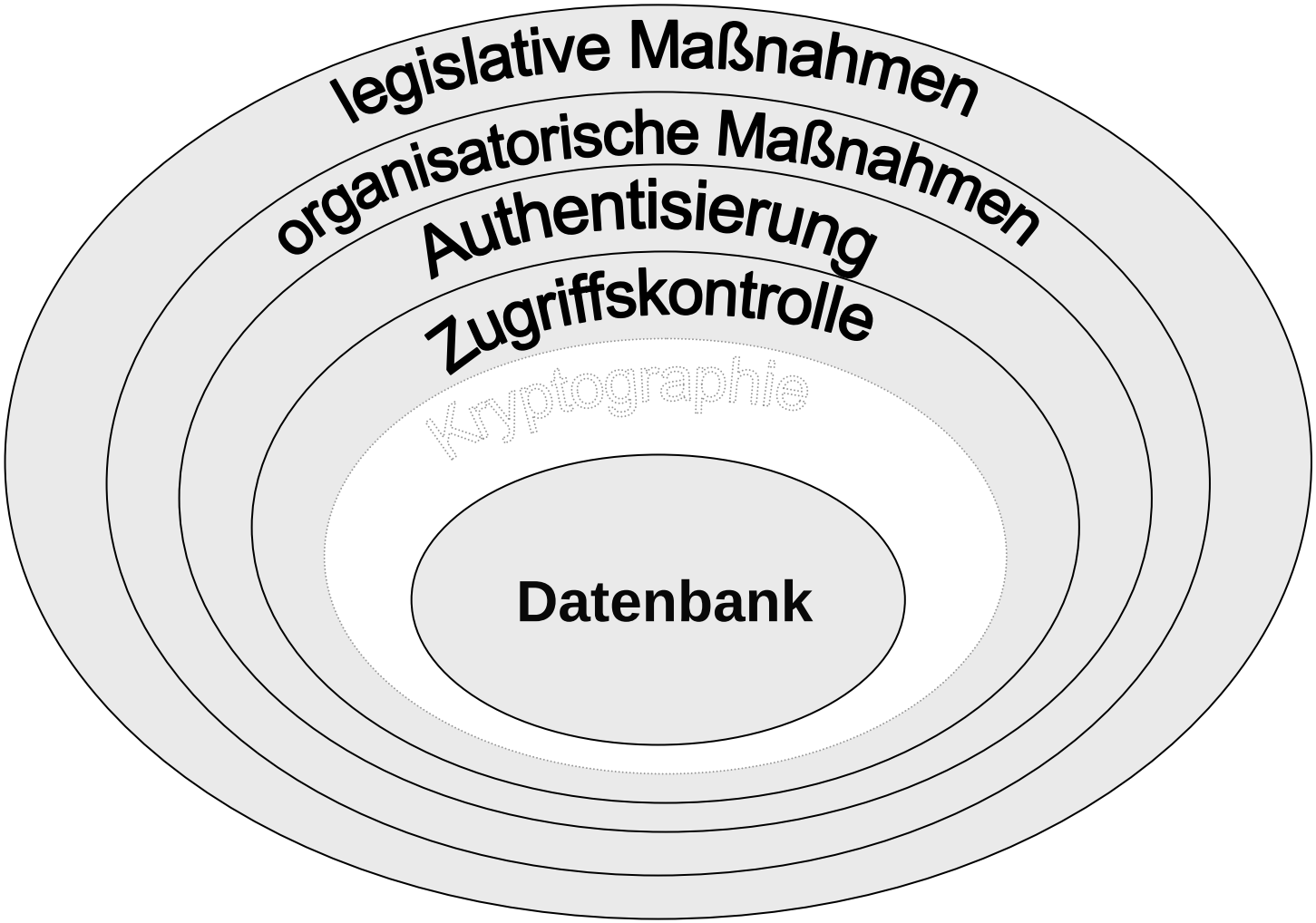
Datenbanksysteme SS 2007

Frank Köster
(Oliver Vornberger)

Institut für Informatik
Universität Osnabrück

Kapitel 15:
Sicherheit

Datenschutz



Legislative Maßnahmen

Gesetz zum Schutz vor Missbrauch personenbezogener Daten

Organisatorische Maßnahmen

- bauliche Maßnahmen
- Pförtner
- Ausweiskontrolle
- Diebstahlsicherung
- Alarmanlage

Authentisierung

- Magnetkarte
- Stimmanalyse
- Fingerabdruck
- Passwort
- dynamisches Passwort

Zugriffskontrolle durch Berechtigungsmatrix

Benutzer	Ang-Nr	Gehalt	Leistung
A (Manager)	R	R	RW
B (Personalchef)	RW	RW	R
C (Lohnbüro)	R	R	-

Zugriff (*A*, Gehalt): *R*: Gehalt < 10.000
W: Gehalt < 5.000

Zugriffskontrolle durch Sichten

```
create view v(angnr, gehalt) as
select angnr, gehalt from angest
where gehalt < 3000
```

Zugriffskontrolle durch Abfrageeinschränkung

```
deny (name, gehalt) where gehalt > 3000
                          +
select gehalt from angest where name = ‘Schmidt‘
                          =
select gehalt from angest
where name = ‘Schmidt‘ and not gehalt > 3000
```

Statistische Datenbanken

Nur aggregierte Werte als Query-Resultat erlaubt!

Obacht!

```
select sum (gehalt) from angest
```

```
select sum (gehalt) from angest
where gehalt < (select max(gehalt) from angest)
```

Zugriffsrechte in SQL-92

```
grant { select |
        insert |
        delete |
        update |
        references |
        all }
on <relation> to <user> [with grant option]
```

***A*: grant read, insert on angest to *B* with grant option**
***B*: grant read on angest to *C* with grant option**
B*: grant insert on angest to *C

Beachte bei Recht auf Fremdschlüssel:

Probeweises Einfügen kann Schlüssel finden !

```
create table Agententest(Kennung character(3) references Agenten)
```

Revoke-Anweisung

```
revoke { select |
         insert |
         delete |
         update |
         references |
         all }
on <relation> from <user>
```

B*: revoke all on angest from *C

Entzug eines Grant

… als wenn es nie gewährt worden wäre:

```
A: grant read, insert, update on angest to D
B: grant read, update         on angest to D with grant option
D: grant read, update         on angest to E
A: revoke insert, update      on angest from D
```

D verliert nur sein insert-Recht, weil update von B erh.

E verliert keine Rechte (weil indirekt von B erhalten)

```
B: revoke update              on angest from D
```

D verliert update-Recht

E verliert update-Recht

Auditing

Beobachtung von DB-Aktionen werden in System-tabellen abgelegt und stehen über spezielle Views zur Verfügung:

```
audit delete any table

noaudit delete any table

audit update on professoren
      whenever not successful
```

Ende von Kapitel 15:
Sicherheit