



GecMeGUI

—

Eine SSO-enabled Cloud WebGUI mit clientseitiger Schlüsselgenerierung

Hochschule Furtwangen
Cloud Research Lab
Frank Dölitzscher

04.04.2011

Cloud
Research Lab

Grundlagen
Shibboleth

Shibboleth
Web-Proxy

Cloud Web GUI

Demo

1. Einführung Cloud Research Lab
2. Absicherung des Service Zugangs
 - Grundlagen Shibboleth
 - Shibboleth Web-Proxy
3. Cloud Web GUI
 - Sicherung des Cloud Zugangs
4. Demo

Cloud Research Lab

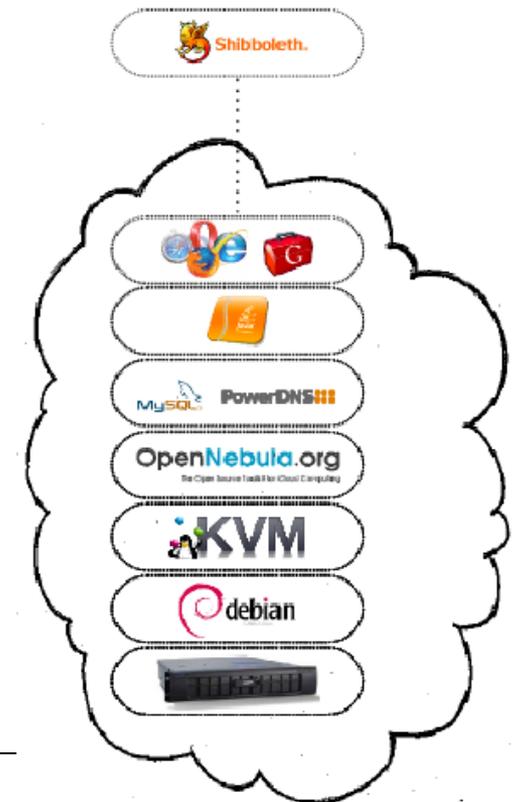
Grundlagen
Shibboleth

Shibboleth
Web-Proxy

Cloud Web GUI

Demo

- Facts & Numbers
 - Gegründet 2009 von Prof. Dr. Reich
 - 1 PhD Student, 5 Master-, 4 Bachelor-, 2 Hiwi-Studenten
 - Cloud Umgebung CloudIA [1]
- Cloud Software Stack
 - SSO via Shibboleth
 - Google GWT GUI
 - Java Voodoo
 - MySQL, PowerDNS, DHCP3
 - OpenNebula cloud management
 - KVM Hypervisor
 - Linux OS (Debian)



Cloud
Research Lab

**Grundlagen
Shibboleth**

Shibboleth
Web-Proxy

Cloud Web GUI

Demo

- Shibboleth ist ein Verfahren zur Authentifizierung und Autorisierung für Web-Applications und – Services
- Entwickelt von Internet2/MACE
- Basiert auf SAML und ermöglicht SSO
- Ist im akademischen Umfeld weit verbreitet
- Wird auch an der HFU eingesetzt (z.B. Authentifizierung an der Felix-Plattform, Integration Bibliothek in DBIS System)

Cloud
Research Lab

**Grundlagen
Shibboleth**

Shibboleth
Web-Proxy

Cloud Web GUI

Demo

Shibboleth Komponenten

- Identity Provider
 - Java Web-Application
 - Anbindung an Identity Management (z.B. LDAP)
 - Authentifizierung von Benutzern
 - Liefert Attribute an Service Provider aus
- Service Provider
 - Shibboleth Daemon und Apache Modul (mod_shib)
 - Verwaltet Zugriff auf Ressourcen (z.B. Auswertung von SAML-Assertions und Attributen)
- Discovery Service (optional)
 - Zur Lokalisierung der Heimatorganisation des Benutzers

Grundlagen Shibboleth

Cloud Research Lab

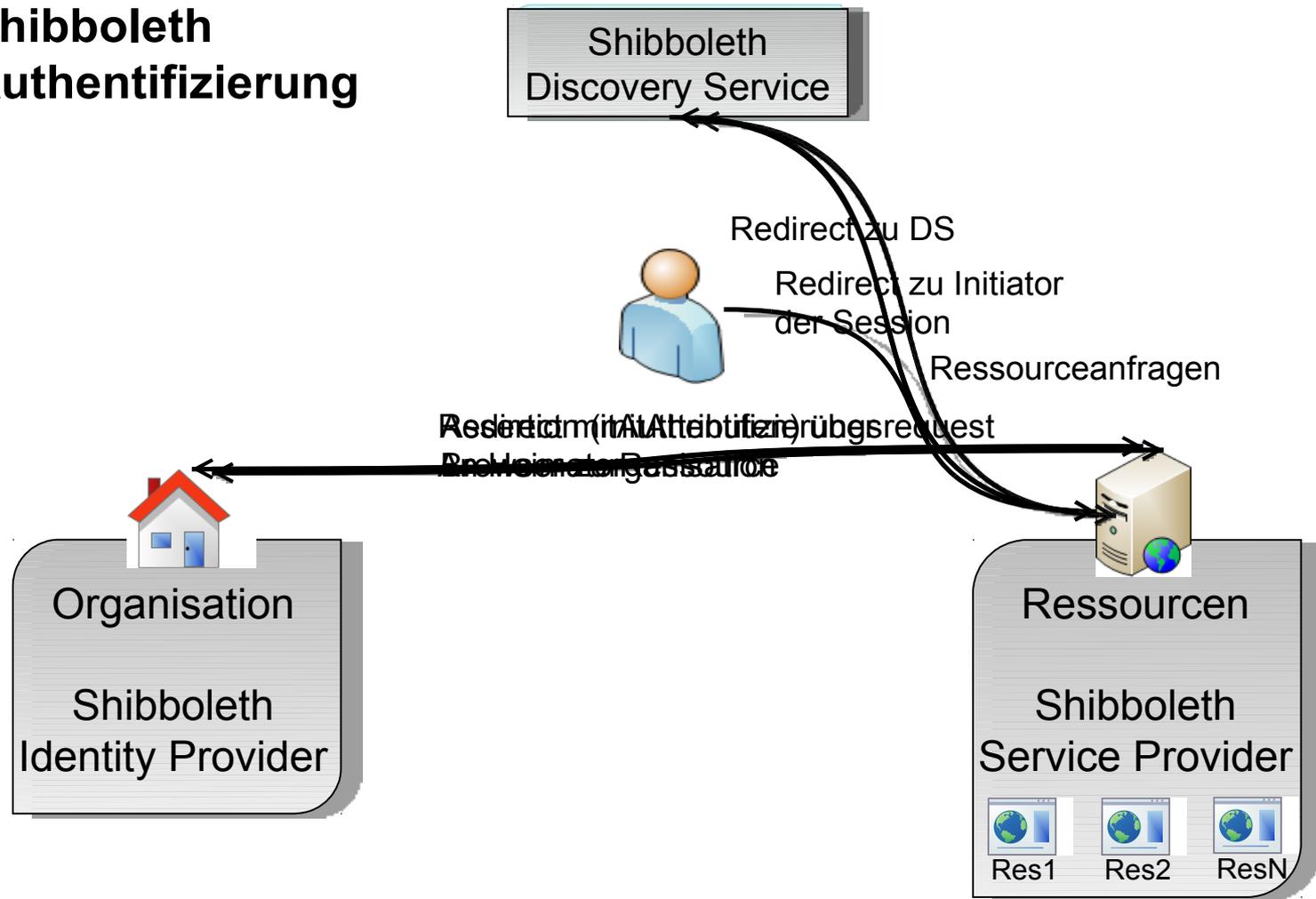
Grundlagen Shibboleth

Shibboleth Web-Proxy

Cloud Web GUI

Demo

Shibboleth Authentifizierung



Cloud
Research Lab

Grundlagen
Shibboleth

**Shibboleth
Web-Proxy**

Cloud Web GUI

Demo

- Szenario Cloud
 - Integration von PaaS und SaaS Szenarien
 - User stellen Services per VM bereit
 - Services kommen und gehen
- Problem SP - IDP:
 - Viele Hosts mit WebApps in Cloud
 - SP muss bei IDP registriert werden
 - Restart IDP dauert sehr lange
 - => Reduzierung der Anzahl an SPs bei vielen Diensten auf vielen (virtuellen) Maschinen
- Lösung:
 - Reverse Proxy (Apache) als vorgeschalteter SP
 - Services hinter Webproxy
 - Zwei mögliche Implementierungen

Cloud
Research Lab

**Grundlagen
Shibboleth**

Shibboleth
Web-Proxy

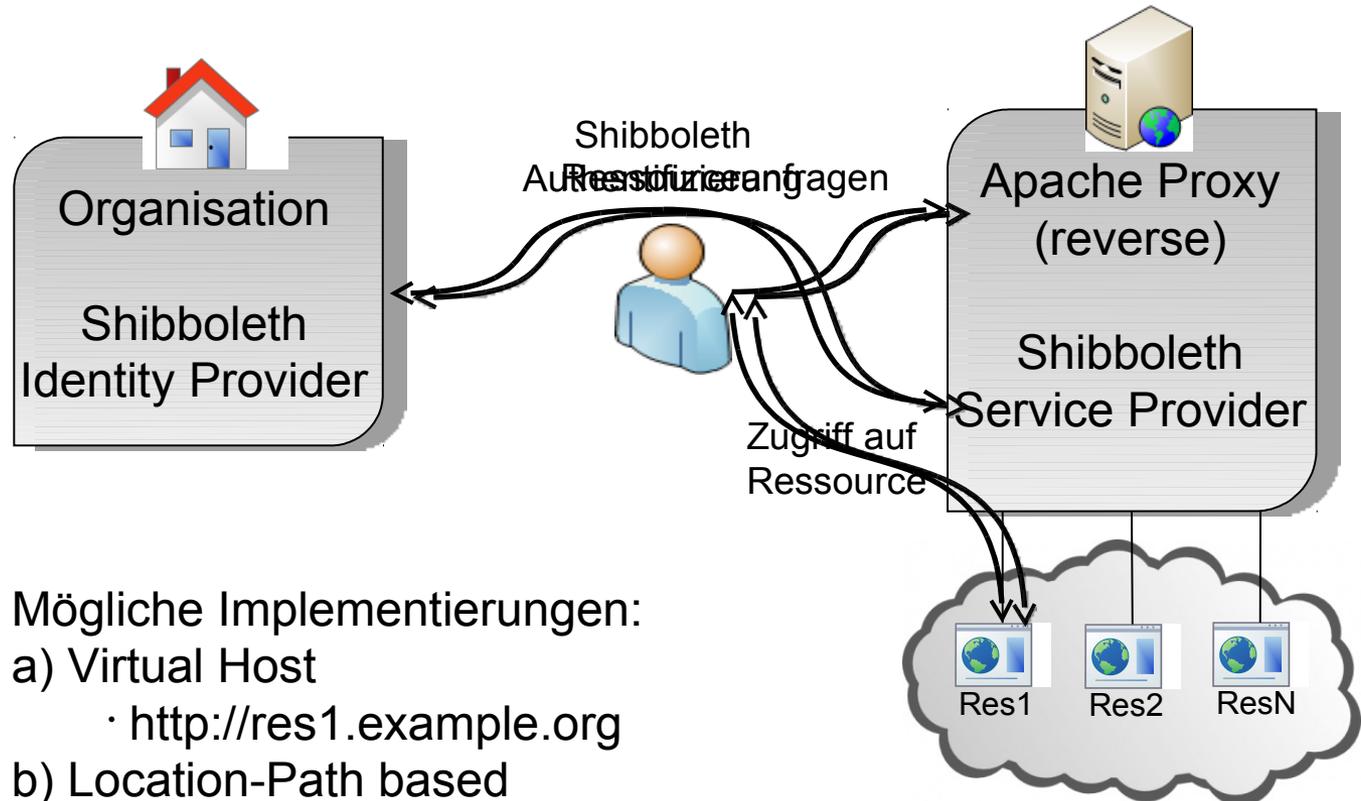
Cloud Web GUI

Demo

Problemstellung

- Idee: Reduzierung der Anzahl an Service Providern bei vielen Diensten auf vielen (virtuellen) Maschinen
- Begrenzte Anzahl verfügbarer öffentlicher IPv4-Adressen
- Hohe Dynamik bei Service-Erstellung und –Entfernung
- Integration in PaaS und SaaS Szenarien (Cloud)

Shibboleth Web-Proxy Überblick



Mögliche Implementierungen:

a) Virtual Host

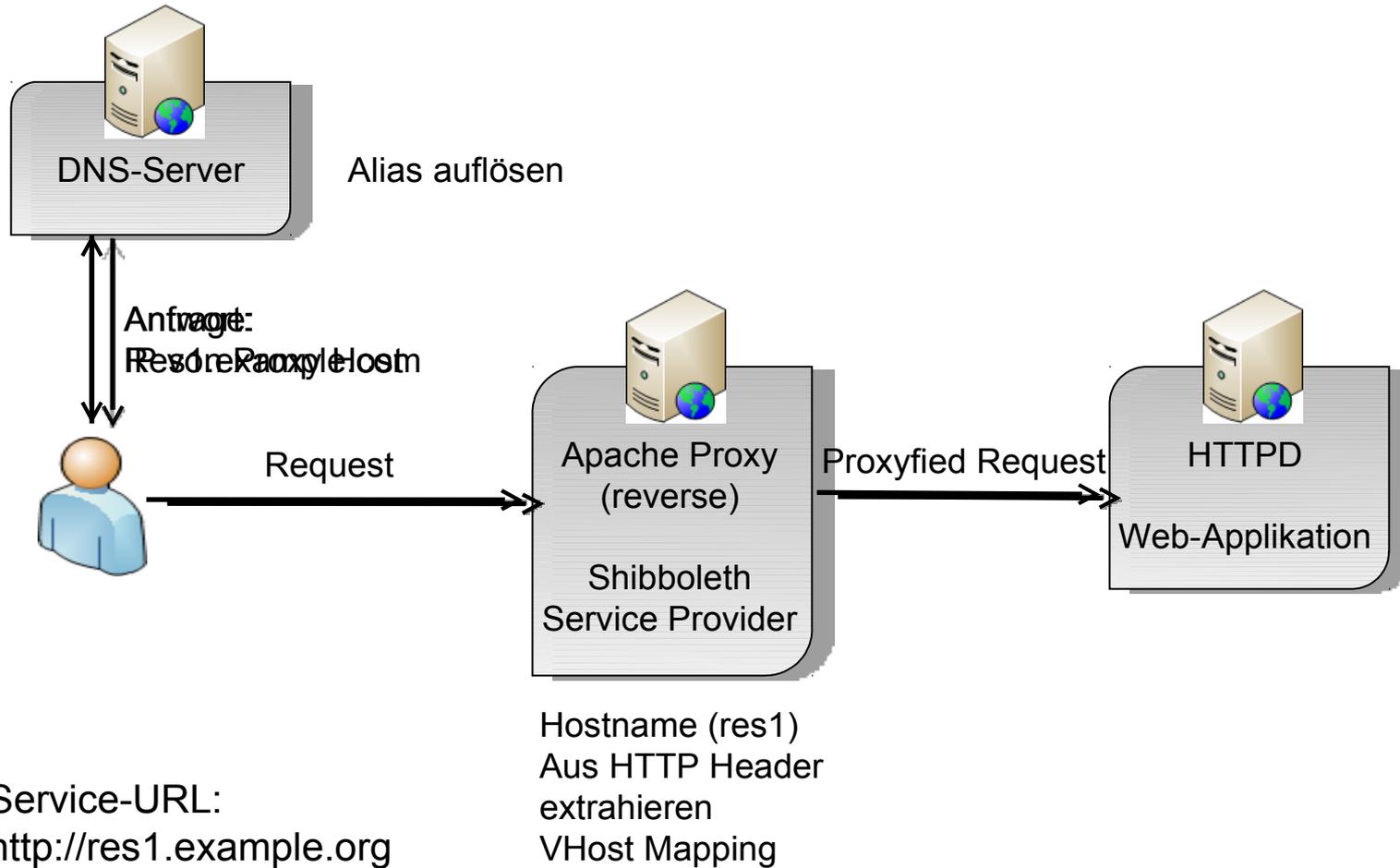
- `http://res1.example.org`

b) Location-Path based

- `https://proxy.example.org/res1`

1. Einleitung
2. Grundlagen Shibboleth
3. Shibboleth Web-Proxy
4. Zusammenfassung und Ausblick

Virtual Host Szenario



Cloud
Research Lab

Grundlagen
Shibboleth

**Shibboleth
Web-Proxy**

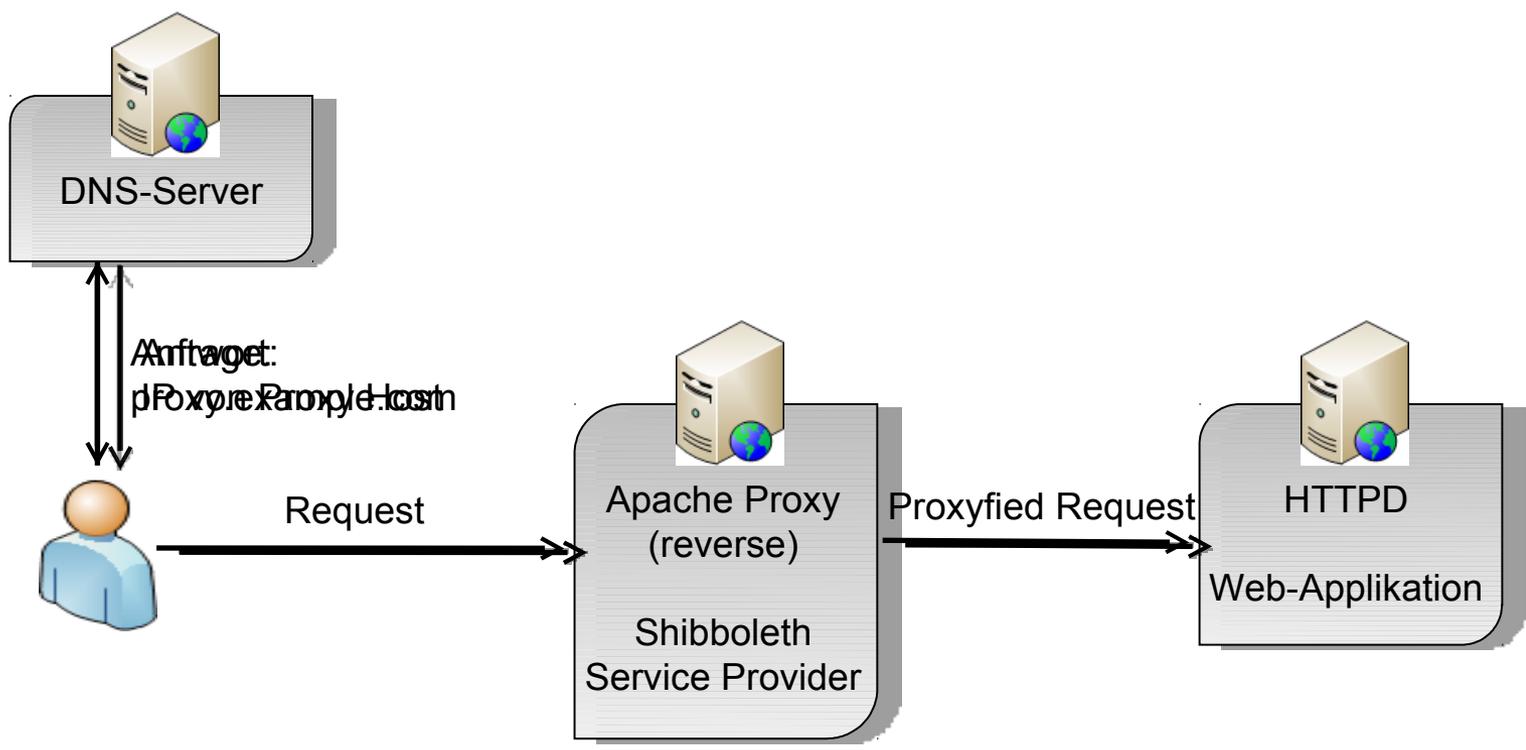
Cloud Web GUI

Demo

Virtual Host Szenario

- Bsp.: `http://res1.example.org/`
- “res1” ist als Alias im CNAME Ressource Record für Proxy definiert
- Dadurch Umleitung aller Requests über Proxy
- Dort vHost-Umsetzung auf tatsächliche Maschine
- Shibboleth Konfiguration pro vHost
- Aber: “Name-based virtual hosting cannot be used with SSL secure servers because of the nature of the SSL protocol” [Apache httpd documentation]
 - Lösung: Wildcard Zertifikat :-(
 - Server Name Indication (SNI)

Location-Path Szenario



Anhand von Location (/res1)
Zielhostermitteln

Service-URL:
<http://proxy.example.org/res1>

Cloud
Research Lab

Grundlagen
Shibboleth

**Shibboleth
Web-Proxy**

Cloud Web GUI

Demo

Location-Path Szenario

- Identifikation der Ressource via Pfa „/res1“
 - Umsetzung auf tatsächliche Maschine erfolgt in Location-Konfiguration des Proxys
- Shibboleth Konfiguration pro Location möglich
- HTTPS für alle Browser möglich
 - Bsp.: <https://proxy.example.org/res1>
- Nachteil:
Zwischen Anwender und Proxy kann nur das SSL-Zertifikat des Proxys verwendet werden.

Cloud
Research Lab

Grundlagen
Shibboleth

**Shibboleth
Web-Proxy**

**Cloud Web
GUI**

Demo

- Cloud Infrastructure and Applications (CloudIA)
- 1 VM per Student
- Anforderungen an Cloud GUI
 - Anbindung an das HFU Usermanagement
 - Shibboleth enabled
 - Sicher und Easy to use
- Analyse Cloud Authentifizierung
 - Bachelorthesis
 - „Rechtmanagement in der Cloud - Design und Implementierung eines Benutzermanagements für Cloud Infrastructures and Applications (CloudIA), Thomas Rübesamen, 2010

Cloud
Research Lab

Grundlagen
Shibboleth

Shibboleth
Web-Proxy

Cloud Web
GUI

Demo

IaaS – Anbieter

	Amazon EC2	Flexiant Flexiscale	ScaleUp
Remotezugriff	SSH	SSH	SSH
VM Authentifizierung	Public-Key	Passwort	Public-Key
VM User	root	root	root

- Amazon EC2
 - Access Key, Secret Access Key, X509 Zertifikat, Private Key
- Sicherheit
 - Wo werden die Keys generiert, gespeichert, übertragen?

Cloud
Research Lab

Grundlagen
Shibboleth

**Shibboleth
Web-Proxy**

**Cloud Web
GUI**

Demo

Own Cloud GUI

Cloud Research Lab

Grundlagen Shibboleth

Shibboleth Web-Proxy

Cloud Web GUI

Demo

Angemeldet als: Frank Doelitzscher



HFU CLOUD

Hostname	IP-Adresse	Status	Typ	
frank1Desktop	141.28.2.101	Running	Ubuntu 10.10 Desktop	<input type="button" value="Löschen"/> <input type="button" value="Anhalten"/>
frank1Basic.r	141.28.2.100	Running	Debian 5.0	<input type="button" value="Löschen"/> <input type="button" value="Anhalten"/>
frank2Desktop.	141.28.2.102	Running	Ubuntu 10.10 Desktop	<input type="button" value="Löschen"/> <input type="button" value="Anhalten"/>

Hinweis

Beachten Sie, dass alle virtuellen Maschinen nachts angehalten werden. Sie können diese jederzeit durch "Fortsetzen" wieder starten.

Cloud GUI – Create VM Wizard

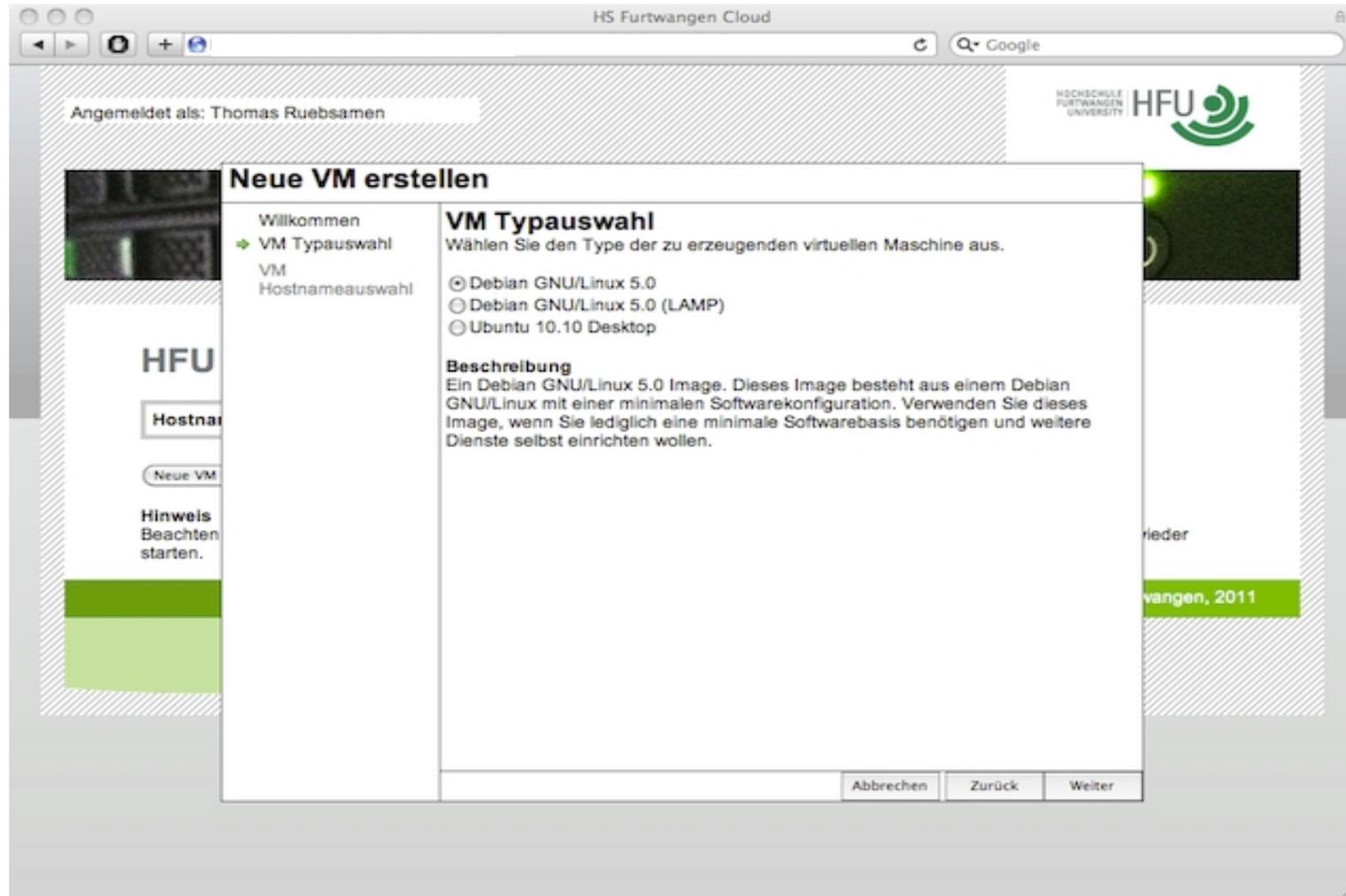
Cloud
Research Lab

Grundlagen
Shibboleth

Shibboleth
Web-Proxy

Cloud Web
GUI

Demo



Cloud GUI – Create VM Wizard

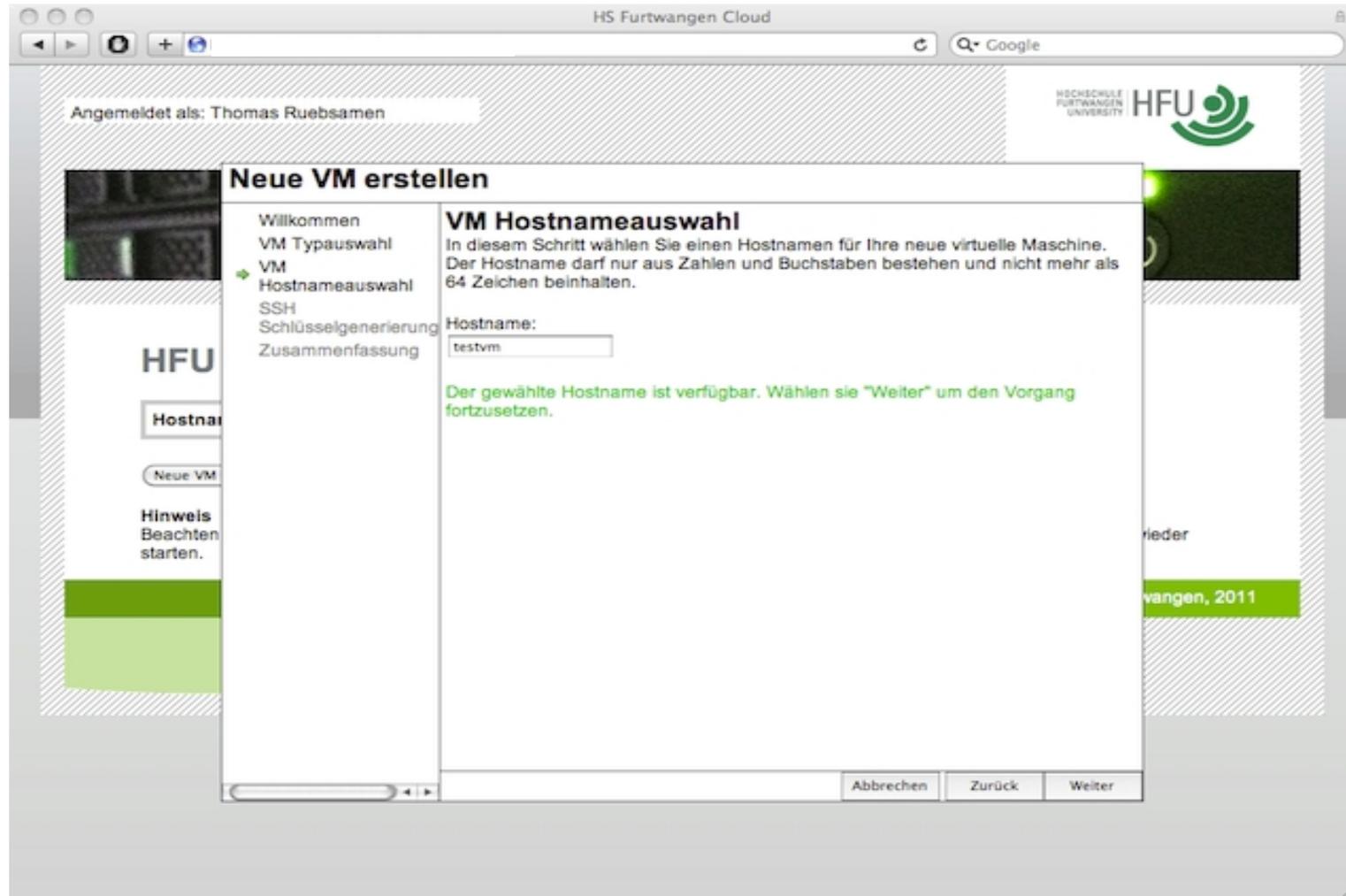
Cloud
Research Lab

Grundlagen
Shibboleth

Shibboleth
Web-Proxy

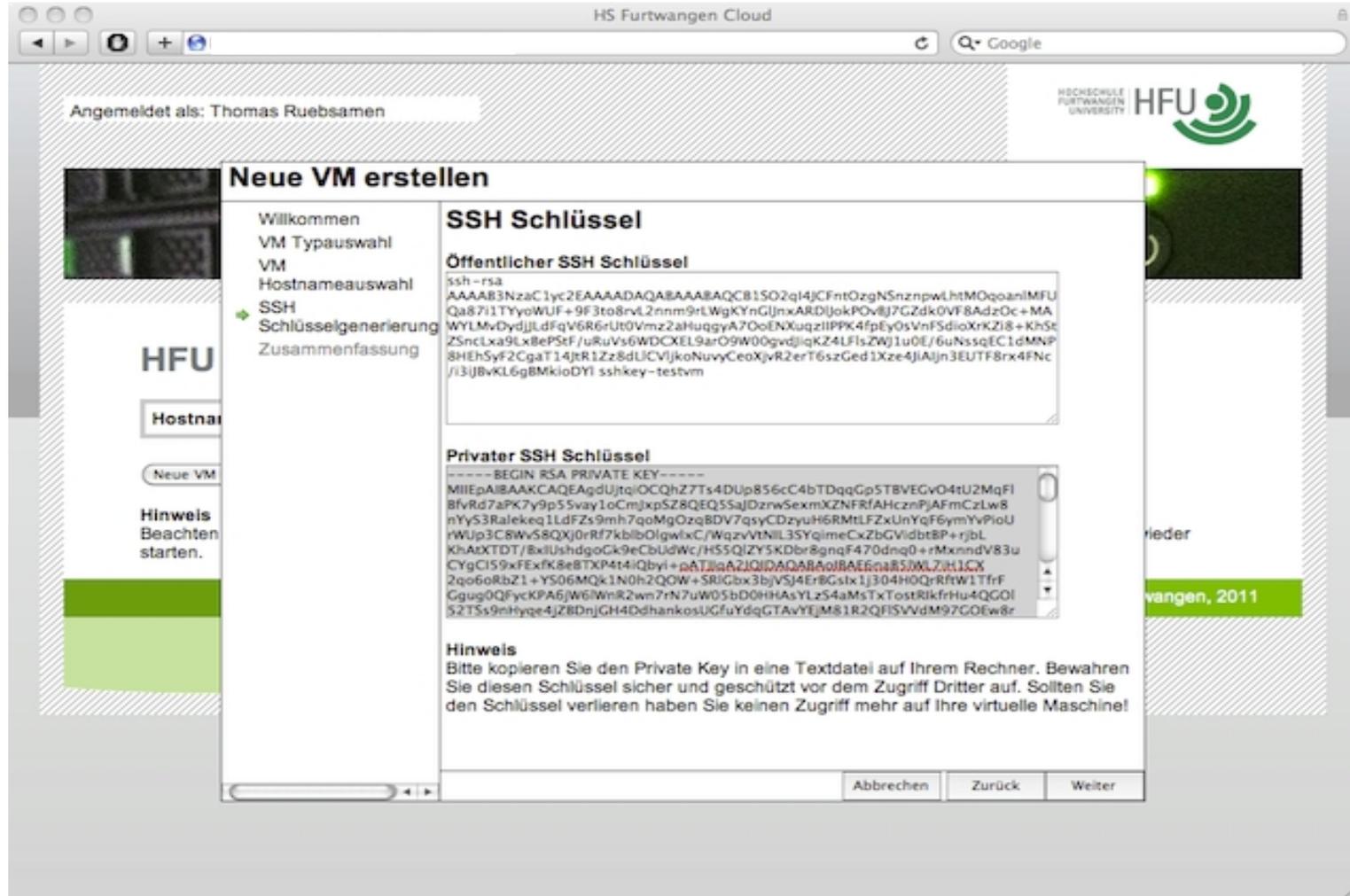
Cloud Web
GUI

Demo



Cloud GUI – Key Generation (1)

Cloud Research Lab
 Grundlagen Shibboleth
 Shibboleth Web-Proxy
 Cloud Web GUI
 Demo



Cloud GUI – Key Generation (2)

Cloud Research Lab
Grundlagen Shibboleth
Shibboleth Web-Proxy
Cloud Web GUI
Demo

The screenshot shows a web-based interface for creating a new VM. A modal window titled "Neue VM erstellen" is open, displaying the "SSH Schlüssel" step. The wizard progress is as follows:

- Willkommen
- VM Typauswahl
- VM
- Hostnameauswahl
- SSH (highlighted with a green arrow)
- Schlüsselgenerierung
- Zusammenfassung

The "SSH Schlüssel" section contains a warning: "Bitte speichern sie die generierten Schlüssel lokal auf ihrem Rechner. Bewahren sie vor allem den privaten Schlüssel sorgfältig an einem geschützten Ort auf. Sollten sie ihn verlieren, haben sie keinen Zugriff mehr auf ihre VM. Dieser Wizard wird erst fortgesetzt, wenn zumindest der private Schlüssel gespeichert wurde!" Below the warning, it states "Schlüsselpaarberechnung erfolgreich abgeschlossen" and provides two buttons: "Public Key speichern" and "Private Key speichern".

In the background, the "Hostname" field is filled with "frank3D". A "Hinweis" box at the bottom left says "Beachten starten." The bottom right of the modal has "Abbrechen" and "Weiter" buttons. The footer of the page includes "wangen, 2011".

Cloud
Research Lab

Grundlagen
Shibboleth

**Shibboleth
Web-Proxy**

**Cloud Web
GUI**

Demo

- Shibboleth Web-Proxy für Cloud Services
- Reduktion von Service Providern
- Im Rahmen des CloudIA-Projektes implementiert
- Shibboleth Aktivierung per Mouse-Klick in PaaS/SaaSzenario möglich
- CloudIA WebGUI per Shibb@HFU LDAP
- Einfache SSH-Key Erstellung im Browser des Clients

Cloud
Research Lab

Grundlagen
Shibboleth

Shibboleth
Web-Proxy

**Cloud Web
GUI**

Demo

- Lasttest und erste Tests (fakultätsintern)
- SSL Proxy
- Beseitigung des SpoF
- Einarbeitung Eurer Kommentare / Anregungen

Fragen & Antworten

Cloud
Research Lab

Grundlagen
Shibboleth

Shibboleth
Web-Proxy

Cloud Web GUI

Demo



©computing.co.uk [1]