Open Security for public institutions

OpenSecurity
open source solution for public institutions

Technical APs Status Report

Wien, 12.12.2013

(by Oliver Maurhart, AIT)

Ausgangspunkt

OpenSecurity
open source solution for public institutions

- Konsortialmeeting 24.09.2013 in Linz
  - Architekturpräsentation
    - Xen basierend
    - VirtualBox basierend
  - Uses Cases
    - Safe Internet Browsing
    - Virus Checking auf Removable Storage Devices
    - Automatsiche Ver- und Entschlüsselung „on the fly“

Ziel

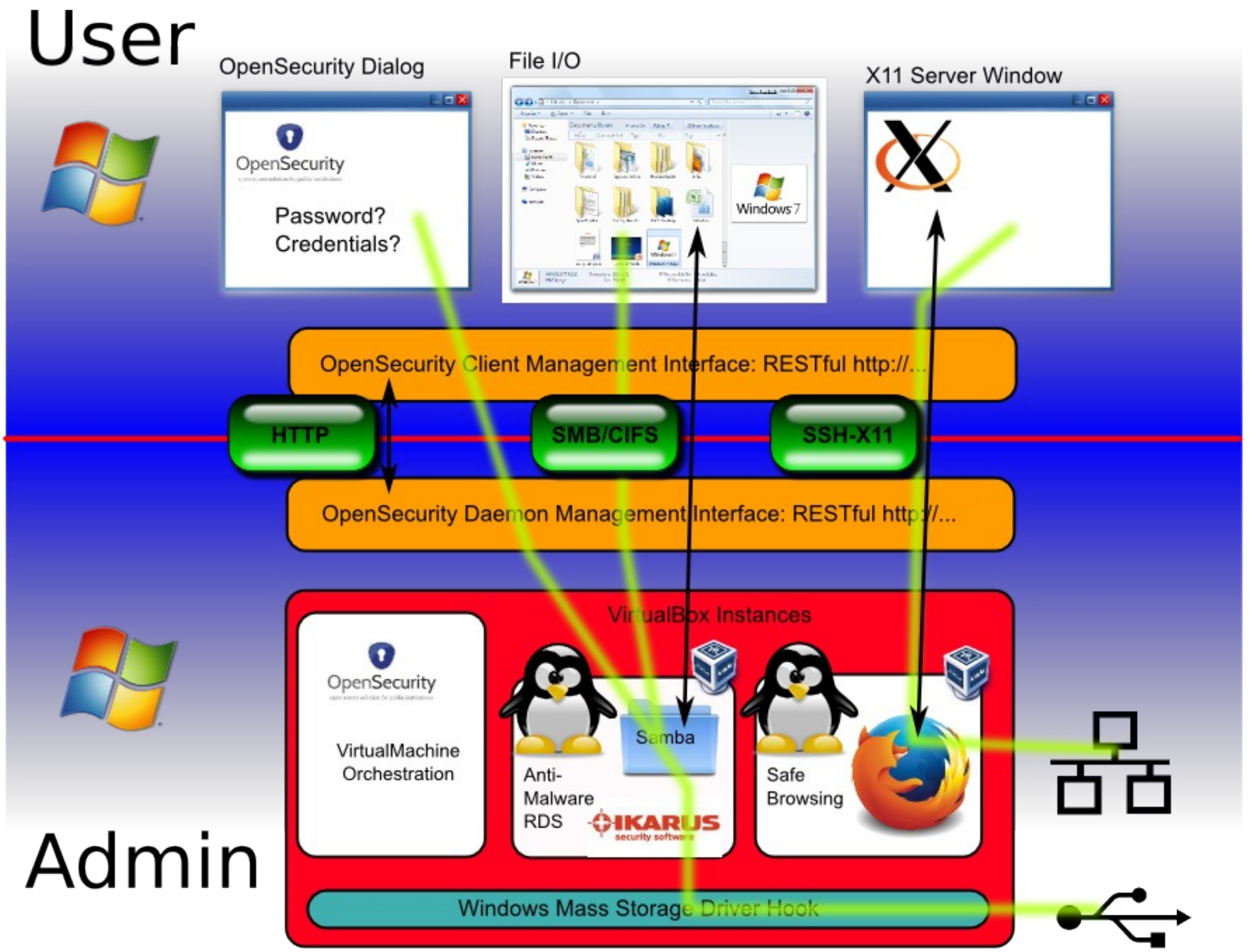
OpenSecurity
open source solution for public institutions

- Im Q1/XIV
  - Windows Host
    - VirtualBox
  - ALLE (!) Uses Cases
    - Safe Internet Browsing
    - Virus Checking auf Removable Storage Devices
    - Automatsiche Ver- und Entschlüsselung „on the fly“
  - Als Easy-to-use Installable
  - Eventuell download von www.opensecurity.at

Architektur

OpenSecurity
open source solution for public institutions

- Kernelemente:
  - Windows 7 64 Bit Referenzearchitektur
  - VirtualBox
  - SecurityVM
    - Immutable disposable VMs
  - USB Driver
  - Encryption
    - TrueCrypt
  - Virus Scanning local & remote with IKARUS


User
OpenSecurity Dialog
File I/O
X11 Server Window
OpenSecurity
Password?
Credentials?
Windows 7
OpenSecurity Client Management Interface: RESTful http://...
HTTP
SMB/CIFS
SSH-X11
OpenSecurity Daemon Management Interface: RESTful http://...
VirtualBox Instances
OpenSecurity
VirtualMachine
Orchestration
Samba
Anti-
Malware
RDS
IKARUS
security software
Safe
Browsing
Windows Mass Storage Driver Hook
Admin

Solution

OpenSecurity
open source solution for public institutions

- Trennung in
  - OpenSecurity Admin
  - OpenSecurity Client
  - RESTful API als Schnittstelle
    - wohlbekannte Technologie
    - kein proprietäres Format
    - flexibel
  - Konsequenz:
    - Alle Elemente sind (theoretisch) austauschbar
    - Isoliert

Solution

OpenSecurity
open source solution for public institutions

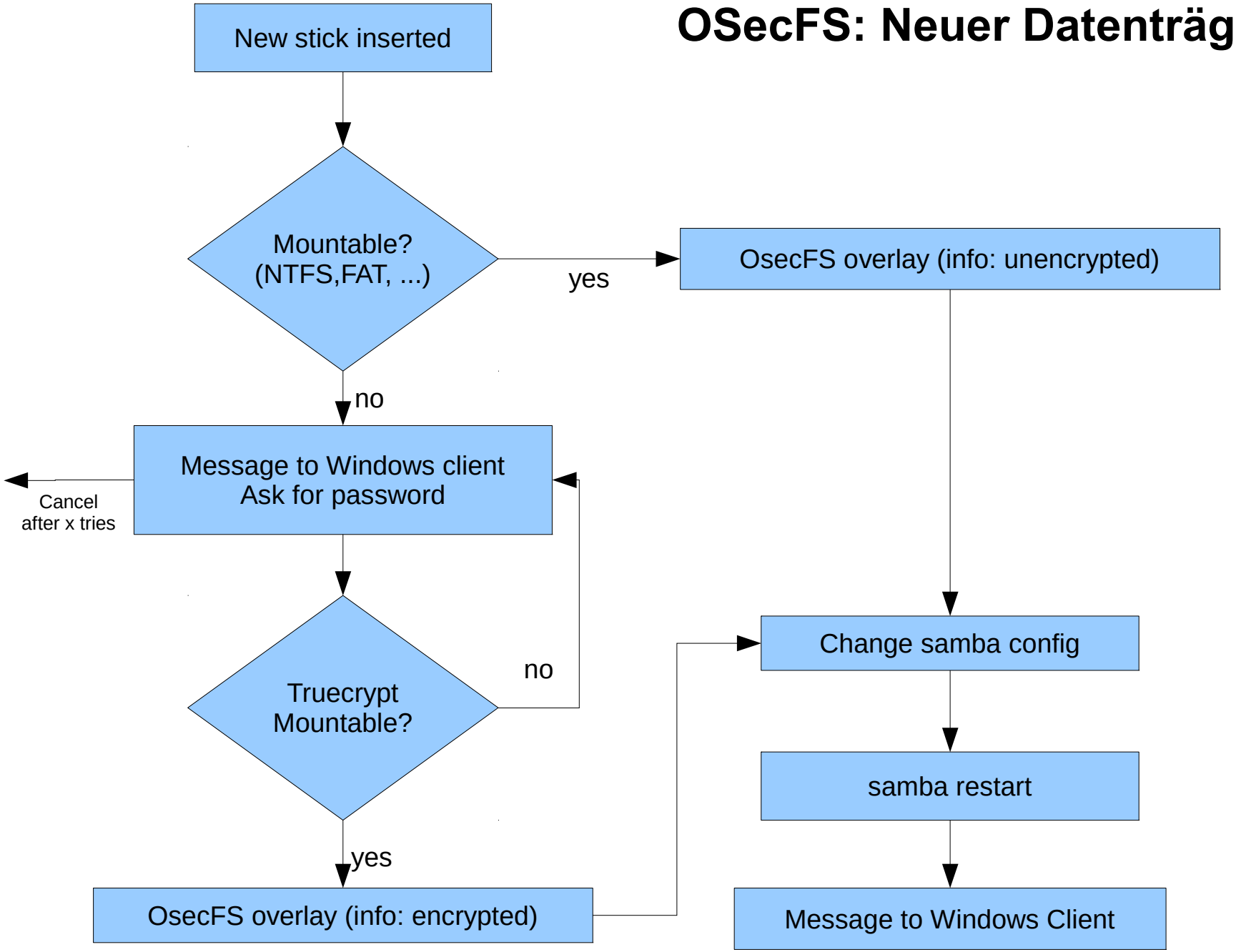
- OpenSecurity Admin
  - Orchestrierung von:
    - SecurityVMs
    - VirtualBox
      - Host-Only IP - Subnetz
      - NAT
    - USB Device Driver
    - Windows Service
    - Einhängen von „Netzlaufwerken“
      - „Downloads“ Verzeichnis
    - Bereitstellung Virtuelle Maschinen
      - X-Net Debian Repository

Solution

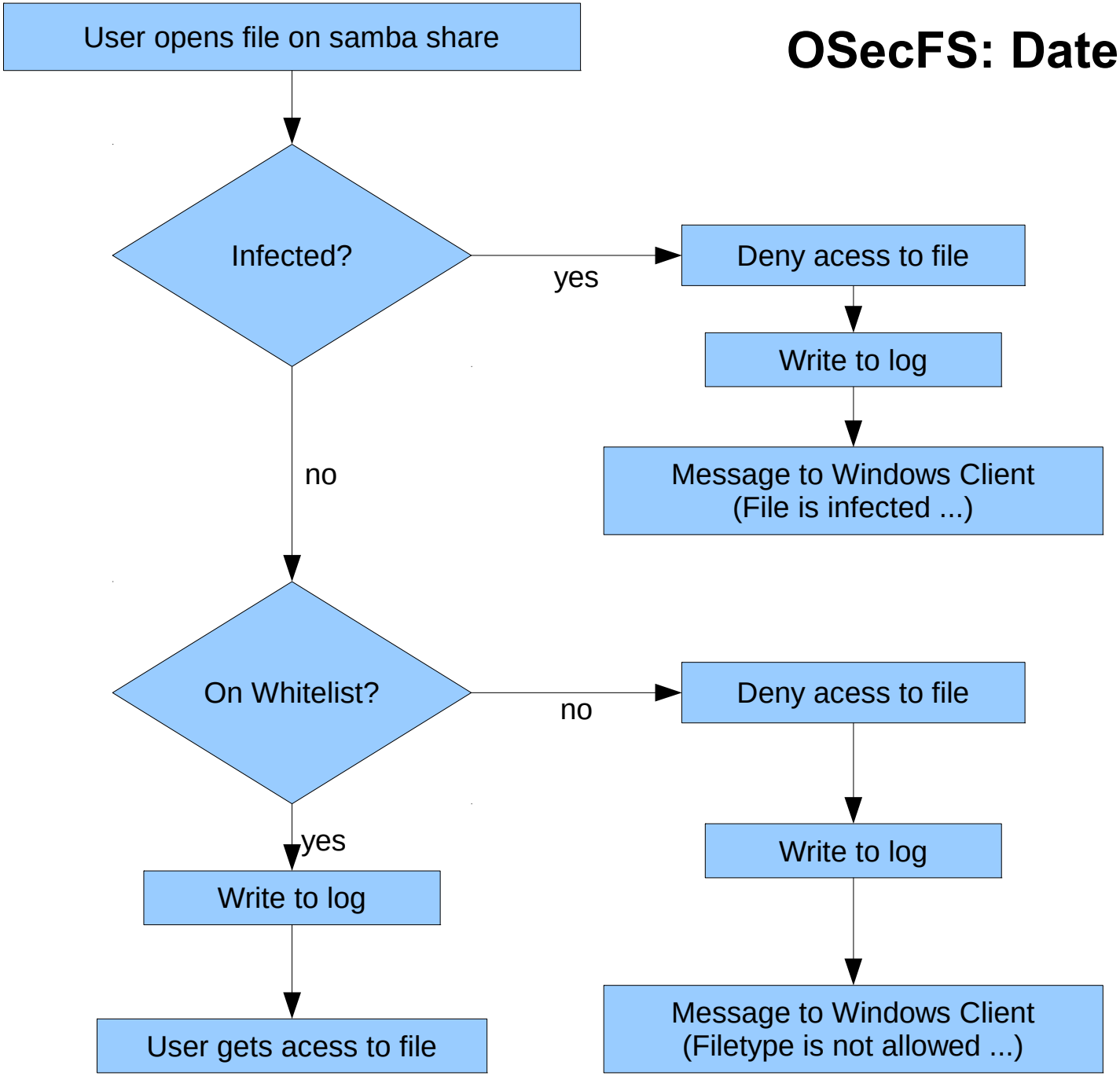
OpenSecurity
open source solution for public institutions

- OSecFS
  - Filesystem Overlay via FUSE
  - Administrieren von SMB/CIFS
  - Verschlüsseln/Entschlüsseln
  - Anstoßen von Virus Scan
- IKARUS AV
  - local / remote Virus Scanning
  - innerhalb der VM - Kommandline

OSecFS: Neuer Datenträger



OSecFS: Dateizugriff



Solution

OpenSecurity
open source solution for public institutions

- OpenSecurity Client
  - X11 SSH Forwarding
  - System Tray Icon
  - Password & Credentials Dialog
    - OSecFS: http://192.168.56.1:8090/password?...
    - OS client: http://192.168.56.101:58080/password?...
  - Fehlermeldungen oder Warnung
    - „Virus XY in Datei ABC.exe identifiziert“

Aktuelle Situation

OpenSecurity
open source solution for public institutions

Implementationsstand 12.12.2013?

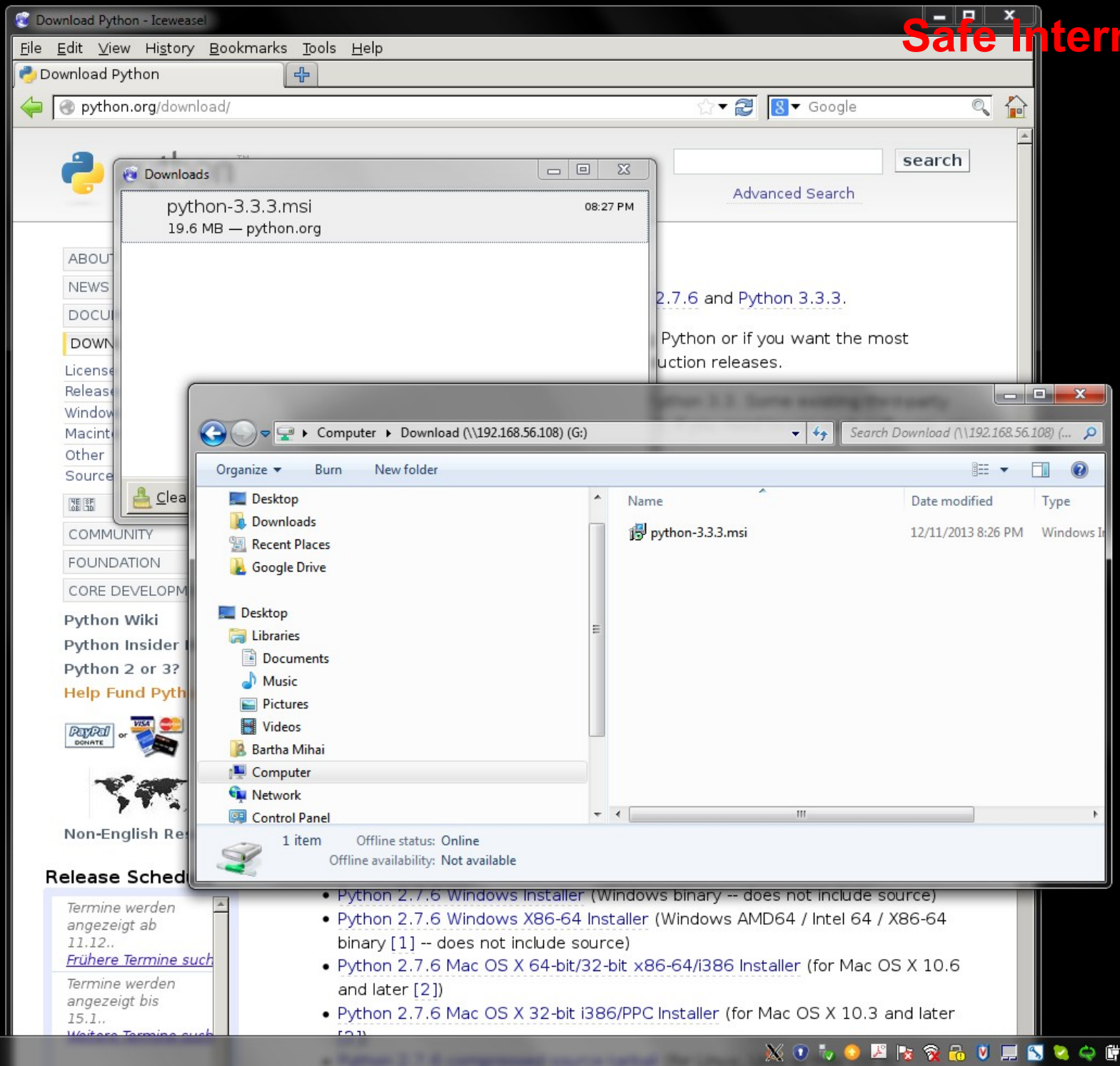
Aktuelle Situation

OpenSecurity
open source solution for public institutions

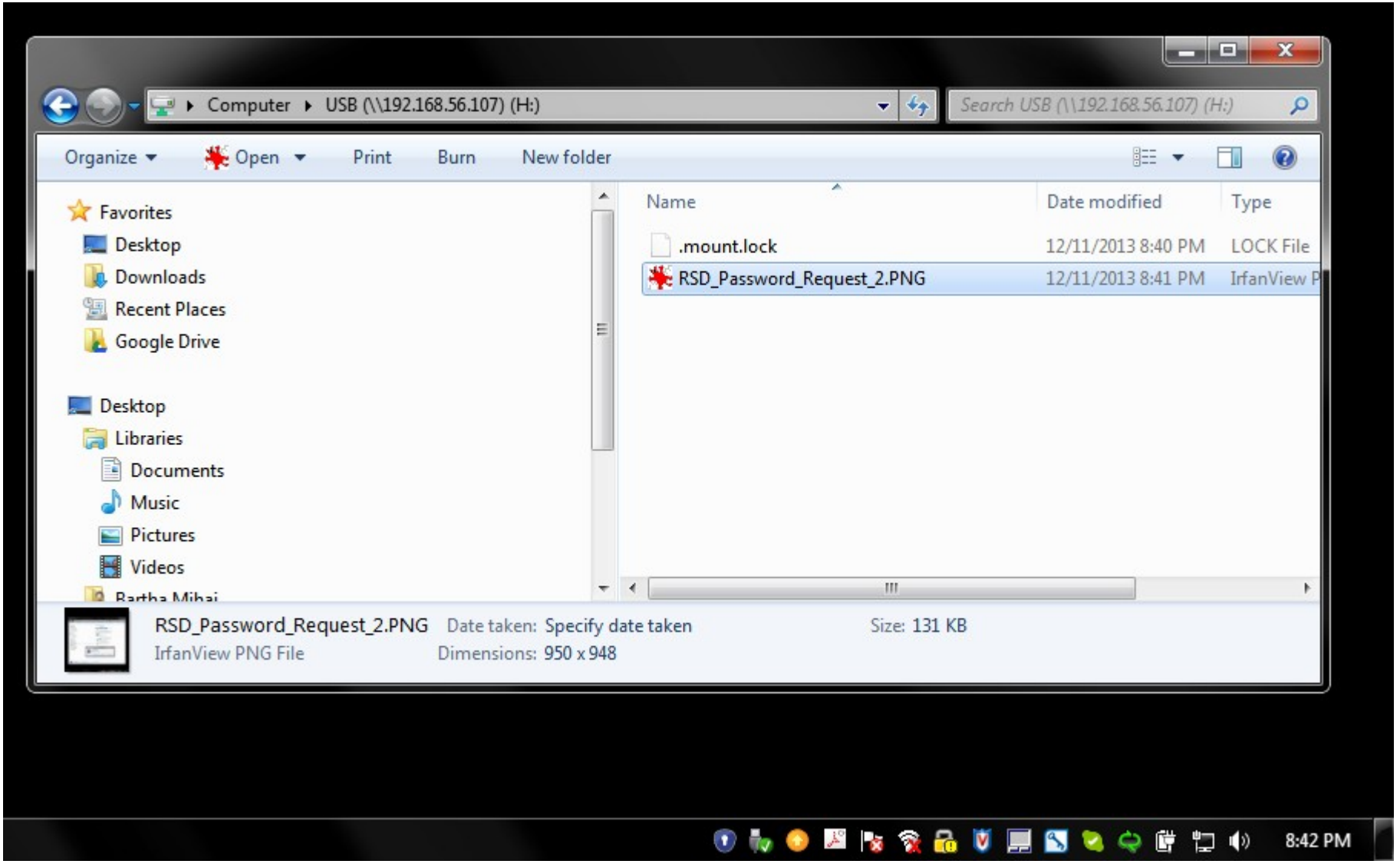
Feature complete!!

(hurray!)

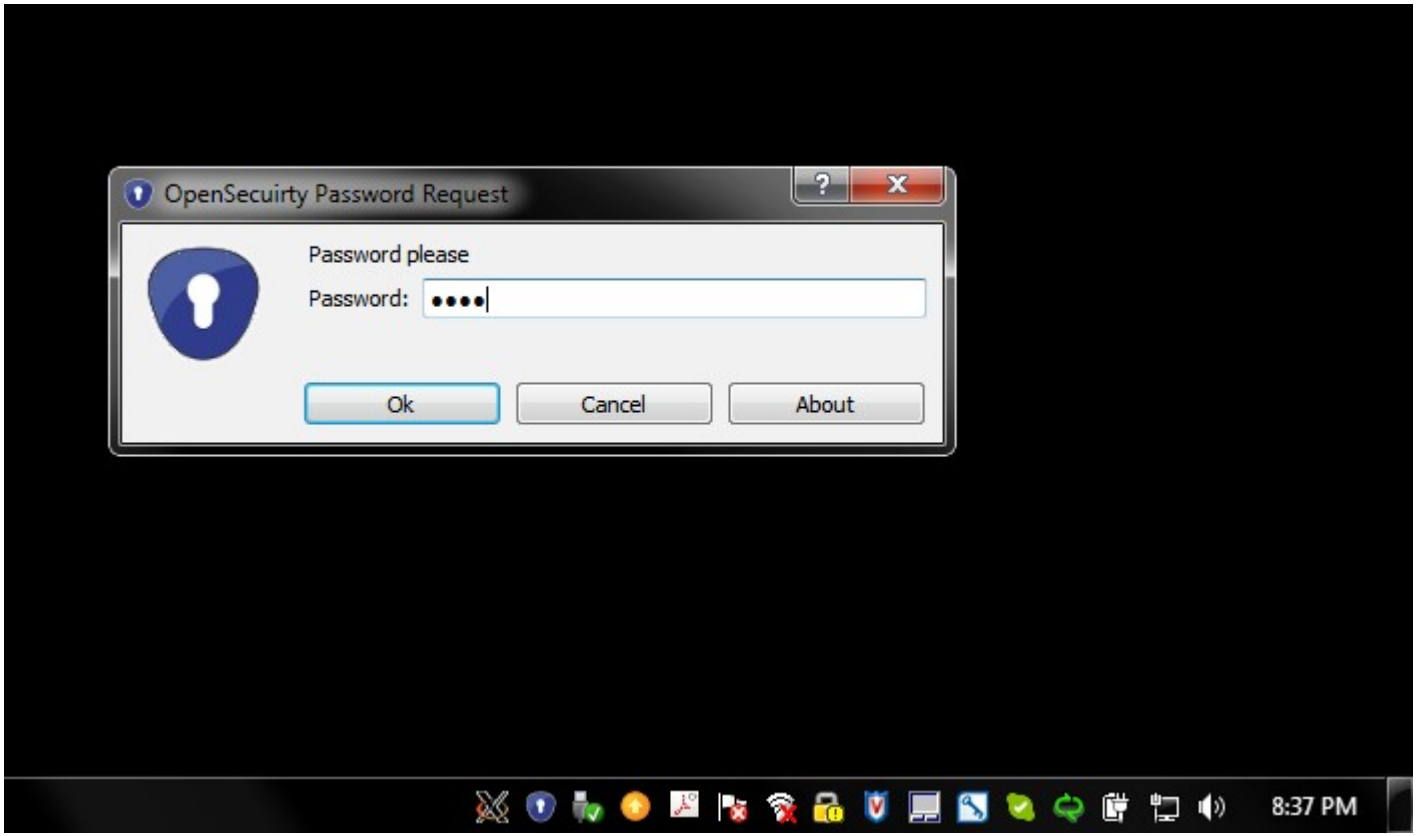
Safe Internet Browsing



USB Stick Zugriff



Entschlüsselng Password Abfrage + OpenSecurity SysTray



Aktuelle Situation

OpenSecurity
open source solution for public institutions

Aber:

- ✓ Zur Zeit kein Deployment/Setup möglich
- ✓ Zahlreiche Hürden und Barrieren in der Systemintegration
  - Windows Firewall
  - Checkpoint
  - Windows User Rechte
  - Relocatables:
    - in welchem Pfad ist XY installiert?
    - welche Version?

Aktuelle Situation

OpenSecurity
open source solution for public institutions

- Security Considerations
  - Was könnte wo im Applikationspfad passieren?
  - Wo sind Security Leaks
- Stabilitätsprobleme
  - Bsp. unerwartete Antworten von Subsystemen
- Bugs
  - In OpenSecurity Software
  - In 3rd Party Software

Next Steps

OpenSecurity
open source solution for public institutions

- ✓ System Integration
- ✓ Stabilisierung
- ✓ Usability
  - bsp. wieviele parallele VMs „verträgt“ Win7?
- ✓ Testing
- ✓ Performance
- ✓ (Polish)

Ende

OpenSecurity

open source solution for public institutions

Danke!

(Next: Demo)