

Exercise for the Topic GnuPG 2014

15 points

Create in your CBWE home directory the directory: **exercises/GPG**

For this exercise you already had to finish the **Task Nr. 1** in the exercise for the Topic: **Mailing** (i.e. you already configured the mails servers (incoming, outgoing) for Icedove so you are able to send/receive emails).

1. Create your PGP private-public key pair for your CBWE account (**5** points)

- Use KDE GnuPG program's (kgpg) Key manager for creating the key pair with the following settings:
 - Expiration: unlimited, Algorithm: RSA, Length: 4096.
- create a screenshot about the kgpg Key Manager, where your key is visible, and save it in the **exercises/GPG** directory as: **keymanager-1.jpg**
- create a screenshot about the Properties of your key and save it, as above, as : **key-properties.jpg**
- export your public PGP key in the **GPG** directory as:
<your-name>-public-cbwe-2013-key.asc

2. Configure Enigmail for Icedove (**7** points)

- Install the Enigmail plugin in Icedove. Create a screen shot about the Icedove -> Tools -> Add-ons -> Extension window, where I can see the installed plugins. Save it in the **exercises/GPG** directory as **icedove-enigmail-inst.jpg**
- import my public PGP key from the <http://moodle.risc.jku.at> server at the CBWE course Topic 8 (Using the Gnu Privacy Guard), with the Key Manager of **Enigmail**. Create a screen shot about the listed keys and save it as **enigmail-keyman-keylist.jpg**
- create a rule for sending emails to me (k.erdei@risc.uni-linz.ac.at) in Icedove. Send the emails to me always encrypted and signed. Use the Menu item: OpenPGP -> Edit per recipient rules. Create a screen shot about this rule and save it as **enigmail-rule-for-KE.jpg** .
- set to my key the Key manager the trust level: 'I trust ultimately'. Create a screen shot about the Key Properties window of my key, on such a way, that the 'OpenPGP - Set owner trust' window is visible, too. Save it as: **enigmail-key-prop-trust.jpg**

3. Send encrypted emails to me (k.erdei@risc.uni-linz.ac.at) (3 points)

- send your public PGP key for your RISC CBWE account to me in an encrypted email. I'll import your public key in my keyring and I'll confirm you in an encrypted email, that your key is OK.
- send an answer to this email simply with a second encrypted email, that you got my confirmation.

Deadline: January 31th, 2014.

Additional task to this topic (8 points)

a/ - If you are a RISC PhD student, you can send me your public PGP key for your standard RISC account (i.e. for your standard RISC email address) in an encrypted email (encrypted with my public PGP key).

- If you are not a RISC PhD student, you can send me your public PGP key for an email address of you, which you use, in an encrypted email (encrypted with my public PGP key).

b/ I'll import this public key of you and I'll confirm your email in an encrypted email, using your this public PGP key.

c/ Answer me simply again encrypted, that you got my confirmation.

That's all.

I'll use this additional points to increase your points at other exercises, for which you did not get there the maximum points.

Deadline: December 8. 2014.