Kód:	SR/8/2023	
Číslo jednací:	UTB/23/006590	
Druh:	SMĚRNICE REKTORA	
Klasifikace dokumentu:	INTERNÍ	
Název:	Elektronické podpisy	
Organizační závaznost:	Univerzita Tomáše Bati ve Zlíně	
Datum vydání:	26.4.2023	Verze: 01
Účinnost od:	1.5.2023	
Vydává:	rektor	
Zpracoval:	Metodička spisové služby – Organizační odbor	
Spolupracoval:	IT technik – Sekretariát kvestora, vedoucí Organizačního odboru, ředitelka Centra výpočetní techniky	
Počet stran:	5	
Počet příloh:	1	
Rozdělovník:	Zaměstnanci UTB	
Podpis oprávněné osoby:	prof. Mgr. Milan Adámek, Ph.D. v. r.	

ČÁST PRVNÍ

Článek 1
I. Úvodní ustanovení

(1) Tato směrnice
- stanovuje pravidla pro podepisování elektronických dokumentů vzniklých z činnosti Univerzity Tomáše Bati ve Zlíně (dále jen „UTB“) jejími zaměstnanci,
- stanovuje postupy pro zřizování, obnovu a rušení certifikátů pro elektronické podpisy.

(2) Legislativní rámec:

Nařízení EU č. 910/2014 o elektronické identifikaci a důvěryhodných službách pro elektronické transakce na vnitřním evropském trhu (eIDAS), v platném znění,

zákon č. 499/2004 Sb., o archivnictví a spisové službě a o změně některých zákonů (dále jen „archivní zákon“), v platném znění,

vyhláška 259/2012 Sb., o podrobnostech výkonu spisové služby, v platném znění,

zákon č. 300/2008 Sb., o elektronických úkonech a autorizované konverzi dokumentů, v platném znění,

zákon č. 297/2016 Sb., o službách vytvářejících důvěru pro elektronické transakce, v platném znění,

zákon č. 250/2017 Sb., o elektronické identifikaci, v platném znění,

zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů, v platném znění.

(3) Tato směrnice navazuje na příslušná ustanovení Statutu UTB a dalších vnitřních předpisů a norem UTB v platném znění, zejména směrnice rektora Organizační řád, Pracovní řád, Podpisový řád, Spisový řád.

II. Základní pojmy

Časové razítko je datová zpráva, kterou vydal kvalifikovaný poskytovatel certifikačních služeb, a která důvěryhodným způsobem spojuje data v elektronické podobě s časovým okamžikem a zaručuje, že uvedená data v elektronické podobě existovala v daný okamžik.

Elektronický podpis jsou údaje v elektronické podobě, které jsou připojené k dokumentu nebo jsou s ním logicky spojené, a které slouží jako metoda k jednoznačnému ověření identity podepsané osoby ve vztahu k dokumentu. Právní předpisy rozlišují několik druhů elektronických podpisů:

- kvalifikovaný elektronický podpis, založený na kvalifikovaném certifikátu pro elektronický podpis a vytvořený pomocí hardwarového prostředku (musí být vytvořen pomocí kvalifikovaného [bezpečného] prostředku, který prošel povinně certifikací);
- zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis,
- zaručený elektronický podpis,
- tzv. „prostý“ elektronický podpis.

Elektronická pečeť jsou data v elektronické podobě, která jsou připojena k jiným datům v elektronické podobě nebo jsou s nimi logicky spojena s cílem zaručit jejich původ a integritu.

ČÁST DRUHÁ

Článek 2
Elektronické podpisy, pečetě, časová razítka

(1) UTB má jako orgán veřejné moci povinnost elektronicky podepisovat či pečetit formalizované dokumenty, které jsou výsledkem právního jednání vůči třetím osobám. Typicky se jedná o rozhodnutí, osvědčení, sdělení, veřejnoprávní smlouvy, doložky autorizované konverze dokumentů atd.

(2) Elektronické dokumenty, kterými UTB právně jedná, podepisuje oprávněný zaměstnanec kvalifikovaným elektronickým podpisem, který je umístěn na externím zařízení – kvalifikovaném prostředku QSCD (token, čipová karta, dále jen „token“). Podepsaný dokument podepisující opatřuje kvalifikovaným elektronickým časovým razítkem. Připojování elektronického podpisu a časového razítka k dokumentu se provádí zpravidla v elektronickém systému spisové služby (dále jen „eSSL“), případně v jiných informačních systémech (např. IS/STAG).

(3) Obecná podpisová oprávnění se řídí ustanoveními Podpisového řádu. Pracovní pozice, které jsou oprávněny mít zřízen elektronický podpis:

- rektor,
- prorektor oprávněný zastupovat rektora v plném rozsahu,
- prorektor,
- kvestor,
- zástupce kvestora,
- děkan, ředitel součásti a jejich zástupci,
- proděkan,
- tajemník fakulty, ekonom součásti,
- určený zaměstnanec Právního odboru,
- určený zaměstnanec Organizačního odboru,
- určení zaměstnanci Ekonomického odboru,

- určený zaměstnanec Personálního oddělení,
- zaměstnanci pověření prováděním konverze dokumentů.

(4) K podepisování elektronických dokumentů, které nezakládají právní jednání za UTB, používá oprávněný zaměstnanec zaručený elektronický podpis založený na kvalifikovaném certifikátu pro elektronický podpis, zaručený elektronický podpis, nebo tzv. „prostý“ elektronický podpis.

(5) Pokud není podpis náležitostí právního jednání a k potvrzení důvěryhodnosti dokumentu je postačující identifikace organizace, oprávněný zaměstnanec podatelny dokument opatří kvalifikovanou elektronickou pečetí a kvalifikovaným elektronickým časovým razítkem. Typicky se jedná např. o výstupy z eSSL jako transakční protokol, doručenky potvrzující přijetí datové zprávy, apod.

(6) Vydávání certifikátu pro elektronický podpis, jakož i jeho zneplatnění či obnovení se řídí postupem uvedeným v článku 3 této směrnice.

ČÁST TŘETÍ

Článek 3
Certifikáty

I. Správa certifikátů

(1) Pověřenou osobou pro správu certifikátů v systému PostSignum (www.postsignum.cz) je vedoucí Personálního oddělení. Provádí zavedení držitele certifikátu do systému, jeho odstranění a zneplatnění certifikátu.

(2) Vedoucí Personálního oddělení vede evidenci certifikátů, která obsahuje:
- identifikační číslo certifikátu,
- počátek a konec platnosti certifikátu,
- datum, čas a důvod zneplatnění certifikátu,
- název kvalifikovaného poskytovatele služeb vytvářejících důvěru,
- údaje identifikující podepisující nebo označující anebo pečetící osobu.

(3) Vedoucí Personálního oddělení odpovídá za včasné zneplatnění a odstranění certifikátu v případě zániku podpisových oprávnění příslušného zaměstnance.

II. Vydávání certifikátů pro elektronický podpis a komerční certifikát

(1) UTB má uzavřenu smlouvu o poskytování certifikačních služeb s kvalifikovaným správcem systému pro elektronickou identifikaci (dále jen „správce“), kterým je Česká pošta, s. p. Na základě této smlouvy zadává vedoucí Personálního oddělení žádost o certifikát pro zaměstnance, uvedené v článku 2 odstavci (3) této směrnice, prostřednictvím systému PostSignum (dále jen „systém“). Požadavek na vydání certifikátu zaměstnancům, neuvedeným v článku 2 odstavci (3) této směrnice, musí být před zadáním do systému schválen rektorem. Vzor žádosti je přílohou č. 1 této směrnice. (Zaměstnanci s žádostí o certifikát dále jen jako „uživatelé“).

(2) Po obdržení potvrzovacího e-mailu od vedoucího Personálního oddělení, že uživatel je zaveden v systému a je mu nastaveno oprávnění pro příslušný certifikát, si držitel certifikátu prostřednictvím aplikace iSignum (dále jen „aplikace“) vygeneruje prvotní žádost o vydání konkrétního certifikátu. Tento krok v případě certifikátu ukládaného na kvalifikovaném prostředku následuje až po provedené konfiguraci tokenu popsané v článku 3 bodu II odstavci (3). Na základě vygenerovaného čísla žádosti se zaměstnanec dostaví na pobočku Czech POINT, kde se prokáže příslušnými doklady a číslem podané žádosti. Po tomto nezbytném administrativním kroku od systému obdrží zaměstnanec e-mailem informaci, že mu byl vydán požadovaný certifikát.

(3) V případě certifikátu ukládaného na kvalifikovaném prostředku bude po zavedení do systému zaměstnanci vydán token zaměstnancem rektorátu (dále jen „IT technik“). Ve spolupráci s IT technikem, který do PC držitele nainstaluje příslušnou obslužnou utilitu, provede držitel tokenu jeho prvotní nakonfigurování dle instrukcí podaných IT technikem. Po této konfiguraci proběhne generování žádosti přes aplikaci včetně následných kroků, které jsou popsány v odstavci (2) tohoto bodu. Po obdržení potvrzovacího e-mailu ze systému si držitel ve spolupráci s IT technikem prostřednictvím aplikace nahraje certifikát na token. *(Poznámka: takto uložený certifikát bude moci držitel užít kdekoliv, kde je nainstalována příslušná utilita, která certifikát na tokenu operačnímu systému zviditelní, jinak nebude certifikát k podepisování k dispozici.)*

(4) Certifikát pro jiný než kvalifikovaný elektronický podpis jeho držitel po obdržení informace, že mu byl certifikát vystaven, importuje z aplikace přímo do úložiště certifikátů systému Windows, či jiného operačního systému. Vždy je v rámci bezpečnosti vyžadováno, aby si klíč k certifikátu i samotný certifikát chránil heslem, které se nastaví při prvotním importu a provedeném zálohování certifikátu. Pro import certifikátu může držitel požádat o pomoc IT technika své součásti. *(Poznámka: takto uložený certifikát bude moci držitel užít pouze z PC, na kterém má certifikát uložen.)*

(5) V případech, kdy držitel má různé typy certifikátů, musí pro každý typ certifikátu vystavit prvotní žádost o vydání daného certifikátu.

III. Zneplatnění certifikátu

(1) Certifikát je vázán na konkrétního zaměstnance, kterému byl vydán. Právo užívat certifikát zaniká v souvislosti se ztrátou podpisového oprávnění, a to zpravidla změnou pracovní pozice či skončením pracovního poměru. Nastane-li tato situace, je zaměstnanec povinen učinit následující:

- V případě, že je držitelem tokenu s certifikátem, odevzdat jej na Personální oddělení. O tomto předání se učiní zápis na předávacím protokolu agendy (při trvání pracovního poměru) nebo na výstupním listu (při ukončení pracovního poměru). Vedoucí Personálního oddělení bez zbytečného odkladu po ztrátě podpisového oprávnění provede zneplatnění tohoto certifikátu. Odevzdaný token předá vedoucí Personálního oddělení pověřenému zaměstnanci rektorátu, který provede odstranění stávajícího certifikátu z tokenu a rekonfigurování tokenu pro další použití.
- V případě, že je zaměstnanec držitelem certifikátu uloženého v úložišti certifikátů systému Windows či jiného operačního systému, je povinen nahlásit tuto skutečnost vedoucímu Personálního oddělení. Ten v součinnosti s IT technikem součásti zajistí odstranění tohoto certifikátu z PC a zneplatnění v systému.

(2) Držitel tokenu je povinen zabezpečit toto zařízení proti ztrátě, odcizení, zničení či zneužití jinou osobou. V případě ztráty či odcizení tokenu je zaměstnanec povinen tuto skutečnost neprodleně oznámit vedoucímu Personálního oddělení, který tuto skutečnost bez zbytečného odkladu ohlásí správci a v systému provede zneplatnění certifikátu uloženého na ztraceném/odcizeném tokenu.

(3) V případě, že dojde ke ztrátě nebo ke zničení tokenu, bude držiteli vydán nový token. Následně se postupuje stejně jako v případě prvotní žádosti o certifikát.

(4) V případě, kdy dojde ke ztrátě certifikátu uloženého v úložišti certifikátů systému Windows či jiného operačního systému, zpravidla ztrátou dat díky zničení systémového disku v PC a neprovedené zálohy certifikátu, je zaměstnanec povinen tuto skutečnost neprodleně oznámit vedoucímu Personálního oddělení, který tuto skutečnost bez zbytečného odkladu ohlásí IT technikovi součásti a v systému provede zneplatnění certifikátu uloženého na poškozeném či zničeném PC. Následně se postupuje stejně jako v případě prvotní žádosti o certifikát.

IV. Obnovení certifikátu

(1) Doba platnosti vydaného certifikátu je 1 nebo 3 roky. O tom, že se blíží vypršení termínu platnosti certifikátu, je držitel certifikátu zpravidla informován e-mailem ze strany certifikační autority, a to 20 a 7 dní před koncem platnosti. Kontrolu platnosti certifikátu si může provést každý držitel certifikátu sám prostřednictvím aplikace, utility k tokenu nebo přímo v úložišti certifikátů daného operačního systému.

(2) Obnovení certifikátu si provádí jeho držitel sám (pouze u certifikátů uložených v úložišti certifikátů operačního systému), nebo za asistence IT technika dané součásti (u ostatních typů úložišť certifikátů). Obnovení certifikátu provádí prostřednictvím aplikace. Po vygenerování žádosti o obnovení certifikátu obdrží držitel informaci, že mu byl obnoven certifikát, který prostřednictvím aplikace nahraje na příslušné úložiště (na token či úložiště certifikátů OS – úložiště musí být stejné jako to, na kterém měl původní certifikát uložen.)

(3) V případech, kdy má držitel různé typy certifikátů, se obnovení provádí pro každý typ certifikátu samostatně.

Z tokenu nebo dalších úložišť certifikátů je potřeba průběžně odstraňovat neplatné certifikáty, aby došlo k uvolnění místa pro další import certifikátů. Pro tyto úkony držitel certifikátu vždy kontaktuje IT technika rektorátu nebo příslušné součásti.

Verze dokumentu			
Datum	Verze	Změněno	Popis změny
25.04.2023	01	Elektronické podpisy	Vytvoření dokumentu