

Aktuality z elektronické identifikace

Jaromír Talíř • jaromir.talir@nic.cz • 21. 06. 2017



CZ.PEPS
CZECH REPUBLIC PAN-EUROPEAN
PROXY SERVICES



Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy

Obsah

- Elektronický občanský průkaz
- Zákon o elektronické identifikaci
- Projekt CZ.PEPS a nařízení eIDAS v oblasti eID
- Datové schránky
- Akademická federace identit eduID
- Ostatní doménové registry



Elektronický občanský průkaz

- Zaveden v roce 2012
- Dlouhou dobu omezen jen na uložení podpisového certifikátu a klíče
- Novela zákona o občanských průkazech platná od 1.1.2016

(§ 3 odstavec 7) Do kontaktního elektronického čipu lze zapsat kryptografické klíče spolu s certifikátem sloužícím k autentizaci držitele občanského průkazu vůči informačním systémům, vydaným akreditovaným poskytovatelem certifikačních služeb, (dále jen „autentizační certifikát“) odpovídajícím těmto klíčům. K zápisu kryptografických klíčů a autentizačního certifikátu je oprávněn pouze držitel občanského průkazu.



Elektronický občanský průkaz

Activities CardManIDCze Wed 09:35 en

Soubor Zobrazit Certifikát Nápověda

Generic Smart Card Reader Inter...
208213389
EOP-CZE-208213389-d68...
Certifikát
Broadcom Corp 5880 [Contacte...]

Čipová karta

Číslo karty:	208213389
Počet pokusů zadání PINu akt./nast. [max. nast.]:	3/3[3]
Počet pokusů zadání PUKu akt./nast. [max. nast.]:	3/3[3]
Počet kontejnerů (použitých/celkem):	1/12
Počet RSA 2048b. klíčů (použitých/celkem):	1/12
Volný prostor:	29184 B
Celkový prostor:	32768 B

 Změna PINu  Změna PUKu  Import pk

MIDDLEWARE

Hotovo

Activities CardManIDCze Wed 09:35 en

Soubor Zobrazit Certifikát Nápověda

Generic Smart Card Reader Inter...
208213389
EOP-CZE-208213389-d68...
Certifikát
Broadcom Corp 5880 [Contacte...]

Kontejner - RSA klíč

Název:	EOP-CZE-208213389-d68147-84d0-5cb80b6
Délka:	2048b.
Typ:	AT_KEYEXCHANGE
Klíče:	Privátní i veřejný klíč

 Test klíč  Export do souboru  Smazání klíče

Certifikáty, vydané k danému klíči:

Sériové číslo:	222E11
Platnost:	16.02.2017 - 08.03.2018
Vydal:	PostSignum Qualified CA 2, Česká pošta, s.p. [IČ 47114983], CZ
Pro:	Jaromír Talíř, CZ.NIC, z.s.p.o. [IČ 67985726], 14, Talíř, Jaromír, CZ



Activities CardManIDCze Wed 09:35 en

Soubor Zobrazit Certifikát Nápověda

Generic Smart Card Reader Inter...
208213389
EOP-CZE-208213389-d68...
Certifikát
Broadcom Corp 5880 [Contacte...]

Certifikát

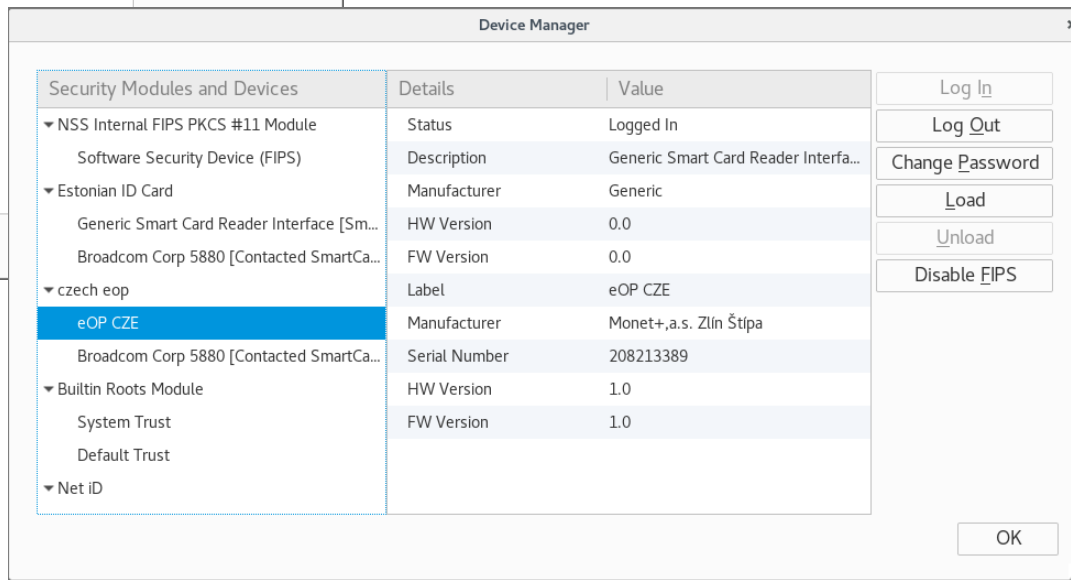
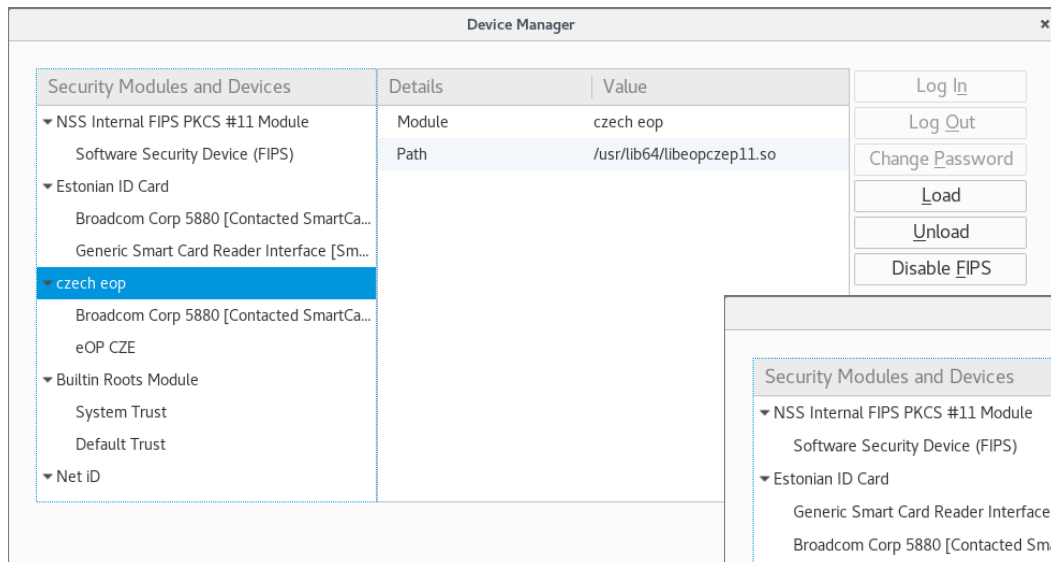
Sériové číslo:	222E11
Platnost:	16.02.2017 - 08.03.2018
Vydavatel:	PostSignum Qualified CA 2, Česká pošta, s.p. [IČ 47114983], CZ
Subjekt:	Jaromír Talíř, CZ.NIC, z.s.p.o. [IČ 67985726], 14, Talíř, Jaromír, CZ
Verze:	V3 (v02)
SHA1:	005F957BC32B561FDB20D11D8DBF83CD809B9725

 Více informací  Export do souboru  Smazání certifikátu

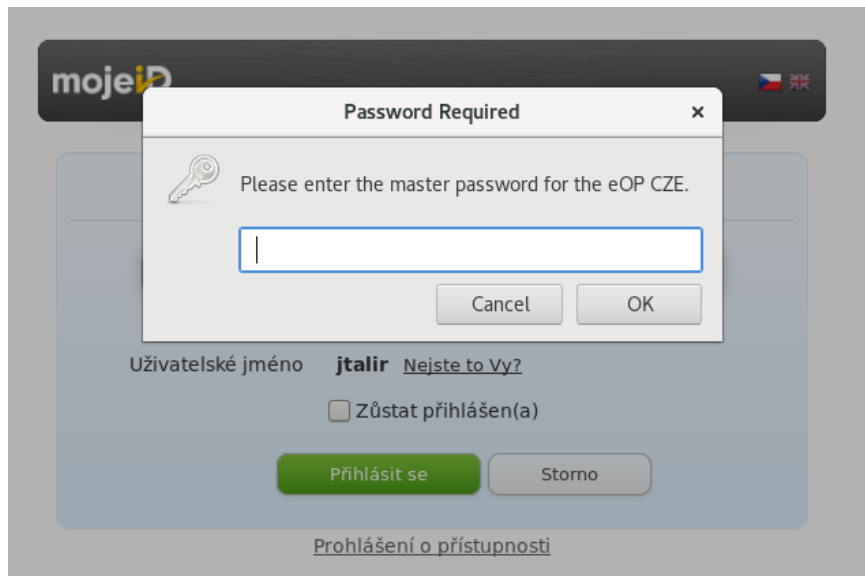
MIDDLEWARE

Hotovo

Elektronický občanský průkaz



Elektronický občanský průkaz



The screenshot shows the 'mojeID' login interface. A modal dialog titled 'Password Required' is open, asking for the master password for the eOP CZE. The background login form shows the username 'jtalir' and a checkbox for 'Zůstat přihlášen(a)'. There are buttons for 'Přihlásit se' and 'Storno', and a link for 'Prohlášení o přístupnosti'.

Password Required

Please enter the master password for the eOP CZE.

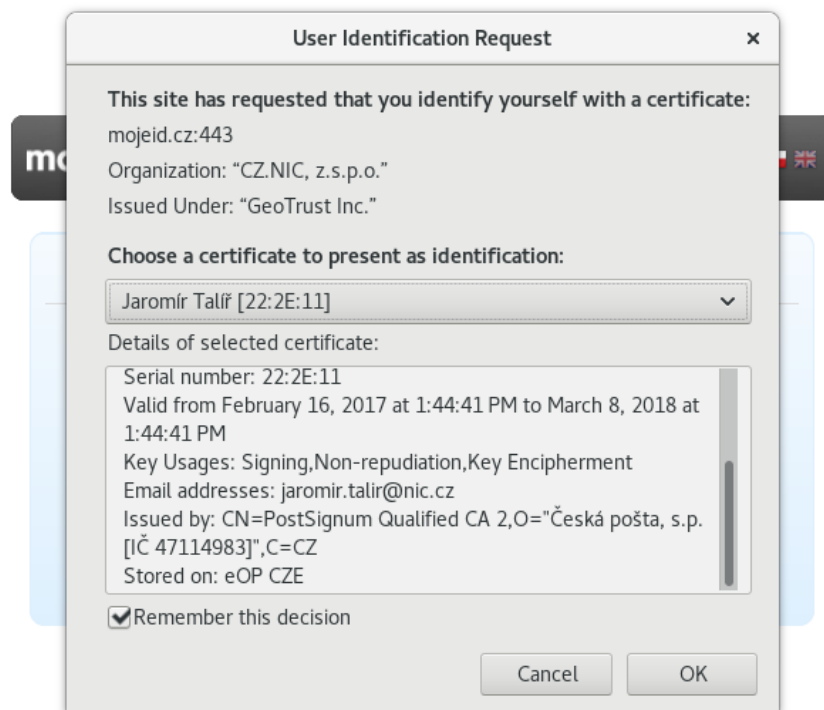
Cancel OK

Uživatelské jméno **jtalir** [Nejste to Vy?](#)

☐ Zůstat přihlášen(a)

Přihlásit se **Storno**

[Prohlášení o přístupnosti](#)



The screenshot shows a 'User Identification Request' dialog box. It informs the user that the site (mojeid.cz:443) has requested identification with a certificate. It lists the organization as 'CZ.NIC, z.s.p.o.' and the issuer as 'GeoTrust Inc.'. A dropdown menu shows the selected certificate 'Jaromír Talíř [22:2E:11]'. Below, the details of the selected certificate are listed, including the serial number, validity period, key usages, email addresses, and issuer information. A checkbox for 'Remember this decision' is checked. There are 'Cancel' and 'OK' buttons at the bottom.

User Identification Request

This site has requested that you identify yourself with a certificate:
mojeid.cz:443
Organization: "CZ.NIC, z.s.p.o."
Issued Under: "GeoTrust Inc."

Choose a certificate to present as identification:

Jaromír Talíř [22:2E:11]

Details of selected certificate:

Serial number: 22:2E:11
Valid from February 16, 2017 at 1:44:41 PM to March 8, 2018 at 1:44:41 PM
Key Usages: Signing, Non-repudiation, Key Encipherment
Email addresses: jaromir.talir@nic.cz
Issued by: CN=PostSignum Qualified CA 2, O="Česká pošta, s.p. [IČ 47114983]", C=CZ
Stored on: eOP CZE

☒ Remember this decision

Cancel OK



Elektronický občanský průkaz

- Aktuální novela - sněmovní tisk 928
 - Včera podepsaná prezidentem
 - Účinnost 12 měsíců po uvedení ve sbírce zákonů
- Změny (1/2)
 - Nový čip – certifikované QSCD pro možnost uložení kvalifikovaného certifikátu podle eIDAS
 - Kvalifikovaný certifikát tam v první fázi nebude, možnost uložit si vlastní podpisový certifikát zůstává



Elektronický občanský průkaz

- Změny (2/2)
 - Od „výrobce“ tam bude autentizační certifikát s platností podle délky platnosti průkazu
 - Možnost obnovit PUK
 - Bude postupně vydáván bezplatně všem podle expirace platnosti aktuálního průkazu
 - Držitelé průkazu s čipem by měli mít možnost vyměnit ho i dříve



Zákon o elektronické identifikaci

- Schválen Poslaneckou sněmovnou 9.6.2017, do 30 dnů by měl projít Senátem
 - Účinnost od 1.8.2018
- Klíčovou komponentou je Národní bod Identifikace a Autorizace (NIA) - propojuje poskytovatele služeb a poskytovatele identit
- Jeho součástí je uzel pro přeshraniční autentizaci (eIDAS Node) - testuje se ve spolupráci s CZ.NIC v rámci projektu CZ.PEPS

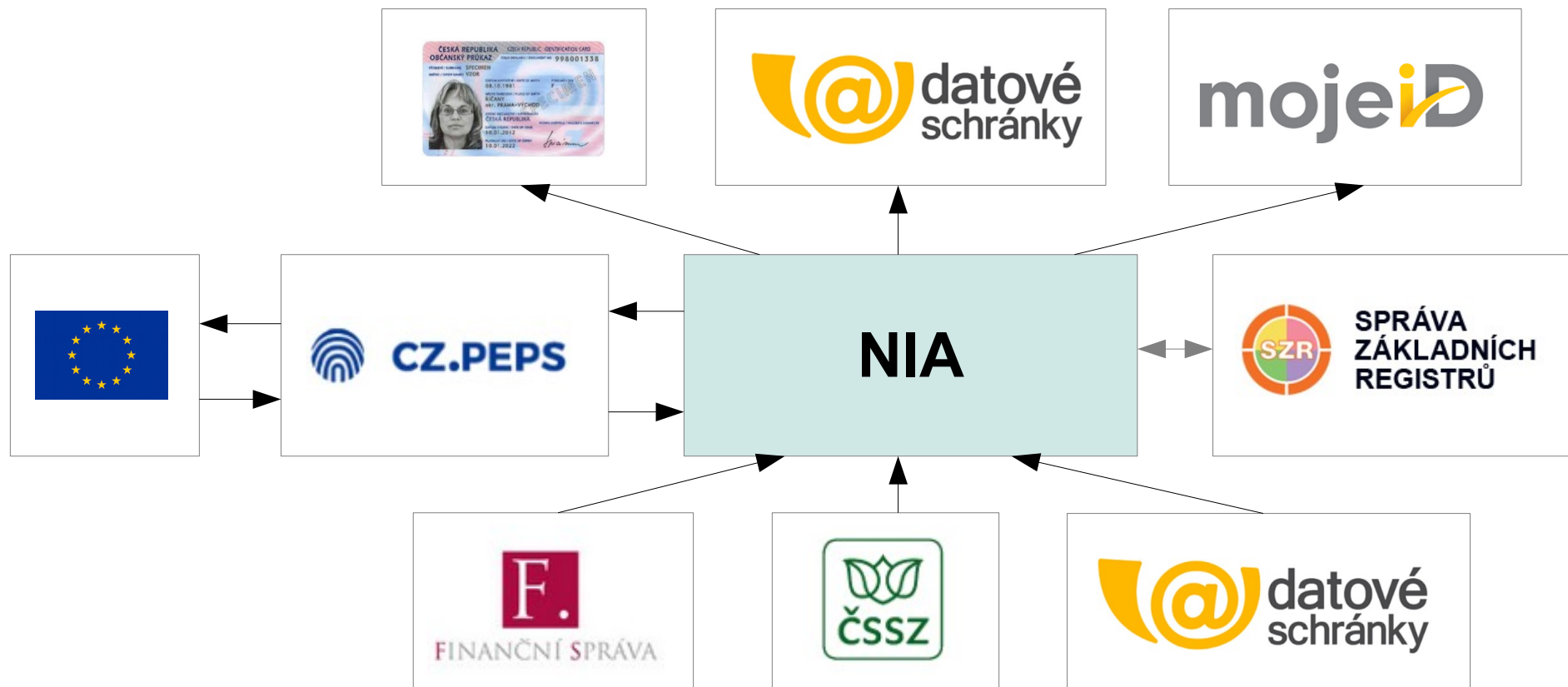


Zákon o elektronické identifikaci

- Technická implementace již nějakou dobu probíhá ve spolupráci MVCR, SZR a NAKIT
 - Usnesením vlády 833/2016 z 21.9.2016 o zřízení testovacího prostředí pro NIA a eOP
 - Probíhá testování s vybranými poskytovateli služeb
 - Probíhá testování napojení na CZ.PEPS
 - Postup pro zapojení na <https://www.eidentita.cz/>



Zákon o elektronické identifikaci



Zákon o elektronické identifikaci

- Kdo bude na straně poskytovatelů služeb?

§ 2 Vyžaduje-li právní předpis nebo výkon působnosti prokázání totožnosti, lze umožnit prokázání totožnosti s využitím elektronické identifikace pouze prostřednictvím kvalifikovaného systému elektronické identifikace (dále jen „kvalifikovaný systém“).



Nařízení eIDAS v oblasti eID

- členský stát má **povinnost** uznávat oznámené prostředky elektronické identifikace ostatních členských států pro **veřejné služby**, které v tomto státě vyžadují prostředek identifikace s úrovní záruky **značnou nebo vysokou**
 - Účinnost od 29.9.2018
- První členský stát, který inicioval proces oznámení, bylo 20.2.2017 Německo



Datové schránky

- Spuštění projektu mojeID datovka pozastaveno
 - Aplikační rozhraní ISDS neumožňuje implementovat plnohodnotnou kopii existujícího webového rozhraní (např. konfigurace uživatelů)
 - Webové rozhraní ISDS bude napojené na NIA takže přihlašování přes mojeID bude možné automaticky



Datové schránky

- Validace přes datovou schránku
 - Online metoda pro fyzické osoby vyžadující pouze přihlašovací údaje ISDS u schránky kterou tato osoba vlastní
 - Prvotní analýza validace uvažovala o využití Autentizační služby => nutnost registrace mojeID jako informačního systému veřejné správy
 - Připravovaná implementace využívá Odesílací bránu a speciální vlastnost OVM datových schránek umožňující zjištění informací o odesílateli datové zprávy



Akademická federace eduID

- Brána eduID-mojeID - 2015
 - Rozhraní, které překládalo SAML 2.0 do OpenID 2.0
 - Poskytovatel služby u mojeID byla brána => problematické řešení rozšířeného přístupu
 - Poskytovatelé si museli explicitně v konfiguraci bránu nastavit
- Implementace eduID požadavků v mojeID - 2016
 - Možnost přímého napojení na mojeID přes SAML
 - Poskytovatelé si stále museli mojeID nastavit



Akademická federace eduID

- Plné členství mojeID v eduID od **19.6.2017**
 - U zhruba 224 entit zapojených do eduID v roli poskytovatele služeb se mojeID objeví v nabídce poskytovatelů identit automaticky
 - Přímé připojení umožňuje uzavřít smlouvu o rozšířeném přístupu
 - Řešíme možnost zjednodušeného zavedení rozšířeného přístupu alespoň pro vybrané akademické poskytovatele služeb



Ostatní doménové registry

- Dánská doména .DK
 - Zavádění povinného ověření údajů držitele domény prostřednictvím dánského systému identifikace NemID
- Holanská doména .NL
 - Správce domény SIDN se propojil s poskytovatelem autentizačních služeb Connectis se záměrem získat know-how v této oblasti
 - Zatím nezveřejnili konkrétní projekty, které by těžili z tohoto spojení



Ostatní doménové registry

- Německá doména .DE
 - Připravují projekt nazvaný DomainID
 - Identifikátor identity je doména
 - Registr jen jako autentizační služba (OpenID Connect) pro tuto doménu/identitu
 - Osobní údaje by měl předat registrátor



Děkuji za pozornost

Jaromír Talíř • jaromir.talir@nic.cz



CZ.PEPS
CZECH REPUBLIC PAN-EUROPEAN
PROXY SERVICES



Spolufinancováno Evropskou unií
Nástroj pro propojení Evropy