Česká národní banka

Příloha č. 4
Pravidel systému CERTIS

Náhradní způsoby předávání a přebírání datových souborů

Verze 6

účinnost od 1. února 2022

OBSAH

1 Úvod

Není-li účastník schopen předávat a přebírat data prostřednictvím AMOSu, lze data, po telefonické dohodě s provozovatelem systému CERTIS, předat/převzít prostřednictvím e-mailu (viz kap. 5) nebo osobně v ČNB (viz kap. 6).

V obou případech musí být data opatřena uznávaným elektronickým podpisem nebo uznávanou elektronickou pečetí a doprovozena průvodním listem (viz kap. 2). Data se předávají zašifrovaná (viz kap. 3), v případě osobního předávání lze předávat i nešifrovaná data. Předpis pro jména souborů je uveden v kapitole 4.

2 Elektronický podpis, průvodní list

Data jsou podepsána uznávaným elektronickým podpisem nebo uznávanou elektronickou pečetí stejně, jako data předávaná prostřednictvím AMOSu.

Použijí se podpisové certifikáty, které jsou zaregistrovány v AMOSu. Počet podpisů nebo pečetí vstupních dat je provozovateli sdělen pověřenou osobou (viz Pravidla CERTIS, článek 16 odst. 2 písm. b).

Výstupní datové soubory ze systému CERTIS budou opatřeny zaručenou elektronickou pečetí s využitím kvalifikovaného certifikátu systému CERTIS (viz příloha č. 2 Pravidel).

Současně s datovými soubory budou předány průvodní listy podepsané osobou uvedenou v podpisových vzorech účastníka systému CERTIS (viz Pravidla CERTIS, článek 16 odst. 2 písm. e a odst. 4). Na jednom tiskopisu je možné uvést více datových souborů s daty.

Pokud provozovatel předává průvodní list v elektronické formě bez podpisu podle předchozího odstavce, musí být opatřen zaručenou elektronickou pečetí s využitím kvalifikovaného certifikátu systému CERTIS (viz příloha č. 2 Pravidel).

Elektronický podpis (pečeť) zajišťuje autorizaci dat. Průvodní list je pokynem pro ČNB, že mají být data vložena do systému CERTIS.

3 Šifrování dat, komerční certifikáty

3.1 Šifrování dat

Vstupní soubory s položkami (INTOCC) a výstupní soubory s položkami (FROMCC) se předávají v zašifrované podobě.

Zašifrovaná zpráva musí být vytvořena ve struktuře envelopedData dle PKCS#7 v DER kódování. Vhodné algoritmy pro šifrování jsou uvedeny v dokumentu Doporučení v oblasti kryptografických prostředků, který je dostupný na stránkách NÚKIB (nukib.cz).

Pro šifrování je nutno používat komerční certifikáty vydané certifikačními autoritami PostSignum, 1.CA nebo e-Identity.

3.2 Komerční certifikáty

Komerční certifikát ČNB, který použije účastník systému CERTIS pro šifrování vstupních INTOCC souborů, je možné stáhnout v AMOSu v sekci „Různé / Nápověda, dokumenty, kontakty“ pod odkazem „Šifrovací certifikát“.

Pro šifrování FROMCC souborů použije ČNB komerční certifikáty účastníků vydané certifikačními autoritami PostSignum, 1.CA nebo e-Identity. Účastníci zašlou své komerční certifikáty e-mailem na adresu certis@cnb.cz. Do předmětu e-mailu uvedou kód účastníka a text „komerční certifikáty“ (např. Předmět: 0800 komerční certifikáty). Certifikát by měl být v DER kódování (přípona .cer). Příponu souboru je potřeba rozšířit o řetězec .txt (např. cert10730772.cer.txt), aby nedošlo k zablokování souboru při odeslání poštou. Před koncem platnosti komerčního certifikátu je účastník povinen zaslat nový komerční certifikát.

4 Jmenné konvence

Jméno datového souboru s položkami má tvar RRRRMMDD_XXXX_NNNNNN, kde

RRRRMMDD je datum účetního dne, ve kterém má být vstupní datový soubor zpracován, resp. ve kterém byl výstupní datový soubor vytvořen,

XXXX je numerický identifikační kód účastníka,

NNNNNN je číslo datového souboru.

Přípona se liší podle obsahu souboru:

- bez přípony – vlastní datový soubor s položkami,
- .ep1 – soubor s prvním podpisem,
- .ep2 – soubor s druhým podpisem,
- .p7e – šifrovaný datový soubor.

ČNB generuje čísla výstupních souborů v rozmezí od 501 do 899. Proto je vhodné, aby účastník čísla z tohoto rozsahu nepoužíval pro vstupní soubory.

5 Předávání souborů e-mailem

5.1 INTOCC soubory

INTOCC soubory se zasílají na adresu certis@cnb.cz. Do předmětu e-mailu se uvede kód účastníka a „INTOCC“ (např. Předmět: 0800 INTOCC). Účastník zasílá emaily ve frekvenci maximálně jedenkrát za hodinu pro neprioritní soubory a maximálně dvakrát za hodinu v případě prioritních souborů, v případě naplnění vstupního souboru na velikost 10MB je možno soubory zasílat častěji.

Přiložený soubor (soubory) by měl být zašifrován. ČNB však akceptuje od účastníka i nezašifrované soubory[1].

Současně s datovými soubory předává účastník průvodní list podepsaný osobou uvedenou v podpisových vzorech. Účastník může předat provozovateli průvodní list e-mailem nebo faxem; zaslání e-mailu nebo faxu je povinen provozovateli neprodleně telefonicky potvrdit.

Po zpracování všech souborů z e-mailu zašle ČNB zpět potvrzovací e-mail. V případě chyb bude přiložen protokol.

5.2 FROMCC soubory

FROMCC soubory zasílá ČNB na e-mailové adresy stanovené účastníkem. V e-mailu ČNB zasílá zašifrované soubory s daty, soubory s podpisy a průvodní listy.

Do předmětu e-mailu se uvede kód účastníka a „FROMCC“ (např. Předmět: 0800 FROMCC).

[1] Ochrana dat, která jsou v držení účastníka, je jeho výhradní zodpovědností. Zašle-li data nezašifrovaná, riskuje tím porušení důvěrnosti dat a je plně zodpovědný za případné následky. ČNB však nemá důvod takto zaslaná data nezpracovat.

Účastníci zašlou své e-mailové adresy, na které bude ČNB zasílat FROMCC soubory, e-mailem na adresu certis@cnb.cz. Do předmětu e-mailu uvedou kód účastníka a text „e-mailové adresy“ (např. Předmět: 0800 e-mailové adresy).

ČNB bude e-mailem zasílat účastníkovi vždy zašifrované soubory.

6 Osobní předávání a přebírání

6.1 INTOCC soubory

Při osobním předávání INTOCC souborů se používá flash disk.

Na médiu jsou uloženy zašifrované soubory s daty a soubory s podpisy. Soubory se šifrují podle popisu v kap. 3.

ČNB akceptuje od účastníka i nezašifrované soubory s daty[1].

Současně s datovými soubory předává účastník průvodní list podepsaný osobou uvedenou v podpisových vzorech. Účastník může předat provozovateli průvodní list i e-mailem, faxem nebo na flash disku; zaslání e-mailu nebo faxu je povinen provozovateli neprodleně telefonicky potvrdit.

Zpracování souborů potvrdí ČNB telefonicky nebo zašle potvrzovací e-mail.

6.2 FROMCC soubory

Při osobním předávání FROMCC souborů se používá flash disk.

Na médiu jsou uloženy zašifrované soubory s daty a soubory s podpisy. K médiu je přiložen průvodní list.

Na žádost účastníka podepsanou pověřenou osobu může ČNB předávat účastníkovi i nezašifrované soubory[2].

[2] Ochrana dat, která jsou v držení účastníka, je jeho výhradní zodpovědností. Po předání dat osobě, kterou určil účastník, jsou data v držení účastníka. Vyžádá-li si účastník data nezašifrovaná, riskuje tím porušení důvěrnosti dat a je plně zodpovědný za případné následky. ČNB tuto variantu nepreferuje, je však připravena účastníkovi vyhovět.