Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Federal Department of Defence,
Civil Protection and Sport DDPS

armasuisse
**Federal Office of Topography swisstopo**

# RSA Key Pair for SSH Authentication

A RSA key pair enables you to access the FSDI (Federal Spatial Data Infrastructure) servers through SSH protocol. In order to prevent misuse please read the following directives carefully and fill the form at the end.

## 1 Generating RSA Key Pair

Create a SSH key pair using a **2048 bit RSA encryption**. Your private key **must include a passphrase** respecting the below listed requirements.

Create a SSH key pair:

```
ssh-keygen -t rsa -b 2048
```

In order to guarantee the confidentiality of your private key the following conditions have to be respected:

1. The private key is personal:
   - do **not share** it with others
   - do **not store** it unprotected (e.g. read permissions of the private key file for other users)

### Passphrase

In order to guarantee a secure passphrase the following conditions have to be respected:

1. The passphrase has to contain at least **10 characters**.
2. The passphrase has to contain different characters from at least 3 of the 4 following categories:
   - **numbers** [0-9]
   - **lower case letters** [a-z]
   - **upper case letters** [A-Z]
   - **special characters**, e.g.,[$,&,%,-,@,+,_,#,etc.]
3. The passphrase is personal:
   - do **not share** it with others
   - do **not store** it unprotected (e.g. unencrypted text file or open memo at your workplace)

**Tip**

In order to build a strong passphrase imagine a sentence which is easy to remember. Then use special characters, numbers and the first letter of each word to compose your password.

Example:

«*In Bern a beefsteak and 5 potatoes costs 30 Dollar*»
becomes
« *IBab&5pc30*$ »

Federal Office of Topography swisstopo

Seftigenstrasse 264, 3084 Wabern
central office +41 31 963 21 11
www.swisstopo.ch

## 2 Changing Passphrase

The passphrase has to be **changed if** you already possess a RSA key which is **not complying** to the requirements above.

Furthermore, it is recommended that you change your passphrase in a monthly interval.

Change the passphrase:

```
ssh-keygen -p -t rsa
```

## 3 Sign Off

Inform swisstopo if you do not require your RSA key pair anymore (e.g. when the related project has finished).

Send an email to helpdeskbgdi@swisstopo.ch with the subject « **RSA Key Pair** ».

Indicate your **name** and your intention to **sign off**.

## 4 Agreement

Please **fill** the form below and **return** it to the following address:

*Federal Office of Topography swisstopo*
*COGIS*
*FSDI Webinfrastructure IWI*
*Seftigenstrasse 264*
*3084 Wabern*

Last Name _____

First Name _____

Organisation _____

Email _____

Telephone _____

Purpose _____

_____

(mission or project the RSA key par is being used for)

By signing below, you certify that you have read, understand and comply to the directives stated in this document :

Place and Date _____

Signature _____

For help or further information contact helpdeskbgdi@swisstopo.ch

# Annexe

On Windows you can use PuTTYgen (http://www.chiark.greenend.org.uk/~sgtatham/putty/) in order to create a RSA key pair. Private keys created with PuTTYgen can notably be used with PuTTY (popular terminal emulator) or WinSCP (popular file transfer client). How to create a key pair with PuTTYgen is explained below.

## Create a RSA Key Pair with PuTTYgen

1. Run PuTTYgen (puttygen.exe)
2. Select the SSH-2 RSA encryption
3. Set the bits generated in the key to 2048
4. Click «Generate» and move the mouse over the appearing area
5. Enter a key passphrase
   (See above for the requirements which have to be respected!)
6. Save the public key and send it to the contact person that will enable you access their machines.
7. Save the private key securely on your computer. (Do not share it with anybody!)