Mandos
Disk encryption without passwords

Teddy Hogeborn, Björn Påhlsson

2020-01-29
When to use Mandos?

1. Physical/bare metal hardware?
2. More than just one physical machine?
3. Want to use full-disk encryption?

You should use Mandos!
Don’t already use full-disk encryption?

You should!
What is Mandos?

One running machine sends password to other rebooting machine

Two (or more) machines can keep each other up

No interactivity needed

- Reboot while you sleep
  - Kernel upgrade
  - Kernel panic
  - Power glitch
  - Watchdog
  - etc.
Noninteractivity

Vital feature!
Set it and forget it; reboot normally
Mandos Features

Supports major initramfs image builders:

- initramfs-tools
- dracut, both with and without systemd

Server controllable by D-Bus

- D-Bus API fully documented
- Command-line utilities provided
But anyone could just...

No they couldn’t.

- TLS-encrypted communication (with PFS)
- OpenPGP-encrypted payload
But what if…

Threat model?
- Smash & grab

Fails safe!
Threat models (continued)

What is your realistic threat model?

Mandos will always be better than no encryption!
OK, but in theory, you could...

Yes, OK, you could.

- But again, what is your threat model?

Sophisticated attackers?

- Could just as well do a cold-boot attack

Mandos can ask for manual approval for every boot
Installing Mandos

```
apt install mandos-client
Then, read
/usr/share/doc/mandos-client/README.Debian.gz

apt install mandos

Latest version (recommended):
Instructions at https://www.recompile.se/mandos
```