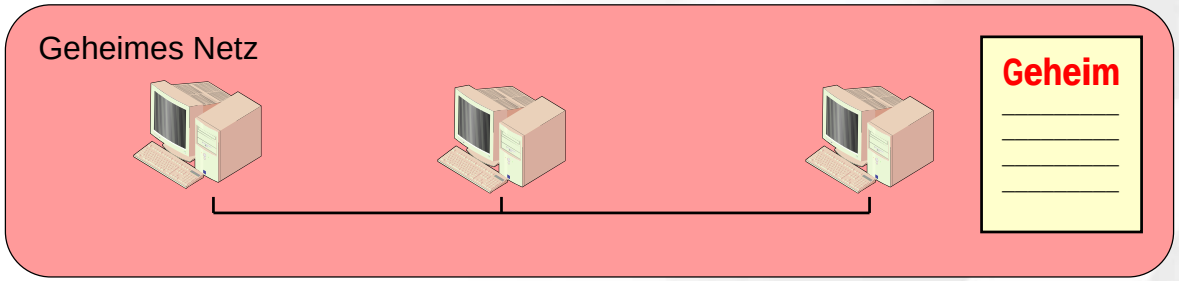
Entwicklung/Evaluierung eines
Hochsicherheits-Gateways
zur Trennung verschieden eingestufter Netze

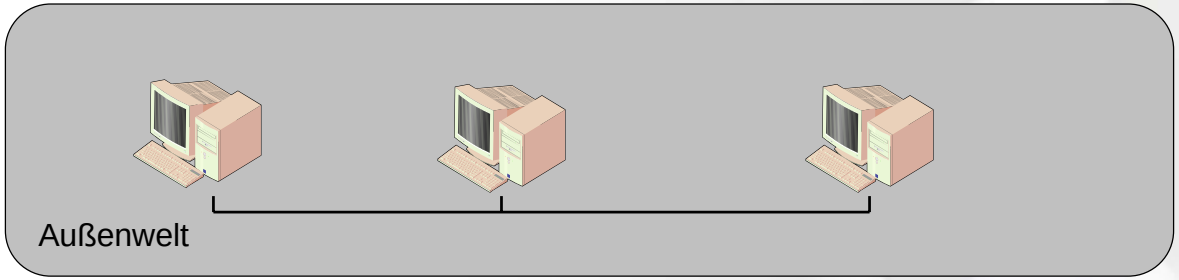
Dirk Loss
IT-Sicherheitsberater, INFODAS GmbH

18.05.2006, IT-Symposium 2006, Neuss

Wie lassen sich Netze absichern, die geheime Daten enthalten?

- Variante 1: Physische Trennung

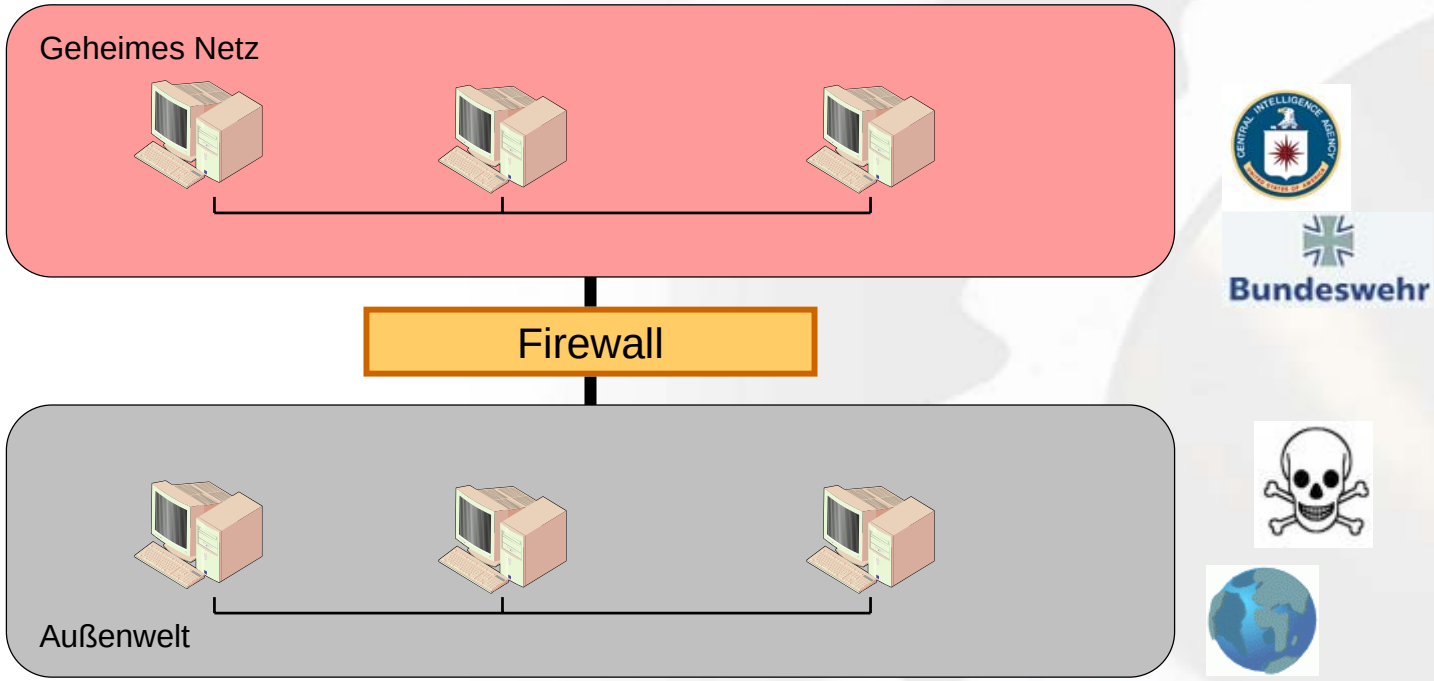




Problem Kein netzbasierter Austausch von Daten

Variante 2: Firewall

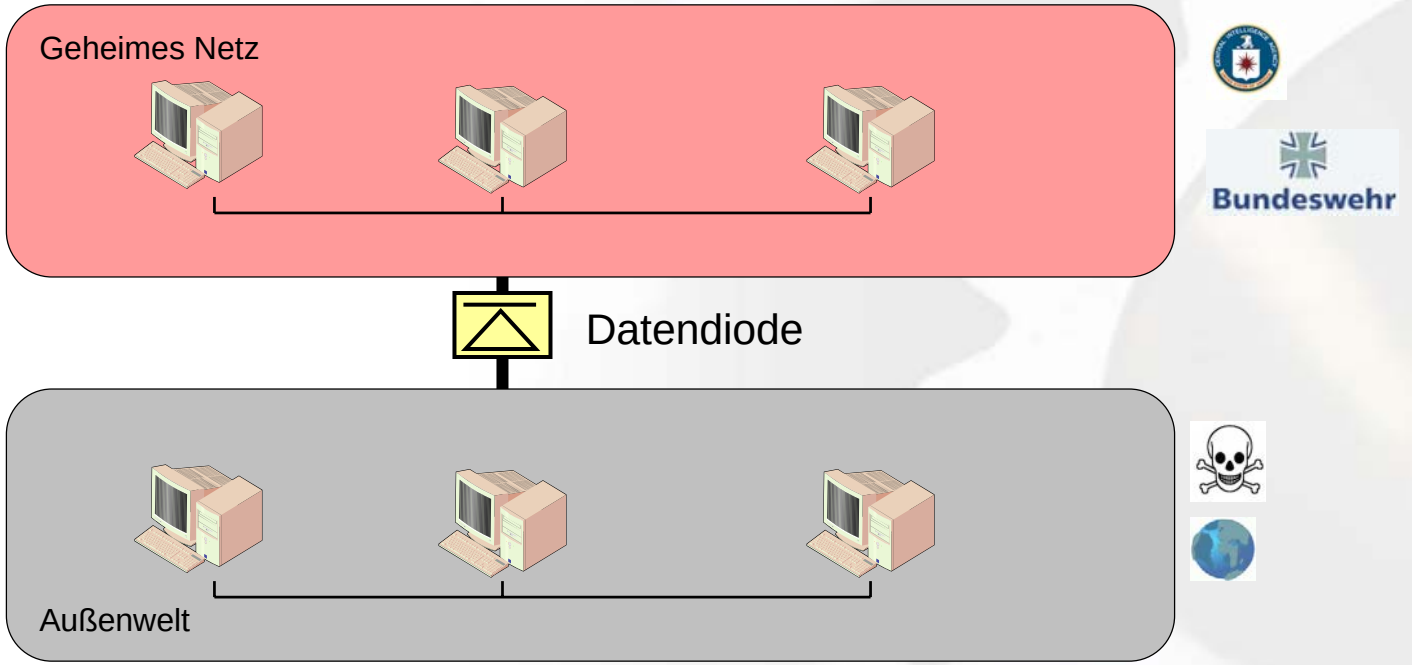
- Schützt vor Angriffen



Problem Verhindern, dass geheime Daten nach außen gelangen

Variante 3: One-Way-Gateway / Datendiode

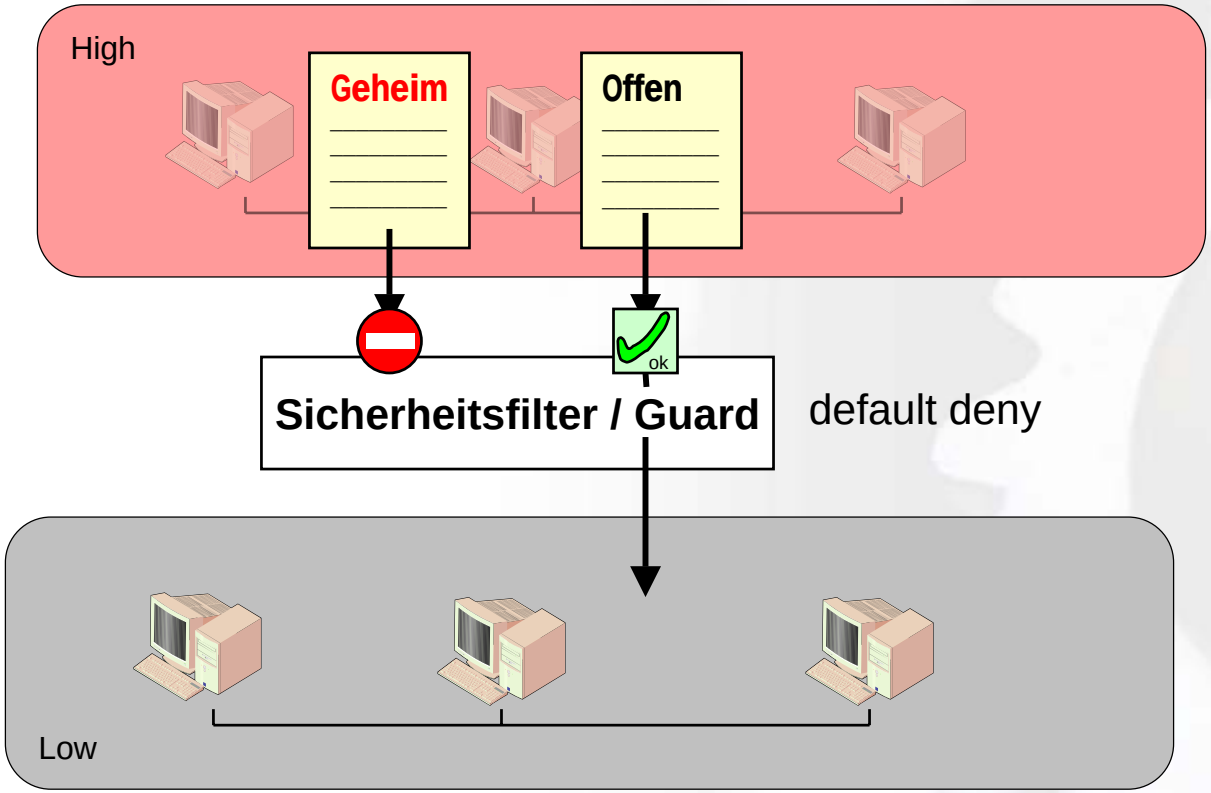
- Verhindert jede Datenübertragung nach außen



Problem Keine Anfragen, keine Quittungen: UDP statt TCP

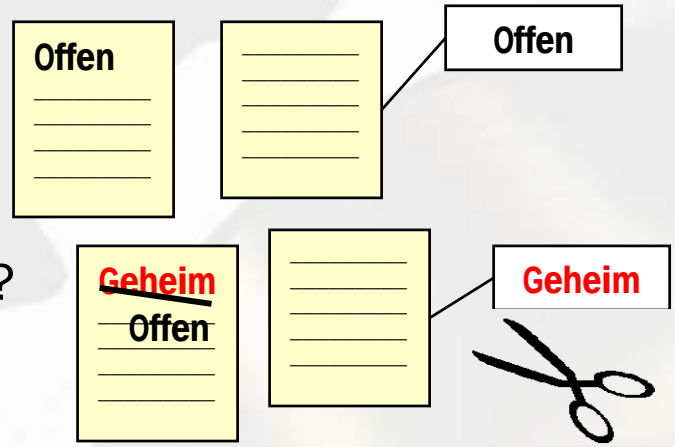
Variante 4: Spezieller Sicherheitsfilter

- Weiterleitung von Dokumenten nur nach Prüfung des Geheimhaltungsgrads



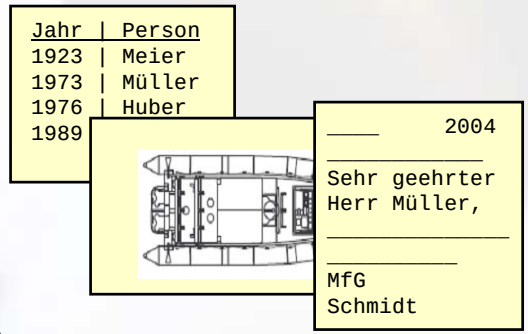
Woran erkennt der Filter den Geheimhaltungsgrad?

a) **Explizite** Information über Einstufung vorhanden
   - innerhalb des Dokuments
   - als externes Label



Problem Ist diese Information vertrauenswürdig?

b) Einstufung ergibt sich **implizit** aus dem Dokument selbst
   - Inhalt, Struktur, Kommunikationsumstände



Problem Nur ein Mensch kann die Bedeutung erfassen

Idee: Manuelle Freigabe

1. Mensch trifft die Entscheidung,
   ob das Dokument übertragen werden darf
   a) Ersteller des Dokuments (am Arbeitsplatz, dezentral)
   b) Evtl. Sicherheitsoffizier (zentral)

problematisch

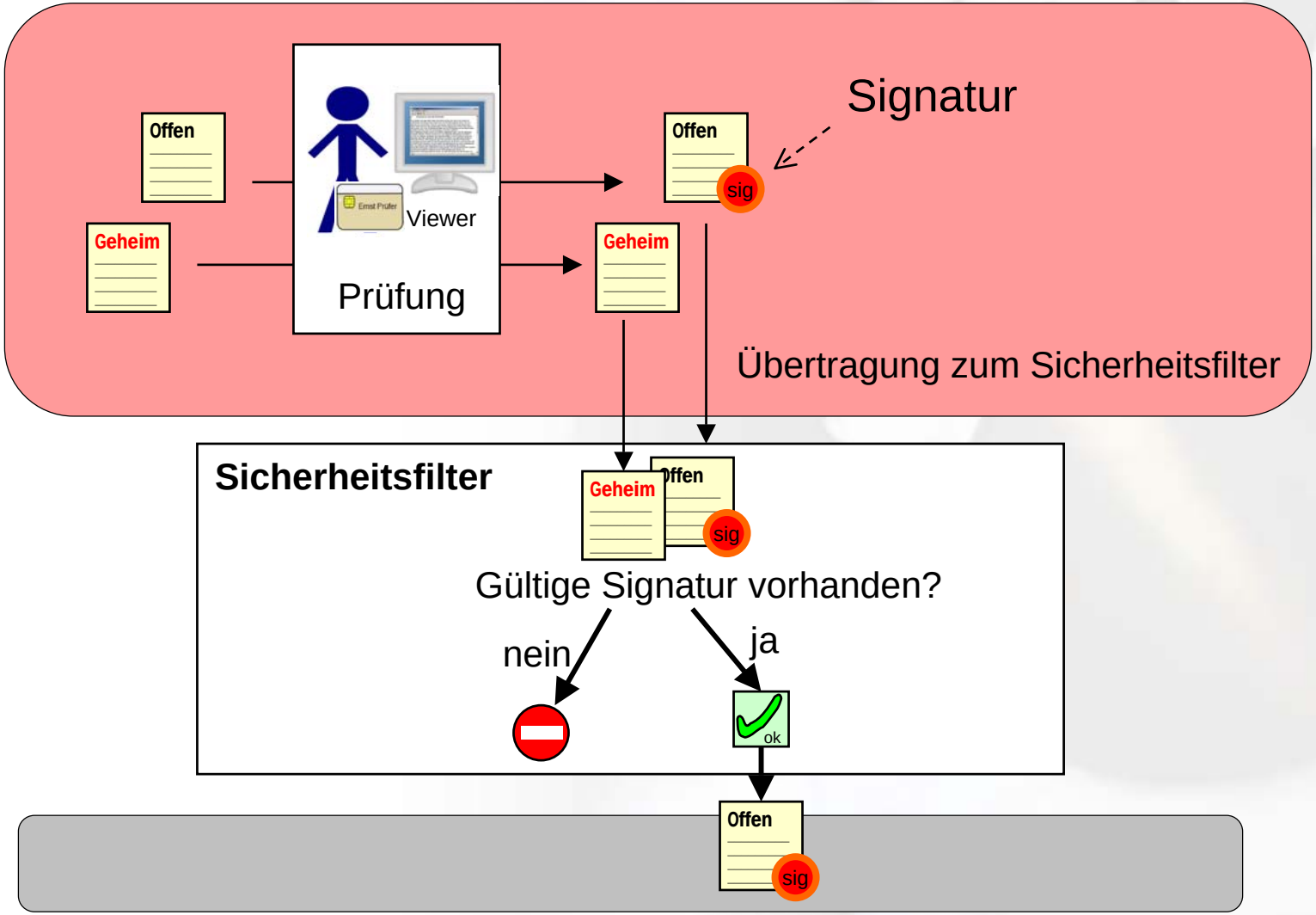
2. Sicherheitsfilter setzt diese Entscheidung um,
   indem er das Dokument nach außen überträgt oder nicht

Problem Wie kommt die vom Menschen getroffene Entscheidung

- auswertbar, unverfälscht, zurechenbar

zum Sicherheitsfilter?

Manuelle Freigabe durch Signieren



„What you see is what you sign“

- Was gebe ich da eigentlich frei?
- Restinformationen in der Datei
  - z.B. Überarbeitungsmarkierungen und Makros in Word-Dateien
- Steganografie
  - z.B. weißer Text auf weißem Grund, Codieren von Texten in Anzahl Leerzeichen
- Trojaner
  - Verdecken der Anzeige, Ausspähen der PIN, Fernsteuern des Viewers, ...

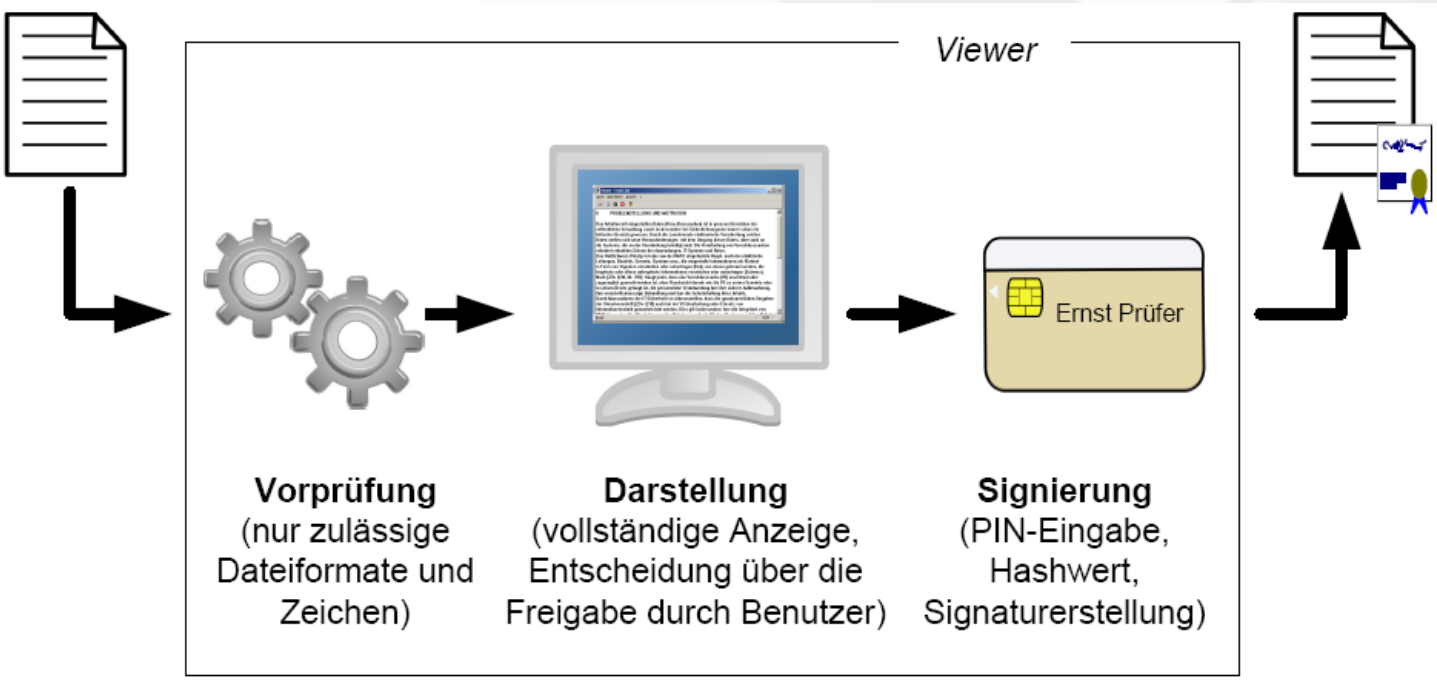
Zulässige Dateiformate?

Gibt es Innentäter?

Sichere Plattform

Secure Viewer

- Gekapselter Prozess: Darstellung+Signierung
- Absicherung der Plattform
- Einschränkung der Dateiformate



Manuelle Freigabe
Nachteile

- Benötigt (zusätzliches) Personal
- Geringe Performance
  - Komplettes Durchlesen ist nur für kurze Dokumente realistisch
  - Langsam: Wenige Dokumente pro Zeiteinheit
- Ermüdung kann zu Fehlern führen

- Vertrauenswürdige Anzeige
  nur für bestimmte Dateiformate realisierbar
- Kein Schutz gegen bewusstes Freigeben geheimer Dokumente durch berechtigte Benutzer

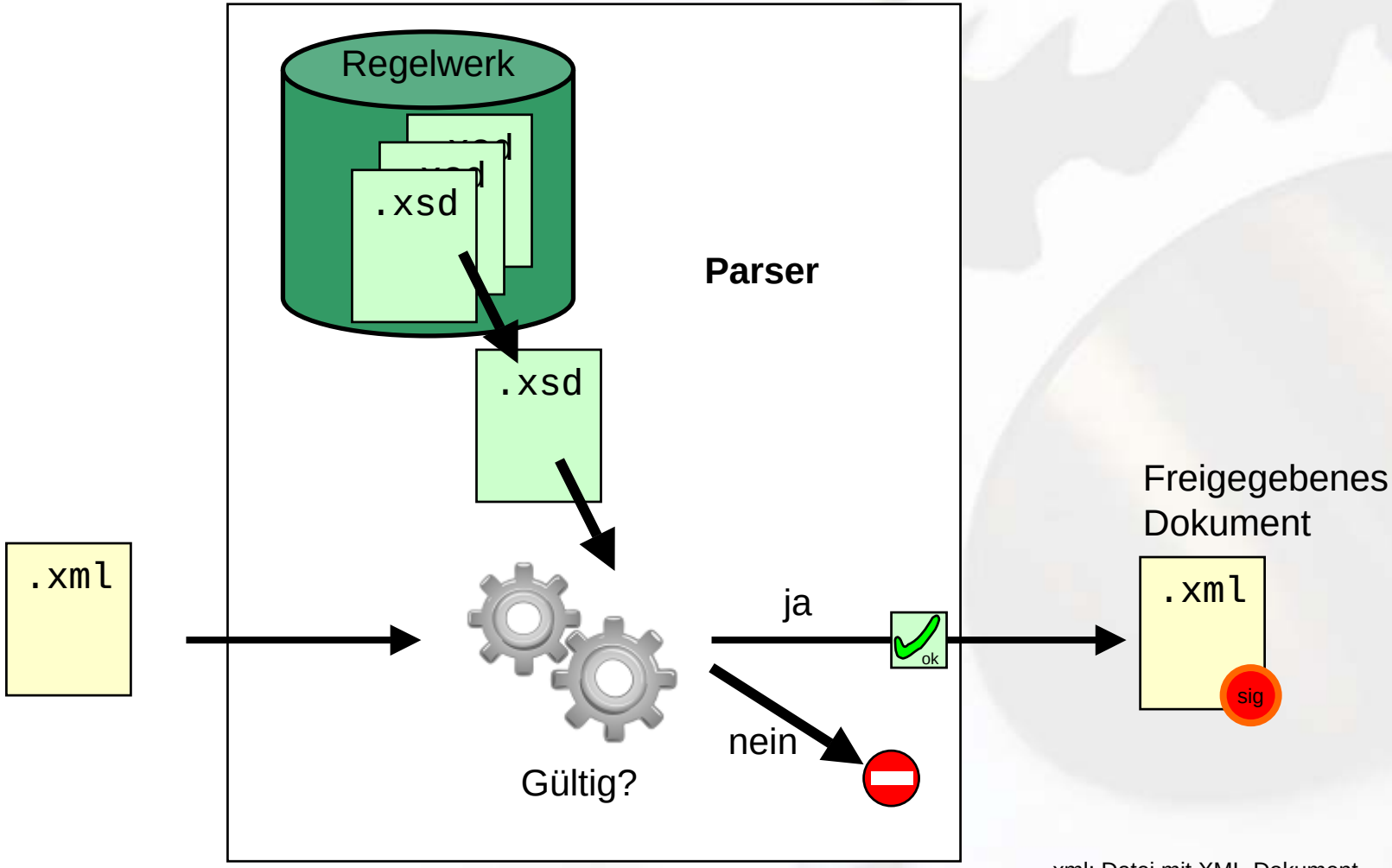
Automatische Prüfung – eine Alternative?

- Automatische Freigabe von speziell strukturierten Dokumenten ist möglich
  - Frei formulierter Text darf aber nicht enthalten sein
- Beispiel: XML-Dateien

```
<airops>
   <day-time> 020200Z </day-time>
   <quantity> 6 </quantity>
   <country> IT </country>
   <aircraft_type> F16 </aircraft_type>
   <track_number> 123 </track_number>
   <course> 160 </course>
   <speed unit="kph"> 700 </speed>
   <altitude unit="feet"> 12000 </altitude>
</airops>
```

- Struktur/Grammatik festlegen
- Zulässige Werte der einzelnen Elemente genau angeben

Automatische Freigabe
Beispiel XML



.xml: Datei mit XML-Dokument

.xsd: Datei mit XML-Schema

Freigabe von XML-Dokumenten Regelwerk

- Die Schemata müssen sicherstellen, dass keine vertraulichen Daten im XML-Dokument enthalten sind
  - Einschränkung durch Angabe von Datentypen und Wertebereichen mit Hilfe von „restrictions“

```
<element name=„quantity">
  <simpleType>
   <restriction base=‚integer'>
     <minInclusive value=‚5'/>
     <maxInclusive value=‚10'/>
   </restriction>
  </simpleType>
</element>
```

Beispiel 1:
Zulässige Intervalle für Zahlen festlegen

```
<xsd:element name=„aircraft_type">
 <xsd:simpleType>
  <xsd:restriction base="xsd:string">
    <xsd:pattern value=""/>
      <xsd:enumeration value=„F16"/>
      <xsd:enumeration value=„F117A"/>
      <xsd:enumeration value="Eurofighter“/>
      <xsd:enumeration value=„Mirage 2000"/>
   </xsd:restriction>
 </xsd:simpleType>
</xsd:element>
```

Beispiel 2: Zulässige Strings auflisten

- Gewährleisten, dass geeignete restrictions vorhanden sind

Konkrete Realisierung: RS-Gate

- Freigeben von Dokumenten durch digitales Signieren
  - Manuell per Viewer
    - TXT (ASCII), BMP (schwarz/weiß), RTF (Subset)
  - Automatisch per XML-Parser
    - Signiert erfolgreich geprüfte XML-Dokumente
    - Regelwerk in Form von XML-Schemata (mit restrictions)
- Dateiübertragung in Form von E-Mail-Attachments (SMTP)
  - Bereinigung von Steuerinformationen
- Sicherheitsfilter am Netzübergang prüft Signaturen
- Firewall zum Schutz vor Angriffen
  - mit Virenscanner
- In Evaluierung nach ITSEC E3 hoch

Bereinigung von Steuerinformationen

- Geheime Informationen in Kommunikationsprotokollen?
- Sicherheitsfilter generiert für freigegebene Dokumente komplett neue E-Mails
  - Neue SMTP Session
  - Neue Mail-Header
  - Betreff normalisieren
  - Mail-Body verwerfen
  - Dateinamen der Anhänge normalisieren

Evaluierung und Zertifizierung

- Prüfung und Bewertung der Sicherheitseigenschaften durch unabhängige Prüfstelle (Evaluator)
  - Gängige Kriterienwerke: Orange Book, ITSEC, Common Criteria
- Nachweise sind in Form von Dokumentationen vorzulegen
  - zusätzliche Tests oder Tätigkeiten des Evaluators, wo erforderlich
- Zertifizierungsstelle prüft, ob Evaluierung ordnungsgemäß durchgeführt wurde und vergibt Zertifikat

Beispiel ITSEC

1. Funktionalität
   - Sicherheitsvorgaben (Sicherheitsspezifische Funktionen, Bedrohungen, Einsatzumgebung)
2. Vertrauenswürdigkeit
   - Korrektheit (nachweisbare Qualität, sichere Konstruktion/sicherer Betrieb)
   - Wirksamkeit (Widerstandsvermögen gegen Angriffe, Zusammenwirken der Mechanismen)

ITSEC
Aspekt Vertrauenswürdigkeit

Korrektheit

E1	informelle Beschreibung des Architekturentwurfs, funktionale Tests und Penetrationstests.
E2	informelle Beschreibung des Feinentwurfs.
E3	Bereitstellung von Quellcode bzw. Hardware-Konstruktionszeichnungen und Abbildung auf die Basiskomponenten.
E4	formales Sicherheitsmodell, semiformale Notation der sicherheitsspezifischen Funktionen, des Architektur- und des Feinentwurfs.
E5	Feinentwurf muss nachvollziehbar auf Quellcode bzw. Hardware-Konstruktionszeichnungen abgebildet werden.
E6	formale Spezifikation des Architekturentwurfs.

Wirksamkeit

Niedrig:	Mechanismen bieten Schutz gegen zufälliges, unbeabsichtigtes Überwinden der Sicherheitsmechanismen
Mittel:	Mechanismen bieten Schutz gegen Angreifer mit beschränkten Gelegenheiten und Betriebsmitteln
Hoch:	Mechanismen können nur von Angreifern überwunden werden, die über sehr gute Fachkenntnisse, Gelegenheiten und Betriebsmittel verfügen, wobei ein solcher erfolgreicher Angriff normalerweise als nicht durchführbar beurteilt wird.

Quelle: http://www.bsi.de/literat/faltbl/itsikrit.pdf

Weitere Aspekte

- Protokollierung
- Administration
- Performance
- (Hoch-)Verfügbarkeit
- Umgebungen mit mehr als zwei Sicherheitsleveln

Fazit

- Um die Weitergabe geheimer Daten zu verhindern, benötigt man Sicherheitsgateways mit speziellen Inhaltsprüfungen
  - Für speziell strukturierte Dokumente ist eine automatische Prüfung und Freigabe möglich
  - Die manuelle Prüfung und Freigabe erfordert eine vertrauenswürdige Anzeigefunktion
- Vertrauen in die Sicherheitseigenschaften kann durch unabhängige Evaluierungen gebildet werden
- Steganographische Angriffe lassen sich erschweren, jedoch nicht völlig ausschließen

Herzlichen Dank für Ihre Aufmerksamkeit!

Dirk Loss
INFODAS GmbH, Rhonestr. 2, 50765 Köln
✉ D.Loss@infodas.de, ☎ (0221) 7 09 12 - 19
🕸 www.infodas.de