guld

guld Operating System (guldOS) Specification

Author: Ira Miller <public@iramiller.com>

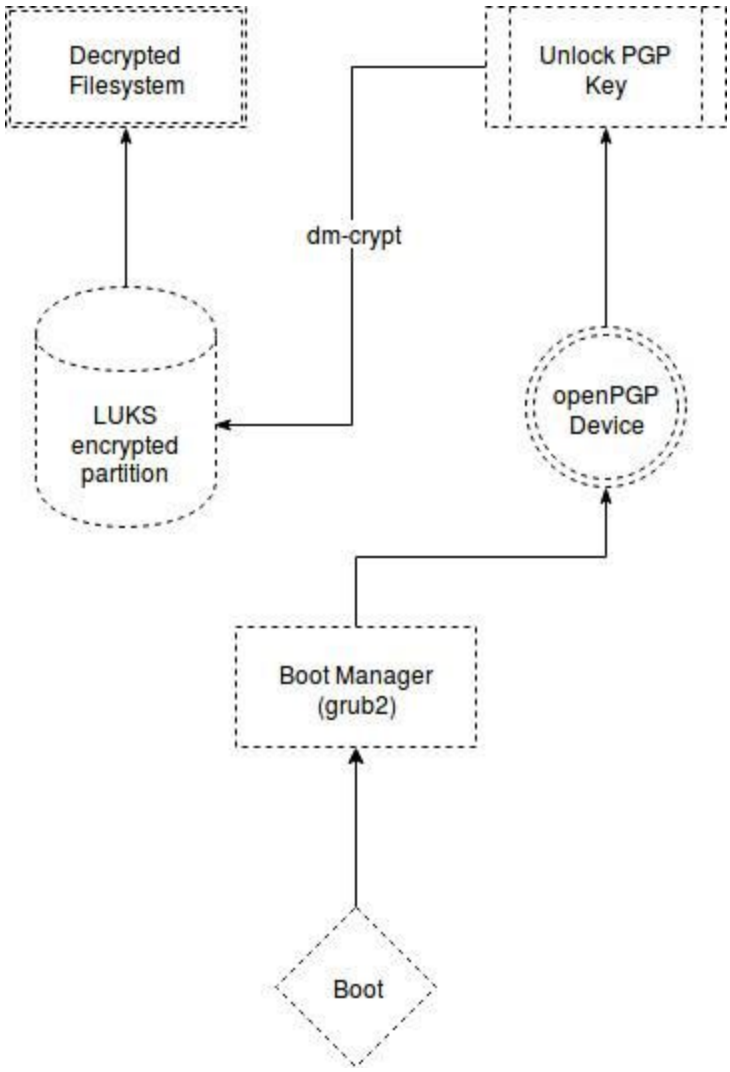
DRAFT
v0.0.1

Overview

The guld Operating System (guldOS) is a security and privacy focused variant of Gentoo Linux.[1] Guld uses Gentoo's package manager (portage) to compile everything from source. The goal of guldOS is to compile a minimum build for each user to do secure signing operations in an environment they can trust.

Disk Encryption

The most distinct functionality of guldOS is around disk encryption. The recommended lowest level filesystem configuration for guldOS is dm-crypt LUKS with a PGP encrypted, detached keyfile.[2]



The keyfile and/or PGP key must be on a second device, preferably a dedicated smart card with openPGP[3] support. In the simplest implementation, this can be a separate partition or a USB drive.

Yubikey[4] is probably the most popular example of an openPGP smart card, but Ledger Wallet[5] also supports cryptocurrency key management, which many guldOS users will find helpful.

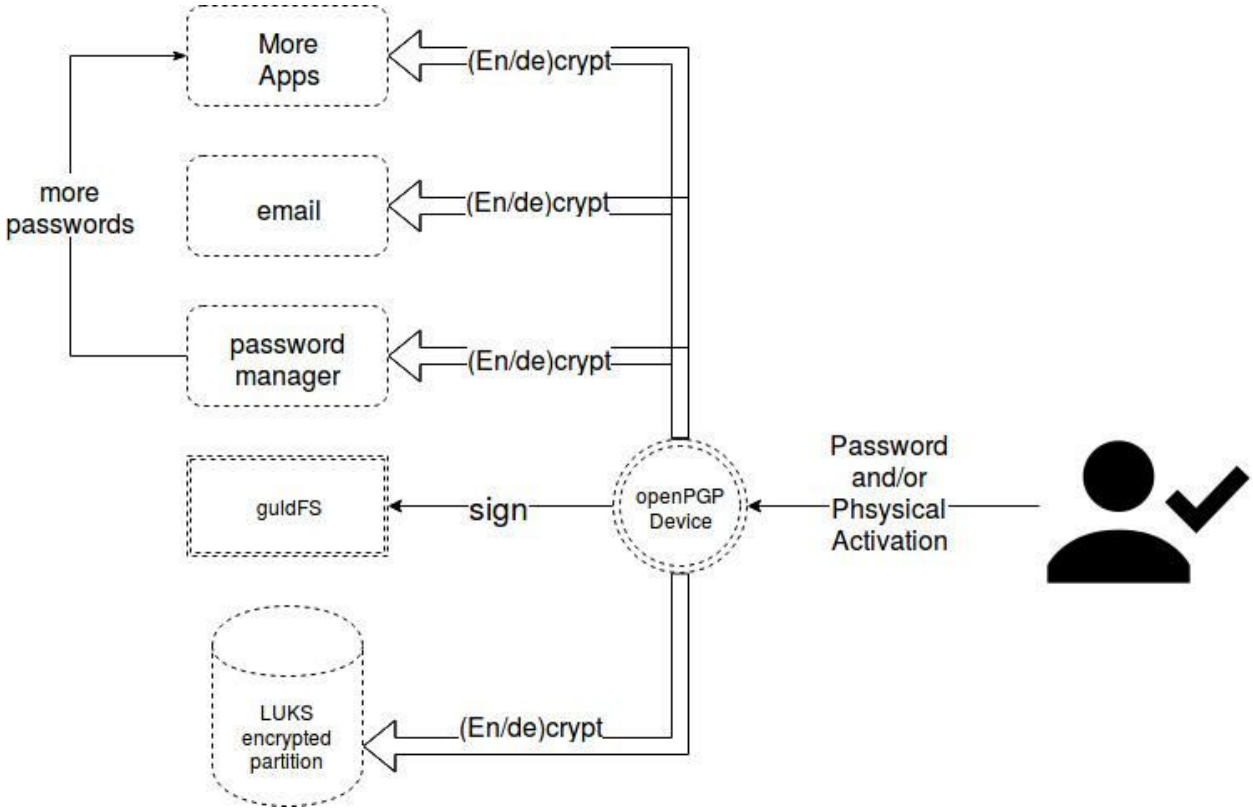
Regardless of what openPGP device is used to unlock the PGP key, the key should then be used to decrypt the LUKS keyfile. The LUKS keyfile is then used to decrypt the partition, which can then be mounted for the user.

---

[1] Gentoo™ the Gentoo Foundation http://gentoo.org/
[2] https://wiki.gentoo.org/wiki/Dm-crypt_full_disk_encryption
[3] http://openpgp.org/
[4] Yubikey™ of Yubico http://yubico.com/
[5] Ledger Wallet™ of Ledger https://www.ledgerwallet.com/

Single Password Environment

Standardization around PGP allows users to fully encrypt their disk using the same key and password that they use at higher levels, such as guldFS[6], as well as with applications like password manager `pass`[7] and with email. This creates an easily managed single password security system for all of the various layers of encryption a user might interact with.



Maintaining this Single Password Environment drives many of the design and application choices throughout guldOS. While it does create a single point of failure, it is the most familiar and practical to expect end users to be able to follow. Furthermore, PGP is so widely supported that the ecosystem of hardware and software options for `openPGP Device` is without equal.

Portage Overlay

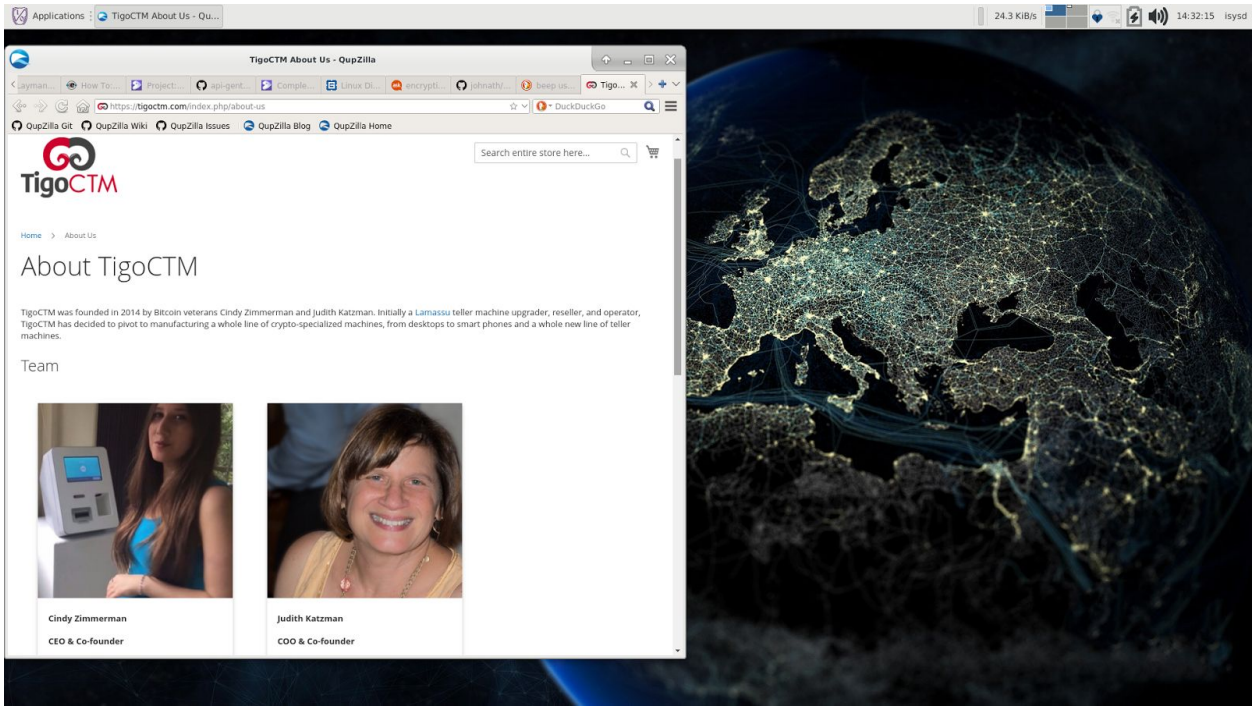
After the crypto layers are configured, guldOS can be treated like any other portage overlay.[8]

[6] Source code coming soon, specification at https://guld.io/guldFS-Specification.pdf
[7] GPG encrypted password manager: https://www.passwordstore.org/
[8] https://overlays.gentoo.org/

The specific choices of applications are to always use source distributions and GPG if possible. Specific applications which are to be emerged are:

- git
- GnuPG
- ledger-cli
- pass
- xfce4
- Offlineimap
- Evolution
- guldFS
- Bitcoin (fork luke-jr build to create plain core)
- Ethereum
- Dash (package needed)

The full list is an order of magnitude longer when including libraries and such (i.e. Berkeley DB 4.8), but these are the most important packages. Some P2P network graphics and guld branding rounds out the user experience



TigoCTM Prototype Screenshot