Provozní řád ISDS

Zpracoval: Ing. Pavel Tesař, projektový manažer ISDS

Schválil: Ing. Ondřej Menoušek, vedoucí projektu ISDS

Ministerstvo vnitra ČR

Datum schválení: 2. 9. 2022

Provozní řád informačního systému datových schránek (ISDS)

Verze k 4. 9. 2022

Provozní řád ISDS je souhrn ustanovení a pravidel vybraných z dokumentů, kterými se řídí Ministerstvo vnitra ČR a spolupracující subjekty a které jsou závazné pro provoz ISDS.

ISDS je zřízen a provozován na základě zákona č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, ve znění pozdějších předpisů, (dále jen „Zákon“). Jeho správcem je Ministerstvo vnitra ČR. Provozovatelem ISDS je držitel poštovní licence, Česká pošta, s.p.

ISDS je informačním systémem veřejné správy ve smyslu zákona č. 365/2000 Sb., o informačních systémech veřejné správy, ve znění pozdějších předpisů.

Obsah

I. Úvod

1. Vymezení pojmů (abecedně)

Autentizační služba PVS

Služba ISDS, která umožňuje zaregistrovaným informačním systémům veřejné správy využívat autentizaci a identifikaci uživatelů na základě jejich uživatelských účtů v datových schránkách.

Datová schránka

Datové schránky představují elektronická úložiště, jejichž posláním je zprostředkovávat komunikaci fyzických osob, podnikajících fyzických osob a právnických osob s orgány veřejné moci a také vzájemnou komunikaci mezi samotnými fyzickými osobami, podnikajícími fyzickými osobami, právnickými osobami či orgány veřejné moci. Datová schránka je součástí ISDS.

Datová zpráva

Datovou zprávou jsou elektronická data, která lze přenášet prostředky pro elektronickou komunikaci a uchovávat na záznamových médiích, používaných při zpracování a přenosu dat elektronickou formou. Ve smyslu nařízení Evropského Parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen Nařízení eIDAS) se jedná o data v elektronické podobě, zejména jako text nebo zvuková, vizuální nebo audiovizuální nahrávka.

Dotovaná datová zpráva

Uživatel datové schránky, případně jiný subjekt, může určit, že bude hradit veškeré Poštovní datové zprávy odeslané z datové schránky jiného uživatele. Obchodní název této služby je Dotovaná datová zpráva.

eObčanka

eObčanka je občanský průkaz s kontaktním elektronickým čipem, který umožňuje online prokazování totožnosti a uložení kvalifikovaných a autentizačních certifikátů. Je to též obslužná aplikace pro používání elektronického občanského průkazu (middleware, ovladač eOP).

Informační systém veřejné správy (též ISVS)

Informační systém ve smyslu § 2 písm. b), zákona č. 365/2000 Sb., o informačních systémech veřejné správy.

Identita občana

Identita občana slouží jako nástroj pro bezpečné a zaručené ověření totožnosti uživatele online služeb veřejné správy. k prokazování totožnosti online slouží různé identifikační prostředky, jejichž poskytovatelé získali akreditaci a jsou napojeni na Národní bod pro identifikaci a autentizaci., označovaný též jako NIA.

ISDS

Informační systém datových schránek zajišťuje bezpečnou a průkaznou elektronickou komunikaci mezi orgány veřejné moci (dále též „OVM“) na straně jedné a fyzickými či právnickými osobami na straně druhé, jakož i mezi OVM a všemi typy subjektů navzájem.

JIP

Jednotný identitní prostor, zabezpečená adresářová služba obsahující údaje pro autentizaci a autorizaci uživatelů, provozovaná MV ČR jakou součást služeb Czech POINT.

Kontaktní místo veřejné správy

Kontaktním místem veřejné správy je dle § 8a odst. 1 a 2 zákona č. 365/2000 Sb., pracoviště Czech POINT (Český podací ověřovací informační národní terminál). Seznam pracovišť je uveden na webu https://www.czechpoint.cz/public/.

Mobilní klíč eGovernmentu

Aplikace Mobilní klíč umožňuje jednoduché a rychlé přihlášení do ISDS bez nutnosti zadávat složité jméno a heslo. Multi-faktorová autentizace pomocí mobilního telefonu nebo tabletu na platformě iOS či Android zároveň zvyšuje úroveň zabezpečení uživatelského účtu.

Odesílací brána

Součást aplikačního rozhraní ISDS, umožňující registrované externí webové aplikaci připravit koncept datové zprávy, který následně může uživatel ISDS po úspěšné autentizaci odeslat.

Odpovědní datová zpráva

Uživatel datové schránky může určit, že bude hradit dodání dokumentu, který je odpovědí na jeho Poštovní datovou zprávu. Obchodní název této služby je Odpovědní datová zpráva.

Orgán veřejné moci

Podle § 1 odst. 1 Zákona se tímto rozumí státní orgány, územní samosprávné celky a fyzické nebo právnické osoby, pokud těmto fyzickým nebo právnickým osobám byla svěřena působnost v oblasti veřejné správy. Zdrojem referenčního údaje o tom, zda je daný subjekt orgánem veřejné moci, je Rejstřík orgánů veřejné moci a soukromoprávních uživatelů údajů, viz § 52b zákona č. 111/2009 Sb., o základních registrech.

Poštovní datová zpráva (PDZ)

Obchodní označení pro zprávy přenesené v rámci komerčního provozu dle § 18a Zákona. Poštovní datové zprávy dodané do konce roku 2021 jsou doručovány okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k tomuto dokumentu. PDZ dodané od 1. ledna 2022 začnou být doručovány buď okamžikem, kdy se do datové schránky přihlásí osoba, která má s ohledem na rozsah svého oprávnění přístup k tomuto dokumentu nebo desátým dnem od dodání, tedy shodně jako běžné datové zprávy.

Provozovatel

Držitel poštovní licence ve smyslu Zákona (Česká pošta, s.p.).

Přístupové rozhraní

Přístupové rozhraní pro poskytovatele internetových služeb provozované jako součást ISDS na základě zmocnění v § 14a Zákona. Přístupové rozhraní může využívat jen osoba, které bylo vydáno povolení k využívání těchto služeb.

Portál veřejné správy (dále též PVS)

Portál veřejné správy slouží především k zajištění přístupu k informacím a pro zveřejňování informací souvisejících s výkonem veřejné správy. PVS je místem, kam mohou orgány veřejné moci automatizovaným způsobem umisťovat jak zákonem stanovené, tak nad rámec zákona vydávané informace a dokumenty. Dále PVS zajišťuje komunikaci uživatelů s orgány veřejné moci prostřednictvím datových schránek a prostřednictvím kontaktních míst veřejné správy Czech POINT.

Rejstřík orgánů veřejné moci a soukromoprávních uživatelů údajů

Součást Registru práv a povinností. Obsahuje referenční údaje o tom, které subjekty jsou ve smyslu zákona o základních registrech i datových schránek orgánem veřejné moci.

Seznam držitelů datových schránek

Plným názvem „Seznam fyzických osob, podnikajících fyzických osob, právnických osob a orgánů veřejné moci, které mají zřízenu a zpřístupněnu datovou schránku“, viz § 14b Zákona.

Spisová služba

Ve smyslu zákona č. 499/2004 Sb., o archivnictví a spisové službě, ve znění pozdějších předpisů, jsou veřejnoprávní původci mimo jiné povinni vést evidenci spisů buď písemnou formou, nebo elektronickou formou za použití výpočetní techniky. ISDS umožňuje napojení elektronické spisové služby pomocí definovaného rozhraní (viz Technická příloha 2).

Správce

Ministerstvo vnitra ČR jako správce ISDS ve smyslu § 14 odst. 2 ve spojení s § 2 odst. 2 Zákona a § 2 písm. c) zákona č. 365/2000 Sb.

Systémová datová zpráva

Specifický typ datové zprávy, odeslané buď ze systémové schránky Správce (aaaaaaa) nebo Provozovatele (zzzzzzq). Slouží k notifikaci o důležitých změnách služeb ISDS, je posílána při vybraných událostech, týkajících se datové schránky, a také jako „uvítací“ zpráva pro nové uživatele. Přehled systémových datových zpráv i příslušných událostí je uveden v Technické příloze 2, v dokumentu WS_Manipulace_s_datovymi_zpravami.pdf.

2. Odkazy

eObčanka

https://info.identitaobcana.cz/eop/

Informační systém registru práv a povinností (AIS RPP působnostní)

https://rpp-ais.egon.gov.cz/AISP/verejne/domu

Informační web datových schránek

https://info.mojedatovaschranka.cz/

Klientský portál datových schránek (ISDS)

https://www.mojedatovaschranka.cz/

Mobilní klíč eGovernmentu

iOS: https://apps.apple.com/cz/app/mobiln%C3%AD-kl%C3%ADč-isds/id1466762017

Android: https://play.google.com/store/apps/details?id=cz.mojedatovaschranka.mobilniklic

Identita občana

https://www.identitaobcana.cz/Home

Podmínky pro využívání přístupového rozhraní

http://www.mvcr.cz/soubor/vestnik-mv-castka-43-2012.aspx

Portál veřejné správy

https://portal.gov.cz/

Rejstřík orgánů veřejné moci a soukromoprávních uživatelů údajů

https://rpp-ais.egon.gov.cz/AISP/verejne/domu

Seznam držitelů datových schránek

https://www.mojedatovaschranka.cz/sds/searchForm.do

Správa dat Seznamu orgánů veřejné moci

https://www.czechpoint.cz/spravadat/

Testovací prostředí pro dodavatele aplikací třetích stran

https://www.czebox.cz/

Veřejné interaktivní testovací prostředí

http://www.isdstest.cz/

II. Informační systém datových schránek

1. Datová schránka

Zřízení datové schránky

Orgánům veřejné moci, právnickým osobám zapsaným v obchodním rejstříku, právnickým osobám zřízeným ze zákona a dále vybraným profesním skupinám podnikajících fyzických osob (advokáti, daňoví poradci, insolvenční správci, statutární auditoři, znalci, soudní překladatelé a tlumočníci) je datová schránka zřízena automaticky ze Zákona. o zřízení datové schránky mohou Správce požádat fyzické osoby, podnikající fyzické osoby a právnické osoby nezapsané v obchodním rejstříku. Náležitosti žádosti definuje Zákon v § 3 odst. 3 a 4 (fyzické osoby), § 4 odst. 4 a 5 (podnikající fyzické osoby) a § 5 odst. 4 a 5 (právnické osoby nezapsané v obchodním rejstříku).

Žádost o zřízení datové schránky lze podat následujícími způsoby:

a) Na kontaktním místě veřejné správy (pracoviště Czech POINT). v tomto případě není nutné žádost opatřovat úředně ověřeným podpisem (viz § 27 odst. 3 Zákona).
b) Vyplněním formuláře žádosti, jeho vytištěním, opatřením úředně ověřeným podpisem a zasláním na poštovní adresu podatelny Správce.
c) Online v prostředí klientského portálu ISDS po přihlášení Identitou občana. Zřízení je možné, pokud se uživatel přihlásil pomocí elektronického prostředku pro identifikaci s minimální úrovní důvěry „značná“. Tato varianta platí jen pro fyzické osoby a podnikající fyzické osoby.

Pokud žádost obsahuje všechny zákonné náležitosti a zároveň (v případě fyzické osoby a podnikající fyzické osoby) byla osoba žadatele jednoznačně ztotožněna (pozn.: identifikace držitele datové schránky primárně probíhá vůči registru obyvatel), Správce zřídí Datovou schránku do 3 pracovních dnů od přijetí žádosti. Přístupové údaje jsou následně žadateli zaslány do jeho datové schránky fyzické osoby jako datová zpráva do vlastních rukou, případně poštovní zásilkou do vlastních rukou výhradně jen adresáta nebo jsou vydány formou tzv. virtuální obálky (viz oddíl Přístupové údaje pro oprávněné osoby datových schránek). Do datové schránky fyzické osoby logicky nemohou být doručovány přístupové údaje náležící k účtu samotného držitele této schránky.

V případě žádosti podané online po přihlášení Identitou občana je datová schránka zřízena i zpřístupněna bezodkladně. Přístupové údaje jsou žadateli vydány teprve na jeho výslovnou žádost, protože přístup do schránky již má zajištěn pomocí Identity občana.

V případě žádosti o zřízení datové schránky právnické osoby nezapsané v obchodním rejstříku, je nutné, aby bylo doloženo, že žadatel je oprávněn za tuto právnickou osobu jednat. Tento doklad není Správcem vyžadován, pokud je osoba žadatele uvedena ve veřejném rejstříku dostupném dálkově (např. RES, ARES apod.)

V opačném případě vyzve Správce žadatele k zaslání kompletně vyplněné žádosti, případně k doplnění údajů.

Zřízení další datové schránky Orgánu veřejné moci dle § 6 Zákona

Další datová schránka orgánu veřejné moci se zřizuje zejména pro potřebu vnitřní organizační jednotky orgánu veřejné moci nebo výkonu konkrétní agendy nebo činnosti orgánu veřejné moci. Žádost zašlete do datové schránky Ministerstva vnitra v podobě běžného úředního dopisu. Náležitosti žádosti jsou:

- název další datové schránky,

- kompletní adresní údaje ve struktuře dle § 6 Vyhlášky č. 359/2011 Sb., o základním registru územní identifikace, adres a nemovitostí,
- osobní údaje fyzické osoby, která bude zavedena jako oprávněná v této další schránce a to buď:
    - jméno, příjmení, číslo občanského průkazu,
    - jméno, příjmení, datum narození, místo narození, stát narození.

Přístupové údaje jsou odeslány poštou na adresu sídla organizační složky do vlastních rukou výhradně jen adresáta osoby uvedené v žádosti.

Zpřístupnění datové schránky

Dle § 10 odst. 2 Zákona je datová schránka zpřístupněna (aktivována) prvním přihlášením osoby uvedené v § 8 odst. 1 až 4 Zákona do datové schránky, nejpozději však patnáctým dnem po dni doručení přístupových údajů. Toto přihlášení je možné pouze prostřednictvím klientského portálu datových schránek. V případě žádosti podané online po přihlášení Identitou občana je datová schránka zřízena i zpřístupněna bezodkladně.

Znepřístupnění datové schránky na žádost

Subjekty, kterým byla datová schránka zřízena na žádost, mohou také požádat o její znepřístupnění. Žádost o znepřístupnění datové schránky lze podat následujícími způsoby:

a) Na kontaktním místě veřejné správy (pracoviště Czech POINT). v tomto případě není nutné žádost opatřovat úředně ověřeným podpisem (viz § 27 odst. 3 Zákona).
b) Odesláním žádosti opatřené ověřeným podpisem na poštovní adresu podatelny Správce.
c) Odesláním žádosti do datové schránky Správce.
d) Zadáním požadavku v prostředí klientského portálu ISDS po přihlášení Identitou občana.

Správce znepřístupní Datovou schránku do 3 pracovních dnů od přijetí žádosti.

Znepřístupnění datové schránky ze zákona

Subjekty uvedené v § 16 Zákona (věznice, vazební věznice, detenční ústavy, soudy) oznamují změny způsobující znepřístupnění datové schránky pomocí rozhraní pro poskytovatele dat, popsaného v Technické příloze 3, případně pomocí Portálu pro poskytovatele dat. Dle povahy nastalé události mají možnost zadat ohlášení vedoucí buď k dočasnému nebo trvalému znepřístupnění datové schránky.

Zrušení datové schránky

Datovou schránku zruší Správce 3 roky po zániku subjektu, pro který byla zřízena, viz § 13 Zákona. Záznamy o přenesených zprávách (obálky těchto zpráv bez příloh) uchovává ISDS trvale.

Žádost o povolení příjmu Poštovních datových zpráv

Žádost o umožnění dodávání Datových zpráv dle § 18a odst. 1 Zákona lze podat následujícími způsoby:

a) Zaškrtnutím příslušné volby v prostředí administrativní části klientského portálu ISDS. Po odeslání žádosti je dodávání Poštovních datových zpráv povoleno ihned, bez dalšího schvalování Správcem.
b) Na kontaktním místě veřejné správy (pracoviště Czech POINT).

Všechny datové schránky fyzických osob, podnikajících fyzických osob a právnických osob (včetně podtypů) jsou iniciálně nastaveny tak, aby do nich bylo možné dodávat PDZ. Možnost ukončit či následně povolit příjem PDZ zůstává výhradně držitelům datových schránek fyzických osob.

Žádost o ukončení povolení příjmu Poštovních datových zpráv

Žádost o ukončení povolení dodávání datových zpráv dle § 18a odst. 1 Zákona lze podat následujícími způsoby:

a) Zaškrtnutím příslušné volby v prostředí administrativní části klientského portálu ISDS. Po odeslání žádosti je dodávání Poštovních datových zpráv ukončeno ihned, bez dalšího schvalování Správcem.
b) Na kontaktním místě veřejné správy (pracoviště Czech POINT).

Příjem PDZ si mohou na žádost ukončit pouze držitelé datových schránek fyzické osoby.

Odesílání Poštovních datových zpráv

Odesílání Poštovních datových zpráv je službou České pošty s.p. Zájemce o tuto službu musí kontaktovat Českou poštu s.p., například pomocí klientské zóny na www.cpost.cz.

2. Přístupové údaje

Přístupové údaje pro oprávněné osoby datových schránek

Oprávněným osobám (uživatelům), kterým byly vytvořeny účty v datové schránce, jsou zasílány přístupové údaje buď datovou zprávou do datové schránky fyzické osoby, případně listovní zásilkou nebo vydány tzv. virtuální obálkou. Pro všechny typy uživatelů (kromě držitele datové schránky fyzické osoby samotného) platí, že primární variantou představuje doručení přístupových údajů do datové schránky fyzické osoby ve formě datové zprávy „do vlastních rukou“.

Pokud uživatel nemá zpřístupněnou datovou schránku fyzické osoby, je využita listovní zásilka v režimu „do vlastních rukou výhradně jen adresáta“. Pravidla adresace jsou následující:

a) Fyzickým osobám a podnikajícím fyzickým osobám budou přístupové údaje zaslány na kontaktní adresu, kterou uvedou v žádosti o zřízení datové schránky. Pokud adresu pro doručení nevyplní, použije se adresa získaná z evidence obyvatel. Žadatel může zvolit pro doručení i zahraniční kontaktní adresu. Pokud se tato nachází v některé ze zemí, do kterých lze prostřednictvím Provozovatele doručovat v režimu „do vlastních rukou výhradně jen adresáta“, jsou mu následně odeslány přístupové údaje. Seznam těchto zemí je zveřejňován na informačním webu datových schránek. Pokud zvolil adresu v zemi, kam nelze doručovat v režimu do vlastních rukou výhradně jen adresáta, je mu zaslán pouze omluvný dopis s informací, jak dále postupovat.
b) Vedoucím Orgánů veřejné moci budou odeslány na adresu jejich úřadu.
c) Statutárním zástupcům právnických osob ztotožněným v registru obyvatel budou zaslány na adresu trvalého pobytu, popř. doručovací adresu uvedenou v registru obyvatel. u neztotožněných osob budou přístupové údaje zaslány na adresu trvalého pobytu uvedenou v obchodním rejstříku.
d) Alternativu vůči listovní zásilce představují přístupové údaje vydávané pro oprávněnou osobu datové schránky fyzické osoby a podnikající fyzické osoby. Pokud je žádost přijata na kontaktním místě veřejné správy, a je z pohledu ISDS úspěšně zpracována, mohou být žadateli na přání vydány přístupové údaje na místě formou tzv. virtuální obálky. Na zadaný email je zaslán odkaz směřující na aktivační portál, kde si žadatel následně vyzvedne přístupové údaje.

Dále, pokud žadatel požádá o zřízení datové schránky online, přístupové údaje jsou vydány teprve na jeho výslovnou žádost, protože přístup do schránky má již zajištěn pomocí Identity občana

Přístupové údaje vydané Správcem při zřízení datové schránky i ve všech dalších případech jsou platné pouze pro první přihlášení, kdy systém uživatele rovnou vyzve ke změně hesla, tak aby si uživatel zadal heslo vlastní. Systém může kdykoliv znovu požádat uživatele o změnu přístupového hesla. Princip změny hesla je poté stejný, jako v případě použití prvních přístupových údajů. V případě, že uživatel používá k přístupu do datové schránky jiný technický prostředek (aplikaci), zajistí systém ISDS pomocí programového rozhraní informování o okamžiku vypršení platnosti hesla a současně umožní heslo změnit bez nutnosti použít webové rozhraní. Podrobná pravidla tvorby hesla jsou popsána v Technické příloze 2 (popis služby ChangeISDSPassword).

Uživatel ISDS si může pomocí klientského portálu na vlastní riziko nastavit neomezenou platnost hesla. Takové heslo pak neexpiruje automaticky, nicméně Správci je ponechána možnost v mimořádných případech změnu hesla vynutit.

Přístupové údaje pro administrátora či pověřenou osobu

Dle § 8 odst. 6 Zákona mohou oprávněné osoby pověřit další fyzické osoby přístupem do své datové schránky, případně dle § 8 odst. 7 Zákona jmenovat administrátora s právem pověřovat další fyzické osoby k přístupu do jejich datové schránky. Žádost o vygenerování přístupových údajů pro tyto osoby lze podat následujícími způsoby:

a) Na kontaktním místě veřejné správy (pracoviště Czech POINT).
b) Vyplněním elektronického formuláře žádosti v prostředí administrativní části klientského portálu ISDS.

Přístupové údaje jsou generovány dle stejných pravidel jako při vzniku účtu, viz kapitola Přístupové údaje pro oprávněné osoby datových schránek.

Pověřené osobě lze přidělit následující práva:

- Číst zprávy
- Číst zprávy určené do vlastních rukou
- Vytvářet a odesílat datové zprávy
- Prohlížet seznam dodaných zpráv i doručenek
- Vyhledávat datové schránky
- Mazat zprávy z trezoru

Jakmile je účet administrátora nebo pověřené osoby zřízen, ISDS odešle systémovou informační zprávu do datové schránky žadatele.

Přístupové údaje pro poskytovatele dat

Externí agendové systémy povinných poskytovatelů dat dle § 16 Zákona přistupují ke službám ISDS po přihlášení pomocí přihlašovacích údajů vydaných Správcem konkrétní fyzické osobě na základě žádosti poskytovatele dat. Údaje potřebné v takové žádosti:

- jméno, příjmení
- vykonávaná funkce uvnitř organizace poskytovatele dat
- datum narození
- jméno poskytovatele dat
- jméno evidence (jména evidencí)
- sídlo (adresa) poskytovatele dat
- korespondenční adresa
- jméno a příjmení nadřízeného pracovníka

Žádost lze podat následujícím způsobem:

a) Odesláním žádosti podepsané uznávaným elektronickým podpisem na e-podatelnu Správce (posta@mvcr.cz).
b) Odesláním žádosti opatřené ověřeným podpisem na poštovní adresu podatelny Správce.
c) Odesláním žádosti do datové schránky Správce.

Oprávněný pracovník poskytovatele dat může následně požádat Správce o umožnění přístupu elektronické aplikace, která se bude ke službám ISDS přihlašovat komerčním systémovým certifikátem.

Zneplatnění přístupových údajů a vydání nových

O zneplatnění vlastních přístupových údajů a vydání nových dle § 12 odst. 1 Zákona lze požádat následujícím způsobem:

a) Na kontaktním místě veřejné správy (pracoviště Czech POINT).
b) Odesláním žádosti opatřené ověřeným podpisem na poštovní adresu podatelny Správce.
c) Odesláním žádosti do datové schránky Správce.
d) Zadáním požadavku v prostředí klientského portálu ISDS po přihlášení Identitou občana.

Změna hesla

Každý uživatel ISDS si může změnit vlastní heslo v prostředí klientského portálu ISDS. Změna hesla není považována za zneplatnění přístupových údajů ve smyslu Zákona.

Změna oprávněné osoby (vedoucí OVM, statutární zástupce)

a) Změny vedoucích představitelů orgánů veřejné moci jsou automatizovaně přebírány z Rejstříku OVM.

- Změny oprávněných osob u právnických osob zapsaných v registru osob jsou automatizovaně přebírány z registru osob, kam je zapisuje věcně příslušný editor po oznámení subjektu, kde došlo ke změně. Změnu statutárního zástupce právnické osoby je též možné ohlásit na kontaktním místě veřejné správy (pracoviště Czech POINT). Přílohou oznámení je v tomto případě listina dokládající změnu, například notářský zápis z valné hromady společnosti.
- Změny v evidenci statutárních auditorů ohlašuje Komora auditorů České republiky pomocí rozhraní pro poskytovatele dat.

Zrušení přístupu pověřené osoby či administrátora

Přístupové údaje pověřené osoby či administrátora Správce zneplatní neprodleně po obdržení žádosti o zrušení pověření. Tuto žádost může podat oprávněná osoba následujícími způsoby:

a) Na kontaktním místě veřejné správy (pracoviště Czech POINT).
b) Vyplněním elektronického formuláře žádosti a jeho následným odesláním v prostředí klientského portálu ISDS.

Změna osobních údajů

ISDS čerpá změny osobních údajů držitelů datových schránek i dalších uživatelů z registru obyvatel(ROB), za předpokladu, že je fyzická osoba v agendě ISDS tzv. ztotožněna, bylo tedy získáno její AIFO. Pokud nebyl uživatel schránky ztotožněn v ROB, spoléhá se na referenční údaje Registru osob (ROS) nebo na údaje poskytnuté příslušným poskytovatelem dat, jako je např. profesní komora.

Pokud fyzická osoba, které byla zřízena datová schránka, změnila své osobní údaje (jméno, příjmení, bydliště) a změna nebyla automaticky provedena, může tuto změnu ohlásit Správci, nejlépe formou datové zprávy, případně jiným způsobem. Správce zajistí opravu údajů po prověření údajů v poskytnutých dokladech.

3. Přihlášení do ISDS

Náležitosti přístupových údajů a elektronické prostředky k přihlášení jsou stanoveny vyhláškou č. 194/2009 Sb., o stanovení podrobností užívání a provozování informačního systému datových schránek (dále jen „vyhláška č. 194/2009 Sb.“). Nově vydané přístupové údaje jsou vždy tvořeny uživatelským jménem a heslem, tak jak je definuje § 1 výše uvedené vyhlášky.

Přihlášení jménem a heslem dle § 1 vyhlášky č. 194/2009 Sb.

Uživatel má možnost zvolit rozšířené zabezpečení přihlašování formou jednorázového hesla (OTP = One Time Password), a to buď formou SMS kódu doručeného pomocí placené služby Premium SMS (Time-based One Time Password - TOTP) nebo formou bezpečnostního kódu generovaného software / hardware prostředkem dle specifikace RFC4226 (HMAC-Based One-Time Password - HOTP). Bezpečnostní heslo ve smyslu vyhlášky č. 194/2009 Sb. je pak tvořeno statickou částí doplněnou o tento jednorázový bezpečnostní kód.

Pokud uživatel zvolí rozšířenou možnost zabezpečení, pak se nadále nemůže přihlašovat pouze jménem a statickým heslem. V případě ztráty mobilního telefonu, hardware prostředku, případně pokud nastane jakákoli jiná situace, která mu znemožní získání jednorázového bezpečnostního kódu, je jedinou možností, jak obnovit přístup k datové schránce, požádat o zneplatnění přístupových údajů a vydání nových.

Přihlášení jménem, heslem a certifikátem dle § 2 vyhlášky č. 194/2009 Sb.

Pokud si uživatel v prostředí klientského portálu ISDS v sekci Nastavení zaregistruje autentizační certifikát, nemůže se nadále přihlašovat bez něj. Certifikát je po přihlášení možné odregistrovat. Dojde-li k tomu, že zaregistrovaný certifikát expiruje, uživatel ztrácí možnost přihlášení pomocí svých přístupových údajů. Jedinou možností je pak požádat o zneplatnění přístupových údajů a vydání nových, čímž dojde k odregistrování certifikátu.

Technický prostředek lze použít k přihlášení, pokud splní technické požadavky uvedené ve vyhlášce č. 194/2009 Sb.

Přihlášení Identitou občana

Uživatelé datových schránek, kteří jsou v rámci ISDS ztotožněni v Registru obyvatel, se mohou ke svým účtům v ISDS přihlásit pomocí libovolného prostředku pro elektronickou identifikaci s minimální úrovní důvěry „značná“. Podrobnější informace o Identitě občana naleznete na webových stránkách těchto služeb, viz kapitola 2 Odkazy. Přihlášení Identitou občana je možné jen v prostředí Klientského portálu ISDS. Z prostředí aplikací třetích stran (přihlášení pomocí webových služeb) není tato autentizační metoda podporována. Používáním Identity občana nedochází k deaktivaci přístupových údajů, každý uživatel tedy má stále možnost přihlášení i pomocí nich, nicméně uživatel má možnost si sám jejich použití deaktivovat a tím zvýšit úroveň zabezpečení přístupu do ISDS.

Držitelé více uživatelských účtů v ISDS si po úspěšném přihlášení mohou zvolit, který ze svých účtů aktuálně chtějí využít. Pokud následně chtějí vstoupit do jiné datové schránky, musí se nejprve odhlásit a následně přihlásit znovu.

Přihlášení pomocí Mobilního klíče eGovernmentu

Každý uživatel ISDS, kterému byly vydány přístupové údaje k účtu v datové schránce, si může po přihlášení do Klientského portálu ISDS aktivovat přihlašování pomocí mobilní aplikace „Mobilní klíč“. Odkazy pro instalaci aplikace do mobilních telefonů a tabletů na platformách iOS a Android naleznete v kapitole 2 Odkazy. Používáním Mobilního klíče nedochází k deaktivaci přístupových údajů, každý

uživatel tedy má stále možnost přihlášení i pomocí nich. Přihlášení pomocí Mobilního klíče je možné jak v prostředí Klientského portálu ISDS, tak i pomocí aplikačního rozhraní ISDS, pokud tuto možnost bude příslušná aplikace třetí strany podporovat.

Držitelé více uživatelských účtů v ISDS mohou používat Mobilní klíč pro jeden i více uživatelských účtů, musí však provést aktivaci Mobilního klíče jednotlivě pro každý zvolený účet.

4. Přihlášení do datové schránky ve smyslu § 17 odst. 3 Zákona

Přihlášení do DS ve smyslu Zákona proběhne automaticky jako důsledek **vybrané množiny operací** prováděných uživatelem datové schránky s jejich přesnou specifikací:

- Uživatel se ve smyslu Zákona ***přihlásil*** do datové schránky VŽDY, kdy se přihlásil MANUÁLNĚ na klientském portálu ISDS. Během této doby uživatel může pracovat s portálem: prohlížet si seznamy zpráv, stahovat došlé zprávy nebo dodejky/doručenky k odeslaným zprávám, konfigurovat svoje nastavení. Toto pravidlo platí, pokud již byla datové schránka zpřístupněna.
- Uživatel se ve smyslu Zákona ***přihlásil*** do datové schránky, pokud se přihlásil prostřednictvím aplikace třetí strany a provedl operaci získání seznamu došlých datových zpráv.
- Uživatel se ve smyslu Zákona ***nepřihlásil*** do datové schránky, pokud se přihlásil prostřednictvím aplikace třetí strany a provedl jakoukoli jinou operaci než získání seznamu došlých datových zpráv.

Přístup do znepřístupněné schránky

K doručení datových zpráv v důsledku přihlášení do DS může dojít pouze v případě, že je tato DS zpřístupněná. Přihlašuje-li se uživatel do dočasně či trvale znepřístupněné DS, může využívat jen určité omezené možnosti práce se schránkou a zprávami. Konkrétně, znepřístupněná DS umožní zobrazit a stáhnout doručenou i odeslanou zprávu i dodejku a doručenku. Dále také umožňuje využívat funkci ověření datové zprávy. Není možné z takové DS odesílat nové zprávy, ani není možné, aby do ní byly nové zprávy dodávány.

Přihlášený uživatel může změnit své heslo a pokud je k tomu oprávněn, může také odebrat některou z pověřených osob. Nemůže však přidat novou pověřenou osobu.

5. Přihlášení pro získání přístupu k funkcím ISDS aplikacemi třetích stran

Způsob přihlášení

Všechny způsoby přihlášení, které umožňuje Portál datových schránek s výjimkou přihlášení Identitou občana, je možné též implementovat v externí aplikaci. Doporučeným způsobem přihlášení aplikace třetí strany je basic autentizace za pomoci systémového certifikátu, a to zejména s ohledem na zabezpečení a dále také proto, že akce vyvolané externí aplikací jsou pak v ISDS korektně logovány jako akce externího systému a nikoli konkrétní fyzické osoby, která svěřila své přístupové údaje aplikaci.

Implementace přihlášení (basic autentizace)

Autentizační kanál je založen na basic http autentizaci, respektive na X509 klientském certifikátu dle zvolené varianty. v této variantě není používána cookie a je tedy nutné, aby každý https požadavek obsahoval hlavičku Authorisation se jménem a heslem, resp. klientský X509 certifikát.

Možné varianty připojení jsou:

a) basic autentizace:
   *https://ws1.mojedatovaschranka.cz/DS/**
b) klientský https certifikát zaregistrovaný jako systémový certifikát:
   *https://ws1c.mojedatovaschranka.cz/cert/DS/**
c) klientský https certifikát zaregistrovaný jako uživatelský certifikát a basic autentizace:
   *https://ws1c.mojedatovaschranka.cz/certds/DS/**
d) klientský https certifikát zaregistrovaný jako certifikát hostované spisové služby a id schránky jako jméno, heslo prázdné:
   *https://ws1c.mojedatovaschranka.cz/hspis/DS/**

Implementace přihlášení (jednorázový bezpečnostní kód)

Aplikace třetí strany mají možnost využít rozšířené zabezpečení a přihlašovat se jménem, statickým heslem a jednorázovým bezpečnostním kódem (viz výše, odstavec Přihlášení jménem a heslem dle § 1 vyhlášky č.194/2009 Sb.). Vzhledem k technické povaze tohoto způsobu přihlášení je nutné, aby aplikace pracovala s autentizační cookie. Detailní popis autentizačního mechanismu pro přihlášení touto metodou je uveden v souboru ISDS_OTP_autentizace.pdf, který je součástí Technické přílohy č.2. Upozorňujeme, že autentizační metoda pomocí HOTP nebude do budoucna již podporována. Jako multi-faktorovou autentizaci doporučujeme buď jméno/heslo/certifikát nebo Mobilní klíč.

Implementace přihlášení (Mobilní klíč)

Aplikace třetí strany mají možnost využít rozšířené zabezpečení a přihlašovat uživatele pomocí aplikace Mobilní klíč. Podrobný popis této metody je součástí Technické přílohy 2, v dokumentu MobilniKlic_autentizace.pdf.

6. Datová zpráva

Formát datové zprávy

Datovou zprávu tvoří obálka a obsah zprávy.

Strukturu datové zprávy určuje Technická příloha 1 (soubor dmBaseTypes.xsd).

Systém ISDS umožňuje získání datové zprávy označené elektronickou pečetí ministerstva založené na kvalifikovaném certifikátu (viz dokumentace webových služeb ISDS v příloze – operace SignedMessageDownload). Pokud uživatel v prostředí klientského portálu ISDS ukládá datovou zprávu do souboru, zpráva se ukládá v tomto tvaru.

Podrobnější informace o ochranných prvcích sloužících v rámci celkového postupu při kontrole pravosti datové zprávy naleznete v kapitole 2.1 „Vytvoření nové zprávy (odeslání zprávy)“ a v kapitole 2.4.2 „Stažení došlé podepsané zprávy“ v dokumentaci „Webové služby rozhraní ISDS pro manipulaci s datovými zprávami“.

Obsahem zprávy může být jedna či více příloh v počítačovém formátu uvedeném v Příloze 3 vyhlášky č. 194/2009 Sb.

Provozovatel má právo nepřijmout k odeslání datovou zprávu obsahující škodlivý kód.

Povolení přenosu formátů elektronických podpisů, pečetí a časových razítek

Vyhláška č. 194/2009 Sb. o stanovení podrobností užívání a provozování informačního systému datových schránek upravuje pouze přípustné formáty příloh datové zprávy dodávané do datové

schránky. Datovou zprávou se dle § 19 Zákona rozumí všechny dokumenty orgánů veřejné moci doručované prostřednictvím datové schránky, úkony prováděné vůči orgánům veřejné moci prostřednictvím datové schránky a dokumenty fyzických osob, podnikajících fyzických osob a právnických osob dodávané prostřednictvím datové schránky. Zákon č. 300/2008 Sb. a související právní předpisy umožňují a v některých případech dokonce přímo ukládají, aby tyto datové zprávy byly elektronicky podepsány a bylo k nim připojeno časové razítko. Proto správce rozhodl, aby Informační systém datových schránek umožňoval kromě doručování vlastních dokumentů i doručování elektronických podpisů, pečetí a časových razítek v běžně rozšířených formátech.

- CER, CRT, DER, PK7 - formáty certifikátů dle standardu X.509
- P7B, P7C, P7F, P7M, P7S - formáty certifikátů a elektronických podpisů dle PKCS#7
- TST, TSR - formáty pro elektronické razítko

Omezení velikosti datové zprávy

ISDS umožňuje odeslat pouze datovou zprávu s přílohami, jejichž celková velikost bude maximálně 20 MB. Celková velikost kompletní datové zprávy, tedy obálky a příloh převedených do Base64 formátu může dosáhnout řádově až 25 MB. Pro další datové schránky OVM zřízené po 1.11.2018 platí, že maximální velikost datové zprávy, kterou tato omezená množina datových schránek umožňuje přijmout, činí až 50 MB, přičemž v Base64 kódování může být celková velikost přiměřeně větší.

Hromadná datová zpráva

Pokud uživatel odesílá prostřednictvím klientského rozhraní datovou zprávu na více příjemců, použije se funkce hromadného zasílání datových zpráv. Způsob odesílání datové zprávy na více příjemců s pomocí technického prostředku (aplikace) se může lišit v závislosti na způsobu implementace jednotlivých dodavatelů těchto aplikací. Jedna hromadná zpráva může mít maximálně 50 adresátů.

Doba uchovávání datové zprávy

ISDS uchová datovou zprávu po dobu 90 dnů od okamžiku, kdy se do datové schránky přihlásila osoba, která má s ohledem na rozsah svých oprávnění přístup k dokumentu v datové zprávě obsaženém (tj. od okamžiku doručení přihlášením). Datovou zprávu, která nebyla doručena přihlášením, uchovává ISDS po dobu nejméně 3 let.

7. Napojení aplikací třetích stran

ISDS umožňuje napojení aplikací třetích stran, jako jsou například Agendové informační systémy orgánů veřejné moci, spisové služby orgánů veřejné moci, ERP systémů nebo DMS systémů komerčních organizací a podobně, pomocí Webových služeb. Podrobný popis dostupných služeb je uveden v Technické příloze 2. Využití aplikačního rozhraní je automaticky povolené, nevyžaduje tedy žádnou registraci, a je bezplatné.

Tyto služby jsou definované soubory dm_operations.wsdl a dm_info.wsdl. Použité datové typy jsou definovány souborem dmBaseTypes.xsd. Podrobnosti a popis parametrů obsahuje soubor WS_Manipulace_s_datovymi_zpravami.pdf (Technická příloha 2).

Webové služby manipulující s datovými zprávami pro použití v externích agendách (včetně elektronických spisových služeb)

V dm_operations jsou definovány následující webové služby:

- vytvoření a odeslání nové zprávy – CreateMessage
- vytvoření a odeslání hromadné zprávy – CreateMultipleMessage

- stažení došlé zprávy – MessageDownload
- stažení došlé zprávy s pečetí MV – SignedMessageDownload
- stažení odeslané zprávy s pečetí MV – SignedSentMessageDownload
- ověření uložené datové zprávy – AuthenticateMessage
- prázdná operace pro navazování nebo udržování spojení – DummyOperation
- přepodepsání zprávy, dodejky či doručenky – Re-signISDSDocument.

V dm_info jsou definovány následující webové služby:

- ověření neporušení datové zprávy – VerifyMessage
- stažení obálky došlé zprávy – MessageEnvelopeDownload
- označení zprávy jako „Přečtená“ – MarkMessageAsDownloaded
- stažení informace o dodání a doručování zprávy – GetDeliveryInfo
- stažení informace o dodání a doručování zprávy, s pečetí MV – GetSignedDeliveryInfo
- stažení seznamu došlých zpráv – GetListOfReceivedMessages
- stažení seznamu odeslaných zpráv – GetListOfSentMessages
- doručení poštovní datové zprávy – ConfirmDelivery
- stažení seznamu zpráv, u kterých došlo ke změně stavu – GetMessageStateChanges
- zjištění identifikace odesílatele zprávy – GetMessageAuthor
- získání rozšířené identifikace odesílatele zprávy – GetMessageAuthor2
- smazání dlouhodbě uložené DZ (trezorové) – EraseMessage
- požadavek na stažení seznamu smazaných zpráv - GetListOfErasedMessages
- vyzvednutí asynchronního požadavku - PickUpAsyncResponse
- registrace externích notifikací - RegisterForNotifications
- stažení záznamů pro notifikace - GetListForNotifications

Aplikace mohou také využívat služby ISDSSearch, FindDataBox, CheckDataBox, GetDataBoxList, GetDataBoxActivityStatus, FindPersonalDataBox, PDZinfo, DataBoxCreditInfo, DTinfo a PDZSendInfo popsané v souboru db_search.wsdl (viz Technická příloha 2). Popis jejich funkčních parametrů je uveden v souboru WS_Vyhledavani_datovych_schranek.pdf (viz Technická příloha 2).

Přihlášení do datové schránky majitele a doručování zpráv ve smyslu § 17 odst. 3 Zákona způsobuje výhradně stažení seznamu došlých zpráv – GetListOfReceivedMessages.

Odesílací brána ISDS

Odesílací brána umožňuje aplikaci poskytovatele předání konceptu datové zprávy do perimetru ISDS, kde tento koncept může autentizovaný uživatel schválit a odeslat. Tato služba je k dispozici všem držitelům datových schránek po předchozí samoobslužné registraci. Využití odesílací brány není chápáno jako přihlášení do datové schránky ve smyslu Zákona. Autentizace uživatele tak nezpůsobuje doručení dodaných datových zpráv. Služba je popsána v dokumentu OdesilaciBrana_ISDS.pdf (Technická příloha 2).

Webové služby související s přístupovými údaji

Tyto služby jsou definované v souboru db_access.wsdl. Použité datové typy jsou definovány souborem dbTypes.xsd. Podrobnosti a popis parametrů obsahuje soubor WS_souvisejici_s_pristupem_do_ISDS.pdf (Technická příloha 2).

V db_access jsou definovány následující webové služby:

- získání informací o schránce přihlášeného uživatel – GetOwnerInfoFromLogin
- získání informací o přihlášeném uživatel – GetUserInfoFromLogin
- získání informace o expiraci hesla – GetPasswordInfo
- změna hesla – ChangeISDSPassword

Volání služeb definovaných v db_access.wsdl nezpůsobuje doručování zpráv dle § 17 odst. 3 Zákona.

Webové služby související OTP autentizací

Tyto služby jsou definované v souboru ChangePassword.wsdl. Použité datové typy jsou definovány souborem ChangePasswordTypes.xsd. Podrobnosti a popis parametrů obsahuje soubor OTP_autentizace.pdf (viz Technická příloha 2).

V ChangePassword.wsdl jsou definovány následující webové služby:

- změna hesla uživatele s OTP autentizací – ChangePasswordOTP
- zaslání jednorázového TOTP kódu formou SMS – SendSMSCode

Volání služeb definovaných v ChangePassword.wsdl nezpůsobuje doručování zpráv dle § 17 odst. 3 Zákona.

Verzování služeb

Některé služby existují ve více verzích, podporovaných souběžně. V technických přílohách tak můžete narazit na službu ISDSSearch2 i ISDSSearch3 atd. Doporučujeme využívat novější verze, nicméně i starší jsou stále funkční a není plánováno jejich ukončení.

8. Napojení povinných subjektů uvedených v Zákoně

ISDS je z titulu § 15 a § 16 Zákona napojen na další agendové informační systémy, jako je například Informační systém evidence obyvatel, obchodní rejstřík a další. s těmito systémy komunikuje ISDS pomocí webových služeb popsaných v Technické příloze 3, případně pomocí rozhraní specifických pro konkrétní technické řešení.

Webové služby manipulující s datovými schránkami pro poskytovatele dat

Slouží pro použití specializovanými programy subjektů uvedených v § 15 a § 16 Zákona. Tyto služby jsou definované pomocí souborů WS_Sprava_datovych_schranek.wsdl. Použité datové typy jsou definovány souborem dbTypes.xsd.

Seznam webových služeb:

- vytvoření datové schránky – CreateDataBox
- trvalé znepřístupnění datové schránky – DeleteDataBox
- změna informací o datové schránce a jejím majiteli – UpdateDataBoxDescr
- přidání oprávněné osoby – AddDataBoxUser
- zrušení oprávněné osoby nebo zneplatnění přístupu při zrušení pověření – DeleteDataBoxUser
- změna informací o pověřené osobě – UpdateDataBoxUser
- znepřístupnění datové schránky při omezení osobní svobody / detenci / omezení způsobilosti nebo přerušení činnosti – DisableDataBoxExternally
- znepřístupnění datové schránky na žádost – DisableOwnDataBox
- znovuzpřístupnění datové schránky – EnableOwnDataBox
- získání seznamu oprávněných osob DS – GetDataBoxUsers a GetDataBoxUsers2

- nastavení přijímání komerčních DZ – SetOpenAddressing
- zrušení nastavení přijímání komerčních DZ – ClearOpenAddressing

Žádná z těchto webových služeb nezpůsobuje přihlášení do datové schránky a doručování zpráv ve smyslu § 17 odst. 3 Zákona.

Verzování služeb

Některé služby existují ve více verzích, podporovaných souběžně. V technických přílohách tak můžete narazit na službu ISDSSearch2 i ISDSSearch3 atd. Doporučujeme využívat novější verze, nicméně i starší jsou stále funkční a není plánováno jejich ukončení.

9. Seznam držitelů datových schránek (SDS)

Kromě webové aplikace, pomocí které může veřejnost vyhledávat držitele zpřístupněných datových schránek, nabízí SDS dvě služby externím aplikacím. Obě tyto služby jsou dostupné zcela veřejně, bez nutnosti autentizace k jejich užití.

Pozn.: Seznam držitelů datových schránek obsahuje informace o všech zpřístupněných datových schránkách s výjimkou fyzických osob, které požádaly o vymazání z tohoto seznamu. Datový obsah SDS je aktualizován nejméně jednou za 24 hodin, obvykle jednou za 3 hodiny.

Webové služby pro vyhledání datové schránky a získání informací o jejím držiteli

Metody GetInfo a SearchSubject jsou detailně popsány v souboru sds_ws.pdf, obsaženém v Příloze 2 tohoto Provozního řádu.

Datové exporty SDS jako otevřená data

SDS publikuje kompletní seznamy schránek v členění na právnické osoby, podnikající fyzické osoby, fyzické osoby a orgány veřejné moci. Tyto čtyři soubory jsou volně ke stažení ve formátu XML. Detailní popis struktury souborů a jejich URL adresy jsou uvedeny v dokumentu sds_datove_soubory.pdf, obsaženém v Příloze 2 tohoto Provozního řádu.

Autentizační služba PVS

Autentizační služba PVS slouží k autentizaci uživatelů jiných informačních systémů na základě ověření identity uživatele v identitním prostoru datových schránek. Kromě potvrzení o úspěšném přihlášení poskytuje služba se souhlasem uživatele též jeho identifikační údaje, jako je např. jméno, příjmení, typ uživatele, typ datové schránky, údaje o datové schránce apod. Přihlášením se do informačního systému za pomoci autentizační služby nedochází k přihlášení do datové schránky ve smyslu § 17 odst. 3 Zákona.

Informační systém může Autentizační službu PVS využívat na základě registrace provedené oprávněnou osobou nebo administrátorem v prostředí Klientského portálu ISDS. Technická specifikace Autentizační služby PVS tvoří Technickou přílohu 5 tohoto Provozního řádu.

Funkčnost Autentizační služby lze kombinovat s Odesílací bránou ISDS, viz část II, kap. 7 tohoto Provozního řádu. Všechny informační systémy, které mají platnou registraci k využití Autentizační služby PVS, mají zároveň rovnou registrováno též využití Odesílací brány ISDS.

Podmínky využívání Autentizační služby PVS

Ministerstvo vnitra z pozice Správce ISDS stanovuje následující podmínky využívání Autentizační služby PVS (dále jen AS).

a) AS slouží výhradně k identifikaci a autentizaci uživatelů jiných informačních systémů veřejné správy, případně jiných informačních systémů ve správě orgánu veřejné moci (dále jen IS).
b) Správce IS zajišťuje taková bezpečnostní pravidla a opatření, aby nedošlo ke zneužití osobních či přihlašovacích údajů uživatelů datových schránek.
c) Správce i provozovatel IS zajišťuje, aby AS byla využívána v souladu s technickou specifikací AS a Provozním řádem ISDS.
d) Správce IS zodpovídá za škodu způsobenou v souvislosti s využíváním AS. Správce IS se odpovědnosti zprostí, prokáže-li, že škodě nemohlo být zabráněno ani při vynaložení veškerého úsilí, které na něm lze spravedlivě požadovat.
e) Ministerstvo vnitra je oprávněno pozastavit využívání AS tomu IS, u kterého by hrozilo zneužití AS, v důsledku kterého by mohla být ohrožena bezpečnost přihlašovacích či osobních údajů uživatelů datových schránek nebo provoz ISDS jako takového.
f) Správce IS zodpovídá za nakládání s osobními údaji uživatelů datových schránek, které získal prostřednictvím AS. Správce IS podléhá příslušným ustanovením zákona č. 110/2019 Sb., o zpracování osobních údajů.
g) Správce IS je povinen nahlásit Správci ISDS jako bezpečnostní incident každý pokus o získání nebo zneužití informací souvisejících s přístupovými nebo osobními údaji uživatelů datových schránek nepovolanou osobou. Nahlášení se provádí na infolinku datových schránek a portálu veřejné správy – technickou podporu.
h) IS může využívat AS na základě registrace provedené v konfiguraci datové schránky OVM. Doporučeným postupem je nejprve provést konfiguraci Autentizační služby v prostředí veřejného testovacího prostředí ISDS a teprve po otestování funkčnosti v produkčním prostředí ISDS.
i) Veřejnou část serverového certifikátu, kterým se aplikace autentizuje pro využití AS, může správce IS samoobslužně vložit do ISDS v prostředí klientského portálu, části „Nastavení / Přístup externích aplikací“. Pokud pracovník správce IS z organizačních důvodů nemá přístup do nastavení datové schránky subjektu, může veřejnou část certifikátu zaslat MV s žádostí o jeho registraci v ISDS. Správce IS bere na vědomí, že neposkytne-li MV nový certifikát své aplikace s předstihem nejméně 30 dnů před expirací zaregistrovaného certifikátu, vystavuje se riziku dočasné nefunkčnosti autentizace.

10. Přístupové rozhraní

Přístupové rozhraní pro poskytovatele internetových služeb (viz § 14a Zákona) slouží k pro správu přístupových údajů a identity osob oprávněných k přístupu do datových schránek a vazby přístupových údajů těchto osob na přístupové údaje k individuálním uživatelským účtům v aplikaci poskytovatele. Prakticky služby tohoto přístupového rozhraní umožňují obsluhu datové schránky z jiné internetové aplikace, a to, aniž by uživatel této aplikace musel pokaždé zadávat své přístupové údaje k datové schránce. Přihlášení k jeho datové schránce je realizováno na základě propojení jeho uživatelského účtu v internetové aplikaci s uživatelským účtem ISDS.

Využití Přístupového rozhraní je možné teprve po vydání povolení Správcem, které je vázáno zejména na splnění Podmínek pro využití přístupového rozhraní, tak jak jsou definovány ve Věstníku Ministerstva vnitra (viz odkazy). Zájemce o využívání služeb Přístupového rozhraní tedy musí nejprve podat žádost na adresu Správce ISDS.

Technická specifikace přístupového rozhraní je obsažena v Technické příloze 6 tohoto Provozního řádu.

Je zodpovědností správce internetové aplikace, aby poskytl MV nový certifikát své aplikace s předstihem nejméně 30 dnů před expirací zaregistrovaného certifikátu. Neučiní-li tak, vystavuje se riziku dočasné nemožnosti využívat přístupové rozhraní.

11. Oznamování změn dodavatelům aplikací

Vzhledem k důležitosti, jakou pro orgány veřejné moci i pro řadu dalších subjektů představuje správná funkčnost napojení vlastních aplikací na Informační systém datových schránek, Správce ISDS věnuje zvláštní pozornost komunikaci se zástupci dodavatelů těchto aplikací. v rámci informačního webu datových schránek je zřízena webová stránka, na které jsou publikovány jednak oznámené změny v oblasti webových služeb, ale také pravidla vzájemného vztahu mezi Správcem ISDS a dodavateli aplikací třetích stran. Více viz https://info.mojedatovaschranka.cz/info/cs/74.html.

Upozornění na plánované změny v ISDS

Na výše uvedené stránce jsou publikována stručná upozornění na budoucí změny aplikačního rozhraní ISDS (změny webových služeb). Změny, které neovlivňují existující funkcionalitu, mohou být nasazeny a oznámeny kdykoli. Oproti tomu změny, které jakýmkoli způsobem mění existující funkčnost webových služeb nebo přihlášení k nim, jsou zveřejňovány obvykle dva měsíce před jejich nasazením, nebrání-li tomu mimořádné provozní či bezpečnostní důvody.

Pracovní prostor pro registrované dodavatele aplikací

Ministerstvo vnitra zřídilo pracovní prostor pro všechny zájemce o novinky a změny aplikačního rozhraní informačního systému datových schránek. Výrobce nebo dodavatel spisové služby, případně jiné aplikace, využívající webové služby ISDS, se může do tohoto prostoru zaregistrovat zde: https://registrace.poradnaisds.cz.

Obsahem pracovního prostoru jsou zejména knihovny obsahující aktuální i starší verze dokumentace k webovým službám, ale i diskuzní fórum moderované Provozovatelem ISDS. Zveřejňování informací o webových službách ISDS v rámci tohoto pracovního prostoru považuje Ministerstvo vnitra za splnění informační povinnosti Správce Informačního systému datových schránek vůči dodavatelům aplikací třetích stran.

Aktivní účast v procesu návrhu změn ISDS

Trvale otevřenou možnost představuje přistoupení k Memorandu mezi Ministerstvem vnitra a zástupci dodavatelů spisových služeb. Signatáři Memoranda jsou zváni na setkání s představiteli ministerstva, provozovatelem ISDS i jeho dodavatelem. Připravované změny jsou s účastníky podrobně diskutovány, přičemž zvolení zástupci dodavatelů se přímo podílí na návrhu standardů, jako je například formát obálky datové zprávy nebo rozhraní pro předávání spisů mezi spisovými službami navzájem. Znění Memoranda i popis, jak k němu přistoupit, je uveden zde:
http://www.mvcr.cz/clanek/datove-schranky-dalsi-krok-pri-zavadeni-datovych-schranek-splnen.aspx.

12. Standardizovaný formát komunikace elektronických spisových služeb

Pracovní skupina reprezentující dodavatele elektronických spisových služeb se dohodla na použití standardního XML schématu pro komunikaci spisových služeb navzájem. Schéma je popsáno soubory ess.xsd a dále Dokumentace_schematu_ess.pdf obsaženými v Technické příloze 4.

13. Důvěrnost informací

ISDS používá a ukládá informace uvedené v § 14 odst. 3. Zákona. Správce ani Provozovatel ISDS nejsou oprávněni k přístupu do datových schránek jiných subjektů. ISDS je ve smyslu zákona č. 365/2000 Sb., informačním systémem veřejné správy, který je podle § 9 odst. 1 tohoto zákona neveřejnou evidencí.

14. Bezpečnost ISDS

ISDS, jakožto informační systém veřejné správy ve smyslu § 2 písm. b) zákona č. 365/2000 Sb., je povinen podrobovat se pravidelnému bezpečnostnímu auditu. Zajištění auditu je zodpovědností Provozovatele.

Bezpečnostní standardy

Návrh a implementace ISDS respektuje zásady následujících standardů:

- ISO/IEC řady 27001:2006 - Systémy řízení bezpečnosti informací ISMS

15. Dodržování přiměřenosti

Při práci s datovou schránkou musí být zohledněna frekvence stahování seznamů zpráv, stahování zpráv a doručenek a odesílání datových zpráv tak, aby uživatel osobně nebo aplikace, kterou pro přihlašování do datové schránky používá, nezatěžovala systém zbytečnými opakovanými dotazy, například na existenci nových datových zpráv.

Aplikace instalované na lokální stanici (jednotlivý počítač) se musí do datové schránky přihlašovat pomocí manuálního příkazu uživatele (např. stisknutím tlačítka pro výběr a odesílání zpráv). Serverové aplikace (případ, kdy s ISDS komunikuje server, který zprostředkovává požadavky klientských stanic) se mohou do datové schránky přihlašovat automatizovaně při zohlednění nezbytně nutné frekvence doručování a odesílání datových zpráv.

Aplikace, kterou pro práci s datovou schránkou uživatel využívá, musí zejména evidovat již doručené datové zprávy a při následných dotazech na existenci nových datových zpráv stahovat jen seznam nově doručených zpráv.

Automatizovaný dohledový systém Provozovatele ISDS sleduje a vyhodnocuje zátěž generovanou jednotlivými účty. Sledováno je pět kategorií činnosti:

- Stahování jednotlivých odeslaných zpráv
- Stahování jednotlivých došlých zpráv
- Stahování dodejek či doručenek
- Označování došlých zpráv jako stažené
- Stahování seznamů zpráv

Při déletrvajícím překračování interních limitů některé z výše uvedených kategorií činnosti může Provozovatel ISDS pomocí systémové zprávy informovat držitele schránky, k níž náleží daný účet, o této skutečnosti. Pokud se situace nezlepší nebo držitel schránky svůj provoz nezdůvodní, může Provozovatel přikročit (v souladu s § 5b zákona č. 365/2000 Sb., o informačních systémech veřejné správy, v platném znění,) k dočasnému aktivaci režimu omezeného přístupu pro daný účet. o zapnutí (i vypnutí) omezujícího režimu bude schránka informována systémovou zprávou.

Jak se projeví režim omezeného přístupu:

1. Nejprve je bez omezení propuštěn stanovený počet požadavků – až do systémem stanovené limitní hranice, odpovídající „normálnímu“ chování uživatele odpovídající běžnému provozu schránky.
2. Při příchodu nového požadavku po překročení limitní hranice v daném dni pro některé ze sledovaných volání webových služeb, pokud se právě nezpracovává jiný požadavek ze stejného účtu schránky, bude aplikováno omezení, spočívající v odložení vyřízení požadavku o nastavený čas T (současné nastavení je T = 3s).
3. Pokud se již zpracovává jiný požadavek ze stejného účtu datové schránky, nový požadavek bude po čase T odmítnut. Tím se zabrání obcházení omezení zvýšením počtu vláken.

Cílem omezujícího režimu není zablokování práce, ale zpomalení na „normální“ úroveň. Popsané omezení může být aplikováno i na více účtů jedné schránky. Přístupy přes klientský portál (i účtem v omezeném režimu) nebudou nijak dotčeny.

16. Dostupnost ISDS

ISDS je provozován nepřetržitě v režimu 24 x 7 s výjimkou plánovaných odstávek a pravidelné údržby. Plánované odstávky zveřejňuje Provozovatel na stránkách https://info.mojedatovaschranka.cz/.

17. Údržba systému

Údržba informačního systému ISDS může být učiněna kdykoliv během provozu, nejvýše však jedenkrát v kalendářním týdnu, a to zpravidla každý pátek od 0:00 do 1:00 hod. v této době nemusí být systém dostupný.

III. Kontakty

Správce:

Ministerstvo vnitra České republiky
odbor eGovernmentu
náměstí Hrdinů 3, 140 21 Praha 4

Provozovatel:

Česká pošta, s.p.
Oddělení rozvoje produktů a služeb eGovernment
Politických vězňů 909/4, 225 99 Praha 1

Informační zdroje:

Informační webové stránky projektu naleznete na adrese:
https://info.mojedatovaschranka.cz/

Primárním kontaktním místem pro uživatele datových schránek i Portálu datových schránek je v případě obtíží či nejasností telefonická linka +420 954 200 200, provozovaná v pracovní dny od 8–18 hodin.

IV. Technické přílohy

Technická příloha 1:
Popis XML struktury obálky datové zprávy

Technická příloha 2:
Popis rozhraní pro komunikaci ISDS s Agendovými Informačními Systémy (AIS) třetích stran (Elektronické spisové služby, agendy, rejstříky, DMS, ERP apod.).

Technická příloha 3:
Popis rozhraní ISDS pro příjem změnových údajů od povinných subjektů ze Zákona.

Technická příloha 4:
Popis XML schématu pro komunikaci elektronických spisových služeb navzájem.

Technická příloha 5:
Popis Autentizační služby PVS a Odesílací brány.

Technická příloha 6:
Popis Přístupového rozhraní pro poskytovatele internetových služeb.