Česká pošta

# Zpráva pro uživatele CA

Verze 3.4

# Obsah dokumentu

# Evidence revizí a změn

| Verze | Datum revize | Důvod a popis změny | Autor | Schválil |
|---|---|---|---|---|
| 0.1 | 26.7.2005 | první verze | Manažer QCA | Manažer QCA |
| 1.01 | 5.9.2005 | menší změny dokumentu | Manažer QCA | Manažer QCA |
| 1.02 | 16.9.2006 | přidány informace o vydávání následných certifikátů | Manažer QCA | Manažer QCA |
| 1.1 | 12.1.2009 | změna struktury dokumentu, přidán seznam uskutečněných auditů a informace o reklamačním řízení | Manažer QCA | Manažer QCA |
| 2.0 | 2.9.2011 | Sloučení zprávy pro uživatele QCA a VCA a aktualizace údajů | Petr Huptich | Manažer CA |
| 2.1 | 1.7.2012 | aktualizován seznam auditů upraveny typy vydávaných certifikátů | Miroslav Trávníček | Manažer CA |
| 2.2 | 21.1.2013 | aktualizován seznam auditů | Miroslav Trávníček | Manažer CA |
| 2.3 | 12.4.2013 | aktualizován seznam auditů | Miroslav Trávníček | Manažer CA |
| 2.4 | 21. 7. 2014 | aktualizován seznam auditů, kontaktní pracoviště a typy certifikátů | Miroslav Trávníček | Manažer CA |
| 2.5 | 20. 2. 2015 | aktualizován seznam auditů a upraven název VOP | Miroslav Trávníček | Manažer CA |
| 2.6 | 1. 6. 2015 | aktualizován seznam auditů | Miroslav Trávníček | Manažer CA |
| 2.7 | 21. 1. 2016 | aktualizován seznam auditů | Miroslav Trávníček | Manažer CA |
| 3.0 | 1. 7. 2016 | změny dle eIDAS | Vosková/Trávníček | Manažer CA |
| 3.1 | 8. 9. 2017 | Změny v souvislosti s akreditací | Miroslav Trávníček | Manažer CA |
| 3.2 | 1. 4. 2018 | aktualizován seznam auditů | Miroslav Trávníček | Manažer CA |
| 3.3 | 3. 12. 2019 | aktualizován seznam auditů | Miroslav Trávníček | Manažer CA |
| 3.4 | 1 .9. 2020 | aktualizovány kontakty a seznam auditů | Miroslav Trávníček | Manažer CA |

# 1. Úvod

## 1.1. Účel dokumentu

Tento dokument poskytuje základní přehled o hierarchii certifikačních autorit PostSignum QCA a PostSignum VCA, právech a povinnostech držitelů certifikátů vydaných PostSignum Qualified CA, PostSignum Public CA a spoléhajících se stran.

Tento dokument má informační charakter, nenahrazuje certifikační politiky a není součástí smlouvy o poskytování certifikačních služeb uzavírané mezi zákazníkem a Českou poštou, s.p. (dále i Česká pošta nebo ČP).

## 1.2. Historie uskutečněných auditů a kontrol systému

| Datum | Typ auditu/kontroly | Výrok auditora/kontrolora |
|---|---|---|
| Květen 2020 | Audit potvrzující, že poskytované kvalifikované služby vytvářející důvěru jsou ve shodě s nařízením eIDAS a příslušnými technickými normami, provedený společností Tayllorcox s.r.o. | Je ve shodě |
| Únor 2020 | Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |
| Listopad 2019 | Posouzení shody dle požadavků Microsoft Root Certificate Program, provedené společností Tayllorcox s.r.o. | Vyhovuje |
| Květen 2019 | Audit potvrzující, že poskytované kvalifikované služby vytvářející důvěru jsou ve shodě s nařízením eIDAS a příslušnými technickými normami, provedený společností Tayllorcox s.r.o. | Je ve shodě |
| Únor 2019 | Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |
| Listopad 2018 | Posouzení shody dle požadavků Microsoft Root Certificate Program, provedené společností Tayllorcox s.r.o. | Vyhovuje |
| Únor 2018 | Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |
| Prosinec 2017 | Posouzení shody dle požadavků Microsoft Root Certificate Program, provedené společností Tayllorcox s.r.o. | Vyhovuje |
| Duben 2017 | Audit potvrzující, že poskytované kvalifikované služby vytvářející důvěru jsou ve shodě s nařízením eIDAS a příslušnými technickými normami, provedený společností Tayllorcox s.r.o. | Je ve shodě |
| Březen 2017 | Recertifikační audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |
| Listopad 2016 | Posouzení shody dle požadavků Microsoft Root Certificate Program, provedené firmou Deloitte Advisory | Vyhovuje |
| Únor 2016 | Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |

| | | |
|---|---|---|
| Září 2015 | Částečné posouzení bezpečnostní shody (interní audit ČP) | Vyhovuje |
| Březen 2015 | Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |
| Září 2014 | Částečné posouzení bezpečnostní shody (interní audit ČP) | Vyhovuje |
| Březen 2014 | Recertifikační audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |
| Září 2013 | Částečné posouzení bezpečnostní shody (interní audit ČP) | Vyhovuje |
| Únor 2013 | Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |
| Prosinec 2012 | Celkové posouzení bezpečnostní shody, provedené firmou Deloitte Advisory. | Vyhovuje |
| Únor 2012 | Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |
| Srpen 2011 | Částečné posouzení bezpečnostní shody (interní audit ČP) | Vyhovuje |
| Únor 2011 | Recertifikační audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |
| Listopad 2010 | Částečné posouzení bezpečnostní shody (interní audit ČP) | Vyhovuje |
| Únor 2010 | Částečné posouzení bezpečnostní shody (Microsoft Root Certificate Program), provedené firmou Deloitte Advisory | Vyhovuje |
| Leden 2010 | Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |
| Říjen 2009 | Částečné posouzení bezpečnostní shody (interní audit ČP) | Vyhovuje |
| Prosinec 2008 | Dozorový audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |
| Prosinec 2008 | Částečné posouzení bezpečnostní shody (interní audit ČP) | Vyhovuje |
| Březen 2008 | Celkové posouzení bezpečnostní shody, provedené firmou Deloitte Advisory. | Vyhovuje |
| Prosinec 2007 | Audit na certifikaci vůči ISO 9001 a ISO 27001, provedený firmou CQS. | Je v souladu |
| Prosinec 2007 | Částečné posouzení bezpečnostní shody (interní audit ČP) | Vyhovuje |
| Prosinec 2006 | Celkové posouzení bezpečnostní shody, provedené firmou Ernst & Young. | Vyhovuje |
| Září 2006 | Částečné posouzení bezpečnostní shody (interní audit ČP) | Vyhovuje |
| Červen 2005 | Celkové posouzení bezpečnostní shody, provedené firmou Ernst & Young. | Vyhovuje |

# 2. Kontaktní informace

## 2.1. Poskytovatel certifikačních služeb

Poskytovatelem certifikačních služeb PostSignum je:
Česká pošta, s.p., IČ 47114983
Politických vězňů 909/4
225 99 Praha 1

## 2.2. Kontaktní pracoviště

Uzavírání smluv se zákazníky PostSignum zajišťují obchodní a kontaktní místa PostSignum a Externí registrační autority. Kontaktní informace jsou k dispozici na webových stránkách PostSignum – www.postsignum.cz.

Vydávání a zneplatňování certifikátů zajišťují obchodní a kontaktní místa a Externí registrační autority.

Zneplatňování certifikátů mimo pracovní dobu kontaktních míst zajišťuje následující pracoviště:

Česká pošta, s.p.
Oddělení uživatelského provozu QCA/VCA
Wolkerova 480
749 20 Vítkov
e-mail: postsignum@cpost.cz
tel.: +420 954 303 303

## 2.3. Komunikace s klienty

Dotazy týkající se poskytování certifikačních služeb lze zasílat na kontaktní pracoviště pro poskytování služeb.

Odborné dotazy zodpovídá následující pracoviště:

e-mail: helpdesk-ca@cpost.cz
tel.: 800 104 410

## 2.4. Zveřejňování informací

Tuto zprávu pro uživatele, certifikační politiky a ostatní veřejné informace lze nalézt na webových stránkách PostSignum:

http://www.postsignum.cz

# 3. Typy certifikátů a ověřovací procedury

## 3.1. Typy vydávaných certifikátů

### 3.1.1. PostSignum Qualified CA

Česká pošta ustavila dvouúrovňovou hierarchii certifikačních autorit s názvem PostSignum QCA. Kořenem této hierarchie je certifikační autorita PostSignum Root QCA, která vydala certifikát pro certifikační autoritu PostSignum Qualified CA.

PostSignum Qualified CA vydává certifikáty koncovým uživatelům, přičemž uplatňuje dva základní modely registrace v závislosti na koncovém uživateli. První model registrace je zaměřen na právnické osoby a podnikající fyzické osoby, druhý model na jednotlivce - nepodnikající fyzické osoby.

PostSignum Qualified CA vydává tyto typy certifikátů:

- kvalifikované certifikáty pro elektronický podpis
- kvalifikované certifikáty pro elektronickou pečeť

Certifikáty veřejných klíčů vydávané v rámci hierarchie PostSignum Qualified CA vyhovují standardu X.509 v3.

Platnost certifikátů je volitelná. Lze požádat o certifikát s platností 385 dní nebo 1115 dní.

### 3.1.2. PostSignum Public CA

Česká pošta ustavila certifikační autoritu s názvem PostSignum Public CA (označovanou také jako PostSignum VCA), které vydala certifikát certifikační autorita PostSignum Root QCA.

PostSignum Public CA vydává certifikáty koncových uživatelů, přičemž uplatňuje dva základní modely registrace v závislosti na koncovém uživateli. První model registrace je zaměřen na právnické osoby a podnikající fyzické osoby, druhý model na jednotlivce - nepodnikající fyzické osoby.

PostSignum Public CA vydává tyto typy certifikátů:

- komerční osobní certifikáty,
- komerční serverové certifikáty,
- komerční doménové certifikáty.

Certifikáty veřejných klíčů vydávané v rámci PostSignum VCA vyhovují standardu X.509 v3.

Platnost certifikátů je volitelná. Lze požádat o certifikát s platností 385 dní (osobní a serverové certifikáty) nebo 397 dní (doménové certifikáty) a 1115 dní (osobní a serverové certifikáty).

## 3.2. Ověření žadatele při vydávání prvotního certifikátu

Během procesu vydávání prvotního certifikátu je vždy ověřována totožnost žadatele o certifikát prostřednictvím jeho osobních dokladů a v případě certifikátu pro právnickou nebo podnikající fyzickou osobu i vazba žadatele o certifikát na toto osobu.

Žadatel o certifikát musí být fyzicky přítomen během procesu vydávání certifikátu, nemůže zplnomocnit svého zástupce.

Pokud to registrační proces umožňuje, je možné totožnost prokázat i jiným způsobem.

Podrobný popis registračních postupů je uveden v příslušných certifikačních politikách.

## 3.3. Ověření žadatele při vydávání následného certifikátu

Během procesu vydávání následného certifikátu je totožnost žadatele o následný certifikát ověřována kontrolou elektronického podpisu na žádosti o následný certifikát.

Podrobný popis registračních postupů je uveden v příslušných certifikačních politikách.

# 4. Omezení použití

### 4.1.1. Kvalifikované certifikáty pro elektronický podpis

Kvalifikované certifikáty pro elektronický podpis vydané PostSignum QCA mohou být použity pouze k ověření elektronického podpisu v souladu s platnými právními předpisy.

Odpovídající soukromý klíč k vydanému kvalifikovanému certifikátu pro elektronický podpis může být uložen na kvalifikovaném prostředku pro vytváření elektronických podpisů, ale není to vyžadováno.

Kvalifikované certifikáty pro elektronický podpis vydávané PostSignum QCA nejsou určené pro komunikaci nebo transakce v oblastech se zvýšeným rizikem škod na zdraví nebo na majetku, jako jsou chemické provozy, letecký provoz, provoz jaderných zařízení apod., nebo v souvislosti s bezpečností a obranyschopností státu.

### 4.1.2. Kvalifikované certifikáty pro elektronickou pečeť

Kvalifikované certifikáty pro elektronickou pečeť vydané PostSignum QCA mohou být použity pouze k ověření elektronické pečetě v souladu s platnými právními předpisy.

Odpovídající soukromý klíč k vydanému kvalifikovanému certifikátu pro elektronickou pečeť může být uložen na kvalifikovaném prostředku pro vytváření elektronických pečetí, ale není to vyžadováno.

Kvalifikované certifikáty pro elektronickou pečeť vydávané PostSignum QCA nejsou určené pro komunikaci nebo transakce v oblastech se zvýšeným rizikem škod na zdraví nebo na majetku, jako jsou chemické provozy, letecký provoz, provoz jaderných zařízení apod., nebo v souvislosti s bezpečností a obranyschopností státu.

### 4.1.3. Komerční certifikáty PostSignum VCA

Certifikáty vydané PostSignum VCA mohou být použity k ověření elektronických podpisů, autentizaci, šifrování dat a k zabezpečení webových stránek.

Certifikáty vydávané PostSignum VCA nejsou určené pro komunikaci nebo transakce v oblastech se zvýšeným rizikem škod na zdraví nebo na majetku, jako jsou chemické provozy, letecký provoz, provoz jaderných zařízení apod., nebo v souvislosti s bezpečností a obranyschopností státu.

# 5. Povinnosti zákazníků a jejich zástupců

Zákazníkem certifikační autority PostSignum je právnická nebo fyzická osoba, která je v příslušném smluvním vztahu s Českou poštou. Zákazník musí zejména

- poskytovat pravdivé a úplné informace při uzavírání smlouvy o poskytování certifikačních služeb,
- neprodleně uvědomit poskytovatele certifikačních služeb o změnách údajů, které jsou uvedeny ve smlouvě nebo v certifikátu.

Žadatelem o certifikát je fyzická osoba, která z pověření zákazníka žádá o vydání certifikátu a spravuje vydaný certifikát (v případě zákazníka-fyzické nepodnikající osoby je žadatelem o certifikát zákazník).

Žadatel musí zejména

- seznámit se s certifikační politikou, podle které má být vydán certifikát,
- poskytovat pravdivé a úplné informace poskytovateli certifikačních služeb,
- neprodleně uvědomit poskytovatele certifikačních služeb o změnách údajů, které jsou uvedeny ve smlouvě o poskytování certifikačních služeb nebo ve vystaveném certifikátu,
- nakládat se soukromým klíčem, který odpovídá veřejnému klíči v certifikátu vydaném podle libovolné certifikační politiky, s náležitou péčí, tak, aby nemohlo dojít k jeho neoprávněnému použití, a užívat soukromý klíč pouze pro účely stanovené v certifikační politice, podle které byl vystaven odpovídající certifikát,
- neprodleně uvědomit poskytovatele certifikačních služeb o skutečnostech, které vedou ke zneplatnění certifikátu, zejména o podezření, že soukromý klíč byl zneužit, a požádat o zneplatnění certifikátu,
- v případě, že soukromý klíč je uložen na kvalifikovaném prostředku pro vytváření elektronických podpisů nebo pečetí:
  - mít generování a používání soukromého klíče pod svou výhradní kontrolou,
- soukromý klíč používat pouze pro vytváření elektronických podpisů nebo pečetí a v souladu s platnými právními předpisy.

# 6. Základní povinnosti spoléhajících se stran a ostatních uživatelů

Spoléhající se strany a ostatní uživatelé musí zejména

- získat certifikáty certifikačních autorit PostSignum Qualified CA, PostSignum Public CA a PostSignum Root QCA z bezpečného zdroje a ověřit otisk („fingerprint“) těchto certifikátů,
- před použitím certifikátu vydaného PostSignum Qualified CA ověřit platnost certifikátu PostSignum Qualified CA, PostSignum Root QCA a následně i platnost vydaného koncového certifikátu,
- před použitím certifikátu vydaného PostSignum Public CA ověřit platnost certifikátu PostSignum Public CA, PostSignum Root QCA a následně i platnost vydaného koncového certifikátu,

- dostatečně zvážit (zejména na základě znalosti příslušné certifikační politiky), zda je certifikát vydaný PostSignum Qualified CA nebo PostSignum Public CA podle příslušné politiky vhodný pro účel, ke kterému jej chce použít.

# 7. Omezení záruky a odpovědnosti

Česká pošta se zavazuje, že splní veškeré povinnosti uložené certifikačními politikami, podle kterých vystavuje certifikáty, a mandatorními ustanoveními příslušných právních předpisů.

Česká pošta poskytuje výše uvedené záruky po celou dobu platnosti smlouvy o poskytování certifikačních služeb uzavřené se zákazníkem.

Záruky uvedené výše jsou výlučnými zárukami České pošty a Česká pošta jiné záruky neposkytuje.

Česká pošta neodpovídá za vady poskytnutých služeb vzniklé z důvodu nesprávného nebo neoprávněného využívání služeb poskytnutých v rámci plnění smlouvy o poskytování certifikačních služeb držitelem, zejména za provozování v rozporu s podmínkami uvedenými v certifikační politice, jakož i za vady vzniklé z důvodu vyšší moci, včetně dočasného výpadku telekomunikačního spojení aj. Dále Česká pošta neodpovídá za škodu vyplývající z použití kvalifikovaného certifikátu pro elektronický podpis nebo certifikátu pro elektronickou pečeť v období po podání žádosti o jeho zneplatnění, pokud Česká pošta dodrží definovanou lhůtu pro zveřejnění zneplatněného kvalifikovaného certifikátu pro elektronický podpis nebo certifikátu pro elektronickou pečeť na seznamu zneplatněných certifikátů (CRL).

# 8. Smlouvy a certifikační politiky

Vztah mezi zákazníkem a Českou poštou jakožto poskytovatelem certifikačních služeb je (kromě příslušných ustanovení mandatorních právních předpisů) upraven smlouvou, jejíž součástí jsou mimo jiné

- Všeobecné obchodní podmínky certifikačních služeb,
- platné certifikační politiky a
- aktuální ceník.

Vztah mezi spoléhající se stranou a Českou poštou (jakožto poskytovatelem certifikačních služeb) je upraven příslušnými ustanoveními platných certifikačních politik.

Vztah České pošty a spoléhajících se stran není upraven smlouvou.

Všechny vyjmenované dokumenty jsou dostupné na webových stránkách PostSignum nebo na obchodních místech certifikační autority.

# 9. Ochrana osobních dat

Česká pošta zajišťuje ochranu osobních údajů osob, k nimž získá přístup při poskytování certifikačních služeb. Zásady ochrany osobních údajů jsou obsaženy v certifikačních politikách, Všeobecných obchodních podmínkách certifikačních služeb a v aktuální certifikační prováděcí směrnici a vycházejí z příslušných ustanovení zákona č. 110/2019 Sb. o zpracování osobních údajů ve znění pozdějších předpisů.

Žadatel o certifikát dává České poště souhlas se zpracováním osobních údajů v rozsahu nezbytném pro vydání a zneplatnění certifikátu s požadovanými údaji.

# 10. Politika náhrady a reklamační řízení

V případě nedodání služeb v definované kvalitě (např. vydání certifikátu se špatným obsahem) má zákazník nárok na vrácení ceny za příslušnou službu nebo poskytnutí nové služby zdarma.

Bližší informace o reklamačním řízení jsou uvedeny na webových stránkách PostSignum.

# 11. Právní prostředí

Činnost PostSignum QCA se řídí příslušnými ustanoveními právního řádu České republiky, zejména

- zákonem č. 297/2016 Sb. o službách vytvářejících důvěru pro elektronické transakce,
- nařízením 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 (eIDAS),
- zákonem č.110/2019 Sb. o zpracování osobních údajů ve znění pozdějších předpisů.

Činnost PostSignum VCA se řídí příslušnými ustanoveními právního řádu České republiky, zejména

- zákonem č.110/2019 Sb. o zpracování osobních údajů ve znění pozdějších předpisů.

# 12. Akreditace a posouzení shody

Česká pošta se jako poskytovatel certifikačních služeb PostSignum QCA stala dne 3. 8. 2005 akreditovaným poskytovatelem certifikačních služeb na základě akreditace udělené Ministerstvem informatiky ČR.

Dne 21. 12. 2007 získal informační systém PostSignum QCA a PostSignum VCA certifikaci shody s ISO 9001 (QMS, systém řízení kvality) a ISO 27001 (ISMS, systém řízení bezpečnosti informací).

Dne 1. 7. 2016 se Česká pošta stala kvalifikovaným poskytovatelem služeb vytvářejících důvěru dle eIDAS pro vydávání kvalifikovaných certifikátů pro elektronický podpis.

Dne 30. 8. 2017 byly v důvěryhodném seznamu kvalifikovaných služeb přidány kvalifikované služby:

- vydávání kvalifikovaných certifikátů pro elektronickou pečeť
- vydávání kvalifikovaných certifikátů pro autentizaci webových stránek

Činnost certifikační autority PostSignum podléhá kontrole. Posouzení shody s platnými právními předpisy a technickými normami provádí externí auditor nezávislý na České poště, s.p. Intervaly konání kontrol jsou uvedeny v certifikačních politikách.