Kerberos

This page describes how Kerberos can be used to authenticate against various services without typing a password, thus providing a true single sign-on (SSO) experience. What can SSO do for you? Watch this!

If you reached this page without typing a password then SSO for HTTP(s) is working with your setup. This is actually the case with the Linux setup at the TI Biel/Bienne site and a domain joined computer using Windows 7 and a recent version of Internet Explorer.

In the realm **BFH.CH** Active Directory (AD) is used as a key distribution center (KDC). Depending on

- wether your machine is domain joined or not,
- which service you like to authenticate against,
- and which operating system is used

some additional configuration may be needed to get SSO working.

Basic Configuration

The basic configuration ensures that you can get a Ticket Granting Ticket (TGT), ready to use Kerberized services. **To get a TGT you have to be inside the BFH network or be connected by VPN!**

Linux

During a login at the TI Biel/Bienne site on our PXE-based Linux setup a TGT is fetched via the Kerberos PAM module.

To get a TGT on your personal machine ensure that you have the Kerberos utilities installed. (Package `krb5-user` on Ubuntu.) Save the text below as `/etc/krb5.conf`:

```
[libdefaults]
        default_realm = BFH.CH

[domain_realm]
        .bfh.ch = BFH.CH
        bfh.ch = BFH.CH
```

Mac OS X

There are several possibilities to get a TGT on your personal Apple computer. By far the simplest one is to open a terminal window and typing

```
kinit BFHusername@BFH.CH
```

If you save the following text

```
[libdefaults]
        default_realm = BFH.CH

[domain_realm]
        .bfh.ch = BFH.CH
        bfh.ch = BFH.CH
```

as `/Library/Preferences/edu.mit.Kerberos` (system-wide) or `~/Library/Preferences/edu.mit.Kerberos` (for a specific user), you can omit the realm to get a TGT.

On a domain joined computer no additional configuration is needed. Ask the helpdesk if you like to have your Apple computer using Mac OS X joined to the domain.

Windows

On a domain joined computer no additional configuration is needed. If you're using a computer installed by the IT services, it is most likely domain joined. It is, however, recommended that you install MIT Kerberos for Windows as described below. The Windows GSSAPI implementation cannot delegate credentials to a remote host, which is necessary to mount your home directory, e.g. when you log in using SSH.

Download the correspondig packages from http://www.secure-endpoints.com/#kfw:

- On a 32-bit system install the 32-bit version of Kerberos for Windows.
- On a 64-bit system install both the 64-bit and the 32-bit version Kerberos of for Windows. The 64-bit version must be installed *before* the 32-bit version.

Usage

On Linux and Mac OS X open a terminal window and type

```
kinit BFHusername
```

to get a TGT. Type `klist` to check if you have a valid TGT. On Linux you'll see a slightly different output than on Mac OS X:

```
BFHusername@linux:~$ klist
Ticket cache: FILE:/tmp/krb5cc_38266
Default principal: BFHusername@BFH.CH

Valid starting     Expires            Service principal
05/29/11 23:58:56  05/30/11 09:59:00  krbtgt/BFH.CH@BFH.CH
    renew until 05/30/11 23:58:56
```

```
macosx:~ BFHusername$ klist
```

```
Kerberos 5 ticket cache: 'API:Initial default ccache'
Default principal: BFHusername@BFH.CH

Valid Starting     Expires            Service Principal
05/30/11 00:06:28  05/30/11 10:06:28  krbtgt/BFH.CH@BFH.CH
    renew until 05/30/11 10:06:28
```

Services

- SSH
- Web Browser Configuration (HTTP)