové Specifikace služby Fraud Protection poskytovateli. V případě dynamického statistického profilu monitoringu provozu je doporučeno zřízení služby Fraud Protection nejdříve k 1. dni následujícího měsíce po zřízení telefonních služeb zahrnutých do monitoringu provozu.
Modul ECD – detekce extrémně dlouhých hovorů je ve standardním nastavení aktivován (zřízen) automaticky současně se zřízením příslušné veřejně dostupné telefonní služby. V případě jiného nastavení modulu ECD dle požadavku účastníka je tento modul aktivován (zřízen) zpravidla do 5 pracovních dní ode dne platného objednání takového modulu prostřednictvím Specifikace služby Fraud Protection nebo Specifikace služby definující konkrétní veřejně dostupnou telefonní službu, nikoliv však dříve než se zřízením příslušné veřejně dostupné telefonní služby, ke které se má tento modul vztahovat.
Modul Blacklist rizikových destinací je aktivován (zřízen) zpravidla do 5 pracovních dní ode dne platného objednání takového modulu prostřednictvím Specifikace služby Fraud Protection nebo Specifikace služby definující konkrétní veřejně dostupnou telefonní službu, nikoliv však dříve než se zřízením příslušné veřejně dostupné telefonní služby, ke které se má tento modul vztahovat.
Ceny za poskytování služby Fraud Protection, resp. za jednotlivé moduly služby Fraud Protection, jsou stanoveny v platném Ceníku služby Fraud Protection, není-li cena služby Fraud Protection výslovně smluvními stranami sjednána jinak.

3.2 Změny služby

Změnu parametrů nebo konfigurace služby Fraud Protection účastník objednává u poskytovatele prostřednictvím příslušné (změnové) Specifikace služby Fraud Protection nebo, pokud je to pro daný modul možné, prostřednictvím (změnové) Specifikace příslušné veřejně dostupné telefonní služby. Změny parametrů služby Fraud Protection jsou zpoplatněny dle platného Ceníku služby Fraud Protection, není-li cena za změnu služby Fraud Protection smluvními stranami výslovně sjednána jinak.
Změny modulu ECD (např. zkrácení nebo prodloužení délky hovoru nebo deaktivace modulu ECD) jsou poskytovatelem provedeny zpravidla do 5 pracovních dní ode dne platného objednání takové změny prostřednictvím Specifikace služby Fraud Protection nebo Specifikace služby definující konkrétní veřejně dostupnou telefonní službu.
Změny modulu Blacklist rizikových destinací jsou poskytovatelem provedeny zpravidla do 5 pracovních dní ode dne platného objednání takové změny prostřednictvím Specifikace služby Fraud Protection nebo Specifikace služby definující konkrétní veřejně dostupnou telefonní službu.

4 Reklamace služby

„Oddělení péče o zákazníky“ je dostupné 24 hodin denně, 365 dní v roce a hovory jsou vyřizovány nepřetržitě. Pro urychlení odstranění závady/reklamace služby Fraud Protection poskytovatel požaduje, aby jej účastník kontaktoval již při prvních známkách závady. Hlášení závady/reklamace služby Fraud Protection je povinen účastník provést telefonicky na pracoviště „Oddělení péče o zákazníky“ poskytovatele. Kontakt je specifikován ve smlouvě. Informace účastníka (hlášení) o závadě/reklamaci služby Fraud Protection musí obsahovat zejména:

- identifikace účastníka (název, IČ, číslo účastníka nebo číslo smlouvy mezi poskytovatelem a účastníkem);
- popis závady/reklamace;
- datum a čas vzniku závady;
- jméno a příjmení osoby jednající jménem účastníka a jeho telefonické spojení.

„Oddělení péče o zákazníky“ podnikne potřebné kroky k odstranění závady/reklamace služby Fraud Protection. Účastníkovi bude přiděleno číslo závady, které bude používat při následných kontaktech, aby bylo možno správně sledovat postup opravy. Reklamace služby Fraud Protection se dále řídí Reklamačním řádem poskytování veřejně dostupné služby elektronických komunikací.