

Deutsches Forschungsnetz

„Starke“ Zertifikate mit wenig Aufwand

-

Welchen Nutzen bringt der neue
DFN Zertifizierungsdienst den Hochschulen?

10. Mai 2005

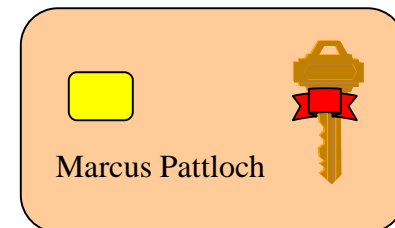
Marcus Pattloch (DFN-Verein)

Frage 1

**Was sind Zertifikate und was
nutzen sie mir?**

Was ist ein Zertifikat?

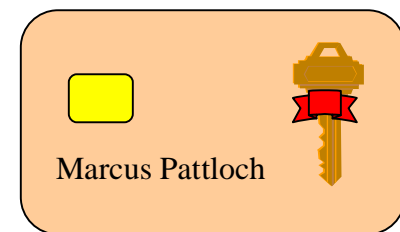
- Zertifikat = persönlicher Ausweis im Internet
- jeder, der ein Zertifikat besitzt, kann im Netz authentisch auftreten
- jeder, dem ich im Netz mein Zertifikat zeige, kann sicher sein, wer ich bin
- häufigste Form als „Chipkarte“
(aber: nicht jede Chipkarte enthält ein Zertifikat)



- Zertifikate ersetzen Passwörter
 - grundsätzlich EIN Zertifikat pro Person (jeder hat auch nur einen Ausweis)
 - Schluss mit vielen verschiedenen Passwörtern (die man sich doch nicht merken kann)
 - Sicherheit von Zertifikaten grundsätzlich deutlich höher als von Passwörtern
 - einfache Nutzung der Zertifikate möglich (weitgehend transparent)

- allgemeine Anwendungen, z.B.
 - Anmelden am Arbeitsplatzrechner
 - E-Mail Passwort
 - Zugriff auf Datenbanken
- Anwendungen in der Hochschulverwaltung
 - (dezentraler) Zugriff auf Haushaltsdaten
 - Austausch von Personaldaten
 - Zugriff auf Drittmitteldaten
 - Zugriff auf Prüfungsnoten (QIS-Module)

- Die Selbstbedienungsfunktion für Studierende unterstützt u.a. folgende Funktionen
 - Anmeldung zu Prüfungen
 - Rücktritt von Prüfungen
 - Kontoauszug (Ansehen und Drucken)
 - Notenübersichten
 - Passwortänderung
 - Bescheinigungen in PDF
 - Digitale Signatur von Bescheinigungen
- Wie weist sich der Studierende online aus?

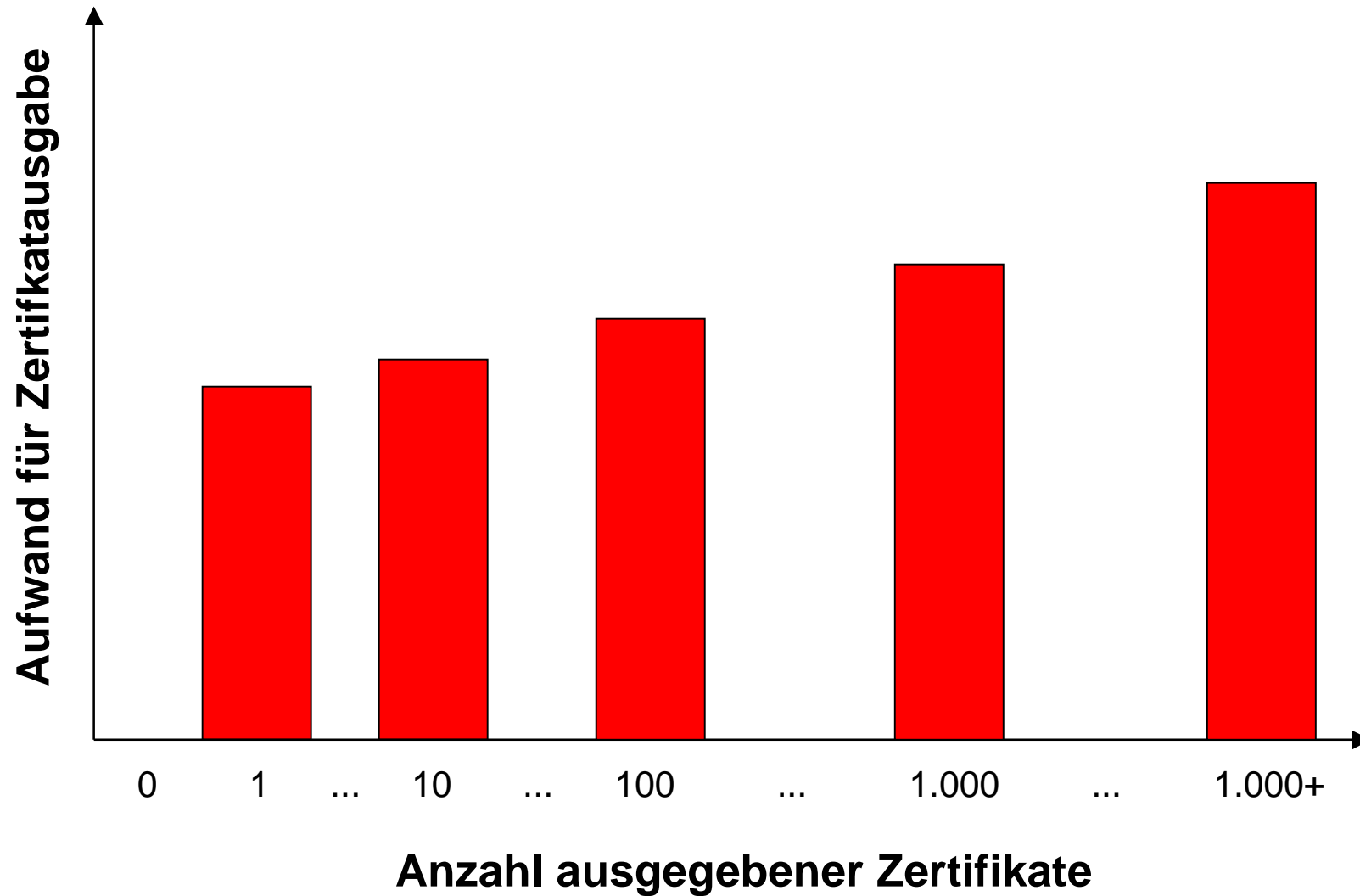


Frage 2

Was „kosten“ Zertifikate?
(oder: braucht jeder eine eigene Bundesdruckerei?)

- viele Einrichtungen benötigen Zertifikate
- ein Zertifizierungsdienst wird aufgesetzt, aber es stellt sich heraus
 - der Aufwand für den Betrieb einer eigenen Zertifizierungsstelle ist sehr hoch
 - insbesondere die Einstiegshürde ist sehr hoch
- der Zertifizierungsdienst „kommt nicht zum Fliegen“

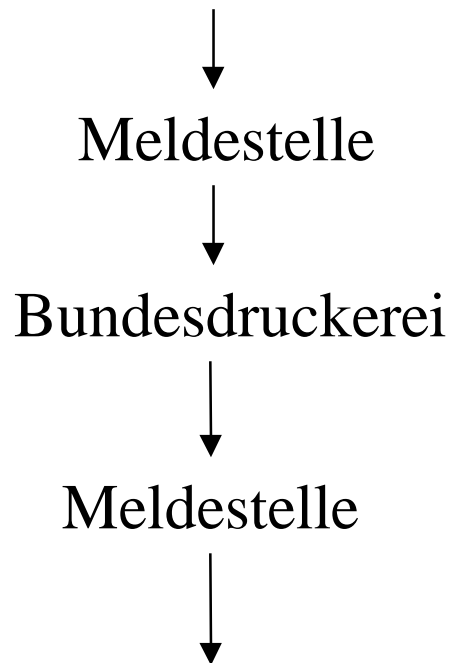
„üblicher“ Aufwand



Wie bekomme ich einen Ausweis?

Personalausweis

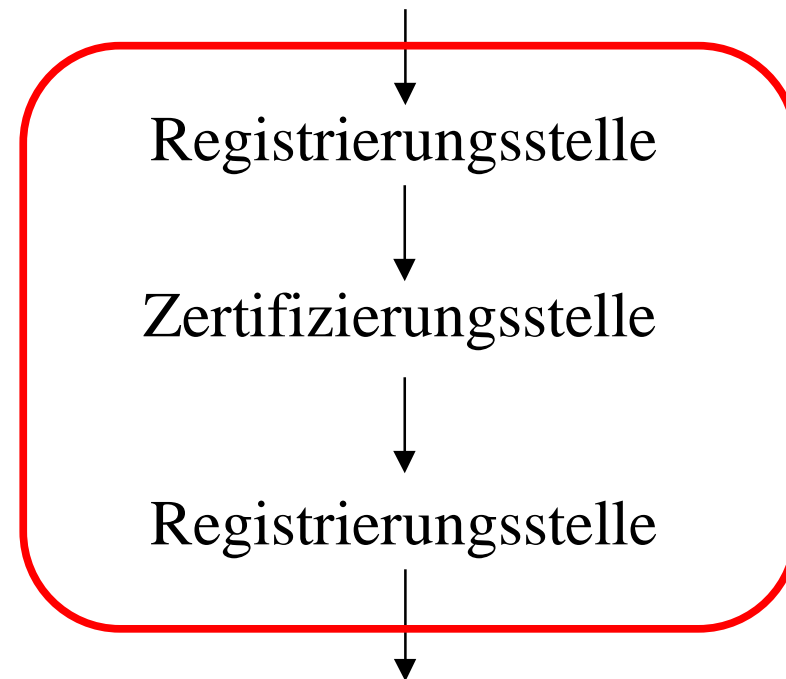
Ich benötige einen Ausweis



Ich habe einen Ausweis

Digitaler Ausweis

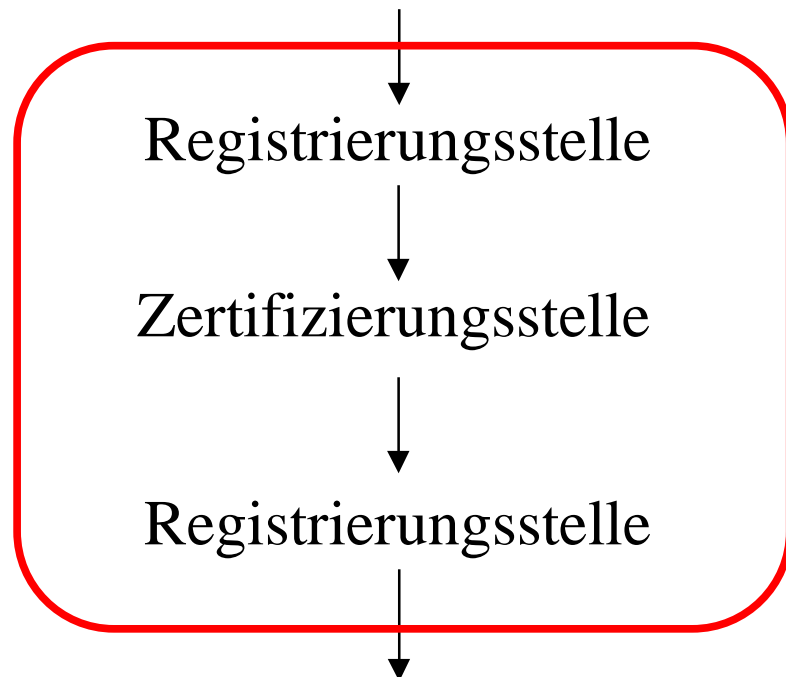
Ich benötige ein Zertifikat



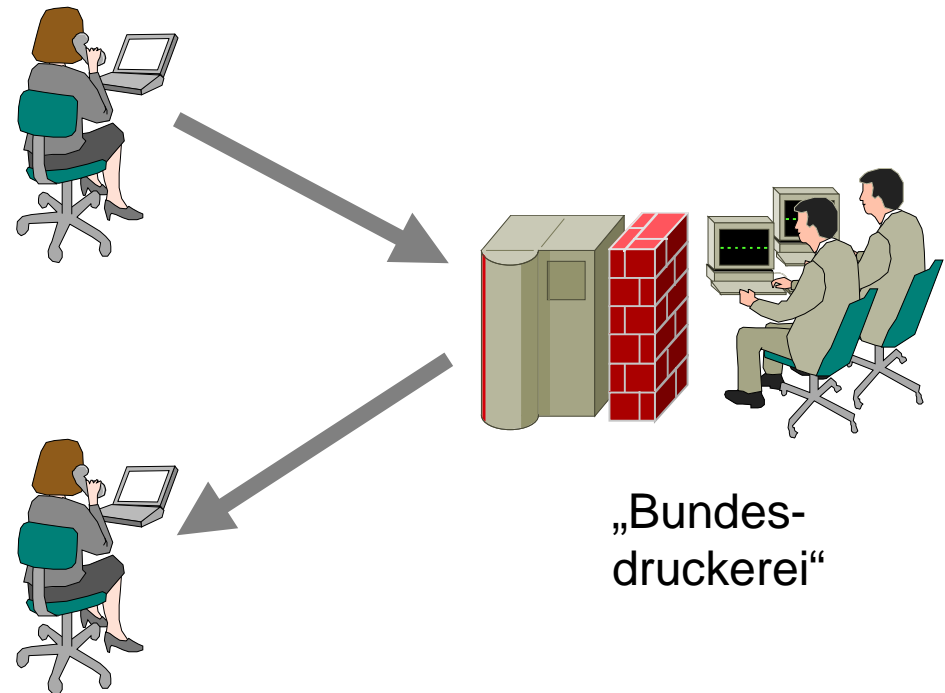
Ich habe ein Zertifikat

Digitaler Ausweis

Ich benötige ein Zertifikat



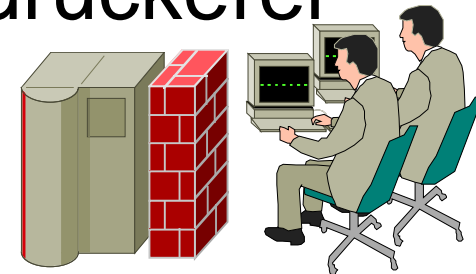
Ich habe ein Zertifikat



- Erfassen und Identifizieren der Benutzer
 - Prüfung Ausweisdokument
 - z.B. bei der Immatrikulation
- Weiterleitung der Zertifikatsanfragen an die Zertifizierungsstelle
- Funktion entspricht der „Meldestelle“
- Wahrnehmung durch „clevere Sekretärin“



- Erstellung der Zertifikate
 - sicherheitskritischer Vorgang in einem gesicherten Raum auf einem gesicherten Rechner
- Kommunikation mit Registrierungsstelle
 - Annahme der Zertifizierungsanträge
 - Rückgabe der erzeugten Zertifikate
- Funktion entspricht der „Bundesdruckerei“

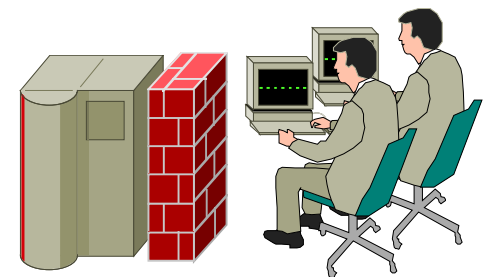


- Wahrnehmung durch technische Experten

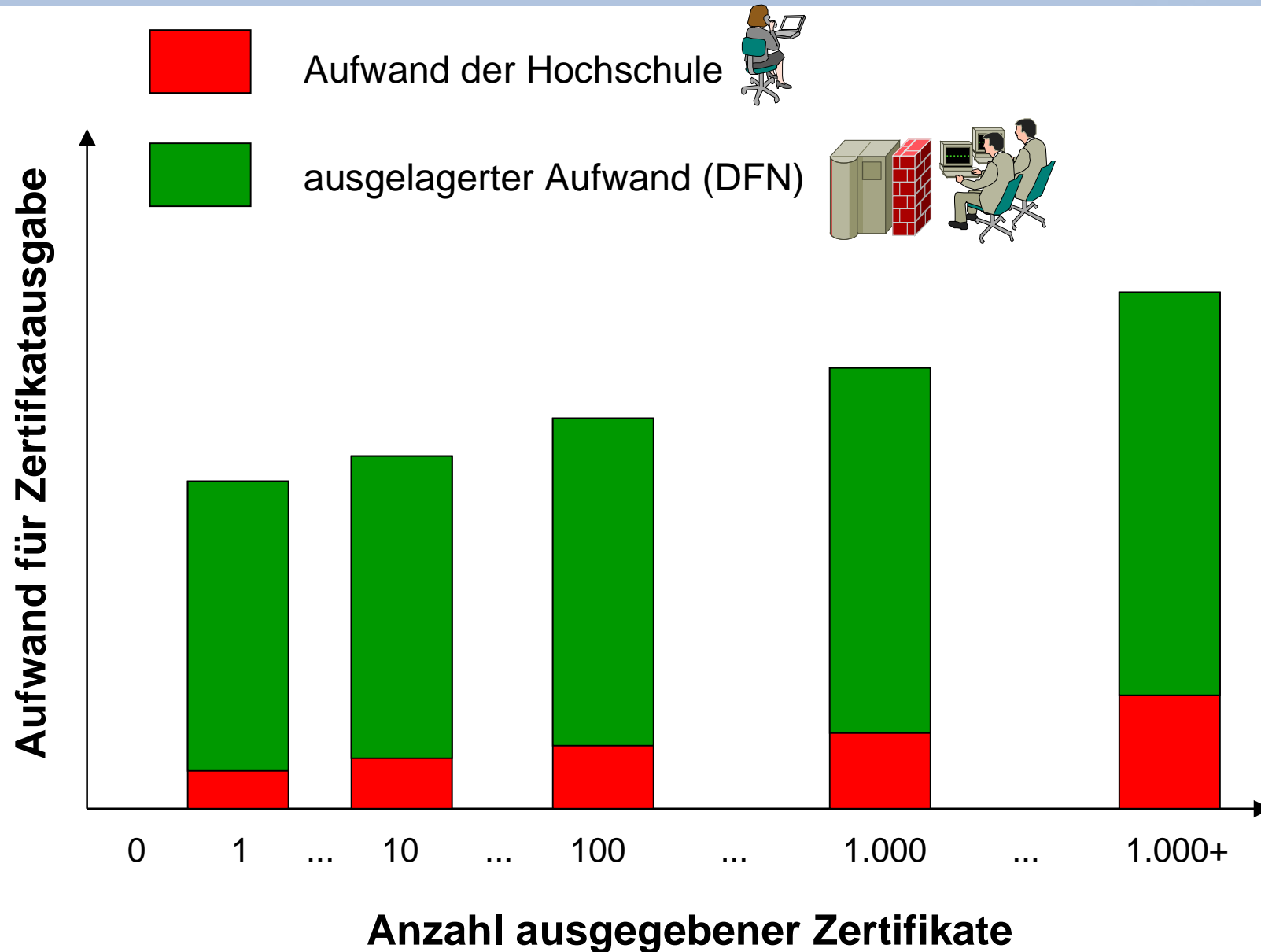
- Registrierungsstelle
 - vergleichbar der Meldestelle
 - administrative Arbeiten
 - verbleibt in der Hochschule



-
- Zertifizierungsstelle
 - vergleichbar der Bundesdruckerei
 - technisch aufwändige Arbeiten
 - kann an DFN ausgelagert werden



Aufwand mit Auslagerung



Frage 3

Wie „sicher“ sind Zertifikate?

- Wie gut (sicher) sind Passwörter?
 - im Prinzip gut, aber ...
 - zu komplex: Zettel unter der Schreibtischunterlage
 - zu einfach: leicht von einem Angreifer zu erraten
 - hängt ab von konkreter Umsetzung
- Wie gut (sicher) sind Zertifikate?
 - im Prinzip gut, aber ...
 - die Anforderungen sind hoch
- DFN Zertifizierungsdienst in allen wesentlichen Punkten auf hohem Niveau

- Anforderungen an einen Zertifizierungsdienst
 - ü rechtliche Regelungen, Datenschutz et al.
 - ü Anwendungsbereich DFN-weit / (inter)national
 - ü hohes Vertrauen in sichere Identifikation und korrekte Zertifikatausstellung
 - ü sehr gut geschultes Personal
 - ü Nachhaltigkeit („Schwarze Listen“ et al.)
 - ü Skalierbarkeit beim Aufbau / Ausbau
(wirtschaftlich für ein Zertifikat und für Übergang zu hunderten / tausenden Zertifikaten)

- ein Zertifikat (= Ausweisdokument) darf nie an eine falsche Person ausgegeben werden
- Sicherheitsniveau des Zertifizierungsdienstes wird definiert durch div. Parameter, z.B.
 - Form der Identitätsprüfung
 - Qualifikation des Personals
 - rechtliche Rahmenbedingungen
- ü Jede Einrichtung muss das für sie erforderliche Sicherheitsniveau selber bestimmen

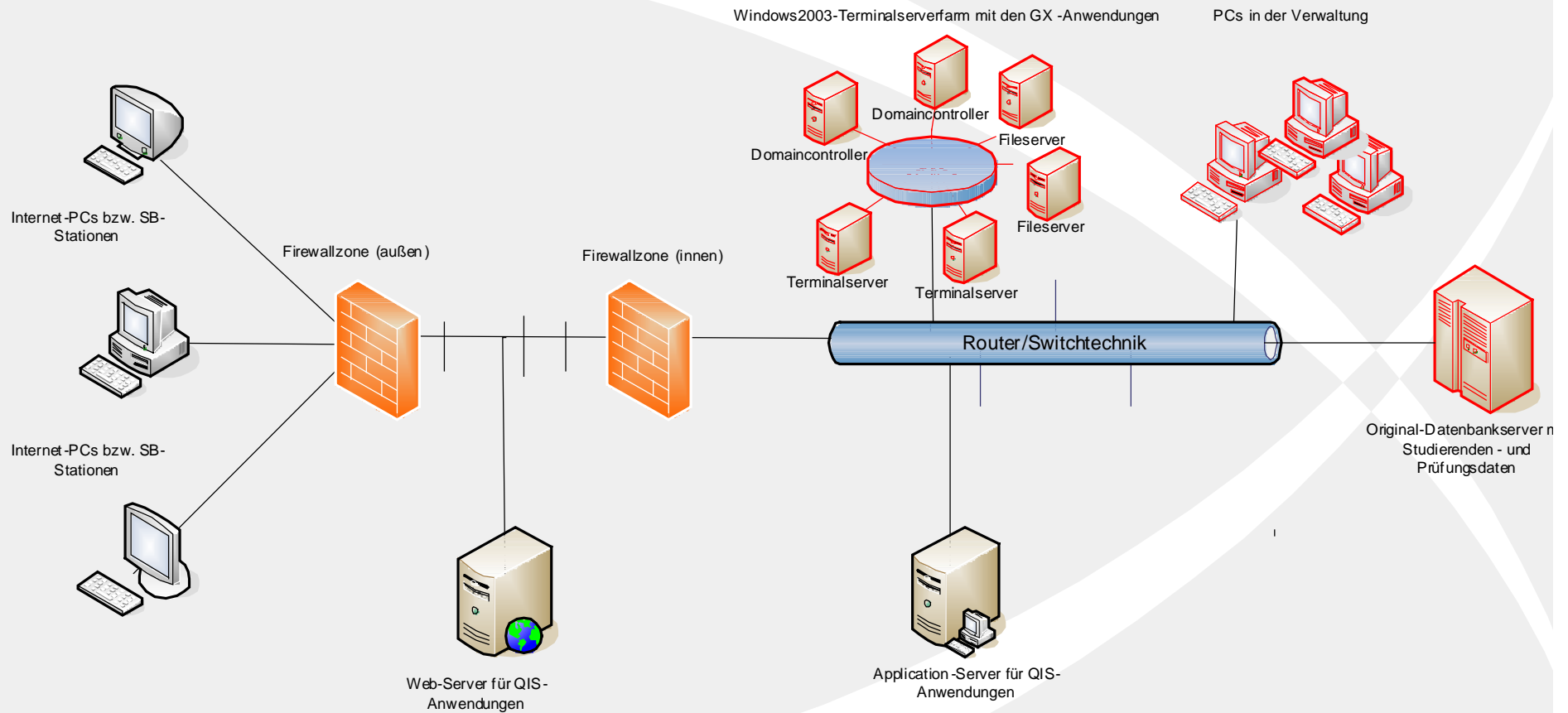
Frage 4

**Zertifikate -
funktioniert das wirklich?**

Beispiel: HU Berlin

HISQIS-Prinzipskizze

Dienstag, 26. April 2005



- Seit Januar 2005
- Teilnehmer u.a.
 - Univ. Hannover, GWDG Göttingen (MPG), LRZ
- Status
 - Umsetzung läuft erfolgreich
 - Abstimmung mit Anforderungen der Anwender
 - Pilotphase endet 31.12.2005
 - jetzt: offen für weitere Teilnehmer

ü Regelbetrieb beginnt am 1.1.2006 (Start X-WiN)

Zusammenfassung

(und Empfehlung)

- In Zusammenarbeit mit Anwendern wurde der DFN Zertifizierungsdienst neu gestaltet
 - hohe Qualität & wirtschaftlich attraktiv
 - Vorteile für Anwender, die bereits etwas haben
 - Möglichkeit zum Einstieg für „kleine“ Anwender
 - Kontakt: **sicherheit@dfn.de**
- ü Wenn Ihre Hochschule einen Zertifizierungsdienst hat oder neu aufbauen will, prüfen Sie die Vorteile des neuen DFN Zertifizierungsdienstes