

Provozní řád ISDS

Zpracoval: projektový manažer ISDS

Ing. Pavel Tesař,
MV ČR,
Sekce rozvoje a projektového řízení
ICT v oblasti veřejné správy

DRAFT

2009

Provozní řád Informačního systému datových schránek (ISDS)

(Verze Draft z 12.3.2008)

Změny provedené k 12.3.

Aktualizován obsah Technické přílohy 4

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 na základě Zákona č.300/2008 Sb. Jeho správcem je Ministerstvo vnitra ČR. Provozovatelem ISDS je Česká pošta, s.p.

ISDS je informačním systémem veřejné správy ve smyslu zák. č. 365/2000 Sb..

Obsah Provozního řádu

Obsah Provozního řádu.....	2
Vymezení pojmů.....	3
ISDS.....	3
Datová schránka.....	3
Datová zpráva.....	3
Kontaktní místo veřejné správy.....	3
Orgán veřejné moci.....	3
Spisová služba.....	4
Datová schránka.....	4
Zřízení datové schránky.....	4
Zpřístupnění datové schránky.....	4
Znepřístupnění datové schránky.....	4
Zrušení datové schránky.....	4
Přístupové údaje.....	5
Jak získat přístupové údaje?.....	5
Jak jmenovat administrátora či oprávněnou osobu.....	5
Zneplatnění přístupových údajů.....	5
Zrušení přístupu pověřené osoby či administrátora.....	5
Přihlášení do ISDS.....	5
Přihlášení do Datové schránky ve smyslu §17 odst. 3 Zákona.....	6
Přihlášení pro získání přístupu k FUNKCÍM ISDS aplikacemi třetích stran....	7
Způsob přihlášení.....	7
Implementace přihlášení.....	7
Datová zpráva.....	7
Formát Datové zprávy.....	7
Omezení velikosti DS.....	8
Doba uchovávání DS.....	8
Napojení aplikací třetích stran.....	8
Webové Služby manipulující s datovými zprávami pro použití v externích agendách (včetně elektronických spisových služeb).....	8
Napojení povinných subjektů uvedených v zákoně.....	8

Webové Služby manipulující s datovými schránkami pro použití specializovanými programy subjektů uvedených v § 15-16 uvedeného zákona	9
Standardizovaný formát komunikace elektronických spisových služeb	9
Důvěrnost informací	9
Bezpečnost ISDS	9
Bezpečnostní standardy	9
Dostupnost ISDS.....	10
Kontakty.....	10
Správce:	10
Provozovatel:	10
Pracoviště technické podpory:	10
Provozní řád schválil:	10
Technické přílohy	11
Technická příloha 1. Popis XML struktury obálky datové zprávy	11
Technická příloha 2. Popis rozhraní pro komunikaci ISDS s Agendovými Informačními Systémy (AIS) třetích stran (Elektronické spisové služby, agendy, rejstříky, DMS, ERP apod.)	11
Technická příloha 3. Popis rozhraní ISDS pro příjem změnových údajů od povinných subjektů ze zákona 300/2008 Sb.....	11
Technická příloha 4. Popis XML schématu pro komunikaci elektronických spisových služeb navzájem.....	11

Vymezení pojmů

ISDS

Informační systém datových schránek zajišťuje bezpečnou a průkaznou elektronickou komunikaci mezi Orgány veřejné moci (dále jen OVM) na straně jedné a fyzickými či právnickými osobami na straně druhé, jakož i mezi OVM navzájem.

Datová schránka

Datová schránka je elektronickým úložištěm, tedy datovým prostorem, který je vyhrazen pro orgán veřejné moci nebo právnickou osobu nebo podnikající fyzickou osobu nebo pro fyzickou osobu, kam jsou orgány veřejné moci doručovány datové zprávy, kde jsou prováděny úkony vůči orgánům veřejné moci.

Datová schránka je součástí ISDS.

Datová zpráva

Datová zpráva je součástí ISDS. Datová zprávu doručí ISDS z Datové schránky odesílatele do Datové schránky příjemce.

Kontaktní místo veřejné správy

Kontaktním místem veřejné správy je pracoviště Czech POINT. Seznam pracovišť je uveden na webu www.czechpoint.cz

Orgán veřejné moci

Ve smyslu zákona č. 300/2008 , §1 odst. 1 se tímto rozumí státní orgány, orgány územních samosprávných celků, Pozemkový fond České republiky i jiné státní fondy, zdravotní pojišťovny, Český rozhlas, Česká televize, samosprávné komory zřízené zákonem, notáři a soudní exekutoři.

Spisová služba

Ve smyslu zákona č. 499/2004 Sb. jsou veřejnoprávní původci 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 č. 2.

Datová schránka

Zřízení datové schránky

Orgánům veřejné moci a právnickým osobám zapsaným v obchodním rejstříku bude Datová schránka zřízena automaticky ze zákona. O zřízení Datové schránky mohou správce požádat fyzické osoby, fyzické osoby podnikající a právnické osobě 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. 2)
 - b) Vyplněním elektronického formuláře žádosti a jeho následným uložením do internetové úschovny. Na pracovišti Czech POINT žadatel předá jednorázové heslo obsluze, která formulář stáhne, vytiskne a nechá žadatele podepsat, přičemž ověří jeho totožnost.
 - c) Odesláním vyplněného elektronického formuláře žádosti, podepsaného zaručeným elektronickým podpisem oprávněné osoby do datové schránky Správce. Formulář je umístěn na stránkách www.datoveschranky.info.
- Správce zřídí Datovou schránku do 3 pracovních dnů od přijetí žádosti.

Zpřístupnění datové schránky

Dle §10 odst. 2 je Datová schránka zpřístupněna prvním přihlášením osoby uvedené v § 8 odst. 1 až 4 nebo administrátora, nejpozději však patnáctým dnem po dni doručení přístupových údajů těmto osobám.

Znepřístupnění datové schránky

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. 2)
- b) Odesláním vyplněného elektronického formuláře žádosti, podepsaného zaručeným elektronickým podpisem oprávněné osoby, do Datové schránky Správce.
- c) Po přihlášení na Webovém portále ISDS v administrativní sekci.

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

Zrušení datové schránky

Datovou schránku zruší správce 3 roky po zániku existence subjektu pro který byla zřízena, viz §13. Záznamy o přenesených zprávách uchovává ISDS trvale.

Přístupové údaje

Jak získat přístupové údaje?

Subjektům, kterým správce vytvoří Datové schránky, budou zaslány přístupové údaje poštou, a to do vlastních rukou oprávněné osoby adresáta.

Jak jmenovat administrátora či oprávněnou osobu

Dle §8 odst. 7 mohou oprávněné osoby pověřit další fyzické osoby přístupem do jejich Datové schránky, případně 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) Z prostředí Webového portálu ISDS odesláním Datové zprávy obsahující žádost do schránky Správce.

b) Na kontaktním místě veřejné správy (pracoviště Czech POINT). V tomto případě není nutné žádost opatřovat úředně ověřeným podpisem (viz §27 odst. 2)

c) Odesláním vyplněného elektronického formuláře žádosti, podepsaného zaručeným elektronickým podpisem oprávněné osoby do datové schránky Správce. Formulář je umístěn na stránkách www.datoveschranky.info.

Zneplatnění přístupových údajů

O zneplatnění vlastních přístupových údajů dle §12 odst. 1 lze požádat následujícími způsoby:

a) Prostřednictvím samoobsluhy v prostředí Webového portálu ISDS. V takovém případě ISDS zajistí okamžitou změnu hesla dle zadání uživatele.

b) Na kontaktním místě veřejné správy (pracoviště Czech POINT). V tomto případě obdrží oprávněná osoba nové přístupové údaje na počkání.

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) Prostřednictvím samoobsluhy v prostředí Webového portálu ISDS.

V takovém případě ISDS zajistí okamžité zneplatnění přístupových údajů pověřené osoby.

b) Z prostředí Webového portálu ISDS odesláním Datové zprávy obsahující žádost do schránky Správce.

c) Na kontaktním místě veřejné správy (pracoviště Czech POINT).

Přihlášení do ISDS

Náležitosti přístupových údajů a elektronické prostředky k přihlášení jsou stanoveny vyhláškou o podrobnostech přístupu do datové schránky xxxx/2009 (odkaz).

Technický prostředek lze použít k přihlášení, pokud splní technické požadavky uveden ve Vyhlášce a v tomto Provozním řádu a pokud jeho vydavatel zveřejní Prohlášení o shodě s těmito požadavky:

Požadavky na OS Microsoft Windows 2000/XP/Vista

Podpora následujících funkcí rozhraní Microsoft CryptoAPI:

CertAddCRLContextToStore

CertAddCertificateContextToStore

CertAddStoreToCollection

CertCloseStore
CertCompareCertificateName
CertCreateCRLContext
CertCreateCertificateContext
CertDuplicateCRLContext
CertDuplicateCertificateContext
CertEnumCRLsInStore
CertEnumCertificatesInStore
CertFindCertificateInCRL
CertFindCertificateInStore
CertFindExtension
CertFreeCRLContext
CertFreeCertificateChain
CertFreeCertificateContext
CertGetCertificateChain
CertGetCertificateContextProperty
CertGetNameStringA
CertGetPublicKeyLength
CertNameToStrA
CertNameToStrW
CertOpenStore
CertOpenSystemStoreA
CertStrToNameA
CertVerifySubjectCertificateContext
CryptAcquireCertificatePrivateKey
CryptImportPublicKeyInfo
PFXImportCertStore
PFXIsPFXBlob
PFXVerifyPassword

Požadavky na OS Linux (certifikováno pro SUSE Linux Enterprise Desktop 10)

Podpora rozhraní PKCS#11 API s využitím funkcí OpenSource knihovny Libp11:

PKCS11_CTX_new
PKCS11_CTX_load
PKCS11_enumerate_slots
PKCS11_enumerate_certs
PKCS11_login
PKCS11_find_key
PKCS11_get_private_key
PKCS11_get_public_key
PKCS11_get_key_type
PKCS11_logout
PKCS11_release_all_slots
PKCS11_CTX_unload(ctx);
PKCS11_CTX_free(ctx);

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 v čase kdy se přihlásil MANUálně na webovém 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.

- Uživatel se ve smyslu zákona **přihlásil** do datové schránky, pokud se přihlásil prostřednictvím aplikace třetí strany a provedl některou z těchto operací: získání kterékoliv došlé datové zprávy nebo její obálky, získání seznamu došlých nebo odeslaných datových zpráv, získání dodejky nebo doručenky k datové zprávě, označení zprávy jako stažené.
- Uživatel se ve smyslu zákona **nepřihlásil** do datové schránky, pokud se přihlásil prostřednictvím aplikace třetí strany a provedl některou z těchto operací: odeslání nové datové zprávy, vyhledávání cizí datové schránky (operace, které nemají efekt pro doručení do datové schránky uživatele aplikace).

Přihlášení pro získání přístupu k FUNKCÍM ISDS aplikacemi třetích stran

Způsob přihlášení

K přihlášení jsou potřebné přístupové údaje, a to:

- buď uživatelské jméno a heslo, vydané správcem ISDS do vlastních rukou odpovědné osoby (pro první přihlášení do systému s možností následných změn);
- anebo elektronický prostředek třetí strany vyhovující podmínkám specifikovaným vyhláškou správce ISDS (MV ČR). S vydáváním elektronických prostředků přímo ministerstvem vnitra se nepočítá (pouze elektronické prostředky třetí strany dle vyhlášky).

Každý uživatel ISDS obdrží uživatelské jméno a heslo. Pokud bude držet elektronický prostředek třetí strany vyhovující podmínkám specifikovaným vyhláškou MV, může si na portále ISDS tento prostředek zaregistrovat a tím si umožnit přihlašování do ISDS pomocí tohoto prostředku (zatím vyhláška předpokládá komerční certifikát vydaný jednou z akreditovaných certifikačních autorit na tokenu nebo čipové kartě).

Implementace přihlášení

Pokud na straně uživatele je aplikace volající webové služby ISDS, přihlášení trvá po dobu, po kterou je kanál otevřen – vytvoření ověřeného komunikačního kanálu vždy vyžaduje přihlášení.

Přihlášení otevře šifrovaný SSL kanál mezi uživatelem DS a ISDS (na základě serverového certifikátu ISDS) a je realizované prostřednictvím přístupových údajů.

Datová zpráva

Formát Datové zprávy

Datovou zprávu tvoří obálka a obsah zprávy.

Strukturu XML obálky Datové zprávy určuje Technická příloha č. 1 (soubor dmBaseTypes.xsd).

Obsahem zprávy může být jedna či více příloh v libovolném počítačovém formátu, s výjimkou spustitelných souborů jako je např. .exe a komprimovaných souborů typu zip, arc, arj, cab, rar, tar, sfx, lha, lzh, hqx, btoa, bz2, tbz, cpt, tgz, bin, sit, sitx, taz, ync. Provozovatel má kromě toho právo nepřijmout k odeslání Datovou zprávu obsahující škodlivý kód.

Omezení velikosti DS

ISDS umožní odeslat Datovou zprávu o maximální velikosti 10 MB.

Doba uchování DS

ISDS uchová doručenou Datovou zprávu po dobu 90-ti dnů od doručení do Datové schránky příjemce.

Nedoručenou Datovou zprávu uchovává ISDS po neomezenou dobu. Provozovatel má právo takové zprávy po 90-ti dnech od fikce doručení přemístit do off-line datového úložiště, ze kterého lze zprávu na žádost uživatele vrátit zpět do jeho Datové schránky.

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.

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

Tyto služby jsou definované soubory `dm_MessCreate.wsdl`, `dm_MessDownload.wsdl`, `dm_MessDelivery.wsdl` a `dm_ListsOfMess.wsdl`. Použité datové typy jsou definovány souborem `dmBaseTypes.xsd` (viz Technická příloha 1). Podrobnosti a popis parametrů obsahuje soubor `dz_ws.doc` (Technická příloha 2).

Seznam Webových Služeb:

1. vytvoření a odeslání nové zprávy - **CreateMessage**
2. ověření kopie uložené zprávy proti originálu v ISDS - **VerifyMessage**
3. stažení došlé zprávy - **MessageDownload**
4. stažení obálky došlé zprávy - **MessageEnvelopeDownload**
5. stažení došlé zprávy s podpisem značkou MV - **SignedMessageDownload**
6. označení zprávy jako „Přečtená“ - **MarkMessageAsDownloaded**
7. stažení informace o dodání a doručování zprávy - **GetDeliveryInfo**
8. stažení informace o dodání a doručování zprávy, s podpisem značkou MV - **GetSignedDeliveryInfo**
9. stažení seznamu došlých zpráv - **GetListOfReceivedMessages**
10. stažení seznamu odeslaných zpráv – **GetListOfSentMessages**

*Všechny tyto webové služby s výjimkou 1. **CreateMessage** způsobují přihlášení do datové schránky majitele a doručování zpráv ve smyslu §17 odst. 3 zákona č. 300/2008 Sb.*

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 popsanych v Technické příloze 3.

Webové Služby manipulující s datovými schránkami pro použití specializovanými programy subjektů uvedených v § 15-16 uvedeného zákona

Tyto služby jsou definované pomocí souborů `db_manipulations.wsdl`. Použité datové typy jsou definovány souborem `dbTypes.xsd`. Podrobnosti a popis parametrů je v souboru `ds_ws.doc`.

Seznam webových služeb:

- nalezení datové schránky - **FindDataBox**
- vytvoření datové schránky - **CreateDataBox**
- zrušení datové schránky - **DeleteDataBox**
- změna informací o majiteli datové schránky - **UpdateDataBoxDescr**
- přidání pověřené osoby - **AddDataBoxUser**
- zrušení oprávněné osoby - **DeleteDataBoxUser**
- změna informací o pověřené osobě - **UpdateDataBoxUser**
- nové vytvoření přístupových údajů - **NewAccessData**
- znepřístupnění datové schránky při nesvépravnosti/detenci - **DisableDataBoxExternally**
- znepřístupnění datové schránky na žádost majitele - **DisableOwnDataBox**
- znovuzpřístupnění datové schránky - **EnableOwnDataBox**

Dále je možno do této kategorie počítat i webovou službu **GetDataBoxUsers** pro získání seznamu oprávněných osob datové schránky definovanou souborem `db_supplementary.wsdl` a popsanou v `sys_ws.doc`.

Žádná z těchto webových služeb nezpůsobují přihlášení do datové schránky majitele a doručování zpráv ve smyslu §17 odst. 3 zákona č. 300/2008 Sb.

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.

Důvěrnost informací

ISDS používá a ukládá informace uvedené v §14 odst 3. Zákona 300/2008 Sb. Tyto údaje jsou neveřejné, s výjimkou kontaktní adresy, na niž má být adresátu doručováno, byl-li dán souhlas k jejímu zveřejnění. Správce ani Provozovatel ISDS nejsou oprávněni k přístupu do datových schránek jiných subjektů.

Bezpečnost ISDS

ISDS, jakožto Informační systém veřejné správy ve smyslu zákona 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:

- ČSN ISO/IEC-15408 - Common Criteria for Information Technology Security Evaluation,

- ČSN ISO/IEC TR 13335- Techniky pro řízení bezpečnosti IT
- ISO/IEC řady 27001:2006 - Systémy řízení bezpečnosti informací ISMS

Dostupnost ISDS

ISDS je provozován nepřetržitě v režimu 24 x 7 s výjimkou plánovaných odstávek v rozsahu max. 96 hodin ročně v rozmezí 18-07 hodin. Mimo plánované odstávky se Provozovatel zavazuje dodržet dostupnost služby v úrovni 99% provozní doby. Plánované odstávky zveřejňuje Provozovatel na stránkách Webového portálu ISDS.

Kontakty

Správce:

Ministerstvo Vnitra České republiky
náměstí Hrdinů 3
140 21 Praha 4

Provozovatel:

Česká pošta, s. p.
Politických vězňů 909/4, Praha 1, 225 99

Pracoviště technické podpory:

Doplň dodavatel

Aplikace Technical Assistance Requester/Reporter
(<https://etar.deltax.cz/ctar>)

Elektronická pošta primární Email: ISCP@deltax.cz
email na SD: ServiceDesk@deltax.cz

Telefon pevná linka: +420 251 029 211
záložní telefonický kontakt: +420 737 860 356

Provozní řád schválil:

Zástupce MV ČR?
Nabývá platnosti: 1.7.2009

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 300/2008 Sb.

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

DRAFT