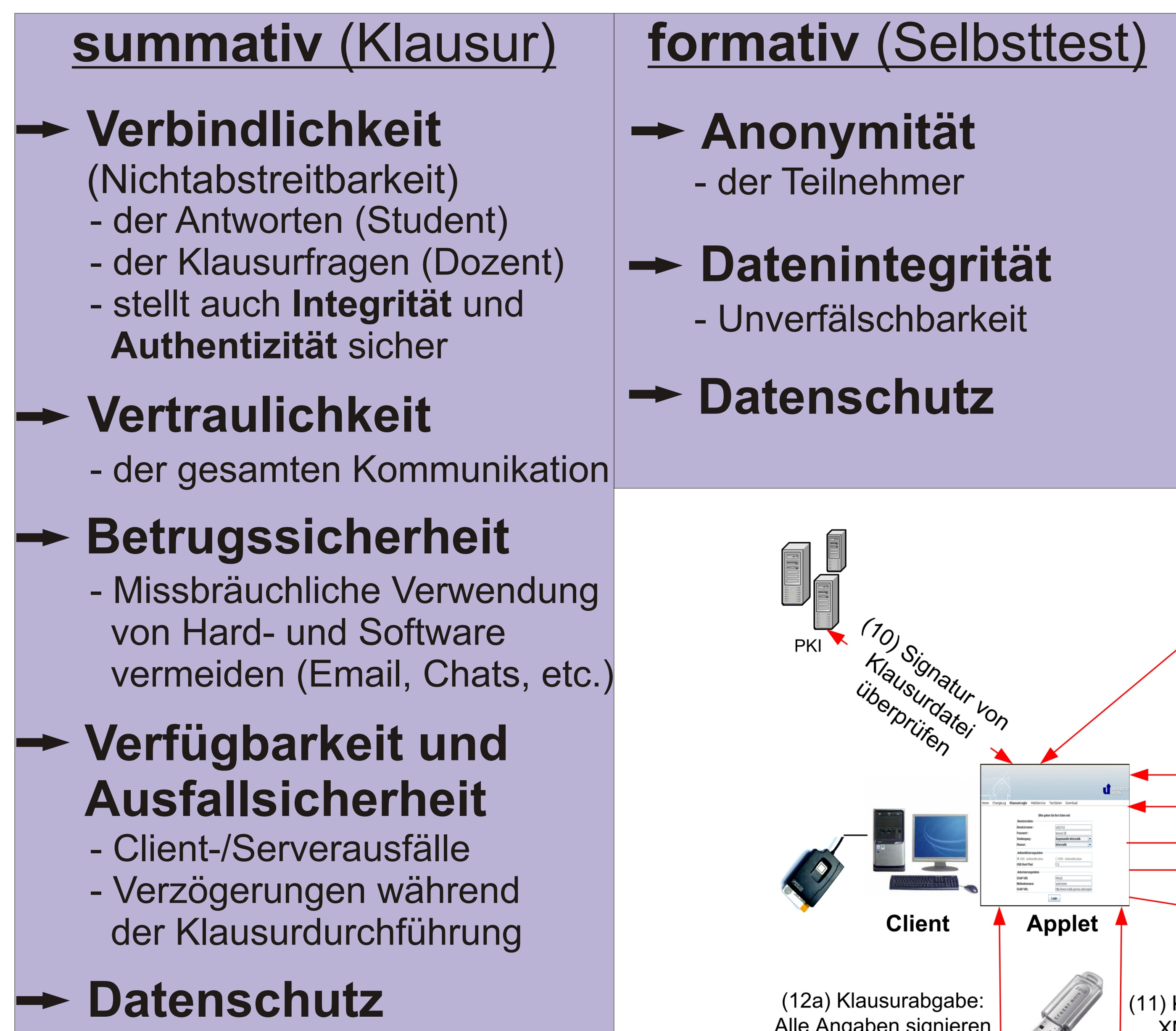


## Ein prozessorientiertes und dienstbasiertes Sicherheitsmodell für elektronische Prüfungen an Hochschulen

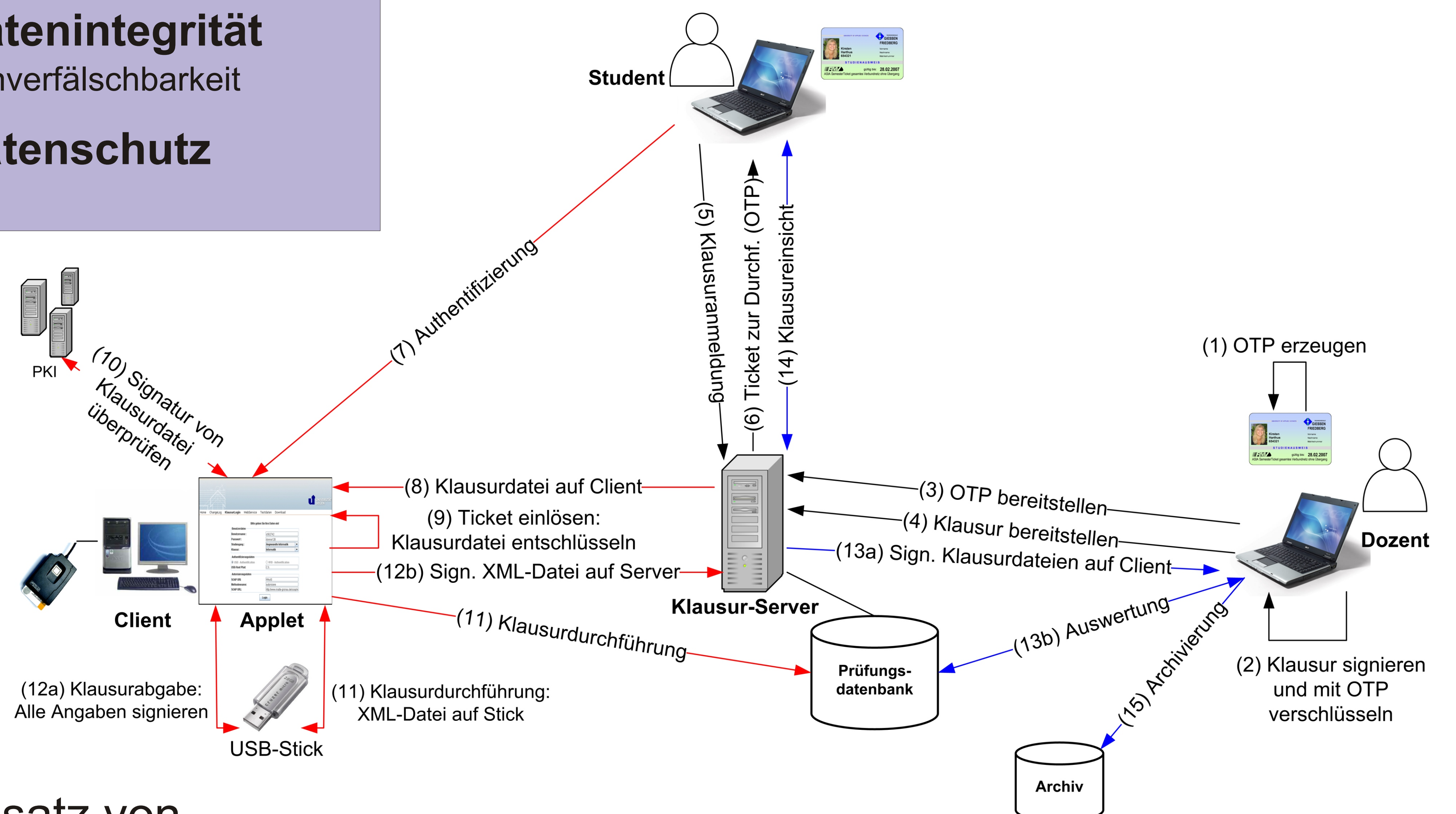
Die Sicherheit von elektronischen Prüfungen ist abhängig von der Prüfungsart (formativ, summativ), der Prüfungsphase (Vorbereitung, Durchführung, Nachbereitung) und der Durchführungsart der einzelnen Prüfungsphasen (lokal oder verteilt).

### Sicherheitsziele



### Realisierungskonzept

- Smartcard basierter Ansatz:
  - ➔ Elektronischer Studierendenausweis
  - ➔ Elektronischer Mitarbeiterausweis

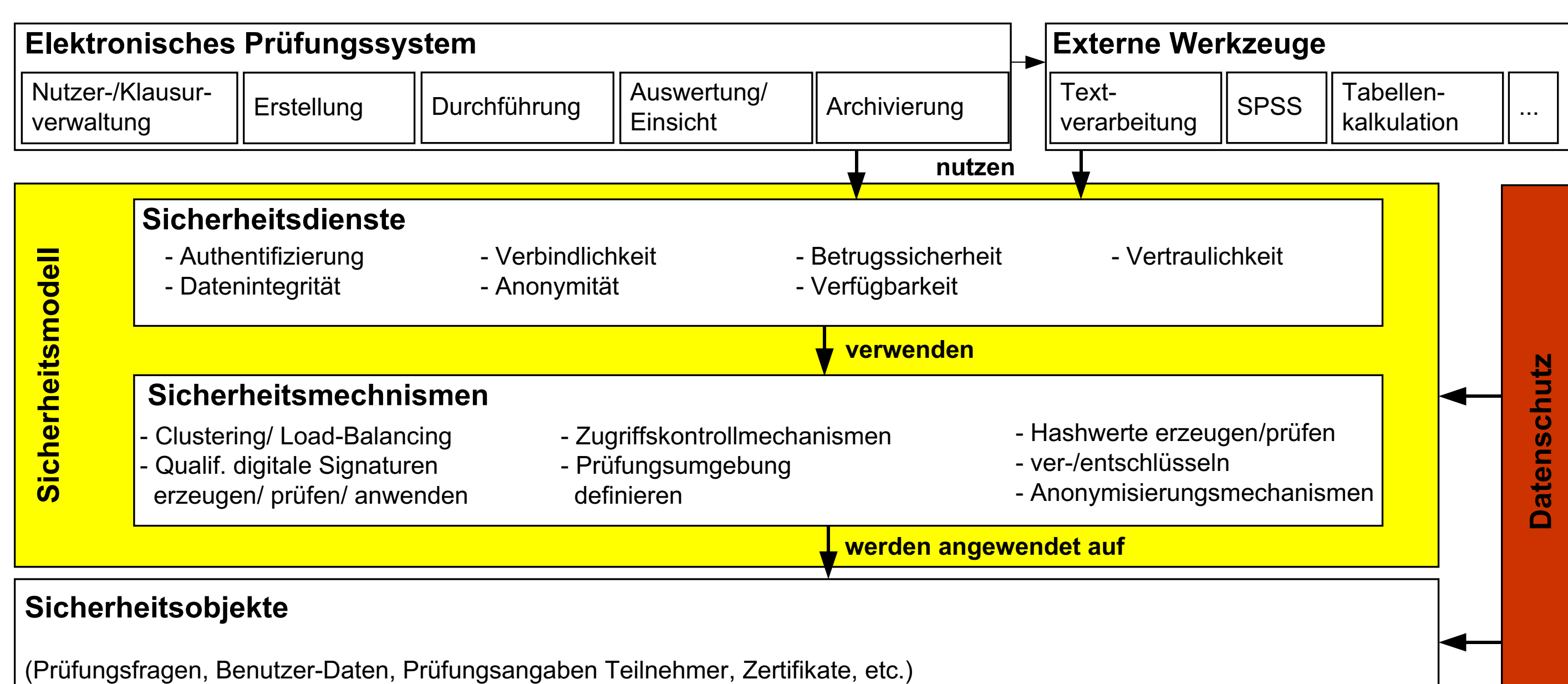


- Verbindlichkeit setzt den Einsatz von qualifizierenden digitalen Signaturen voraus
- Zielkonflikt: Anonymität ⚡ Verbindlichkeit
- Datenschutz: "Der Student muss Herr über seine Daten bleiben!"

### Virtuelles, ticketbasiertes Dateisystem der elektronischen Gesundheitskarte als Grundlage

- ➔ Anonymität trotz Authentizität
- ➔ Verbindlichkeit durch Einsatz von qualifizierenden digitalen Signaturen
- ➔ Gruppen- und Individualrechte
- ➔ Qualitätssicherung durch transparente und standardisierte Verfahren
- ➔ Der Student bleibt Herr über seine Daten

### Sicherheitsmodell



### Knoppix-basierte Client-Lösung

- ➔ definierte Prüfungsumgebung

### Ausfallsicherheit durch lokale und verteilte Speicherung der Daten

- ➔ Klausurdurchführung trotz Netzwerk- oder Serverausfall

- Sicherheitsdienste werden in Abhängigkeit der jeweiligen Prozesse verwendet
- Externe Werkzeuge sind auch während der Prüfung einsetzbar

Fachbereich 12 - Elektrotechnik und Informatik