# **Mozilla Thunderbird Edition**

| Revisi | Revision History  |   |        |  |  |  |
|--------|-------------------|---|--------|--|--|--|
| Rev.   | Date (YYYY/MM/DD) | Description   | Editor |  |  |  |
| V.1.0  | 2015/4/1          | First revision  | NII    |  |  |  |
| V.1.1  | 2016/12/26        | Amendment with addition of [NII Open Domain S/MIME CA] as a new Certificate Authority | NII    |  |  |  |
| V2.0   | 2018/2/26         | Supported environment update: Mozilla Thunderbird 52.0 or later                       | NII    |  |  |  |

#### Table of Content

- 1. Installing the S/MIME Certificate
- 1-1. Operating Environment
- 1-2. Prerequisites
- 1-3. Install Procedure
- 2. Sending Digitally Signed E-mails
- 2-1. Sending Digitally Signed E-mails 2-2. How to Confirm a Sent E-mail That Was Digitally Signed

## 1. Installing the S/MIME Certificate

### 1-1. Operating Environment

The procedures only in the following environment are described in this document:

# Supported environment:

Mozilla Thunderbird 52.0 or later

### 1-2. Prerequisites

The prerequisites for using the S/MIME Certificate in Mozilla Thunderbird are described. Replace the technical terms according to the user environment in which the S/MIME Certificate will be used. (The procedures required for Mozilla Thunderbird 52.0 are described in this document.)

#### Prerequisites

- 1. The S/MIME Certificate has been installed in the web browser
- (described in the User's Manuals for Installation in Different Web Browsers: Mozilla Firefox Edition); and
- 2. Mozilla Thunderbird 52.0 or later is installed.

### 1-3. Install Procedure

Installing the Certificate

1. Open Mozilla Thunderbird, right click on the [mailuser] (account name) and select [Settings (E)].

| 🖂 mailuser<br>📩 Get Messages | Account with d  | igital sigr<br>🗭 Chat | nature<br><b>1</b> Ad       | dress Book |
|------------------------------|---|-----------------------|-----------------------------|------------|
| ✓ <mark>&gt; mailuser</mark> | <u>G</u> et Messages<br>Open in New <u>I</u><br><u>O</u> pen in New V<br><u>S</u> earch Messag<br><u>N</u> ew Folder<br>S <u>e</u> ttings | ab<br>Vindow<br>es    | erb                         | oird Mai   |
|                              |   | Acc                   | Write a<br>ounts<br>View se | new messa  |

2. The [Account Settings] screen will appear. Select [Security] in the account profile, listed on the left. Click [Manage Certificates...(M)].



3. In the [Certificate Manager] pane, select [Your Certificates] tab and click [Import... (M)].

|                  | increasing and a state of the function of the |               |            |  |
|------------------|---|---------------|------------|--|
| Certificate Name | Security Device                               | Serial Number | Expires On |  |
|                  |   |               |            |  |
|                  |   |               |            |  |
|                  |   |               |            |  |
|                  |   |               |            |  |
|                  |   |               |            |  |
|                  |   |               |            |  |

4. As you can browse the certificate file(s) to import, select the certificate to import and click [Open (O)].

| rganize 👻 New f | older          |                   |                    |      | E== - |  |
|-----------------|----------------|-------------------|--------------------|------|-------|--|
|                 | Name           | Date modified     | Туре               | Size |       |  |
| Quick access    | 🍃 mailuser.p12 | 1/30/2018 6:35 PM | Personal Informati | 6 KB |       |  |
|                 |                |                   |                    |      |       |  |
|                 |                |                   |                    |      |       |  |
| Network         |                |                   |                    |      |       |  |
|                 |                |                   |                    |      |       |  |
|                 |                |                   |                    |      |       |  |
|                 |                |                   |                    |      |       |  |
|                 |                |                   |                    |      |       |  |
|                 |                |                   |                    |      |       |  |
|                 |                |                   |                    |      |       |  |
|                 |                |                   |                    |      |       |  |
|                 |                |                   |                    |      |       |  |

5. The [Password Entry Dialog] box will pop up. Enter the password for encrypting this certificate backup in the [Password:] box, and click [OK].

| Password | d Required  | ×   |
|----------|---|-----|
| ?        | Please enter the password that was used to encrypt this certificate back. | ib: |
|          | •••••   |     |
|          | OK Cancel   |     |

6. Click [OK] in the [Alert] dialog box.

| Alert    |   | × |
|----------|---|---|
| <u> </u> | The certificate and private key were successfully restored. |   |
|          | ОК  |   |

7. In the [Certificate Manager] pane, make sure that the certificate is now installed, and click [OK].

| A   |                          |                         |            | - |
|---|--------------------------|-------------------------|------------|---|
| Certificate Name  | Security Device          | Serial Number           | Expires On | e |
| <ul> <li>National Institute of Info<br/>mailuser</li> </ul> | Software Security Device | 0C:68:CB:B2:0B:53:0E:BF |            |   |
|   |                          |                         |            |   |
|   |                          |                         |            |   |
|   |                          |                         |            |   |
|   |                          |                         |            |   |
|   |                          |                         |            |   |
|   |                          |                         |            |   |

8. The [Account Settings] screen will appear. Select [Security] in the account profile, listed on the left. Click [Select...(S)].



9. In the [Select Certificate] dialog box, select the S/MIME Certificate from the [Certificate] drop down list, and click [OK].
Select Certificate

| sued to: CN-mailuser OU-                 |  |
|--|--|
| sueu to: crit=manuser, 00=               | O=National Institute of                            |
| nformatics,L=Academe,C=JP                |  |
| 0C:68:CB:B2:0B:53:0E:BF                  |  |
| Valid from to                            |  |
| Signing,Key Encipherment                 |  |
| Email:                                   |  |
| sued by: CN=NII Open Domain S/MIME CA, C | D=National Institute of Informatics,L=Academe,C=JP |
| tored in: Software Security Device       |  |
| tored in: Software Security Device       |  |

| 10. | Click [No | lo (N)].   |           |
|-----|-----------|--|-----------|
|     | Thunder   | rbird  | ×         |
|     | ?         | You should also specify a certificate for other people to use when they send you encrypted messages. Do you want to use the same certificate to encrypt & decrypt messages sent to g | l<br>you? |
|     |           | <u>Y</u> es <u>N</u> o   |           |

11. Check the [Digitally sign messages (by default) (D)] checkbox, and click [OK].

| ⊠ <u>mailuser</u>  | Security   |                    |
|--|--|--------------------|
| Server Settings<br>Copies & Folders<br>Composition & Addressing<br>Junk Settings | To send and receive signed or encrypted messages, you<br>digital signing certificate and an encryption certificate.<br>Digital Signing<br>Use this certificate to digitally sign messages you send | should specify bo  |
| Disk Space<br>Return Receints  | mailuser [00:68:08:82:08:53:0E:8F] <u>S</u> elect  | <u>C</u> lear      |
| Security   | Digitally sign messages (by default)   |                    |
| Junk Settings<br>Disk Space<br>Nutgoing Server (SMTP)                            | Encryption<br>Use this certificate to encrypt & decrypt messages sen<br>Select   | t to you:          |
|  | Default encryption setting when sending messages: <ul></ul>  | have certificates) |
|  | Certificates   |                    |
|  | Manage Certificates Security Devices   |                    |
|  |  |                    |
| Account Actions •  | ]  |                    |
| Account Actions +  | ]  |                    |

This completes the S/MIME Certificate installation.

## 2. Sending Digitally Signed E-mails

## 2-1. Sending Digitally Signed E-mails

How to Send Digitally Signed E-mails

1. Open Mozilla Thunderbird, and click the [Write] button.

| 🖂 mailuser  |                                       |
|---|---------------------------------------|
| 📩 Get Messages 🔻 📝 Write 🔻                          | 🗭 Chat 👤 Address Book 📗               |
| ✓⊠ mailuser<br>ا Inbox<br>Trash<br>✓ ■ Local folder | Thunderbird Mai                       |
| 🗑 Trash 🚵 Outbox                                    | Email Read messages Write a new messa |
|   | Accounts                              |

2. In the [Write: Foobar] screen, click the downward arrow on the right side of the [Security] button and select [Digitally Sign This Message (M)] from the drop down list.

| 🖳 Write: (no subject)                       |                                       | _ |       | $\times$ |
|---|---------------------------------------|---|-------|----------|
| <u>File Edit View Insert Format Options</u> | <u>T</u> ools <u>H</u> elp            |   |       |          |
| 💢 Send 📔 🗸 Spelling 🖛 🔘 Attach 🖛            | 🖴 Security 💌 🕂 Save 🔻                 |   |       |          |
| From: mailuser <                            | Encrypt This Message                  |   |       | ~        |
|   | ✓ Digitally Sign This <u>M</u> essage |   |       |          |
| 10:   | View Security Info                    |   |       |          |
|   |                                       |   |       |          |
|   |                                       |   |       |          |
| <u>S</u> ubject:                            |                                       |   |       |          |
| Paragraph \vee 🛛 Variable Width             | Y ■ A4 A A A A A                      |   | ≣ - ■ | • @ •    |
|   |                                       |   |       |          |
|   |                                       |   |       |          |
|   |                                       |   |       |          |
|   |                                       |   |       |          |
|   | ·····                                 |   |       | ×.       |

**3.** Write the message. When finished, click [Send].

| 🔄 Write: test                                      |   | _   |             | ×     |
|--|---|-----|-------------|-------|
| <u>F</u> ile <u>E</u> dit <u>V</u> iew <u>I</u> ns | sert F <u>o</u> rmat O <u>p</u> tions <u>T</u> ools <u>H</u> elp  |     |             |       |
| 🛱 Send 🗹 Spel                                      | ling 🔻 🔘 Attach 💌 🖴 Security 💌 🕂 Save 💌   |     |             |       |
| F <u>r</u> om:                                     | mailuser < > mailuser   |     |             | ~     |
| 🛩 То:  | maiuser2@   |     |             |       |
|  |   |     |             |       |
| _  |   |     |             |       |
| <u>S</u> ubject:                                   | test  |     |             |       |
| Paragraph 🗸 Va                                     | ariable Width $\checkmark = \mathbf{A} \cdot \mathbf{A} \cdot \mathbf{A} \cdot \mathbf{A} \cdot \mathbf{A} = \frac{1}{2}$ | € € | <b>≣</b> •∎ | • 🙂 • |
| test   |   |     |             |       |
|  |   |     |             |       |
|  |   |     |             |       |
|  |   |     |             |       |
|  |   |     |             | ×     |

This completes sending digitally signed e-mails.

## 2-2. How to Confirm a Sent E-mail That Was Digitally Signed

#### How to Confirm a Sent E-mail That Was Digitally Signed

1. Select a sent e-mail that was digitally signed from the [Sent] folder.

| Sent                       |  |    |                          | 7  | -    |   | ×           |
|----------------------------|--|----|--------------------------|--|------|---|-------------|
| 📩 Get Messages 🖙 🖉 Write 🖛 | 👎 Chat 👤 Address Book 🛛 🗞 Tag 👻 🔽 Quick Filter       |    | Search <ctrl+k></ctrl+k> |  |      | ٩ | ≡           |
| √⊠ mailuser                | 🛠   🚥 Unread 🖈 Starred 🛔 Contact 🗣 Tags 🖉 Attachment |    | Filt                     | ter these messages <ctrl+shift< th=""><th>+K&gt;</th><th></th><th>٩</th></ctrl+shift<> | +K>  |   | ٩           |
| Drafts                     | ት 🖈 🥙 Subject  | 00 | Correspondents           | ú  | Date |   | <u>~</u> EŞ |
| Sent .                     | 🚖 test   | ٠  | 🔿 mailuser@              | 0  |      |   |             |
| 🔯 Trash                    |  |    |                          |  |      |   |             |
| √ 🖳 Local folder           |  |    |                          |  |      |   |             |
| 🔯 Trash                    |  |    |                          |  |      |   |             |
| 🟝 Outbox                   |  |    |                          |  |      |   |             |
|                            |  |    |                          |  |      |   |             |
|                            |  |    |                          |  |      |   |             |
|                            |  |    |                          |  |      |   |             |
|                            |  |    |                          |  |      |   |             |

2. Click the [Envelope] icon.

| Sent                                | 🖂 test - Sent         | × 7 7              | - 🗆 ×             |
|-------------------------------------|-----------------------|--------------------|-------------------|
| 📩 Get Messages 🖙 🛛 🖉 Write 🖙        | 🗭 Chat 👤 Address Book | 💊 Tag 🔻 🝸 Qu       | ick Filter 🛛 🔎 🔳  |
| From mailuser 😭                     | ← Reply → Forward     | 🖥 Archive 🧯 🖕 Junk | 🛇 Delete 🛛 More 👻 |
| Subject <b>test</b><br>To mailuser🈭 |                       |                    |                   |
| test                                |                       |                    |                   |
|                                     |                       |                    |                   |
|                                     |                       |                    |                   |
|                                     |                       |                    |                   |
|                                     |                       |                    |                   |
|                                     |                       |                    |                   |
|                                     |                       |                    |                   |
|                                     |                       |                    |                   |
| <u>9</u>                            |                       |                    | 遊 Today ペイン 🔺 🔒   |

3. In the [Message Security] dialog box, click [View Signature Certificate].

| Message Security  | × |
|---|---|
| Message Is Signed   |   |
| This message includes a valid digital signature. The message has not been altered since it was sent.  |   |
| Signed by: mailuser   |   |
| Email address:  |   |
| Certificate issued by: NII Open Domain S/MIME CA  |   |
| View Signature Certificate  |   |
| Message Is Not Encrypted  |   |
| This message was not encrypted before it was sent. Information sent over the Interne without encryption can be seen by other people while in transit. | t |
| ОК  |   |

4. The [Certificate Viewer] will appear. Select the [General (G)] tab and make sure that the tab shows "This certificate has been verified for the following uses:" on its top.

| ertificate Viewer: "mailuser"   |   |   |
|---------------------------------|---|---|
| <u>G</u> eneral <u>D</u> etails |   |   |
| ertificate Viewer: "mailuser"   | >   | < |
| <u>G</u> eneral <u>D</u> etails |   |   |
| This certificate has been       | verified for the following uses:  |   |
| SSL Client Certificate          |   |   |
| Email Signer Certificate        |   |   |
| Email Recipient Certificat      | ce  |   |
| Issued To                       |   |   |
| Common Name (CN)                | mailuser  |   |
| Organization (O)                | National Institute of Informatics   |   |
| Organizational Unit (OU)        |   |   |
| Serial Number                   | 0C:68:CB:B2:0B:53:0E:BF   |   |
| Issued By                       |   |   |
| Common Name (CN)                | NII Open Domain S/MIME CA   |   |
| Organization (O)                | National Institute of Informatics   |   |
| Organizational Unit (OU)        | <not certificate="" of="" part=""></not>  |   |
| Period of Validity              |   |   |
| Begins On                       |   |   |
| Expires On                      |   |   |
| Fingerprints                    |   |   |
| SHA-256 Fingerprint             | 95:0E:32:76:74:4B:FF:46:44:01:0D:59:B3:67:4B:A6:<br>7E:F0:29:DC:0A:29:54:D6:96:97:E0:C0:86:EA:B8:15 |   |
| SHA1 Fingerprint                | CC:CE:D1:23:8C:E1:B6:37:01:AE:C0:2B:7C:14:CC:CC:0B:E3:B3:19   |   |

This completes confirmation of a sent e-mail that was digitally signed.