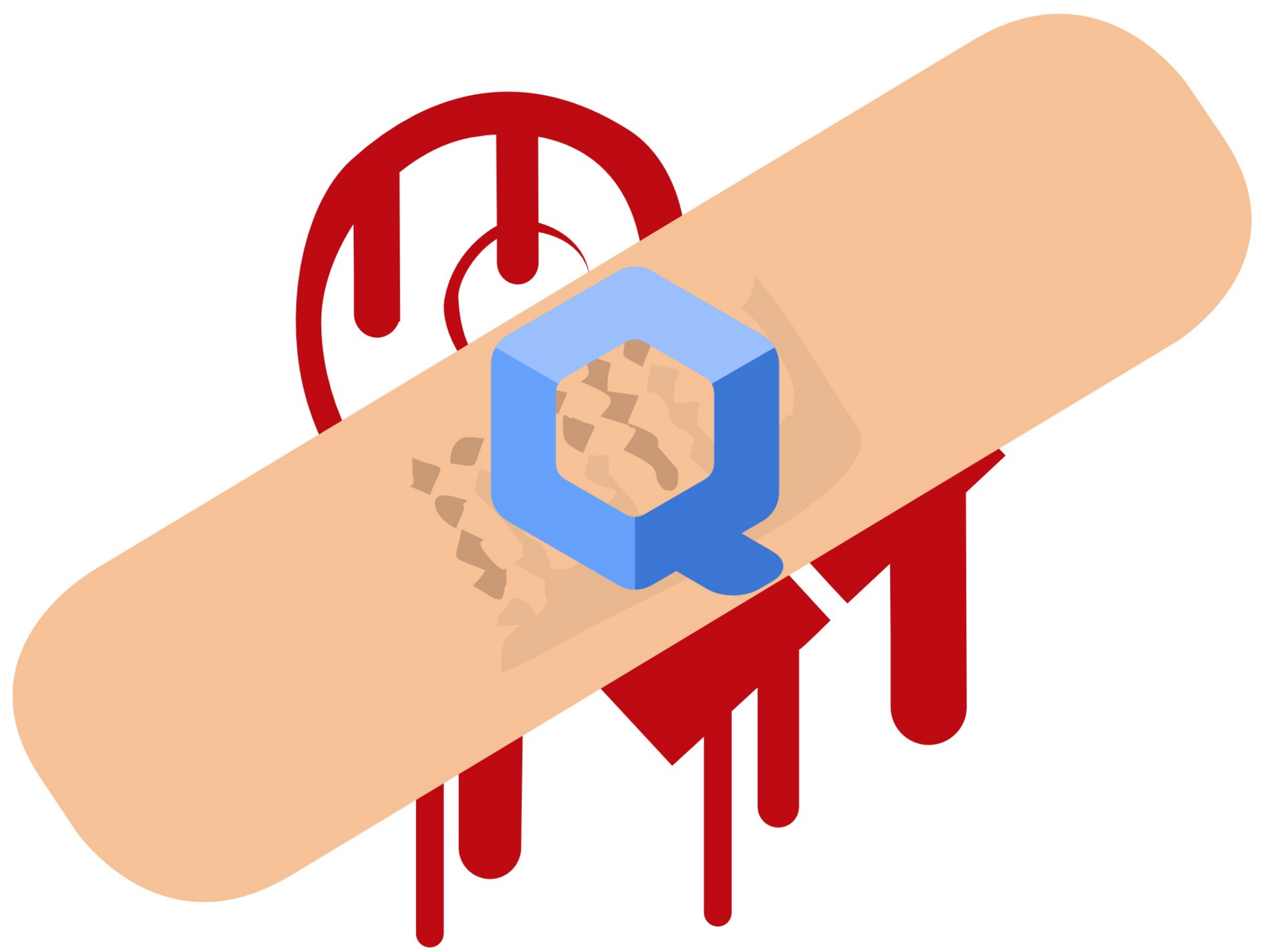


QUBES OS

A reasonably secure operating system

Agenda

- Das Problem mit „normalen“ Betriebssystemen
- Was ist Qubes OS
- Wie löst Qubes die Probleme
- Die Architektur von Qubes ...
- Beispiele
- Wie ich Qubes nutze ...
- Dokumentation
- Links

Das Problem mit „normalen“ Betriebssystemen

- Keine Freie Software (OSS)
- Vertrauenswürdigkeit
- Wichtige Daten
- Malware (Drive by, E-Mail, Download)
- USB Devices

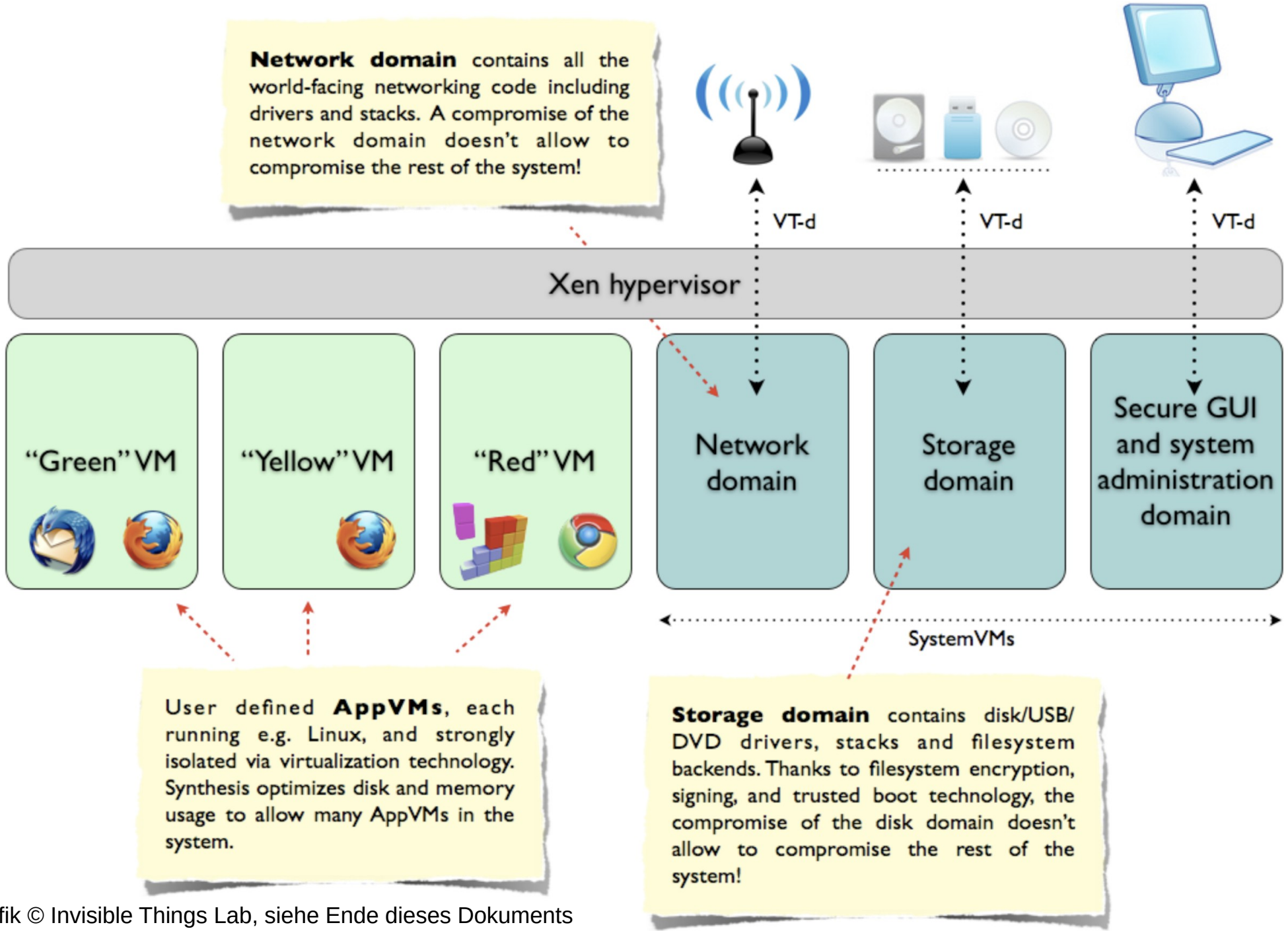
Was ist Qubes OS [1]

- Ein sicherheitsorientiertes Betriebssystem
- Free & Open Source Software (FOSS)
- Kompartmentalisierung mit Qubes
  (auch VM oder Dömane genannt)
- Basis
  - XEN Hypervisor [3]
  - Linux

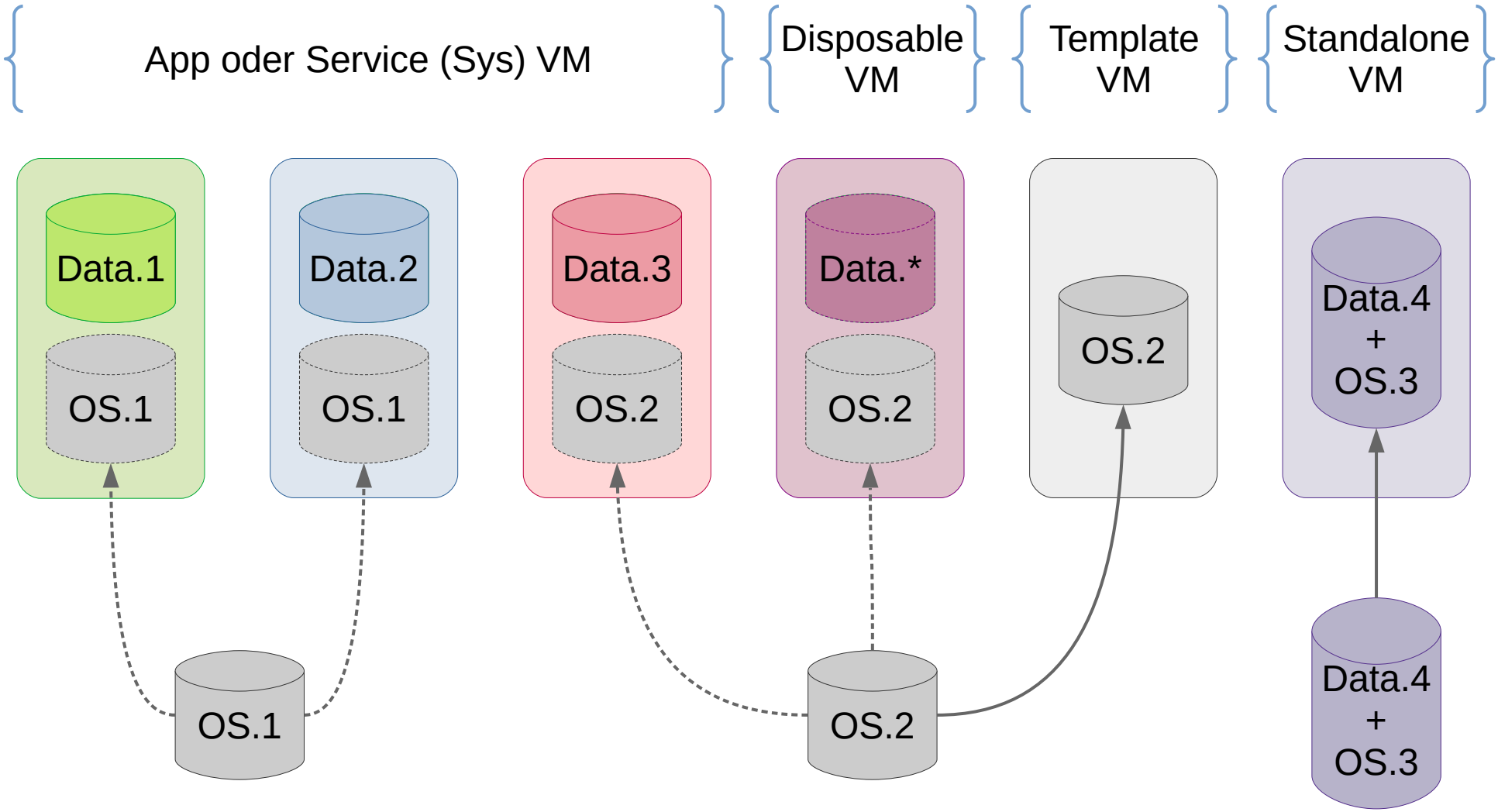
Wie löst Qubes die Probleme

- Qubes nutzt Virtualisierung für Kompartmentalisierung (Qube)
- Qubes haben unterschiedliche, farblich markierte Vertrauensstufen
- Daten kommen – je Vertrauensstufe - in einen eigenen Qube
- Verwendung von vertrauenswürdigen Repositories
- Kritische Programme kommen in eigene Qubes
- USB Devices werden nicht automatisch genutzt (eigener Qube)
- Externe Netzwerkanbindung in eigenem Qube
- Optional VPN &| Firewall → eigener Qubes
- Nicht kompromentierbarer Window-Manager

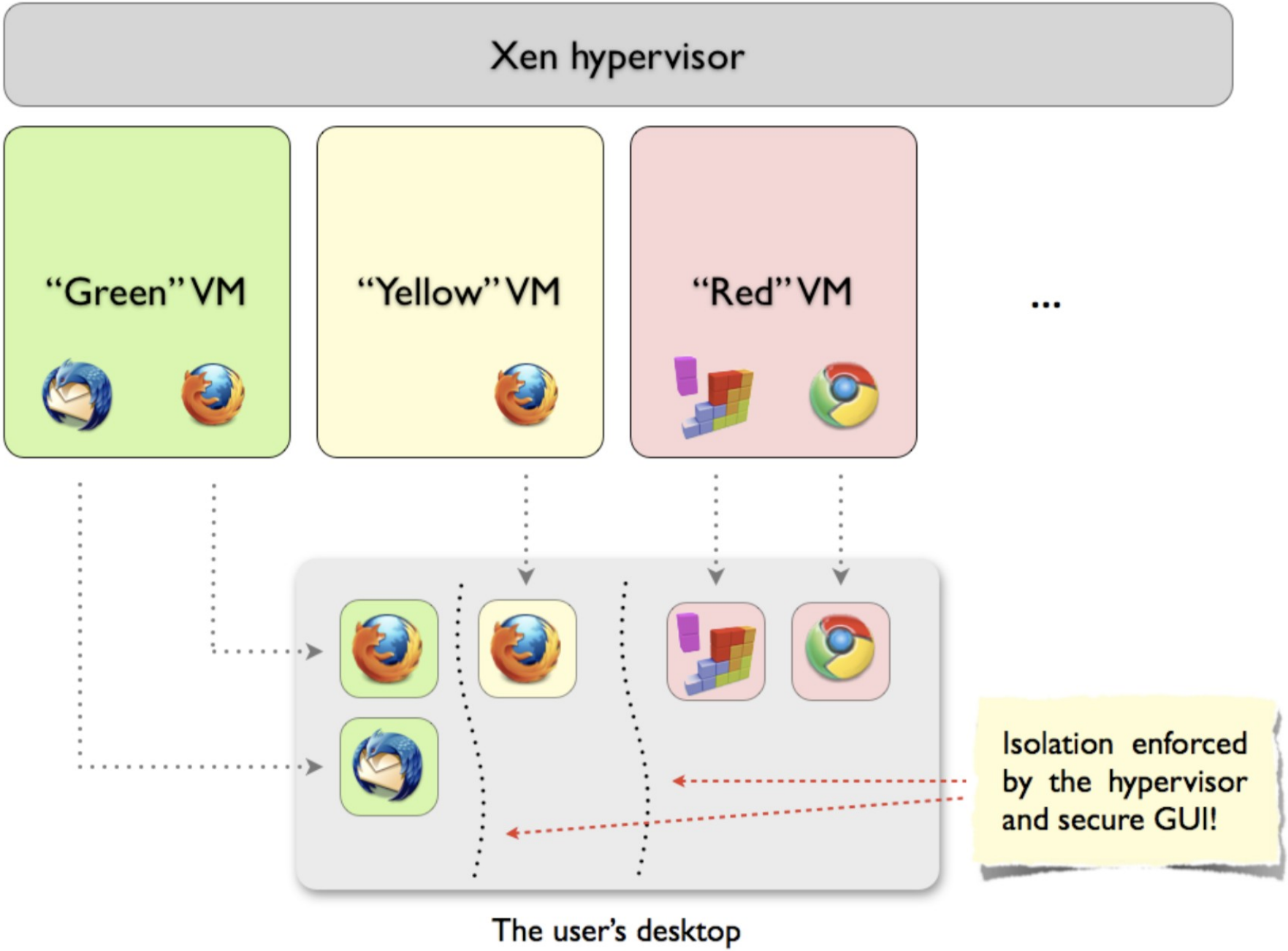
Architektur: Domänen



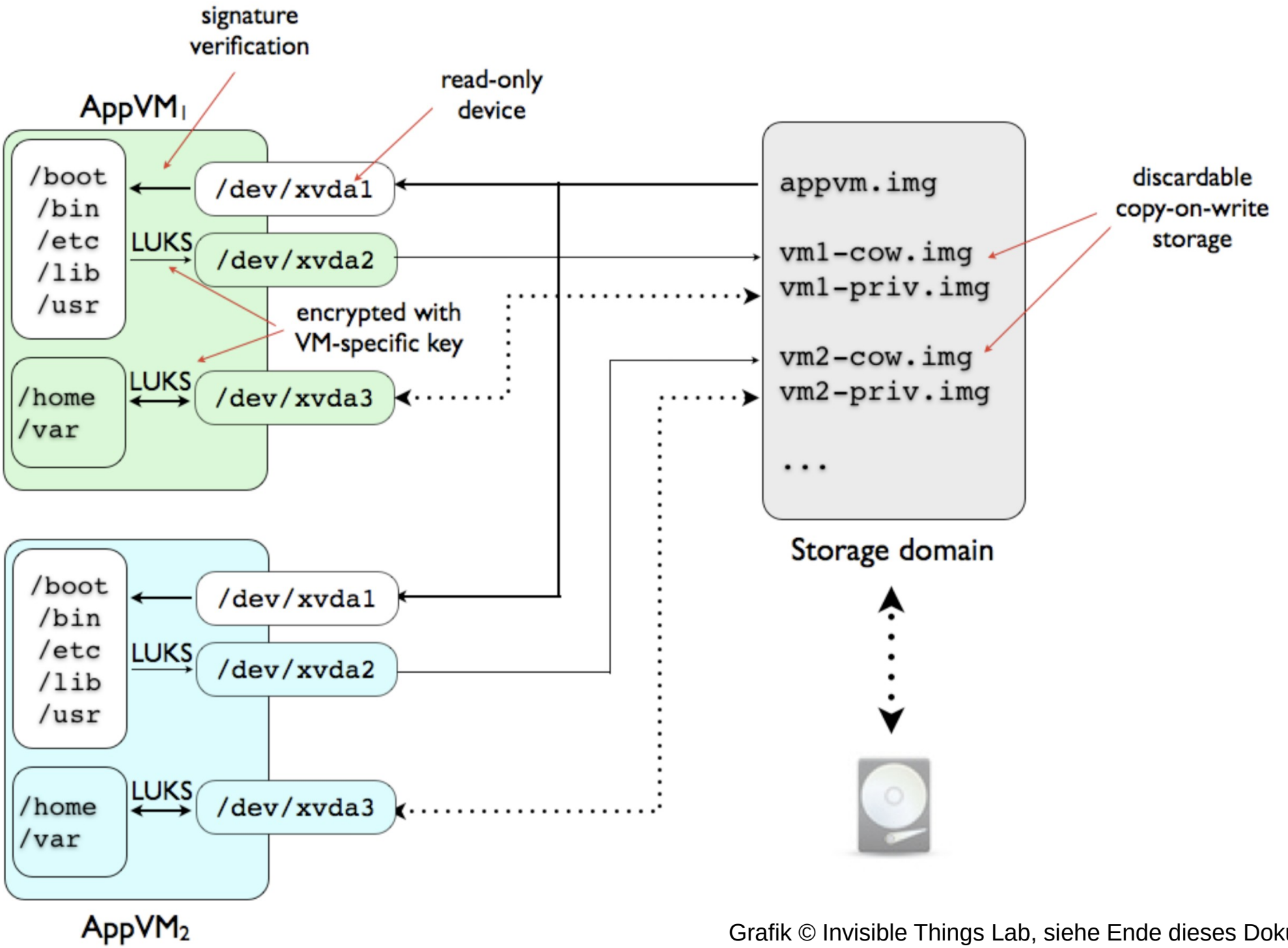
Architektur: Qubes VMs



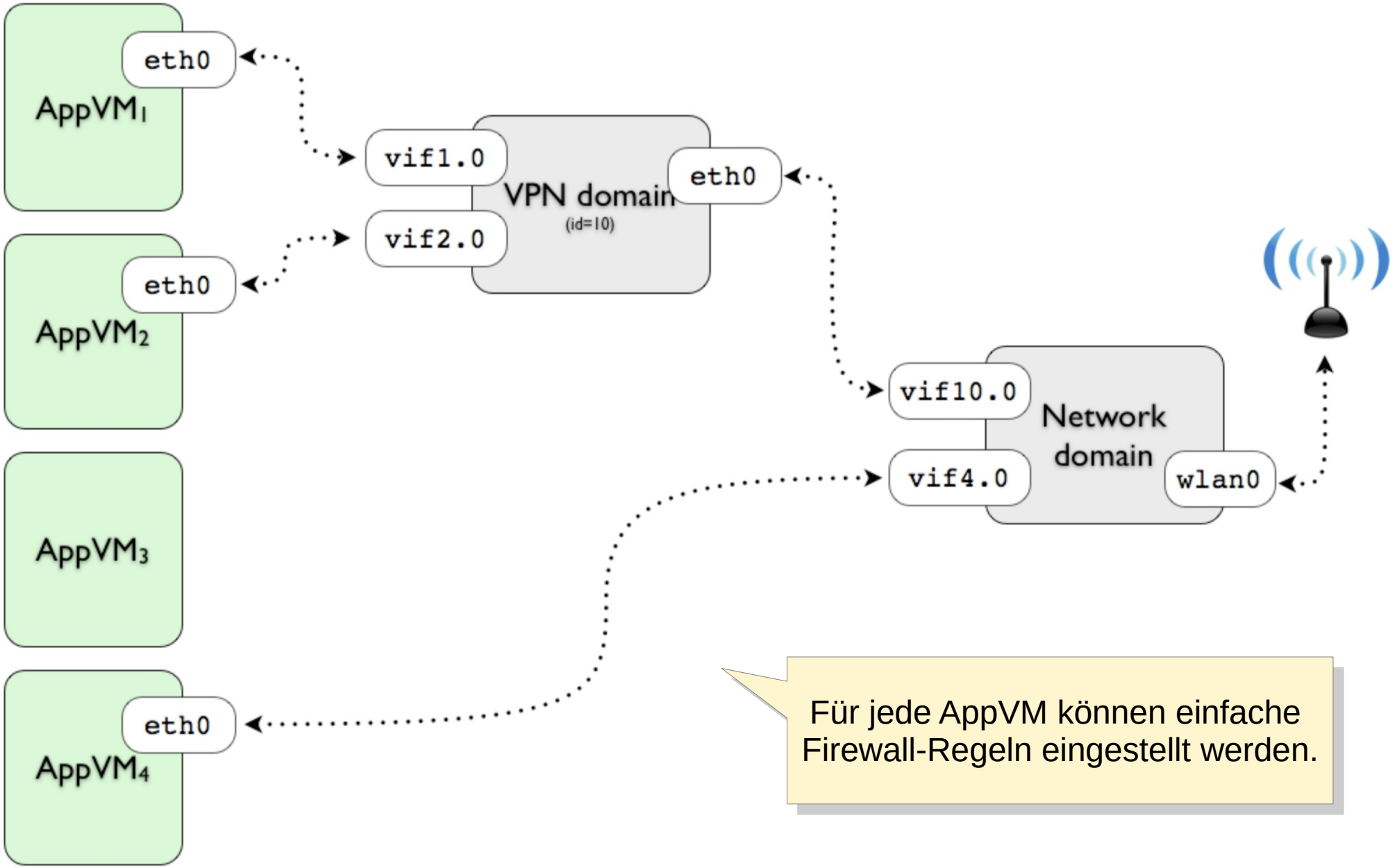
Architektur: Qubes Desktop



Architektur: Filesystem



Architektur: Netzwerk

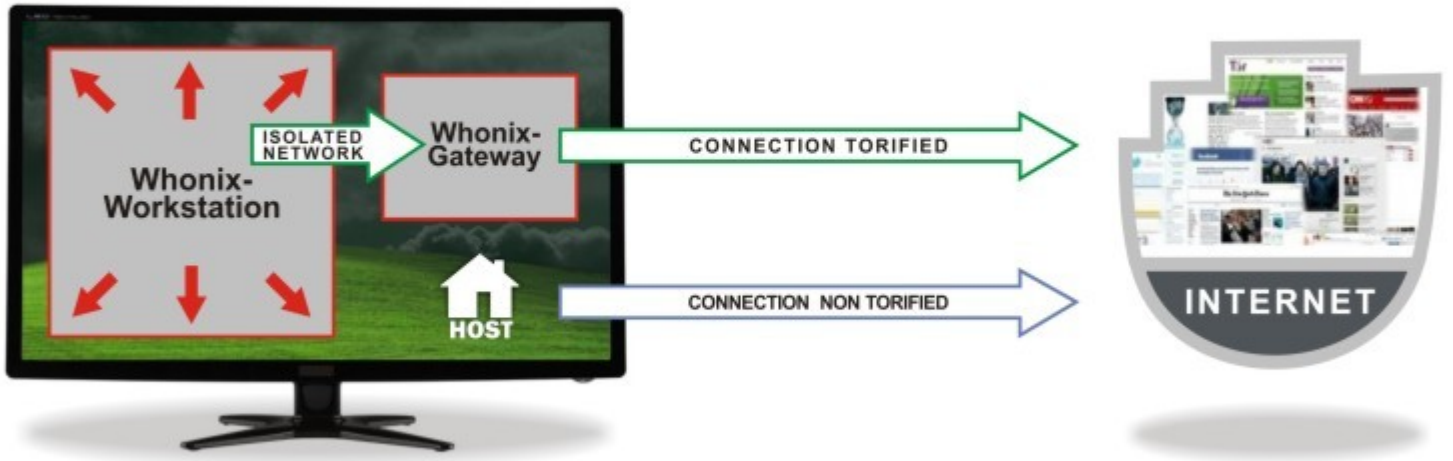


whonix

PRIVACY & ANONYMITY OS

(4)

Whonix
Anonymous Operating System



The red arow ↗ indicate that misbehaving / leaky applications can't break out of the **Whonix Workstation**.

All network connections ⇨ are forced to go through **Whonix Gateway** *where they are torified and routed to the Internet.*

Architektur: Backup

- Sicherung ganzer VMs
- Auch während des Betriebs (Snapshot nach dem letzten Beenden)
- Keine inkrementellen Backups
- Neues, inkrementelles Backup-System geplant, basierend auf BorgBackup (5)

- Eigene Backup Verfahren weiter möglich

Benutzbarkeit (usability)

- Copy & Paste – mit [shift] zu/von Display VM
- Kopieren/Verschieben von Dateien zwischen Qubes über Datei-Manager
- Dokumente einfach via Datei-Manager in Disposable-VM darstellbar
- PDFs in sichere Versionen konvertieren
- Alles auch Kommandozeile möglich
- Template VM Updates mit einem Klick ;)

Beispiele

- E-Mail Anhänge
- Banking
- Software ausprobieren
- OS Test (Windows, ...)
- Anonymität mit Whonix

Betriebssysteme und Qubes die ich nutze

Fedora (x 3):

- Privat
- Untrusted
- Fotos
- E-Mail
- Programmierung
- Password Manager
- Digitale Währung

Andere:

- (Debian)
- Windows
- Disposable
- Whonix

Herausforderungen

- USB-Memory
- Tastatur
- Netzwerk
- Drucker & Scanner
- Yubi-Key
- SSD Trim
- UI Glitches (Libre Office)
- Qubes OS Update

Anforderungen

- Intel oder AMD CPU mit Virtualisierung
- Kaum CPU Last durch Qubes
- 12 GB RAM (4 - ∞ GB)
- SSD (min. 32 GB)
- Multiboot funktioniert

https://www.qubes-os.org/doc/system-requirements/

Bedrohungen

- Meltdown, Spectre, ZombieLoad, ff
- Schwachstellen in XEN
- User

Alternativen

- Separate Rechner / air gap
- Whonix (4)
- VirtualBox (6)
- Tor-Browser (7)
- AppArmor / SELinux
- Aufgabenbezogene User-Konten
- Docker & Co ?

Mein Resumé

- In der normalen täglichen Nutzung problemlos
- Andere Anforderungen meist mit etwas mehr Aufwand umsetzbar
- Gibt ein vernünftiges Maß an Sicherheit, bei verhältnismäßig geringen Einschränkungen

➔ Mehr Vertrauen in mein System

Dokumentation (2)

- Umfangreich
- Verständlich (meistens)

Common Tasks

- Copying and Pasting Text Between Domains
- Copying and Moving Files Between Domains
- Copying from (and to) dom0
- Installing and Updating Software in dom0
- Installing and Updating Software in VMs
- Backup, Restoration, and Migration

Security Guides

- Qubes OS Project Security Information
- Security Guidelines
- Understanding Qubes Firewall
- Understanding and Preventing Data Leaks
- Installing Anti Evil Maid
- Using Multi-factor Authentication with Qubes
- Using GPG more securely in Qubes: Split GPG
- The Qubes U2F Proxy
- How to Set Up a Split Bitcoin Wallet in Qubes
- [Unofficial] Split dm-crypt
- Configuring YubiKey for user authentication
- Security Considerations When Handling Devices
- Note regarding password-less root access in VM

Links

(1) https://www.qubes-os.org/

(2) https://www.qubes-os.org/doc/

(3) https://xenproject.org/

(4) https://www.whonix.org/

(5) https://www.borgbackup.org/

(6) https://www.virtualbox.org/

(7) https://www.torproject.org/download/

(8) https://www.qubes-os.org/doc/architecture/

Fragen?

Danke!

Alexander Kulbartsch

a-qubes@alice-and-bob.de

Matrix: @alexanderk:matrix.org

Die Grafiken to den Themen „Domänen“, „Desktop“, „Filesystem“ und „Netzwerk“ wurden, mit freundlicher Genehmigung von Joanna Rutkowska, aus dem PDF Dokument „Qubes OS Architecture, Version 0.3, January 2010“ entnommen.
Erstellt wurde das Dokument von Joanna Rutkowska und Rafal Wojtczuk, beide vom „Invisible Things Lab“.

Das Dokument ist unter
https://www.qubes-os.org/doc/architecture/
zu finden.