

Implementace požadavků eIDAS do prostředí aplikace EVID

NABÍDKA

Objednavatel:

Český statistický úřad
Na padesátém 81
100 82 Praha 10

Dodavatel:

ORSIA, spol. s r.o.
Čs. armády 1181
562 01, Ústí nad Orlicí



ORSIA
software

Obsah

1	Úvodní informace	3
1.1	Účel dokumentu a manažerské shrnutí	3
2	Historie dokumentu	3
2.1	Historie změn	3
2.2	Schválení	3
2.3	Distribuce	3
2.4	Použité zkratky a slovníček pojmů	3
3	Popis současného stavu	4
4	Specifikace vynucených změn ve funkčním bloku	5
4.1	Etapa č. 1 - odesílání elektronicky podepsaných Oznámení a Dodatků	5
4.1.1	Úprava v Oznámení a v generování Zpravodajské povinnosti respondentů	5
4.1.2	Úprava v předávání souborů do datových schránek.....	6
4.1.3	Úprava zobrazení „Oznámení“ v části „Informace“	6
4.1.4	Úprava klientské aplikace.....	6
4.2	Etapa č. 2 – pečetění souborů zpravodajské povinnosti respondentů	6
4.2.1	Úprava v generování Zpravodajské povinnosti respondentů	6
5	Stanovení pracnosti	7
6	Návrh harmonogramu	7

1 Úvodní informace

1.1 Účel dokumentu a manažerské shrnutí

Nabídka je předkládána Odboru bezpečnosti a krizového řízení.

Materiál obsahuje nabídku pro Český statistický úřad v souvislosti s počátkem platnosti nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu – dopady do aplikací EVID a Výkazy podle IČO.

Účelem dokumentu je:

- popsat dopady nařízení eIDAS na funkční bloky,
- navrhnout takové úpravy v EVID, aby bylo možné provozovat aplikaci v souladu s uvedeným nařízením.

2 Historie dokumentu

2.1 Historie změn

Verze	Datum verze	Popis změn
1.0	12. 10. 2018	První verze dokumentu

2.2 Schválení

Tento dokument vyžaduje následující schválení:

Jméno a příjmení	Funkce
Ing. Jaromír Makovec	Ředitel Odboru bezpečnosti a krizového řízení

2.3 Distribuce

Tento dokument je distribuován:

Jméno a příjmení	Funkce
Ing. Jaromír Makovec	Ředitel Odboru bezpečnosti a krizového řízení
RNDr René Matýšek	Ředitel Odboru realizačního a vývojového programování

2.4 Použité zkratky a slovníček pojmů

Zkratka	Význam
eIDAS	nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu
HSM	Hardware security module – vysoce specializovaný hardware, jehož primárním úkolem je bezpečně ukládat a spravovat kryptografické objekty (nejčastěji klíče a certifikáty)
HW	Hardware
MD	Man day (práce jednoho člověka v průběhu jednoho dne po dobu osmi hodin)
SIS	Statistický informační systém

3 Popis současného stavu

V souvislosti s počátkem platnosti nařízení Evropské unie č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu vznikají nové požadavky na funkční bloky SIS (Statistického informačního systému). Tyto požadavky je možné realizovat:

- organizačními změnami,
- nákupem služeb a drobného HW spojených s dodávkou kvalifikovaného elektronického podpisu založený na kvalifikovaném certifikátu vytvářeného pomocí kvalifikovaného prostředku,
- nákupem HSM modulu sloužícího jako bezpečné úložiště certifikátů,
- úpravami aplikačního vybavení jednotlivých funkčních bloků SIS.

V současnosti (k 12.10.2018) jsou v souvislosti s počátkem platnosti eIDAS provedeny změny v organizační struktuře, jsou nakupeny služby a drobný hardware pro služby kvalifikovaného elektronického podpisu. Dále je připravováno výběrové řízení na dodávku HSM modulů. Postupně jsou též analyzovány dopady do jednotlivých funkčních bloků SIS.

V souvislosti s dopady eIDAS na funkční bloky EVID a Výkazy podle IČO je vytvářena tato nabídka na vynucené úpravy v uvedených funkčních blocích.

Dopady eIDAS na uvedené funkční bloky lze kategorizovat v souvislosti s dostupností specializovaného HW (v tomto případě HSM Modulu) na:

- změny realizovatelné bez nutnosti využít HSM Modul (v nabídce označeno jako Etapa č. 1)
- změny, které lze realizovat pouze s dostupným HSM modulem (v nabídce označeno jako Etapa č. 2)

V této souvislosti je zapotřebí uvést, že předpokládaný okamžik nákupu HSM modulu, a tedy jeho praktické využitelnosti pro ostatní funkční bloky SIS, je přibližně počátek 2. čtvrtletí 2019.

V Etapě č. 1 je možné realizovat následující požadavky eIDAS:

- odesílání elektronicky podepsaných Oznámení a Dodatků k Oznámení

V Etapě č. 2 je možné realizovat následující požadavky eIDAS:

- pečetění souborů obsahujících uvedení zpravodajské povinnosti elektronickou pečetí ČSÚ

Realizace díla je rozdělena do dvou etap zejména proto, že v lednu roku 2019, tj. v okamžiku, kde bude generováno a následně respondentům rozesíláno nejvíce dokumentů „Oznámení o zpravodajské povinnosti“, nebude dostupný HSM modul bezpečně uchovávací elektronickou pečetí ČSÚ (nákup tohoto HW je očekáván v 1. čtvrtletí 2019).

Aby pro největší dávku rozesílaných Oznámení bylo vyhověno alespoň části požadavků nařízení eIDAS, je realizace díla rozčleněna tak, aby na počátku roku byl respondentům odeslán dopis s Oznámením v podobě dokumentu:

- podepsaného kvalifikovaným elektronickým podpisem,
- opatřeného časovým razítkem ČSÚ.

Pro tuto etapu pak platí, že soubor se „Zpravodajskou povinností respondenta“ není pečetěn elektronickou pečetí ČSÚ.

Každá z etap je tvořena několika dílčími činnostmi popsány dále v tomto dokumentu.

4 Specifikace vynucených změn ve funkčním bloku

Kapitola obsahuje detailní popis změn ve funkčním bloku EVID vynucených implementací požadavků eIDAS.

4.1 Etapa č. 1 - odesílání elektronicky podepsaných Oznámení a Dodatků

V této etapě bude implementována možnost odesílat respondentům pomocí systému datových schránek Oznámení a Dodatek Oznámení opatřené kvalifikovaným elektronickým podpisem. V této souvislosti budou upraveny moduly:

- Oznámení – bude umožněno vložit elektronicky podepsaný dokument,
- Generování souborů se zpravodajskou povinností respondentů vůči ČSÚ,
- Předávání dokumentů do datových schránek,
- Zobrazení dokumentů „Oznámení“ a „Zpravodajská povinnost“,
- Klientská aplikace sloužící k downloadu pdf souborů Oznámení a Dodatků na lokální file systém.

4.1.1 Úprava v Oznámení a v generování Zpravodajské povinnosti respondentů

V současné době obsahuje dokument „Oznámení o zpravodajské povinnosti respondenta“ dvě části tvořící spolu jeden pdf soubor. Nově budou tyto části od sebe odděleny, přičemž část „Dopis k Oznámení“ bude vznikat vně aplikace a druhá část „Zpravodajská povinnost“ bude generována vlastními prostředky aplikace. Systém potlačí aktuálně využívaný algoritmus generování první části ze šablon a místo toho přijme první část vytvářenou vně vlastního systému. Tato první část „Dopis k Oznámení“ bude vkládána ve dvou variantách:

- Dopis k Oznámení,
- Dopis k Dodatku k oznámení.

Vložení první části tak bude v modulu „Oznámení“ realizováno pomocí tlačítek „Upload Dopisu k Oznámení“ a „Upload Dodatku k dopisu k Oznámení“. Uploadované soubory budou opatřeny kvalifikovaným elektronickým podpisem a časovým razítkem ČSÚ již v okamžiku jejich uploadu do aplikace.

V okamžiku generování zpravodajské povinnosti budou vygenerovány pdf soubory se „Zpravodajskou povinností respondentů“. Algoritmus generování musí být upraven tak, aby zohlednil skutečnost, že adresní

štítek respondenta je přesunut z první části dokumentu, tj. z „Dopisu k Oznámení“ do části „Zpravodajská povinnost“.

Vygenerované soubory „Zpravodajské povinnosti respondenta“ nebudou v první etapě opatřeny elektronickou pečeti ČSÚ. Tato úprava bude předmětem druhé etapy, tj. v okamžiku dostupnosti HSM modulu.

4.1.2 Úprava v předávání souborů do datových schránek

Databázový job řídící předávání dokumentů s „Oznámením o zpravodajské povinnosti respondenta“ do systému ESSL (vstupní část systému správy datových schránek ČSÚ) bude upraven tak, aby dokázal dopravit a připravit k odeslání oba soubory tvořící dohromady „Oznámení“, tj. jak soubor „Dopis k oznámení“ tak i soubor „Zpravodajská povinnost respondenta“. V současném stavu je algoritmus připraven pro každého respondenta dopravit do systému datových schránek pouze jeden (původně sloučený) soubor tvořící Oznámení.

4.1.3 Úprava zobrazení „Oznámení“ v části „Informace“

Systém bude upraven tak, že umožní zobrazení jak souboru „Dopis k oznámení“ tak i souboru „Zpravodajská povinnost respondenta“. V současném stavu je algoritmus zobrazení připraven zobrazit pouze jeden (původně sloučený) soubor.

4.1.4 Úprava klientské aplikace

Klientská aplikace slouží k downloadu pdf souborů Oznámení a Dodatků na lokální file systém. Tyto na lokální file systém stažené soubory jsou dále předávány k vytištění na další pracoviště. Poté co dojde k rozdělení původního „Oznámení“ do dvou samostatných souborů je nutné zajistit jejich sloučení do jednoho souboru, a to před jejich downloadem na lokální file systém.

Zároveň je nutné upravit vkládání prázdných stránek tak, aby sloučený a následně stažený pdf soubor měl vždy sudý počet stran a zároveň, aby adresní štítek respondenta byl vždy umístěn poslední liché straně dokumentu.

4.2 Etapa č. 2 – pečetení souborů zpravodajské povinnosti respondentů

V této etapě bude implementováno automatické vkládání elektronické pečeti do souborů zpravodajské povinnosti respondentů vůči ČSÚ.

4.2.1 Úprava v generování Zpravodajské povinnosti respondentů

Algoritmus bude upraven tak, aby v okamžiku, kdy se dokončí generování souboru, došlo k automatickému vyžádání elektronické pečeti z HSM modulu a jejímu připojení k výslednému souboru zpravodajské povinnosti respondenta s následným uložením do databáze.

5 Stanovení pracnosti

Položky „Analytické práce“, „Programování“ a „Testování a ověřování“ obsahují stanovení pracnosti transformace současného stavu jednotlivých modulů a jejich funkcionalit do stavu cílového, popsaného v předchozích kapitolách. Položka „Projektová režie“ zahrnuje čas nutný k úspěšnému zvládnutí projektu na administrativní a projektové rovině.

Celkový rozsah projektu zahrnuje všechny činnosti požadované ke zdárnému dokončení projektu a je stanoven jako konečný a z pozice dodavatele nepřekročitelný.

Tabulka 1 Odhad pracnosti

Činnost	Etapa 1	Etapa 2
	MD	MD
Analytické práce	3	2
Programování	10	2
Testování a ověřování	3	2
Projektová režie	1	0,5
Celkem vývoj	17	5,5
Cena za 1 MD platná pro obě etapy projektu	= 10 000 Kč bez DPH	

Celková cena za obě etapy projektu 225 000 Kč bez DPH. Sazba DPH = 21 %.

6 Návrh harmonogramu

Harmonogram vychází z činností, které bude nutné provést během fáze vytvoření, testování, ověřování a nasazení nové, transformované aplikace do testovacího a posléze i do produkčního prostředí ČSÚ.

Tabulka 2 - Harmonogram úprav v jednotlivých prostředích

Činnost	Ukončení činnosti v týdnech	
	Etapa 1	Etapa 2
Popis smlouvy / potvrzení výzvy k plnění		
Zahájení prací – čas T	T	T
Analytické práce	T+1	T+1
Dodání požadovaných funkcionalit do testovacího prostředí	T+3	T+2
Předání do plného provozu	T+4	T+3

Čas „T“ – označuje počáteční okamžik (start) dané etapy projektu.

Za ORSIA spol. s r. o. zpracoval

X

Petr Gregor

Petr Gregor
prokurista