

ROZHODNUTÍ

ROZHODNUTÍ EVROPSKÉ CENTRÁLNÍ BANKY

ze dne 11. ledna 2013,

kterým se stanoví rámec infrastruktury veřejných klíčů Evropského systému centrálních bank

(ECB/2013/1)

(2013/132/EU)

RADA GUVERNÉRŮ EVROPSKÉ CENTRÁLNÍ BANKY,

s ohledem na Smlouvu o fungování Evropské unie, a zejména na článek 127 této smlouvy,

s ohledem na statut Evropského systému centrálních bank a Evropské centrální banky (dále jen „statut ESCB“), a zejména na článek 12.1 ve spojení s článkem 3.1, článkem 5, článkem 12.3 a články 16 až 24 tohoto statutu,

vzhledem k těmto důvodům:

- (1) Podle článku 12.1 statutu ESCB Rada guvernérů přijímá obecné zásady a činí rozhodnutí nezbytná pro zajištění plnění úkolů svěřených Evropskému systému centrálních bank (ESCB) a Eurosystemu Smlouvou a statutem ESCB. To zahrnuje pravomoc rozhodovat o organizaci podpůrných činností, které jsou pro plnění těchto úkolů nezbytné a mezi něž se řadí například vydávání a správa elektronických certifikátů k zabezpečení informací uložených a zpracovávaných v elektronických aplikacích, systémech, platformách a službách ESCB a Eurosystemu, jakož i pro datovou komunikaci těchto aplikací, systémů, platform a služeb.
- (2) Podle článku 12.3 statutu ESCB má Rada guvernérů rovněž pravomoc upravit vnitřní organizaci Evropské centrální banky (ECB) a jejích rozhodovacích orgánů. Rada guvernérů má tedy pravomoc rozhodnout, že ECB bude používat elektronické certifikáty vydané vlastní infrastrukturou veřejných klíčů Eurosystemu.
- (3) Zvyšuje se počet uživatelů, kteří mají přístup k rostoucímu počtu elektronických aplikací, systémů, platform a služeb ESCB a Eurosystemu, jež se neustále vyvíjejí. Rada guvernérů dospěla k závěru, že jsou zapotřebí rozvinuté služby v oblasti bezpečnosti informací, kterými jsou například silná autentizace, elektronické podpisy a šifrování pomocí elektronických certifikátů.
- (4) Jen některé centrální banky ESCB mají svou vlastní infrastrukturu veřejných klíčů a mnoho uživatelů z řad třetích osob, které spolupracují s centrálními bankami ESCB, nemá snadný přístup k certifikační autoritě, kterou ESCB uznává v souladu se svým rámcem pro akceptaci certifikátů.
- (5) Je třeba, aby si Eurosystem vytvořil svou vlastní infrastrukturu veřejných klíčů, která bude moci vydávat všechny druhy elektronických certifikátů, jako jsou například osobní a technické certifikáty pro uživatele z řad ESCB i mimo ESCB, a která bude dostatečně pružná, aby se přizpůsobovala vývoji elektronických aplikací, systémů, platform a služeb ESCB a Eurosystemu. Tato infrastruktura veřejných klíčů (dále jen „infrastruktura veřejných klíčů ESCB“) by měla doplňovat služby, které poskytují jiné certifikační autority, jež ESCB uznává v souladu s rámcem ESCB pro akceptaci certifikátů, nebo které poskytují certifikační autority, které ESCB uznává pro účely TARGET2 a TARGET2-Securities pro tyto dvě aplikace.
- (6) Dne 29. září 2010 rozhodla Rada guvernérů o zahájení projektu infrastruktury veřejných klíčů ESCB s cílem vytvořit a zavést infrastrukturu veřejných klíčů ESCB, jakož i o poskytnutí zdrojů nezbytných pro plnou realizaci tohoto projektu. Rozhodla, že vývoj, platformu a provoz infrastruktury veřejných klíčů ESCB zabezpečí Banco de España.
- (7) Infrastruktura veřejných klíčů ESCB nepřímo podporuje plnění úkolů ESCB a Eurosystemu. Jejím základem jsou tři úrovně řízení: první úroveň sestává z Rady guvernérů a Výkonné rady, druhá úroveň z centrálních bank Eurosystemu a třetí úroveň z poskytující centrální banky.
- (8) Na první úrovni odpovídá Rada guvernérů za řízení, správu a kontrolu činností a výstupů, které jsou třeba pro vývoj a provoz infrastruktury veřejných klíčů ESCB. Odpovídá rovněž za rozhodování ohledně infrastruktury veřejných klíčů ESCB a rozhoduje o přidělování úkolů, které nejsou konkrétně svěřeny druhé a třetí úrovni.
- (9) Centrální banky Eurosystemu v rámci obecného rámce vymezeného Radou guvernérů odpovídají za úkoly přidělené druhé úrovni. Mají pravomoc v oblasti technických prostředků realizace infrastruktury veřejných klíčů ESCB.

- (10) Výbor ESCB pro informační technologie řídí vývoj infrastruktury veřejných klíčů ESCB. Vede, hodnotí, kontroluje a schvaluje projektové výstupy na základě akceptačních kritérií podle rámce ESCB pro akceptaci certifikátů, rozsahu a harmonogramu schváleného Radou guvernérů.
- (11) Na třetí úrovni byla jako poskytovající centrální banka jmenována Banco de España, aby vykonávala úkoly, které jí jsou přiděleny na základě obecného rámce vymezeného Radou guvernérů. Poskytovající centrální banka zavedla technickou infrastrukturu a bezpečné prostředky a služby, jež jsou třeba k vytvoření a užívání infrastruktury veřejných klíčů v souladu s: a) vnitrostátním právním předpisem, kterým se provádí směrnice Evropského parlamentu a Rady 1999/93/ES ze dne 13. prosince 1999 o zásadách Společenství pro elektronické podpisy ⁽¹⁾, v rozsahu, který se na infrastrukturu veřejných klíčů vztahuje; b) vnitrostátním právním předpisem, kterým se provádí směrnice Evropského parlamentu a Rady 95/46/ES ze dne 24. října 1995 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů ⁽²⁾, v rozsahu, který se na infrastrukturu veřejných klíčů vztahuje, a c) nařízením Evropského parlamentu a Rady (ES) č. 45/2001 ze dne 18. prosince 2000 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů orgány a institucemi Společenství a o volném pohybu těchto údajů ⁽³⁾.
- (12) Jelikož elektronické certifikáty jsou základními prvky, které se v elektronických aplikacích používají jako prostředky autentizace k provedení elektronických podpisů, jakož i k šifrování na základě veřejného klíče, zohlední infrastruktura veřejných klíčů ESCB stávající elektronické aplikace, systémy, platformy a služby ESCB a Eurosystemu a současné projekty ESCB s cílem zajistit jejich potřeby.
- (13) Národní centrální banky mimo eurozónu mohou rozhodnout, že budou využívat certifikáty a služby poskytované infrastrukturou veřejných klíčů ESCB,
- k elektronickým aplikacím, systémům, platformám a službám ESCB a Eurosystemu. Veškeré odkazy na certifikát nebo elektronický certifikát v tomto rozhodnutí zahrnují odkaz na zařízení pro přenos dat, na nichž je certifikát nebo elektronický certifikát uložen;
2. „elektronickými aplikacemi, systémy, platformami a službami ESCB a Eurosystemu“ elektronické aplikace, systémy, platformy a služby, které ESCB a/nebo Eurosystem využívají při plnění úkolů, které jim byly svěřeny na základě Smlouvy a statutu ESCB;
 3. „infrastrukturou veřejných klíčů“ soubor fyzických osob, politik, postupů a počítačových systémů, které jsou nezbytné k poskytování služeb autentizace, šifrování, integrity a nepopiratelnosti prostřednictvím šifrování pomocí veřejného a soukromého klíče a elektronických certifikátů;
 4. „uživatel“ držitel certifikátu nebo spoléhající se strana či obě tyto osoby;
 5. „autentizační“ postup ověřování totožnosti žadatele o certifikát nebo držitele certifikátu;
 6. „centrální bankou ESCB“ centrální banka Eurosystemu nebo národní centrální banka mimo eurozónu;
 7. „centrální bankou Eurosystemu“ buď národní centrální banka členského státu, jehož měnou je euro, včetně poskytovající centrální banky, nebo ECB;
 8. „poskytovající centrální bankou“ národní centrální banka, kterou Rada guvernérů jmenovala, aby vyvinula infrastrukturu veřejných klíčů ESCB a aby jménem a ve prospěch centrálních bank Eurosystemu poskytovala služby infrastruktury veřejných klíčů ESCB;
 9. „národní centrální bankou mimo eurozónu“ národní centrální banka členského státu, jehož měnou není euro;
 10. „certifikační autoritou infrastruktury veřejných klíčů ESCB“ subjekt, který je pro uživatele důvěryhodný a který jménem centrálních bank ESCB nebo centrálních bank Eurosystemu vydává, spravuje, odvolává a obnovuje certifikáty v souladu s rámcem ESCB pro akceptaci certifikátů;
 11. „validační autoritou infrastruktury veřejných klíčů ESCB“ subjekt, který je pro uživatele důvěryhodný a který poskytuje informace o platnosti certifikátů vydaných certifikační autoritou infrastruktury veřejných klíčů ESCB;
 12. „držitelem certifikátu“ buď fyzická osoba, na kterou se elektronický certifikát vztahuje a již byl elektronický certifikát vydán, nebo správce technické komponenty, který přijal elektronický certifikát vydaný certifikační autoritou infrastruktury veřejných klíčů ESCB pro tuto technickou komponentu, či obě tyto osoby;
 13. „rámcem ESCB pro akceptaci certifikátů“ kritéria, která zavedl Výbor ESCB pro informační technologie s cílem určit certifikační autority, a to jak v rámci, tak i vně

PŘIJALA TOTO ROZHODNUTÍ:

Článek 1

Definice

Pro účely tohoto rozhodnutí se rozumí:

1. „certifikátem“ nebo „elektronickým certifikátem“ elektronický soubor vydaný certifikační autoritou, který spojuje veřejný klíč s totožností určitého držitele certifikátu a který se používá k následujícím účelům: a) k ověření, že veřejný klíč patří určitému držiteli certifikátu; b) k autentizaci držitele certifikátu; c) ke kontrole podpisu držitele certifikátu; d) k šifrování zpráv adresovaných držiteli certifikátu; e) k ověření přístupových práv držitele certifikátu

⁽¹⁾ Úř. věst. L 13, 19.1.2000, s. 12.

⁽²⁾ Úř. věst. L 281, 23.11.1995, s. 31.

⁽³⁾ Úř. věst. L 8, 12.1.2001, s. 1.

ESCB, jimž lze důvěřovat ve vztahu k elektronickým aplikacím, systémům, platformám a službám ESCB a Eurosystemu;

14. „registrační autoritou“ subjekt, který je pro uživatele důvěryhodný a který ověřuje totožnost žadatele o certifikát předtím, než certifikační autorita infrastruktury veřejných klíčů ESCB certifikát vydá;
15. „spoléhající se stranou“ fyzická osoba nebo subjekt, který není držitelem certifikátu a který certifikát přijímá a spoléhá se na něj;
16. „pravidly pro provádění auditu“ pravidla pro provádění auditu, která vymezila Rada guvernérů dne 7. října 1998 a která jsou zveřejněna na internetových stránkách ECB ⁽¹⁾;
17. „žadatelem o certifikát“ fyzická osoba, která žádá o vydání certifikátu pro sebe nebo pro technickou komponentu;
18. „technickou komponentou“ veškeré programové vybavení (software) či technické zařízení (hardware), jež lze identifikovat elektronickým certifikátem.

Článek 2

Oblast působnosti

1. Toto rozhodnutí zavádí rámec pro infrastrukturu veřejných klíčů ESCB. Infrastruktura veřejných klíčů ESCB je vlastní infrastruktura veřejných klíčů Eurosystemu, kterou jménem a ve prospěch centrálních bank Eurosystemu vyvíjí poskytující centrální banka, která vydává, spravuje, odvolává a obnovuje certifikáty v souladu s rámcem ESCB pro akceptaci certifikátů.
2. Vzhledem k tomu, že služby infrastruktury veřejných klíčů ESCB mohou mít dopad na spoléhající se strany, stanoví toto rozhodnutí rovněž podmínky, za nichž se tyto strany mohou spoléhat na certifikáty infrastruktury veřejných klíčů ESCB.

Článek 3

Rozsah a cíle infrastruktury veřejných klíčů ESCB

1. Elektronické aplikace, systémy, platformy a služby ESCB a Eurosystemu se středním nebo vyšším než středním stupněm kritičnosti lze zpřístupnit a používat jen tehdy, pokud byla provedena autentizace uživatele pomocí elektronického certifikátu, který vydává a spravuje certifikační autorita, kterou ESCB uznává v souladu s rámcem ESCB pro akceptaci certifikátů, včetně certifikační autority infrastruktury veřejných klíčů ESCB nebo certifikačních autorit, které ESCB uznává pro účely TARGET2 a TARGET2-Securities pro tyto dvě aplikace.
2. Certifikační autorita infrastruktury veřejných klíčů ESCB vydává elektronické certifikáty a poskytuje další elektronické certifikační služby pro držitele certifikátů z řad centrálních bank ESCB a třetích osob, které s nimi spolupracují, s cílem umožnit jim bezpečný přístup a použití elektronických aplikací, systémů, platforem a služeb ESCB a Eurosystemu.

3. Infrastruktura veřejných klíčů ESCB poskytuje tyto certifikační služby:

- a) vydávání, obnovu a odvolání certifikátů a potvrzování platnosti certifikátů s ohledem na různé druhy certifikátů;
- b) vydávání certifikátů pro autentizaci, elektronický podpis a šifrování ve vztahu k uživatelům z ESCB i mimo ESCB, jakož i technických certifikátů;
- c) obnovu soukromého klíče s cílem zajistit opětovné získání informací šifrovaných veřejným klíčem v případě ztráty certifikátu;
- d) doručení kryptografických tokenů držitelům certifikátů a jejich správu, je-li to třeba;
- e) poskytování informací o postupech správy certifikátů v rámci infrastruktury veřejných klíčů ESCB, jakož i technické podpory projektovým manažerům ESCB s cílem pomoci jim integrovat certifikáty infrastruktury veřejných klíčů ESCB do jejich aplikací.

Podle potřeby elektronických aplikací, systémů, platforem a služeb ESCB a Eurosystemu lze v budoucnu přidávat další služby.

Článek 4

Rámec infrastruktury veřejných klíčů ESCB

1. Na základě tohoto rozhodnutí jsou odpovědnost a funkce poskytující centrální banky a ostatních centrálních bank Eurosystemu ve vztahu k provádění, provozu a používání infrastruktury veřejných klíčů ESCB stanoveny v dohodě mezi druhou a třetí úrovní řízení a dále podrobně vymezeny v certifikační politice v rámci infrastruktury veřejných klíčů ESCB a v certifikační praxi v rámci infrastruktury veřejných klíčů ESCB.
2. Dohoda mezi druhou a třetí úrovní řízení, která zahrnuje dohodu o úrovni služeb, obsahuje dohodu, kterou poskytující centrální banka sjednala s centrálními bankami Eurosystemu, pokud jde o odpovědnost a funkce poskytující centrální banky a centrálních bank Eurosystemu. Bude předložena ke schválení Radě guvernérů, a potom ji podepíše poskytující centrální banka a centrální banky Eurosystemu.
3. Dohoda o úrovni služeb je dohodou, která vymezuje úroveň služeb, jež má poskytující centrální banka poskytovat Eurosystemu, jakož i dohodou, která vymezuje úroveň služeb, jež má Eurosystem v souvislosti s infrastrukturou veřejných klíčů ESCB poskytovat národním centrálním bankám mimo eurozónu a třetím osobám.
4. Certifikační praxe v rámci infrastruktury veřejných klíčů ESCB je soubor pravidel, jež upravují životní cyklus elektronických certifikátů od počáteční žádosti po skončení platnosti či odvolání, jakož i vztahy mezi žadatelem o certifikát nebo držitelem certifikátu, certifikační autoritou infrastruktury veřejných klíčů ESCB a spoléhajícími se stranami. Vztahuje se na elektronické certifikáty, které spadají do oblasti působnosti směrnice 1999/93/ES, i na elektronické certifikáty, které do oblasti působnosti této směrnice nespádají. Rovněž vymezuje úlohu a odpovědnost všech stran a zavádí postupy pro vydávání a správu certifikátů. Tvoří přílohu dohody mezi druhou a třetí úrovní řízení.

⁽¹⁾ www.ecb.europa.eu.

5. Certifikační politika v rámci infrastruktury veřejných klíčů ESCB je soubor pravidel, jež platí pro každý druh vydaného certifikátu. Každý soubor stanoví podrobnosti provádění certifikační praxe v rámci infrastruktury veřejných klíčů ESCB pro každý druh vydaného certifikátu. Certifikační politika v rámci infrastruktury veřejných klíčů ESCB tvoří přílohu dohody mezi druhou a třetí úrovní řízení.

6. Certifikační politika v rámci infrastruktury veřejných klíčů ESCB a certifikační praxe v rámci infrastruktury veřejných klíčů ESCB se zveřejňují na internetových stránkách infrastruktury veřejných klíčů ESCB ⁽¹⁾.

7. Informace o certifikační autoritě infrastruktury veřejných klíčů ESCB včetně její totožnosti a technických komponent jsou vymezeny v příloze tohoto rozhodnutí.

Článek 5

Odpovědnost a úloha poskytující centrální banky

1. Poskytující centrální banka odpovídá za provoz a udržování infrastruktury veřejných klíčů ESCB ve prospěch centrálních bank Eurosystemu, včetně zabezpečení platformy, provozu a správy vykonávané v souladu s dohodou mezi druhou a třetí úrovní řízení. Zejména vydává certifikáty a poskytuje služby infrastruktury veřejných klíčů ESCB v souladu s obchodními požadavky a technickými specifikacemi, kterými jsou například rámec ESCB pro akceptaci certifikátů a požadavky a specifikace uvedené v dohodě mezi druhou a třetí úrovní řízení.

2. Poskytující centrální banka zavede nezbytnou organizační infrastrukturu pro vytváření, vydávání a správu certifikátů a zajistí udržování této infrastruktury. Za tímto účelem může poskytující centrální banka po konzultaci s Výborem pro informační technologie přijmout pravidla své vnitřní organizace a správy.

3. Poskytující centrální banka jedná jako certifikační autorita infrastruktury veřejných klíčů ESCB a jako validační autorita infrastruktury veřejných klíčů ESCB.

4. Dohoda mezi druhou a třetí úrovní řízení stanoví úpravu odpovědnosti platnou pro poskytující centrální banku.

Článek 6

Odpovědnost a úloha centrálních bank Eurosystemu

1. Každá centrální banka Eurosystemu odpovídá za identifikaci svých držitelů certifikátů. Za účelem plnění tohoto úkolu zřídí úlohu registračního úředníka, který má pravomoc provádět registrace uživatelů z řad třetích osob.

2. Každá centrální banka Eurosystemu jedná jako spoléhající se strana ve vztahu k certifikátům pro šifrování a elektronický podpis, které infrastruktura veřejných klíčů ESCB vydala pro jiné centrální banky Eurosystemu nebo pro držitele certifikátů, kteří jsou uživateli z řad třetích osob.

3. Každá centrální banka Eurosystemu, která využívá služby infrastruktury veřejných klíčů ESCB, jedná jako registrační autorita pro své žadatele o certifikát a zajistí, že její žadatelé o certifikát souhlasí s podmínkami pro uživatele, které jsou uvedeny ve formuláři žádosti o služby certifikační autority infrastruktury veřejných služeb ESCB, a podle těchto podmínek postupují.

Článek 7

Vztahy mezi centrálními bankami Eurosystemu, třetími osobami a držiteli certifikátů

Každá centrální banka Eurosystemu přijme opatření týkající se bezpečného přístupu třetích osob k elektronickým aplikacím, systémům, platformám a službám ESCB a Eurosystemu a jejich bezpečného používání těmito osobami pomocí certifikátů infrastruktury veřejných klíčů ESCB. Tato opatření upravují výlučně vztah mezi příslušnou centrální bankou Eurosystemu a třetími osobami, které používají certifikáty infrastruktury veřejných klíčů ESCB. Všechny třetí osoby postupují v souladu s certifikační politikou v rámci infrastruktury veřejných klíčů ESCB, certifikační praxí v rámci infrastruktury veřejných klíčů ESCB a podmínkami pro uživatele, které jsou uvedeny ve formuláři žádosti o služby certifikační autority infrastruktury veřejných služeb ESCB.

Článek 8

Vztahy se spoléhajícími se stranami

Na elektronický certifikát vydaný na základě tohoto rozhodnutí se lze spoléhat, pokud spoléhající se strana:

- s použitím aktuálních informací o stavu odvolání certifikátů ověří platnost, pozastavení nebo odvolání certifikátu;
- zohlední všechna uživatelská omezení vymezená v certifikátu a
- vysloví souhlas s certifikační praxí v rámci infrastruktury veřejných klíčů ESCB i s příslušnou certifikační politikou v rámci infrastruktury veřejných klíčů ESCB.

Článek 9

Práva k infrastruktuře veřejných klíčů ESCB

1. Infrastruktura veřejných klíčů ESCB je v úplném vlastnictví centrálních bank Eurosystemu.

2. S ohledem na tuto skutečnost poskytující centrální banka v rozsahu, který umožňují příslušné právní předpisy, udělí centrálním bankám Eurosystemu veškeré licence týkající se práv duševního vlastnictví, jež jsou zapotřebí k tomu, aby centrální banky Eurosystemu mohly využívat infrastrukturu veřejných klíčů ESCB a její komponenty i celý rozsah služeb infrastruktury veřejných klíčů ESCB a aby rovněž mohly poskytovat služby infrastruktury veřejných klíčů ESCB třetím osobám na základě certifikační praxe v rámci infrastruktury veřejných klíčů ESCB i certifikační politiky v rámci infrastruktury veřejných klíčů ESCB. Poskytující centrální banka odškodní centrální banky Eurosystemu v případě, že dojde k uplatnění nároků z porušení práv ze strany třetích osob ve vztahu k těmto právům duševního vlastnictví.

3. Podrobnosti týkající se práv centrálních bank Eurosystemu k infrastruktuře veřejných klíčů ESCB budou mezi druhou a třetí úrovní dohodnuty v dohodě mezi druhou a třetí úrovní řízení.

Článek 10

Odpovědnost centrálních bank Eurosystemu vůči uživatelům

1. Ledaže centrální banky Eurosystemu prokážou, že nejednaly z nedbalosti, odpovídají v souladu se svými funkcemi

⁽¹⁾ <http://pki.escb.eu>.

a odpovědností v rámci infrastruktury veřejných klíčů ESCB za škodu způsobenou uživateli, který se důvodně spoléhá na kvalifikovaný certifikát, tj. kvalifikované osvědčení ve smyslu směrnice 1999/93/ES, pokud jde o:

- a) přesnost veškerých informací obsažených v kvalifikovaném certifikátu ke dni jeho vydání a o otázku, zda osvědčení obsahuje veškeré údaje stanovené pro kvalifikovaný certifikát ve smyslu směrnice 1999/93/ES;
- b) ujištění, že v době vydání kvalifikovaného certifikátu byl držitel certifikátu uvedený v kvalifikovaném certifikátu držitelem dat pro vytváření podpisu odpovídajících datům pro ověřování podpisu uvedeným nebo označeným v certifikátu;
- c) ujištění, že zařízení pro vytváření podpisu a zařízení pro ověřování podpisu fungují společně doplňujícím způsobem v případě, kdy infrastruktura veřejných klíčů ESCB vytváří obě tyto složky;
- d) opomenutí zaregistrovat odvolání kvalifikovaný certifikátu.

2. Centrální banky Eurosystemu nepřebírají žádné závazky, neposkytují žádné záruky a nepřebírají žádnou odpovědnost vůči uživatelům, jestliže to není výslovně uvedeno v tomto rozhodnutí a v certifikační praxi v rámci infrastruktury veřejných klíčů ESCB.

Článek 11

Účast národních centrálních bank mimo eurozónu v infrastruktuře veřejných klíčů ESCB

1. Národní centrální banka mimo eurozónu může jednat jako registrační autorita pro své interní uživatele i pro uživatele z řad třetích osob a za účelem plnění tohoto úkolu může zřídit úlohu registračního úředníka.
2. Se souhlasem Rady guvernérů mohou národní centrální banky mimo eurozónu rovněž rozhodnout, že budou využívat služby infrastruktury veřejných klíčů ESCB za stejných podmínek, které platí pro centrální banky Eurosystemu. Za tímto účelem národní centrální banky mimo eurozónu předloží Radě guvernérů prohlášení, v němž potvrdí, že budou plnit povinnosti uvedené v tomto rozhodnutí a v dohodě mezi druhou a třetí úrovní řízení. Národní centrální banka mimo eurozónu se nestane spoluvlastníkem infrastruktury veřejných klíčů ESCB a není povinna přispívat na finanční krytí infrastruktury veřejných klíčů ESCB.

Článek 12

Ochrana údajů

Centrální banky Eurosystemu postupují v souladu s právními předpisy o ochraně údajů, které se vztahují na zpracování osobních údajů těmito bankami při plnění jejich funkcí souvisejících s infrastrukturou veřejných klíčů ESCB.

Článek 13

Audit

Audit infrastruktury veřejných klíčů ESCB se provádí v souladu se zásadami a opatřeními obsaženými v pravidlech pro provádění auditu. Auditem nejsou dotčeny interní kontroly a pravidla pro provádění auditu, jež platí pro centrální banky Eurosystemu nebo jež tyto banky přijímají.

Článek 14

Finanční ujednání

Centrální banky Eurosystemu nesou náklady na vývoj a provoz infrastruktury veřejných klíčů ESCB, jež jsou dále podrobně uvedeny ve finančním krytí infrastruktury veřejných klíčů ESCB.

Článek 15

Úloha Výkonné rady

1. V souladu s článkem 17.3 rozhodnutí ECB/2004/2 ze dne 19. února 2004, kterým se přijímá jednací řád Evropské centrální banky (¹), Rada guvernérů přenáší své normotvorné pravomoci na Výkonnou radu za účelem přijetí opatření k provedení tohoto rozhodnutí, jež jsou nezbytná pro účinnost a bezpečnost infrastruktury veřejných klíčů ESCB, a za účelem přijímání změn, které se týkají technických aspektů infrastruktury veřejných klíčů ESCB a služeb infrastruktury veřejných klíčů ESCB stanovených v přílohách dohody mezi druhou a třetí úrovní řízení, po zohlednění stanoviska Výboru pro informační technologie, případně Řídícího výboru Eurosystemu pro informační technologie.
2. Výkonná rada bez zbytečného odkladu informuje Radu guvernérů o všech prováděcích opatřeních, která přijme v souladu s odstavcem 1, a řídí se všemi rozhodnutími, která Rada guvernérů v této věci přijme.

Ve Frankfurtu nad Mohanem dne 11. ledna 2013.

Prezident ECB
Mario DRAGHI

(¹) Úř. věst. L 80, 18.3.2004, s. 33.

PŘÍLOHA

Informace o certifikační autoritě infrastruktury veřejných klíčů ESCB včetně její totožnosti a technických komponent

Certifikační autorita infrastruktury veřejných klíčů ESCB je ve svém certifikátu určena jako vydavatel a její soukromý klíč se používá k podpisu certifikátů. Certifikační autorita infrastruktury veřejných klíčů ESCB odpovídá za:

- i) vydávání certifikátů soukromých a veřejných klíčů,
- ii) vydávání seznamů odvolaných certifikátů,
- iii) vytváření párů klíčů spojených s určitými certifikáty, např. těmi, u nichž je nutná obnova klíče,
- iv) zajištění celkové odpovědnosti za infrastrukturu veřejných klíčů ESCB a zajištění splnění všech nezbytných požadavků na provoz této infrastruktury.

Certifikační autorita infrastruktury veřejných klíčů ESCB zahrnuje všechny fyzické osoby, politiky, postupy a počítačové systémy, jimž bylo svěřeno, aby vydávaly elektronické certifikáty a aby je přidělovaly držitelům certifikátů.

Certifikační autorita infrastruktury veřejných klíčů ESCB zahrnuje dvě technické komponenty:

- **Kořenová certifikační autorita infrastruktury veřejných klíčů ESCB:** Tato certifikační autorita první úrovně jen vydává certifikáty pro sebe a jí podřízené certifikační autority. Je v provozu, jen když plní své úzce vymezené povinnosti. Její nejvýznamnější údaje jsou:

Distinguished name (Jednoznačné jméno)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Sériové číslo)	596F AC4C 218C 21BC 4E00 6B42 A164 46DD
Distinguished name of issuer (Jednoznačné jméno vydavatele)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Doba platnosti)	From 21-06-2011 11:58:26 to 21-06-2041 11:58:26
Message digest (SHA-1) (Otisk zprávy)	CEFE 6C32 E850 994A 09EA 1A77 0C60 3D90 ADC9 9192

- **Online certifikační autorita infrastruktury veřejných klíčů ESCB:** Tato certifikační autorita druhé úrovně je podřízena kořenové certifikační autoritě infrastruktury veřejných klíčů ESCB. Odpovídá za vydávání certifikátů infrastruktury veřejných klíčů ESCB uživatelům. Její nejvýznamnější údaje jsou:

Distinguished name (Jednoznačné jméno)	CN=ESCB-PKI ONLINE CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Serial number (Sériové číslo)	2C13 E18F FDB5 91CE 4E29 550B B5A3 F59C
Distinguished name of issuer (Jednoznačné jméno vydavatele)	CN=ESCB-PKI ROOT CA, O=EUROPEAN SYSTEM OF CENTRAL BANKS, C=EU
Validity period (Doba platnosti)	From 22-07-2011 12:46:35 to 22-07-2026 12:46:35
Message digest (SHA-1) (Otisk zprávy)	D316 026C D2CF 1A8C 4AA3 8C29 EE3D 591E 4286 AD08