# Table of Contents

**Smart Cards revisited - in 2012**

- Prerequisites ................................................................. 1
- Software installation ...................................................... 1
- (Re)Configuration ............................................................. 1
- Kerberos - pkinit - configuration ........................................ 2
- pam_pkcs11 configuration .................................................. 2
- Configure PAM ................................................................. 3
- Configuring krb5-auth-dialog ........................................... 4
- Troubleshooting .............................................................. 4
- Problems ........................................................................ 5
Smart Cards revisited - in 2012

The goal is to integrate CERN Smartcards with the system and different applications.

So far following has been implemented:

- authentication with smartcard, including obtaining Kerberos ticket and AFS token, with fallback to password authentication.
- using smartcard as security device in Firefox/Thunderbird.
- using smartcard in krb5-auth-dialog (hmm : not very useful since kerberos ticket is refreshed with every login and screen unlock ... also buggy, may lock up your smartcard with too many PIN entry attempts, requiring its PUK)
- using smartcard with esc (Enterprise Security Client): does not work, esc supports only coolkey library, no possibility of pluggin-in replacement one.

To be investigated:

- rdesktop: rdesktop -r scard cerntsnew works (1.6.0-8.slc5/6.*2* with scard patch) (cernts does not .... but is it configured ?)
- freerdp: xfreerdp --no-nla --plugin rdpdr --data scard:scard -- cerntsnew.cern.ch works (1.0.1-2e049c6 with a patch) (cernts does not .... but is it configured ?) and smart card forwarding within a Microsoft Virtual machine works too.
- esc - `Enterprise Smart Cards' - will not work since esc supports only a small subset of cards: in addition it interferes with proper operation of SafeSign cards - uninstall

Prerequisites

- A 2012 CERN Smart Card with your certificate (not distributed to public yet)
- A card reader (SCR3311 - the default CERN one or universal USB reader)
- System running fully updated Scientific Linux CERN 6 (SLC6)
- and on CERN internal network.

Software installation

Following steps are to be performed as root on your system

- run: yum --enablerepo=slc6-cernonly install cern-smartcard krb5-pkinit-openssl (to add basic smartcard and pkinit support to your system, including NSS db modifications)
- run: yum --enablerepo=slc6-cernonly install firefox-aetssic thunderbird-aetssic (to add smartcard support to Firefox and Thunderbird)
- run: yum remove esc (to remove esc - Enterprise Smart Cards manager which interferes with proper SafeSign cards operation)
- run: yum remove openct (removes openct including pcscd driver which interferes with SafeSign smart cards one)

(note: Fedora 16: need to install krb5-pkinit-openssl package too !)

(Re)Configuration

Following steps are to be performed as root on your system
run: /sbin/service openct stop
run: /sbin/chkconfig --del openct
Edit /etc/reader.conf.d/openct.conf, comment out all the content
run: /sbin/chkconfig --levels 345 pcscd on
run: /sbin/service pcscd restart

and as user:

• restart Firefox (if installed firefox-aetssic)
• restart Thunderbird (if installed thunderbird-aetssic)

Kerberos - pkinit - configuration

Edit /etc/krb5.conf to contain:

```
[libdefaults]
default_realm = CERN.CH
ticket_lifetime = 25h
renew_lifetime = 120h
forwardable = true
proxiable = true
pkinit_anchors = FILE:/etc/pki/tls/certs/CERN-bundle.pem
pkinit getIdentities = PKCS11:libaetpkss.so
pkinit_eku_checking = kpServerAuth
pkinit_kdc_hostname = cerndc.cern.ch
pkinit_cert_match = &&<EKU>msScLogin,<KU>digitalSignature

[realms]
CERN.CH = {
default_domain = cern.ch
 kdc = cerndc.cern.ch
}

[domain_realm]
.cern.ch = CERN.CH

[appdefaults]
; options for Red Hat pam_krb5-2 - ARE THESE REALLY NEEDED ?
pam = {
   external = true
ticket_lifetime = 25h
}
```

(above configuration is a minimum one: make sure that your configuration does not contain any other lines defining pkinit settings, nor allow_weak_crypto or default_tkt_enctypes).

pam_pkcs11 configuration

Edit /etc/pam_pkcs11/pam_pkcs11.conf to contain:

```
pam_pkcs11 {
nullok = true;
debug = false;
card_only = true;
use_first_pass = false;
try_first_pass = false;
use_authok = false;
use_pkcs11_module = safesignic;
screen_savers = "gnome-screensaver", xscreensaver, kscreensaver;
```
enable_ocsp=true; #### NO: we do not use OCSP at present - enabling it causes gnome screensaver smart card unlock 'hang' for 3 minutes then restarting auth. dialog (once every 5-10 tries)
enable_ocsp=false;

pkcs11_module safesignic {
    module = libaetpkss.so;
    description = "SafeSign IC";
    slot_num = 0;
    nss_dir = /etc/pki/nssdb;
    #crl_dir = /etc/pki/tls/crls;  #### same comment as above, to be investigated further
    #crl_policy = ca,crl_auto;  #### same comment as above, to be investigated further
    crl_policy=none; #### NOT for production !
}

use_mappers = cn; #pwent;

mapper pwent {
    debug = false;
    ignorecase = false;
    module = internal;
    # module = /usr/$LIB/pam_pkcs11/pwent_mapper.so;
}

mapper cn {
    debug = false;
    module = internal;
    # module = /usr/$LIB/pam_pkcs11/cn_mapper.so;
    ignorecase = false;
    #mapfile = "file:///etc/pam_pkcs11/cn_map";
}

(WARNING: pwent pkcs11 mapper is .... er ... not too strict about mapping - matches on shortest string ... so if you have accounts alike 'user' 'userone' 'usertwo' .. etc and certificate on smart card is for 'user' and 'user', 'userone' 'usertwo' accounts do exist on system] ... 'user' could get access to 'userone' and/or 'usertwo' account - but not his kerberos credentials) (again - this is minimal configuration, this config file contains other sections, which are not interfering with setup)

Configure PAM

Edit /etc/pam.d/system-auth-ac to contain:

auth  required   pam_env.so
auth  sufficient pam_fprintd.so
auth  [success=1 default=ignore] pam_succeed_if.so service notin login:xdm:kdm:xscreensaver
auth  [success=ok authinfo_unavail=ignore ignore=ignore default=die] pam_pkcs11.so
auth  sufficient pam_unix.so nullok try_first_pass
auth  sufficient pam_krb5.so no_initial_prompt no_subsequent_prompt tokens
auth  requisite pam_succeed_if.so uid >= 500 quiet
auth  sufficient pam_sss.so use_first_pass
auth  required   pam_deny.so

account required  pam_unix.so broken_shadow
account sufficient pam_localuser.so
account sufficient pam_krb5.so
account sufficient pam_succeed_if.so uid < 500 quiet
account [default=bad success=ok user_unknown=ignore] pam_sss.so
account required  pam_permit.so

password optional  pam_pkcs11.so
password requisite pam_cracklib.so try_first_pass retry=3 type=
password sufficient pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password  sufficient  pam_krb5.so
password  sufficient  pam_sss.so use_authok
password  required  pam_deny.so

session  optional  pam_keyinit.so revoke
session  required  pam_limits.so
session  [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session  required  pam_krb5.so
session  required  pam_unix.so
session  optional  pam_sss.so

(WARNING: not very well tested so far ... check ALL scenarios ... login with/without password ,
with/without smartcard , as root, sudo , su ... etc ... etc)

Configuring krb5-auth-dialog

Note: slc6 uses a patched krb5-auth-dialog 0.17 (RHEL6 - 0.16) which acquires afs token automagically via
afs plugin)
right click on 'keys' icon in desktop panel, choose 'Preferences', then 'Kerberos' tab. Click 'Use Smartcard' and
close preferences window. open 'Preferences' again: fill in Kerberos principal yourloginid@CERN.CH ,
uncheck 'Use Smartcard', fill in 'Userid' to contain PKCS11:libaetpkss.so fill in 'X509 trust anchors' to
contain FILE:/etc/pki/tls/certs/CERN-bundle.pem then close preferences window and kill the application
killall -9 krb5-auth-dialog , next restart it again (Alt-F2, krb5-auth-dialog). Now you should be able to renew
your kerberos ticket by left-clicking on 'keys' icon.
YES - IT IS buggy .... and be warned: if you 'left-click' multiple times on it and then choose cancel without
entering PIN it still sends an empty PIN to smartcard and since the smartcard has limited count of PIN
failures before it locks and requests PUK .... you may find yourself locked out...

Since this method of getting Kerberos credentials is not really necessary (as every screen unlock will refresh
your ticket anyway) ... maybe it would be better to not even advertise it ...

Troubleshooting

• Reboot your system first ... (avoid clearing some issues with some libraries already preloaded in
memory and gnome components as screensaver not being able to reconfigure themselves on the fly ..
sometimes)
• Be aware that lcm may reconfigure your /etc/krb5.conf and /etc/pam.d/system-auth-ac files ... (while
running lcm --update_ or when new lcm-profile is deployed).
• verify NSS db modules list: /usr/bin/modutil -list -dbdir /etc/pki/nssdb should show
SafeSign PKCS#11 module installed:

3. SafeSign IC PKCS#11 Module=
library name: libaetpkss.so
slots: 5 slots attached
status: loaded

• verify NSS db trusted certificates: /usr/bin/certutil -L -d /etc/pki/nssdb should show CERN
Root CA and CERN Trusted Certification Authority certificates:

CERN Root CA                                                 CT,C,C
CERN Trusted Certification Authority                         CT,C,C
• verify card functionality, start /usr/bin/tokenadm (or select 'SafeSign Identity Client Token Manager'
from menu 'Applications' , submenu 'System Tools')
verify that the PKCS#11 module is loaded in firefox/thunderbird (select 'Edit' - 'Preferences' - 'Advanced' - 'Encryption' - 'Security Devices') - you should see 'A.E.T. SafeSign IC PKCS#11 Module' loaded.

• verify pam_pkcs11 mapper with pkcs11_inspect:

PIN for token:
Printing data for mapper cn:
jpolok
423567
Jarek Polok

• verify if you can obtain a Kerberos ticket/AFS token: run kinit, you should see a prompt:

FirstName Name PIN:

enter your smartcard PIN, and check: Kerberos tickets: klist

Ticket cache: FILE:/tmp/krb5cc_14213
Default principal: jpolok@CERN.CH

<table>
<thead>
<tr>
<th>Valid starting</th>
<th>Expires</th>
<th>Service principal</th>
</tr>
</thead>
<tbody>
<tr>
<td>03/22/12 16:57:54</td>
<td>03/23/12 17:57:54</td>
<td>krbtgt/CERN.CH@CERN.CH</td>
</tr>
<tr>
<td>renew until 03/27/12 17:57:54</td>
<td></td>
<td></td>
</tr>
<tr>
<td>03/22/12 16:57:58</td>
<td>03/23/12 17:57:54</td>
<td>afs/cern.ch@CERN.CH</td>
</tr>
<tr>
<td>renew until 03/27/12 17:57:54</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

AFS tokens:_tokens_

Tokens held by the Cache Manager:

User's (AFS ID 14213) tokens for afs@cern.ch [Expires Mar 23 17:57]

--End of list--

Problems

All problems listed below (except kinit one ?) seem to be related to crash/hang in libaetpkss.so — to be rechecked after we get official RHEL6 SafeSign IC packages — Q2 2012* Got these ... (3.0.77) in .. November 2012.

• sometimes Gnome screen saver (or rather pcscd) does not observe card removal correctly (or immediately) – as a result the screen is not locked automatically. (use Ctrl-Alt-Del as workaround) (seems solved with SafeSign 3.0.77 library update in November)
• sometimes Gnome screen saver unlock dialog hangs for 3 minutes or so, then restarts ... (remove card, switch to different virtual console, login with password and killall -9 gnome-screensaver-dialog then switch back to X ... or wait 3 minutes) (seems solved with SafeSign 3.0.77 library update in November)
• on system boot pcscd dies: switch to console, login as root, execute service pcscd restart, logout, switch back to X, kill GDM (Ctrl-Alt-Backspace) to get ‘smartcard authentication’ option. (not needed if opencnt removed from system)
• kinit hangs segfaults when called without username by different user, than the certificate is for and there is no krb5 cache:

# whoami & & kinit
jarek
Jarek Polok PIN:
kinit: Client name mismatch while getting initial credentials
Segmentation fault (core dumped)
(the certificate is for jpolok) Use:

```bash
# whoami && kinit jpolok
jarek
Jarek Polok PIN:
```

instead.

```
• git https crashes:

xenophile kernel: git-remote-http[28390]: segfault at 27ba000 ip 00007f1325c3cb8b sp 00007f1325ad0000

```

```bash
git clone https://github.com/FreeRDP/FreeRDP.git
Initialized empty Git repository in /tmp/FreeRDP/.git/
error: child process died of signal 11
fatal: ref parsing thread failed
```

(does not happen after complete removal of openct) -- JaroslawPolok - 23-Nov-2012