Erfahrungen mit dem DFN-SLCS

Stefan Pinkernell

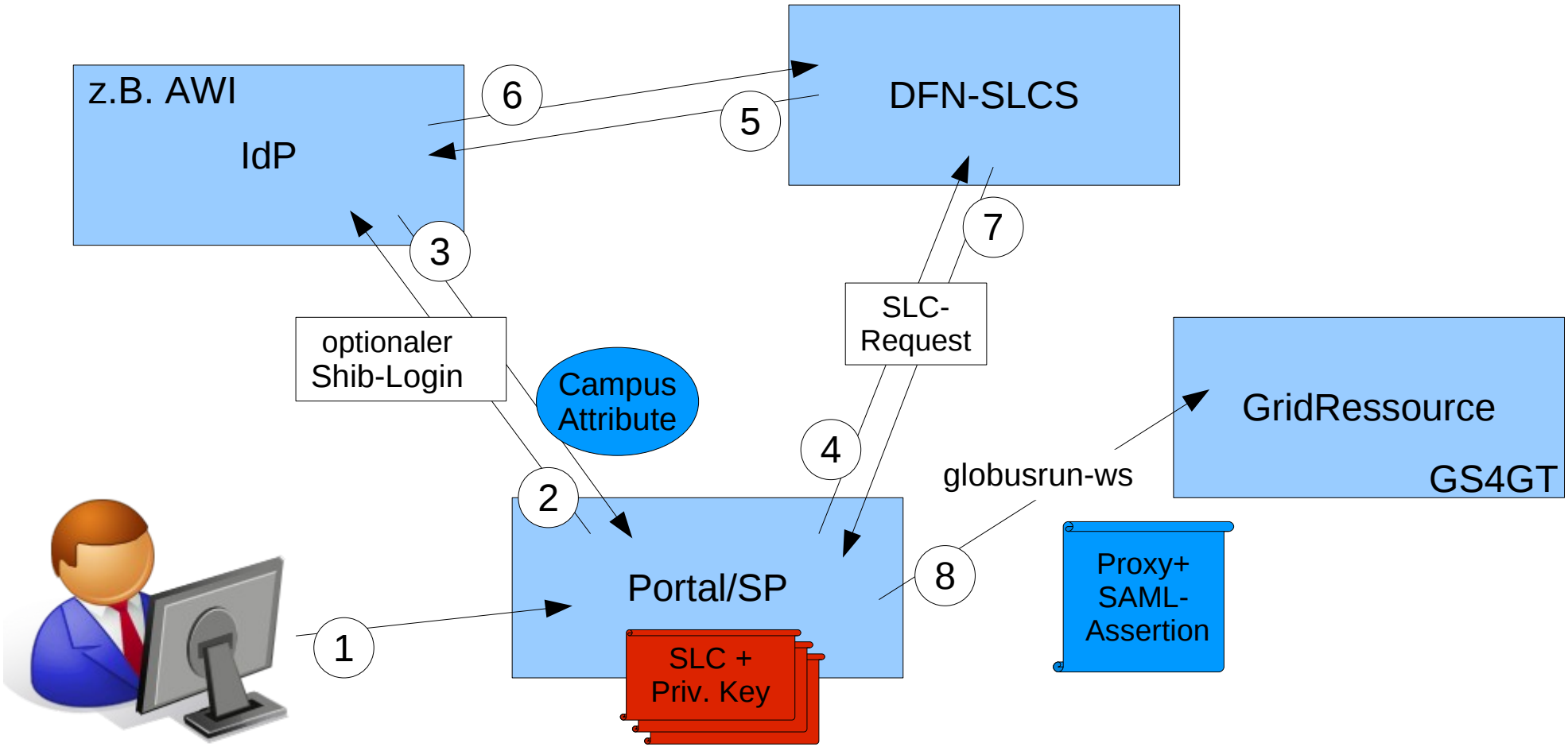
“Gap-SLC“ Workshop

21. September 2009
Göttingen

Übersicht

- Unser Use-Case / Testumgebung
- Portal Delegation
- Integration C3-Grid aus Nutzersicht
- Attribut-basierte Autorisierung

Unser Use-Case (Testumgebung)

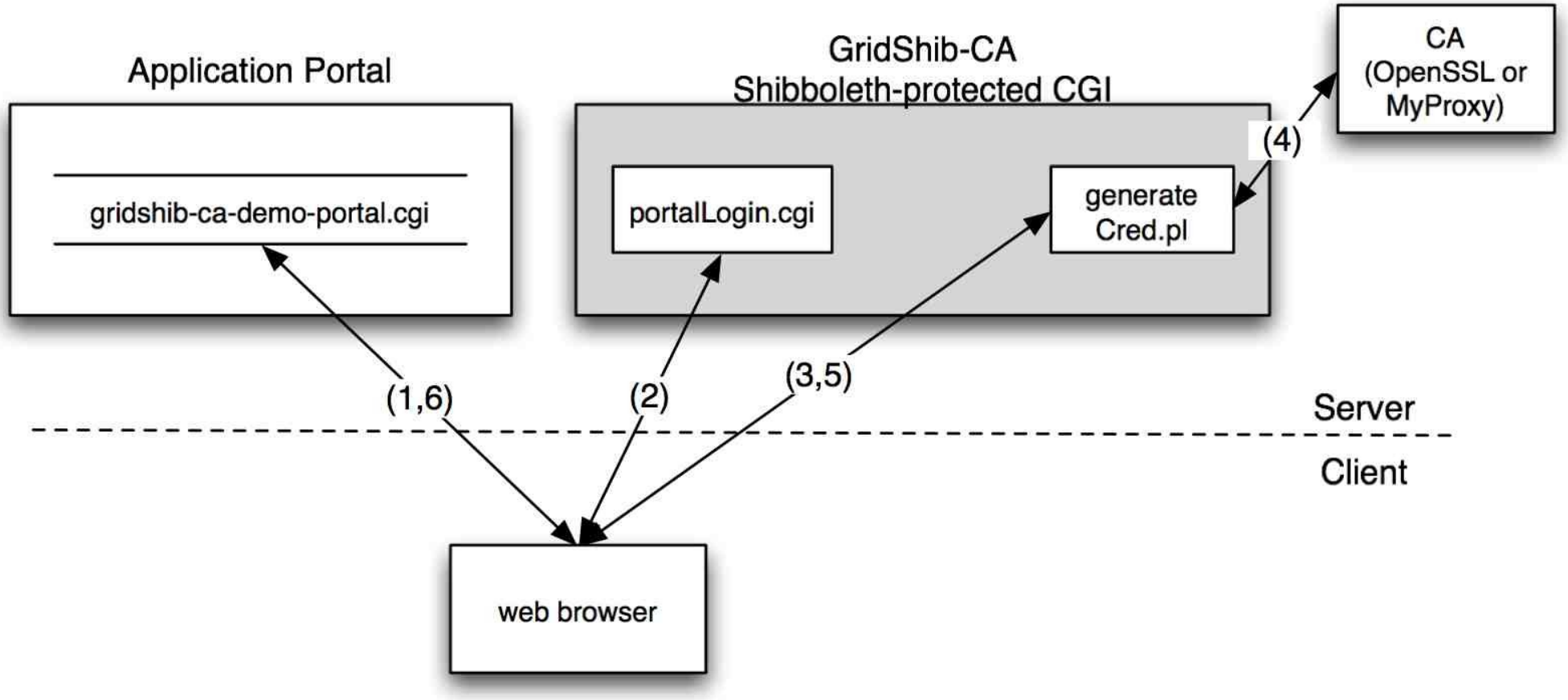


Portal Delegation

- Voraussetzungen Portal:
  - Zugang nur über https
  - Authentifizierung des Users
  - Generierung: Cert-Request und Key-Pair

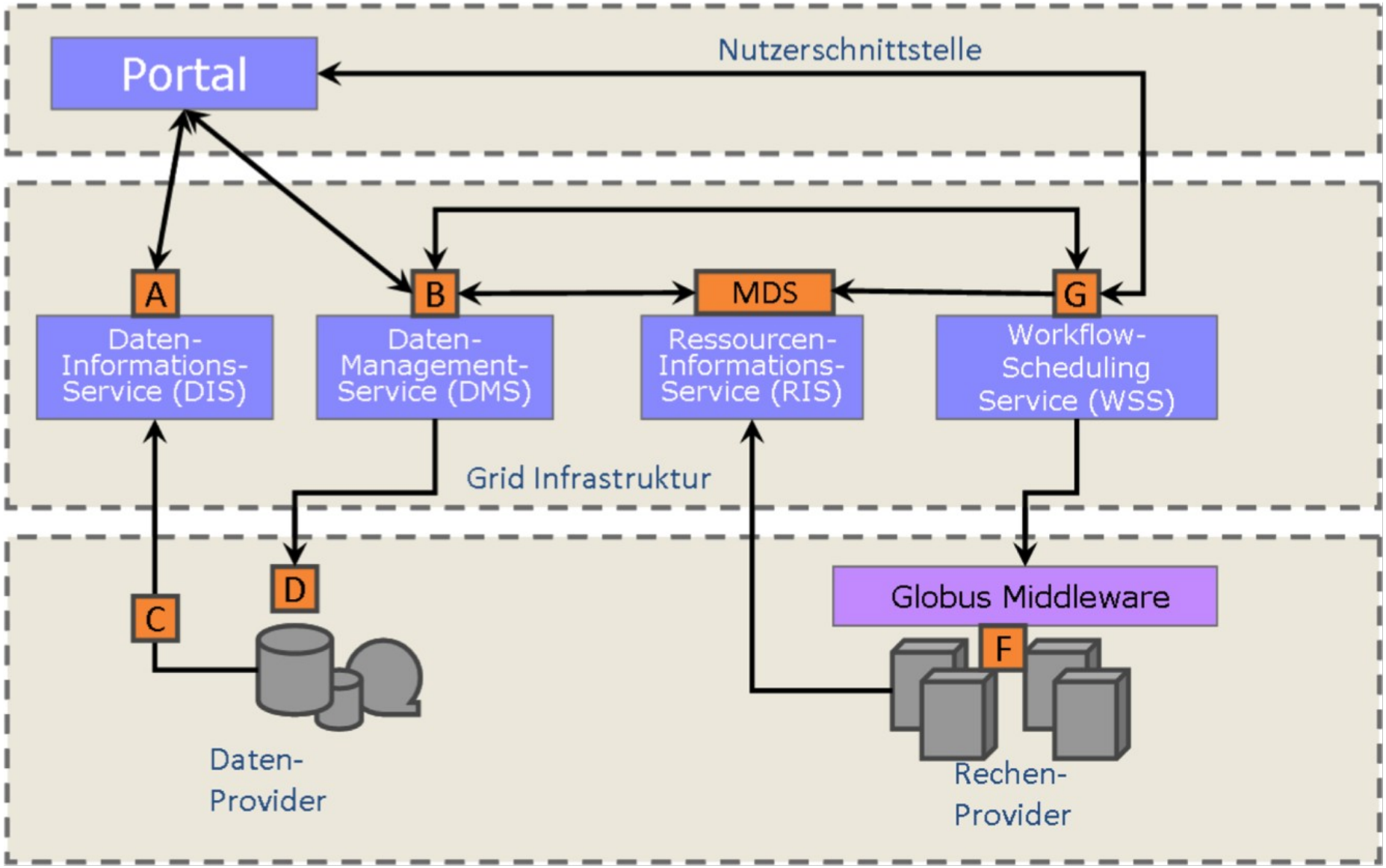
Resultat:
SLC und priv. Schlüssel liegen am Portal vor

GridShib-CA Portal Delegation

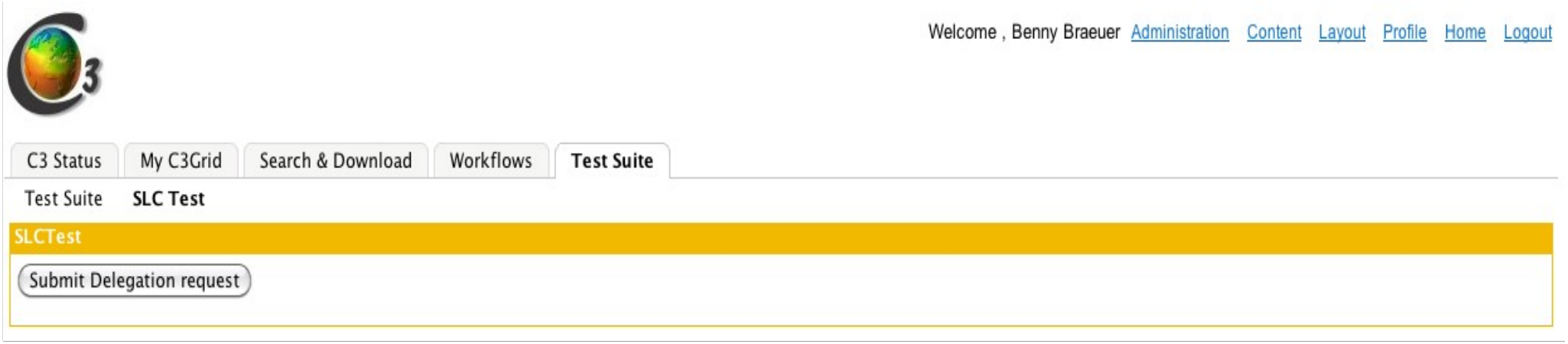


Integration in C3-Grid

- Collaborative Climate Community Data and Processing Grid
- Verteilte Datenbestände
- zentraler Zugriff über Portal
- effizientes Daten-Prozessing

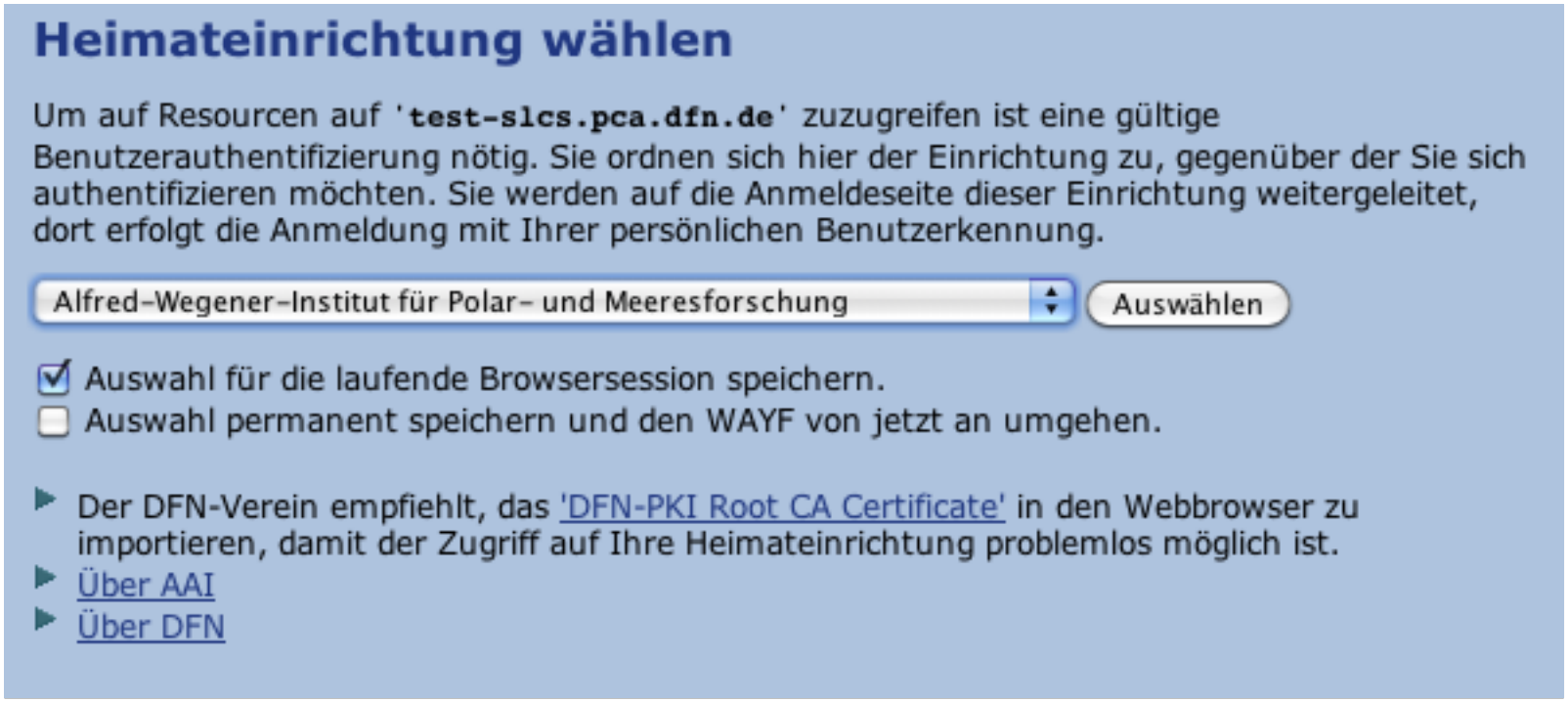

Portal
Nutzerschnittstelle
A
B
MDS
G
Daten-
Informations-
Service (DIS)
Daten-
Management-
Service (DMS)
Ressourcen-
Informations-
Service (RIS)
Workflow-
Scheduling
Service (WSS)
Grid Infrastruktur
C
D
Globus Middleware
F
Daten-
Provider
Rechen-
Provider

Voraussetzung:
Anmeldung am Portal über Nutzerdatenbank / Shib-Login



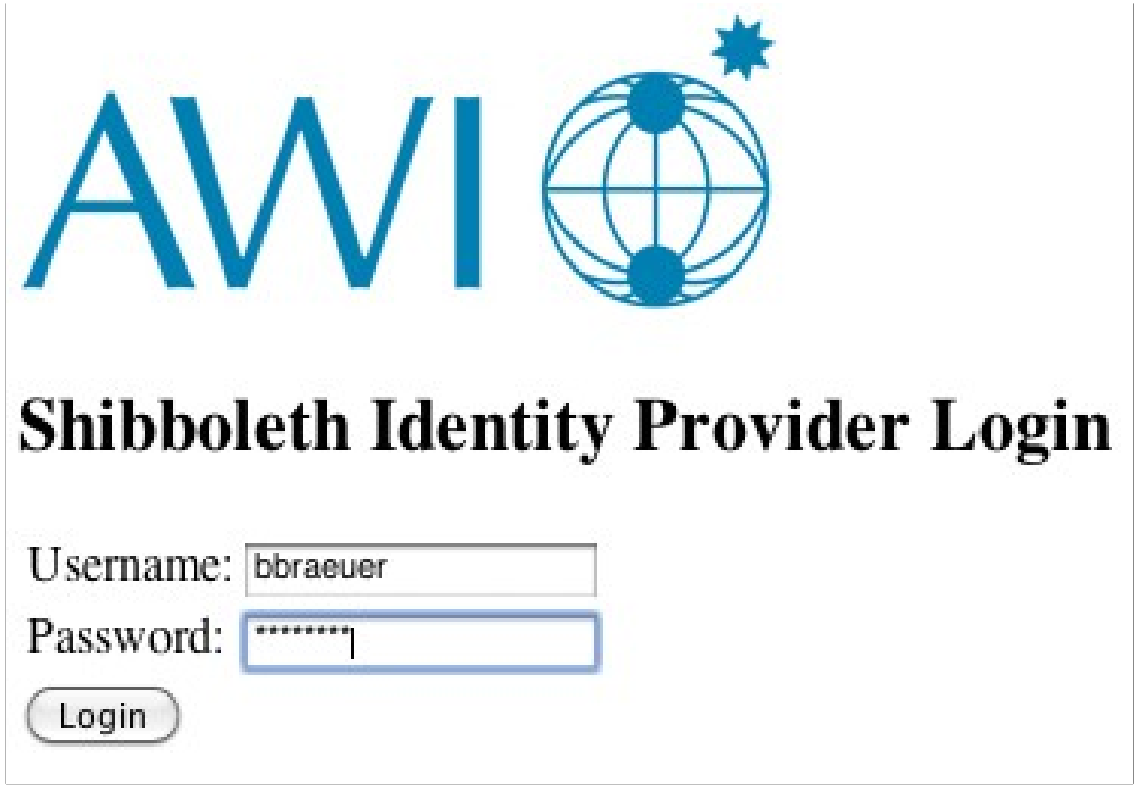
Schritt 1: Portal Delegation Script

Am Portal:
- Key Pair
- Certificate request



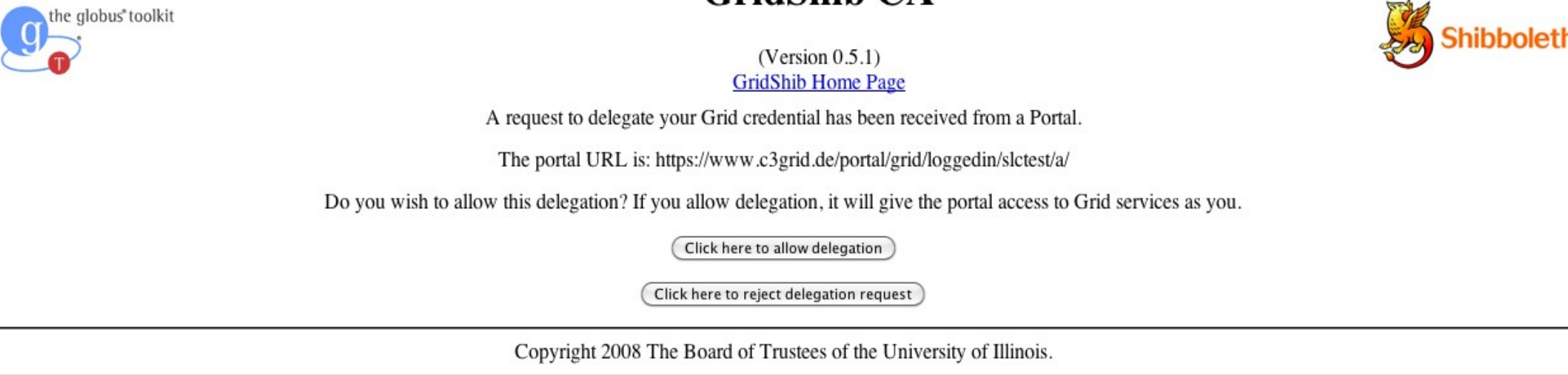
Schritt 2: WAYF

Natürlich nur, wenn zuvor noch kein Shibboleth-Login erfolgt ist!



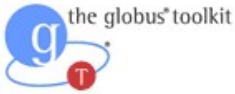
Schritt 3: Login am IdP der Heimateinrichtung

Natürlich nur, wenn zuvor noch kein Shibboleth-Login erfolgt ist!



Schritt 4: Bestätigen

→ Request wird abgeschickt
→ Zertifikat wird generiert



GridShib CA

(Version 0.5.1)
GridShib Home Page

Your certificate is ready to be returned to the portal.

Click here finish delegation and return to the portal

Schritt 5: Zurück zum Portal...

→SLC wird übergeben

SLCTest

Submit Delegation request

Certificate: /tmp/cert2476977466672782527.pem

Key: /tmp/key2476977466672782527.pem

-----BEGIN CERTIFICATE----- MIIEnDCCA4SgAwIBAgIEDr2ziDANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQGEwJE
RTETMBEGA1UEChMKREZOLVZlcmVpbjEQMA4GA1UECxMHREZOLVBLSTEkMCIGA1UE AxMbREZOLVZlcmVpbiBUZXN0LUFBSSBTTENTIENBMB4XDTA5MDkwMjA5MDgwOFoX
DTA5MDkwMjIxMDcwMVowgZQxCzAJBgNVBAYTAkRFMRMwEQYDVQQKEwpERk4tVmVy ZWluMRAwDgYDVQQLEwdERk4tUEtJMQ0wCwYDVQQLEwRTTENTMSAwHgYDVQQLExdB
bGZyZWQtV2VnZW5lci1JbnN0aXR1dDEtMCsGA1UEAxQkQmVubnkgQnJhZXVlciAt IEJlbm55LkJyYWV1ZXJAYXdpLmRlMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDIhSBNLEniQdmeXbpTUEFtkG3Ut+nErulSliZD2hzaAn6RnYQAkV4l6IhxrZVX aWvYUafN0ZXtjC65NmEWJiYaS/5VkeL8nQelax816C1QoCIzBPLfUqrAP2M8DGG7
IfURjel16gHjinSeaEBkjynSOIxzRbJkE7VbBkUPIm4bfQIDAQABo4IBsTCCAa0w DgYDVR0PAQH/BAQDAgSwMBMGA1UdJQQMMAoGCCsGAQUFBwMCMB0GA1UdDgQWBBTm vvmkTZG
+LROAWtINRdcXWzz1sjAfBgNVHSMEGDAWgBQjANzmoaLdQ3AsDyGR+qDF EHbzKTAfBgNVHREEGDAWgRRCZW5ueS5CcmFldWVyQGF3aS5kZTCBgwYDVR0fBHww
ejA7oDmgN4Y1aHR0cDovL2NkcDEucGNhLmRmbi5kZS9zbGNzLXRlc3QtY2EvcHVi L2NybC9jYWNybC5jcmwwO6A5oDeGNWh0dHA6Ly9jZHAyLnBjYS5kZm4uZGUvc2xj
cy10ZXN0LWNhL3B1Yi9jcmwvY2FjcmwuY3JsMIGeBggrBgEFBQcBAQSBkTCBjjBF BggrBgEFBQcwAoY5aHR0cDovL2NkcDEucGNhLmRmbi5kZS9zbGNzLXRlc3QtY2Ev
cHViL2NhY2VydC9jYWNlcnQuY3J0MEUGCCsGAQUFBzAChjlodHRwOi8vY2RwMi5w Y2EuZGZuLmRlL3NsY3MtdGVzdC1jYS9wdWlvY2FjZXJ0L2NhY2VydC5jcnQwDQYJ
KoZIhvcNAQEFBQADggEBAKjarbliqbHPtx772lSKejZi3EpQ6LgpngVYxJKlGQuc CxdJa5Mj3DBWQrVsPe2gFiD7GHDGuVT3aTE5a5cgt+WsZvFXa6s1yg9OBpuUF7Rc zXwFpsMeVBbr
+DabmE7GVgZCxaJ8otnNOnKTm4pcNpTK2At5TEhrzfCutIJFm2Ao HEjCmzcuNTGmbTEjtgR+4iuJvSFZ59FWue9/rICI2WKqQYiyM0vxAJFL4FBpcCto
O19N9OMrFIVZBFMvguL9HTkSW5X2eGUKF7qJw50ybBEdZk0pedAcf10xRrfUSdNT 7QCYgyUDAyyR1F7wDApW8ssKouegdndQ9MiFoZt9+ck= -----END CERTIFICATE-----

Creating Proxy...

Proxy: /tmp/proxy2476977466672782527.pem

-----BEGIN CERTIFICATE----- MIICozCCAgygAwIBAgIDDV3mMA0GCSqGSIb3DQEBBQUAMIGUMQswCQYDVQQGEwJE
RTETMBEGA1UECgwKREZOLVZlcmVpbjEQMA4GA1UECwwHREZOLVBLSTENMAsGA1UE CwwEU0xDUzEgMB4GA1UECwwXQWxmcmVkLVdlZ2VuZXItSW5zdGl0dXQxLTArBgNV
BAMMJEJlbm55IEJyYWV1ZXIgLSBCZW5ueS5CcmFldWVyQGF3aS5kZTAeFw0wOTA5 MDIwOTAzNDZaFw0wOTA5MDIyMTA4NDZaMIGoMQswCQYDVQQGEwJERTETMBEGA1UE
CgwKREZOLVZlcmVpbjEQMA4GA1UECwwHREZOLVBLSTENMAsGA1UECwwEU0xDUzEg MB4GA1UECwwXQWxmcmVkLVdlZ2VuZXItSW5zdGl0dXQxLTArBgNVBAMMJEJlbm55
IEJyYWV1ZXIgLSBCZW5ueS5CcmFldWVyQGF3aS5kZTESMBAGA1UEAxMJMjg2NjA3 NDMwMFwwDQYJKoZIhvcNAQEBBQADSwAwSAJBAJUkRDeNWc9wElabUZR6/1n6yqYZ
Ib2pyJBGkB4rP9MT0Ayswa5fR+6lKd2uZ2ygZOtdjCeLi7mqrCLYRtHtcbECAwEA AaMxMC8wHQYIKwYBBQUHAQ4BAf8EDjAMMAoGCCsGAQUFBxUBMA4GA1UdDwEB/wQE
AwIEsDANBgkqhkiG9w0BAQUFAAOBgQAmQhluWx0spSk0HZMcSMyb9COJ50HbK5yd h4u1cMx0U2WCn+BvtTZmY1sdMGFLp/Ev7EGR/iPohymvPXqsLdLSIsxi3yR/KxK6 PwGabEu/
iAhiRPSnbLcYfmTZrSMf9xCQrzI1yYkNCa073KsinBMrVLF4OxPZWBx0 uQe+/cpvKQ== -----END CERTIFICATE-----

-----BEGIN CERTIFICATE----- MIIEnDCCA4SgAwIBAgIEDr2ziDANBgkqhkiG9w0BAQUFADBaMQswCQYDVQQGEwJE
RTETMBEGA1UEChMKREZOLVZlcmVpbjEQMA4GA1UECxMHREZOLVBLSTEkMCIGA1UE AxMbREZOLVZlcmVpbiBUZXN0LUFBSSBTTENTIENBMB4XDTA5MDkwMjA5MDgwOFoX
DTA5MDkwMjIxMDcwMVowgZQxCzAJBgNVBAYTAkRFMRMwEQYDVQQKEwpERk4tVmVy ZWluMRAwDgYDVQQLEwdERk4tUEtJMQ0wCwYDVQQLEwRTTENTMSAwHgYDVQQLExdB
bGZyZWQtV2VnZW5lci1JbnN0aXR1dDEtMCsGA1UEAxQkQmVubnkgQnJhZXVlciAt IEJlbm55LkJyYWV1ZXJAYXdpLmRlMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKB
gQDIhSBNLEniQdmeXbpTUEFtkG3Ut+nErulSliZD2hzaAn6RnYQAkV4l6IhxrZVX aWvYUafN0ZXtjC65NmEWJiYaS/5VkeL8nQelax816C1QoCIzBPLfUqrAP2M8DGG7
IfURjel16gHjinSeaEBkjynSOIxzRbJkE7VbBkUPIm4bfQIDAQABo4IBsTCCAa0w DgYDVR0PAQH/BAQDAgSwMBMGA1UdJQQMMAoGCCsGAQUFBwMCMB0GA1UdDgQWBBTm vvmkTZG
+LROAWtINRdcXWzz1sjAfBgNVHSMEGDAWgBQjANzmoaLdQ3AsDyGR+qDF EHbzKTAfBgNVHREEGDAWgRRCZW5ueS5CcmFldWVyQGF3aS5kZTCBgwYDVR0fBHww
ejA7oDmgN4Y1aHR0cDovL2NkcDEucGNhLmRmbi5kZS9zbGNzLXRlc3QtY2EvcHVi L2NybC9jYWNybC5jcmwwO6A5oDeGNWh0dHA6Ly9jZHAyLnBjYS5kZm4uZGUvc2xj
cy10ZXN0LWNhL3B1Yi9jcmwvY2FjcmwuY3JsMIGeBggrBgEFBQcBAQSBkTCBjjBF BggrBgEFBQcwAoY5aHR0cDovL2NkcDEucGNhLmRmbi5kZS9zbGNzLXRlc3QtY2Ev
cHViL2NhY2VydC9jYWNlcnQuY3J0MEUGCCsGAQUFBzAChjlodHRwOi8vY2RwMi5w Y2EuZGZuLmRlL3NsY3MtdGVzdC1jYS9wdWlvY2FjZXJ0L2NhY2VydC5jcnQwDQYJ
KoZIhvcNAQEFBQADggEBAKjarbliqbHPtx772lSKejZi3EpQ6LgpngVYxJKlGQuc CxdJa5Mj3DBWQrVsPe2gFiD7GHDGuVT3aTE5a5cgt+WsZvFXa6s1yg9OBpuUF7Rc zXwFpsMeVBbr
+DabmE7GVgZCxaJ8otnNOnKTm4pcNpTK2At5TEhrzfCutIJFm2Ao HEjCmzcuNTGmbTEjtgR+4iuJvSFZ59FWue9/rICI2WKqQYiyM0vxAJFL4FBpcCto
O19N9OMrFIVZBFMvguL9HTkSW5X2eGUKF7qJw50ybBEdZk0pedAcf10xRrfUSdNT 7QCYgyUDAyyR1F7wDApW8ssKouegdndQ9MiFoZt9+ck= -----END CERTIFICATE-----

Schritt 6: SLC auf Server

Attribut-basierte Autorisierung

- Autorisierungsentscheidung an GridRessource
- SAML-Attribut (Secure Assertion Markup Language)
- Proxy-Zertifikat
- Campus Attribute, VO-Attribute, sonst. Einträge

Attributbasierte Autorisierung
- Ausblick -

- Neues Feature: signierte SAML Assertion wird am Portal hinzugefügt
- Zusammengesetzt aus untersch. Quellen
- Auswertung an GridRessource: Erweiterungen notwendig!

→ weitere Szenarien: Vortrag J. Falkner!

Zusammenfassung

- PortalDelegation Testbed
- Integration in C3-Grid
- Attribut-basierte Autorisierung

- Zu DFN-SLCS: funktioniert,
  guter Support durch DFN

Vielen Dank!

Fragen, Anregungen ?