

Sichere Self-Service-Funktionen mit HISQIS

Dr. Martin Klingspohn, klingspohn@his.de

Gliederung

- Vorbemerkungen
 - Architektur (Internetszenario)
 - Datenkonsistenz
 - Datensicherheit
 - Datenschutz
 - Einzelne Maßnahmen
- } Datenintegrität

Qualitätssteigerung
der Hochschulverwaltung im
Internet durch
Selbstbedienungsfunktionen

Grundidee

Ausgewählte Funktionen
der HIS-Verwaltungssysteme
werden für **berechtigte Dritte** in
vereinfachter bzw.
eingeschränkter Form
angeboten.

Zielgruppen

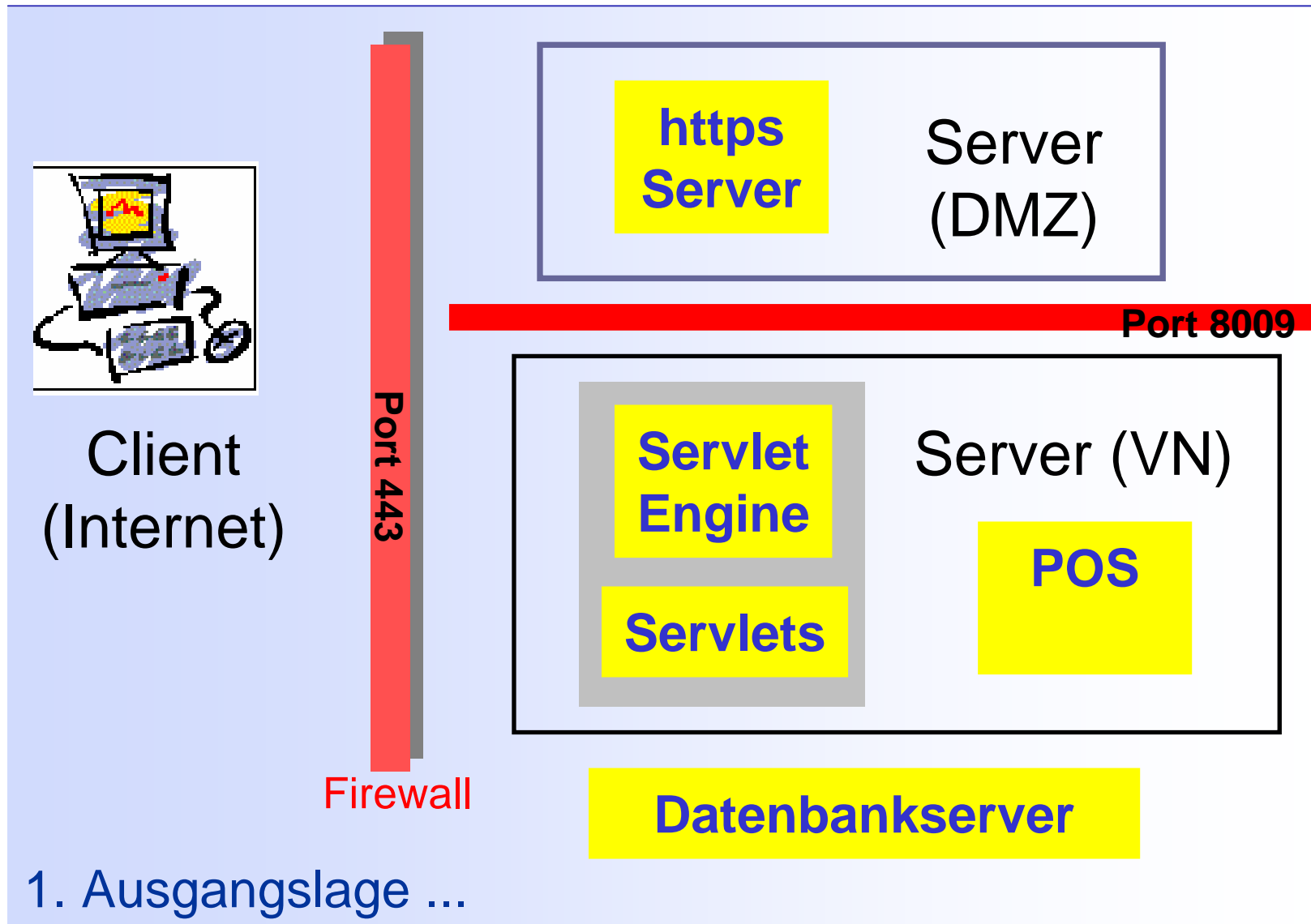
- Studierende
 - Prüfungsanmeldung
- Prüfer/in
 - Leistungsverbuchung
- Studiendekan/in
 - Studienberatung
- Mitarbeiter/in

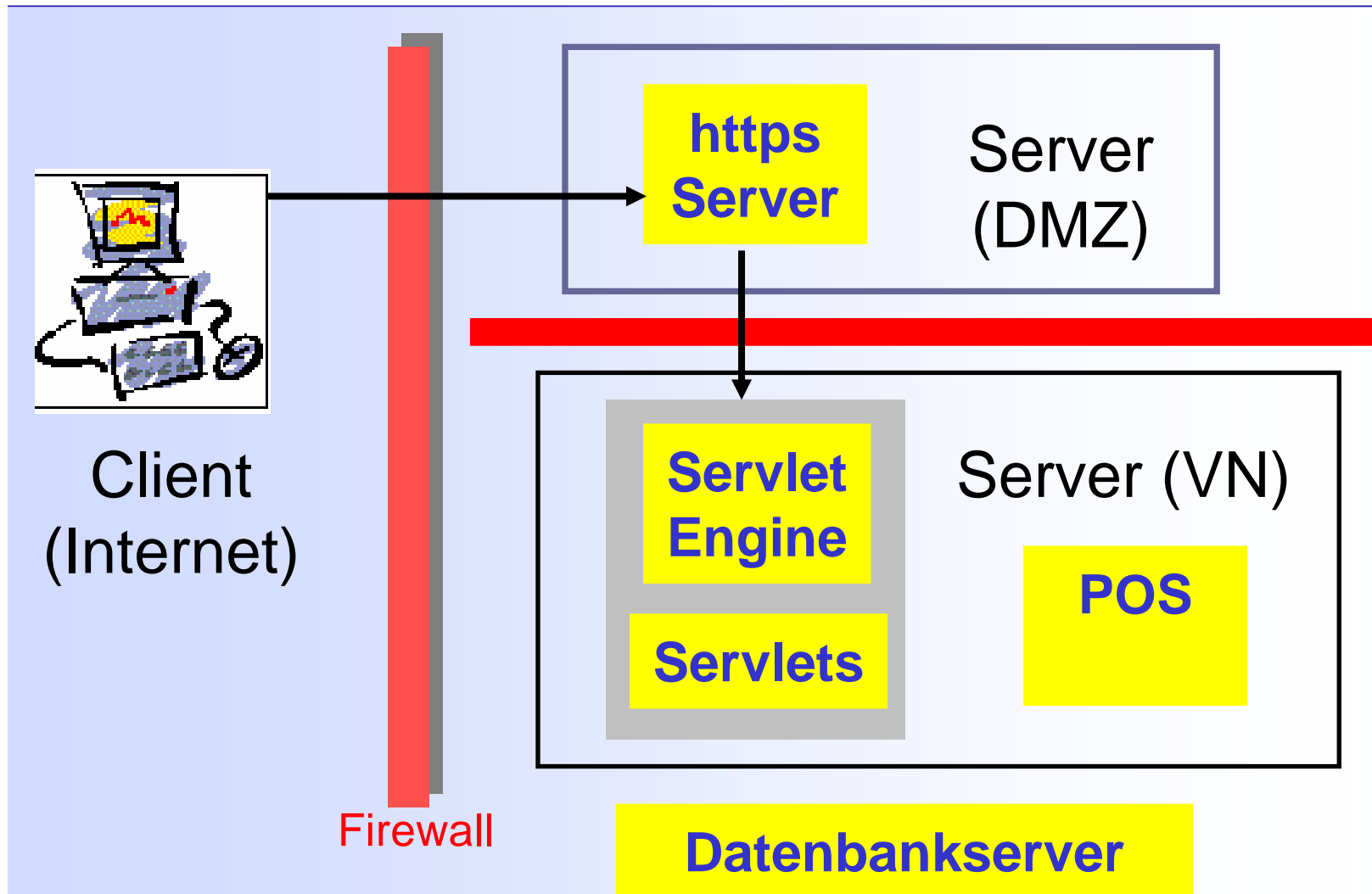
Evaluation des QIS Modul POS durch die ZENDAS

(01.10.2003-31.07.2004)

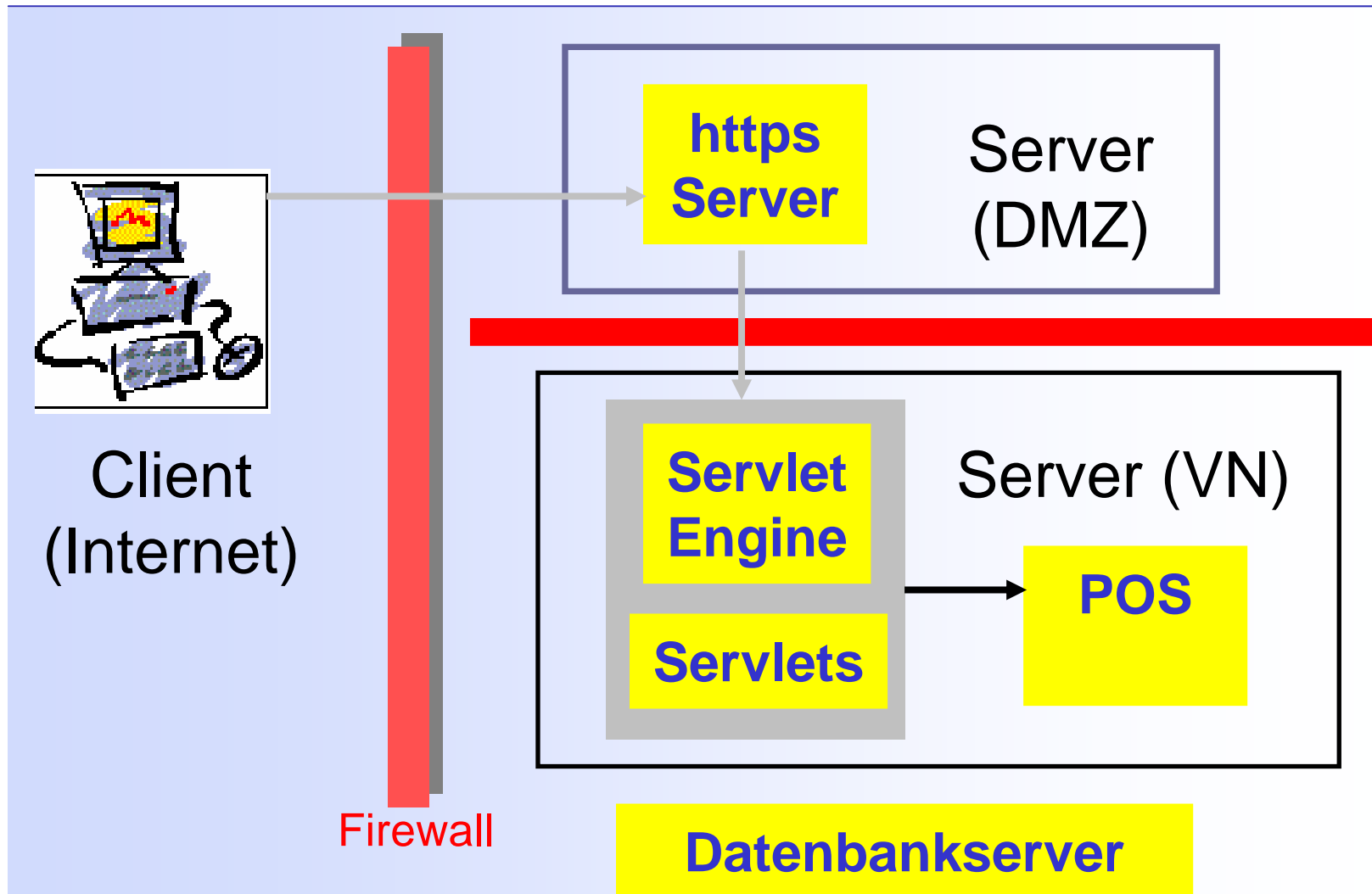
- Applikation QISPOS
- Härtung der Serverarchitektur

- Vorbemerkungen
- **Architektur (Internetszenario)**
- Datenkonsistenz
- Datensicherheit
- Datenschutz
- Einzelne Maßnahmen

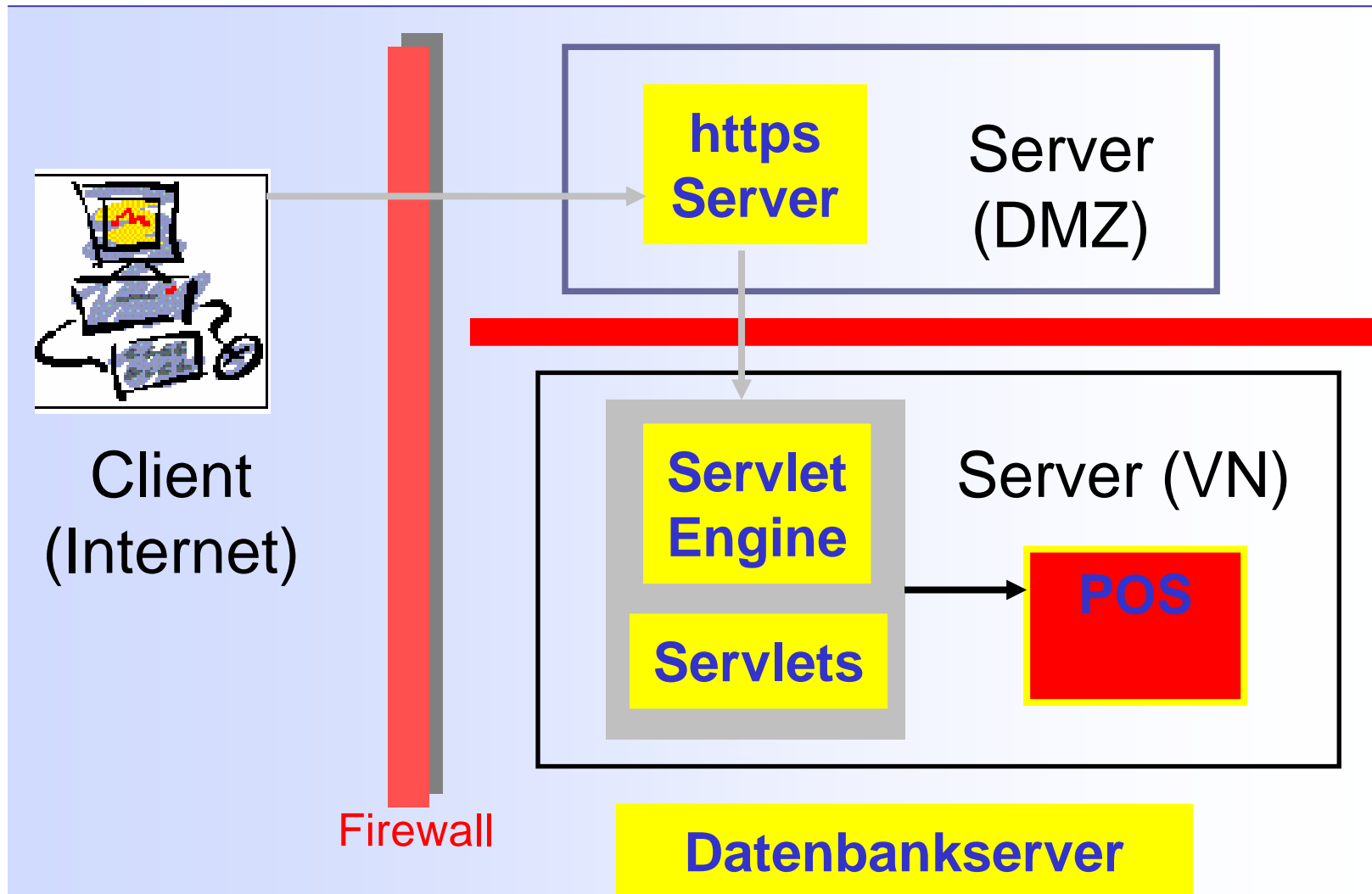




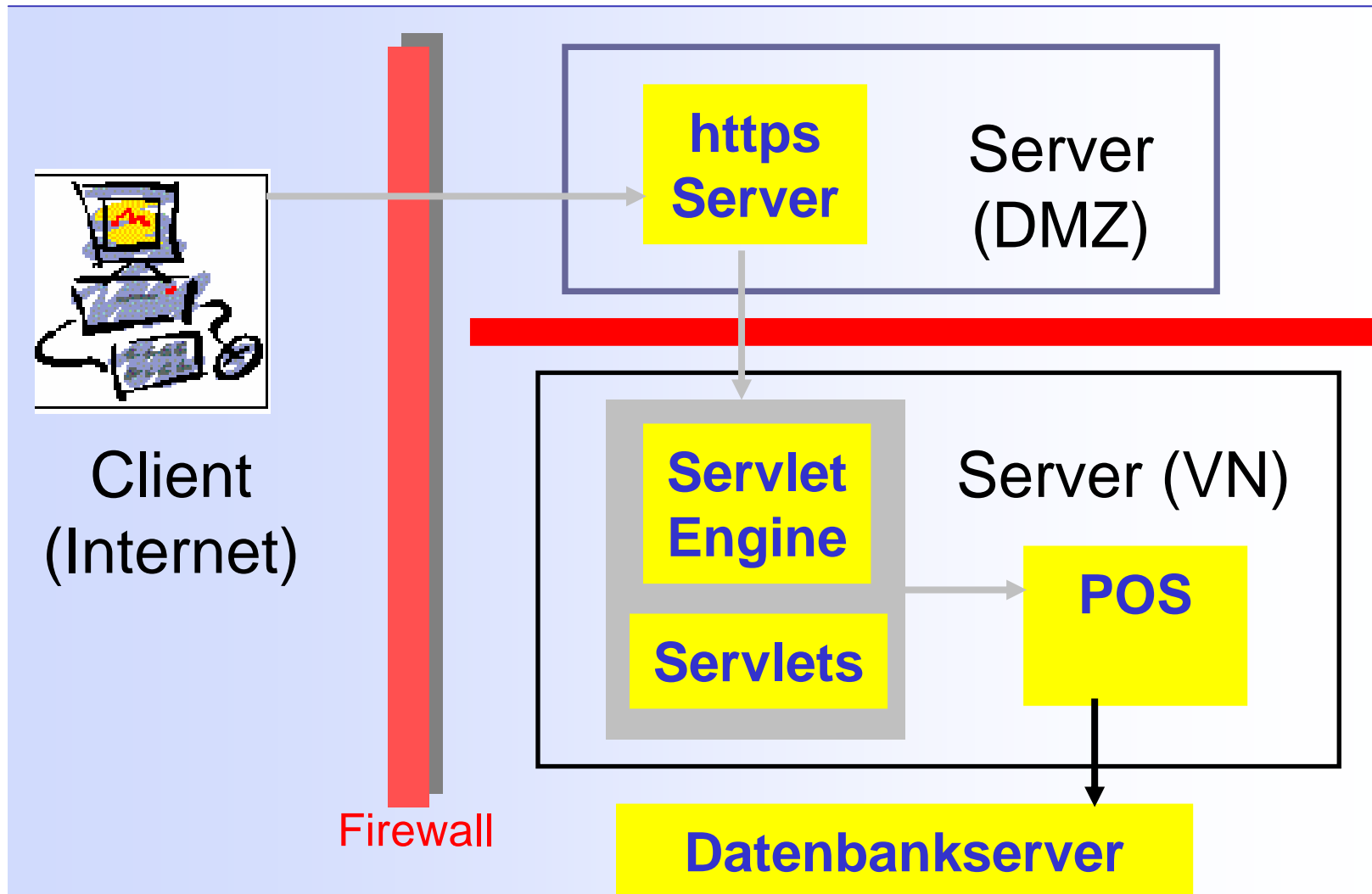
2. Client sendet Anfrage ...



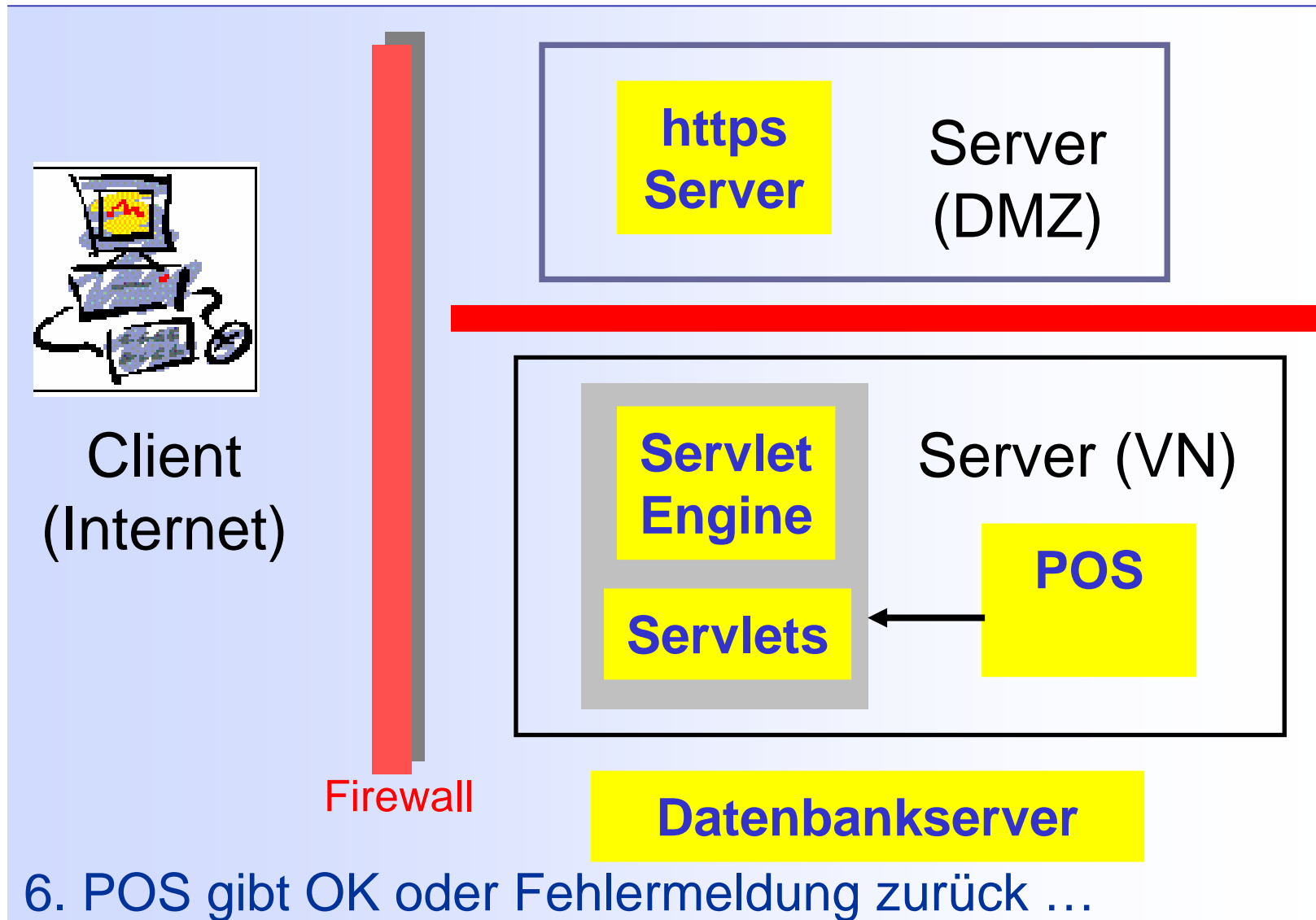
3. Servlet erstellt Anfrage für POS ...



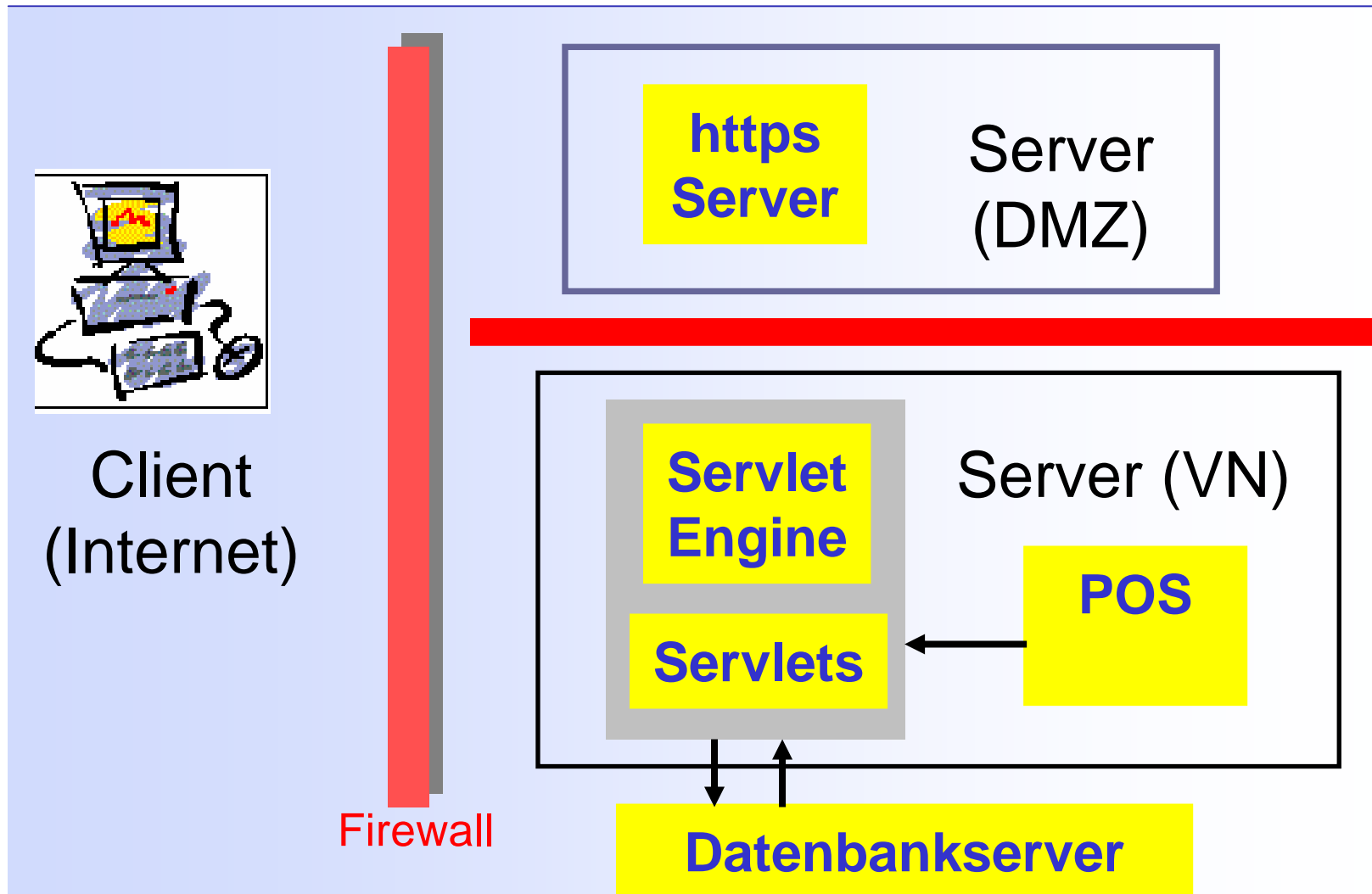
4. POS: Voraussetzungsprüfung, Generierung, ...



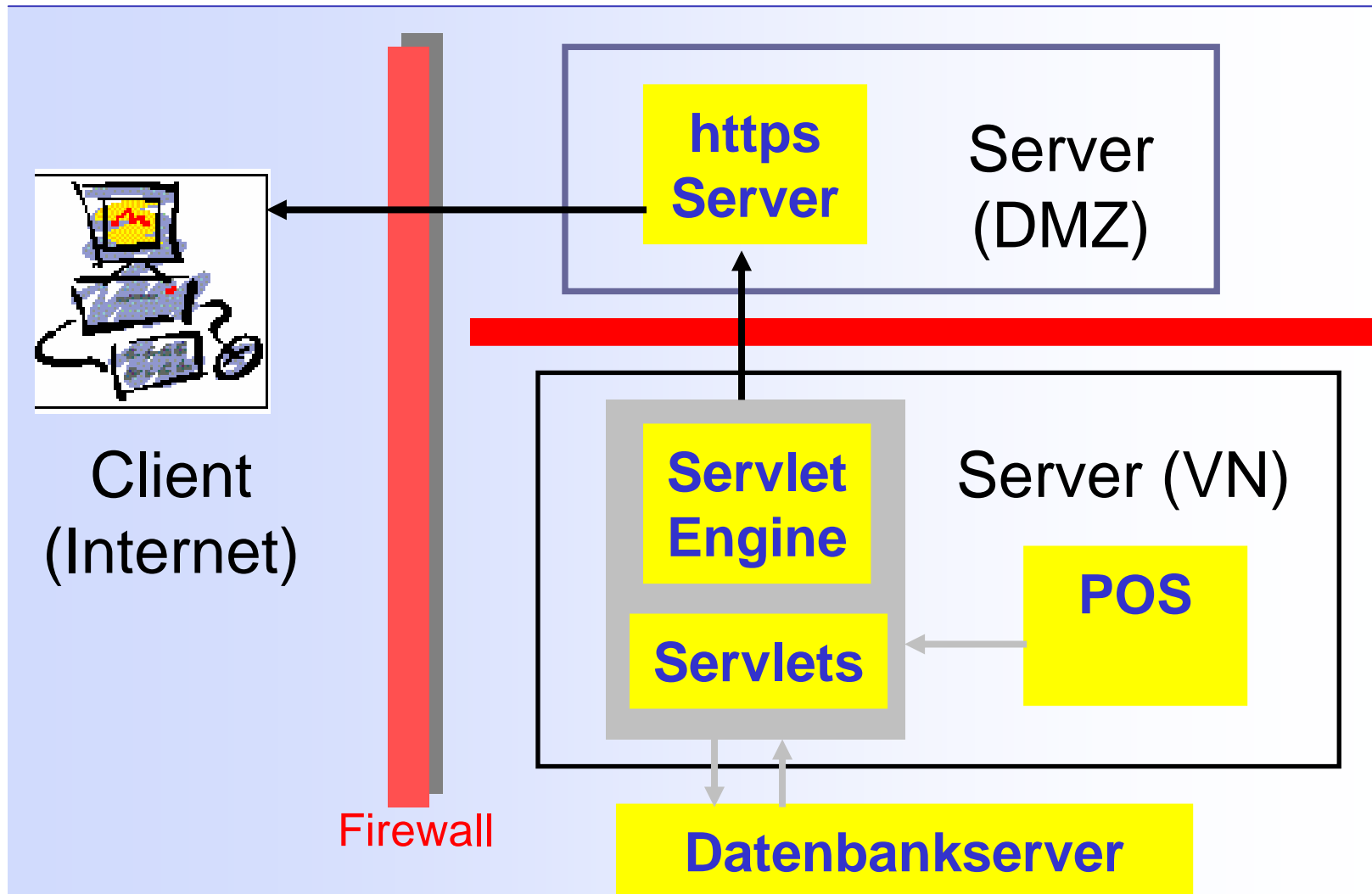
5. POS führt insert, update auf die Datenbank durch ...



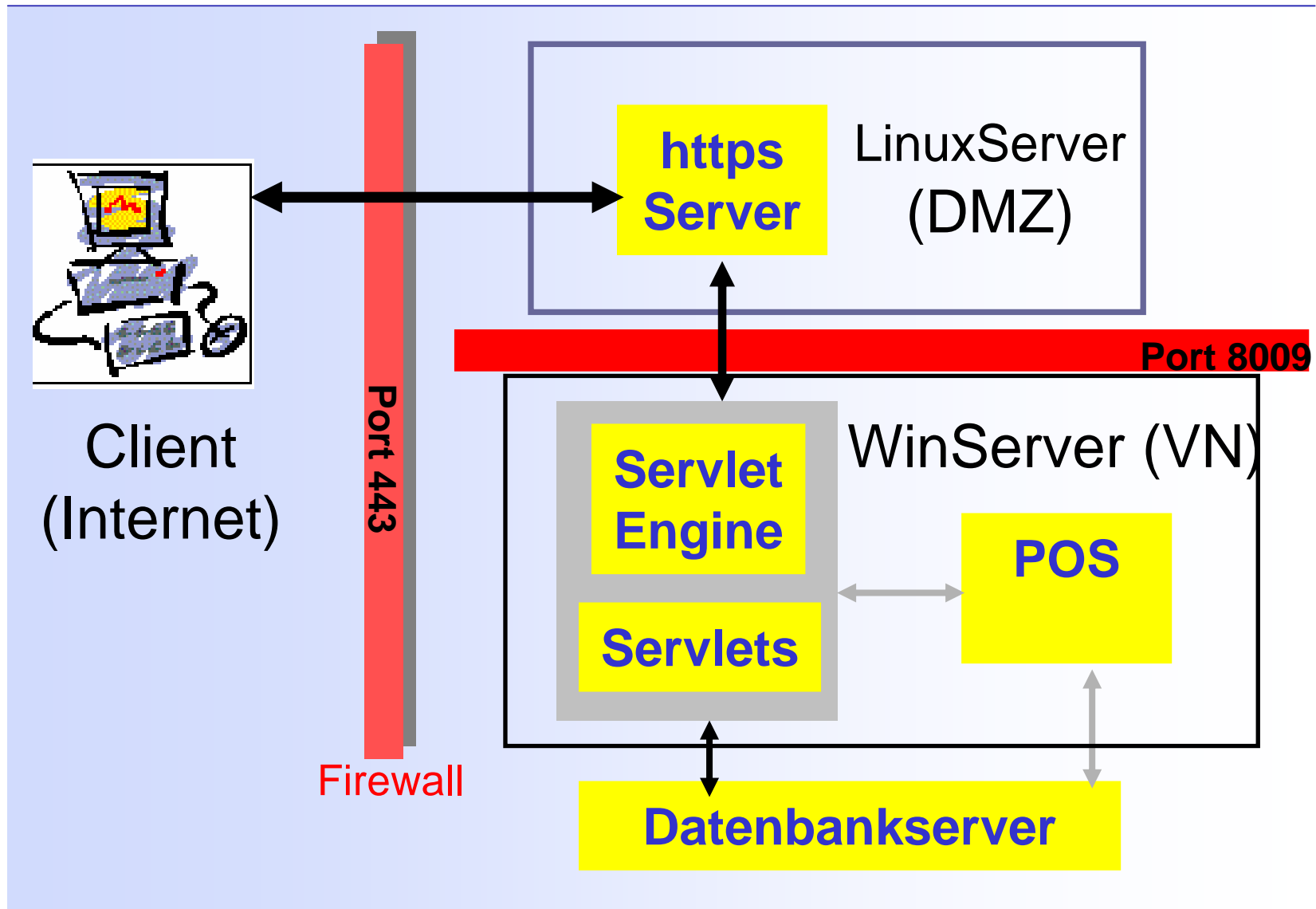
6. POS gibt OK oder Fehlermeldung zurück ...



7. Servlet selektiert neue Leistungsdaten ...



8. Ergebnis wird dem Client übermittelt ...



- Vorbemerkungen
- Architektur (Internetszenario)
- **Datenkonsistenz**
- Datensicherheit
- Datenschutz
- Einzelne Maßnahmen

Datenkonsistenz

Erhalt der Widerspruchsfreiheit der Daten.

Die Plausibilisierung der Daten wird über das jeweilige operative System (POS-GX) durchgeführt.

- Vorbemerkungen
- Architektur (Internetszenario)
- Datenkonsistenz
- **Datensicherheit**
- Datenschutz
- Einzelne Maßnahmen

Authentifizierung sorgt dafür, dass die **Identität** des Benutzers **verifiziert** wird.

Verfahren im Internet

- Dauer-Passworte (Verschlüsselt in sospos , radius, ldaps)
- SSL-Zertifikate
(Transaktionen können mit TAN geschützt werden)

SB-Stationen

- „Unpersönliche“ Chipkarten (Seriennummer)
- Personalisierte Chipkarten ...

Probleme

- Übertragungswege unverschlüsselt
- Kritische Applikation
- Passwort ist unverschlüsselt in der Datenbank oder Verzeichnisdienst gespeichert

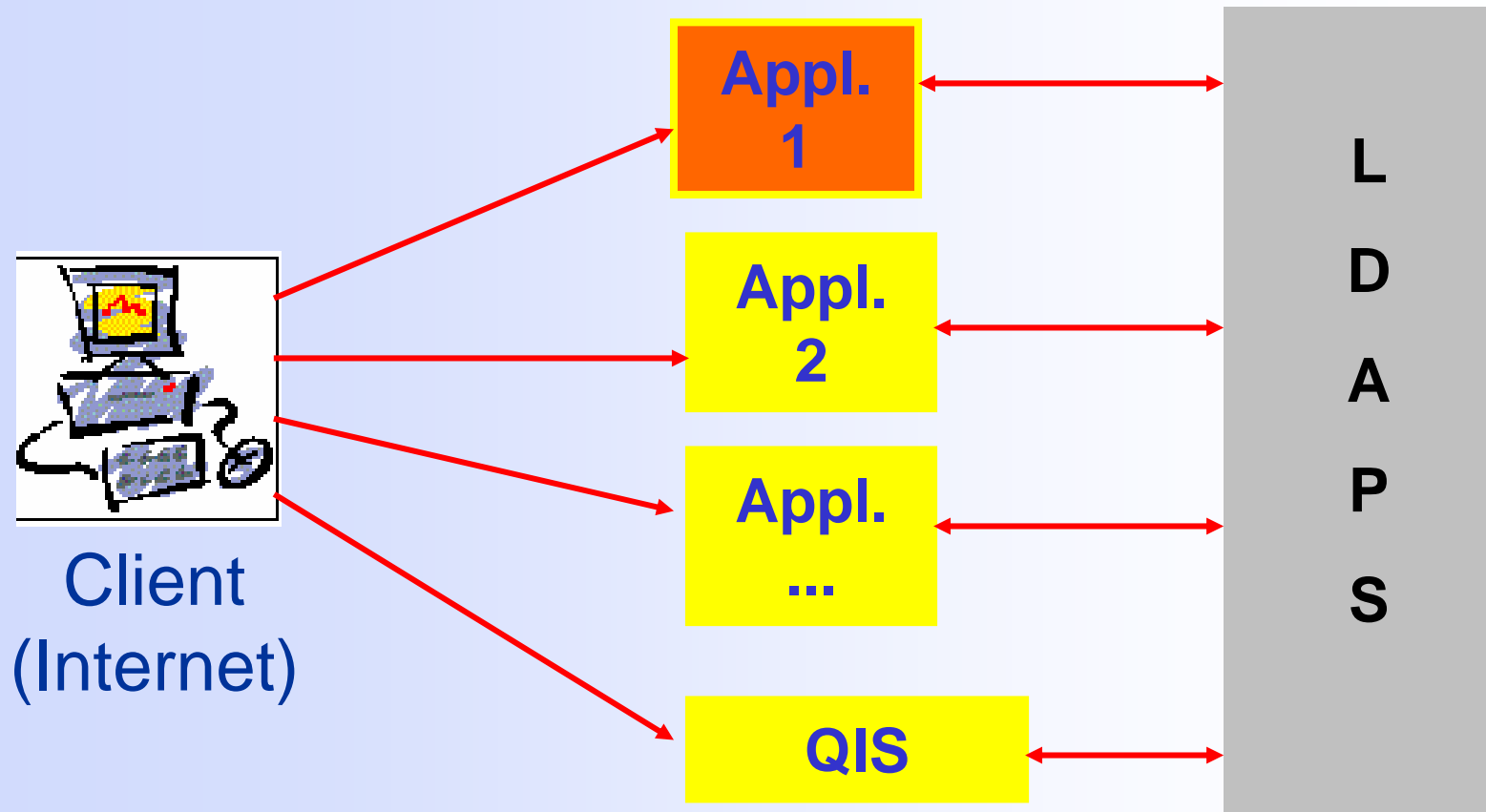
Vorteile Loginverwaltung im Verzeichnisdienst der HS:

- Verringerung des Verwaltungsaufwands
- Logindaten gelten für viele Anwendungen der Hochschule

Warnung:

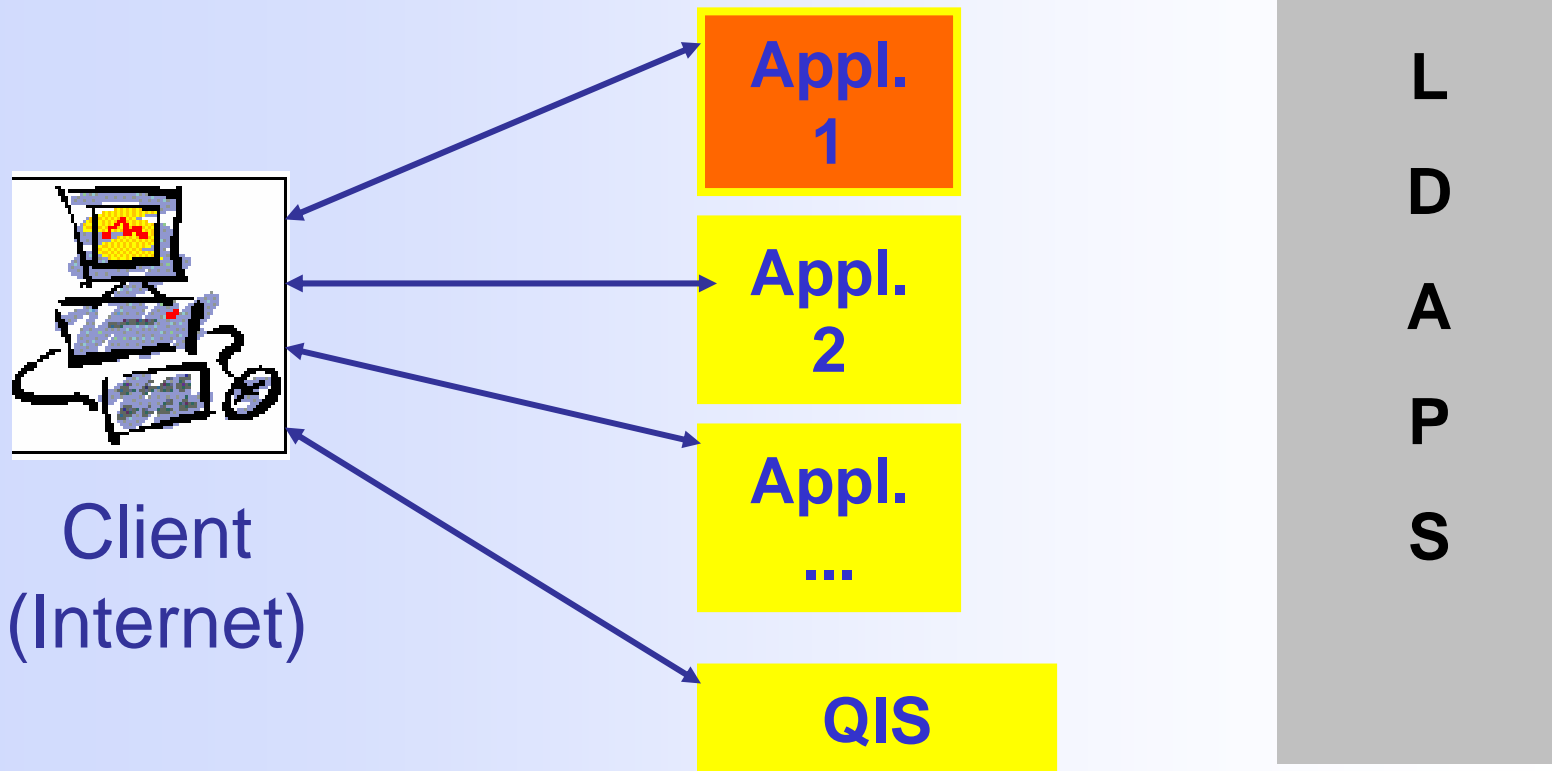
**Ein Login und ein Passwort für
viele Anwendungen ist noch
kein „Single Sign On“!
(Maximal ein „Shared Password“)**

Shared Password



Authentifizierung über die Applikation gegen LDAPS

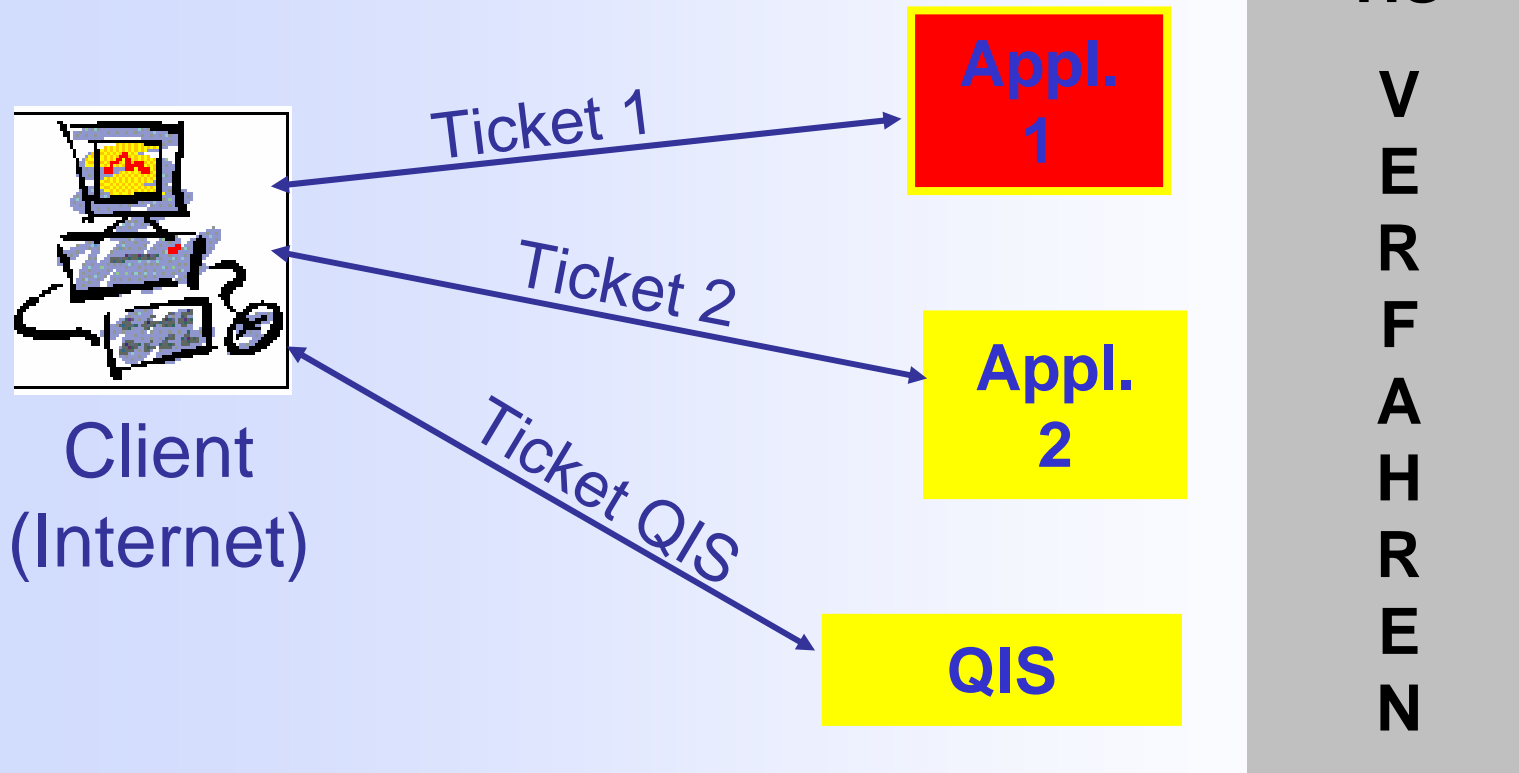
Shared Password



Single Sign On



Single Sign On



Nachteile Loginverwaltung im Verzeichnisdienst der HS:

- „Shared Password“
 - bei unsicheren Anwendungen
- Authentifizierung nur über „Wissen“
- „Authentifizierungs-Plugin“
muss speziell für jede Hochschule
angepasst werden (Single Sign On)

- Vorbemerkungen
- Architektur (Internetszenario)
- Datenkonsistenz
- Datensicherheit
- **Datenschutz**
- Einzelne Maßnahmen

Datenschutz bezieht sich auf die
rechtliche Seite des unbefugten
Zugriffs und der unbefugten
Weitergabe **personenbezogener**
Daten.

Personenbezogene Daten müssen
verschlüsselt übertragen werden!

Wie?

- Secure socket layer (SSL)
- Ipsec (PORT 8009,1526,5432)

Aufbau eines Servers siehe Installationsanleitung!

Sicherheit beim Client

- Die Darstellung im Browser ist in reinem HTML realisiert, es werden keine **aktiven Inhalte wie JAVA, JAVA-Script oder ActiveX** verwendet.
- Ein sicherheitsbewusster Internet-Nutzer kann solche **aktiven Inhalte** für seinen Browser **deaktivieren**, ohne dass dies Einfluss auf die Funktionalität von QIS hat.
- Nutzer darauf hinweisen, dass sie für die Sicherheit ihres Rechners verantwortlich sind. **Hilfestellungen geben!**

- Vorbemerkungen
- Architektur (Internetszenario)
- Datenkonsistenz
- Datensicherheit
- Datenschutz
- **Einzelne Maßnahmen**

Es sollte für jede Rolle ein spezieller Datenbanknutzer angelegt werden.

Beispiel:

- QIS-Bearbeiter (POS)
- Student
- Prüfer
- Fachbereich

Prozeduren der HIS beschränken die Rechte auf der LSF- bzw. SOSPOS-Datenbank.

Achtung: An Datenbanknutzer Public denken!

Vielen Dank
für Ihre Aufmerksamkeit!