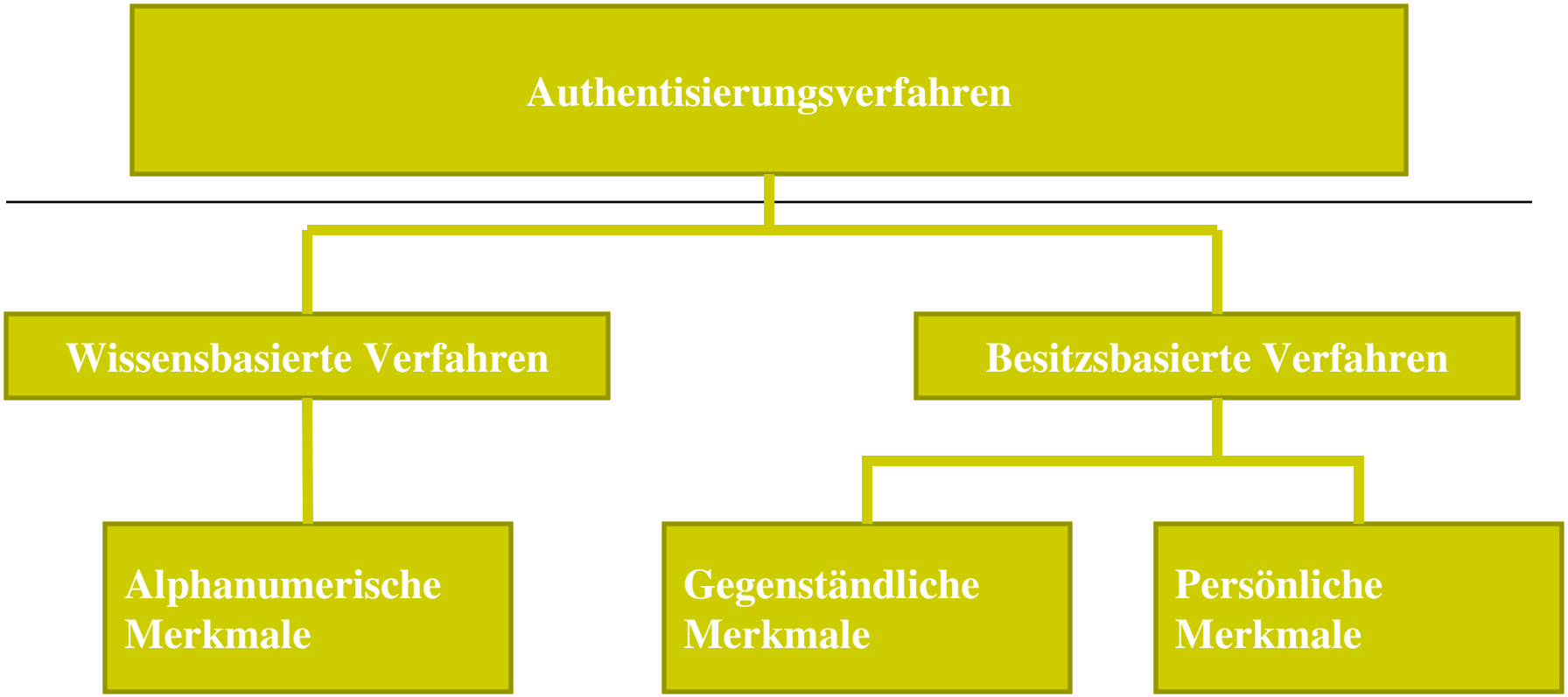
5. Authentifizierung: Biometrie

Universitatea “TRANSILVANIA” din Brasov

1. Authentifizierung

1. Wissen und Besitz
2. Challenge Response Verfahren
3. Kerberos
4. Chipkarte und Biometrie
5. Public-Key Infrastructure und Signaturgesetz



Biometrische Verfahren

Verschiedene Authentifikationsprotokolle
zwischen anfragenden Client und Dienste anbietenden Server

3.Biometrische Authentifizierungssysteme(1)

- **Sicherheit basiert auf nicht fälschbaren körperlichen Merkmalen**
- **Fingerabdruck, Iris, Farbe der Hornhaut, Stimmfrequenz,**

markante Gesichtsknotenpunkte (Stirn, Augenhöhlen, Nase)

- **scheiderten bisher an der riesigen Datenflut**
- **nunmehr Reduktion der Information auf wenige, aber wesentliche Daten möglich**

Prinzip Einmalige Erfassung der biometrischen Daten als Referenzwerte in geschütztem Medium des Systems (Datenbank, Chipkarte etc.).Sensor nimmt die aktuellen Messwerte zur Authentifizierung auf Verarbeitungseinheit vergleicht die aktuellen Merkmale mit den Referenzwerten und je nach Übereinstimmungsgrad erfolgt die Autorisierung

Erfassungsgeräte: Scanner für Finger, Iris etc., Infrarotgerät, Videokamera,Mikrophon

3.Biometrische Authentifizierungssysteme(2)

- **Persönliches Merkmal:**

-**Verfügbarkeit:** alle Benutzer verfügen über dieses persönliche Merkmal

-**Unveränderbarkeit:** Merkmal verändert sich nicht in kurzen Abständen

-**Eindeutigkeit:** Eindeutigkeit: unverwechselbare Identifikation des Benutzers

- **Verwendete biometrische Merkmale :**

-**Hand:** Abdruck von Finger bzw. Handballen, Venenmuster auf Handrücken

-Gesicht: Auswertung von charakteristischen Punkten im Bereich Nase, Mund und Augenbrauen

-Auge: Struktur der Retina (Augenhintergrund) und Iris (Muskel um die Pupille)

-Sprache: Frequenzspektrum der Stimme

3.Biometrische Authentifizierungssysteme(3)

Problem Fehlerkennungen und Fehlabweisungen

- Authentifizierung basiert auf der Wiedererkennung des Referenzmerkmals nach dem Lesen und Vergleich mit dem aktuellen Merkmal
- Jeder Benutzer ist ein Individuum und seine körperlichen Merkmale sind einmalig !
- Aber: Zwei digitale Abbilder biometrischer Merkmale sind niemals wirklich identisch, da zeitlich bedingte Änderungseffekte eintreten

Neue Fehlerarten, die in der klassischen Authentifikation nicht vorhanden sind :

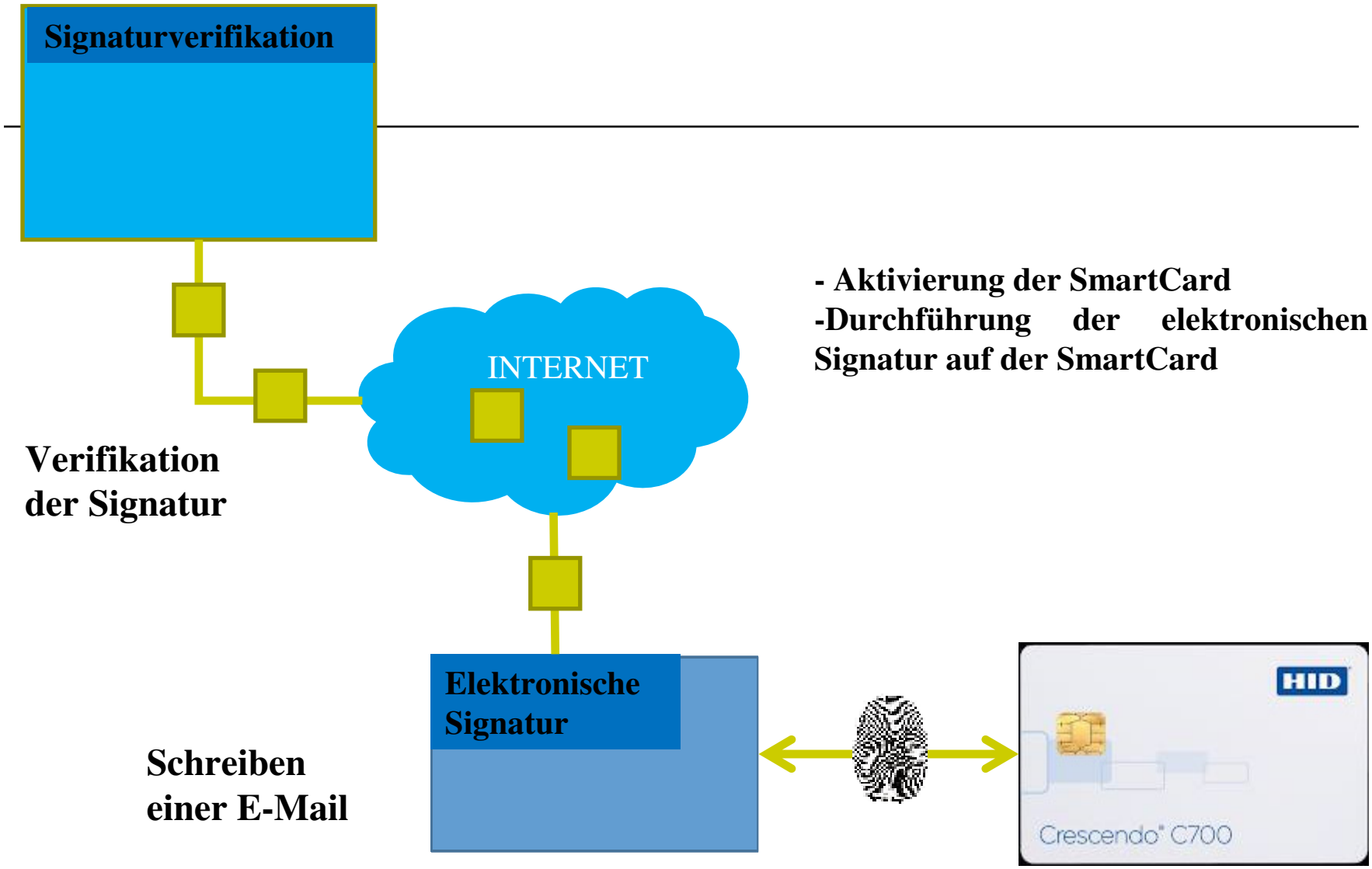
False Acceptance Rate: Anteil der fälschlich akzeptierten Benutzer

False Reject Rate Anteil: der fälschlich abgewiesenen Benutzer

False Enrolment Rate : Kein geeignetes Merkmal

Failure to Acquire: Vorhandenes geeignetes Merkmal verändert sich zu schnell

4.Fingerprint und eMail-Sicherheit



5.Fingerprint und Datei-Sicherheit