

Mandos

<http://www.recompile.se/mandos>

Disk encryption is essential for physical computer security, but seldom used due to the trouble of remembering and typing a password at every restart. We describe Mandos, a program which solves this problem, its security model, and the underlying concepts of its design.

Any security system must have a clear view of its intended threat model - i.e. what threats it is actually intended to protect against; the specific choices and tradeoffs made for Mandos will be explained. Another danger of security system design is the risk of its non-use; i.e. that the system will not be used for some real or perceived drawbacks, such as complexity. The deliberate design choices of Mandos, involving low-interaction, "invisible" and automatic features, will be covered.

Mandos

<http://www.recompile.se/mandos>

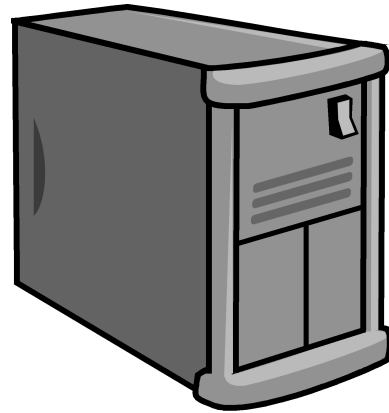
TL;DL

```
aptitude install mandos
```

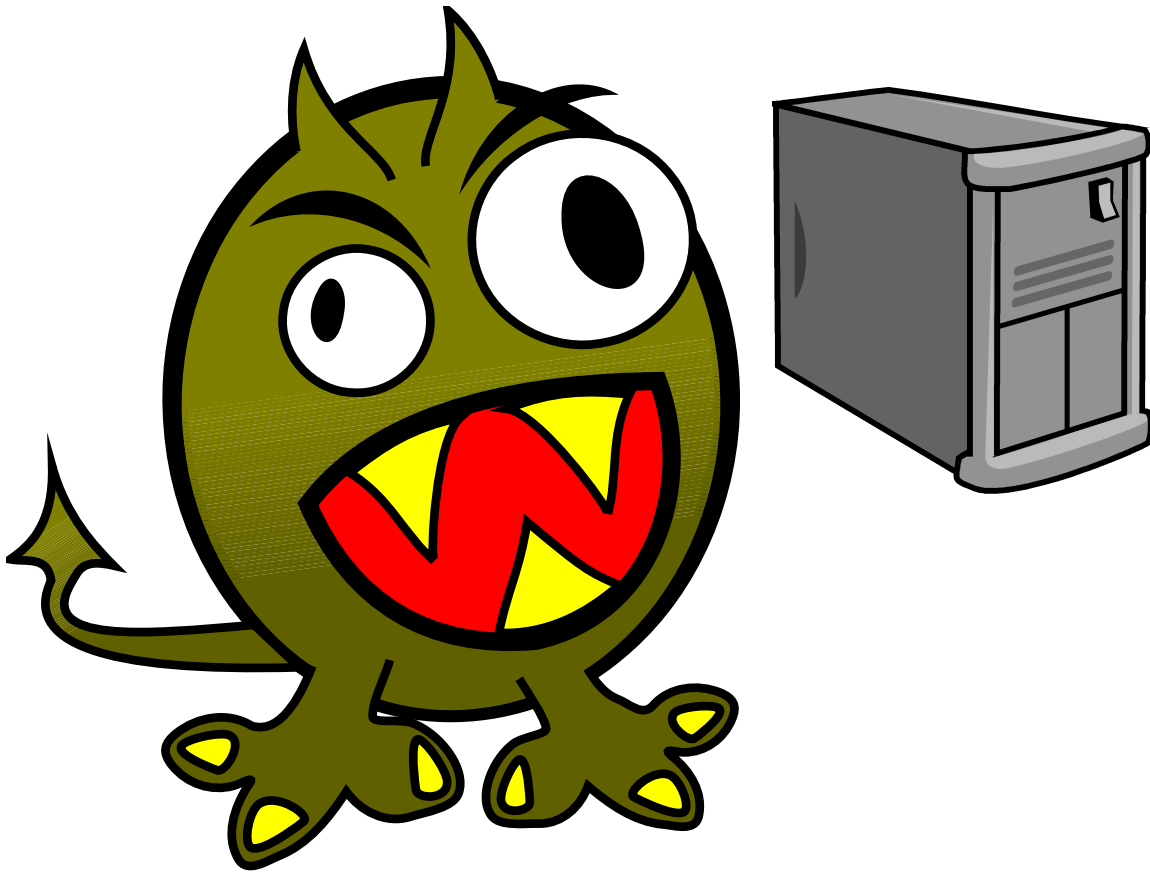
```
aptitude install mandos-client
```

Threat Model

Threat Model



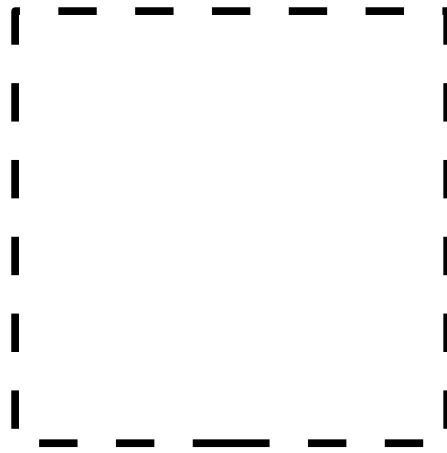
Threat Model



Threat Model

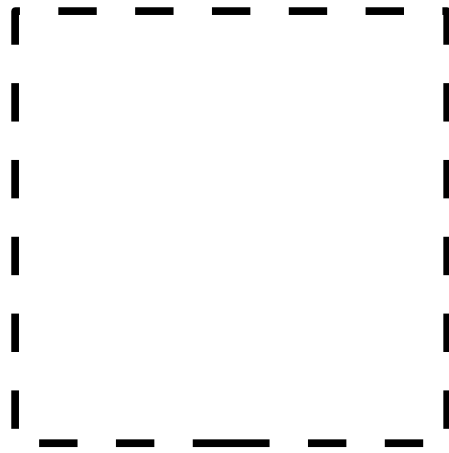


Threat Model



No Server

Threat Model



No Server



Threat Model



[!!] Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

Guided - use entire disk

Guided - use entire disk and set up LVM

Guided - use entire disk and set up encrypted LVM

Manual

<Go Back>

Booting the kernel.

Loading, please wait...

Volume group "glorfindel" not found

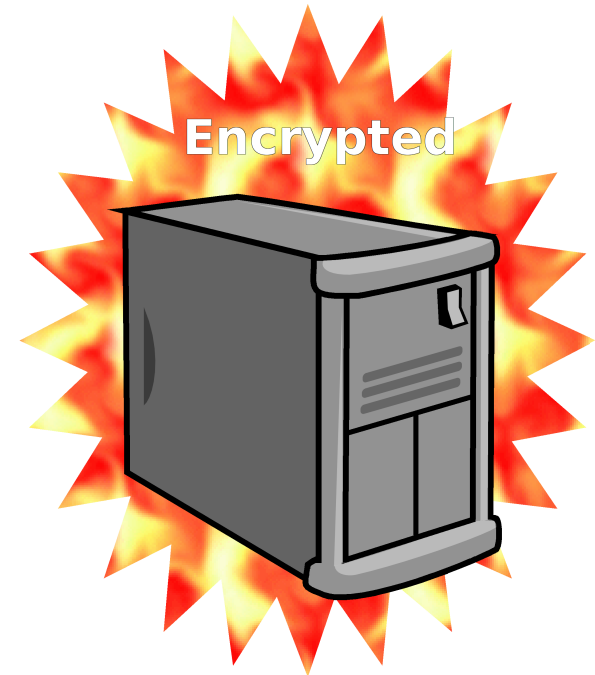
Volume group "glorfindel" not found

Enter passphrase to unlock the disk /dev/hda2 (hda2_crypt): _

Kernel alive

kernel direct mapping tables up to 1000000000 @ 8000-d000

Threat Model



New threat: non-use

Inconvenient

Burdensome

“I’ll do it some day”

New threat:



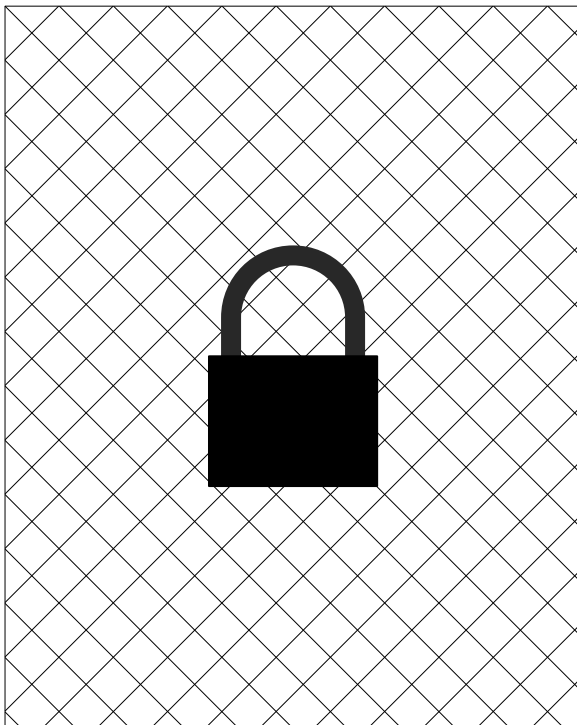
**Security needs to be
*transparent***

Full Disk Encryption

/boot



(rest of disk)

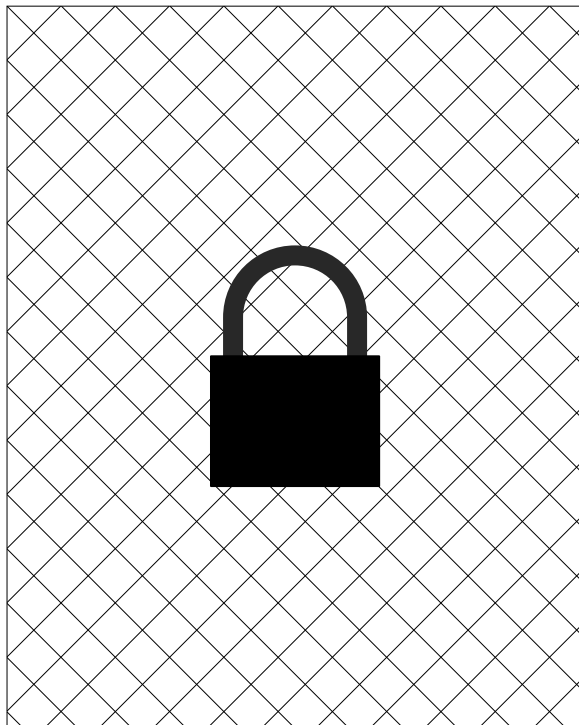


Full Disk Encryption

/boot



(rest of disk)

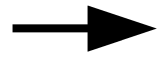
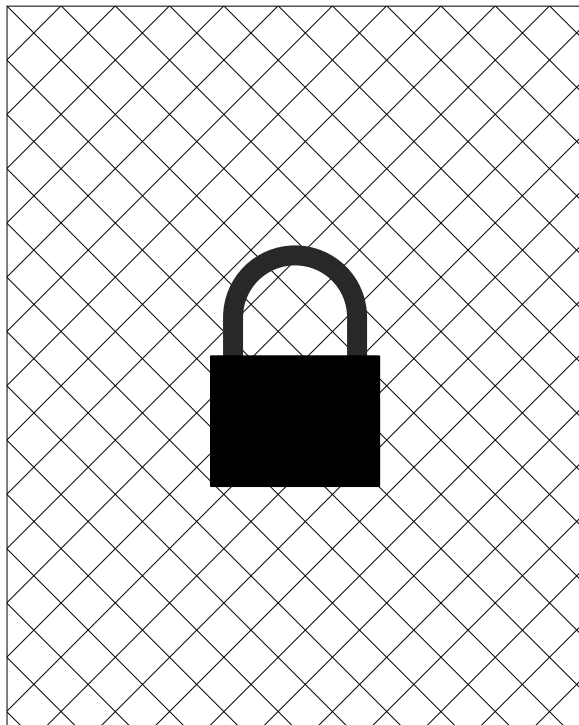


Full Disk Encryption

/boot



(rest of disk)

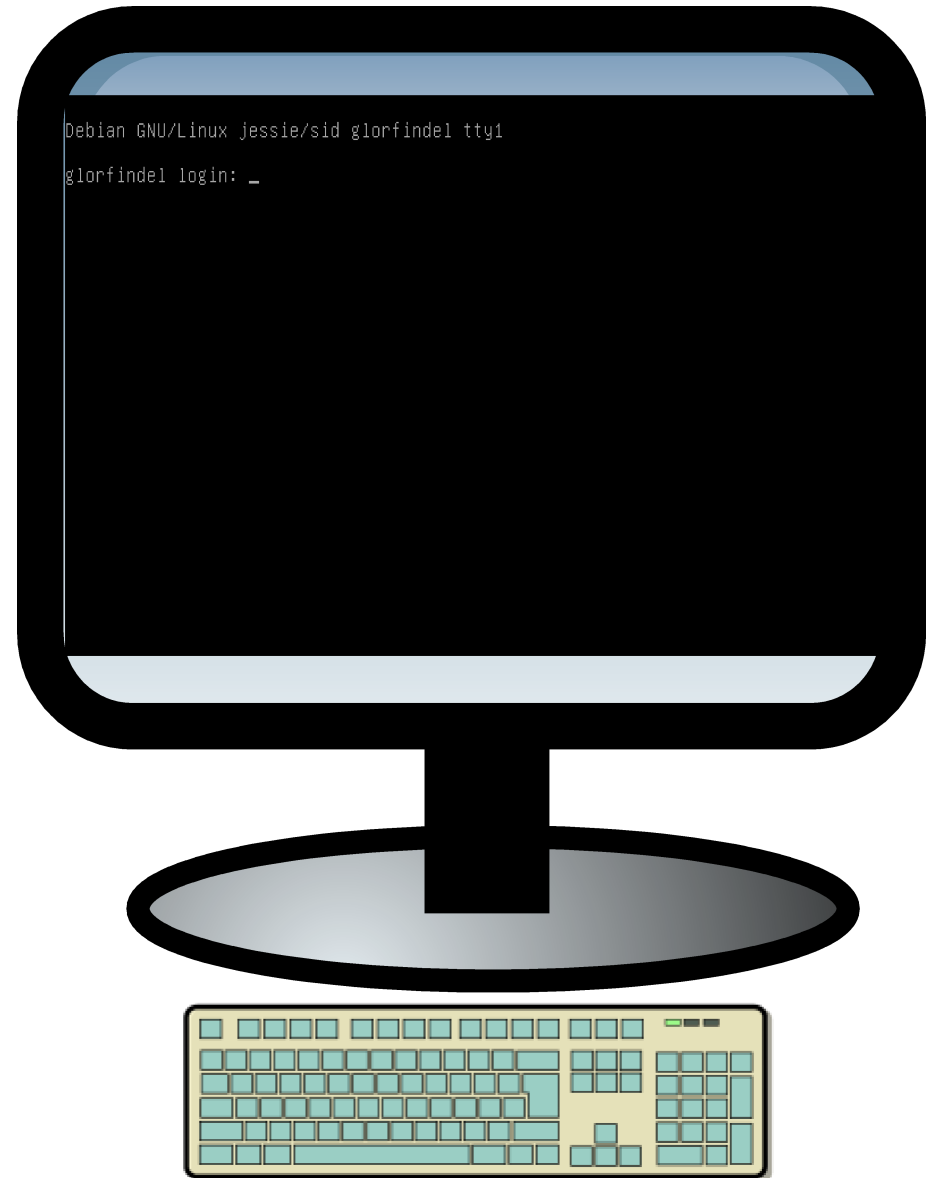
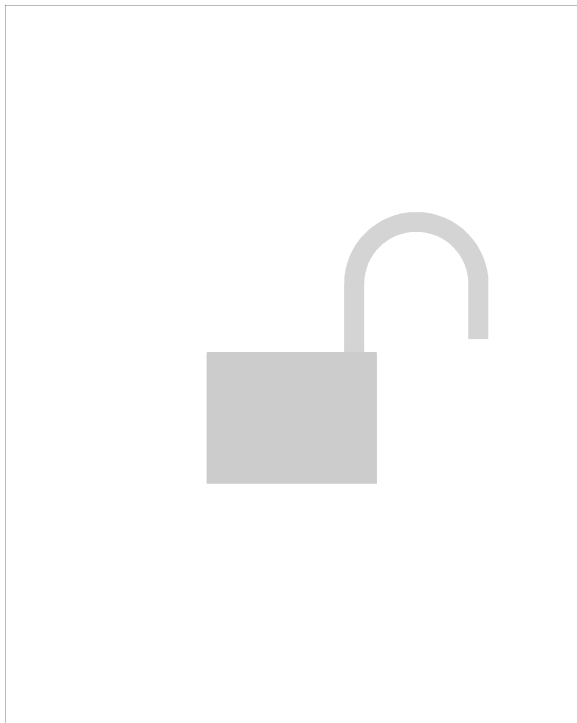


Full Disk Encryption

/boot



(rest of disk)



Mandos

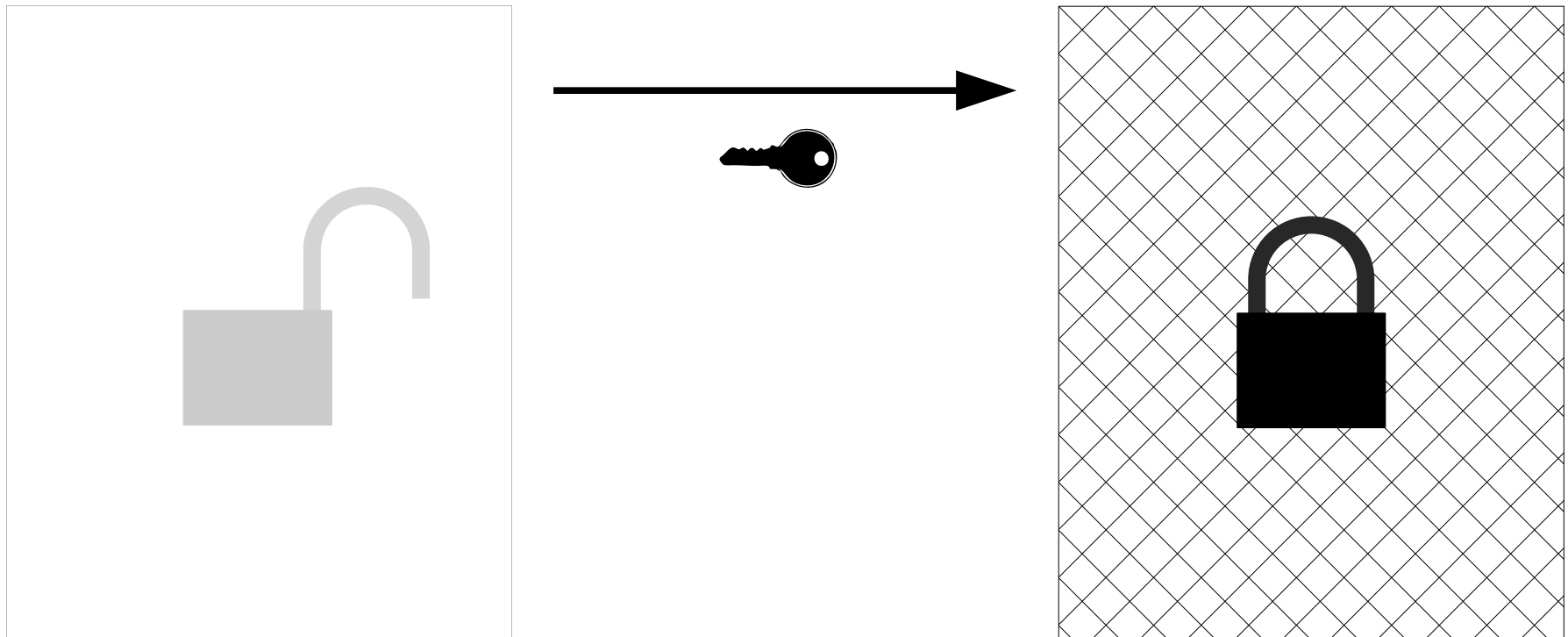
<http://www.recompile.se/mandos>

Servers provide passwords to *each other*

Mandos

<http://www.recompile.se/mandos>

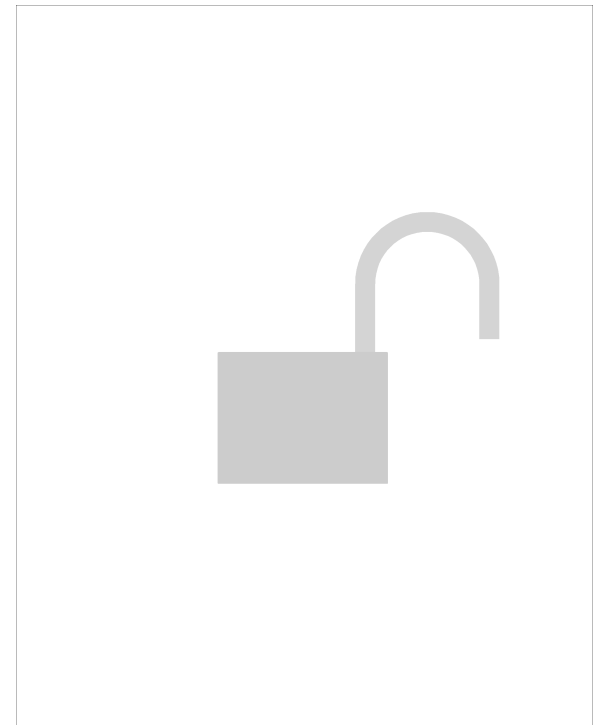
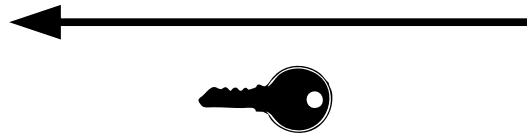
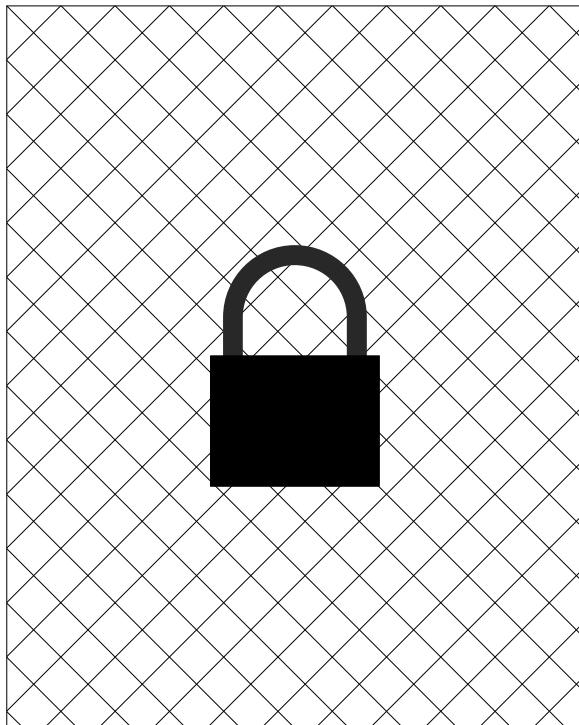
Normal operation



Mandos

<http://www.recompile.se/mandos>

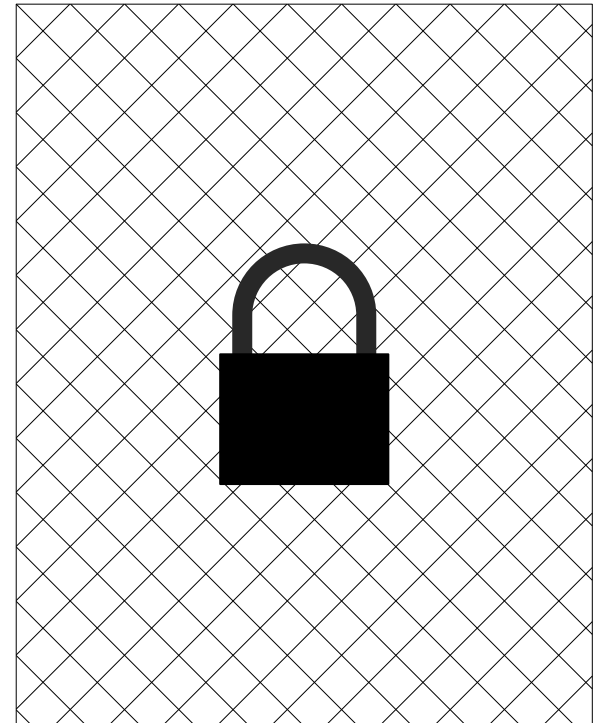
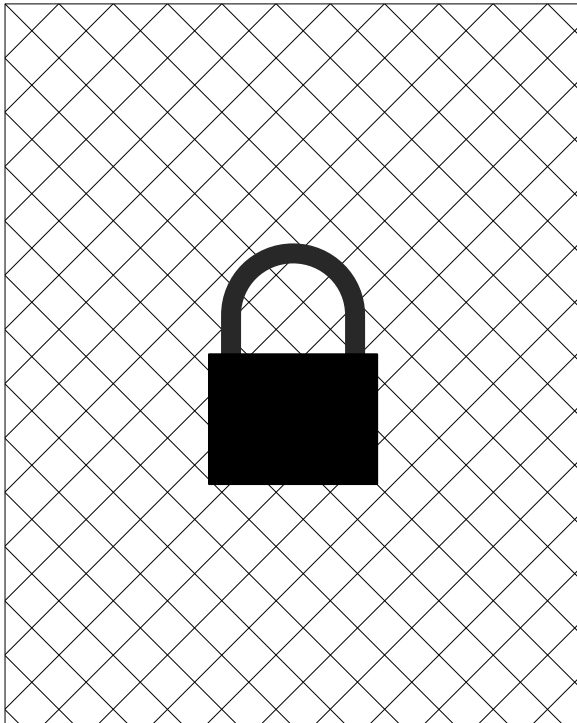
Normal operation



Mandos

<http://www.recompile.se/mandos>

Lockdown state
Administrator attention required



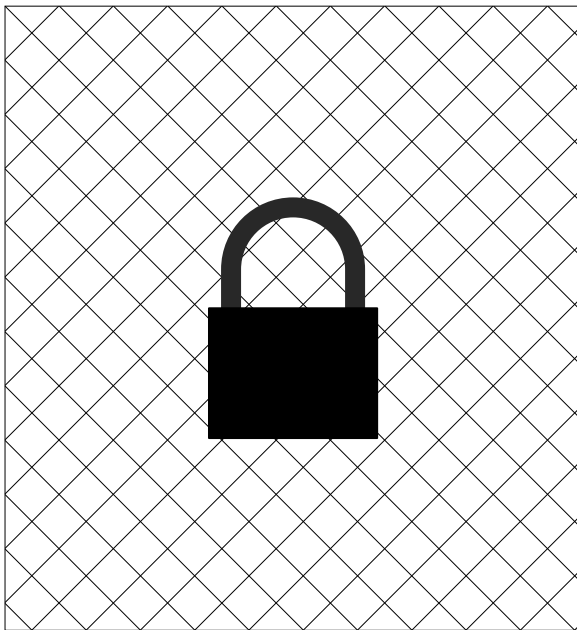
Mandos

<http://www.recompile.se/mandos>

/boot



(rest of disk)



Client



Server

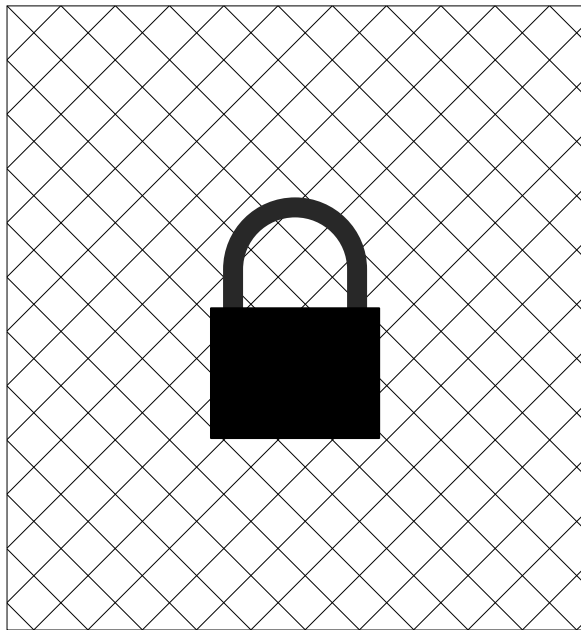
Mandos

<http://www.recompile.se/mandos>

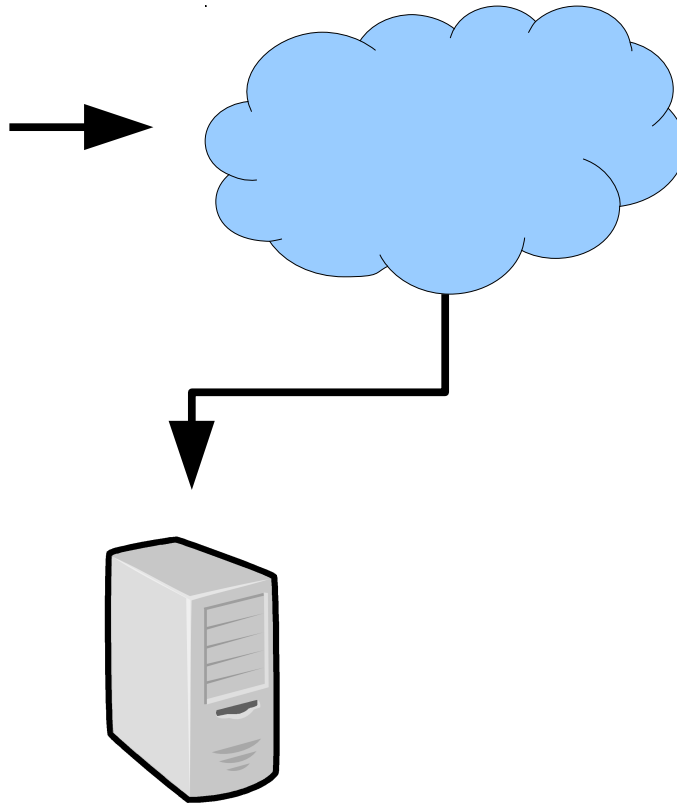
/boot



(rest of disk)



Client

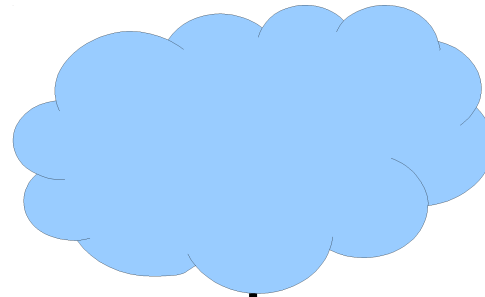


Server

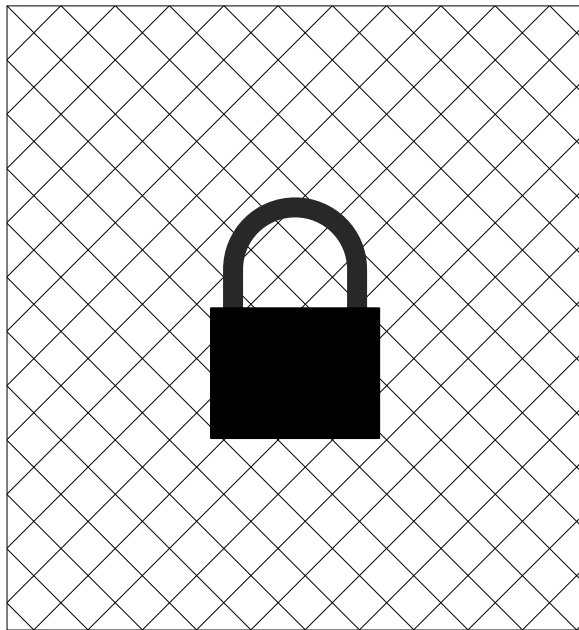
Mandos

<http://www.recompile.se/mandos>

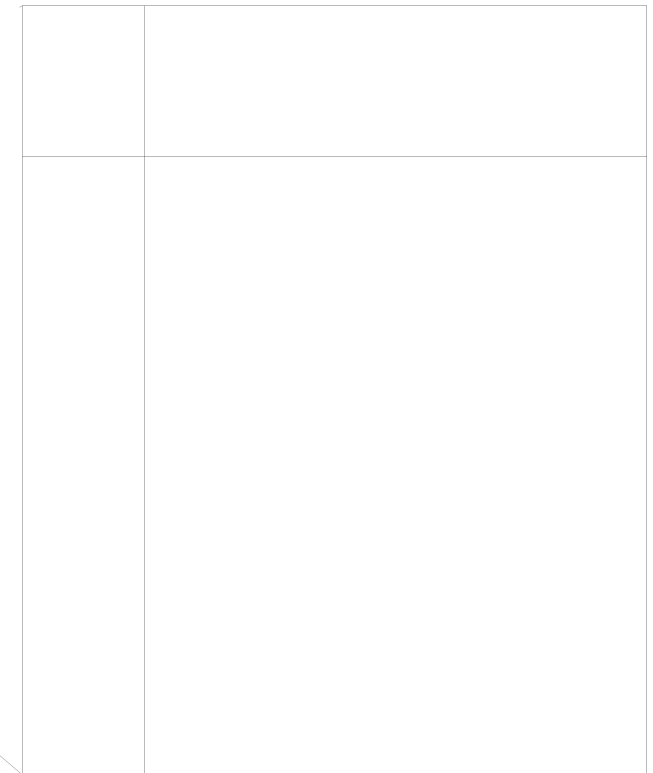
/boot



(rest of disk)



Server

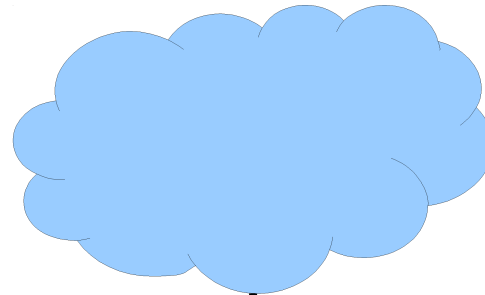


Client

Mandos

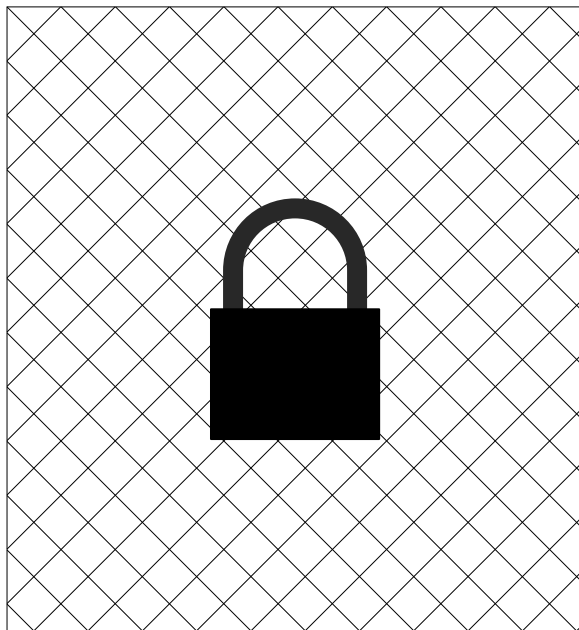
<http://www.recompile.se/mandos>

/boot






Server

(rest of disk)

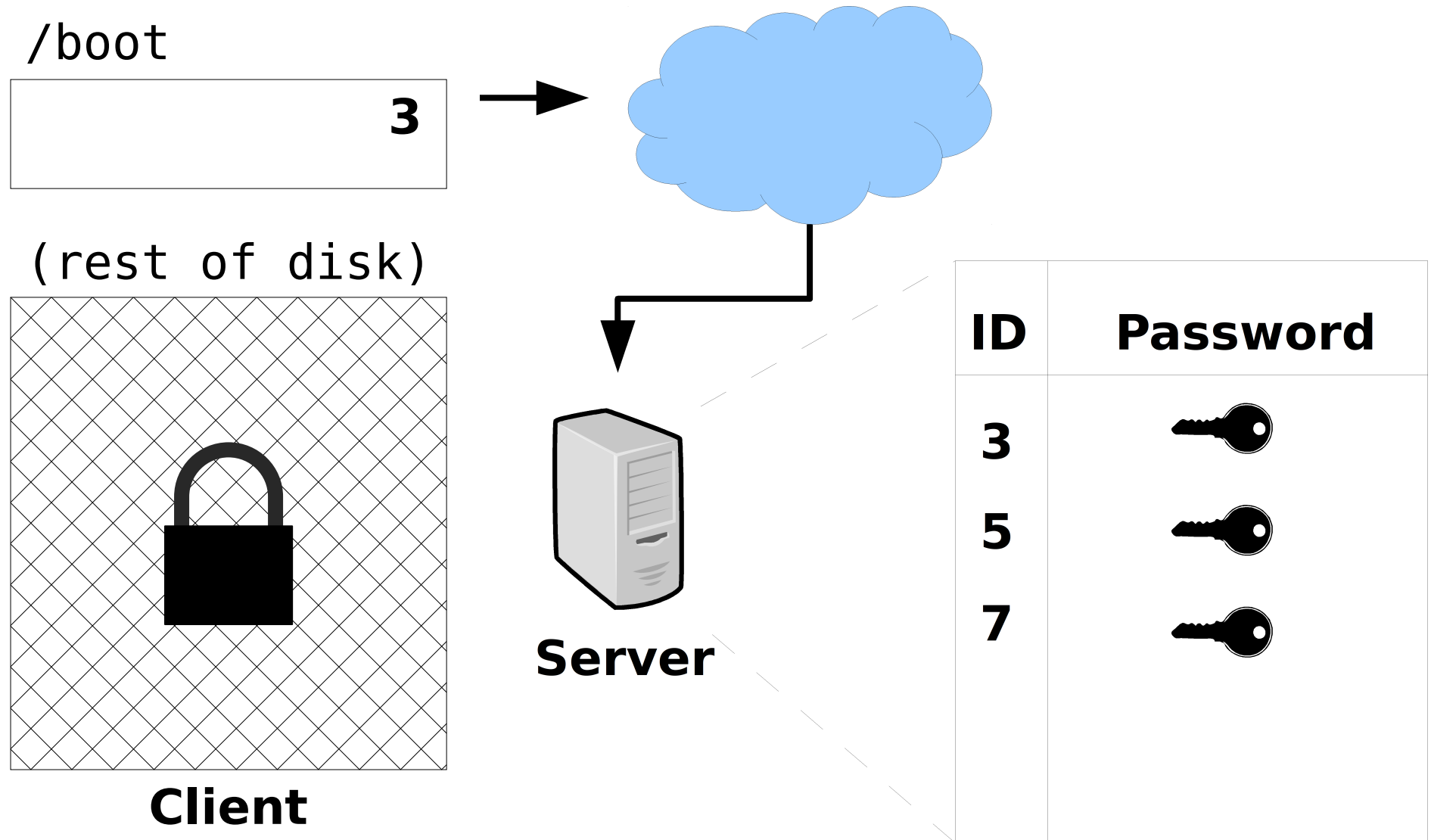


Client

	Password
	
	
	

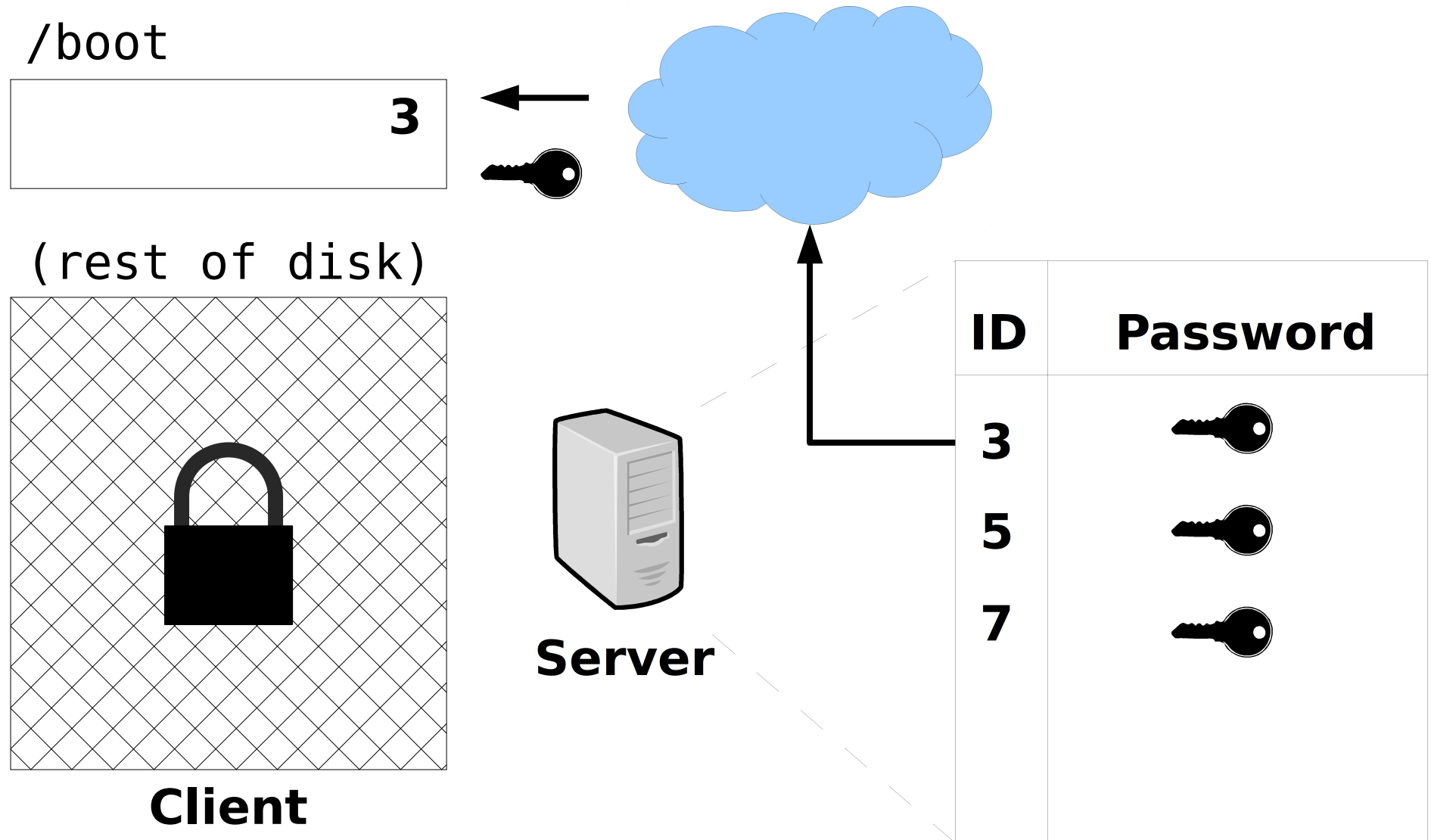
Mandos

<http://www.recompile.se/mandos>



Mandos

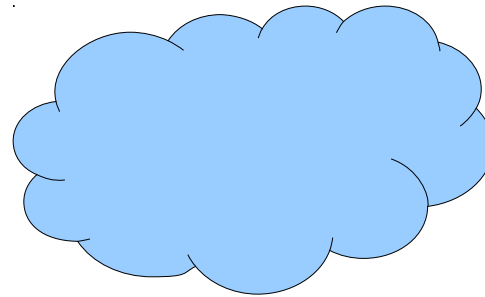
<http://www.recompile.se/mandos>



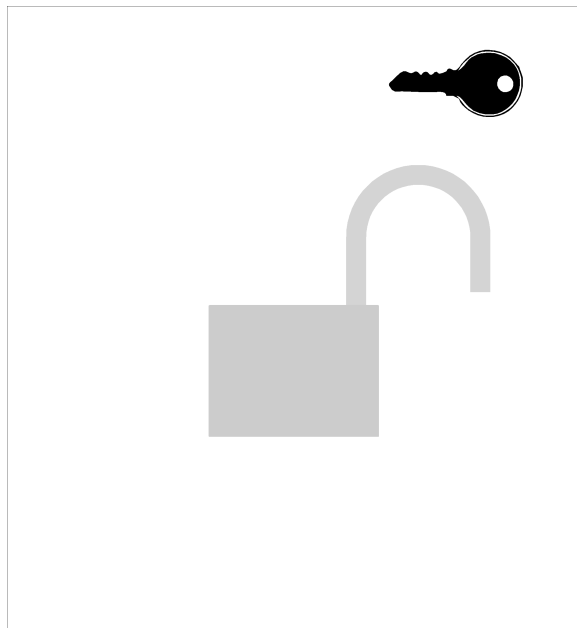
Mandos

<http://www.recompile.se/mandos>

/boot



(rest of disk)



Client

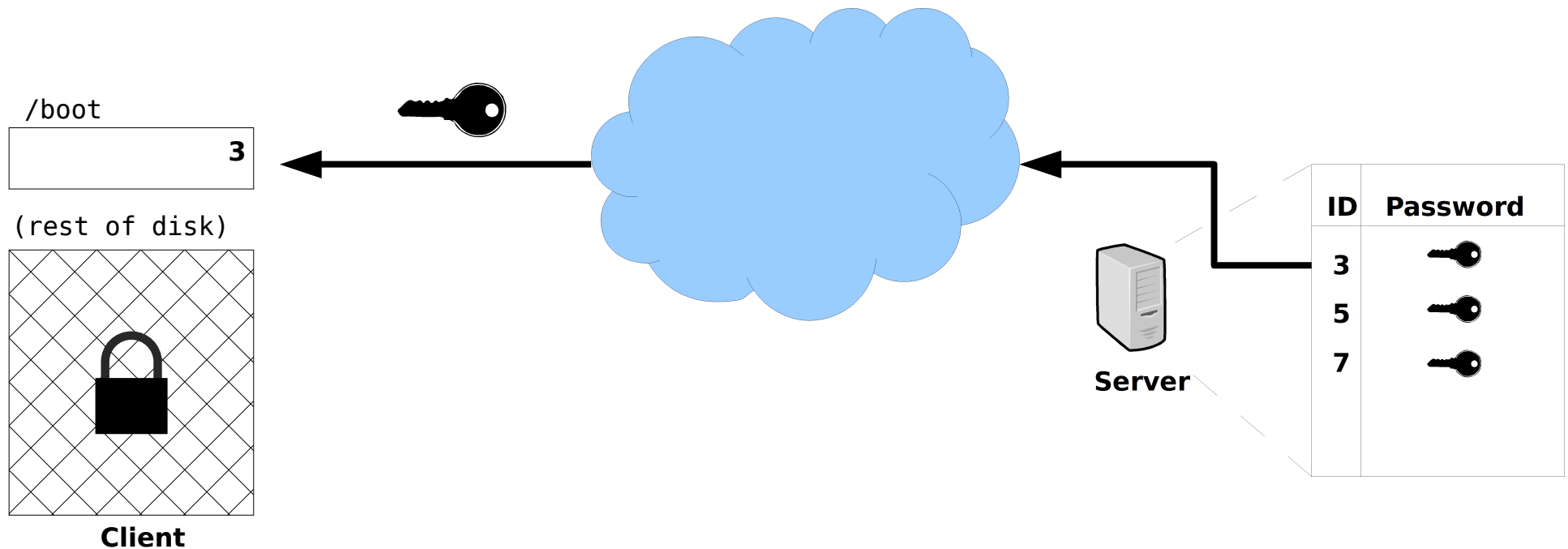


Server

ID	Key
3	
5	
7	

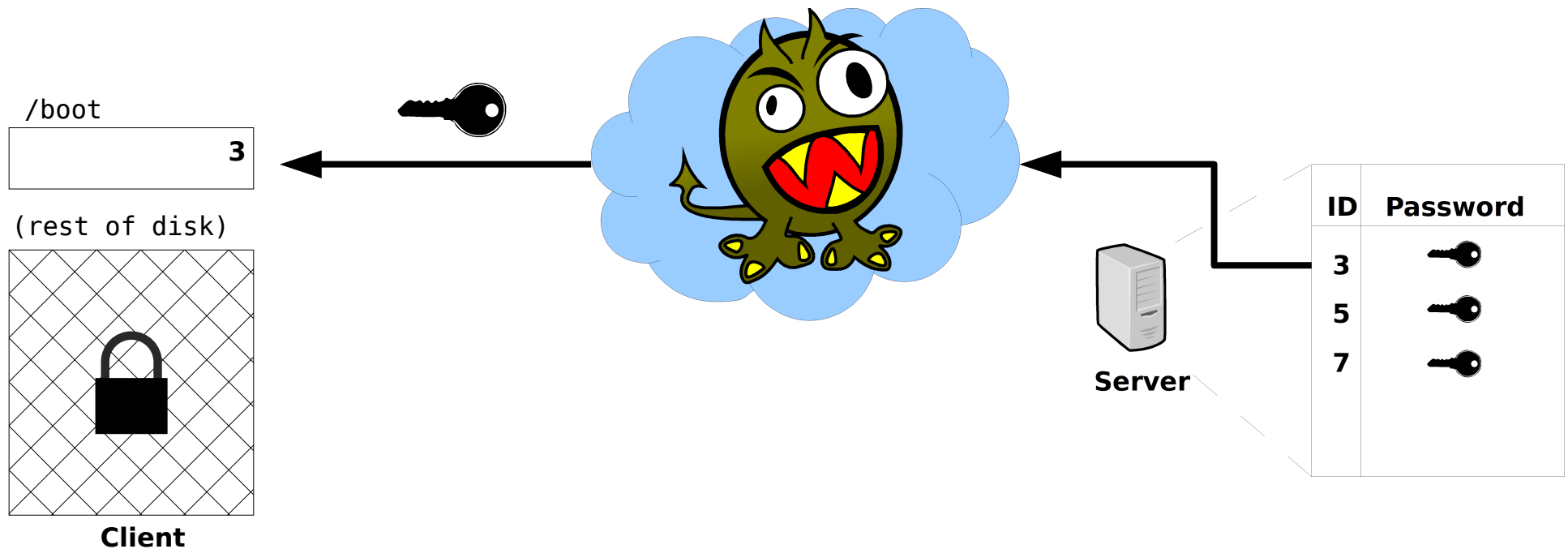
Mandos

<http://www.recompile.se/mandos>



Mandos

<http://www.recompile.se/mandos>



“GPG for data at rest. TLS for data in motion.”

If You're Typing The Letters A-E-S Into Your Code, You're Doing It Wrong
<http://www.cs.berkeley.edu/~daw/teaching/cs261-f12/misc/if.html>

TLS has a “server” side and a “client” side,
and the “server” side *needs* a key.

The TLS key can be a X.509 certificate

X.509:

“Someone tried to explain public-key-based authentication to aliens. Their universal translators were broken and they had to gesture a lot.”

— Peter Gutmann

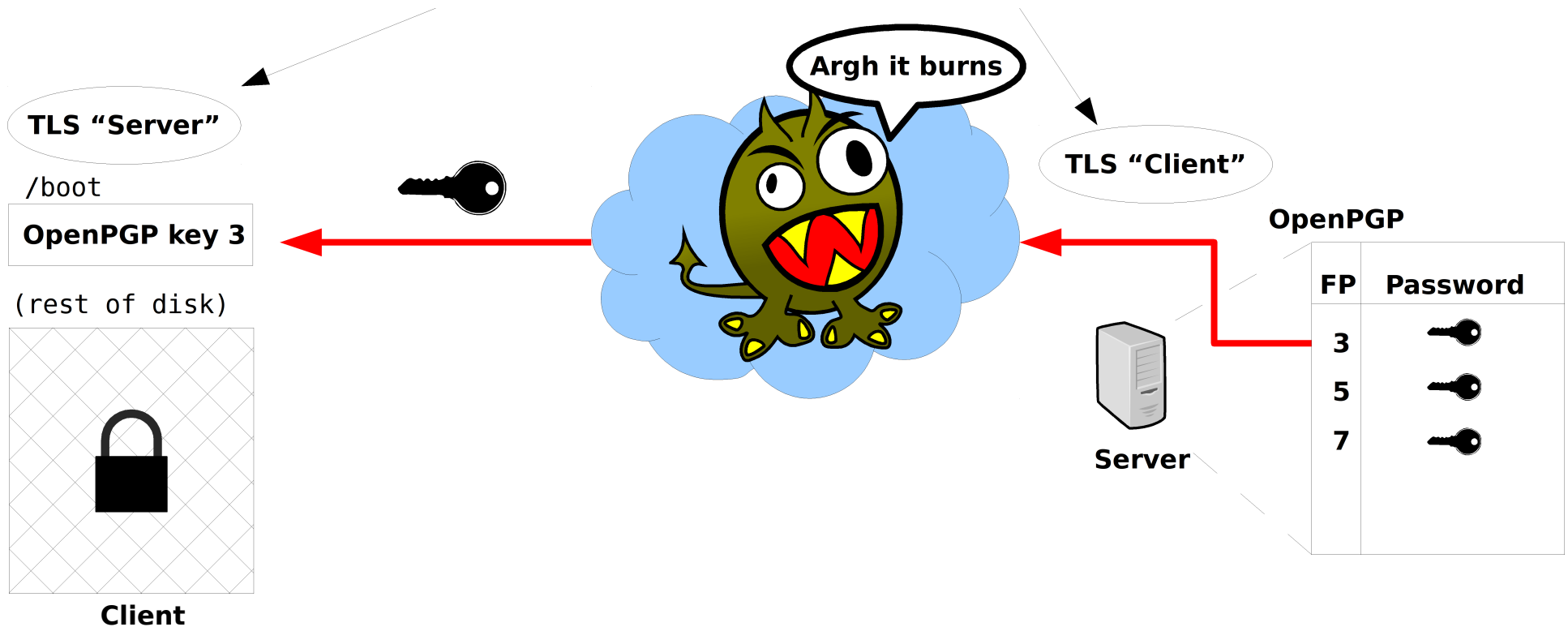
Everything you Never Wanted to Know about PKI but were Forced to Find Out

Alternatively, the TLS key can be an
OpenPGP key

Mandos

<http://www.recompile.se/mandos>

TLS for data in motion

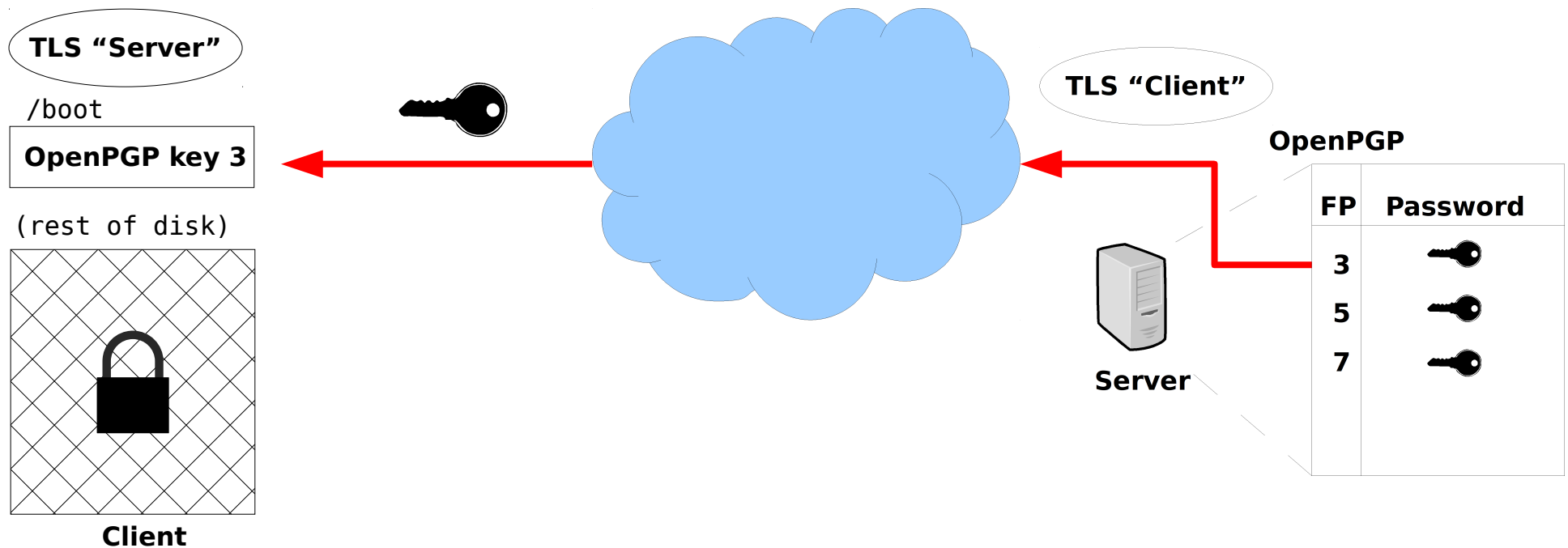


“GPG for data at rest”?

Mandos

<http://www.recompile.se/mandos>

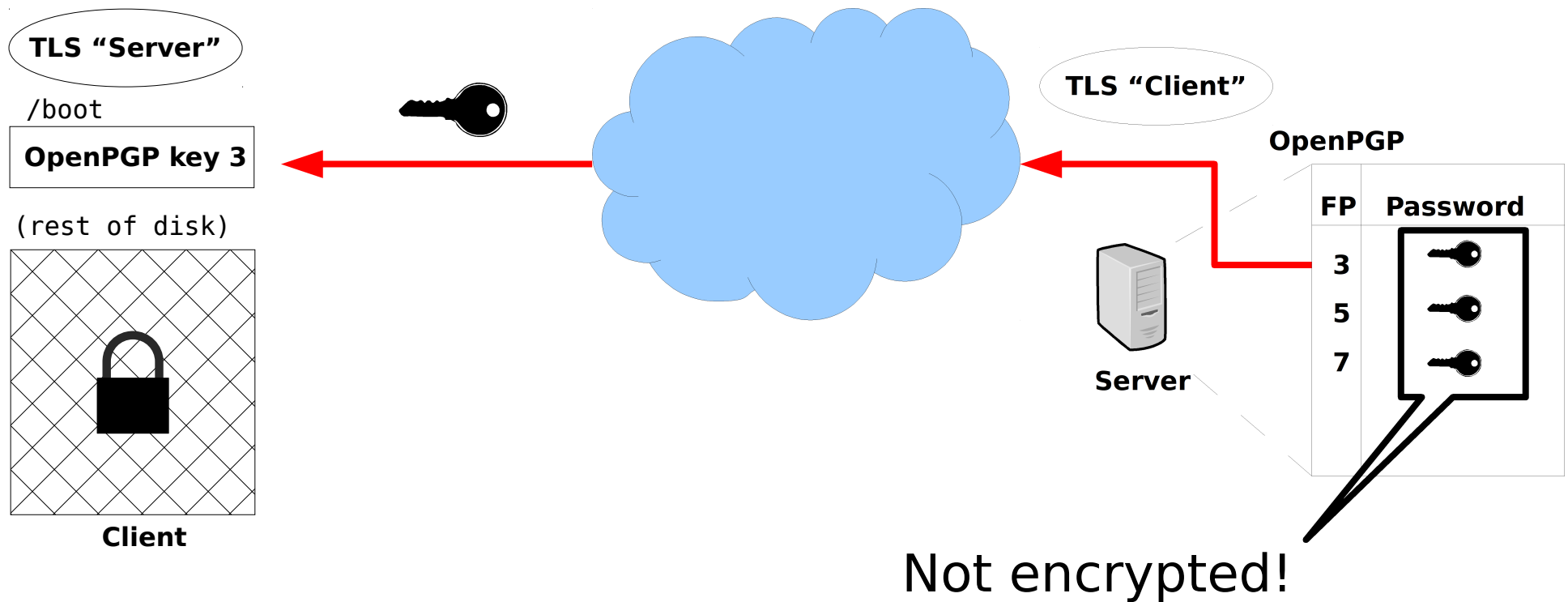
TLS for data in motion



Mandos

<http://www.recompile.se/mandos>

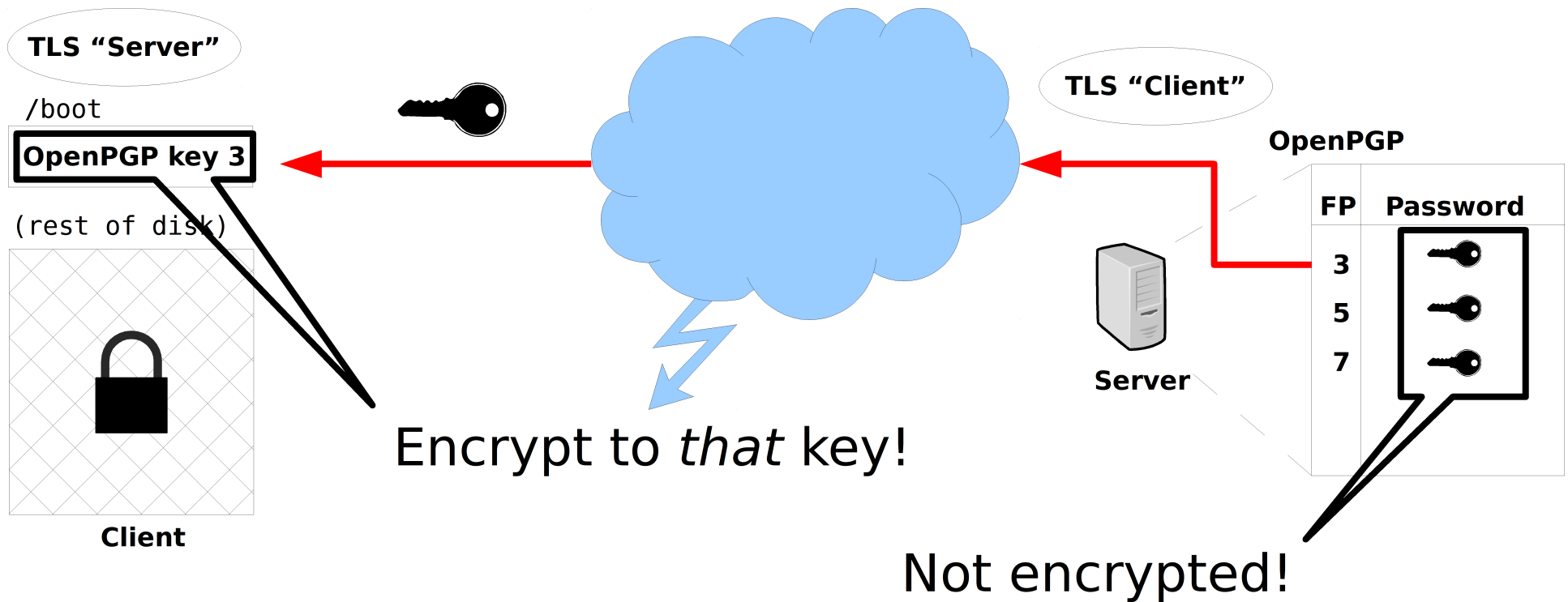
TLS for data in motion



Mandos

<http://www.recompile.se/mandos>

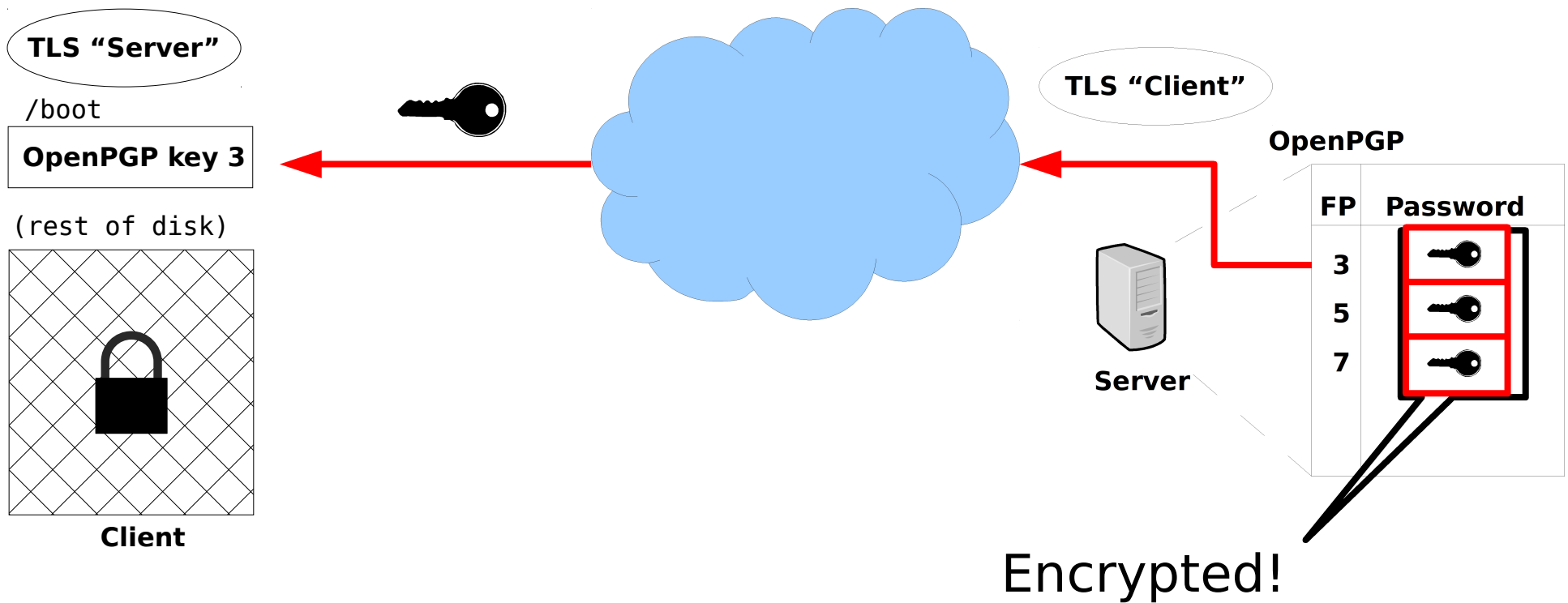
TLS for data in motion



Mandos

<http://www.recompile.se/mandos>

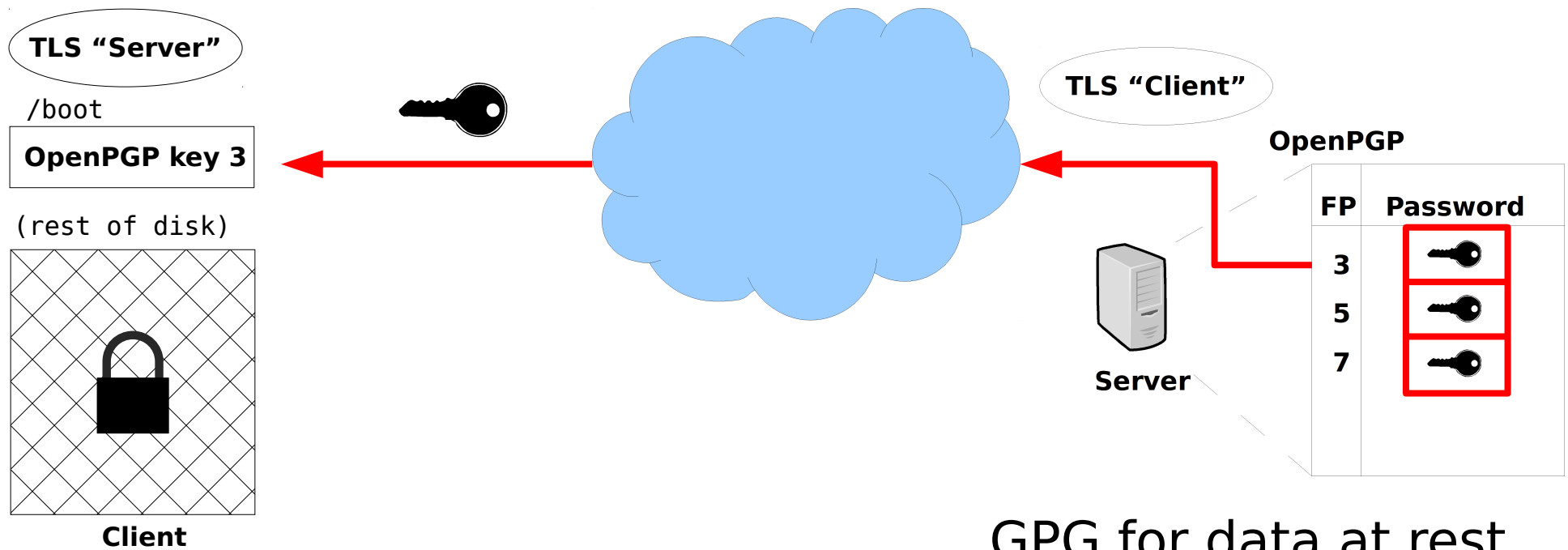
TLS for data in motion



Mandos

<http://www.recompile.se/mandos>

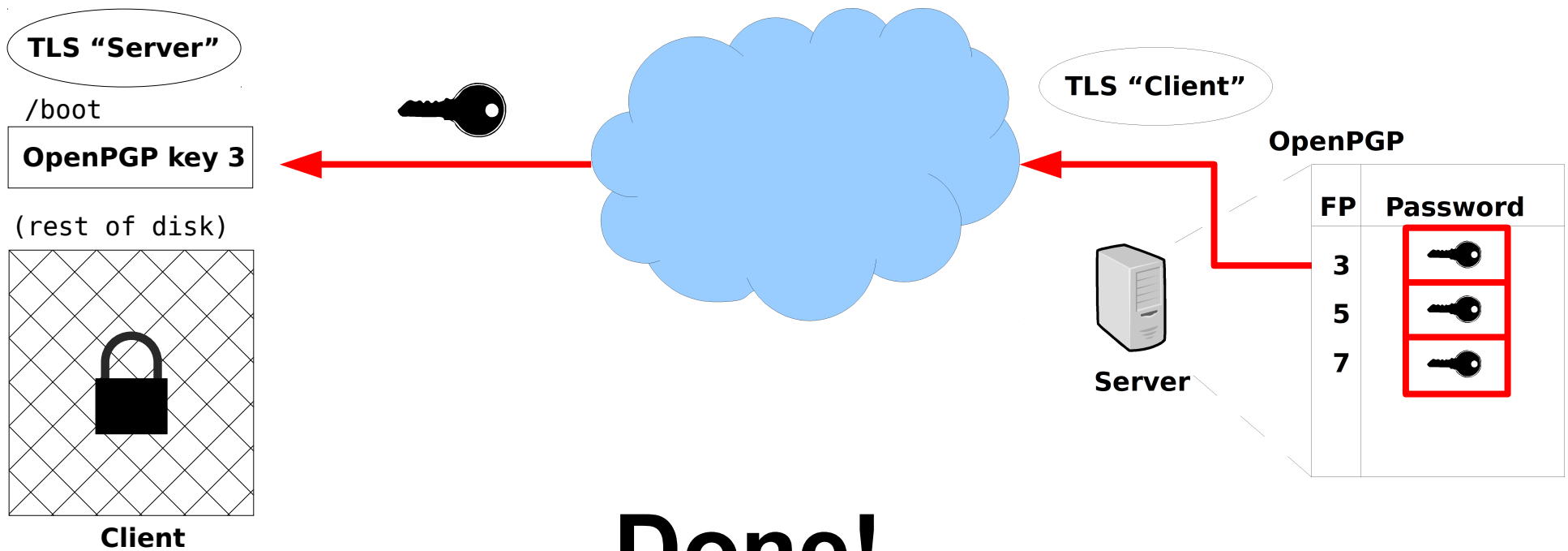
TLS for data in motion



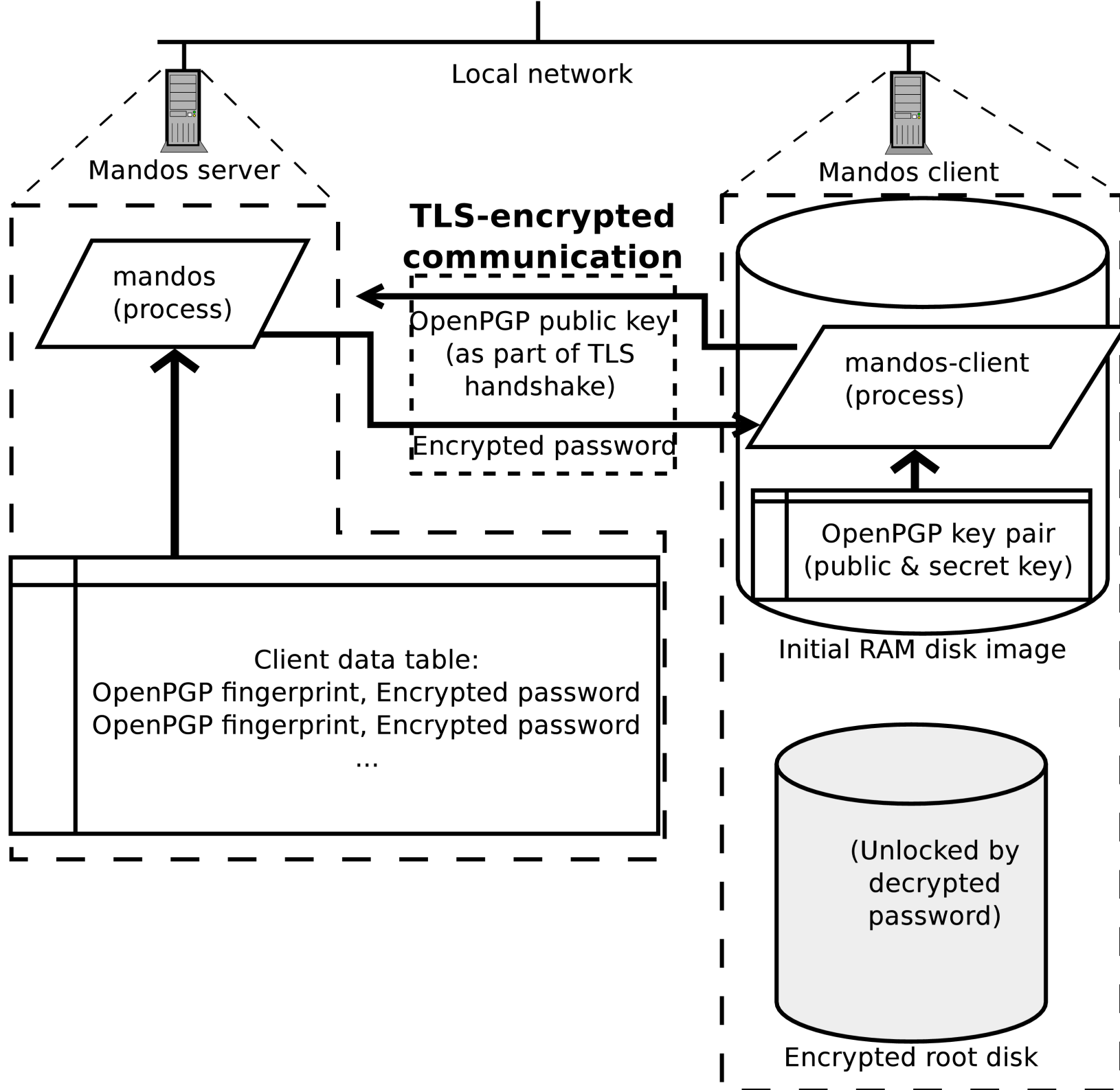
GPG for data at rest

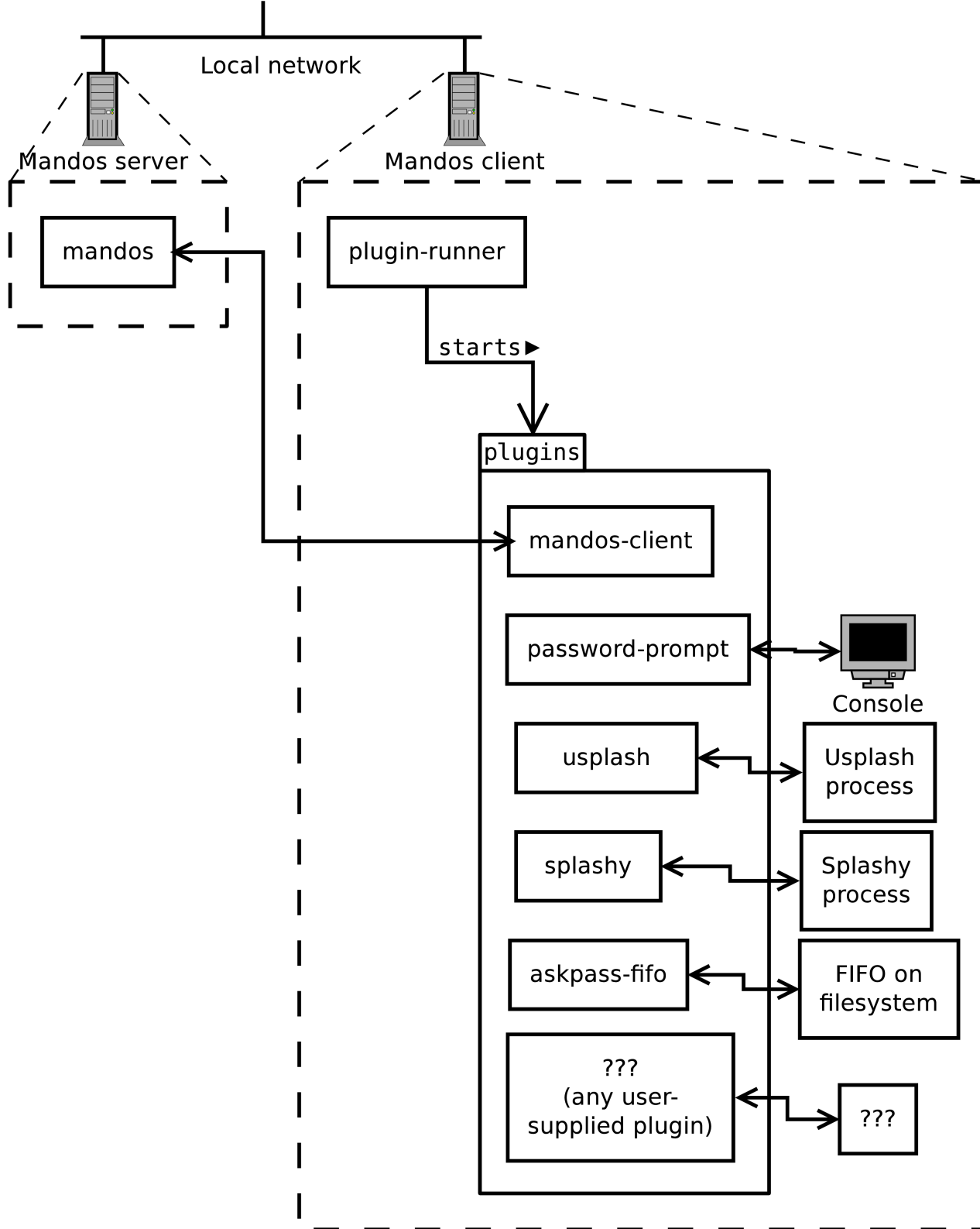
Mandos

<http://www.recompile.se/mandos>



Done!





FAQ

Grabbing the Mandos client key from the /boot partition's `initramfs` image really quickly?

Mandos

<http://www.recompile.se/mandos>

- **In Ubuntu “universe” since 2009**
- **In Debian since 2011**

```
aptitude install mandos
```

```
aptitude install mandos-client
```

Mandos

<http://www.recompile.se/mandos>

The image shows a browser window displaying the Mandos wiki page. The browser's address bar shows the URL <https://wiki.recompile.se/wiki/Mandos>. The page content includes a navigation menu with options like 'page', 'discussion', 'view source', and 'history'. The main heading is 'Mandos', followed by a description: 'Mandos is a system for allowing servers with encrypted root file systems to reboot *unattended and/or remotely*. See [the manual](#) for more information, including an FAQ list.' Below this, it states 'Mandos is Free Software, licensed using the [GNU General Public License v3](#) or later.' and includes a quote from *The Halls of Mandos*. A 'GPLv3 Free Software' logo is visible on the right. Two green callout boxes are overlaid on the page: one labeled 'Download' and another labeled 'Documentation' containing a list of links: 'Intro & FAQ', 'Diagrams', 'Manual pages', and 'Support'. The left sidebar contains sections for 'navigation' (Main page, Recent changes, Random page), 'search' (input field, Go, Search), and 'tools' (What links here, Related changes, Special pages, Printable version, Permanent link).

Mandos

<http://www.recompile.se/mandos>

<http://ftp.recompile.se/pub/mandos/misc>

Mandos

<http://www.recompile.se/mandos>

Disk encryption is essential for physical computer security, but seldom used due to the trouble of remembering and typing a password at every restart. We describe Mandos, a program which solves this problem, its security model, and the underlying concepts of its design.

Any security system must have a clear view of its intended threat model - i.e. what threats it is actually intended to protect against; the specific choices and tradeoffs made for Mandos will be explained. Another danger of security system design is the risk of its non-use; i.e. that the system will not be used for some real or perceived drawbacks, such as complexity. The deliberate design choices of Mandos, involving low-interaction, "invisible" and automatic features, will be covered.

Mandos

<http://www.recompile.se/mandos>

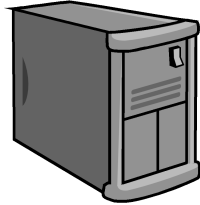
TL;DL

```
aptitude install mandos
```

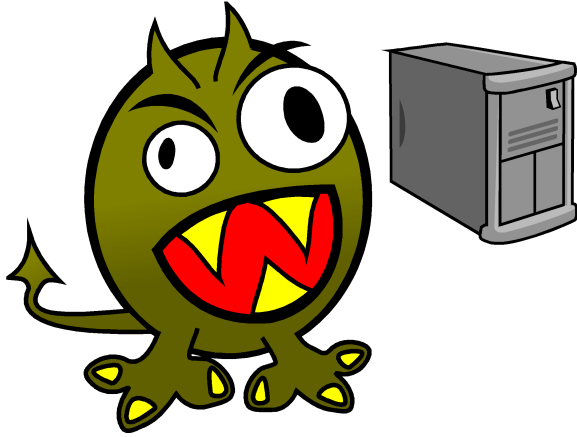
```
aptitude install mandos-client
```

Threat Model

Threat Model



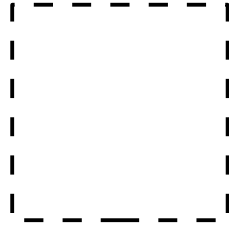
Threat Model



Threat Model

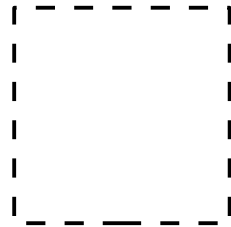


Threat Model



No Server

Threat Model



No Server



Sad users

Threat Model



[!] Partition disks

The installer can guide you through partitioning a disk (using different standard schemes) or, if you prefer, you can do it manually. With guided partitioning you will still have a chance later to review and customise the results.

If you choose guided partitioning for an entire disk, you will next be asked which disk should be used.

Partitioning method:

Guided - use entire disk

Guided - use entire disk and set up LVM

Guided - use entire disk and set up encrypted LVM

Manual

<Go Back>

<Tab> moves between items; <Space> selects; <Enter> activates buttons

Booting the kernel.

Loading, please wait...

Volume group "glorfindel" not found

Volume group "glorfindel" not found

Enter passphrase to unlock the disk /dev/hda2 (hda2_crypt): _

Kernel alive

kernel direct mapping tables up to 100000000 @ 8000-d000

Threat Model



New threat: non-use

**Inconvenient
Burdensome
“I’ll do it some day”**

Mail servers especially common to not be encrypted. Co-location make passwords inconvenient.

New threat:



Security needs to be *transparent*

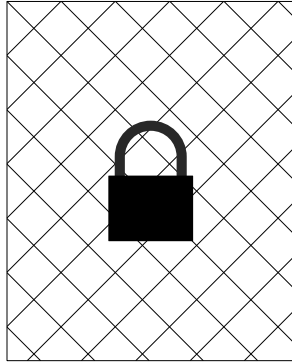
Model after IPsec.
User behavior can stay unchanged.

Full Disk Encryption

/boot



(rest of disk)

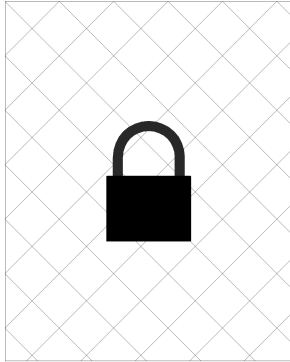


Full Disk Encryption

/boot



(rest of disk)

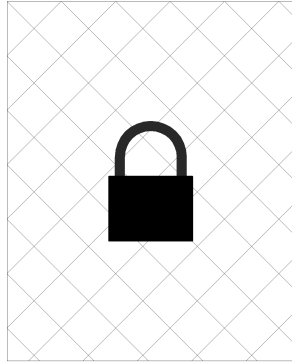


Full Disk Encryption

/boot



(rest of disk)

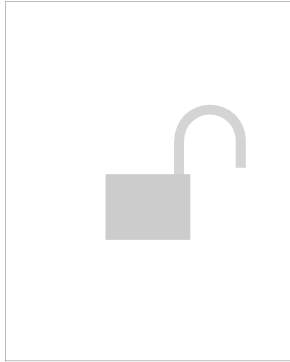


Full Disk Encryption

/boot



(rest of disk)



Mandos

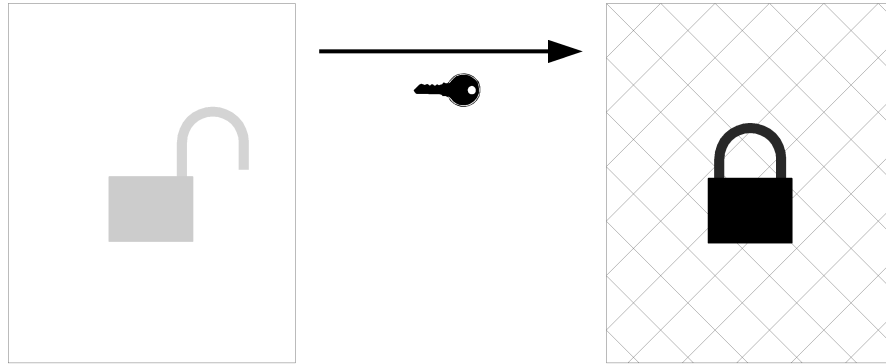
<http://www.recompile.se/mandos>

Servers provide passwords to *each other*

Mandos

<http://www.recompile.se/mandos>

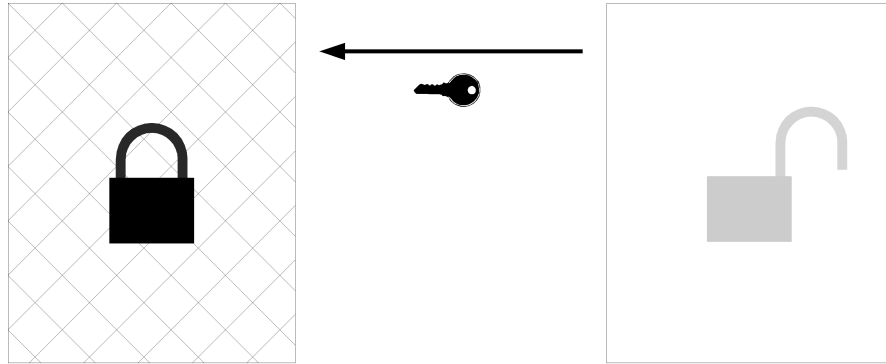
Normal operation



Mandos

<http://www.recompile.se/mandos>

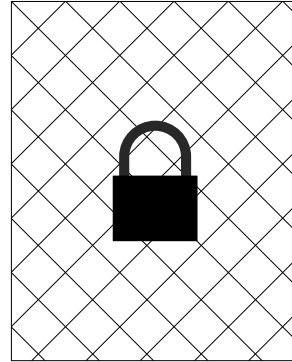
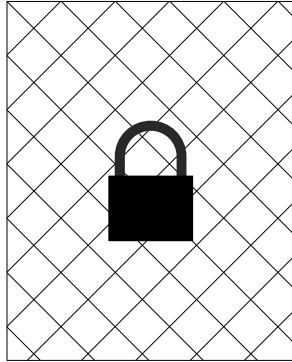
Normal operation



Mandos

<http://www.recompile.se/mandos>

Lockdown state
Administrator attention required



Deadlock / bootstrap problem as security feature!

This is the usual state when you really need encryption.

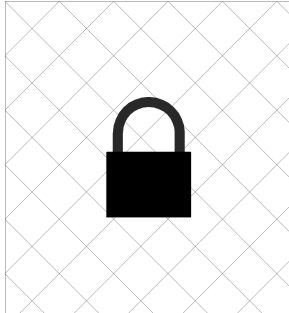
Mandos

<http://www.recompile.se/mandos>

/boot



(rest of disk)



Client

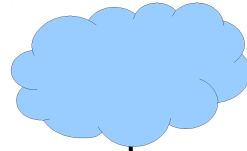


Server

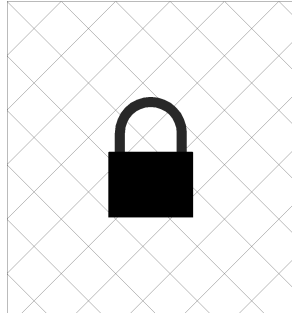
Mandos

<http://www.recompile.se/mandos>

/boot



(rest of disk)



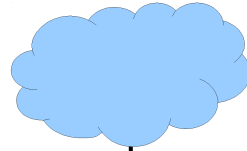
Server

Client

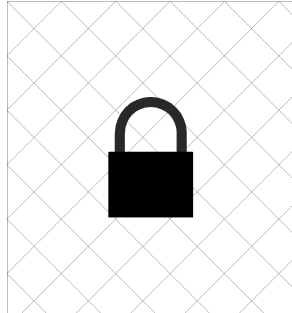
Mandos

<http://www.recompile.se/mandos>

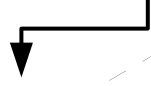
/boot



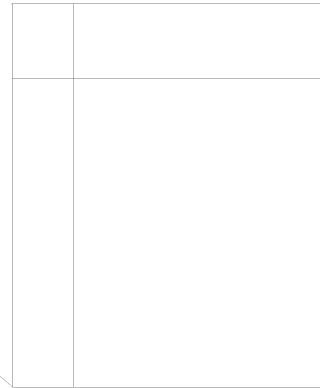
(rest of disk)



Client



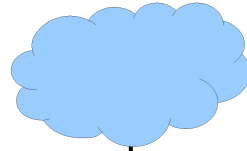
Server



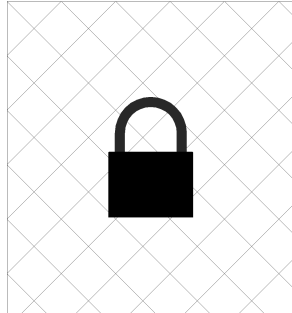
Mandos

<http://www.recompile.se/mandos>

/boot



(rest of disk)






Client



Server

Password



Password	
	
	
	

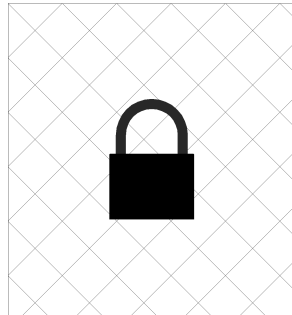
Mandos

<http://www.recompile.se/mandos>

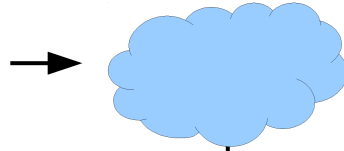
/boot






(rest of disk)



Client



Server

ID	Password
3	
5	
7	

Mandos

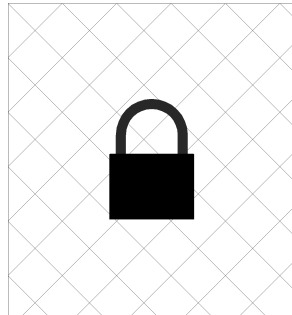
<http://www.recompile.se/mandos>

/boot

3



(rest of disk)



Client



Server

ID	Password
3	
5	
7	

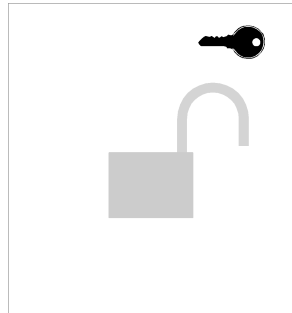
Mandos

<http://www.recompile.se/mandos>

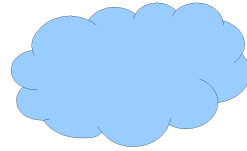
/boot

3




(rest of disk)



Client

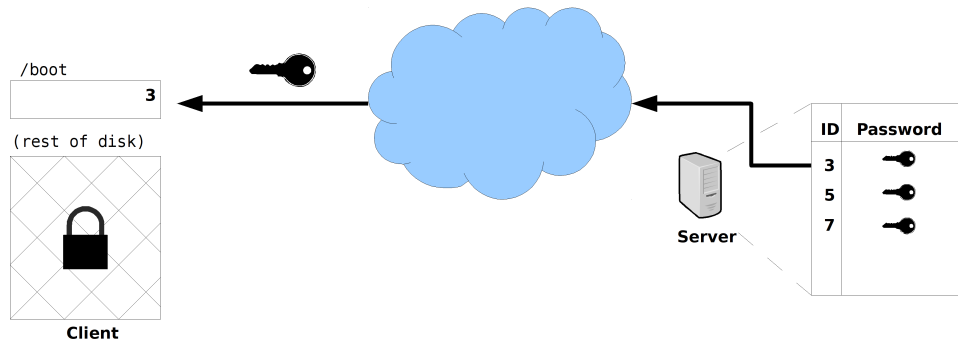


Server

ID	Key
3	
5	
7	

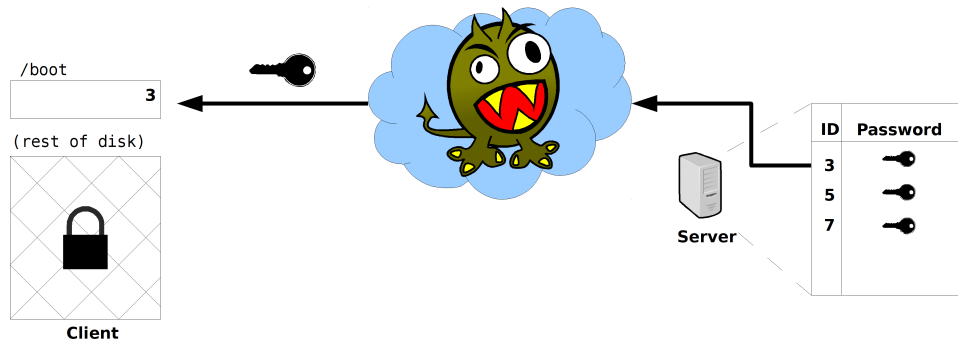
Mandos

<http://www.recompile.se/mandos>



Mandos

<http://www.recompile.se/mandos>



“GPG for data at rest. TLS for data in motion.”

If You're Typing The Letters A-E-S Into Your Code, You're Doing It Wrong
<http://www.cs.berkeley.edu/~daw/teaching/cs261-f12/misc/if.html>

TLS has a “server” side and a “client” side,
and the “server” side needs a key.

The TLS key can be a X.509 certificate

X.509:

“Someone tried to explain public-key-based authentication to aliens. Their universal translators were broken and they had to gesture a lot.”

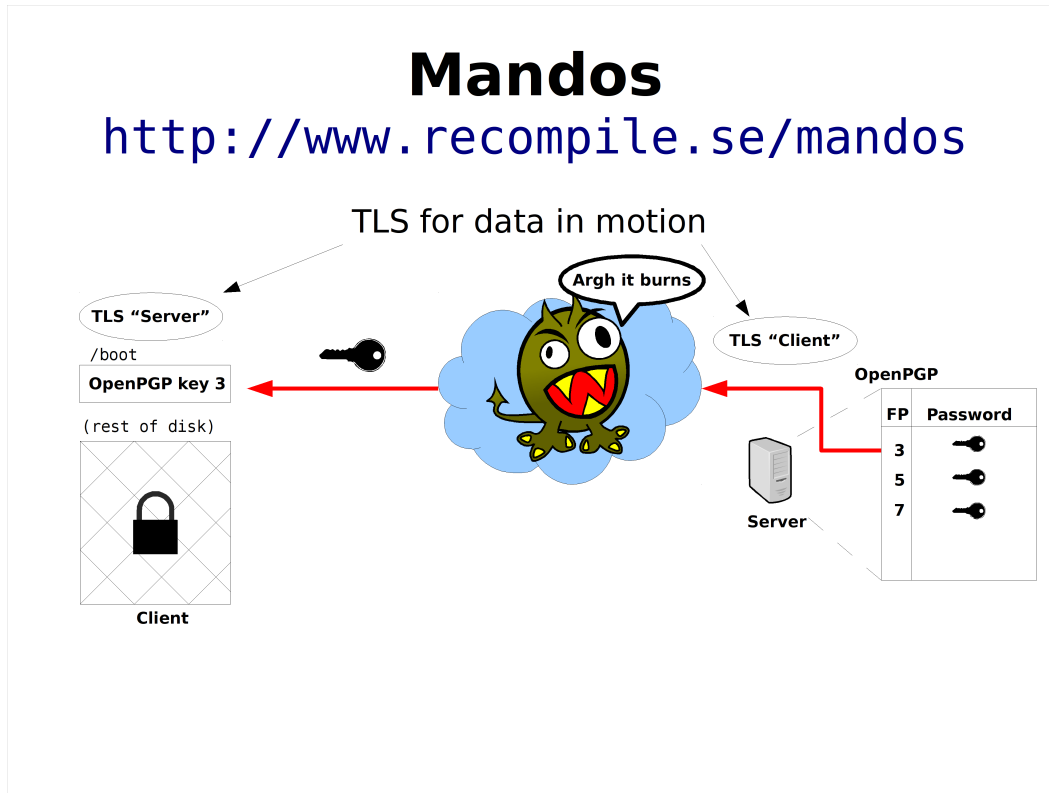
— Peter Gutmann

Everything you Never Wanted to Know about PKI but were Forced to Find Out

Alternatively, the TLS key can be an
OpenPGP key

Mandos

<http://www.recompile.se/mandos>



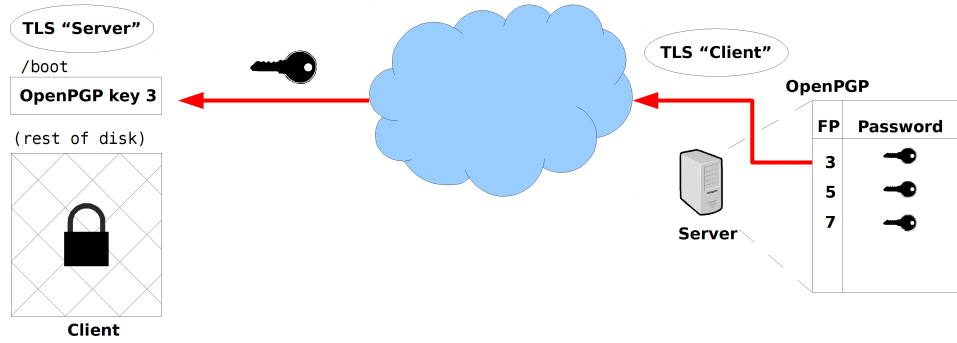
“FP” means fingerprint

“GPG for data at rest”?

Mandos

<http://www.recompile.se/mandos>

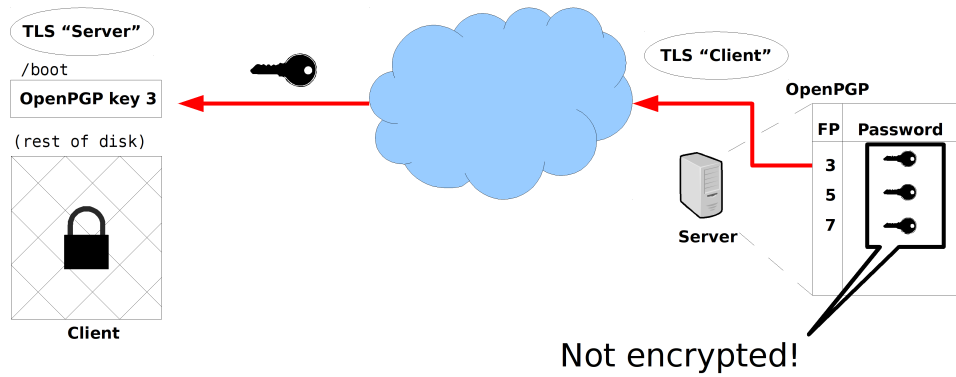
TLS for data in motion



Mandos

<http://www.recompile.se/mandos>

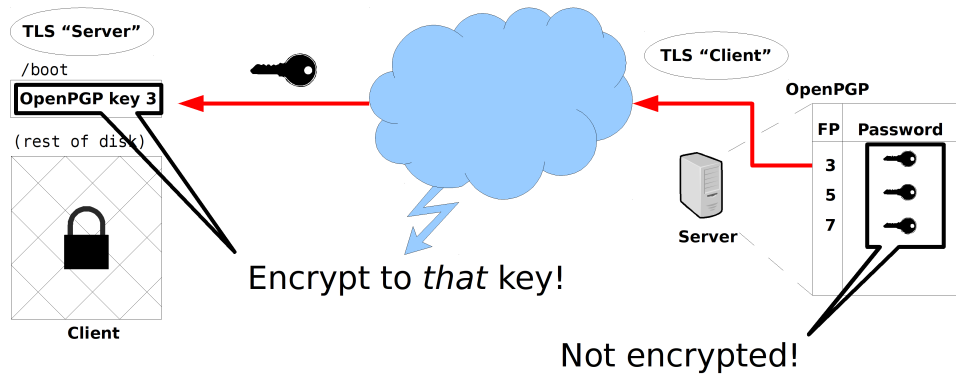
TLS for data in motion



Mandos

<http://www.recompile.se/mandos>

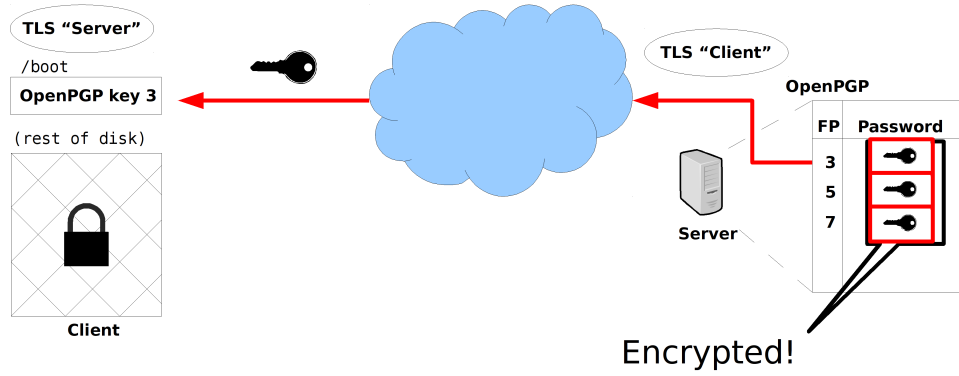
TLS for data in motion



Mandos

<http://www.recompile.se/mandos>

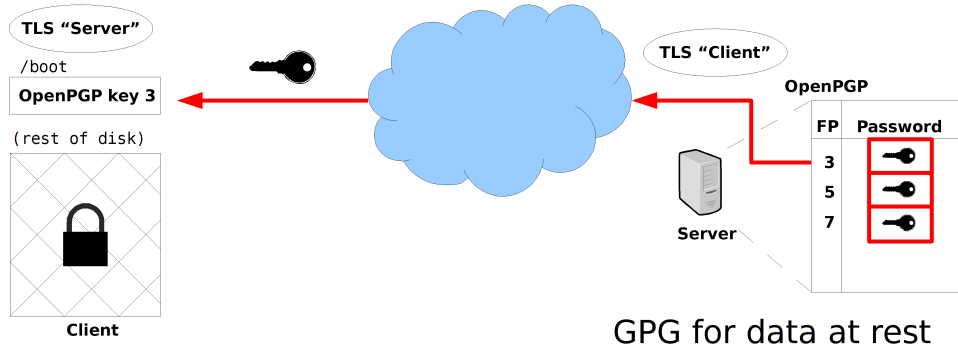
TLS for data in motion



Mandos

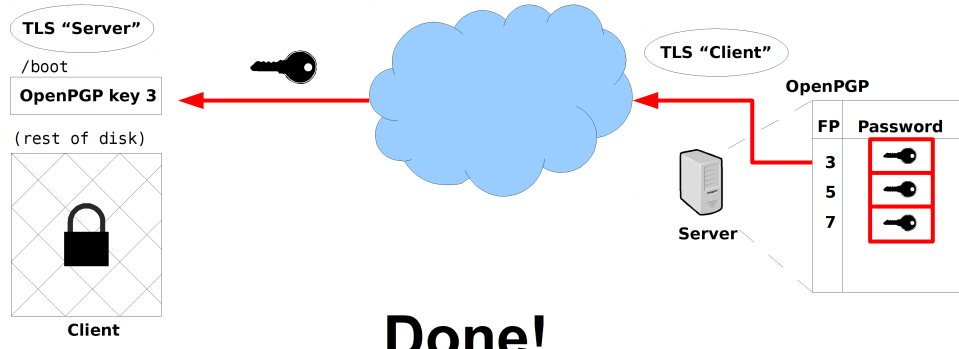
<http://www.recompile.se/mandos>

TLS for data in motion

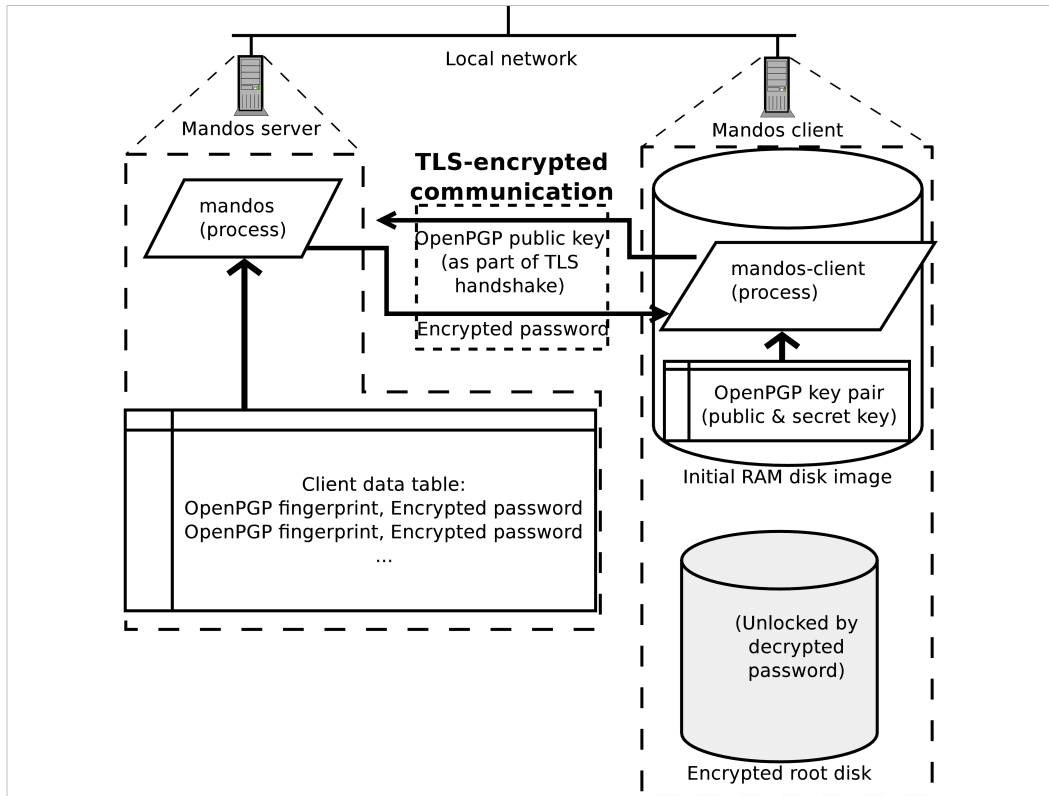


Mandos

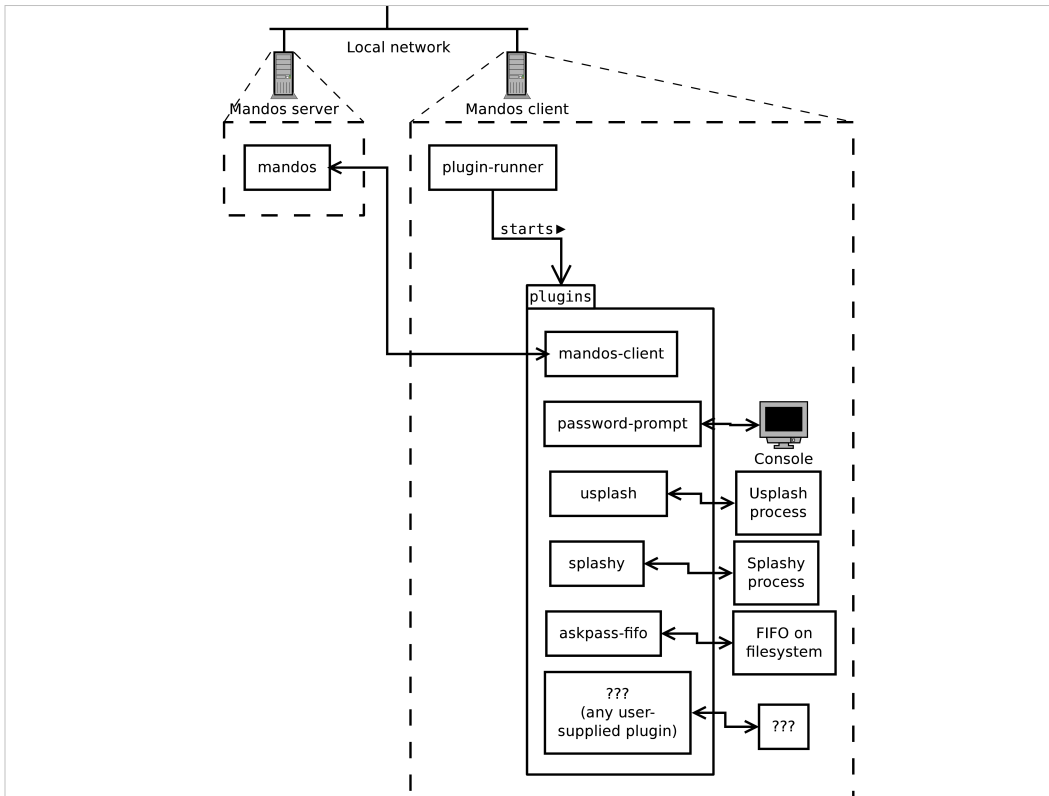
<http://www.recompile.se/mandos>



Finished



Older diagram attempting to show the same thing



Client-side process model with plugins for various input methods, etc.

FAQ

Grabbing the Mandos client key from the /boot partition's initramfs image really quickly?

Threat model: people grabbing servers fast. Sophisticated attackers can and will do cold-boot.

Mandos shrinks the window of opportunity to default 5 minutes, customizable

Mandos

<http://www.recompile.se/mandos>

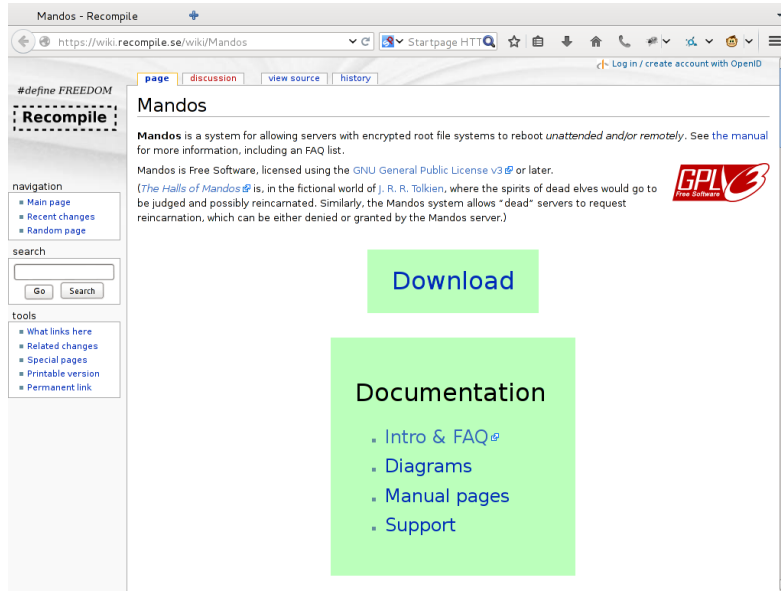
- **In Ubuntu “universe” since 2009**
- **In Debian since 2011**

```
aptitude install mandos
```

```
aptitude install mandos-client
```

Mandos

<http://www.recompile.se/mandos>



The screenshot shows a web browser window displaying the Mandos page on the recompile.se wiki. The browser's address bar shows the URL <https://wiki.recompile.se/wiki/Mandos>. The page content includes a navigation sidebar on the left with sections for navigation, search, and tools. The main content area features the title "Mandos", a description of the system, and a GPL logo. Two green navigation boxes are overlaid on the page: one for "Download" and another for "Documentation" with a list of links.

#define FREEDOM

Recompile

navigation

- [Main page](#)
- [Recent changes](#)
- [Random page](#)

search

Go Search

tools

- [What links here](#)
- [Related changes](#)
- [Special pages](#)
- [Printable version](#)
- [Permanent link](#)

Mandos

Mandos is a system for allowing servers with encrypted root file systems to reboot *unattended and/or remotely*. See the [manual](#) for more information, including an FAQ list.

Mandos is Free Software, licensed using the [GNU General Public License v3](#) or later.

(*The Halls of Mandos* is, in the fictional world of J. R. R. Tolkien, where the spirits of dead elves would go to be judged and possibly reincarnated. Similarly, the Mandos system allows "dead" servers to request reincarnation, which can be either denied or granted by the Mandos server.)

Download

Documentation

- [Intro & FAQ](#)
- [Diagrams](#)
- [Manual pages](#)
- [Support](#)

Mandos

<http://www.recompile.se/mandos>

<http://ftp.recompile.se/pub/mandos/misc>

These slides and more