

Das Projekt NDS-AAI

5. Shibboleth Workshop

Berlin, 17.10.2007

Peter Gietz, CEO, DAASI International
GmbH

Peter.gietz@daasi.de

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Agenda

- **Nds-AAI Motivation**
- **Projektplanung**
- **Bemerkungen zu**
 - **Fragen zur Erhebung**
 - **Anforderungen an zu shibbolisierende Anwendungen**
 - **SAML-Profil**
 - **Anschluss eines LDAP-Servers**
 - **Stresstests**
- **Status des Projekts**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Das Projekt Nds-AAI

- **Das Projekt Nds-AAI ist eine Initiative von LANIT**
 - **Landesarbeitskreis Niedersachsen für Informationstechnik der Hochschulrechenzentren**
- **Finanziert vom Niedersächsisches Ministerium für Wissenschaft und Kultur**
- **Durchgeführt im Wesentlichen durch die DAASI International GmbH**
- **Mit Mitarbeit der einzelnen Hochschulrechenzentren**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Motivation für Nds-AAI

- Das Projekt Nds-AAI baut eine landesweite Föderation auf, die es auf Grundlage einer technischen Infrastruktur ermöglicht, den lokal in ihren Heimatorganisationen verwalteten Benutzern Ressourcen der gesamten Föderation kontrolliert zur Verfügung zu stellen.
- Diese Infrastruktur soll insbesondere Studierenden ermöglichen, Lerninhalte von E-Learning-Plattformen der verschiedenen Hochschulen zu nutzen, ohne in all diesen Hochschule einen Benutzeraccount haben zu müssen.
- Die erste Anwendung, die über die Nds-AAI zugänglich gemacht werden soll, ist die E-Learning-Software StudIP.

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Warum nicht gleich DFN-AAI?

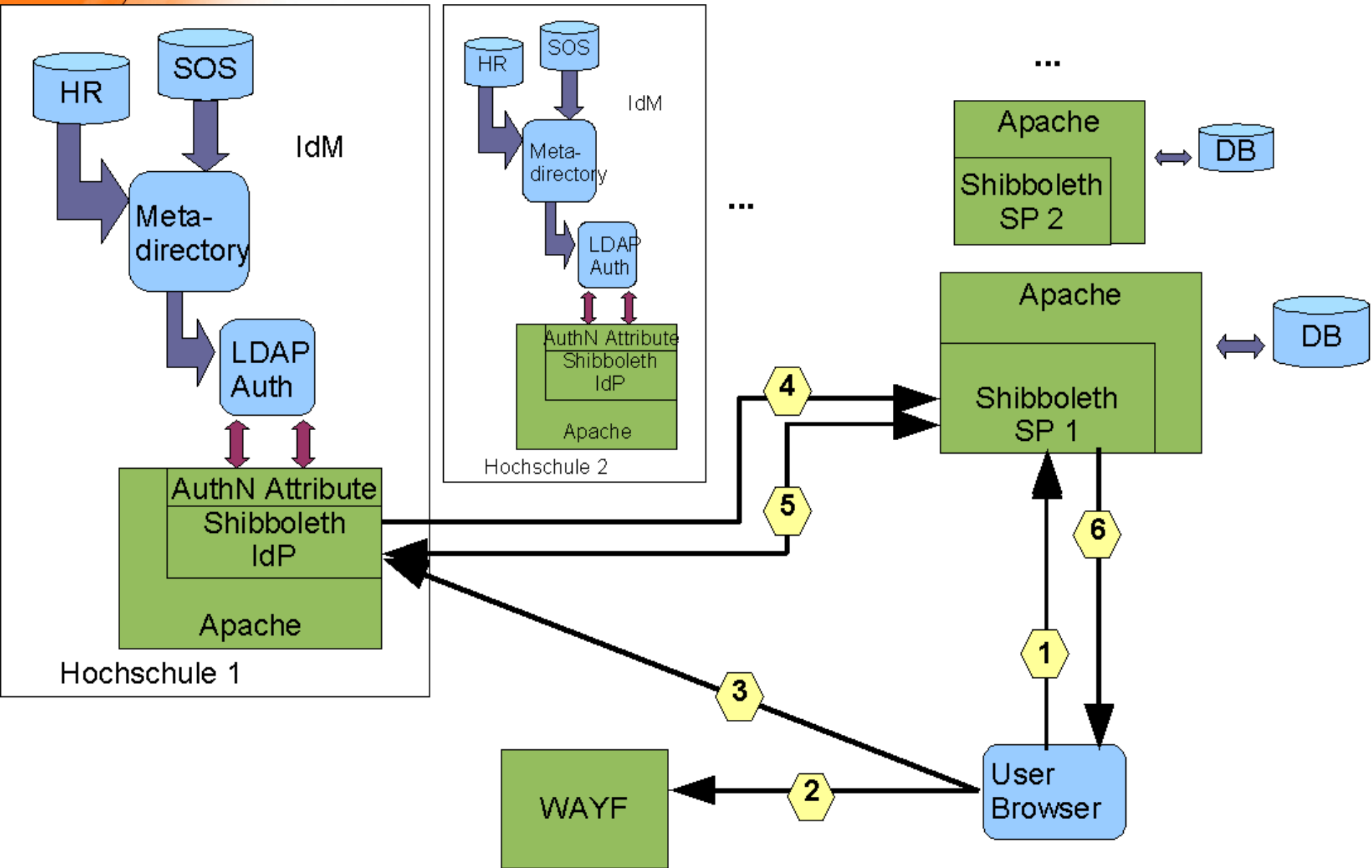
- Festdefinierter Kreis der Mitglieder: Hochschulen in Niedersachsen
- Nds-AAI ist zunächst für einen bestimmten Zweck gedacht: eLearning mit StudIP
 - Es gibt bereits eLearning-Kooperationen in Niedersachsen
- Anforderungen an die Benutzerverwaltungen können flexibel den Einsatzszenarien angepasst werden
- Im Projekt können die Hochschulen gemeinsam Voraussetzungen für die Teilnahme an der DFN-AAI erarbeiten
- Sie können aber zu unterschiedlichen Zeitpunkten der DFN-AAI beitreten
- Hochschulen können mit dem selben IdP an verschiedenen Föderationen teilnehmen

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Nds-AAI Architektur



Projektplan

➤ Phase I: Planung

- Ist-Analyse an 17 Hochschulen
- Spezifikation der Anforderungen
- Spezifikation einer Plattform (Hardware/Software)
- Implementierungsplan
- Erstellung eines Feinkonzepts
- Sicherheitsanalyse zum Feinkonzept

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Projektplan

- **Phase II: Aufbau und Test eines Prototypen**
 - **Aufbau Prototyp**
 - **Spezifikation von Testszenarien und deren Implementierung**
 - **Installation von Shibboleth IdP und SP auf drei Rechnern, Installation eines WAYF-Servers auf einem der drei Rechner**
 - **Implementierung der Shibbolisierung von StudIP**
 - **Konfiguration und Dokumentation der Konfiguration**
 - **Gesamtdokumentation Prototyp**
 - **Test Prototyp**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Projektplan

- **Phase III: Implementierung und Pilot**
 - **Implementierung**
 - **Installation und Test des getesteten Prototyps auf 18 Rechnern**
 - **Implementierungsbericht**
 - **Anschluss an die lokalen Infrastrukturen**
 - **Hochschulspezifische Betriebsdokumentationen**
 - **Exemplarische Anbindung an bestehende Förderationen**
- **Dokumentation des Gesamtsystems**
- **Pilotbetrieb, einschließlich Helpdesk über 4 Wochen**
- **Abschlussbericht**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Projektplan

- **Phasenbegleitende Maßnahmen**
 - **Schulungs- und Marketingmaßnahmen**
 - **Durchführung eines Workshops zur Einführung in Shibboleth, Diskussion der individuellen Voraussetzungen an den einzelnen Hochschulen und Projektvorstellung**
 - **Durchführung eines Workshops zum Betrieb der Infrastruktur**
 - **Vorträge zum Nds-AAI-Projekts in einschlägigen Arbeitskreisen, insbesondere im ZKI-AK Verzeichnisdienste und DFN-AAI-Veranstaltungen**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Projekt – Phase I

- **Ist-Analyse an 17 Hochschulen**
 - **Interview-Fragebogen definieren**
 - **Erhebung der Kontaktdaten der an den einzelnen Hochschulen zuständigen Mitarbeiter**
 - **Datenerhebung während der Telefoninterviews**
 - **Erstellung von Interview-Protokollen**
 - **Analyse der Interview-Ergebnisse**
- **Erstellung eines Bericht zur Ist-Analyse**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Projekt – Phase I

- **Spezifikation der Anforderungen**
 - **Anforderungen, die sich aus der Ist-Analyse ergeben**
 - **Funktionale Anforderungen**
 - **Anforderungen an das Benutzer-Interface (Login, WAYF)**
 - **Anforderungen, die sich aus den anzuschließenden Anwendungen ergeben (StudIP)**
 - **Anforderungen, die sich aus einem möglichen Beitritt zur DFN AAI ergeben**
 - **Sicherheitsanforderungen**
 - **Datenschutzanforderungen**
 - **Spezifikation einer Plattform (Hardware/Software)**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Projekt – Phase I

- **Erstellung eines Feinkonzepts**
 - **Funktionelle Beschreibung des Gesamtsystems**
 - **Architektur des Gesamtsystems**
 - **Schnittstellenbeschreibung (LDAP, SAML, PKI)**
 - **Spezifikation der Authentifizierungsvorgänge und Autorisierungsvorgänge**
 - **Spezifikation eines LDAP-Schemas für Autorisierungsattribute**
 - **Spezifikation eines SAML-Profiles**
 - **Mindestvoraussetzungen an die Identity-Management-Systeme der Einzelhochschulen**
 - **Spezifikation der einzelnen Komponenten des Gesamtsystems (PKI, IdP, SP, WAYF, Policy Server)**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Projekt – Phase I

- **Sicherheitsanalyse zum Feinkonzept**
 - **Datenschutzanalyse (Datenarten, Datenhoheit, Datenübertragung, Einverständnis der Teilnehmer)**
 - **Spezifikationen der Sicherheitsmaßnahmen**
 - **Sicherheitsanalyse (mögliche Angriffe auf das System, Analyse, ob Sicherheitsmaßnahmen solche Angriffe verhindern können)**
 - **Anpassung der Datenschutzvereinbarung**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Projekt – Phase II

- **Aufbau Prototyp**
 - **Spezifikation von Testszenarien und deren Implementierung**
 - **Installation von Shibboleth 1.3 IdP und SP auf drei Rechnern, Installation eines WAYF-Servers auf einem der drei Rechner**
 - **Implementierung der Shibbolisierung von StudIP**
 - **Konfiguration und Dokumentation der Konfiguration**
 - **Gesamtdokumentation Prototyp**
- **Test Prototyp**
 - **Durchführung der Testszenarien**
 - **Testbericht und Abnahme**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Projekt – Phase III

- **Anschluss an die lokalen Infrastrukturen**
 - **Vorbereitung der lokalen IdPs und Beratung der einzelnen Hochschulen (LDAP-Schema, Attribut-Mapping, Hilfe bei eventuellen Datenmigrationen, etc.)**
 - **Anschluss der IdPs an die vorhandenen Identity Management Systeme, zentralen Authentifizierungs- Server oder zentralen Benutzerverwaltungen**
- **Hochschulspezifische Betriebsdokumentationen**
- **Pilotbetrieb**
- **Abschlussbericht**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Relevante Fragenbereiche

- **Gibt es überhaupt eine geeignete zentrale Benutzerverwaltung**
 - über die Authentifizierungsprozesse abgewickelt werden können in der zum Zwecke der Autorisierung föderationsrelevante Informationen über die Benutzer gepflegt werden.
- **Welche relevanten Attribute werden vorgehalten**
 - Zur Basisrolle (Studierender, Dozent, Angestellter, Mitglied, etc.)
 - Zugehörigkeit zu einzelnen Organisationseinheiten oder Fakultäten
 - Eindeutige Ids, sowie Kontaktdaten gelegt wurde.

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Relevante Fragenbereiche

- **Aktualität der Daten**
 - **Ob Account frühzeitig nach Eintritt in die Hochschule (ob als Studierender oder Mitarbeiter) angelegt werden**
 - **ob Accounts bzw. föderationsspezifische Attributinformationen auch zeitnah nach dem Austritt aus der Hochschule deaktiviert bzw. gelöscht oder geändert werden (z.B. die Basisrolle von „student“ zu „alumn“ ändern).**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Relevante Fragenbereiche

- **Password-Policy**
 - Je einfacher ein Passwort zu erraten ist (z.B. mittels eines Dictionary-Attack), desto eher ist die Möglichkeit gegeben, dass sich ein Unberechtigter über den Account eines Benutzers authentifiziert.
- **Password-Sicherheit**
 - ob das Passwort nur über verschlüsselte Verbindungen (z.B. SSL bzw. TLS) abgefragt wird und deshalb nicht von einem Unberechtigten abgehört werden kann.
- **Alternativ zu LoginID und Passwort würden sich User-Zertifikate im Rahmen einer X.509-basierten Public Key Infrastructure (PKI) als noch stärkerer Authentifizierungsmechanismus eignen.**
 - Vorhandensein einer sicheren PKI in den einzelnen Hochschulen

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Relevante Fragenbereiche

- Da die E-Learning-Software StudIP im Rahmen der Föderation als erste Anwendung genutzt werden soll, ist es relevant, ob diese Software bereits an den einzelnen Hochschulen eingesetzt wird.
- Welcher zusätzlicher Aufwand ist an den einzelnen Hochschulen notwendig, um eine für die Föderation geeignete Authentifizierungsinfrastruktur zu implementieren.
 - Gegenwärtigen Anbindung der Benutzerverwaltungen an Quell-Systeme
 - Inwieweit die Benutzerverwaltungen bereits zur Provisionierung oder zur Authentifizierung von Anwendungen genutzt wird.
 - Zuständigkeiten für die einzelnen für Identity Management relevanten Systeme
 - Quelldatenbanken, Bibliotheksverwaltungen, Benutzerverwaltung und Datenschutz.

DAASI
International

Directory Applications
for Advanced Security
and Information Management



SAML Profil für Nds-AAI

- **SP-initiiert**
- **WAYF-vermittelt**
- **Attribut-Pull, wobei der Austausch von Attributen erst dann zwingend vorgeschrieben werden kann, wenn alle angeschlossenen Hochschulen diese bereit stellen.**

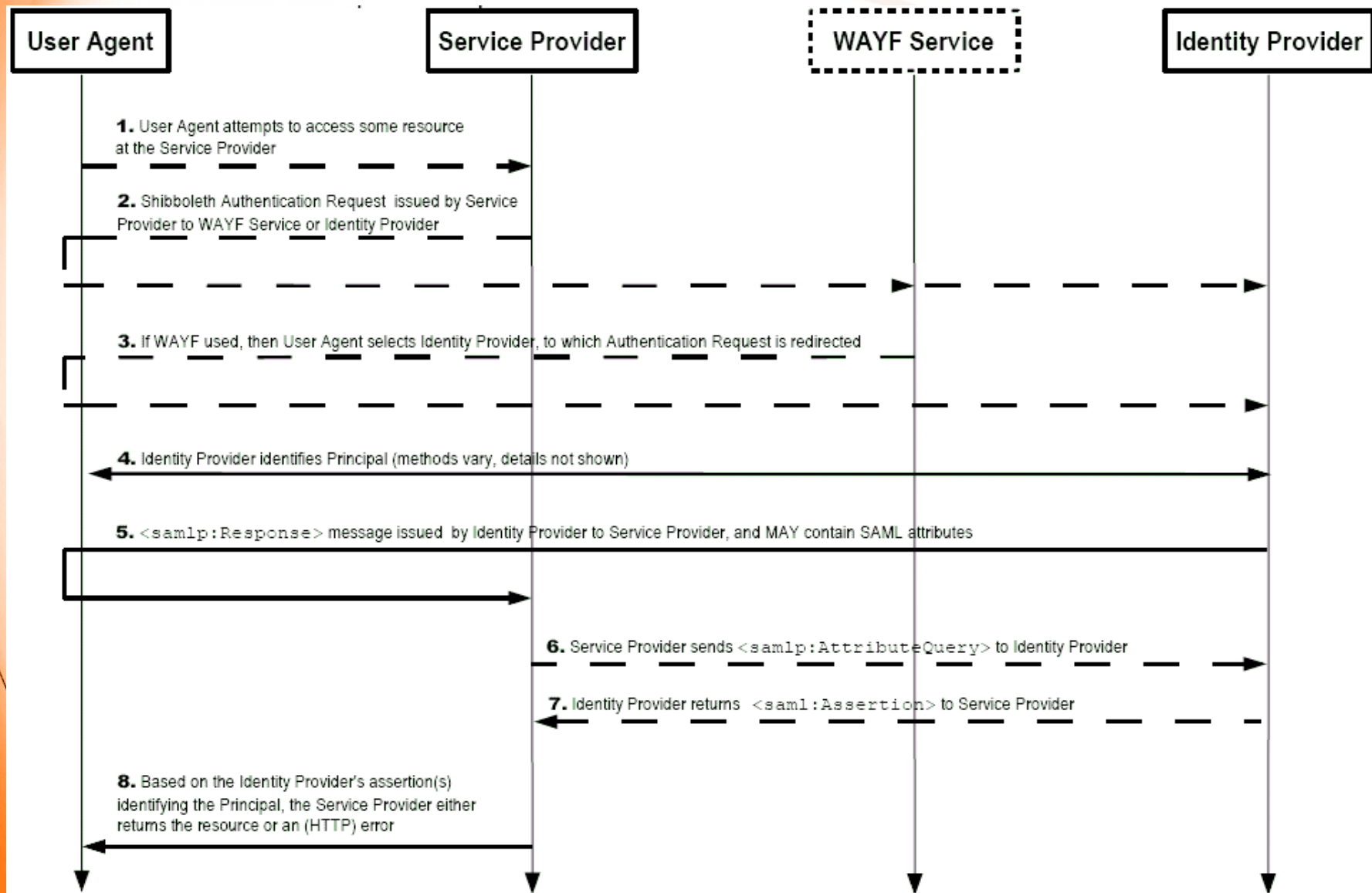


DAASI
International

Directory Applications
for Advanced Security
and Information Management



SAML Profil für Nds-AAI



Browser/POST Authentication Resonse

- Der IdP antwortet dem SP mit einer digital signierten (ds) SAML Response,
 - die ein Authentication Statement enthält,
 - im Conditions-Block wird in einem Audience-Element der SP benannt, an den die SAML Response gerichtet ist.
 - Es besteht die Möglichkeit, in der SAML Authentication Response direkt Attribute zu übergeben (Attribute Push)
- Im Fall der Nds-AAI werden jedoch standardmäßig Attribute per Pull angefordert.
 - Hierbei veranlasst der SP ein Attribute Request, das ein AttributeQuery-Element enthält.
 - Die AA (Attribute Authority) des IdP antwortet mit einer SAML Response, die ein Attribute Statement enthält



Vhosts und Zertifikate

- **IdP und SP sollen auf dem gleichen Rechner implementiert werden können**
 - **Ein vhost auf Port 443 mit allgemeinen IdP- und SP-relevanten Einstellungen und**
 - **ein vhost auf Port 8443 für die AA.**
 - **Beide vhosts verwenden dasselbe Schlüssel/Zertifikatspaar und binden ein Wurzelzertifikat ein**
- **Es werden aber augenblicklich noch weitere Lösungen dieses Problems evaluiert:**
 - **verschiedene Vhosts mit je einer eigenen IP-Adresse**
 - **alle Teile IdP, SP, AA mit je einem eigenen Port**
 - **Über SubjectAltName in ein Zertifikat mehrere Vhost-Namen eintragen.**



Anschluss des LDAP-Servers

- Der IdP kann über LDAP authentifizieren. Hierfür stehen zwei Möglichkeiten zur Verfügung:
 - die Authentifizierung erfolgt durch Apache: Einfache Konfiguration von Basic Authentication mit `mod_auth_LDAP`
 - die Authentifizierung erfolgt direkt von Tomcat. Diese Variante hat den Vorteil, dass man statt eines nicht konfigurierbaren Pop-Up-Fensters eine gestaltete Login-Seite verwenden kann
- Beide Varianten unterstützen auch Verschlüsselung via `ldaps` bzw. `START_TLS`
- Die Tomcat-Authentifizierung findet in den Niederungen der Java-Welt statt (JNDI, JSSE, JAAS)
 - Die Server- bzw. CA-Zertifikate müssen für die Zertifikatsprüfung in den Keystore von Java geladen werden

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Anschluss des LDAP-Servers

- Der LDAP-Server kann das gleiche Server-Zertifikat wie der Apache verwenden (wenn beide Server auf dem gleichen Rechner implementiert werden)
- Um sicher zu stellen, dass das Passwort nie unverschlüsselt über das Netz geht, muss im LDAP-Server entsprechende Konfigurationsparameter gesetzt werden

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Funktions- und Belastungstests

- **Der Prototyp wurde auf 4 Rechnern implementiert:**
 - 4 IdPs mit je einem LDAP-Server
 - 4 SPs
 - 1 WAYF
- **Die Funktionstests zur Authentifizierung, Autorisierung und SSO wurden erfolgreich abgeschlossen**
- **Es wurden mittels Web-Client-Skripte Belastungsszenarien simuliert und gemessen**
 - **Verschiedene Szenarien für Spitzen- und Dauerlasten**
 - **Um weitere SP-Aktivitäten zu simulieren wurden gleichzeitig Primzahlberechnungen durchgeführt**
 - Nicht ganz realitätsnah, da kein I/O

DAASI
International

Directory Applications
for Advanced Security
and Information Management



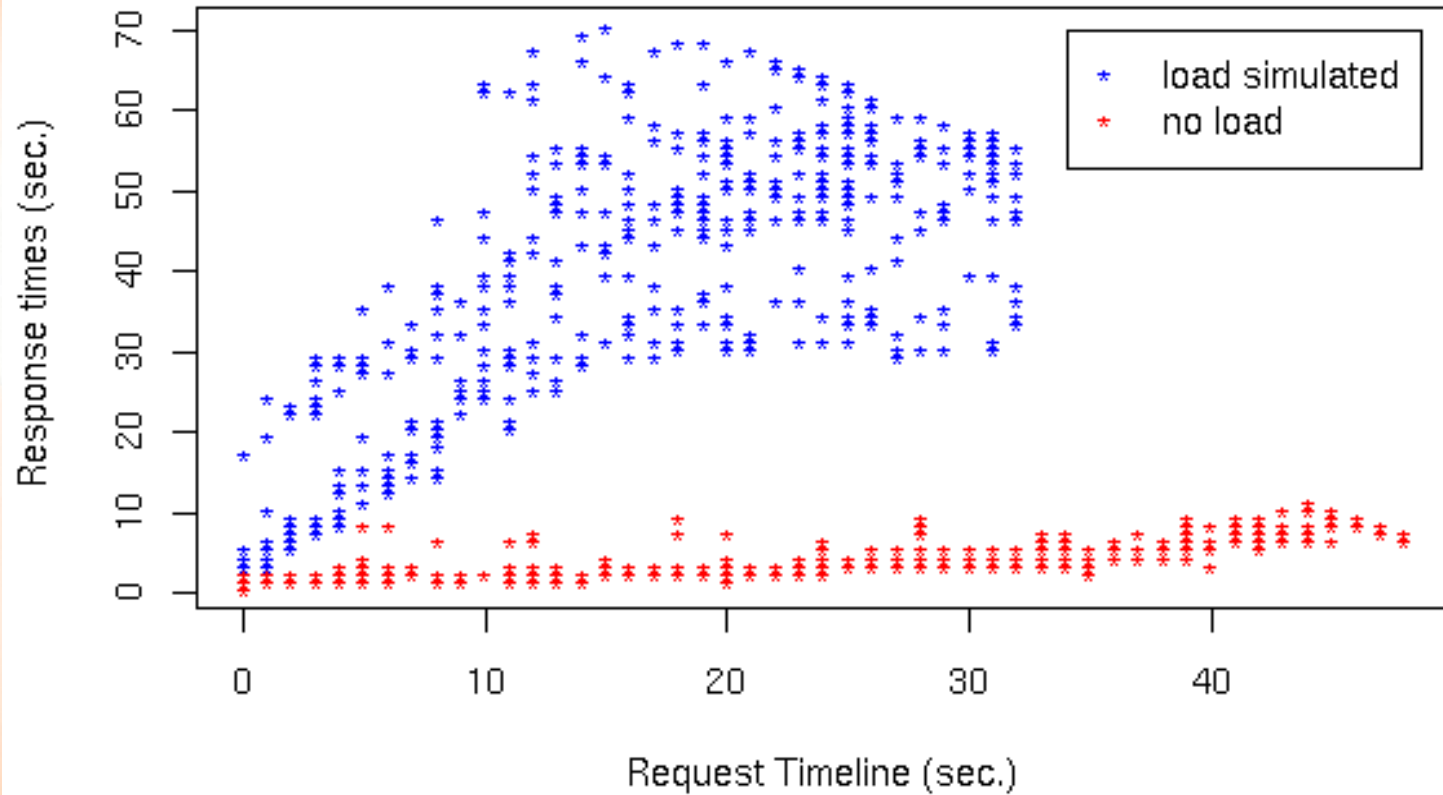
Test-Szenario 1

- Der IdP, der SP und der WAYF liegen zusammen auf einem Server und werden von einem der gerade nicht benutzen Servern gleicher Bauart gestresst.
- Es werden zwei Durchläufe gestartet.
 - Beim ersten berechnet die SP-Ressource über einen primitiven Algorithmus die ersten 3000 Primzahlen mit einer Laufzeit von $o(n^2)$,
 - im zweiten Durchlauf wird lediglich ein Text ausgegeben.

Modus	CPU-Auslastung auf Server	Load auf Server
Mit Primzahlberechnung	ca. 95%	ca. 17,20
Ohne Primzahlberechnung	ca. 80%	ca. 8,50



Test-Szenario 1

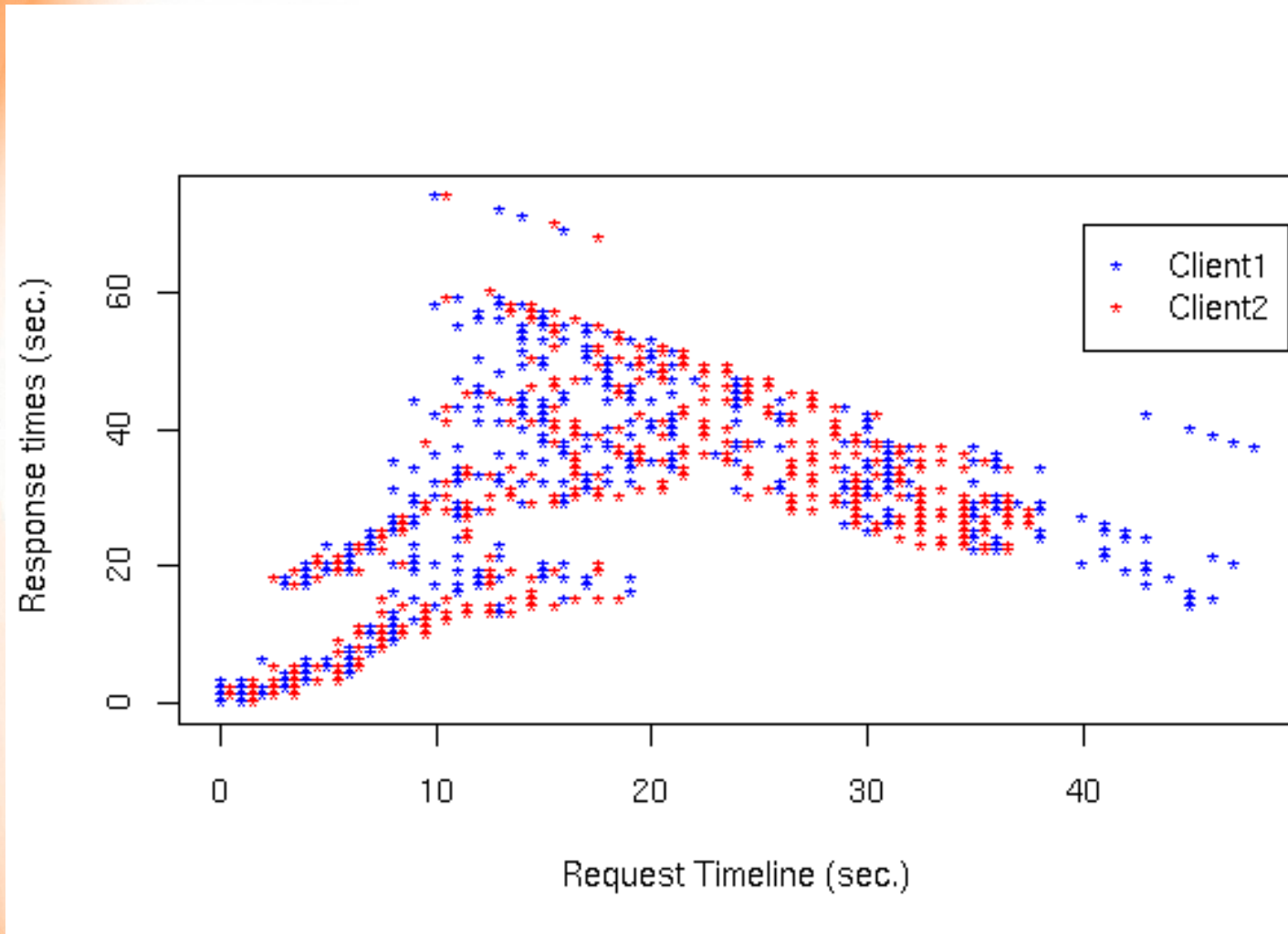


Szenario 2

- Der IdP und der WAYF liegen zusammen auf einem Server, die angeforderte Ressource liegt auf einem zweiten, identischen Server.
- Durch den Aufruf der Ressource werden beide Server gestresst, wobei die Ressource selbst (ein PHP-Skript, das einen Text ausgibt) nur geringe Rechenzeit beansprucht.
- Jeder der stressenden Clients stellt 500 Anfragen in möglichst kurzer Zeit. Simuliert wird hierdurch eine temporäre Spitze.
- Die durchschnittliche Anzahl von Anfragen pro Sekunde betrug 27,78.



Szenario 2



DAASI
International

Directory Applications
for Advanced Security
and Information Management



Szenario 3

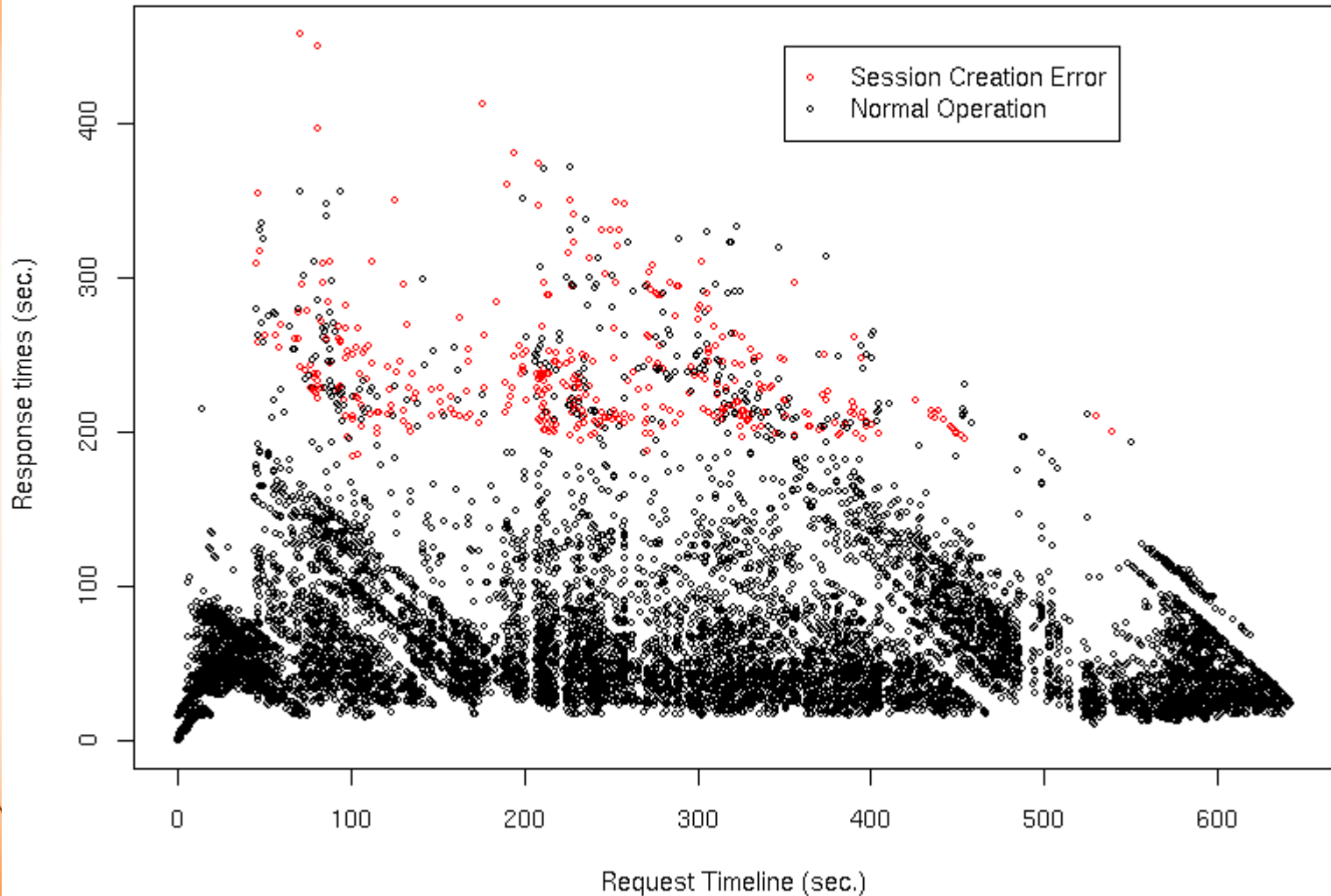
- Der IdP und der WAYF liegen zusammen auf einem Server, die angeforderte Ressource liegt auf einem zweiten, identischen Server.
- Durch den Aufruf der Ressource werden beide Server gestresst, wobei die Ressource selbst (ein PHP-Skript, das einen Text ausgibt) nur geringe Rechenzeit beansprucht.
- Jeder der beiden baugleichen Clients stellt 5000 Anfragen in möglichst kurzer Zeit. Dadurch wird eine anhaltende hohe, aber in Schüben auftretende Belastung simuliert.
- Beim Übergang von 500 zu 5000 Requests zeigt es sich, dass plötzlich deutlich viele Session Creation Errors zurück geliefert werden.
 - Als Ursache lässt sich nur vermuten, dass das Problem bei den Clients liegt, die 5000 gleichzeitige Prozesse nicht verarbeiten können.
- Es zeigt sich auch, dass der hauptsächlich gestresste IdP die Anfragen offensichtlich in Schüben abarbeitet

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Szenario 3



Szenario 4

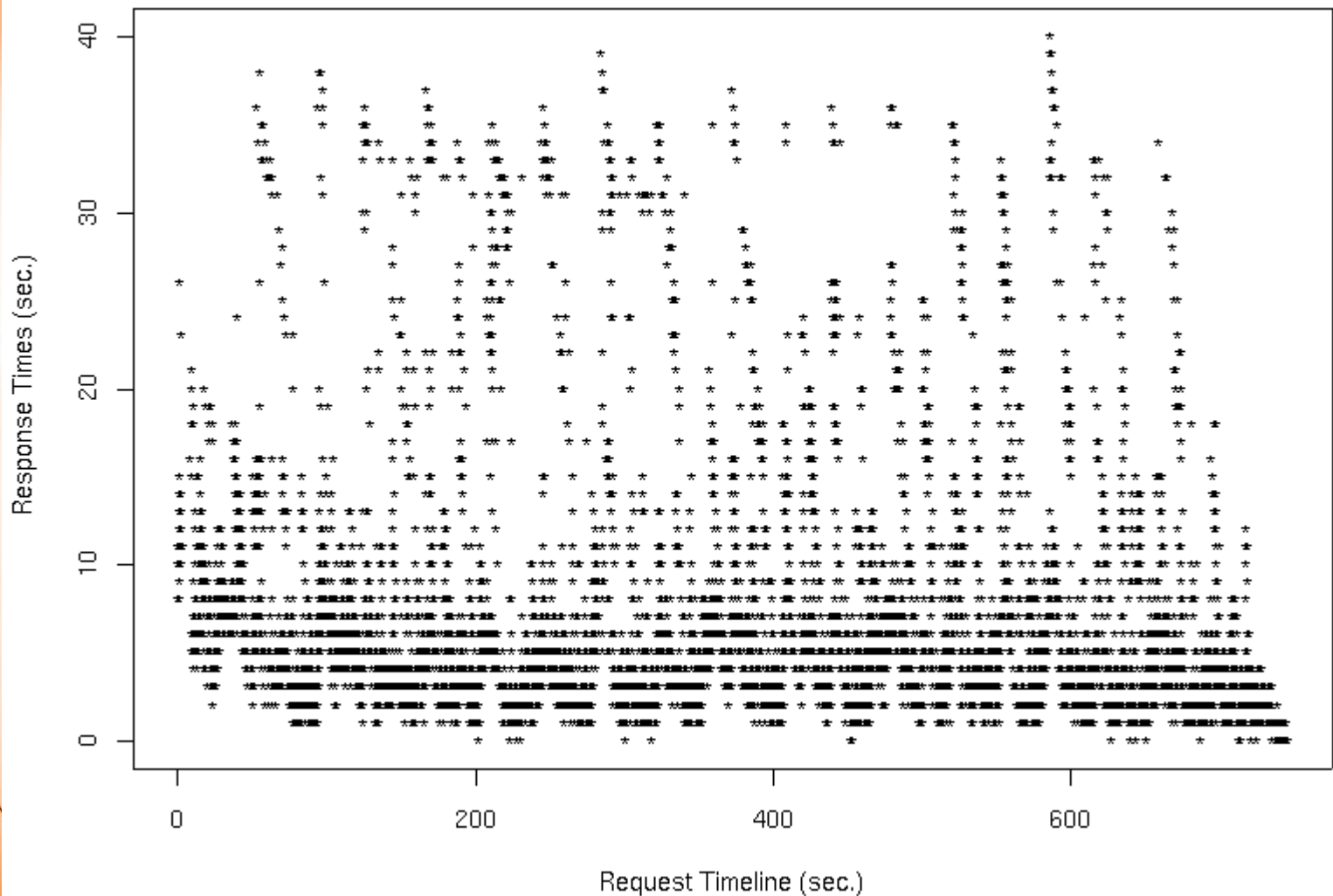
- Um die Clients nicht zu überlasten, wurden jeweils weniger (von 10 ansteigend bis zu 50) parallele Prozesse erzeugt, die dann aber sequentiell je 100 Anfragen stellen, wobei jede dieser Anfragen auf das Resultat der vorherigen Anfrage wartet.
- Jeder der Clients stellt 1000-5000 Anfragen, wobei gleichzeitig immer nur insgesamt 20-100 Anfragen beim Server eintreffen. Dadurch wird eine anhaltend hohe, konstant bleibende Belastung simuliert.
- Als Ergebnis zeigt sich, dass mit der Anstieg der Anzahl der gleichzeitig eintreffenden Anfragen auch der Mittelwert der Dauer, die von Anfrage bis Antwort vergeht, ansteigt.
 - Dies ist scheinbar linear: für die Experimentreihe 2x10, 2x20, 2x30, 2x40 und 2x50 waren die Mittelwerte 1.4535, 2.897, 4.2745, 5.691375 und 6.9587.
 - Die Anzahl der abgesetzten Anfragen pro Sekunde schwankte unregelmäßig zwischen 13.8 und 16.

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Szenario 4



Projektstatus

- **Phase I: Design: fast abgeschlossen:**
 - Erhebung, Anforderungen, Feinkonzept
 - Die Sicherheitsanalyse ist im Entstehen
- **Phase II: Prototyp: fast abgeschlossen**
 - Testsystem aus drei Rechnern installiert
 - Stud.IP (1.5 und 1.6) erfolgreich shibbolethisiert (Dank an E. Ludwig, Virtuos)
 - Testszenariendefinition und Entwicklung von Testclients für Belastungstests fertiggestellt
 - Basistests und Belastungstests wurden bereits erfolgreich durchgeführt
 - Installationsanleitung für OS und Shibboleth erstellt
- **Phasenbegleitende Maßnahmen**
 - Mehrere Workshops durchgeführt



Projektstatus

- **Phase III: Implementierung findet gegenwärtig statt**
 - **Rechner wurden an die einzelnen Hochschulen geschickt**
 - **Anleitung für eine AutoYast-gestützte SuSE-Installation erstellt**
 - **Beschreibung der Installation und Konfiguration von Shibboleth erstellt**
 - **Erste Rechner an den Hochschulen werden gegenwärtig angeschlossen**
 - **Pilotphase wird in Kürze starten**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Ausblick

- **Shibboleth 2.0 kommt langsam, aber es kommt**
 - insbesondere Single Log Out interessant
- **Weitere Anwendungen sollen angeschlossen werden**
 - weitere eLearning-Systeme
 - andere Anwendungen
- **Anschluss einzelner Hochschulen an die DFN-AAI**

DAASI
International

Directory Applications
for Advanced Security
and Information Management



Vielen Dank für Ihre Aufmerksamkeit!

➤ Kontakt und weitere Informationen:

- **DAASI International GmbH**
Wilhelmstr. 106
D-72074 Tübingen

Web: <http://www.daasi.de>

Mail: info@daasi.de

- **Mail: peter.gietz@daasi.de**

DAASI
International

Directory Applications
for Advanced Security
and Information Management

