

Using certificates in Mozilla Thunderbird

Contents

| Con | tents | 1 |
|-----|---|---|
| 1. | Import certificate in PFX format | 2 |
| 2. | Introduction of support for certificates stored on the smart card with the I.CA SecureStore application | 4 |
| 3. | Setting trust for root certificates | 7 |
| 4. | Assign a certificate to a user account | 9 |
| 5. | Signing an e-mail message1 | 1 |





1. Import certificate in PFX format

To import a certificate, you will first need to have a backup of the certificate in PFX format. You can make a backup by following the instructions found here: <u>I.CA | Záloha certifikátu (ica.cz)</u>. Open Mozilla Thunderbird. Click on the gear icon in the bottom left corner.

| | E5 | 🐼 Account Setup X 🕸 Settings X | - 0 | × |
|---|---|--|------------------|---|
| A | 🔀 Get Messages 🗸 🖉 Write | Tag 🗸 ili QuickFilter 🖉 Search <ctrl+k></ctrl+k> | | ≡ |
| | Folders | | Account Settings | 5 |
| Q | ➢ INDOX ➢ Místní složky im Deleted im Outbox | 🗟 Read messages 🖉 Write a new message 🔍 Search messages 👬 Manage message filters 🧬 End-to-end Encryption | | |
| | | Choose What to Set Up | | |
| | | 🖻 Email 🛅 Calendar 🙆 Address Book 🤤 Chat 🧬 Filelink 🥻 Feeds 🔮 Newsgroups | | |
| | | Import from Another Program | | |
| | | Thunderbird lets you import mail messages, address book entries, feed subscriptions, settings, and/or filters from other mail programs and common address book formats. | | |
| | | (i) Import | | |
| | | About Mozilla Thunderbird | | |
| | | Thunderbird is the leading open source, cross-platform email and calendaring client, free for business and personal use. We want it to stay secure and become even better. A donation will allow us to hire developers, pay for infrastructure, and continue to improve. | | |
| | | Resources | | V |
| | | Participation and the second s | | |
| ٩ | | | | |
| ⊬ | ((*)) | | | |

Here, go to "Privacy and Security", scroll down and click on "Manage Certificates".

| | ₽ <u>₽</u> | 🕼 Account Setup X 🚯 Settings X | - 0 | × |
|----|--------------------|--|-----|---|
| Ø | | ₽ Find in Settings | | |
| | | | | |
| | र्छि General | Allow Thunderbird to send technical and interaction data to Mozilla Learn more | | |
| Q | Composition | Allow Thunderbird to send backlogged crash reports on your behalf Learn more | | |
| | | | | |
| 1. | Privacy & Security | Security | | |
| | 💭 Chat | | | |
| | | Scam Detection Thunderbird can analyse messages for suspected email scams by looking for common techniques used to deceive you. | | |
| | | ☑ Tell me if the message I'm reading is a suspected email scam | | |
| | | | | |
| | | Antivirus | | |
| | | Thunderbird can make it easy for anti-virus software to analyse incoming mail messages for viruses before they are stored locally. | | |
| | | Allow anti-virus clients to quarantine individual incoming messages | | |
| | | | | |
| | | Certificates | | |
| | | When a server requests my personal certificate: | | |
| | | Select one automatically O Ask me every time | | |
| | | Query OCSP responder servers to confirm the current validity of certificates 2. Manage Certificates | | |
| | Account Settings | Security Devices | | |
| | Add-ons and Themes | | | |
| Ŵ | | | | |
| ⊬ | ((*)) | | | |
| | | | | |
| | | _ | | |



A window will open where you click on the "Your Certificates" tab at the top and select "Import"

| 1. | Certificat | te Manager | | | |
|----------------------------|---------------------------|-----------------|----------------|----------------|-----|
| Your Certificates | Authentication Decisio | ons People | e Server | rs Authorities | |
| You have certificates fro | m these organisations tha | t identify you | | | |
| Certificate Name | Security Device | Serial Nur | nber | Expires On | E\$ |
| | | | | | |
| | | | | | |
| | | 2 | | | |
| | | 2. | | | |
| <u>V</u> iew <u>B</u> acku | ip Bac <u>k</u> up All | I <u>m</u> port | <u>D</u> elete | | |
| | | | | Ok | C |
| | | | | | |

In the following window, set the path for backing up the certificate in PFX format and confirm your selection.

| Certificate File to Import | | | | | | | | × |
|---|------------|------------------|--------------------|--------|-----|----------------------|--------|---|
| \leftrightarrow \rightarrow \checkmark \uparrow | > Desktop | | | | ~ C | Search Desktop | | Q |
| Organise 👻 New folder | | | | | | ≣ | • | • |
| A Home | Name | Date modified | Туре | Size | | | | |
| > 📥 OneDrive - Persona | 🍺 Backup | 18/04/2023 13:02 | Personal Informati | і З КВ | | | | |
| E Desktop ★ ↓ Downloads ★ E Documents ★ N Pictures ★ | | | | | | | | |
| Music M | | | | | | | | |
| File <u>n</u> an | ne: Backup | | | | ~ | PKCS12 Files Open | Cancel | ~ |
| | | | | | | | | |



After selecting the file, you need to fill in the certificate backup password that was set when the backup was created.

| | | Certific | ate Manager | | | | | |
|--------------------------|----------------|---------------------|-----------------|----------------|--------------|-------|----------|----|
| Your Certificate | s Aut | hentication Decisi | ions Pe | ople | Servers | Au | thoritie | S |
| ou ha Password Re | quired - Moz | illa Thunderbird | | | | × | | |
| Certi | | | | | | | n | E. |
| Ŷ | Please enter t | the password that w | as used to en | crypt this cer | tificate bao | :kup: | | |
| | •••• | | | | | | | |
| | | | | Sign in | Cance | : | | |
| Manu |) a aluum | De deux All | lunn out | Dalata | | | | |
| <u>v</u> iew <u>E</u> | аскир | Bac <u>k</u> up All | I <u>m</u> port | Delete | | | | |
| | | | | | | | C | K |

2. Introduction of support for certificates stored on the smart card with the I.CA SecureStore application

Open Mozilla Thunderbird. Click the gear icon in the bottom left corner.

| ⊠ | Eb | 🛱 Account Setup X 🕸 Settings X | - 0 |
|----|--|---|------------------|
| A | 🖾 Get Messages 🗸 🖌 Write | | |
| | Folders | | Account Settings |
| 2 | ✓ Mistni složky iiii Deleted iiii Outbox | B Read messages P Write a new message Q. Search messages iii Manage message filters P End-to-end Encryption | |
| | | Choose What to Set Up | |
| | | 😆 Email 🛅 Calendar 🖪 Address Book 🤤 Chat 🔗 Filelink 🦣 Feeds 创 Newsgroups | |
| | | Thunderbird is the leading open source, cross-platform email and calendaring client, free for business and personal use. We want it to stay secure and become even better. A donation will allow us to him developers, pay for infrastructure, and continue to improve. | |
| \$ | | Resources | |
| ÷ | ((o)) | | |
| | | | |



| × | 88 | Account Setup X 🕲 Settings X | ð X |
|----|--|--|-----|
| 8 | | | |
| 2 | द्धिः General | Allow Thunderbird to send technical and interaction data to Mozilla Learn more Allow Thunderbird to send backlogged crash reports on your behalf Learn more | |
| 1. | Privacy & Security Chat | Security Scan Detection Thunderbird can analyse messages for suspected email scams by looking for common techniques used to deceive you. Image: Tell me if the message I'm reading is a suspected email scam | |
| | | Antivirus Thunderbird can make it easy for anti-virus software to analyse incoming mail messages for viruses before they are stored locally. Allow anti-virus clients to quarantine individual incoming messages | |
| | | Certificates When a server requests my personal certificate: Select one automatically O Ask me every time | |
| ø | Account Settings Add-ons and Themes | Query OCSP responder servers to confirm the current validity of certificates Manage Certificates | |
| ← | (rai) | | |

Here, go to "Privacy & Security", scroll down and click on "Security Devices".

A new window will open, in which you click on "**Load**" on the right. In the new window you can choose the name of the module and then choose "**Browse**".

| Details | Value | Log I <u>n</u> |
|------------------------------------|---|---|
| | | Log <u>O</u> ut |
| | | Change Password |
| Enter the information for the mode | × | 1. Load |
| Module Name New PKCS#11 Mod | <u>U</u> nload | |
| Module <u>f</u> ilename | Browse | Enable <u>E</u> IPS |
| | OK Cancel | |
| | | |
| | | |
| | | |
| | Load PKCS#11 Device Driver Enter the information for the modu Module Name New PKCS#11 Mo Module filename | Control of the module you want to add. Module Name New PKCS#11 Module 2. Module filename OK Cancel |



L

You will need to set the path to the PKCS11 library in the computer's storage. The path to the library is as follows: C:\Windows\System32\SecureStorePkcs11.dll

| \leftarrow \rightarrow \checkmark \uparrow | ; | \rightarrow This PC \rightarrow Windows (C:) \rightarrow Windows \rightarrow | System32 | | | ~ C | Search System32 | | P |
|--|----------|--|------------------|-------------------|----------|-----|-------------------------------|--------|----|
| Organise 🔻 🛛 Ne | w folder | | | | | | 1 | ≣ ▼ 🔲 | () |
| A Home | 1 | Name | Date modified | Туре | Size | | | | |
| > 📥 OneDrive - P | ersona | SECOCL64 | 10/11/2022 23:07 | Application | 1,391 KB | | | | |
| | _ | SECOMN64.dll | 10/11/2022 23:07 | Application exten | 8,751 KB | | | | |
| E Desktop | * | SECOMN64 | 10/11/2022 23:07 | Application | 748 KB | | | | |
| L Downloads | | 🚡 secpol | 07/05/2022 12:14 | Microsoft Comm | 118 KB | | | | |
| | | 🚳 secproc.dll | 20/03/2023 14:21 | Application exten | 420 KB | | | | |
| Disture | | 🚯 secproc_isv.dll | 20/03/2023 14:21 | Application exten | 420 KB | | | | |
| Pictures | | secproc_ssp.dll | 07/05/2022 07:19 | Application exten | 132 KB | | | | |
| Music | * | secproc_ssp_isv.dll | 07/05/2022 07:19 | Application exten | 132 KB | | | | |
| Videos | * | 🚳 secur32.dll | 07/05/2022 07:19 | Application exten | 48 KB | | | | |
| | | SecureAssessmentHandlers.dll | 07/05/2022 12:14 | Application exten | 208 KB | | | | |
| | | SecureBootEncodeUEFI | 20/03/2023 14:22 | Application | 56 KB | | | | 1 |
| | | securekernel | 10/05/2023 03:41 | Application | 1,102 KB | | | | |
| | | 2. 📧 securekernella57 | 10/05/2023 03:42 | Application | 1,050 KB | | | | |
| | - 1 | SecureStorePkcs11.dll | 30/08/2022 15:14 | Application exten | 8,593 KB | | | | |
| 1. 🛆 OneDrive | | SecureTimeAggregator.dll | 07/05/2022 07:19 | Application exten | 104 KB | | | | |
| > 💻 This PC | | 🚳 security.dll | 07/05/2022 07:19 | Application exten | 12 KB | | | | |
| | File nam | ne: SecureStorePkcs11.dll | | | | | All Files | | ~ |
| | | | | | | | 3 Open | Cancel | |

After setting the path to the library, confirm the following window.

Device Manager

| Security Modules and Devices | Details | Value | Log I <u>n</u> |
|---|--------------------------------------|------------------|---------------------|
| ✓ NSS Internal PKCS #11 Module Generic Crypto Services | | | Log <u>O</u> ut |
| Software Security Device | Cal Load PKCS#11 Device Driver | – – × | Change Password |
| ✓ Builtin Roots Module NSS Builtin Objects | Enter the information for the module | you want to add. | Load |
| | Module Name New PKCS#11 Modul | e | <u>U</u> nload |
| | Module filename C:\Windows\System | M32\Sr Browse | Enable <u>F</u> IPS |

První certifikační autorita, a.s., se sídlem Podvinný mlýn 2178/6, 190 00 Praha 9 - Libeň, zapsaná dne 12. 3. 2001v Obchodním rejstříku, vedeném u Městského soudu v Praze, spisová značka: oddíl B, vložka 7136. IČ: 26 43 93 95, DIČ: CZ26439395. Tel.: +420 284 081 940, e-mail: info@ica.cz, www.ica.cz

//.

AUTHORITY

On the left side of the window, you will see the module you have set up, where you will see the name of the reader you clicked on, and on the top right you will click "**Log In**". In the password window, enter the PIN for the card and confirm the login.

Device Manager

| Security Modules and Devices | Details | Value | 2. | Log I <u>n</u> |
|--------------------------------------|------------------------|--|--------------|---------------------|
| \sim NSS Internal PKCS #11 Module | Status | Not Logged In | | Log Out |
| Generic Crypto Services | Password Required - Mo | ozilla Thunderbird | \times | Log Out |
| Software Security Device | | | | Change Password |
| ✓ New PKCS#11 Module | Please enter | r the password for the PKCS#11 token 92030 | 90300001124. | Load |
| L INGENICO iHC Smart Card Terminal 0 | 3 | | | Unload |
| INGENICO IHC Smart Card Terminal 1 | | 4 Sign in | Cancel | Onload |
| | | | cuncer | Enable <u>F</u> IPS |
| NSS Builtin Objects | Serial Number | 9203090300001124 | | |
| | HW Version | 3.7 | | |
| | FW Version | 1.7 | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | ОК |

3. Setting trust for root certificates

Click on the gear icon in the bottom left corner.

🖂 🛯 📴 Account Setup × 🕸 Se 🕅 Get M R A Write Tag > ili Ouick Filter Search <Ctrl+K> Folders Aci ~ 🖂 2 🔁 In Q 🗸 🛅 Místní sle Deleted Outbox Read messages Q. Search messages ili Manage message filters End-to-end Encrypti Choose What to Set Up 🔟 Calendar 🤤 Chat Feeds Address Book 🔗 Filelink Mewsgroups 🖂 Email Import from Another Program Thunderbird lets you import mail messages, address book entri filters from other mail programs and common address book fo Import About Mozilla Thunderbird ind caleri... **er. A do derbird is the leading open source, cross-platform ema personal use. We want it to stay secure and become ew lopers, pay for infrastructure, and continue to improve. Resources Explore Features ② Support Get Involved S Developer Docu 鐐



| nere, g | |
|---------------|---|
| | al Allow Thunderbird to send technical and interaction data to Mozilla Learn more Allow Thunderbird to send backlogged crash reports on your behalf Learn more osition |
| 1. 🖻 M Q o | y & Security Security Scan Detection Thunderbird can analyse messages for suspected email scams by looking for common techniques used to deceive you. Image: The state of the message is a suspected email scame in the state of the |
| | Antivirus Thunderbird can make it easy for anti-virus software to analyse incoming mail messages for viruses before they are stored locally. Allow anti-virus clients to quarantine individual incoming messages |
| | Certificates When a server requests my personal certificate: Select one automatically Ask me every time Image Certificates Image Certificates |
| () Act | t Settings Security Devices |
| Ad | s and Themes |
| 23 | |

In the following window, go to the **"Authorities**" tab and find the root certificates from the First CA in the list. The list should be sorted alphabetically. Highlight the certificate in the image below and select "**Edit Trust**". In the new window, check all the trust setting options and confirm. **Repeat the process for the other root certificates.**

| 1 | | | | Certifi | cate Manager | | L. |
|---------|----------------------|------------------------|--------------------|--------------------|-------------------|----------------------------|-------------|
| | Edit CA certificate | trust settings | | | | × | |
| rd ca | The certificate "I | .CA EU Qualified (| CA2/RSA 06/2022 | " represents a Cer | tificate Authorit | у. | Authorities |
| e if tł | 4 Edit trust setting | S: | | | | | |
| | This certificat | te can identify web | o sites. | | | | Ę |
| | This certificat | te can identify mai | il users. | | | _ | |
| | | | | 5. | ОК | Cancel | |
| rd ca | 2. | I.CA EU C | Qualified CA2/RS | SA 06/2022 | 920309030 | 0001124 | |
| anti-v | virus clients to | I CA Test | EU Oualified CA | 2/RSA 04/2022 | 920309030 | 0001124 | |
| | | <u>∨</u> iew 3. | <u>E</u> dit Trust | I <u>m</u> port | E <u>x</u> port | <u>D</u> elete or Distrust | |
| es | | | | | | | ОК |
| rver | reauests mv pe. | | | | | | 14. |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | _ _ |



4. Assign a certificate to a user account

In the open application, click the gear icon in the bottom left corner.

| \boxtimes | 26 | Lege Account Setup X Lege Settings X | - D X |
|-------------|---|--|------------------|
| R | 🔀 Get Messages 🗸 🖉 Write | ⑦ Tag ∨ Hi Quick Filter Ø Search <ctrl+k></ctrl+k> | = |
| | Folders | | Account Settings |
| Q | Inbox Mistní složky Deleted Outbox | 🗟 Read messages 🥒 Write a new message 🔍 Search messages 👬 Manage message filters 🎤 End-to-end Encryption | |
| | | Choose What to Set Up | |
| | | 🖾 Email 💼 Calendar 🖲 Address Book 🤤 Chat 🔗 Filelink 🦣 Feeds 🍘 Newsgroups | |
| | | Import from Another Program Thunderbird lets you import mail messages, address book entries, feed subscriptions, settings, and/or filters from other mail programs and common address book formats. Import Import | |
| | | About Mozilla Thunderbird Thunderbird is the leading open source, cross-platform email and calendaring client, free for business and personal use. We want it to stay secure and become even better. A donation will allow us to hire donation. The best way for you to ensure Thunderbird remains available is to make a donation. | |
| | | everopers, pay for intrastructure, and continue to improve. Resources | |
| \$ | | Explore Features | |
| ⊬ | ((0)) | | P 1 |

Select "Account Settings" at the bottom left.

| | 🛃 obrusnik@ica.cz | 🗟 Account Setup X 🔞 Settings X 🕲 Account Settings X | | 6 > | ¢. | |
|---|--|---|--|-----|----|--|
| | 양강 General | Find in Settings Allow Thunderbird to send technical and interaction data to Mozilla Learn more Allow Thunderbird to send backlogged crash reports on your behalf Learn more | | | | |
| | Privacy & Security Chat Account Settings Add-ons and Themes | Security Commentation Tunderbind can analyse messages for suspected email scans by looking for common techniques used to deceive you. I ell me if the message fur reading is a suspected email scans Attivins Tunderbind can make it easy for anti-vinus software to analyse incoming mail messages for vinuses before they are stored locally. I obser anti-vinus clients to quarantine individual incoming messages Certificate Wene aver requests my personal certificate: I eled one automatically As kine every time I gluery OCSP responder servers to confirm the current validity of certificates | | | | |
| * | ((*)) | | | | | |



In the account settings on the left, select "End-to-end encryption". In the "Personal certificate for electronic signature" box, click "Select". A new window will open for you to select a certificate. In the top row you can switch certificates and in the details you can check if you are selecting the correct certificate. Once you have selected a certificate, confirm your selection. Always select a qualified certificate for signing.

| A | | |
|---|---|---|
| | × 🖻 | End-To-End Encryption |
| 9 | Server Settings Copies & Folders Composition & Addressing Junk Settings Synchronisation & Storage | To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME. Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key. Learn more OpenPGP |
| | Return Receipts | Thunderbird doesn't have a personal OpenPGP key for |
| | Mistní složky Junk Settings Disk Space Outgoing Server (SMTP) | Use the Op Select Certificate 2. all other keys not listed above. OpenPGI Certificate DB:TwinsQD 10/03/2023 12:15:30 (00:89:07: V |
| | | S/MIME Issued to: senialNumber=ICA SN= givenName: C=CZserialNumber=IDCCZ- Personal ce 206116268,CN= 00890704 Valid form pätek 10, března 2023 to sobota 9, března 2024 Personal ce Issued by: C=CZ,OID.2.5.4.97=NTRCZ-26433939,O="Pvni certifikačni autorita, a.st:/CN=ICA EQualified CA2/RSA 06/2022 Stored in: Solved ca2/RSA 06/2022 Select |
| | | Manage 3. OK Cancel |
| | | |
| | Account Actions ∨ | Default settings for sending messages Without and to and approximation the contents of messages are easily expected to your amail provider and to mass supplications |
| | | Disable encryption for new messages |
| | to Thunderbird Settings | Enable encryption for new messages |
| _ | Add-ons and Themes | You will be able to disable encryption for individual messages. |
| 1 | | A digital signature allows recipients to verify that the message was sent by you and its content was not changed. Encrypted |
| 1 | ((a)) | |

After confirming the certificate selection, you will be presented with a menu to set the encryption certificate. If you will not encrypt, you can decline the offer. Alternatively, the encryption certificate can always be set. Acommercial certificate is set for encryption. Then check the option "**Sign unencrypted messages**" below.

| R | To send encrypted or digitally signed messages, you need to configure an encryption technology, either OpenPGP or S/MIME. | | | |
|---|---|---|--|--|
| | × B | Select your personal key to enable the use of OpenPGP, or your personal certificate to enable the use of S/MIME. For a personal key or certificate you own the corresponding secret key. Learn more | | |
| 2 | Server Settings Copies & Folders | OpenPGP | | |
| Q | Composition & Addressing Junk Settings Synchronisation & Storage | Thunderbird doesn't have a personal OpenPGP key for | | |
| | End-To-End Encryption | Use the OpenPGP Key Manager to view and manage public keys of your correspondents and all other keys not listed above. | | |
| | Return Receipts Místní složky Junk Settings | OpenPGP Key Manager | | |
| | Disk Space | S/MIME | | |
| | Outgoing Server (SMTP) | Personal certificate for digit Thunderbird × | | |
| | | IO0:B9:07:0- Image: Construction of the second | | |
| | | Xes No | | |
| | | Manage S/MIME Certificates S/MIME Security Devices | | |
| | | Default settings for sending messages | | |
| | | Without end-to-end encryption the contents of messages are easily exposed to your email provider and to mass surveillance. | | |
| | | Disable encryption for new messages | | |
| | Account Actions V | Epable encryption for new messages | | |
| | | You will be able to disable encryption for individual messages. | | |
| | 🕄 Thunderbird Settings | A digital signature allows recipients to verify that the message was sent by you and its content was not changed. Encrypted | | |
| | Add-ons and Themes | messages are always signed by default. | | |
| ¢ | ER. Has one and memory | 2. Sign unercrypted messages | | |
| ⊬ | ((*)) | | | |
| | | | | |



5. Signing an e-mail message

If you don't have a "**Sign**" button in your new message, you can add one by customizing the toolbars. When you right-click on a toolbar, a menu will appear where you select "**Customize...**".



You will see the toolbar edit where the sign button is. Click and move the mouse to select where you want to place the "**Sign**" button on the toolbar. Then confirm with the "**Done**" button.





Now you can sign email messages. To sign a message, click on "**Sign**" in the message. The message will be signed when it is sent.





soudu v Praze, spisová značka: oddíl B, vložka 7136. IČ: 26 43 93 95, DIČ: CZ26439395. Tel.: +420 284 081 940, e-mail: info@ica.cz, www.ica.cz