EnvIAM – Uživatelská příručka – část AM

Obsah

Seznam obrázků

1 Úvod

Tato příručka byla vytvořena v souladu s vyhláškou č. 529/2006 §11 odst. (6) a má za cíl popsat koncovému uživateli funkce systému EnvIAM určeného pro zprostředkování ověření identity uživatele a přístupových práv agendovým informačním systémům, aplikacím a informačním systémům v rámci Ministerstva životního prostředí (dále jen „systémy IS/AIS MŽP“) a zajistit tak uživatelům přístup k neveřejným informacím systémů IS/AIS MŽP.

V rámci procesu přihlášení uživatele k systému IS/AIS MŽP systém EnvIAM využívá informace o uživateli, které jsou uvedené v Centrálním registru životního prostředí (dále jen „CRŽP“). Z tohoto důvodu je nezbytné, aby uživatel využívající funkcí EnvIAM, měl založen validní účet v CRŽP.

Systém EnvIAM, kromě zprostředkování ověření identity uživatele a přístupových práv, poskytuje také funkcionalitu SSO, která umožňuje uživateli ověřit identitu uživatele pouze jednou pro více systémů IS/AIS MŽP v rámci jednoho procesu přihlášení. Po ukončení práce v IS/AIS je třeba pamatovat na bezpečné odhlášení a kliknout na „Odhlásit“ a uzavřít všechna okna prohlížeče.

Dokument je průběžně aktualizován.

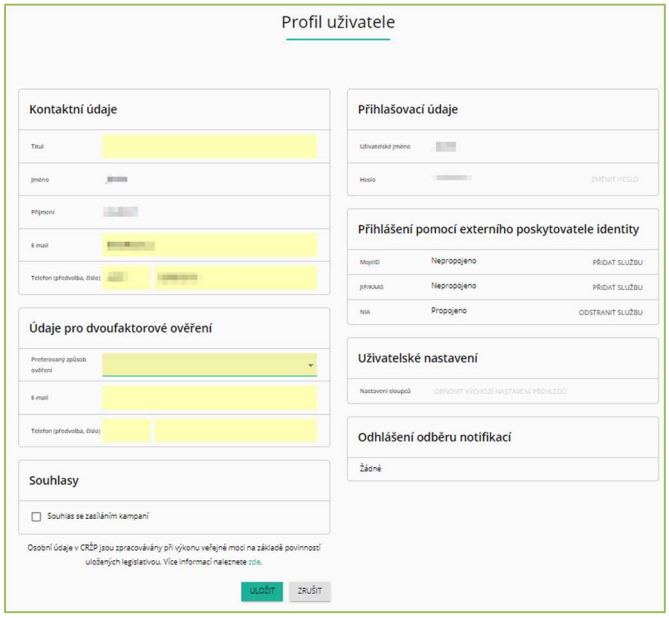
1.1 Vymezení pojmů a zkratek

Zkratka	Význam
Autentizace uživatele	Ověření identifikačních údajů uživatele, např. zadáním hesla, případě více faktorovou autentizací, tj. zadáním dalších informací. Zpravidla se v rámci procesu autentizace počítá i s procesem identifikace.
CRŽP	Agendový informační systém Centrální registr životního prostředí. (https://crzp.mzp.cz)
EnvIAM	Aplikace, která poskytuje autentizační služby systémům IS/AIS MŽP. (https://iam.env.cz/cas/login)
IS	Informační systém
JIP/KAAS	JIP je zkratka pro Jednotný identitní prostor - zabezpečená adresářová služba, obsahující údaje pro autentizaci a autorizaci uživatelů, která je součástí systému Czech POINT. KAAS je zkratka pro Katalog autentizačních a autorizačních služeb – rozhraní webových služeb, které umožňují jednak autentizaci uživatelů přistupujících do AIS či ISVS pomocí přihlašovacích údajů v JIP, jednak umožňují editaci údajů subjektů a uživatelských účtů v JIP.
MFA (vícefaktorová autentizace)	Zvýšení důvěryhodnosti procesu autentizace poskytnutím dvou nebo více důkazů (faktorů) potvrzujících identitu uživatele: znalost (něco, co ví pouze uživatel, např. heslo), vlastnictví (něco, co má pouze uživatel – telefon, email) a charakteristika (něco, čím je pouze daný uživatel – biometrie). EnvIAM nabízí možnost dvoufaktorové autentizace, kdy prvním faktorem je heslo uživatele a druhým faktorem je jednorázový kód s omezenou časovou platností (OTP) zaslané uživateli prostřednictvím SMS nebo email zprávy.
MŽP	Ministerstvo životního prostředí
NIA	Národní bod pro identifikaci a autentizaci je českým státem provozovaný informační systém veřejné správy podporující proces elektronické identifikace a autentizace prostřednictvím kvalifikovaného systému. https://info.identitaobcana.cz/
SSO	Metoda přihlašování Single Sign-On umožňuje použít jedno přihlášení do více AIS systémů zároveň. Uživatel se tak v rámci typicky jednoho webového prohlížeče přihlásí k jednomu systému, který uživatele ověří. Pokud se následně uživatel v rámci daného prohlížeče pokusí přihlásit do jiného systému, který disponuje propojením s EnvIAM, je daným AIS systémem považován jako ověřený a nevyžaduje po uživateli opětovné zadání přihlašovacích údajů.

Zkratka	Význam
Systémy IS/AIS	V rámci této příručky se jedná se o agendové informační systémy (AIS), aplikace a informační systémy MŽP, které jsou s aplikací EnvIAM integrovány, tj. využívají její služby poskytování identity. Jedná se např. o systémy ISOH, IPO, HNVO, SEPNO, ISPOP a CRŽP.

2 REGISTRACE UŽIVATELE

Pro přihlášení uživatele do některé z integrovaných aplikací s EnvIAM je zapotřebí mít platný účet v Centrálním registru životního prostředí. Pokud tomu tak není, je nutné se do systému CRŽP zaregistrovat na stránkách https://crzp.mzp.cz/registrace. V rámci profilu uživatele systému CRŽP je kromě kontaktních údajů možné nastavit údaje pro dvoufaktorové ověření (viz kap. 4) a také připojit externí účet poskytovatele identity (viz kap. 5). Více informací o systému CRŽP je k dispozici na https://crzp.mzp.cz/portal .



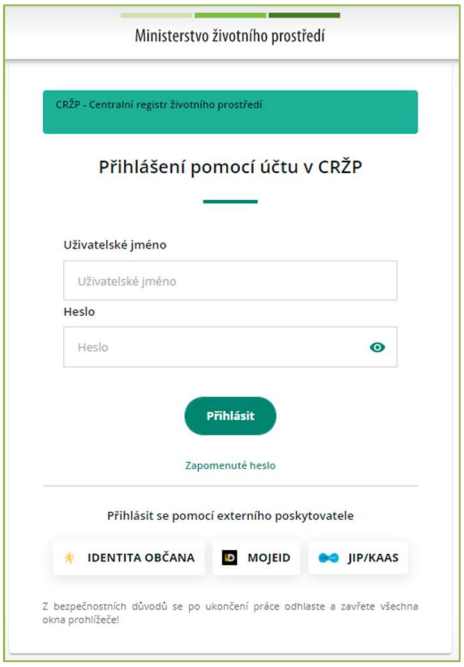
Obrázek 1: Profil uživatele v CRŽP

3 PŘIHLÁŠENÍ UŽIVATELE

V případě, že systém IS/AIS MŽP vyžaduje přihlášení uživatele, je uživatel automaticky přesměrován na přihlašovací stránku EnvIAM. V daném formuláři je uživateli umožněno přihlásit se pomocí uživatelského účtu vedeného v CRŽP nebo účtem externího poskytovatele jako je NIA, JIP/KAAS a MojeID.

V případě přihlášení prostřednictvím účtu v CRŽP musí uživatel vyplnit uživatelské jméno a heslo (pro kontrolu správnosti hesla může uživatel zobrazit heslo v čitelné formě stisknutím symbolu oka (tato funkcionalita je dostupná pouze ve webovém prohlížeči na počítači, nikoliv na mobilním zařízení). Heslo je zobrazeno jen po dobu stisknutí daného symbolu oka, kdy se změní na symbol přeškrtnutého oka – pokud

uživatel při stisku souběžně odjede myší mimo tento symbol, bude heslo viditelné trvale až do opětovného stisknutí tlačítka).



Obrázek 2: Formulář přihlášení uživatele.

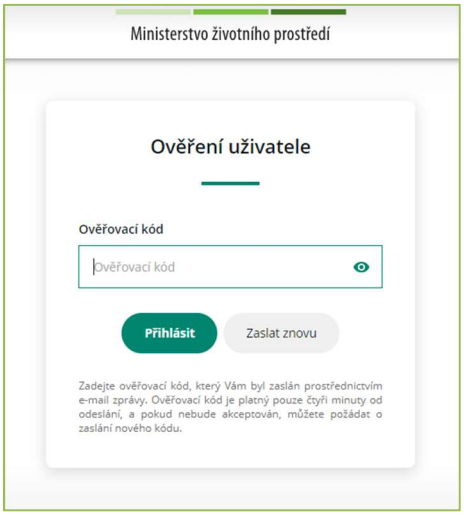
V případě, kdy se uživatel pokusil přihlásit nesprávnými údaji, systém mu zobrazí chybovou hlášku „Neplatné přihlašovací údaje“ tak, jak je vidět na obrázku níže.

Obrázek 3: Neplatné přihlašovací údaje CRŽP

Pro úspěšné přihlášení je třeba zadat platné přihlašovací údaje evidované v rámci CRŽP.

4 VÍCE FAKTOROVÁ AUTENTIZACE

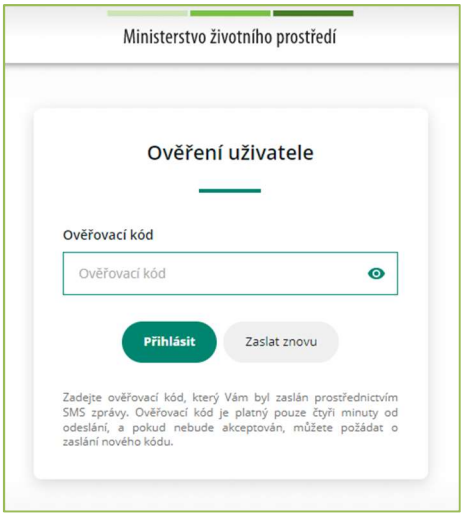
V rámci procesu přihlášení je uživatel po zadání přihlašovacích údajů vyzván k zadání ověřovacího kódu, který byl uživateli zaslán na email či telefon. Výběr komunikačního kanálu pro zaslání ověřovacího kódu si uživatel volí v osobním profilu CRŽP. Ověřovací kód je platný 4 minuty od pokusu o přihlášení a v rámci doručení kódu je v textu uvedena jeho platnost. Obdržený ověřovací kód se vloží do formuláře pro zadání ověřovacího kódu, jak je v případě nastavení emailu jako druhého faktoru vidět na obrázku níže.



Obrázek 4: Zadávací formulář ověřovacího kódu - email

Pokud uživateli do 4 minut nedorazí email s ověřovacím kódem, je třeba nejprve ověřit, zda-li email není v emailové složce určené pro spam. Pokud není, je možné opětovně požádat o zaslání ověřovacího kódu pomocí tlačítka „Zaslat znovu“.

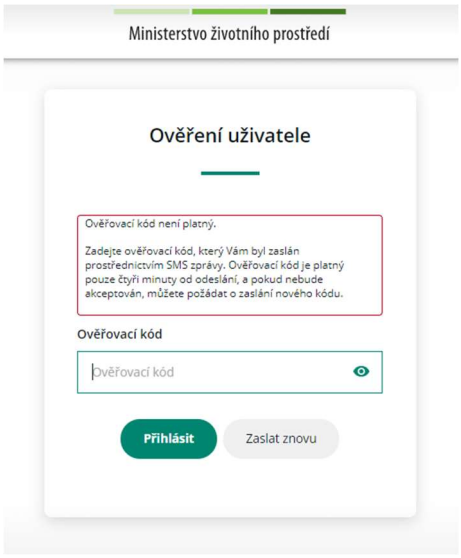
V případě, že má uživatel nastaveno v profilu CRŽP jako preferovaný způsob ověření druhého faktoru SMS, je mu po zadání přihlašovacích údajů zobrazen následující formulář:



Obrázek 5: Zadávací formulář ověřovacího kódu – SMS

V případě, že uživateli nepřijde SMS zpráva s ověřovacím kódem, je možné zažádat o opětovné vygenerování a zaslání ověřovacího kódu pomocí tlačítka „Zaslat znovu“.

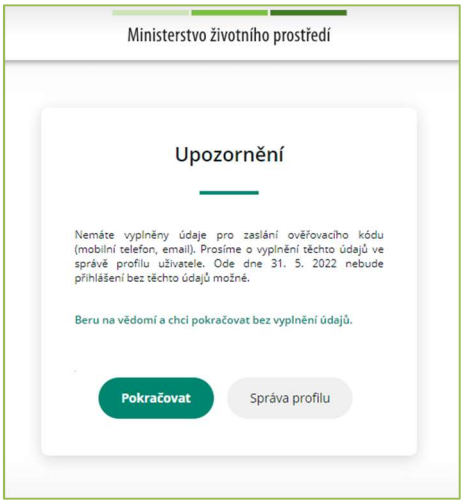
Pokud uživatel zadá neplatný ověřovací kód, je na tuto skutečnost upozorněn chybovou zprávou „Ověřovací kód není platný," jak je vidět na obrázku níže.



Obrázek 6: Neplatný ověřovací kód

V případě opakovaného neobdržení ověřovacího kódu je třeba kontaktovat servisní podporu systému CRŽP a společně provést kontrolu nastavení osobních údajů v profilu CRŽP. Bližší detail je uveden v uživatelské příručce CRŽP umístěné na portále https://crzp.mzp.cz/portal. Pokud i po ověření správnosti údajů nebude doručen ověřovací kód, je třeba kontaktovat servisní podporu MŽP skrz systém EnviHELP.

Pro plynulé zavedení dvoufaktorové autentizace systém EnviIAM upozorní uživatele viz Obrázek 7, pokud ještě nemá uživatel vyplněné údaje pro dvoufaktorové ověření, aby tak učinil ve správě profilu v rámci CRŽP (https://crzp.mzp.cz/crzp/profil). Tato hláška se bude zobrazovat při každém přihlášení, dokud si uživatel nenastaví údaje pro dvoufaktorové ověřování.



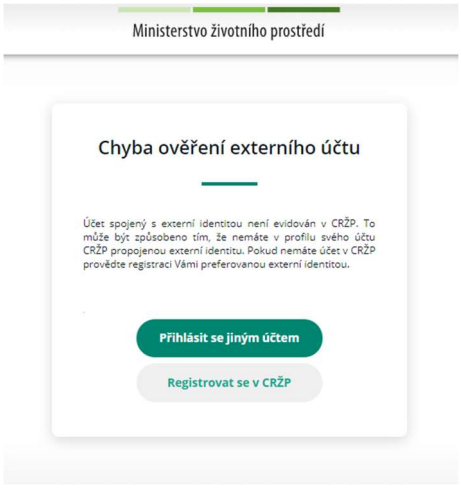
Obrázek 7: Nevyplněné údaje pro více faktorovou autentizaci

5 PŘIHLÁŠENÍ EXTERNÍM ÚČTEM

Systém EnviIAM umožňuje uživatelům využívat pro přihlášení ověřování digitální identity pomocí externích autentizačních poskytovatelů NIA, JIP/KAAS a MojeID. Za tímto účelem je nutné si nejdříve ve

svém uživatelském profilu CRŽP (https://crzp.mzp.cz/crzp/profil) propojit ke svému účtu účet externí. Bližší informace o procesu registrace a úpravy profilu lze nalézt v uživatelské příručce CRŽP umístěné na portále https://crzp.mzp.cz/portal.

V případě, že dojde k chybě při přihlášení pomocí externího účtu, je uživateli zobrazena chybová hláška s možností přihlásit se jiným účtem nebo provést registraci v CRŽP za účelem propojení účtu v CRŽP a účtu externího poskytovatele NIA, MojeID či JIP/KAAS.



Obrázek 8: Chyba při ověření externího účtu

6 NEOPRÁVNĚNÝ PŘÍSTUP K APLIKACI

Po úspěšném ověření identity uživatele systém EnviIAM provede kontrolu, zda-li přihlášený uživatel má přístup k požadovanému systému IS/AIS MŽP. V případě, že uživatel nemá oprávnění k přístupu, je mu zobrazena chybová zpráva „Neoprávněný přístup k aplikaci“, jak je vidět na obrázku níže. V takovém případě je třeba se obrátit na Helpdesk/správce příslušného systému IS/AIS MŽP. Bližší informace o způsobu nastavení oprávnění k požadovanému systému IS/AIS MŽP najdete v příslušné uživatelské příručce daného systému.

Obrázek 9: Neoprávněný přístup k aplikaci

7 DOBA PLATNOSTI PŘIHLÁŠENÍ

Systém EnviIAM rozlišuje 2 doby platnosti přihlášení. Tzv. dobu nečinnosti (Time To Kill), která stanovuje dobu, po kterou uživatel, resp. používaný systém neprovede žádnou akci (tj. nekomunikuje se systémem EnviIAM) a po jejím vypršení je uživatel automaticky odhlášen ze všech IS/AIS. Druhý typ, maximální doba přihlášení (Time To Live) představuje maximální možnou dobu platnosti přihlášení, po jejímž uplynutí je přihlášení automaticky zneplatněno. To způsobí vynucení opětovného přihlášení uživatele systémem

IS/AIS, ve kterém uživatel pracuje, resp. pracoval. Způsob reakce systému na tyto události je popsán v uživatelských příručkách jednotlivých systémů IS/AIS.

Aktuálně je v případě překročení časového limitu sezení, například z důvodu nečinnosti uživatele, dojde k deaktivaci sezení. Pokud mají cílové aplikace implementovanou službu SLO, bude díky ukončení sezení uživatel odhlášen ze všech aplikací využívající stejné sezení a bude následně vynuceno opětovné přihlášení uživatele.

Doba nečinnosti (Time To Kill) je nastavena na 5 hodin a maximální doba (Time To Live) přihlášení je nastavena na 12 hodin. Pokud toto nastane, je uživatel přesměrován na přihlašovací obrazovku AIS systému.

8 ODHLÁŠENÍ UŽIVATELE

Po ukončení práce v systému IS/AIS MŽP je třeba se řádně odhlásit. Způsob odhlášení je pro každý systém IS/AIS různý a je popsán v uživatelských příručkách jednotlivých systémů IS/AIS. Bývá to zpravidla zvolením volby „Odhlásit“ v daném systému. Z důvodu použití SSO si použitý webový prohlížeč pamatuje údaje o přihlášení. Pro zajištění bezpečnosti je důležité po ukončení práce a úspěšném odhlášení uzavřít všechna okna prohlížeče.

9 ŘEŠENÍ PROBLÉMŮ

V případě problémů s přihlášením/ověřením identity uživatele do systémů IS/AIS MŽP se obraťte na servisní podporu MŽP pomocí aplikace EnviHELP.