NAME

pam_keyinit − Kernel session keyring initialiser module

SYNOPSIS

pam_keyinit.so [debug] [force] [revoke]

DESCRIPTION

The pam_keyinit PAM module ensures that the invoking process has a session keyring other than the user default session keyring.

The module checks to see if the process's session keyring is the **user-session-keyring**(7), and, if it is, creates a new **session-keyring**(7) with which to replace it. If a new session keyring is created, it will install a link to the **user-keyring**(7) in the session keyring so that keys common to the user will be automatically accessible through it. The session keyring of the invoking process will thenceforth be inherited by all its children unless they override it.

In order to allow other PAM modules to attach tokens to the keyring, this module provides both an *auth* (limited to **pam_setcred**(3) and a *session* component. The session keyring is created in the module called. Moreover this module should be included as early as possible in a PAM configuration.

This module is intended primarily for use by login processes. Be aware that after the session keyring has been replaced, the old session keyring and the keys it contains will no longer be accessible.

This module should not, generally, be invoked by programs like **su**, since it is usually desirable for the key set to percolate through to the alternate context. The keys have their own permissions system to manage this.

The keyutils package is used to manipulate keys more directly. This can be obtained from:

Keyutils[1]

OPTIONS

debug

Log debug information with **syslog**(3).

force

Causes the session keyring of the invoking process to be replaced unconditionally.

revoke

Causes the session keyring of the invoking process to be revoked when the invoking process exits if the session keyring was created for this process in the first place.

MODULE TYPES PROVIDED

Only the **session** module type is provided.

RETURN VALUES

PAM_SUCCESS

This module will usually return this value

PAM_AUTH_ERR

Authentication failure.

PAM_BUF_ERR

Memory buffer error.

PAM_IGNORE

The return value should be ignored by PAM dispatch.

PAM_SERVICE_ERR

Cannot determine the user name.

PAM_SESSION_ERR

This module will return this value if its arguments are invalid or if a system error such as ENOMEM occurs.

PAM_USER_UNKNOWN

User not known.

EXAMPLES

Add this line to your login entries to start each login session with its own session keyring:

```
session  required  pam_keyinit.so
```

This will prevent keys from one session leaking into another session for the same user.

SEE ALSO

pam.conf(5), **pam.d**(5), **pam**(7), **keyctl**(1)

AUTHOR

pam_keyinit was written by David Howells, <dhowells@redhat.com>.

NOTES

1. Keyutils
   http://people.redhat.com/˜dhowells/keyutils/