MINISTERSTVO PRO MÍSTNÍ ROZVOJ ČR

PODMÍNKY PRO AKREDITAČNÍ ORGÁN A CERTIFIKAČNÍ ORGÁNY

při certifikaci elektronických nástrojů ve smyslu § 213 odst. 4 zákona č. 134/2016 Sb., o zadávání veřejných zakázek

Zpracoval: **Ministerstvo pro místní rozvoj ČR**

Odbor elektronizace veřejných zakázek

Verze: **1.0**

V Praze dne: **30. 1. 2018**

Východiska zpracování dokumentu

V souladu s ustanovením § 213 odst. 4 zákona č. 134/2016 Sb., o zadávání veřejných zakázek, ve znění pozdějších předpisů, dále též ZZVZ, vytvořilo Ministerstvo pro místní rozvoj ČR (dále též „MMR“) nový způsob ověřování shody elektronických nástrojů s legislativními požadavky a formou vyhlášky stanovilo podrobnosti týkající se podmínek pro vydání certifikátu shody, údajů o certifikátu shody a platnosti certifikátu shody. Přílohu vyhlášky tvoří standard pro posuzování shody elektronických nástrojů s legislativními požadavky.

V tomto dokumentu jsou obsaženy podmínky pro akreditační orgán a certifikační orgány stanovené ze strany MMR jako správce systému certifikace elektronických nástrojů.

Akreditace certifikačních orgánů a certifikace elektronických nástrojů bude prováděna v souladu s národními a mezinárodními standardy pro akreditace a certifikace s tím, že **MMR upřesňuje některé požadavky** na provádění akreditace certifikačních orgánů a certifikace elektronických nástrojů. Požadavky jsou členěny na:

- Požadavky na akreditační orgán,
- Požadavky na certifikační orgán.

1. Požadavky na akreditační orgán

Akreditační orgán provádí posuzování odborné způsobilosti certifikačních orgánů v souladu s ČSN EN ISO/IEC 17011.

1.1. Kompetence skupiny posuzovatelů akreditačního orgánu

A. MMR nominuje do akreditačního týmu odborného posuzovatele/experta, který bude garantovat, že v průběhu akreditačního procesu certifikačního orgánu budou uplatněny všechny požadavky MMR ve vztahu k certifikačnímu orgánu. Odborný posuzovatel/expert musí mít prokazatelné znalosti požadavků standardu a možných způsobů jejich naplnění a znalost zákona č. 134/2016 Sb., o zadávání veřejných zakázek a souvisejících prováděcích právních předpisů v platném znění a jiných relevantních právních předpisů.[1]

B. Akreditační orgán doplní skupinu posuzovatelů o další odborné posuzovatele/experty, kteří budou mít alespoň znalosti:

   i. Problematiky bezpečnosti informací, aby byli schopni odhalit nedostatky v analýze rizik (identifikovat aktiva, hrozby a zranitelnosti aktiv) a byli schopni posoudit účinnost realizovaných opatření k dosažení stanovené úrovně bezpečnosti informací.

   ii. Systému řízení služeb IT, aby byli schopni posoudit úroveň splnění systémových požadavků standardu, které vyplývají z požadavků ČSN ISO/IEC 20000-1.

1.2. Výkaznictví o udělených akreditacích

A. Akreditační orgán povede evidenci akreditovaných certifikačních orgánů akreditovaných k provádění certifikací elektronických nástrojů. Akreditační orgán informuje v listinné podobě či elektronicky MMR o zveřejnění údaje o vydání, pozastavení či zrušení osvědčení o akreditaci ve Věstníku ÚNMZ a, pakliže k tomu certifikační orgán udělí souhlas, informuje akreditační orgán MMR i o změně rozsahu udělené akreditace, ve lhůtě 15 dnů od data účinnosti příslušného rozhodnutí.

[1] Nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES, a národní prováděcí předpisy.

2. Požadavky na certifikační orgán

Certifikační orgány posuzují shodu v souladu s ČSN EN ISO/EC 17065 a kritérii 7 a 9 z ČSN EN ISO/IEC 17021-1 pro případ posuzování prostředí a kritéria 6.1 z ČSN EN ISO/IEC 17020 pro případ posuzování pouze funkcionality.

2.1. Kompetence vrcholového vedení a týmu auditorů certifikačního orgánu

A. Všichni auditoři certifikačního orgánu musí disponovat znalostí problematiky zadávání veřejných zakázek v rozsahu kurzu, organizovaném MMR, a to obvykle po dosažení minimálně 4 žadatelů o kurz. Kurz bude zakončen přezkoumáním získaných znalostí písemnou zkouškou (testem), na základě které MMR vydá osvědčení o získané úrovni znalostí absolventů kurzu. Rozsah znalostí zadávání veřejných zakázek bude zahrnovat zejména:

   i. Základní principy ZZVZ.

   ii. Kategorie veřejných zakázek podle výše předpokládané hodnoty, druhy zadávacích řízení, hlavní úkony v zadávacím řízení.

   iii. Provádění úkonů v zadávacím řízení v elektronické podobě.

   iv. Jednotlivé instituty elektronického zadávání veřejných zakázek.

   v. Požadavky na elektronické nástroje a právní předpisy, ze kterých vyplývají.

   vi. Ustanovení souvisejících právních předpisů s přímým dopadem na provádění úkonů v zadávacím řízení v elektronické podobě.

B. Auditor musí disponovat prokazatelnou znalostí auditních postupů tak, aby byl schopen provést audit na místě u klienta certifikace.

C. Auditor musí disponovat prokazatelnou znalostí problematiky bezpečnosti informací v takovém rozsahu, aby byl schopen odhalit nedostatky v analýze rizik (identifikovat aktiva, hrozby a zranitelnosti aktiv), a byl schopen posoudit účinnost realizovaných opatření k dosažení stanovené úrovně bezpečnosti informací.

D. Auditor musí disponovat prokazatelnou znalostí systému řízení služeb v IT (ITSMS), v takovém rozsahu, aby byl schopen posoudit úroveň plnění SLA parametrů, procesů a řízení služeb v IT, které vyplývají z požadavků normy ČSN ISO/IEC 20000-1.

2.2. Výkaznictví o udělených certifikátech shody

A. Certifikační orgán povede seznam vydaných, ukončených a odňatých certifikátů. Certifikační orgán oznámí v listinné podobě či elektronicky MMR vydání certifikátu, změnu jeho rozsahu, ukončení platnosti certifikátu na základě žádosti provozovatele, odnětí certifikátu shody nebo jakékoliv jiné relevantní skutečnosti, nejpozději do 15 dnů ode dne účinnosti příslušného rozhodnutí. Součástí oznámení, v případě vydání, bude kopie Certifikátu včetně přílohy, v ostatních případech bude součástí oznámení kopie rozhodnutí.

B. Oznámení dle bodu 2.2. A. bude certifikační orgán zasílat na e-mailovou adresu oevz.certifikaty@mmr.cz.

2.3. Podmínky pro certifikační audit

2.3.1. Rozsah certifikačního auditu

A. Minimální rozsah každého certifikačního auditu je požadován na jeden auditoden pro první stupeň a 4 hodiny pro druhý stupeň auditu.

B. Certifikační orgán stanoví písemný postup pro výpočet doby trvání auditu v závislosti na rozsahu certifikace.

C. Počty zaměstnanců provozovatele elektronického nástroje nebudou brány v úvahu.

D. Auditor musí provést audit postupem stanoveným bodem 2.3.2.

2.3.2. Průběh certifikačního auditu

A. Každý certifikační audit bude prováděn dvoustupňově.

i. V prvním stupni tým auditorů posoudí soulad předložené dokumentace s požadavky standardu a konkrétním prostředím, ve kterém je elektronický nástroj provozován, o čemž vyhotoví zprávu, která bude obsahovat zjištěné nedostatky.

ii. Ve druhém stupni tým auditorů posoudí soulad funkcionality a/nebo prostředí, popsaných v dokumentaci vůči reálnému stavu. Prostředí ověří auditor ve všech lokalitách, ve kterých provozuje žadatel o certifikaci elektronický nástroj a ověří smlouvy v případě, kdy k provozování elektronického nástroje využívá službu druhé strany.[2]

3. Účinnost

Tyto podmínky se uplatní ode dne vydání tohoto dokumentu.

Certifikační orgány mají povinnost doložit plnění těchto podmínek v rámci nejbližšího dozorového nebo akreditačního auditu.

[2] Poznámka: Předmětem posouzení smluv budou SLA parametry uvedené v těchto smlouvách a jejich dostatečnost pro zajištění důvěrnosti, dostupnosti a integrity elektronického nástroje a jeho provozu.