9/2011 Sb.

VYHLÁŠKA

ze dne 10. ledna 2011,

kterou se stanoví podrobnější podmínky týkající se elektronických nástrojů a úkonů učiněných elektronicky při zadávání veřejných zakázek a podrobnosti týkající se certifikátu shody

Ministerstvo pro místní rozvoj stanoví podle § 159 odst. 3 zákona č. 137/2006 Sb. , o veřejných zakázkách, ve znění zákona č. 179/2010 Sb. , (dále jen „zákon“) k provedení § 149 odst. 8 a 9 zákona :

ČÁST PRVNÍ

OBECNÁ USTANOVENÍ

§ 1

Předmět úpravy

Tato vyhláška upravuje

a) podrobnější podmínky týkající se elektronických nástrojů a úkonů učiněných elektronicky při zadávání veřejných zakázek,

b) podrobnosti týkající se podmínek pro vydání certifikátu shody, údajů v certifikátu shody a platnosti certifikátu shody.

§ 2

Vymezení pojmů

Pro účely této vyhlášky se rozumí

a) veřejným klíčem zadavatele jedinečná elektronická data, která jednoznačně odpovídají soukromému klíči zadavatele a slouží dodavateli k zašifrování obsahu nabídky podle této vyhlášky,

b) soukromým klíčem zadavatele jedinečná elektronická data, která jednoznačně odpovídají veřejnému klíči zadavatele a slouží zadavateli k odšifrování obsahu nabídky podle této vyhlášky,

c) certifikátem veřejného klíče datová zpráva [1)] , která důvěryhodným způsobem spojuje veřejný klíč zadavatele se zadavatelem, slouží k přenášení veřejného klíče a může sloužit k ověřování identity zadavatele a adresy jeho internetových stránek,

d) elektronickým úkonem v zadávacím řízení úkon jednající osoby provedený prostřednictvím elektronického nástroje,

e) provozními parametry soubor požadavků vztahujících se k funkčním vlastnostem elektronického nástroje a k prostředí, ve kterém je elektronický nástroj provozován, jež vyplývají z

přílohy této vyhlášky,

f) funkcionalitou souhrn funkčních vlastností, které elektronický nástroj má,

g) prostředím podmínky, za kterých je elektronický nástroj provozován,

h) provozovatelem elektronického nástroje fyzická nebo právnická osoba, která konkretizuje provozní parametry a zajišťuje provoz elektronického nástroje, jehož prostřednictvím jsou nebo mají být prováděny elektronické úkony za účelem zadávání veřejných zakázek nebo za účelem získání návrhu v soutěži o návrh a který splňuje požadavky stanovené zákonem a touto vyhláškou,

i) žadatelem provozovatel, který požádá o posouzení shody a udělení certifikátu shody,

j) nešifrovanou datovou zprávou datová zpráva, ve které nejsou přenášené údaje skryty například šifrováním a jsou přímo čitelné,

k) šifrovanou datovou zprávou datová zpráva, ve které jsou přenášené údaje skryty pomocí šifrování a nejsou tak přímo čitelné,

l) časovou informací zaznamenání data a času elektronického úkonu s uvedením hodiny, minuty a sekundy,

m) certifikačním auditem proces ověřování shody elektronického nástroje prováděný subjektem posuzování shody akreditovaným vnitrostátním akreditačním orgánem na základě jiného právního předpisu [2)] (dále jen „certifikační orgán“),

n) certifikačními pravidly souhrn podmínek a předpokladů stanovených certifikačním orgánem,

o) vyhlášením oznámení o zahájení zadávacího řízení, předběžné oznámení, pravidelné předběžné oznámení, oznámení soutěže o návrh, oznámení o výsledku zadávacího řízení, oznámení o zrušení zadávacího řízení nebo soutěže o návrh nebo i jiné údaje, jež se uveřejňují v informačním systému o veřejných zakázkách, případně v Úředním věstníku Evropské unie,

p) aktivem jakákoli součást elektronického nástroje a provozního prostředí včetně zdrojů, která je nezbytná k provozování elektronického nástroje v zamýšleném rozsahu.

ČÁST DRUHÁ

ELEKTRONICKÉ ÚKONY A ELEKTRONICKÉ NÁSTROJE

§ 3

Obecné požadavky na provádění elektronických úkonů při zadávání veřejných zakázek

V zadávacím řízení určí zadavatel oprávněné osoby, které jsou za zadavatele oprávněné činit v tomto řízení elektronické úkony, zejména činit výzvy k účasti nebo k podání nabídek, poskytovat zadávací dokumentaci a dodatečné informace, potvrzovat doručení nabídek, provádět otevírání nabídek a zasílat pozvání k jednání o nabídkách.

§ 4

Poskytování zadávací dokumentace a dodatečných informací

(1) Zadávací dokumentaci, kterou zadavatel poskytuje prostřednictvím elektronických

nástrojů, poskytuje zadavatel formou neomezeného dálkového přístupu na svém profilu nebo i na jiné adrese internetových stránek bez předchozí žádosti, nebo ji poskytuje na základě písemné žádosti opatřené elektronickým podpisem.

(2) Poskytuje-li zadavatel zadávací dokumentaci neomezeným dálkovým přístupem na svém profilu nebo i na jiných internetových stránkách bez předchozí žádosti, zajistí, aby

a) každý se mohl ujistit o identitě zadavatele i o identitě provozovatele internetových stránek formou certifikátu veřejného klíče vydaného k profilu zadavatele nebo k adrese internetových stránek, prostřednictvím kterých zadavatel poskytuje zadávací dokumentaci,

b) zadávací dokumentace byla chráněna proti neoprávněné změně a

c) zadávací dokumentace byla ve stanovené lhůtě přístupná na profilu zadavatele nebo na jiných internetových stránkách nepřetržitě.

(3) Poskytuje-li zadavatel zadávací dokumentaci na základě písemné žádosti dodavatele, zajistí, aby

a) zadávací dokumentace byla poskytnuta jen na základě platně doručené žádosti osoby, jejíž elektronický podpis byl úspěšně ověřen,

b) zadávací dokumentace byla opatřena elektronickým podpisem oprávněné osoby zadavatele nebo elektronickou značkou zadavatele, pokud bude zadávací dokumentace poskytnuta formou odeslání na požadovanou elektronickou adresu dodavatele, a

c) byly splněny požadavky podle odstavce 2 , pokud bude zadávací dokumentace poskytnuta formou individuálního zpřístupnění zadávací dokumentace prostřednictvím profilu zadavatele nebo jiných internetových stránek.

(4) Na poskytování dodatečných informací k zadávacím podmínkám se použijí ustanovení odstavců 1 až 3 obdobně.

§ 5

Podávání a otevírání nabídek

(1) Ve vyhlášení nebo ve výzvě se uveřejňuje elektronická adresa pro podávání nabídky, předběžné nabídky, žádosti o účast, návrhu v soutěži o návrh a podávání aukčních hodnot (dále jen „nabídka“).

(2) Nabídky musí být za účelem zajištění důvěrnosti údajů v nich obsažených vždy chráněny šifrováním jejich obsahu v souladu s požadavky stanovenými touto vyhláškou. To neplatí v případě podávání aukčních hodnot za podmínky, že je technicky v souladu s touto vyhláškou zajištěno zachování důvěrnosti obsahu nabídky.

(3) Zadavatel zajistí, aby

a) veřejný klíč zadavatele určený k šifrování obsahu nabídek jednoznačně odpovídal soukromému klíči zadavatele,

b) nebylo možné za vynaložení přiměřeného úsilí certifikát veřejného klíče padělat,

c) nebylo možné za vynaložení přiměřeného úsilí soukromý klíč zadavatele padělat a

d) soukromý klíč zadavatele byl zajištěn proti ztrátě a neoprávněnému přístupu po celou dobu

platnosti odpovídajícího certifikátu veřejného klíče.

(4) Za účelem šifrování obsahu nabídky poskytuje zadavatel dodavatelům prostřednictvím svého profilu, případně jiných internetových stránek nebo zasláním na základě vyžádání certifikát veřejného klíče.

(5) Je-li stanovena v souladu se zákonem lhůta pro podávání nabídky, zadavatel zajistí, aby nabídka podaná na adresu podle odstavce 1

a) před uplynutím stanovené lhůty byla dále zpracována v souladu s touto vyhláškou a uložena v nezměněné podobě do doby jejího otevření; zároveň bude odesláno dodavateli na jeho elektronickou adresu oznámení o jejím doručení a

b) po uplynutí stanovené lhůty byla označena jako nepřijatelná; v takovém případě bude odesláno dodavateli na jeho elektronickou adresu oznámení o této skutečnosti.

(6) Podání nabídky musí být opatřeno záznamem časové informace podle § 7 .

(7) Po podání nabídky bude ověřena platnost elektronického podpisu dodavatele a výsledek ověření se zaznamená k doručené nabídce.

(8) Zadavatel nebo osoby oprávněné k otevírání nabídek zajistí odšifrování obsahu nabídek s využitím soukromého klíče zadavatele.

(9) Zadavatel zajistí, aby odšifrování i otevření nabídek s využitím soukromého klíče zadavatele prováděly oprávněné osoby tak, aby

a) odšifrování nebo otevření bylo provedeno vždy za účasti dvou nebo více oprávněných osob,

b) nebylo možné použít soukromý klíč zadavatele k odšifrování nabídek jiným způsobem než za účasti oprávněných osob.

(10) Provozovatel zajistí, aby elektronický nástroj neumožnil odšifrování a otevření nabídky před lhůtou stanovenou k jejímu otevření. Čas odšifrování a otevření nabídky musí být v souladu s § 6 zaznamenán.

(11) Elektronická nabídka, po jejím otevření, přečtení, posouzení nebo hodnocení, musí spolu se záznamem o ověření platnosti elektronického podpisu zůstat uložena u zadavatele v zašifrované podobě, v jaké byla zadavateli doručena. Tím není dotčena možnost zadavatele ponechat vedle toho nabídky uložené rovněž v odšifrované podobě.

§ 6

Pořizování záznamů o elektronických úkonech

(1) O provedených elektronických úkonech a veškerých dalších činnostech elektronického nástroje zadavatel povede evidenci. Součástí této evidence musí být alespoň

a) určení elektronického úkonu nebo další činnosti elektronického nástroje,

b) čas provedení elektronického úkonu nebo činnosti uvedený s přesností na sekundu,

c) identifikátor osoby, která elektronický úkon provedla nebo činnost elektronického nástroje zahájila,

d) záznam o případném chybovém výsledku elektronického úkonu nebo další činnosti

elektronického nástroje.

(2) Kromě záznamů podle odstavce 1 musí být zaznamenány i informace o systémovém stavu elektronického nástroje podle písmen b) a c) s uvedením časové informace podle § 7 . Systémovým stavem je stav, ve kterém se v daném okamžiku nebo intervalu nachází elektronický nástroj, a který odpovídá jedné ze tří možných hodnot

a) v provozu,

b) mimo provoz,

c) omezení funkcionality neumožňující realizovat elektronické úkony, které jinak prostřednictvím daného elektronického nástroje realizovat lze.

(3) Veškeré údaje podle odstavců 1 a 2 musí být chráněny proti neoprávněnému přístupu, změně a zničení.

§ 7

Zaznamenávání časové informace

(1) Časová informace musí být poskytovaná operačním systémem navázaným na zdroj reprodukující světový koordinovaný čas UTC například na státní etalon času a frekvence nebo pomocí přijímače globálního systému určování polohy (GPS).

(2) Synchronizace času měřeného operačním systémem podle odstavce 1 s koordinovaným světovým časem se provádí alespoň jedenkrát za 24 hodin v průběhu zadávacího řízení.

(3) Synchronizace podle odstavce 2 musí být zajištěna i v případě výskytu přestupné sekundy.

ČÁST TŘETÍ

CERTIFIKACE SHODY ELEKTRONICKÝCH NÁSTROJŮ

§ 8

Certifikát shody

(1) Shoda elektronického nástroje se posuzuje z hlediska funkcionality elektronického nástroje a z hlediska prostředí, ve kterém je elektronický nástroj provozován. Podrobné požadavky týkající se funkčních vlastností elektronického nástroje a prostředí, ve kterém má být elektronický nástroj provozován, jsou uvedeny v příloze této vyhlášky.

(2) Pro účely posuzování shody funkcionality elektronického nástroje jsou elektronické úkony rozděleny na

a) elektronické úkony nezahrnující přenos a příjem nabídek
1. odesílání a příjem datových zpráv,
2. elektronické úkony zadavatele bez odesílání datové zprávy,
3. jednání zadavatele nebo orgánu ustanoveného zadavatelem (komise) s dodavatelem prostředky umožňujícími dálkový přístup,
4. poskytování dokumentů dálkovým přístupem,

b) elektronické úkony spočívající v přenosu a příjmu nabídek.

(3) Certifikát shody musí obsahovat alespoň tyto údaje:

a) obchodní firmu nebo název, sídlo, právní formu, identifikační číslo osoby, bylo-li přiděleno, pokud jde o právnickou osobu, a obchodní firmu nebo jméno a příjmení, místo podnikání, popřípadě místo trvalého pobytu, identifikační číslo osoby, bylo-li přiděleno, pokud jde o fyzickou osobu, certifikačního orgánu, který certifikát shody vydal,

b) obchodní firmu nebo název, sídlo a právní formu provozovatele, jedná-li se o právnickou osobu,

c) jméno a příjmení, popřípadě obchodní firmu, a místo podnikání, popřípadě místo trvalého pobytu provozovatele, jedná-li se o fyzickou osobu,

d) identifikační číslo osoby provozovatele, pokud bylo přiděleno,

e) obchodní označení a verzi elektronického nástroje,

f) uvedení skupiny elektronických úkonů v členění podle odstavce 2 , pro které byl elektronický nástroj certifikován v souladu s požadavky stanovenými touto vyhláškou, a výčet elektronických úkonů v rámci této skupiny,

g) datum vydání certifikátu shody,

h) dobu platnosti certifikátu shody a

i) podpis osoby oprávněné jednat za certifikační orgán.

(4) Certifikát shody je možno vydat v listinné podobě nebo v elektronické podobě s platným elektronickým podpisem osoby oprávněné jednat jménem nebo za certifikační orgán.

(5) Certifikát shody se vydává v českém jazyce.

(6) Pokud provozovatel předloží platný certifikát shody, prokazuje, že v rozsahu skupiny elektronických úkonů a údajů uvedených v certifikátu shody splňuje jím provozovaný elektronický nástroj požadavky stanovené zákonem a touto vyhláškou.

(7) Pokud je elektronický nástroj provozován jinou osobou než žadatelem, který prokázal shodu a disponuje platným certifikátem shody, může pro takový elektronický nástroj tato jiná osoba k prokázání splnění požadavků stanovených právními předpisy předložit platný certifikát shody tohoto jiného provozovatele. V takovém případě elektronický nástroj splňuje v rozsahu skupiny elektronických úkonů uvedených v certifikátu shody požadavky stanovené zákonem na funkční vlastnosti elektronického nástroje. Předložením certifikátu shody jiného provozovatele však nelze prokázat shodu s požadavky týkajícími se prostředí, ve kterém je elektronický nástroj provozován.

§ 9

Podrobnosti týkající se podmínek pro vydání certifikátu shody

(1) Žádost o vydání certifikátu shody podává žadatel certifikačnímu orgánu. Žadatel prokazuje v žádosti a následném certifikačním auditu shodu elektronického nástroje s požadavky stanovenými právními předpisy ve vztahu k funkcionalitě elektronického nástroje a ve vztahu k prostředí, v němž je elektronický nástroj provozován. Shodu elektronického nástroje prokáže žadatel, pokud elektronický nástroj splňuje alespoň požadavky stanovené v příloze této vyhlášky.

(2) Pokud má elektronický nástroj platný certifikát shody ve vztahu k funkcionalitě a je provozován jinou osobou než žadatelem, kterému byl certifikát shody vydán, prokazuje tato jiná osoba jako žadatel certifikačnímu orgánu pouze splnění požadavků ve vztahu k provoznímu prostředí, v němž je elektronický nástroj provozován, ve smyslu přílohy této vyhlášky.

(3) Žádost o vydání certifikátu shody musí splňovat minimálně náležitosti stanovené v § 10 . V případě uvedeném v odstavci 2 musí být přílohou žádosti o vydání certifikátu shody platný certifikát shody, který byl pro elektronický nástroj vydán. Certifikační orgán vydá certifikát shody pro elektronický nástroj, pokud byla zjištěna shoda elektronického nástroje s požadavky uvedenými v příloze této vyhlášky, a to v rozsahu zjištěné shody. Certifikační orgán není oprávněn vydat certifikát shody pro elektronický nástroj nad rámec podané žádosti o vydání certifikátu shody.

(4) Podrobná certifikační pravidla stanoví certifikační orgán. Certifikační pravidla musí s ohledem na jednotlivé druhy certifikátů shody obsahovat aspoň

a) adresu pro podání žádosti o vydání certifikátu shody,

b) obsahové a formální náležitosti žádosti o vydání certifikátu shody,

c) popis jednotlivých kroků certifikačního auditu,

d) časovou náročnost certifikačního auditu,

e) obsahové a formální náležitosti výstupu z certifikačního auditu,

f) ceník odměn za úkony činěné certifikačním orgánem, který bude obsahovat aspoň
1. výši odměny za provedení certifikačního auditu,
2. výši odměny za provedení certifikačního auditu na prodloužení platnosti certifikátu shody osvědčujícího soulad s požadavky kladenými na prostředí podle § 11 odst. 1 ,
3. výši odměny za změnu certifikátu v důsledku změny vlastností či podmínek elektronického nástroje podle § 11 odst. 2 ,
4. výši odměny za změnu rozsahu certifikátu shody podle § 11 odst. 4 a
5. výši odměny pro případ, že bude certifikační orgán postupovat podle § 11 odst. 3 ,

g) opatření k nápravě.

(5) Certifikační pravidla je certifikační orgán povinen uveřejnit na svých internetových stránkách.

§ 10

Minimální náležitosti žádosti o vydání certifikátu shody

(1) V žádosti o vydání certifikátu shody uvede žadatel své identifikační údaje, kterými jsou obchodní firma nebo název, sídlo, právní forma, identifikační číslo, bylo-li přiděleno, pokud jde o právnickou osobu, a obchodní firma nebo jméno a příjmení, místo podnikání, popřípadě místo trvalého pobytu, identifikační číslo, bylo-li přiděleno, pokud jde o fyzickou osobu.

(2) V případě, že žadatelem o vydání certifikátu shody je osoba, která není výrobcem elektronického nástroje, uvede žadatel v žádosti o vydání certifikátu shody identifikační údaje výrobce, kterými jsou obchodní firma nebo název, sídlo, právní forma, identifikační číslo, bylo-li přiděleno, pokud jde o právnickou osobu, a obchodní firma nebo jméno a příjmení, místo podnikání, popřípadě místo trvalého pobytu, identifikační číslo, bylo-li přiděleno, pokud jde o fyzickou osobu.

(3) V žádosti o vydání certifikátu shody uvede žadatel obchodní označení a verzi elektronického nástroje a uvede v souladu s § 8 skupinu nebo skupiny, do kterých elektronický nástroj spadá, a výčet elektronických úkonů v rámci této skupiny, které elektronický nástroj zajišťuje.

§ 11

Platnost certifikátů shody

(1) Není-li stanoveno jinak, platí, že pokud provozovatel prokáže certifikačnímu orgánu shodu elektronického nástroje s požadavky kladenými na funkční vlastnosti u elektronického nástroje, má certifikát shody v rozsahu skupiny elektronických úkonů a údajů uvedených v certifikátu shody, které se týkají funkčních vlastností elektronického nástroje, neomezenou platnost. Pokud provozovatel prokáže certifikačnímu orgánu i shodu elektronického nástroje s požadavky kladenými na prostředí, v němž je nebo má být elektronický nástroj provozován, má certifikát shody v rozsahu údajů uvedených v certifikátu shody, které se týkají provozního prostředí, platnost 3 roky ode dne jeho vydání. Uplynutím uvedené doby není dotčena platnost certifikátu shody v rozsahu údajů týkajících se funkčních vlastností elektronického nástroje. Platnost certifikátu shody osvědčujícího soulad s požadavky kladenými na prostředí je možné na žádost provozovatele prodloužit o další 3 roky, a to i opakovaně.

(2) Dojde-li ke změně vlastností či podmínek provozu elektronického nástroje oproti vlastnostem či podmínkám provozu elektronického nástroje, na základě kterých byl certifikát shody vydán, a tato změna by mohla mít za následek neprokázání shody s požadavky stanovenými právními předpisy ve stanoveném rozsahu, je provozovatel povinen do 15 dnů ode dne, kdy ke změně došlo, oznámit tuto skutečnost certifikačnímu orgánu a současně předložit návrh opatření k nápravě. V opačném případě certifikační orgán odejme certifikát shody, případně změní jeho rozsah, pokud to změna vlastností či podmínek provozu elektronického nástroje umožňuje.

(3) Certifikační orgán dále odejme nebo změní certifikát shody v případě, že provozovatel

a) nesplňuje podmínky pro vydání certifikátu shody, nebo

b) použil jako podklady pro vydání certifikátu shody doklady či informace, které se ukázaly jako nepravdivé či neúplné.

(4) Žadatel je oprávněn podat návrh na změnu rozsahu certifikátu shody. V takovém případě prokáže provozovatel certifikačnímu orgánu pouze splnění požadavků, kterých se změna týká.

(5) Žadatel je oprávněn se vzdát certifikátu shody. Vzdání se certifikátu shody je povinen žadatel písemně oznámit certifikačnímu orgánu.

ČÁST ČTVRTÁ

ZÁVĚREČNÁ USTANOVENÍ

§ 12

Zrušovací ustanovení

Vyhláška č. 329/2006 Sb. , kterou se stanoví bližší požadavky na elektronické prostředky, elektronické nástroje a elektronické úkony při zadávání veřejných zakázek, se zrušuje.

§ 13

Účinnost

Tato vyhláška nabývá účinnosti dnem jejího vyhlášení.

Ministr:

Ing. Jankovský v. r.

Příloha

SPECIFIKACE POŽADAVKŮ PRO PROKAZOVÁNÍ SHODY ELEKTRONICKÝCH NÁSTROJŮ

I. Seznam použitých zkratek

ČSN EN ISO 9001	Česká technická norma - Systémy managementu kvality - Požadavky
ČSN EN/IEC 27001	Česká technická norma - Informační technologie - Bezpečnostní techniky - Systémy managementu bezpečnosti informací - Požadavky
EU	Evropská unie
GPS	Globální polohový systém
IETF	Internet Engineering Task Force, česky „Komise techniky Internetu“.
IS VZ US	Informační systém o veřejných zakázkách - uveřejňovací subsystém
JŘSU	Jednací řízení s uveřejněním
OJS eSender	Official Journal Supplement. Úřední věstník EU (tj. evropské uveřejňovací místo).
OPOCE	Úřad pro publikace Evropské unie

PDF/A, ISO 19005	Portable Dokument Format/Archive. Archivační verze formátu PDF definovaná standardem ISO 19005
SD	Soutěžní dialog
ÚOHS	Úřad pro ochranu hospodářské soutěže
UŘ	Užší řízení
UTC	Coordinated Universal Time, česky koordinovaný světový čas
ZD	Zadávací dokumentace
ZVZ	Zákon č. 137/2006 Sb., o veřejných zakázkách, ve znění pozdějších předpisů

II. Úvodní ustanovení

1. **Předmět**

Specifikace požadavků pro prokazování shody elektronických nástrojů (dále jen „standard“) vymezuje způsob prokázání shody elektronických nástrojů s požadavky stanovenými v ZVZ a jeho prováděcích právních předpisech (dále jen „legislativní požadavky“).

1.1 Systém řízení elektronického nástroje a související požadavky

Požadavky obsažené v tomto standardu se aplikují na

1. zavedení systému řízení elektronického nástroje tak, aby byl elektronický nástroj vytvořen a provozován v souladu s legislativními požadavky a

2. certifikaci shody elektronického nástroje tj. shody systému řízení elektronického nástroje s legislativními požadavky.

Provozovatel prokáže shodu elektronického nástroje s legislativními požadavky, pokud prokáže splnění požadavků ve vztahu k

1. funkcionalitě elektronického nástroje a

2. prostředí, ve kterém je elektronický nástroj provozován.

Systém řízení elektronického nástroje je znázorněn na následujícím schématu.

Schéma I. Systém řízení elektronického nástroje

Legenda ke schématu

Jednotlivé požadavky související se systémem řízení elektronického nástroje jsou popsány v tomto standardu následujícím způsobem

1. požadavky na elektronický nástroj (tj. legislativní a technické požadavky na funkcionalitu elektronického nástroje) - technické požadavky viz hlava 2. tohoto standardu,

2. požadavky na řízení zdrojů (provozního prostředí a lidských zdrojů) v souvislosti s provozem elektronického nástroje - viz hlava 3. tohoto standardu,

3. systémové požadavky na elektronický nástroj - viz hlava 4. tohoto standardu.

1.2 Rozsah certifikace shody elektronického nástroje ve vazbě na rozsah funkcionality

Provozovatel elektronického nástroje může požádat o certifikaci elektronického nástroje pro následující skupiny elektronických úkonů

1. úkony nezahrnující přenos a příjem nabídek:

a) odesílání a příjem datových zpráv,

b) elektronické úkony zadavatele bez odesílání datové zprávy,

c) jednání zadavatele nebo orgánu ustanoveného zadavatelem (komise) s dodavatelem prostředky umožňujícími dálkový přístup,

d) poskytování dokumentů dálkovým přístupem.

2. úkony spočívající v přenosu a příjmu nabídek.

Ve vztahu k zadávacím postupům upraveným v ZVZ se certifikace shody elektronického nástroje vztahuje na

1. zadávací řízení ve smyslu ustanovení § 21 ZVZ,

2. zvláštní postupy v zadávacím řízení v rozsahu ustanovení § 89 až § 97 ZVZ a

3. soutěž o návrh ve smyslu ustanovení § 102 a násl. ZVZ.

Rozsah certifikace shody elektronického nástroje ve vazbě na rozsah funkcionality elektronického nástroje je uveden na Schématu II. „Certifikace elektronického nástroje ve vazbě na rozsah jeho funkcionality“. Certifikace bude vždy prováděna pro skupiny elektronických úkonů, které zadavatel uvede v žádosti o vydání certifikátu.

Schéma II. Certifikace elektronického nástroje ve vazbě na rozsah jeho funkcionality

Obrazek 09-2011b.jpg
Plná velikost obrázku

1.3 Splnění jakých požadavků musí provozovatel elektronického nástroje prokázat pro účely certifikace

Pro získání certifikátu shody musí provozovatel elektronického nástroje prokázat splnění

1. obecných legislativních požadavků, a to bez ohledu na to, pro jakou skupinu elektronických úkonů provozovatel žádá o vydání certifikátu shody,

2. specifických legislativních požadavků, a to v rozsahu stanoveném pro příslušnou skupinu elektronických úkonů, pro kterou provozovatel žádá o vydání certifikátu shody,

3. požadavků na řízení zdrojů, a to bez ohledu na to, pro jakou skupinu elektronických úkonů provozovatel žádá o vydání certifikátu shody a

4. systémových požadavků, a to bez ohledu na to, pro jakou skupinu elektronických úkonů provozovatel žádá o vydání certifikátu shody.

III. Požadavky na elektronické nástroje

2. **Technické požadavky**

Technické požadavky představují minimální úroveň, kterou musí elektronický nástroj splňovat. Provozovatel může zajistit naplnění jednotlivý požadavků technicko-technologicky pokročilejším řešením/opatřením. Ověření shody elektronického nástroje bude certifikačním orgánem prováděno v oblasti splnění technických požadavků dle specifikace uvedené v následujících kapitolách, přičemž budou akceptována i pokročilejší řešení/opatření.

2.1 Zaznamenání času elektronického úkonu (T 1)

Zadavatel zajistí, aby zaznamenání času elektronického úkonu bylo provedeno jedním z následujících způsobů

1. záznam času, získaný ze zdroje časové informace, je připojen k datové zprávě,

2. po provedení postupu dle bodu 1. je k datové zprávě s připojeným záznamem času připojen elektronický podpis nebo elektronická značka nebo

3. zaznamenání času je provedeno připojením kvalifikovaného časového razítka k datové zprávě.

2.2 Pořízení záznamu o elektronickém úkonu (T 2)

Zadavatel zajistí, aby veškeré záznamy o elektronických úkonech obsahovaly

1. jednoznačné určení daného konkrétního úkonu v rámci organizace zadavatele,

2. identifikaci osoby, která elektronický úkon provedla v případě, že jde o úkon učiněný konkrétní fyzickou osobou a nejedná o úkon provedený automaticky elektronickým nástrojem (např. příjem nabídek),

3. informaci o nestandardním výsledku úkonu, pokud nastala při provedení úkonu chyba a

4. zaznamenání času elektronického úkonu dle oddílu 2.1.

2.3 Řízení přístupu k aktivům v rámci zadávacích postupů (T 3)

Zadavatel zajistí, aby řízení přístupu k aktivům v rámci zadávacích postupů bylo provedeno jednou z následujících variant

1. autentizace a autorizace přistupující osoby je založena na zadání jména a hesla.

Poskytovatel dokumentu musí zajistit, aby distribuce jména a hesla přistupujícím osobám proběhla přiměřeně bezpečným způsobem,

2. autentizace a autorizace přistupující osoby je založena na certifikátu veřejného klíče přistupující osoby nebo

3. autentizace a autorizace přistupující osoby je založena i na jiných technologiích; vždy však musí probíhat přiměřeně bezpečným způsobem.

2.4 Použití otevřených formátů dokumentů (T 4)

Zadavatel zajistí, aby formátem datových zpráv, které jsou vyměňovány během zadávacích postupů, byl otevřený formát.

2.5 Archivace dokumentace o veřejné zakázce (T 5)

Zadavatel zajistí, aby dokumentace o veřejné zakázce, ke které je vyžadováno připojení zaručeného elektronického podpisu, byla uchovávána v datovém úložišti s řízeným přístupem. Řízení přístupu se musí řídit pravidly dle oddílu 2.3. Elektronický nástroj musí zajistit, aby při uložení dokumentace do datového úložiště bylo k dokumentaci připojeno kvalifikované časové razítko.

Dokumentace o veřejné zakázce, která obsahuje důvěrné informace, musí být uchovávána v datovém úložišti s řízeným přístupem. Řízení přístupu se musí řídit pravidly dle oddílu 2.3. Dokumentace může být uchovávána ve své šifrované podobě. Pokud je dokumentace uchovávána v šifrované podobě, musí zadavatel bezpečně uchovávat soukromý klíč zadavatele, odpovídající veřejnému klíči zadavatele, kterým byl dokument šifrován. Doba uchování soukromého klíče zadavatele musí odpovídat době uchování dokumentace.

2.6 Omezené poskytování zabezpečeného dokumentu dálkovým přístupem (T 6)

Zadavatel zajistí, aby k zabezpečenému dokumentu, který bude omezeně poskytován dálkovým přístupem, byl připojen zaručený elektronický podpis poskytovatele dokumentu. Formát dokumentu musí odpovídat požadavkům dle oddílu 2.4. K dokumentu musí být řízený přístup. Řízení přístupu k dokumentu se musí řídit pravidly dle oddílu 2.3.

2.7 Neomezené poskytování zabezpečeného dokumentu dálkovým přístupem (T 7)

Zadavatel zajistí, aby k zabezpečenému dokumentu, který bude neomezeně poskytován dálkovým přístupem, byl připojen zaručený elektronický podpis poskytovatele dokumentu. Formát dokumentu musí odpovídat požadavkům dle oddílu 2.4.

2.8 Neomezené poskytování dokumentu dálkovým přístupem (T 8)

Při poskytování dokumentu neomezeným dálkovým přístupem zadavatel pořídí záznam o elektronickém úkonu dle oddílu 2.2. Formát dokumentu musí odpovídat požadavkům dle oddílu 2.4.

2.9 Odeslání datové zprávy v rámci organizace zadavatele (T 9)

Formát datové zprávy odesílané v rámci organizace zadavatele bude zvolen podle potřeb zadavatele. Zadavatel vždy zvolí takový formát, který ochrání dokument proti neoprávněné změně. Elektronický protokol použitý k přenosu datové zprávy bude zvolen podle potřeb zadavatele. Zadavatel určí, zda datová zpráva bude šifrována a určí pravidla, jaký klíč bude používán k šifrování.

2.10 Příjem datové zprávy v rámci organizace zadavatele (T 10)

Při příjmu datové zprávy, přenášené v rámci organizace zadavatele, musí zadavatel respektovat formát a elektronický protokol příchozí zprávy. V případě šifrované datové zprávy zadavatel stanoví pravidla určující, zda bude datová zpráva dešifrována.. Pravidla pro to, zda bude pro datovou zprávu ověřena platnost tohoto elektronického podpisu, resp. značky, stanoví zadavatel. O příjmu datové zprávy musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2.

2.11 Odeslání šifrované datové zprávy opatřené elektronickým podpisem (T 11)

Přípustné formáty odesílané datové zprávy musí stanovit zadavatel. Formát dokumentu musí odpovídat požadavkům dle oddílu 2.4. Elektronický protokol použitý k přenosu datové zprávy, stanoví zadavatel. Příjemce datové zprávy musí odesílateli poskytnout certifikát veřejného klíče. Datová zpráva musí být šifrována veřejným klíčem příjemce. Datová zpráva musí mít připojen zaručený elektronický podpis nebo elektronickou značku, založenou na kvalifikovaném systémovém certifikátu. Pokud je zpráva odesílána zadavatelem, musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2.

2.12 Odeslání otevřené datové zprávy opatřené elektronickým podpisem (T 12)

Přípustné formáty odesílané datové zprávy stanoví zadavatel. Formát dokumentu musí odpovídat požadavkům dle oddílu 2.4. Elektronický protokol použitý k přenosu datové zprávy, stanoví zadavatel.. Datová zpráva musí mít připojen zaručený elektronický podpis nebo elektronickou značku, založenou na kvalifikovaném systémovém certifikátu. Pokud je zpráva odesílána zadavatelem, musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2.

2.13 Odeslání otevřené datové zprávy (T 13)

Přípustné formáty odesílané datové zprávy stanoví zadavatel. Formát dokumentu musí odpovídat požadavkům dle oddílu 2.4. Elektronický protokol použitý k přenosu datové zprávy stanoví zadavatel. Pokud je zpráva odesílána zadavatelem, musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2.

2.14 Příjem šifrované datové zprávy opatřené elektronickým podpisem (T 14)

Při příjmu datové zprávy musí zadavatel respektovat formát a elektronický protokol příchozí zprávy. Zadavatel zajistí ověření platnosti připojeného elektronického podpisu, resp. elektronické značky. Datová zpráva může být dešifrována. Pravidla určující, zda bude datová zpráva dešifrována, stanoví příjemce. Pokud je zpráva přijímána zadavatelem, musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2.

Pokud je připojen zaručený elektronický podpis, příjemce musí datovou zprávu odmítnout v případě, kdy zaručený elektronický podpis není platný nebo jeho kvalifikovaný certifikát byl zneplatněn. Pokud je připojena elektronická značka, příjemce musí datovou zprávu odmítnout v případě, kdy elektronická značka není platná nebo její kvalifikovaný systémový certifikát byl zneplatněn.

2.15 Příjem otevřené datové zprávy opatřené elektronickým podpisem (T 15)

Při příjmu datové zprávy musí zadavatel respektovat formát a elektronický protokol příchozí zprávy. Zadavatel musí zajistit ověření platnosti připojeného elektronického podpisu, resp. elektronické značky. Pokud je zpráva přijímána zadavatelem, musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2. Pokud je připojen zaručený elektronický podpis, příjemce musí datovou zprávu odmítnout v případě, kdy zaručený elektronický podpis není platný nebo jeho kvalifikovaný certifikát byl zneplatněn. Pokud je připojena elektronická značka, příjemce

musí datovou zprávu odmítnout v případě, kdy elektronická značka není platná nebo její kvalifikovaný systémový certifikát byl zneplatněn.

2.16 Příjem otevřené datové zprávy (T 16)

Při příjmu datové zprávy musí zadavatel respektovat formát a elektronický protokol příchozí datové zprávy.V případech, kdy je k datové zprávě připojen zaručený elektronický podpis nebo elektronická značka, ačkoliv to zákon ani zadavatel nepožadoval, nemůže příjemce datovou zprávu odmítnout, a to ani v případě, kdy elektronický podpis nebo elektronická značka nejsou platné

2.17 Příjem a uložení nabídky (T 17)

Při příjmu datové zprávy nabídky musí zadavatele respektovat formát a elektronický protokol příchozí zprávy. Zadavatel musí zajistit ověření platnosti připojeného zaručeného elektronického podpisu, resp. elektronické značky. Pokud není ověřena platnost připojeného zaručeného elektronického podpisu, resp. elektronické značky během příjmu nabídky, musí být ověřena v průběhu úkonu otevírání obálek. Datová zpráva nabídky nesmí být dešifrována. Zadavatel musí pořídit záznam o elektronickém úkonu dle oddílu 2.2. V průběhu příjmu nabídky nesmí být pořízeny žádné kopie datové zprávy nabídky.

Zadavatel zajistí, aby po příjmu datové zprávy nabídky neprodleně následovalo bezpečné uložení datové zprávy nabídky. Bezpečné uložení datové zprávy nabídky musí být provedeno způsobem, aby přístup k šifrované nabídce, uložené v datovém úložišti, nebyl možný před uplynutím lhůty pro podání nabídek.

Zadavatel zajistí, aby datová zpráva nabídky byla uložena takovým způsobem, aby byl zjistitelný pokus o přístup k uložené nabídce před termínem otevírání nabídek. Při jakémkoli takovém pokusu o přístup k nabídce před termínem otevírání nabídek musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2.

2.18 Otevírání nabídek podaných elektronickými prostředky (T 18)

Zadavatel zajistí, aby otevření nabídek podaných elektronickými prostředky bylo provedeno jednou z následujících variant

1. otevření nabídky podané elektronickými prostředky bude provedeno způsobem navazujícím na příjem nabídky dle oddílu 2.17. Přístup k šifrované nabídce uložené v datovém úložišti, bude proveden součinností minimálně dvou osob, resp. i většího počtu osob, stanoví-li tak zadavatel, s neúplnými právy přístupu k uložené nabídce. Kombinací přístupových práv těchto osob bude umožněn přístup k uložené nabídce. Nabídka pak bude dešifrována soukromým klíčem zadavatele příslušejícím veřejnému klíči zadavatele, který byl použit k šifrování datové zprávy nabídky nebo

2. otevření nabídky podané elektronickými prostředky bude provedeno způsobem, navazujícím na příjem nabídky dle oddílu 2.17. Šifrovaná datová zpráva nabídky je dešifrována součinností osob, majících přístup k soukromým klíčům zadavatele příslušejícím veřejným klíčům zadavatele, které byly použity k šifrování datové zprávy nabídky.

2.19 Jednání komise / poroty / zadavatele (T 19)

Zadavatel zajistí, aby součástí záznamu o jednání komise / poroty / zadavatele byl dokument zápisu z jednání. Musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2.

2.20 Elektronický podpis dokumentu (T 20)

Zadavatel zajistí, aby elektronický podpis dokumentu byl proveden jedním z následujících způsobů

1. formát dokumentu musí odpovídat požadavkům dle oddílu 2.4. Dokument musí být podepsán připojením zaručeného elektronických podpisu nebo zaručené elektronické značky k dokumentu. Po připojení elektronického podpisu nebo elektronické značky zadavatele musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2, nebo

2. u vícestranného zaručeného elektronického podpisu bude dokument oboustranně podepsán postupnou výměnou zpráv. V tomto případě zadavatel musí odeslat datovou zprávu s dokumentem s připojeným zaručeným elektronickým podpisem dodavateli způsobem dle oddílu 2.11. Dodavatel musí při příjmu datové zprávy respektovat formát příchozí zprávy. V případě, že byla datová zpráva šifrovaná, provede dodavatel její dešifrování. Dodavatel ověří platnost připojeného zaručeného elektronického podpisu. Dodavatel musí datovou zprávu odmítnout v případě, kdy zaručený elektronický podpis není platný nebo jeho kvalifikovaný certifikát byl zneplatněn. Dále dodavatel musí k dešifrovanému dokumentu připojit vlastní zaručený elektronický podpis a odeslat jej v datové zprávě v souladu s oddílu 2.11. Zadavatel při příjmu této zprávy musí postupovat dle oddílu 2.14. Postup vícestranného elektronického podpisu lze realizovat v opačném pořadí, tj. dokument nejdříve podepíše dodavatel a následně ho předá zadavateli. Veškeré výše uvedené požadavky se použijí obdobně.

2.21 Odeslání datové zprávy webové služby (T 21)

Klientská aplikace musí při odeslání zprávy webové službě dodržet pravidla komunikace stanovená službou. Musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2.

2.22 Příjem datové zprávy webové služby (T 22)

Klientská aplikace musí při příjmu zprávy webové služby dodržet pravidla komunikace stanovená službou. Musí být pořízen záznam o elektronickém úkonu dle oddílu 2.2.

2.23 Zpřístupnění návrhu v soutěži o návrh soutěžní porotě (T 24)

Elektronický nástroj musí zadavateli umožnit zpřístupnění návrhu v soutěži o návrh soutěžní porotě tak, aby pro osoby, jež jsou součástí soutěžní poroty, nebylo možné na základě informací poskytnutých elektronickým nástrojem identifikovat dodavatele, který návrh podal (dále jen „anonymizace návrhu“). K anonymizaci návrhu musí dojít až po otevření a dešifrování návrhu. Soutěžní porotě zpřístupní zadavatel anonymizovaný návrh v dešifrované podobě.

Elektronický nástroj musí i po anonymizaci návrhu poskytnout zadavateli informaci o dodavateli, jež návrh podal.

Zadavatel zajistí, aby o zpřístupnění návrhu v soutěži o návrh soutěžní porotě byl pořízen záznam o elektronickém úkonu dle oddílu 2.2.

2.24 Zajištění zákazu diskriminace (T 25)

Provozovatel musí provozovat elektronický nástroj v takovém prostředí a takovým způsobem, aby užívání elektronického nástroje nebylo podmiňováno používáním běžně nedostupných nebo nákladných technologií, což by způsobilo vyloučení určitého dodavatele z účasti na zadávacích postupech.

2.25 Zpřístupnění informací pro využití elektronického nástroje (T26)

Elektronický nástroj musí umožnit zadavateli poskytovat dodavatelům, kteří mají zájem účastnit se zadávacích postupů, k dispozici veškeré informace technické povahy, včetně

případného kódování a šifrování, které jsou nezbytné pro komunikaci elektronickými prostředky, zejména pro elektronické podání nabídek a žádostí o účast, a to po celou dobu používání elektronického nástroje.

Zadavatel zajistí, aby o zpřístupnění informací pro využití elektronického nástroje byl pořízen záznam o elektronickém úkonu dle oddílu 2.2.

2.26 Zajištění technické podpory a servisu elektronického nástroje (T27)

Provozovatel elektronického nástroje musí zajistit technickou podporu a servis elektronického nástroje v takové míře, aby bylo možné zajistit řádný provoz elektronického nástroje a splnění ostatních požadavků tohoto standardu. Technickou podporu a servis musí provozovatel elektronického nástroje poskytovat v rozsahu přiměřeném složitosti funkcionality elektronického nástroje.

3. **Požadavky na řízení zdrojů**

Provozovatel elektronického nástroje musí určovat a zajistit zdroje potřebné pro efektivní a účinný provoz elektronického nástroje. Zdroje pro účely tohoto standardu tvoří

1. prostředí,, ve kterém je elektronický nástroj provozován a které zahrnuje hardware, operační systémy a další systémové programové vybavení a prostory nezbytné pro zajištění požadovaných parametrů elektronického nástroje a

2. lidské zdroje, které jsou nezbytné pro provozování elektronického nástroje (správu a obsluhu) v zamýšleném rozsahu a pro dodržování stanovených požadavků na elektronický nástroj. Provozovatel elektronického nástroje musí specifikovat požadavky na řízení zdrojů (provozního prostředí a lidských zdrojů) a jeho části tak, aby bylo zajištěno, že elektronický nástroj plní stanovené požadavky při jeho provozování v provozním prostředí v zamýšleném rozsahu.

3.1 Požadavky na prostředí

Provozovatel elektronického nástroje musí dokumentovaným způsobem stanovit požadavky na prostředí, a to zejména hardware, software a prostory nezbytné pro provozování elektronického nástroje v zamýšleném rozsahu. Musí vést záznamy o tom, že jsou tyto požadavky při provozu elektronického nástroje plněny. Rozsah požadavků je závislý na složitosti elektronického nástroje (tj. komptabilitě funkcionality).

3.2 Požadavky na procesy řízení lidských zdrojů

Provozovatel musí provést taková opatření v oblasti řízení lidských zdrojů, která minimalizují negativní vliv pracovníků na provoz elektronického nástroje ve stanoveném rozsahu při dodržení všech stanovených požadavků. Požadavky na řízení lidských zdrojů jsou zde následně členěny jako doporučené a minimální. Doporučené procesy řízení lidských zdrojů a jejich plnění zajistí provozovateli elektronického nástroje ucelenější nástroj řízení . Pro plnění požadavků tohoto standardu však provozovateli elektronického nástroje postačí naplnění minimálních požadavků na procesy řízení lidských zdrojů. Způsob naplnění níže uvedených požadavků musí být dokumentován a musí existovat záznamy jako důkazy o plnění požadavků.

Minimální procesy řízení lidských zdrojů jsou definovány v následující matici.

Tabulka I. Struktura (matice) procesů oblasti řízení lidských zdrojů

PROCESY		

Před započetím práce s elektronickým nástrojem nebo v provozním prostředí elektronického nástroje	Během práce s elektronickým nástrojem nebo v provozním prostředí elektronického nástroje	Při ukončení práce s elektronickým nástrojem nebo v provozním prostředí elektronického nástroje
Vytvoření role	Provádění vzdělávacích aktivit	
Stanovení požadavků na odbornou způsobilost pracovníka v roli	Disciplinární řízení	Ukončení práce v roli
Ustanovení pracovníka do role a jeho proškolení		

Pozn. 1: Pracovníkem se rozumí zaměstnanec provozovatele elektronického nástroje nebo i jiná osoba, která se podílí na provozování elektronického nástroje.

Pozn. 2: Disciplinárním řízením se rozumí uplatňování odpovědnosti za činnost spočívající v provozování elektronického nástroje a uplatňování sankcí bez ohledu na to, zda se jedná o odpovědnost vyplývající z pracovního poměru nebo jiného vztahu.

3.2.1 Před započetím práce s elektronickým nástrojem nebo v provozním prostředí elektronického nástroje

Provozovatel elektronického nástroje

1. stanoví role nutné pro provozování elektronického nástroje, jejich odpovědnosti, pravomoci a požadavky na odbornou způsobilost,

2. definuje odpovědnosti a postupy seznamování pracovníků určovanými pro danou roli s jejich odpovědnostmi, povinnostmi a pravomocemi,

3. definuje odpovědnosti, pravomoci a postupy určování pracovníků do rolí.

3.2.2 Během práce s elektronickým nástrojem nebo v provozním prostředí elektronického nástroje

Provozovatel elektronického nástroje plánuje a zajišťuje vzdělávací aktivity, prostřednictvím nichž zajistí, že pracovníci budou splňovat požadavky na odbornou způsobilost stanovené pro zastávanou roli. V případě, že jsou činnosti zajištěny smluvní stranou, provozovatel vyžaduje naplnění tohoto požadavku po smluvní straně.

Provozovatel elektronického nástroje stanoví odpovědnosti a postupy pro zahájení, provedení a ukončení disciplinárního řízení pro případ, že pracovník poruší stanovené povinnosti při provozu elektronického nástroje.

3.2.3 Při ukončení práce s elektronickým nástrojem nebo v provozním prostředí

elektronického nástroje

Provozovatel elektronického nástroje stanoví odpovědnosti a postupy pro řádný průběh ukončení práce pracovníka s elektronickým nástrojem (včetně ukončení případných smluvních vztahů), které zahrnují zejména odevzdání přidělených aktiv a odejmutí přístupových práv k elektronickému nástroji.

4. **Systémové požadavky na elektronický nástroj**

Prostřednictvím systémových požadavků na elektronické nástroje zajišťuje provozovatel plnění legislativních požadavků již v průběhu návrhu a vývoje elektronického nástroje a po celou dobu provozování elektronického nástroje.

4.1 Požadavky na bezpečnost informací

Provozovatel elektronického nástroje musí eliminovat dopady identifikovaných hrozeb, které mohou mít za následek neplnění stanovených požadavků na elektronický nástroj. Příklady struktury hrozeb a z ní vyplývající důvody členění požadavků jsou uvedeny na následujícím Schématu. Při provádění úkonů v zadávacích postupech musí být ve všech případech zajištěna dostupnost a integrita předávaných a zpracovávaných informací a ve stanovených případech musí být navíc zajištěna i důvěrnost těchto informací.

Schéma III. Stěžejní faktory ovlivňující plnění požadavků na elektronický nástroj

Obrazek 09-2011c.jpg
Plná velikost obrázku

Dostupnost, integritu a důvěrnost musí provozovatel dokumentovaným způsobem zabezpečit a to aplikováním vybraných postupů mezinárodních norem v oblasti bezpečnosti informací.

Provozovatel musí zajistit provedení alespoň následujících kroků

1. určit rozsah a hranice elektronického nástroje na základě posouzení jeho uspořádání, struktury, umístění (lokality), aktiv a technologií,

2. definovat politiku bezpečnosti informací elektronického nástroje, která

a) stanovuje principy, zásady a celkový rámec řízení bezpečnosti informací,

b) bere v úvahu zákonné nebo regulatorní požadavky a smluvní závazky provozovatele elektronického nástroje a stanovuje kritéria, kterými budou hodnocena rizika,

3. stanovit přístup provozovatele elektronického nástroje k rizikům bezpečnosti informací

a) identifikovat metodiku hodnocení rizik, která vyhovuje stanovené úrovni bezpečnosti informací, zákonným a regulatorním požadavkům, a zajistí reprodukovatelnost a porovnatelnost výsledků,

b) vytvořit kritéria pro akceptaci rizik a identifikovat jejich akceptační úrovně,

4. identifikovat rizika

a) identifikovat aktiva v rámci rozsahu elektronického nástroje a jejich vlastníky,

b) identifikovat hrozby pro tato aktiva,

c) identifikovat zranitelnosti, které by mohly být hrozbami využity,

d) identifikovat jaké dopady na provoz elektronického nástroje by mohla mít ztráta důvěrnosti, integrity a dostupnosti aktiv,

5. analyzovat a vyhodnotit rizika,

6. identifikovat a stanovit varianty pro zvládání rizik, kterými může být

a) aplikování vhodných opatření k eliminaci či snížení dopadu rizik,

b) vědomé a objektivní akceptování rizik za předpokladu, že zřetelně naplňují politiky organizace a kritéria pro akceptaci rizik

c) vyhnutí se rizikům,

d) přenesení rizik spojených s činností organizace na třetí strany, např. na pojišťovny, dodavatele,

7. vybrat a aplikovat jednotlivá bezpečnostní opatření pro zvládání rizik.

Provozovatel elektronického nástroje musí v rámci provozování elektronického nástroje:

1. monitorovat, přezkoumávat a zavádět další opatření

a) pro včasnou detekci chyb zpracování,

b) pro včasnou identifikaci úspěšných i neúspěšných pokusů o narušení bezpečnosti a detekci bezpečnostních incidentů,

c) umožňující vedení provozovatele elektronického nástroje určit, zda bezpečnostní aktivity prováděné pověřenými osobami, nebo pro které byly implementovány technologie, fungují podle očekávání,

d) umožňující detekci bezpečnostních událostí, které mohou způsobit bezpečnostní incident,

2. měřit účinnost zavedených opatření pro ověření toho, že byly naplněny požadavky na bezpečnost,

3. provádět interní audity bezpečnosti informací v plánovaných intervalech a přijímat účinná opatření k odstranění nedostatků a

4. pravidelně přezkoumávat rizika, přiměřenost a účinnost přijatých opatření pro zvládání rizik, výskyt bezpečnostních událostí a incidentů, výsledky interních auditů a na základě toho přijímat opatření ke zlepšování nastaveného systému řízení bezpečnosti informací.

4.2 Požadavky na procesy řízení dokumentů

Provozovatel elektronického nástroje musí řídit (vytváří, klasifikuje, schvaluje, označuje, eviduje, ukládá, distribuuje, reviduje, provádí změny, chrání, uchovává a likviduje) veškeré dokumenty související s provozováním elektronického nástroje s ohledem na jejich klasifikaci po celou dobu jejich životního cyklu. Součástí řízení je i zajišťování stanovené úrovně dostupnosti, integrity a důvěrnosti informací v dokumentech. Provozovatel elektronického nástroje musí vytvořit dokumentované postupy, které stanoví odpovědnosti, pravidla a postupy zejména pro

1. vytváření, identifikaci a evidenci dokumentů,

2. klasifikaci dokumentů,

3. schvalování dokumentů,

4. distribuci dokumentů.

5. nakládání s dokumenty podle pravidel odpovídající klasifikaci dokumentů,

6. zajištění aktuálnosti dokumentů jejich revidováním a aktualizací včetně opakovaného schvalování,

7. zajištění identifikovatelnosti změn dokumentů a jejich aktuálního stavu,

8. zajištění čitelnosti a snadné identifikovatelnosti dokumentů,

9. zajištění stanovené dostupnosti dokumentů,

10. zajištění integrity dokumentů,

11. zajištění identifikace a řízení dokumentů externího původu.

Vytváření dokumentů souvisejících s provozem elektronického nástroje mohou být v jakékoliv podobě (tj. listinné či elektronické) a na jakémkoliv nosiči.

4.3 Požadavky na procesy řízení záznamů

Záznamy jako zvláštní kategorie dokumentů musí být vytvořeny a udržovány tak, aby poskytovaly důkaz o shodě se stanovenými požadavky na provoz elektronického nástroje. Záznamy musí být chráněny a řízeny, musí zůstat čitelné, snadno identifikovatelné a musí být možné je snadno vyhledat. Opatření potřebná k identifikaci, uložení, ochraně, vyhledání, době platnosti a uspořádání záznamů musí být dokumentována.

Provozovatel elektronického nástroje musí zajistit kontinuitu verzí dokumentu a zajistit požadavek dohledatelnosti u každého dokumentu a záznamu.

Vytváření záznamů souvisejících s provozem elektronického nástroje mohou být v jakékoliv podobě (tj. listinné či elektronické) a na jakémkoliv nosiči.

4.4 Požadavky na vytváření elektronického nástroje

Provozovatel elektronického nástroje musí zajistit dokumentovaným způsobem objektivní důkazy o tom, že vytváření elektronického nástroje probíhalo v souladu s jím stanovenými požadavky na návrh a vývoj elektronického nástroje, které zahrnují minimálně požadavky tohoto standardu a požadavky na bezpečnost zpracovávaných informací. Dále musí vést záznamy o tom, že v průběhu plánování návrhu a vývoje byly stanoveny

1. odpovědnosti a pravomoci při návrhu a vývoji elektronického nástroje,

2. vhodné etapy návrhu a vývoje elektronického nástroje (minimálně návrh a vývoj elektronického nástroje a integrace elektronického nástroje do provozního prostředí),

3. způsoby a podmínky testování (ověření) a validace elektronického nástroje, v každé stanovené etapě návrhu a vývoje elektronického nástroje.

Ve stanovených etapách musí provozovatel elektronického nástroje provádět systematická přezkoumání návrhu a vývoje tak, aby

1. byla průběžně vyhodnocována schopnost elektronického nástroje plnit stanovené požadavky,

2. byly včas identifikovány všechny problémy a mohla být navržena nezbytná opatření k zajištění splnění požadavků na elektronický nástroj.

Provozovatel elektronického nástroje musí vést záznamy o výsledcích a průběhu testování elektronického nástroje, které bylo prováděno tak, aby bylo prokázáno, že plní stanovené požadavky na elektronický nástroj.

Provozovatel musí vést záznamy o výsledcích a průběhu validace elektronického nástroje, která byla prováděna tak, aby bylo zajištěno, že elektronický nástroj provozovaný ve specifikovaném prostředí je schopen plnit požadavky specifikovaného nebo zamýšleného použití.

Musí být zpracována uživatelská dokumentace elektronického nástroje a dokumentace související se správou elektronického nástroje. Provozovatel musí vést dokumentaci zdrojového kódu, a to v případě, že je oprávněn provádět změny v tomto zdrojovém kódu.

4.5 Požadavky na provádění změn elektronického nástroje

Pro provádění změn elektronického nástroje platí stejné požadavky jako na vytváření elektronického nástroje.

Všechny změny elektronického nástroje musí být v souladu s legislativními požadavky a požadavky tohoto standardu. Tyto změny musí být identifikovatelné, musí být dokumentovány a schváleny odpovědnou osobou před jejich realizací.

4.6 Požadavky na monitorování, měření a přezkoumávání provozu elektronického nástroje

Provozovatel elektronického nástroje musí aplikovat vhodné metody monitorování a podle okolností také měření stanovených provozních parametrů elektronického nástroje.

Výsledky monitorování nebo měření musí být zaznamenány a analyzovány s cílem identifikovat neshody a jejich příčiny. Provozovatel elektronického nástroje musí neprodleně po zjištění neshody přijmout účinná opatření k nápravě pro odstranění dopadu neshody a jejích příčin. Po stanovené době musí provozovatel elektronického nástroje přezkoumat, zda přijatá opatření byla účinná. Neshody a jejich příčiny, přijatá opatření i přezkoumání účinnosti přijatých opatření musí být dokumentováno.

1) Zákon č. 227/2000 Sb. , o elektronickém podpisu a o změně některých dalších zákonů (zákon o elektronickém podpisu), ve znění pozdějších předpisů.

2) Zákon č. 22/1997 Sb. , o technických požadavcích na výrobky a o změně a doplnění některých zákonů, ve znění pozdějších předpisů.