MINISTERSTVO VNITRA
ČESKÉ REPUBLIKY

MVCRX059RB5Q
prvotní identifikátor

odbor eGovernmentu
náměstí Hrdinů 1634/3
140 21 Praha 4

Č. j. MV- 31130-82/EG-2018

Praha 21. října 2020

Mendelova univerzita v Brně
Rektorát MENDELU
Oddělení spisové a archivní služby a podatelna
Mgr. Veronika Nechvátalová Aiblová
Zemědělská 1665/1 613 00 Brno
613 00 Brno
ID DS: 85ij9bs

Na vědomí:

odbor archivní správy a spisové služby
Nad Štolou 3
170 34 Praha 7

Odpověď na emailový dotaz týkající se kvalifikovaných prostředků pro vytváření elektronických podpisů

K emailovému podání ze dne 21.09.2020 paní Mgr. Veroniky Nechvátalové Aiblové, vedoucí oddělení spisové a archivní služby a podatelny Mendelovy univerzity v Brně.

Odboru eGovernmentu byla předána žádost od odboru archivní správy a spisové služby o přímé vyřízení dotazu č. 3 obsaženého v emailovém podání ze dne 21.09.2020 paní Mgr. Veroniky Nechvátalové Aiblové, vedoucí oddělení spisové a archivní služby a podatelny Mendelovy univerzity v Brně. Dotaz se týká otázky, z jakého právního předpisu vyplývá skutečnost, že zapamatování PINu pro vytvoření kvalifikovaného elektronického podpisu po určitou stanovenou dobu je protiprávní. Konkrétní znění dotazu:

Časovač při používání tokenu – z jaké legislativy to konkrétně vyplývá, že je to protiprávní?

Při online školení, pořádaného spol. Exponet zazněla informace, že užívání pomocných funkcí, které obcházejí nastavení důvěryhodného nosiče kvalifikovaného elektronického podpisu, kdy podepisující osoba musí vždy zadat pin svého podpisu pro každý podpis jednotlivě, je protiprávní. Je možné nám sdělit, z jakých konkrétních předpisů protiprávnost takového aktu vyplývá? Případně zda jsou za něj nějaké postihy nebo důsledky takového jednání pro organizaci?

K výše uvedenému dotazu uvádíme následující:

Právní předpisy regulující oblast služeb vytvářejících důvěru jsou zejména nařízení Evropského parlamentu a Rady (EU) č. 910/2014 ze dne 23. července 2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu a o zrušení směrnice 1999/93/ES (dále jen „nařízení eIDAS“) a v rámci České republiky také zákon č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce, ve znění pozdějších předpisů (dále jen „zákon č. 297/2016 Sb.“).

Nařízení eIDAS v souvislosti se zaručenými elektronickými podpisy a kvalifikovanými prostředky pro vytváření elektronických podpisů v této souvislosti stanovuje následující:

Článek 26 - Požadavky na zaručené elektronické podpisy – písmeno c):
c) je vytvořen pomocí dat pro vytváření elektronických podpisů, která podepisující osoba může s vysokou úrovní důvěry použít pod svou výhradní kontrolou; a

PŘÍLOHA II - POŽADAVKY NA KVALIFIKOVANÉ PROSTŘEDKY PRO VYTVÁŘENÍ ELEKTRONICKÝCH PODPISŮ („QSCD“) – odst. 1 písm. a) a zejména písm. d):

a) byla přiměřeně zajištěna důvěrnost dat pro vytváření elektronických podpisů, která byla použita při vytváření elektronického podpisu;
[…]
d) oprávněná podepisující osoba měla možnost data pro vytváření elektronických podpisů použitá při vytváření elektronického podpisu spolehlivě chránit před jejich zneužitím třetí osobou.

Jsme toho názoru, že z výše uvedených požadavků nelze jednoznačně vyvodit povinnost zadání PIN před každou operací elektronického podpisu. Je otázkou výkladu, jak striktně výše uvedené požadavky na zaručené elektronické podpisy a kvalifikované prostředky pro vytváření elektronických podpisů realizovat do aplikační praxe.

Podle našeho názoru obligatorní zadání PIN před každou operací elektronického podpisu nevyplývá ani z technických norem, na které nařízení eIDAS, respektive jeho prováděcí rozhodnutí Komise (EU) 2016/650 ze dne 25. dubna 2016, kterým se stanoví normy pro posuzování bezpečnosti kvalifikovaných prostředků pro vytváření elektronických podpisů a pečetí podle čl. 30 odst. 3 a čl. 39 odst. 2 nařízení Evropského parlamentu a Rady (EU) č. 910/2014 o elektronické identifikaci a službách vytvářejících důvěru pro elektronické transakce na vnitřním trhu, odkazuje v souvislosti s certifikací kvalifikovaných prostředků pro vytváření elektronických podpisů. K tomuto dodáváme, že předmětem certifikace je pouze prostředek (např. token nebo čipová karta), ale ne již aplikace pro vytváření elektronického podpisu.

Shrneme-li výše uvedené, skutečnost, zda kvalifikovaný prostředek pro vytváření elektronických podpisů vyžaduje před každou operací elektronického podpisu zadání PIN, se podle našeho názoru tedy odvíjí zejména od technické specifikace daného prostředku a od podmínek provozu taktového prostředku stanovené obvykle výrobcem prostředku. Platí, že je nutné dodržovat podmínky certifikace a provozu konkrétního kvalifikovaného prostředku pro vytváření el. podpisů, aby byla zajištěna korektní implementace procesu vytváření kvalifikovaného elektronického podpisu.

Z bezpečnostního hlediska je jistě vhodné, aby uživatel před každým podpisem zadal PIN, jelikož se tím minimalizuje riziko, že by byl podepsán dokument, který daný uživatel podepsat nechtěl. Pokud před každou operací elektronického podpisu není vyžadováno zadání PIN ze strany kvalifikovaného prostředku pro vytváření elektronických podpisů (PIN je zadán při první operaci elektronického podpisu a např. po stanovenou dobu/do ukončení programu používaného k elektronickému podepisování není třeba zadání PIN), pak je nutné dbát dle našeho názoru ještě další zvýšené bezpečnosti prostředí, kde dochází k vytvoření takového elektronického podpisu - prostředí musí být adekvátně zabezpečeno tak, aby nedošlo k tomu, že bude podepsán dokument, který podepisující osoba podepsat nechtěla.

Závěrem si dovoluji upozornit, že výše uvedené je pouze názorem odboru eGovernmentu Ministerstva vnitra, který není oprávněn k autoritativnímu výkladu právních předpisů; k takovému výkladu je oprávněn pouze příslušný soud.

Ing. Roman Vrba
ředitel

Vyřizuje: Mgr. Filip Bílek
tel. č.: 974 817 518
e-mail: filip.bilek@mvcr.cz