

# **Grid Security and Identity Management**

## **Certificates - Regular, Grid and Short-lived -**

Marcus Pattloch (DFN-Verein)

GridKA School 2009

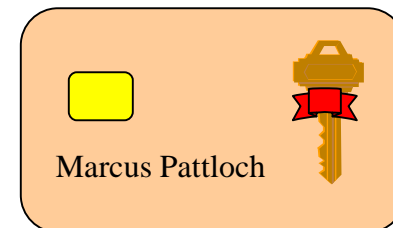
1. September 2009, Karlsruhe

- Certificates
  - what are they good for (and what not)?
- Regular Certificates
  - what (almost) everyone needs
- Grid Certificates
  - why another hierarchy?
- Short-lived Certificates (SLCS)
  - shibboleth, DFN-AAI, identity management
- Conclusions

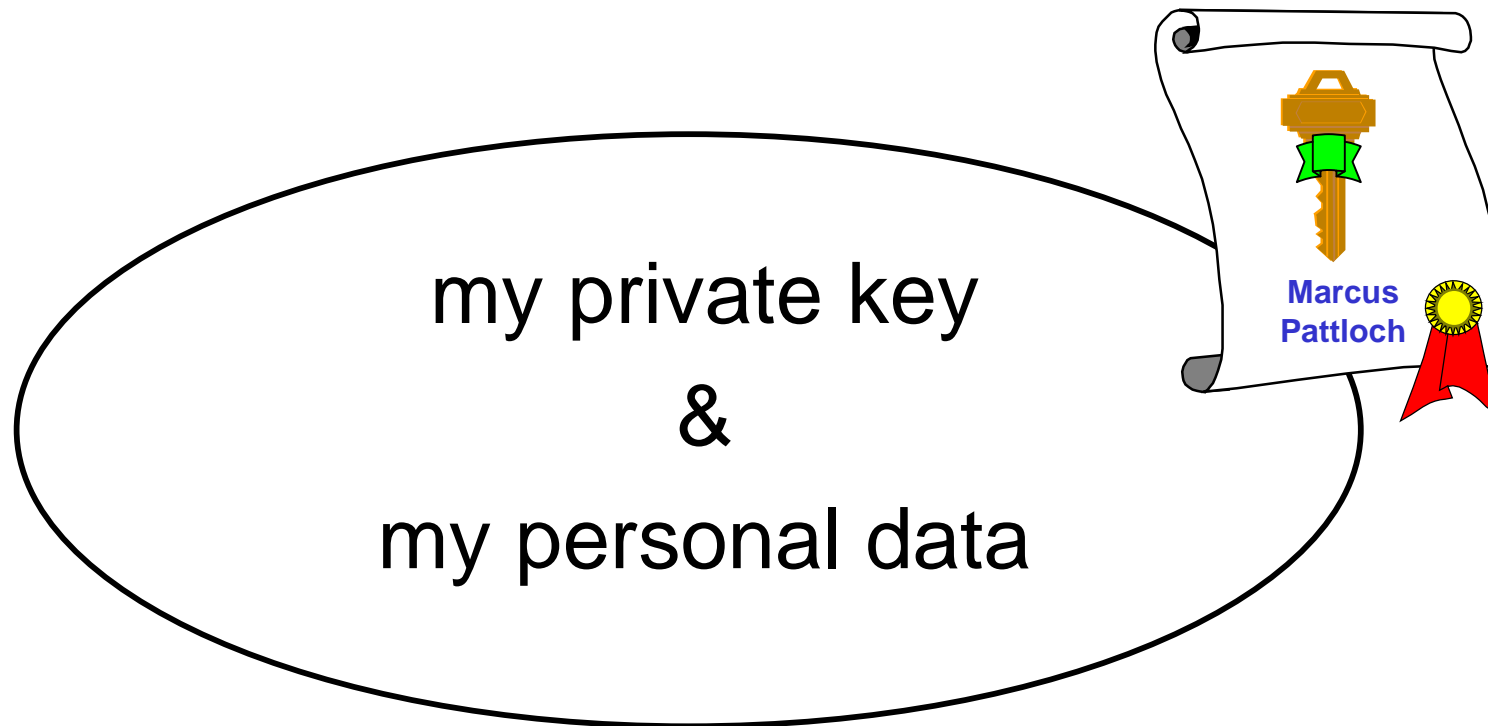
# Certificates

# What is a certificate?

- Certificate = digital identity card for use on the internet
- Once I have a certificate and use it in electronic communication, everyone can prove that I am who I claim to be
- E.g. on a „chipcard“  
(but: not every chipcard contains a certificate)



- Confidentiality
  - encryption of documents and e-mails
- Signature
  - signing .pdf documents
  - signing e-mails
  - creating time stamps on documents
- Authentication (not authorization!!)
  - server identification (SSL, https)
  - ID for access to protected websites
  - ID for access to databases etc. (ssh, IPsec)



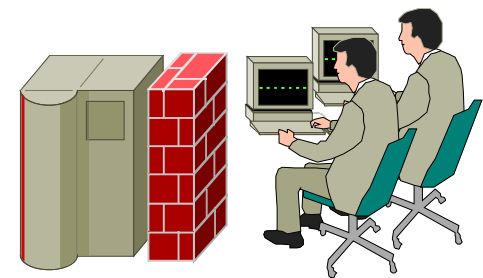
An infrastructure is needed to guarantee the link between the private key and the personal data. This is done by a public key infrastructure (PKI)

- A PKI is an infrastructure „generating“ certificates and consisting of the following main components
  - Registration Authorities (RA)
  - Certification Authorities (CA)
  - Policies
  - Directory Service for certificates
  - (PKI-aware applications)

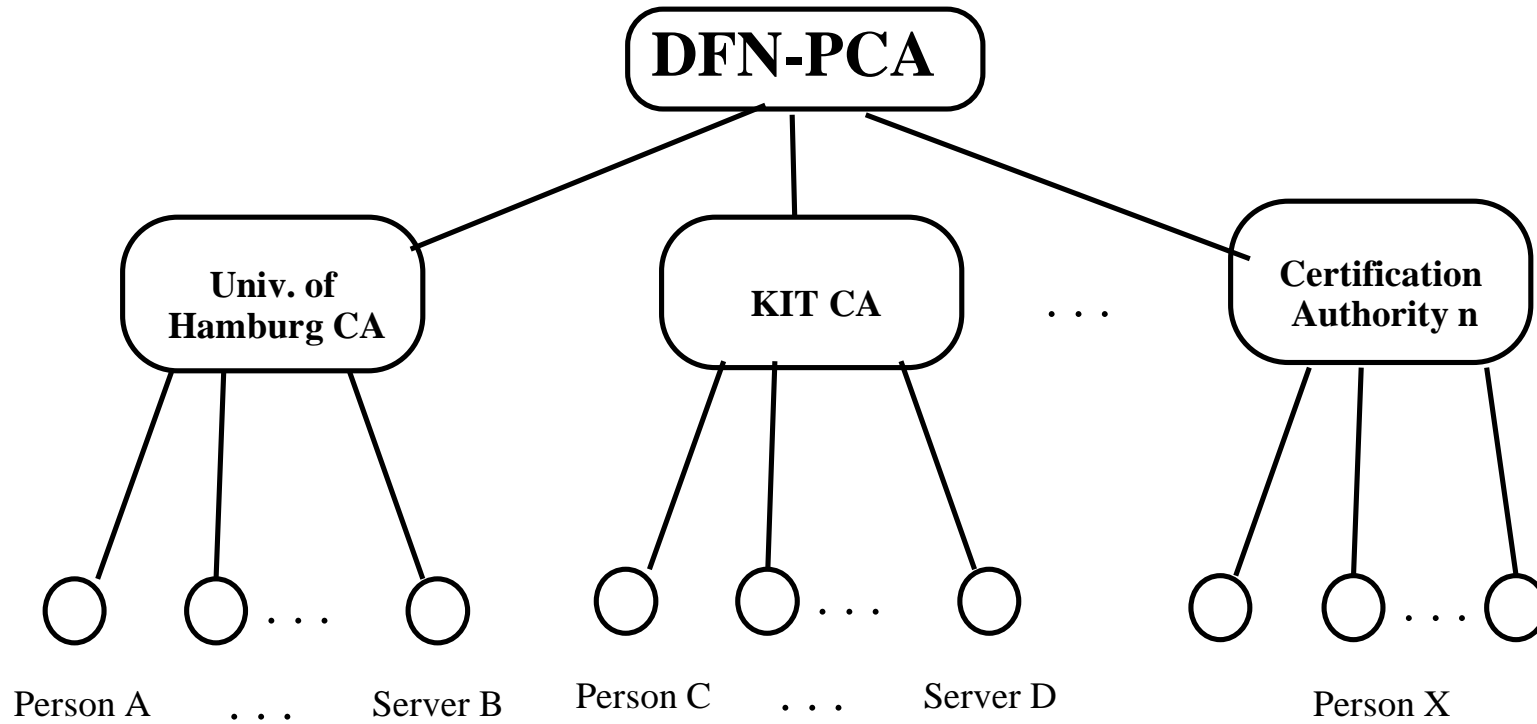
- Registration Authority
  - administrative tasks
  - done on site



- 
- Certification Authority
    - technically demanding tasks
    - organisationally demanding tasks
    - operated by DFN for all (!) sites



# Hierarchy of CAs



# List of DFN-PKI participants



Liste der ausgelagerten CAs in der DFN-PKI	
ALP Dillingen	Info-Seite
AWI - Stiftung Alfred-Wegener-Institut für Polar- und Meeresforschung	Info-Seite
Badische Landesbibliothek	Info-Seite
Bayerische Staatsbibliothek (BSB-CA)	Info-Seite
Bayerische Staatsbibliothek	Info-Seite
Berliner Elektronenspeicherring-Ges. für Synchrotronstrahlung	Info-Seite
Bibliotheksservice-Zentrum Baden-Württemberg	Info-Seite
Brandenburgische Technische Universität Cottbus	Info-Seite
Bundesamt für Kartographie und Geodäsie	Info-Seite
Bundesanstalt für Geowissenschaften und Rohstoffe	Info-Seite
Bundesanstalt für Wasserbau	Info-Seite
Bundesinstitut für Risikobewertung	Info-Seite
Campus Berlin-Buch	Info-Seite
Charite Berlin	Info-Seite
DESY	Info-Seite
DFN-CERT Services GmbH	Info-Seite
DFN-Geschäftsstelle	Info-Seite
DFN-PKI Global Services CA	Info-Seite
DIFE	Info-Seite
Deutsche Forschungsgemeinschaft e.V.	Info-Seite
Deutsche Nationalbibliothek	Info-Seite
Deutsches Telekom AG Labor CA	Info-Seite
Deutscher Bundestag	Info-Seite
Deutscher Wetterdienst	Info-Seite
Deutsches Inst. für internationale pädagogische Forschung	Info-Seite
Deutsches Institut für Urbanistik	Info-Seite
Deutsches Institut für Wirtschaftsforschung e.V.	Info-Seite
Deutsches Klimarechenzentrum	Info-Seite
Deutsches Krebsforschungszentrum	Info-Seite

<http://www.pki.dfn.de>

# Regular Certificates

- Regular (non-grid) certificates are what most people need
- Validity of certificates
  - server certificates max. 5 years
  - user certificates max. 3 years
  - CA certificate max. 12 years
- Certificates are linked into standard web-browsers, i.e.
  - no „pop-up boxes“ from web servers
  - e-mail signatures can automatically be verified

- Status of integration of Telekom Root CA2, thus also of root of DFN-PKI Global
  - **Windows:** all desktop versions (2k, XP, Vista, 7)
  - **Apple:** since June 2008 (OS X, iPod, iPhone)
  - **Opera:** since 2008
  - **Mozilla:** since Firefox 3.0.12, TB 2.0.0.23
  - **Sun Java:** since V6u11 (11.08)
  - **Google Chrome:** yes, independent of OS
- All details about integration:
  - [www.pki.dfn.de/integration](http://www.pki.dfn.de/integration)

# Obtaining a regular certificate is easy

**DFN-Test-PKI**

DFN  
Deutsches  
Forschungsnetz

Zertifikate | CA-Zertifikate | Gespernte Zertifikate | Self-Service | Polides | Hilfe | Beenden

Nutzerzertifikat | Serverzertifikat | Zertifikat sperren | Zertifikat suchen

Willkommen zur DFN-PKI  
Schnittstelle für Nutzer und Administratoren - Zertifikate  
Hier können Sie Zertifikate beantragen, sperren lassen und nach Zertifikaten suchen.

- Bitte importieren Sie alle CA-Zertifikate in Ihren Browser über die Registerkarte "CA-Zertifikate".
- Bitte wählen Sie aus den Registerkarten eine Funktion aus.

Kontaktinformationen für Rückfragen finden Sie unter "Hilfe"

<http://www.pki.dfn.de/testpki-zugang>

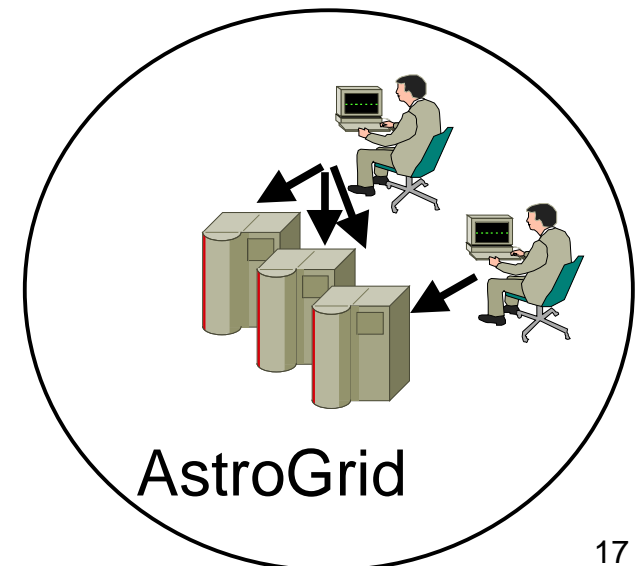
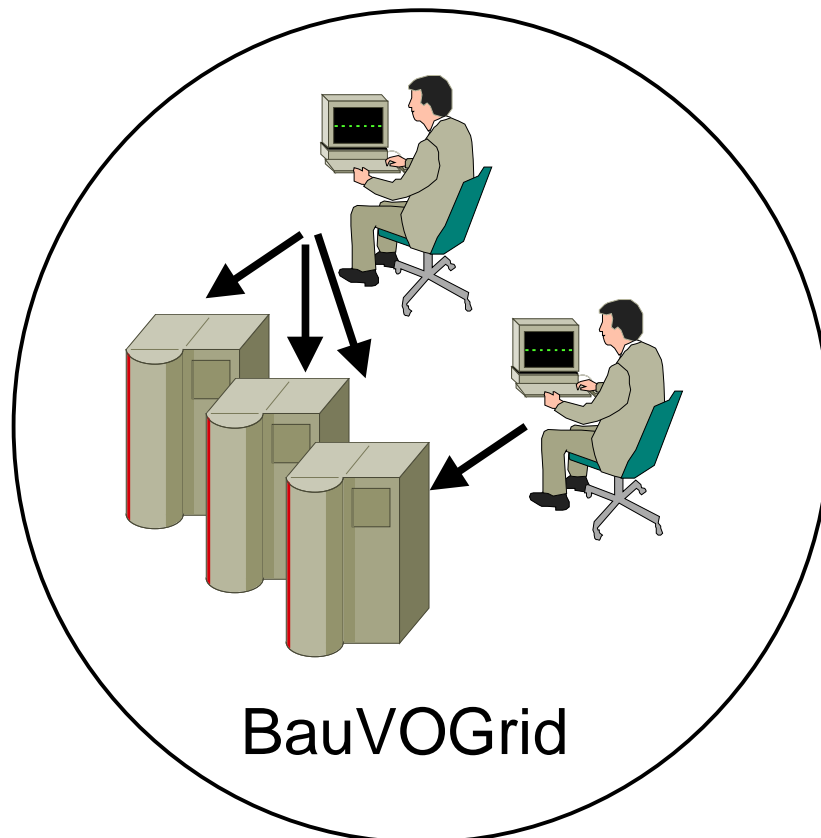
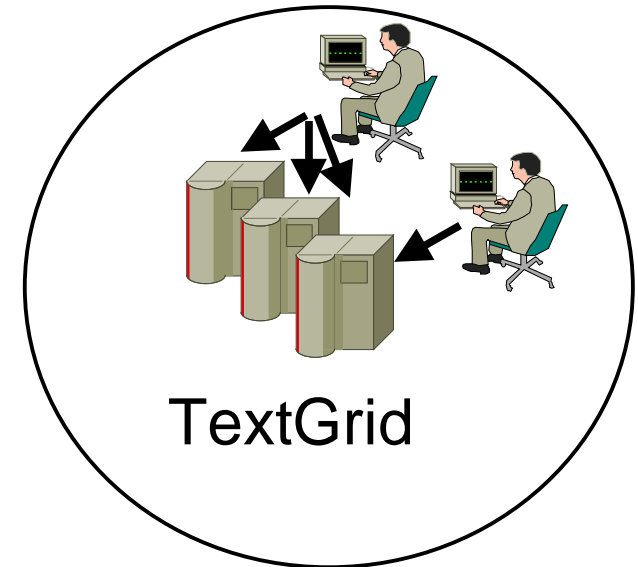
# Summary: Regular certificates

- More than 250 sites in Germany have a CA within DFN-PKI
- More than 80.000 valid certificates issued
- Regular certificates do the job and are what everyone needs
  - but there is one exception ...

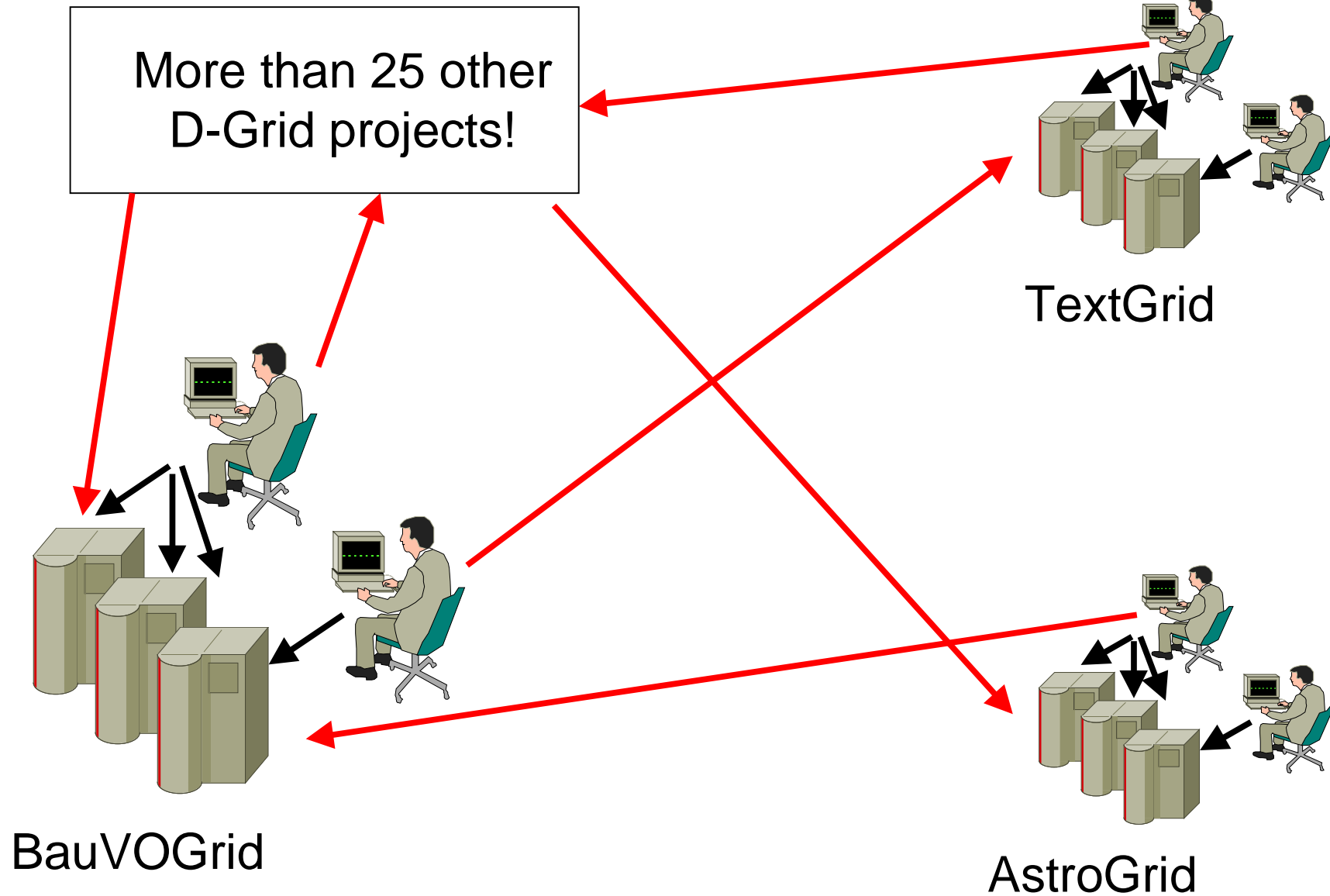
# Grid Certificates

# Accessing resources in D-Grid (1)

**Within a VO no (grid)  
certificates necessary**



# Accessing resources in D-Grid (2)



- To deal with certificates in grids a new body was set-up by grid / HEP people
- European Grid Policy Management Authority (EUGridPMA)
  - definition of policies and procedures for (world-wide) use of grid certificates
- International Grid Trust Federation IGTF
  - EUGridPMA
  - Asia Pacific PMA
  - The Americas PMA

# Grid certificates in Germany

- DFN Grid CA (DFN-Verein) and GridKA CA (FZ Karlsruhe) are both accredited to EUGridPMA

DFN Grid CA	GridKA CA
C= DE	C= DE
O= GridGermany	O= GermanGrid
OU= site name	OU= site name
[OU] = e.g. name of division	
CN= given name surname [hostname/service]	CN= given name surname [hostname/service]

# Obtaining a grid certificate

The screenshot shows a web interface for the DFN-Grid. At the top right is the DFN logo. Below it is a navigation menu with tabs: **Zertifikate**, CA-Zertifikat, Gesperrte Zertifikate, Policies, Hilfe, Beenden. Below the navigation menu are four buttons: Nutzerzertifikat, Serverzertifikat, Zertifikat sperren, and Zertifikat suchen. The main content area has a blue background and contains the following text:

**Willkommen zur DFN-PKI**  
**- Sicherheitsniveau Grid -**  
**Schnittstelle für Nutzer und Administratoren - Grid-Zertifikate**  
Hier können Sie Grid-Zertifikate beantragen, sperren lassen und nach Grid-Zertifikaten suchen.

- Bitte importieren Sie alle CA-Zertifikate in Ihren Browser über die Registerkarte "CA-Zertifikate".
- Bitte wählen Sie aus den Registerkarten eine Funktion aus.

Kontaktinformationen für Rückfragen finden Sie unter "Hilfe"

Impressum

- Why not just use regular certificates in grids?
  - technically no difference (both based on X.509)
- But grid certificates have to follow some „strange rules“, e.g.
  - basically just one CA per country
  - no sub-CAs thus no CA-hierarchies
  - very short validity of certificates (max. 13 months)
- „Strange rules“ for grid certificates force users to have more than just one certificate
  - hard to see a practical reason for this ...

- Issuing grid certificates in Germany works
- Number of issued certificates is much smaller than in the regular world
- Users complain
  - that they need different certificates
  - that they have to obtain a new grid certificate every 12 month
- The question remains whether current grid certificates are the perfect solution ...

- Documents about certificates in D-Grid
  - „Authentifizierung im D-Grid“ (12.2005)
    - Split between authentication and authorization
    - Registration authorities (RAs) per site, not for dynamic structures like projects or VOs
    - Non-academic partners can basically be served by every RA
  - „Verwendung von Zertifikaten im D-Grid“ (3.2008)
    - „New“ types of Grid certificates possible (SLCS, Robot-certificates for use in portals)
    - **All** D-Grid certificates require face-to-face identification of subscribers (= someone who wants a certificate)

# Short-lived Certificates

- Some grid users don't want to have a certificate at all
  - but: use of grid middleware is only possible with certificates
- Idea for new type of grid certificates was born
  - SLCS (Short Lived Credential Services)
  - idea: create short-lived certificate on-the-fly using standard user credentials (userid, password)
  - this should make everything much easier, but ...

- Security requirements for SLCS are as high as for grid certificates
  - e.g. face-to-face identification of subscribers
- This results in an even more complicated basic infrastructure
  - GridShib software
  - Shibboleth based authentication / authorization infrastructure (DFN-AAI)
  - identity management system in place, data must be updated regularly

# Live Demo: SLCS Certificate



The screenshot shows a web page for the DFN Short Lived Credential Service (SLCS) test. The page has a blue header with the DFN logo and navigation links: 'Zertifikate', 'CA-Zertifikate und Signing Policy Dateien', 'Hilfe', and 'Beenden'. The main content area is a light blue box with the following text:

Willkommen zum Test Short Lived Credential Service (SLCS) der DFN-PKI  
Hier können Sie Zertifikate des Test SLCS der DFN-PKI beantragen.

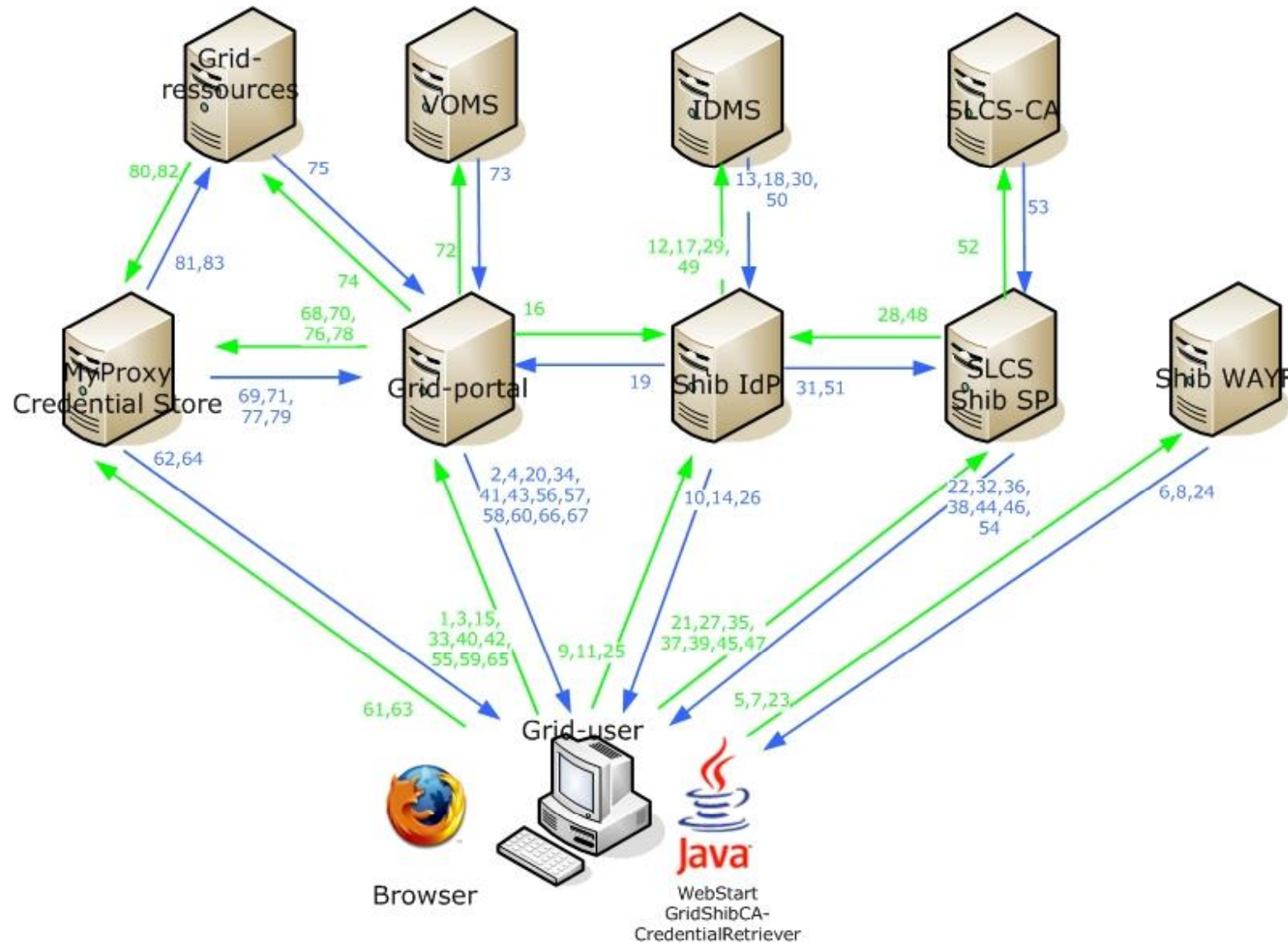
- Beantragen Sie hier Ihr Test SLC:

Kontaktinformationen für Rückfragen finden Sie unter "Hilfe"

Impressum

<https://test-slcs.pca.dfn.de/gridshib-ca/>

# SLCS architecture for portals



# Conclusions

- DFN offers different kinds of certificates
  - regular, grid, SLCS
  - share of regular certificates is around 98% (!)
- For the time being grid users need at least two certificates (no technical reasons)
  - with SLCS things get more complicated (e.g. IdM)
  - with SLCS and Portals even more
  - Goal: 1 certificate per user (1 ID card per person)
- More information
  - [www.pki.dfn.de](http://www.pki.dfn.de) / [pki@dfn.de](mailto:pki@dfn.de)