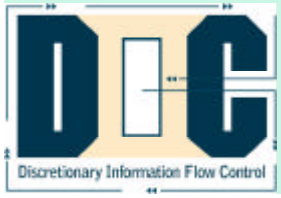
Common Criteria Protection Profile

Regelbasierte Informationsflusssteuerung

(Benutzerbestimmbare Informationsflusssicherheit *BISS*)



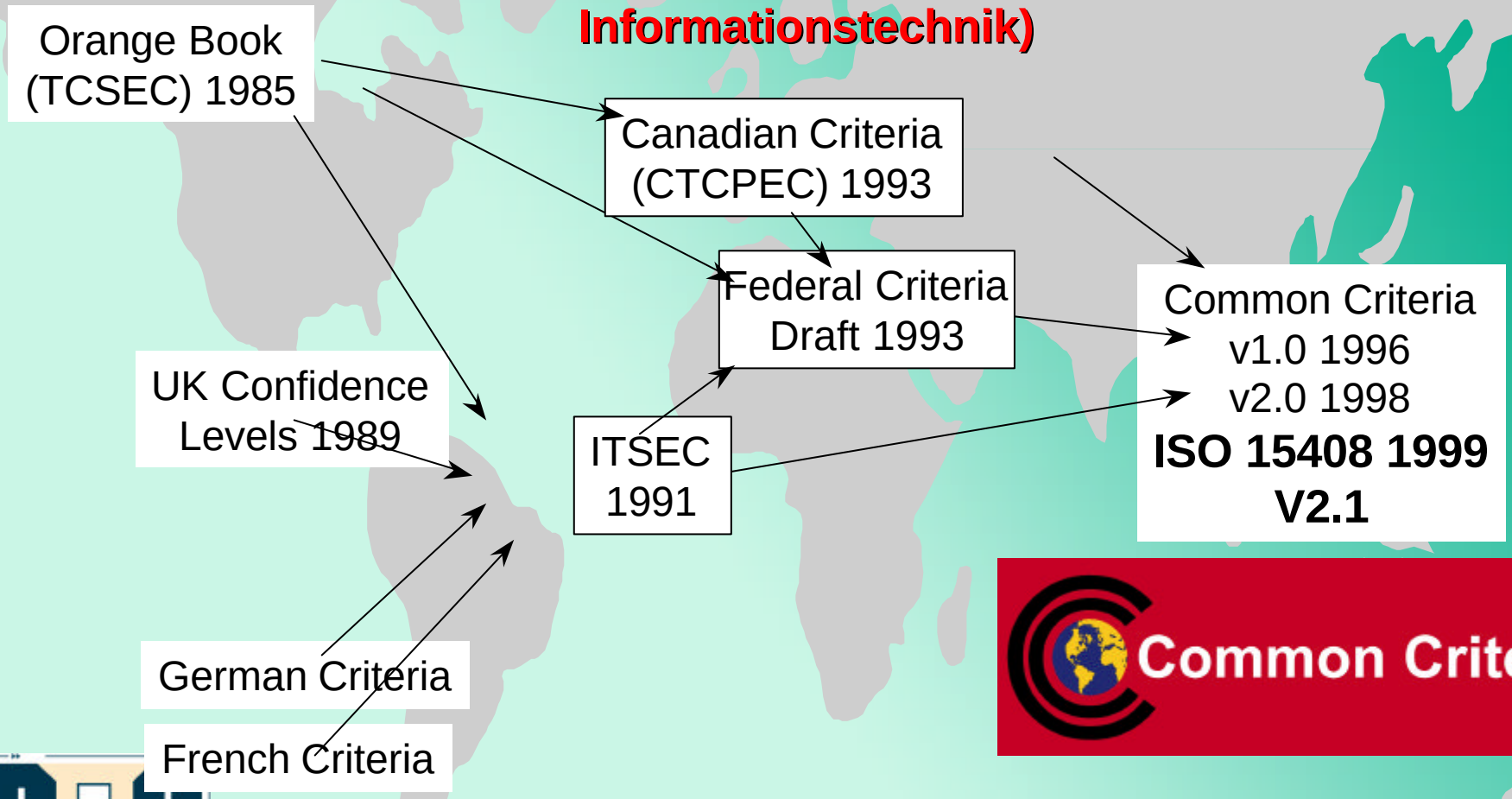
Marcel Weinand

- Die CC und das Konstrukt der Schutzprofile (Protection Profiles PP)
- Wozu das BISS-Schutzprofil?
- Welche Idee steckt hinter BISS?
- Beispiele
- Wie kann BISS realisiert werden?
- Wer kann von BISS profitieren?
- Perspektiven von BISS
- Zusatz: BISS und TCPA

Kriterienwerk CC - ISO 15408

Common Criteria for Information Technology Security Evaluation

(Gemeinsame Kriterien für die Prüfung und Bewertung der Sicherheit von Informationstechnik)



Ziele des Projektes

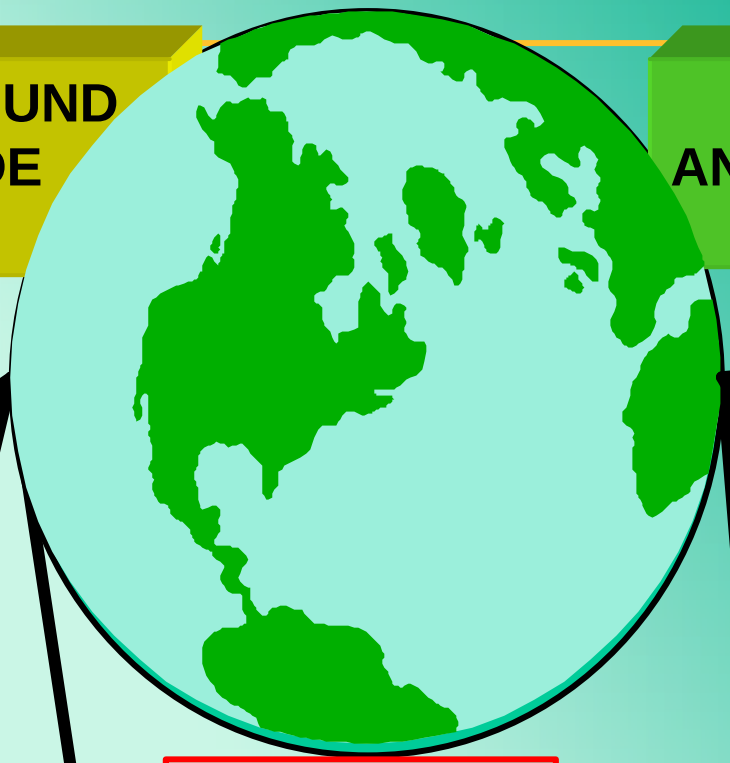
- Ein gemeinsames Kriterienwerk für Produkte und Systeme
  - basierend auf den bisherigen Kriterien
  - eine internationale Basis für Hersteller
- Standardisierung durch ISO
- Gegenseitige internationale Anerkennung von Zertifikaten
- Bessere Verfügbarkeit von hochwertiger IT-Sicherheitstechnik
- Vergleichbarkeit der Ergebnisse von Prüfungen und Bewertungen der Sicherheit

Internationale Anerkennung

BSI

ZERTIFIZIERENDE UND ANERKENNENDE NATIONEN

NUR ANERKENNENDE NATIONEN



- *Australien / Neuseeland*
- *Kanada*
- *Frankreich*
- *Deutschland*
- *Großbritannien*
- *USA*
- *Schweden*
- *Israel*
- *Spanien*
- *Norwegen*
- *Niederlande*
- *Österreich*
- *Griechenland*
- *Italien*
- *Finnland*

DIG Discretionary Information Flow Control

Wer benötigt Schutzprofile?

- IT-Benutzer - jeder, der Sicherheitsbedarf hat
  z.B. kommerzielle Anwender, Anwendergruppen:
  - Unter der Fragestellung: “Was will ich haben oder was benötige ich!” (Vergleichbar mit Pflichtenheft)
- IT-Hersteller - für Produktklassen
  - Hersteller definieren damit IT-Sicherheitsstandards für Produktklassen
- PP ist Produktklassen-orientiert (EVG-Klasse)

Merkmale von Protection Profiles

- PP basiert auf einem Sicherheitsbedarf (Konzept)
  - Enthält Beschreibung der angenommen Einsatzumgebung sowie die vorgesehene Nutzung
- PP deckt alle genannten Sicherheitsziele **vollständig** ab durch kompletten Satz von
  - Anforderungen an die IT-Sicherheits-Funktionalität
  - Anforderungen an die Vertrauenswürdigkeit
- Verwendbar für unterschiedliche Realisierungen
  - Abstraktionsgrad ist unabhängig von der Implementierung
  - hohe Flexibilität durch Platzhalter und Operationen

Bedeutung eines Schutzprofils

- Zertifizierte Schutzprofile werden national registriert und international anerkannt
- Registrierung durch ISO in Vorbereitung
- Schutzprofile haben den Charakter einer *Norm* oder eines *normativen Dokuments*
- Hersteller können die Anforderungen der Schutzprofile erfüllen
  - Nachweis durch Zertifikat möglich
  - Nachweis beinhaltet Vollständigkeit, Korrektheit, Schwachstellenanalyse gemäß EAL-Stufe

Discretionary Information Flow Control

Vorteile von Protection Profiles

- Produkte, die auf einem gemeinsamen Schutzprofil basieren, haben ein gemeinsames Sicherheitskonzept
  - daher gute Vergleichbarkeit verschiedener Produkte
- Vorteile für Anwender von IT (Benutzer-Verbände)
  - Formulierung ihres realen Sicherheitsbedarfs
- Vorteile für Hersteller
  - Erkennen des Marktbedarfs
  - Erfüllung eines Quasistandards durch Zertifikat
- für Forschung/Entwicklung
  - Statuieren sinnvoller Konstrukte von Sicherheitsanforderungen

Discretionary Information Flow Control

Vordefiniertes Sicherheitskonzept als Bestandteil des PP/ST

Beschreibung des zu evaluierenden Gegenstandes *EVG* aus Anwendersicht

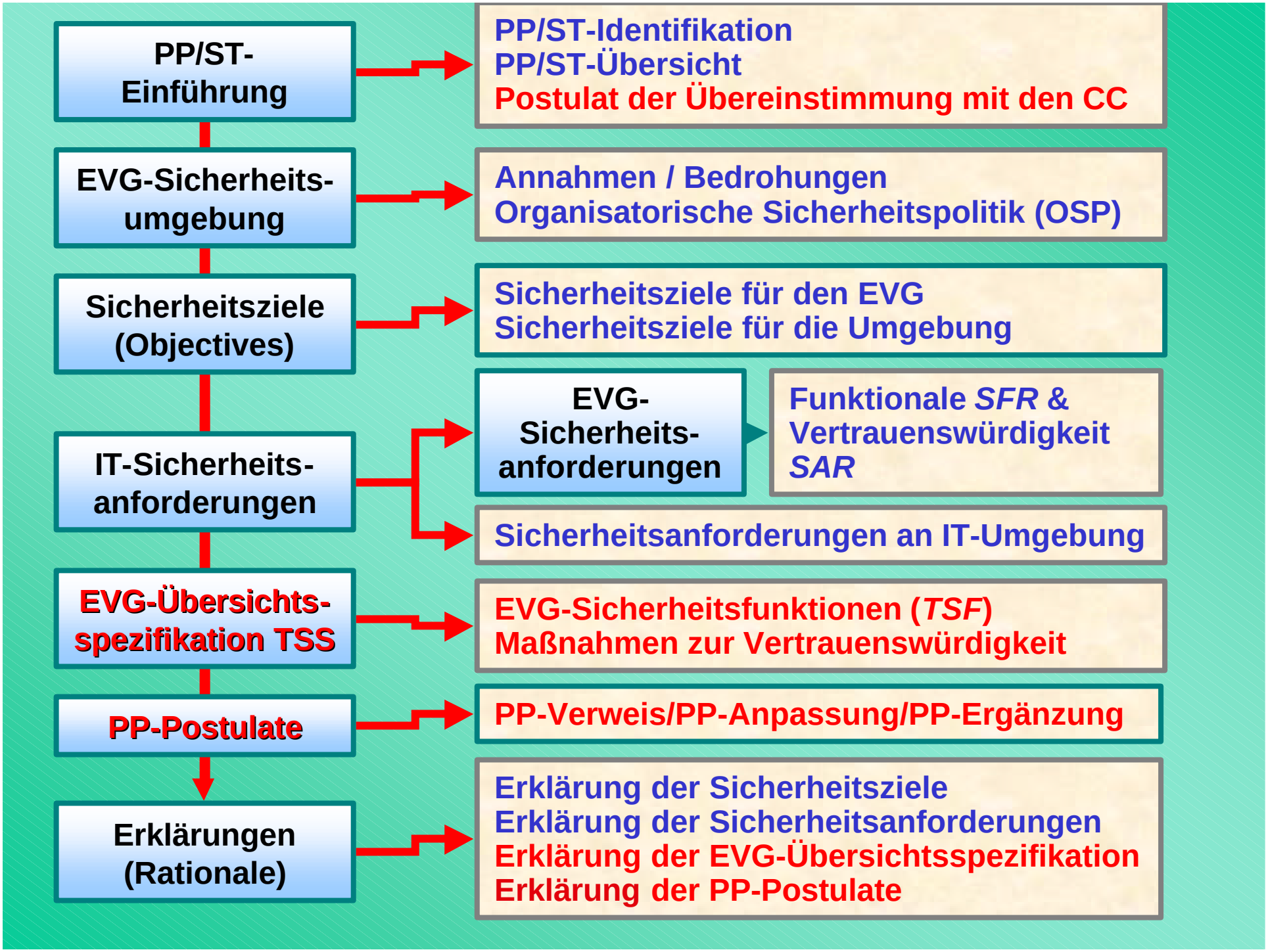
Annahmen zur Einsatzumgebung

Bedrohungen

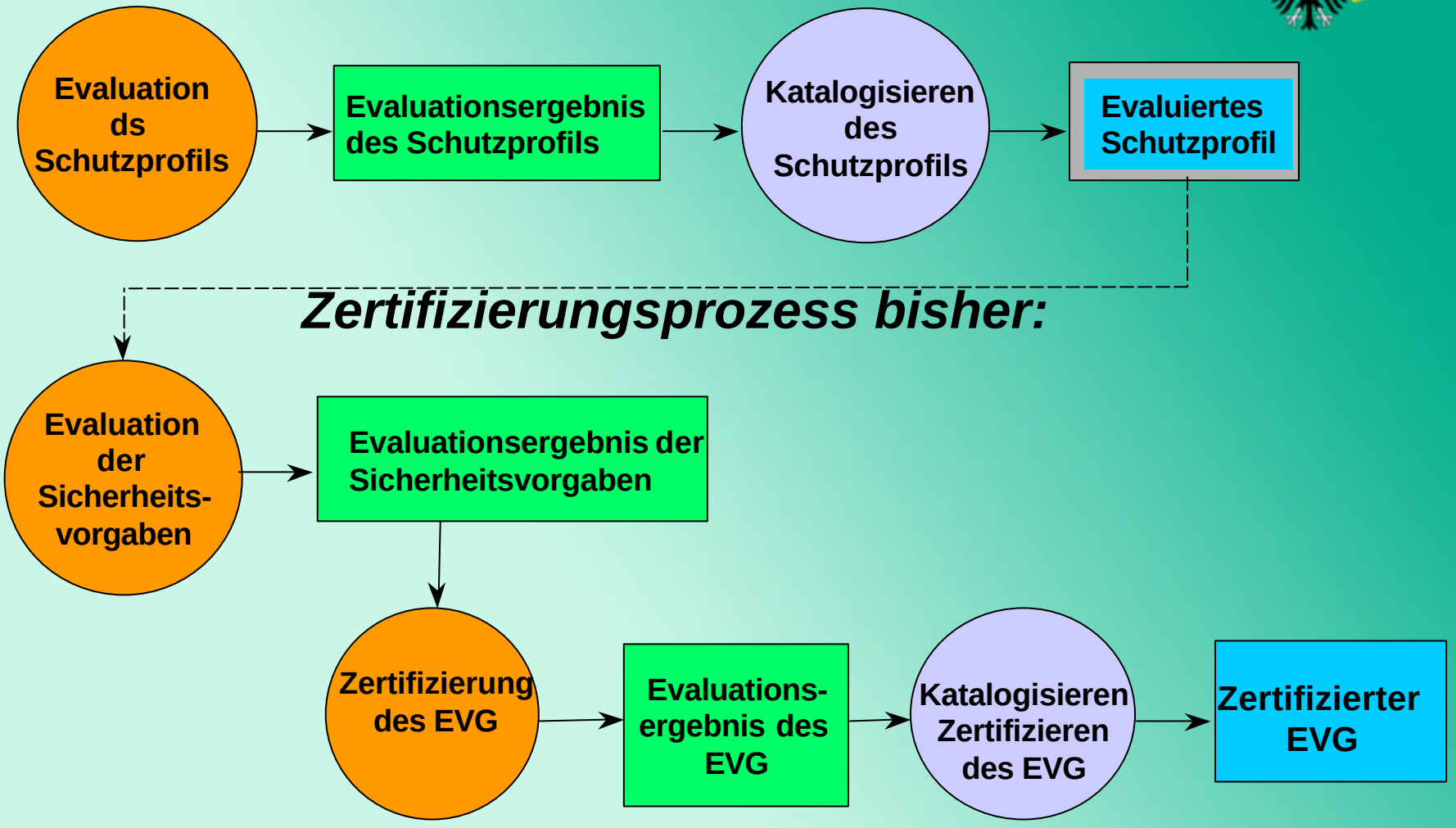
Organisatorische Sicherheitspolitik

Sicherheitsziele

Sicherheitsanforderungen


PP/ST-Einführung
PP/ST-Identifikation
PP/ST-Übersicht
Postulat der Übereinstimmung mit den CC
EVG-Sicherheits-umgebung
Annahmen / Bedrohungen
Organisatorische Sicherheitspolitik (OSP)
Sicherheitsziele (Objectives)
Sicherheitsziele für den EVG
Sicherheitsziele für die Umgebung
IT-Sicherheits-anforderungen
EVG-Sicherheits-anforderungen
Funktionale SFR & Vertrauenswürdigkeit SAR
Sicherheitsanforderungen an IT-Umgebung
EVG-Übersichts-spezifikation TSS
EVG-Sicherheitsfunktionen (TSF)
Maßnahmen zur Vertrauenswürdigkeit
PP-Postulate
PP-Verweis/PP-Anpassung/PP-Ergänzung
Erklärungen (Rationale)
Erklärung der Sicherheitsziele
Erklärung der Sicherheitsanforderungen
Erklärung der EVG-Übersichtsspezifikation
Erklärung der PP-Postulate

Zertifizierungsprozess nach CC



Typen von Zertifizierungsergebnissen

Regelbasierte Informationsflusssteuerung

Modell einer anwenderfreundlichen Sicherheitsarchitektur

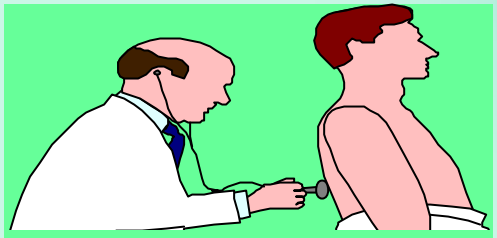
Darstellung anhand des Schutzprofils

Benutzerbestimmbare Informationsflusssicherheit *BISS*

(Discretionary Informationflow Control *DIC*)

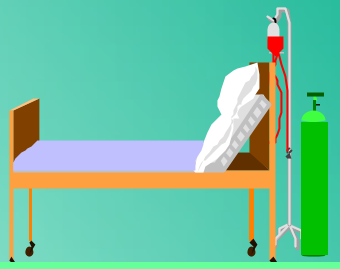
Marcel Weinand
BSI, Bonn

Wozu das BISS-Schutzprofil?
BISS-Historie

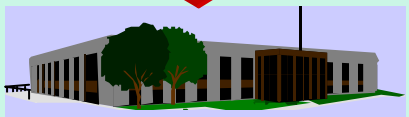


niedergelassene Ärzte

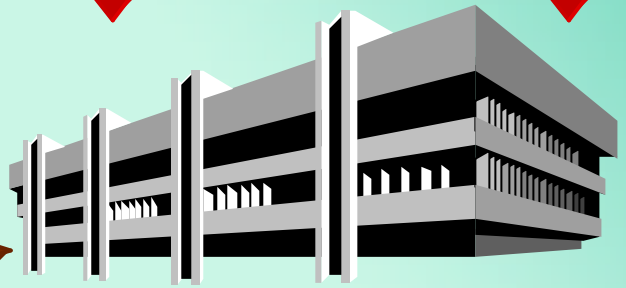
Leistungserbringer



Krankenhäuser



Kassenärztliche Vereinigungen



Datenannahmestellen

Krankenkassen

Gesundheitsreformgesetz 2000

IT im Gesundheitswesen

Aufsichtsbehörden

Rentenversicherungen

Krankenhäuser

Patienten

Apotheken

Informationsdienste

Praxen

Krankenkassen

Labors

Beispiel: Studiennetzwerke

„Maligne Lymphome“

„German Acupuncture Trials (gerac)“

Ministerien

Ärztekammern

Forschungsinstitute

Universitäten

Kassenärztliche Vereinigungen

Apothekerkammern

Pflegedienste

Notfalldienste

Probleme (im Gesundheitswesen)

- Verstreute Information
- Datentransfer in heterogenen Netzen
- Unsichere IT-Ausstattung
- Unerfahrene Benutzer (im Sinne von verantwortlichem IT-Betreiber)
- Existierende Applikationen und Dienste

Datenschutzanforderungen

Beispiel: Datenschutzerklärung der "German acupuncture trials" (gerac):

"Ich bin damit einverstanden, dass … meine Krankheitsdaten ***aufgezeichnet*** und ... ***weitergegeben*** werden. Ich bin auch mit der Einsichtnahme ... in meine Krankenakte einverstanden.

Die Beauftragten der Studienleitung sind … zur ***strengsten Verschwiegenheit*** verpflichtet.

Sie dürfen meine Krankheitsdaten nur in ***verschlüsselter Form*** weitergeben und ***keine Kopien oder Abschriften*** von meinen personenbezogenen Daten herstellen."

Aktive und passive IT-Sicherheit aus Anwendersicht

IT-Sicherheit aus Benutzersicht

- Bewegung und Verarbeitung von Informationen durch Anwendungen
- Spezifikation der IT-Sicherheit aus Sicht von ausgelösten Informationsflüssen
- Benutzerbegriff im Sinne von IT-Betreiber

Technische Anforderungen

- Einfachste Administration
- Schutz sensitiver Information gegen ...
  - ... fehlerhaftes Benutzerverhalten
  - ... unberechtigte Kenntnisnahme / Manipulation
  - ... unzulässige Verarbeitung
- Betriebssystemunabhängigkeit
- Externen Wartungstechniker
- Flexibilität bei Einführung

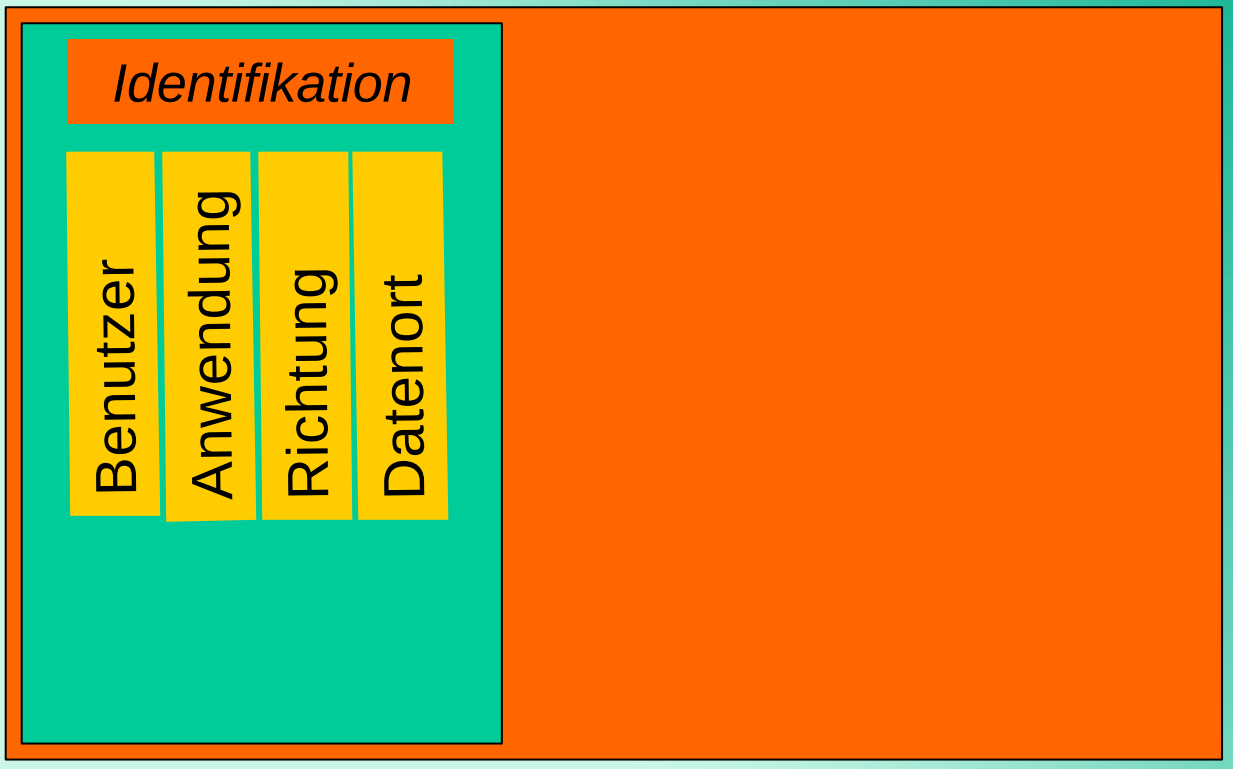
Discretionary Information Flow Control

Technische Anforderungen:

- Transparenz für Applikationen
  - Gleiches IT-Verhalten
  - existierende Anwendungen bleiben unberührt
- Transparenz für alle Benutzer
  - Sicherheitsfunktionen sind immer aktiv
- kein Bedarf für weitere Sicherheitssoftware

Regelbasierte IT-Sicherheit

1. Aufgabe: Eindeutige Identifizierung eines jeden möglichen Informationsflusses aus Sicht des IT-Anwenders



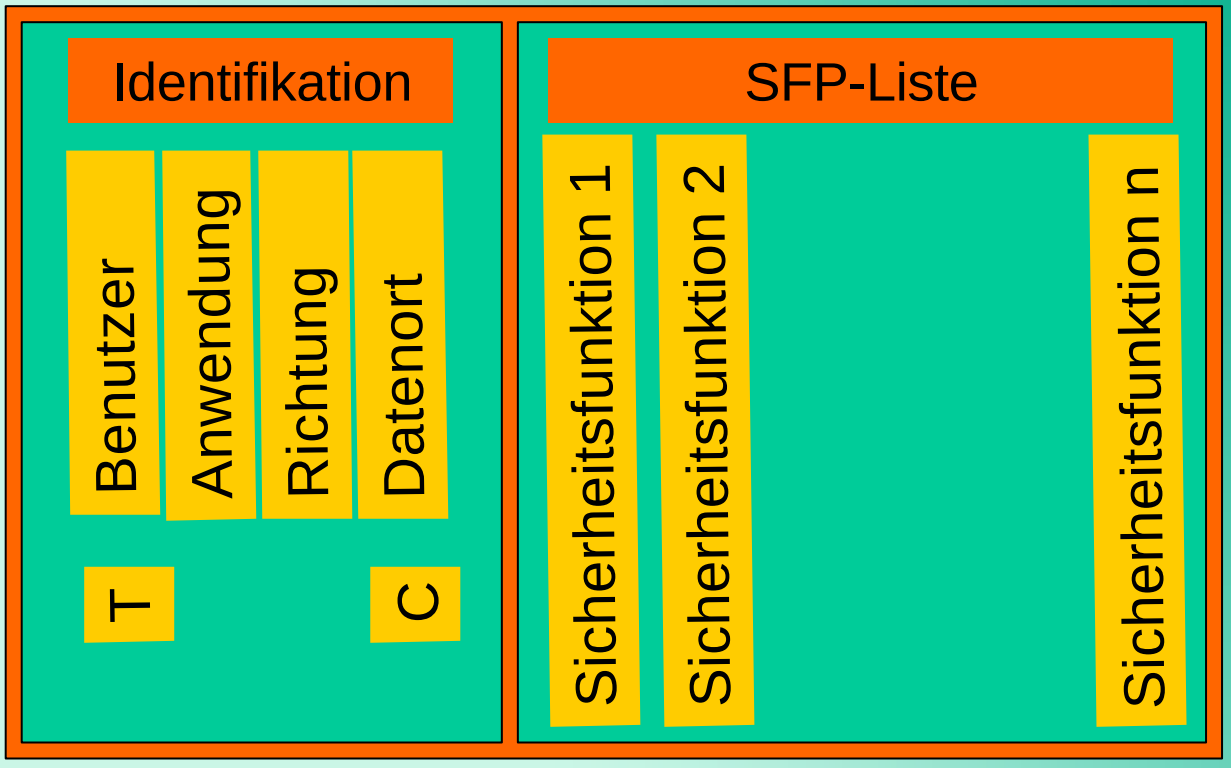
Discretionary Information Flow Control

2. Zulässigkeitsprüfung durch Security Attribute

Category	***Attribute***	***Values***
Object O	Control status C(O)	strong / weak
Subject S	Security level L(S)	high / low

- T=1 „Vertrauenswürdiges Subjekt“
  - Das vertrauenswürdige Subjekt darf Informationen von kontrollierten Datenorten an unkontrollierte Datenorte weiter leiten.
- BISS kontrolliert nur die Datenorte, die in der Informationsflussliste genannt sind

3. Schutz des Informationsflusses durch regelbasierte IT-Sicherheit



Informationsflussregeln als Konzept zur Umsetzung eines Konzeptes

- BISS dient als Rahmen zur Umsetzung des Sicherheitskonzeptes des Hauses
- Abbildung des Sicherheitskonzeptes des Hauses mit Hilfe der IF-Regeln
- Umsetzung des Konzeptes durch die IT
- Mächtigkeit der Regeln nur abhängig von der angebotenen Funktionalitätsvielfalt

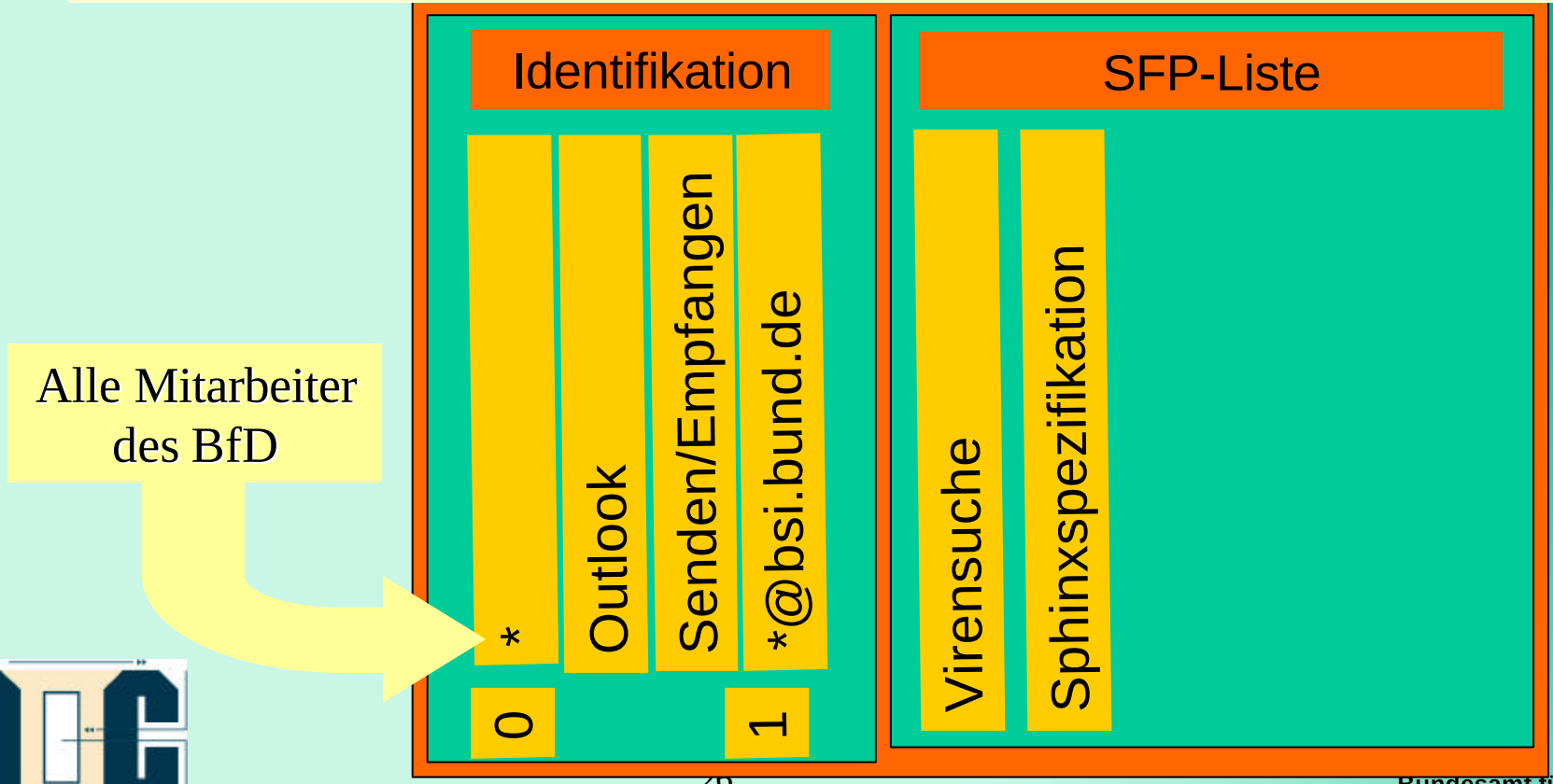
Discretionary Information Flow Control

Einige umsetzbare Konzepte mit BISS

- Anforderungen des Datenschutzes
- Sicherheitsphilosophien/-prinzipien des Anwenders/der Firma
  - wer darf was
  - in welcher Reihenfolge
  - Erleichterung durch Automatisierung von regelmäßigen Abläufen
- Unterbindung des Versendens schutzbedürftiger Informationen an unbefugte Empfänger

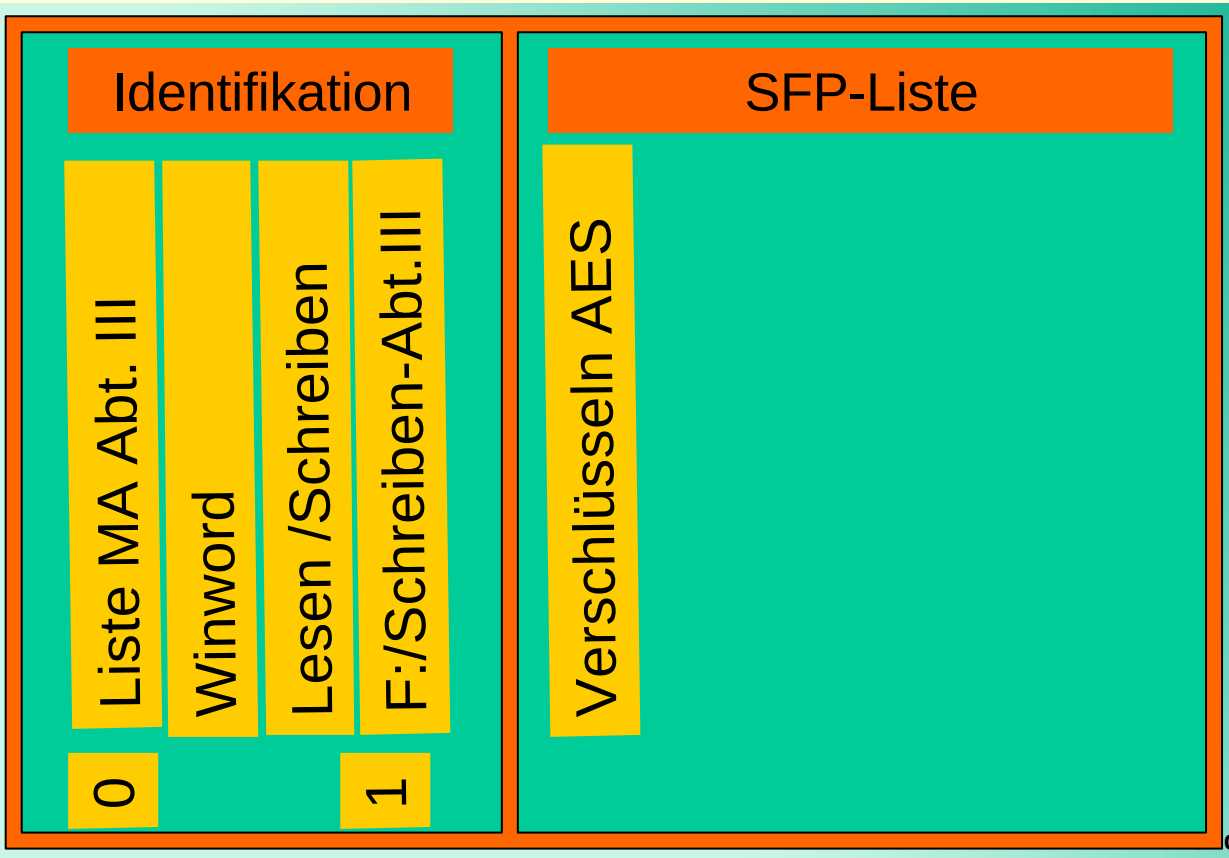
Regelbasierte IT-Sicherheit

- **Beispiel 1:** BfD kommuniziert nur noch verschlüsselt mit BSI, ferner sollen alle Emails auf Viren geprüft werden



Regelbasierte IT-Sicherheit

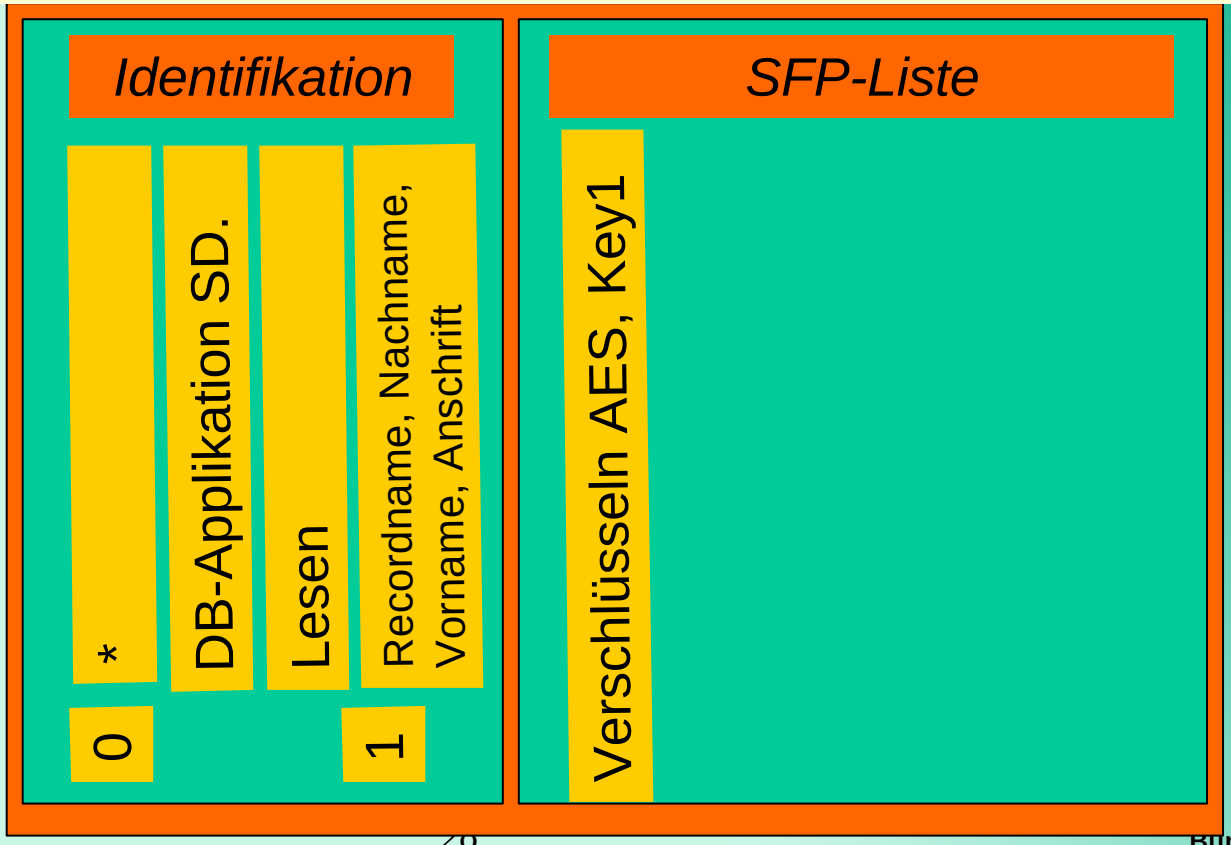
- **Beispiel 2:** alle Schreiben der Abteilung III sollen nur mit Winword bearbeitbar sein und nur für Abt. III bearbeitbar sein



Discretionary Information Flow Control

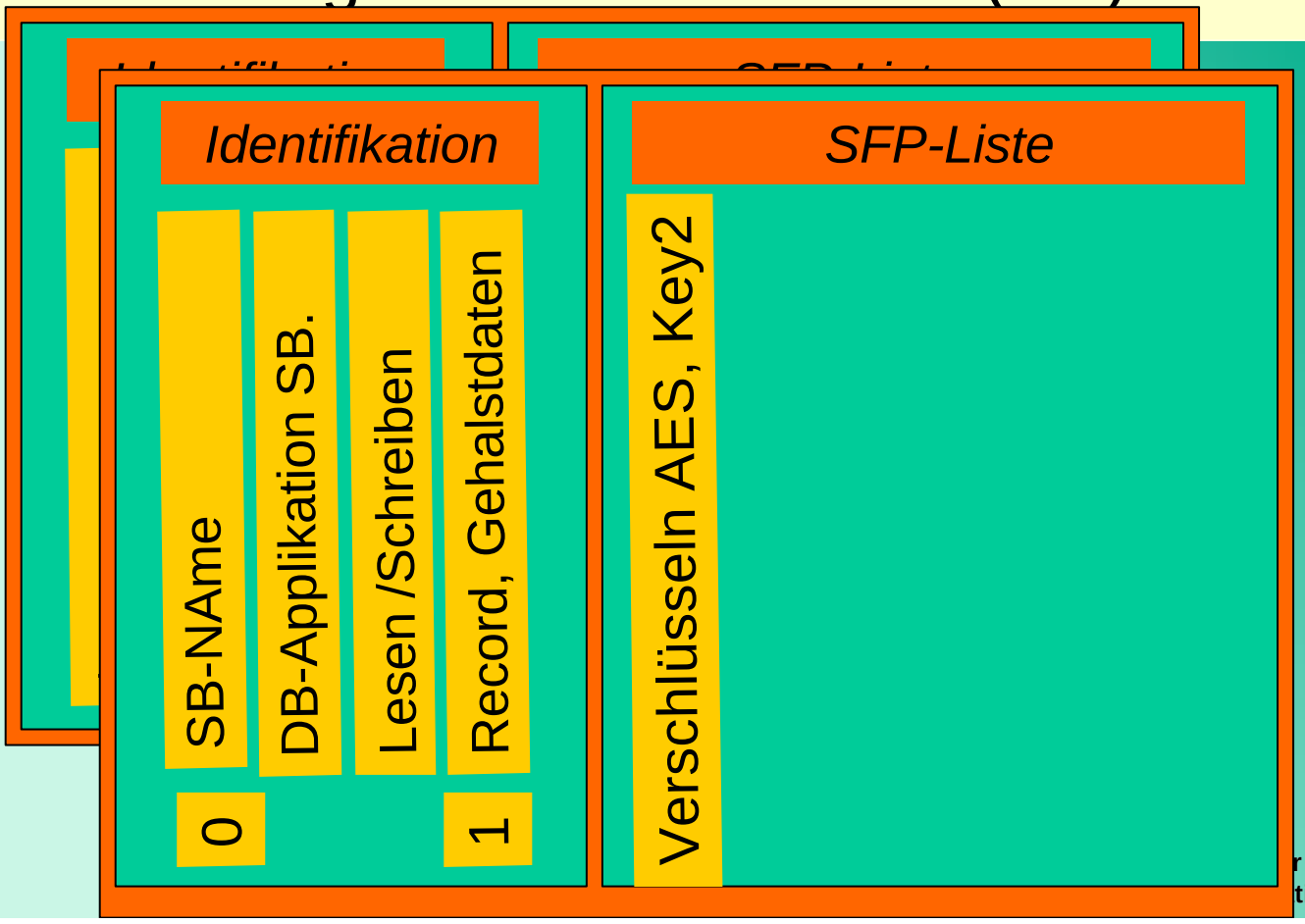
Regelbasierte IT-Sicherheit

- **Beispiel 3:** Stammdaten (SD) der Datenbank sind von allen IT-Anwendern bearbeitbar, andere Felder nur für den zuständigen Sachbearbeiter



Regelbasierte IT-Sicherheit

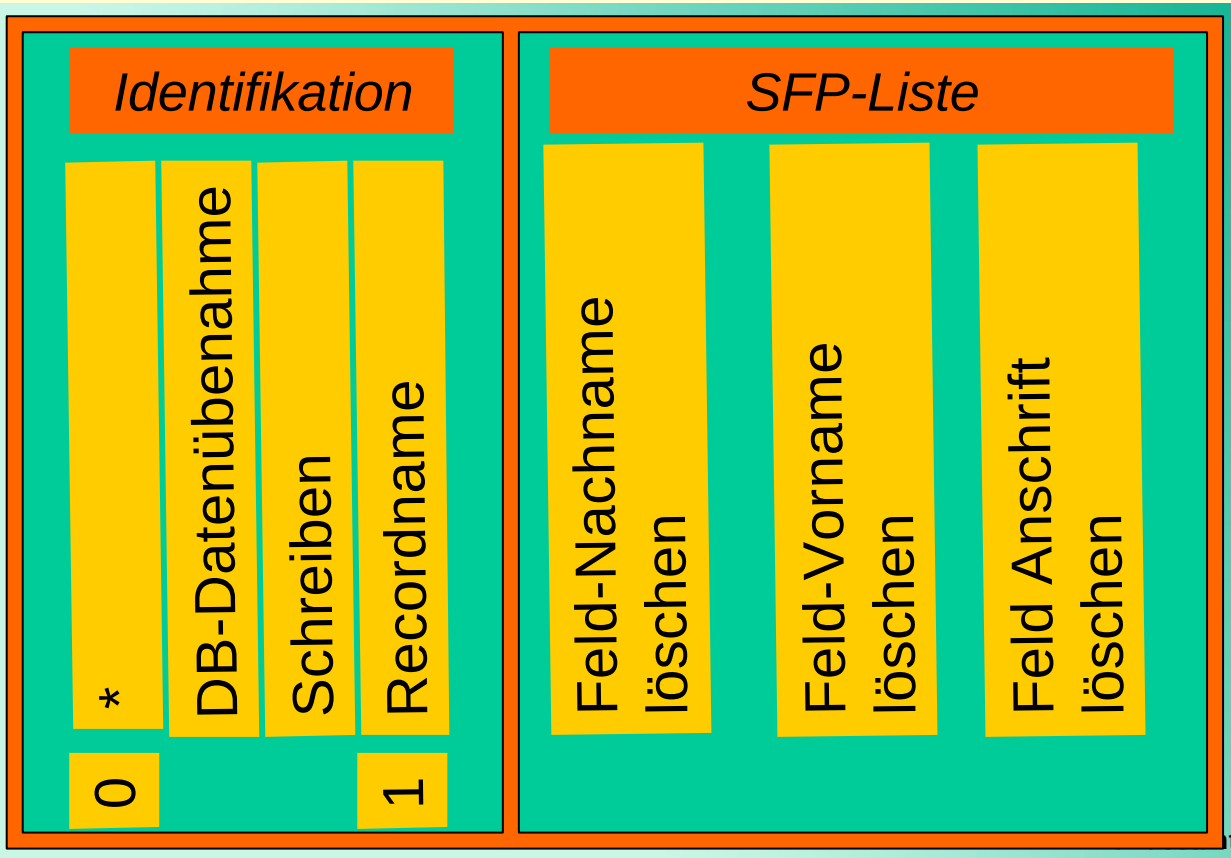
- **Fortsetzung 3:** Stammdaten (SD) der Datenbank sind von allen IT-Anwendern bearbeitbar, andere Felder nur für den zuständigen Sachbearbeiter (SB)



Discretionary Information Flow Control

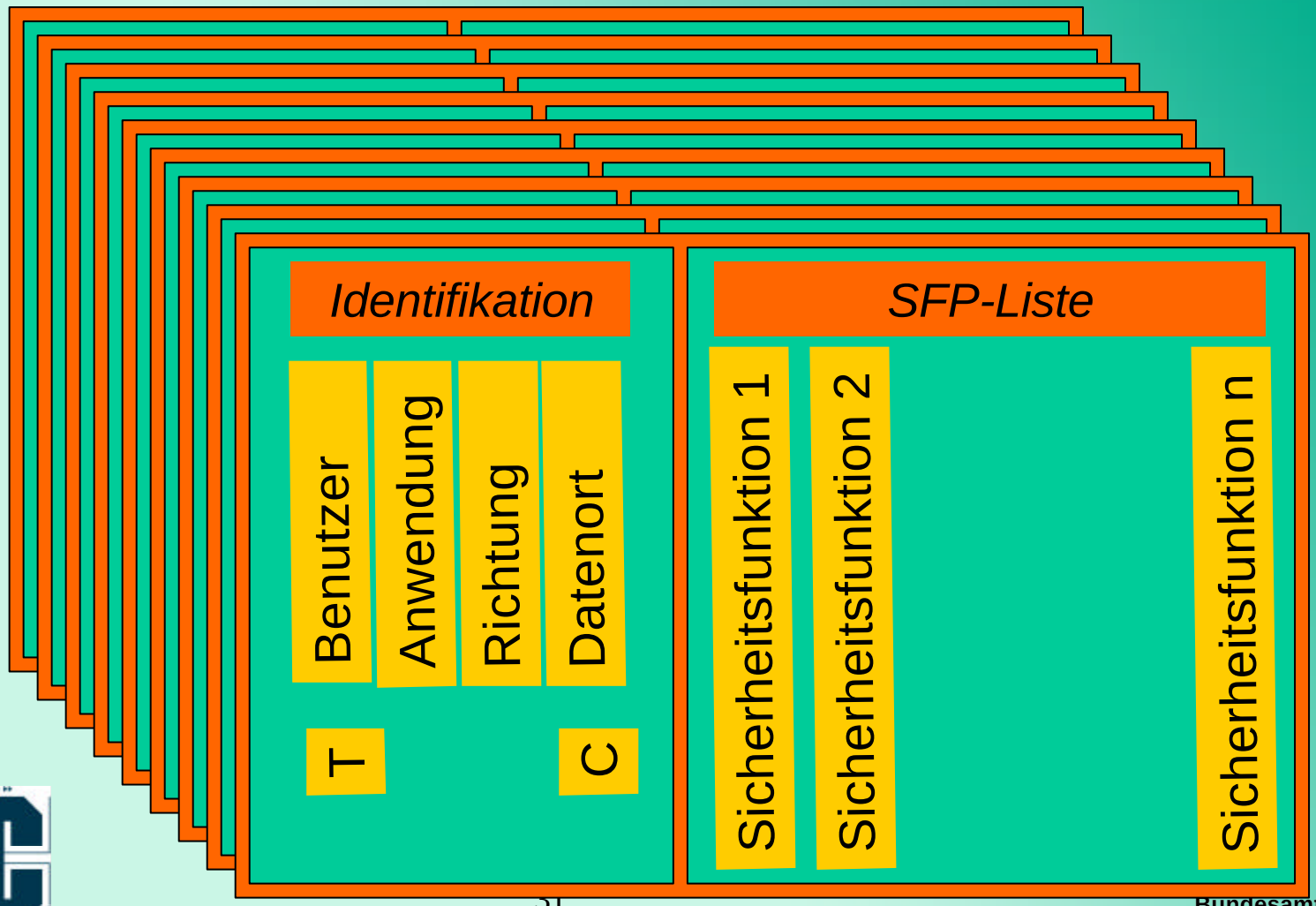
Regelbasierte IT-Sicherheit

- **Beispiel 4: Datenreduzierung** bei Datenübernahme um Stammdaten (etwa für statistische Auswertungen)



Discretionary Information Flow Control

Basis für regelbasierte Sicherheit: Die Informationsflussregel-Liste



DIC
Discretionary Information Flow Control

Konzepte

- Kontrolle von Informationsflüssen
  - Verbleib innerhalb kontrollierter Bereiche
  - Gewährleistung zweckgebundener Verarbeitung
    - Daten dürfen nur zu dem Zweck erhoben, verarbeitet oder genutzt werden, zu dessen Erfüllung sie bestimmt sind. Es muss genau festgelegt werden, wer die Daten wie, mit welchen Hilfsmitteln, in welchen Abständen und zu welchen Zwecken auswerten darf.
- Schutz von Informationsflüssen
  - Vertraulichkeit, Integrität, Authentizität, ...
  - Realisierung durch konfigurierbare PlugIns
- Flexible Konfiguration
  - Schrittweise Konstruktion sicherer Netzwerke

Oberste Zielsetzung: Benutzerfreundlichkeit

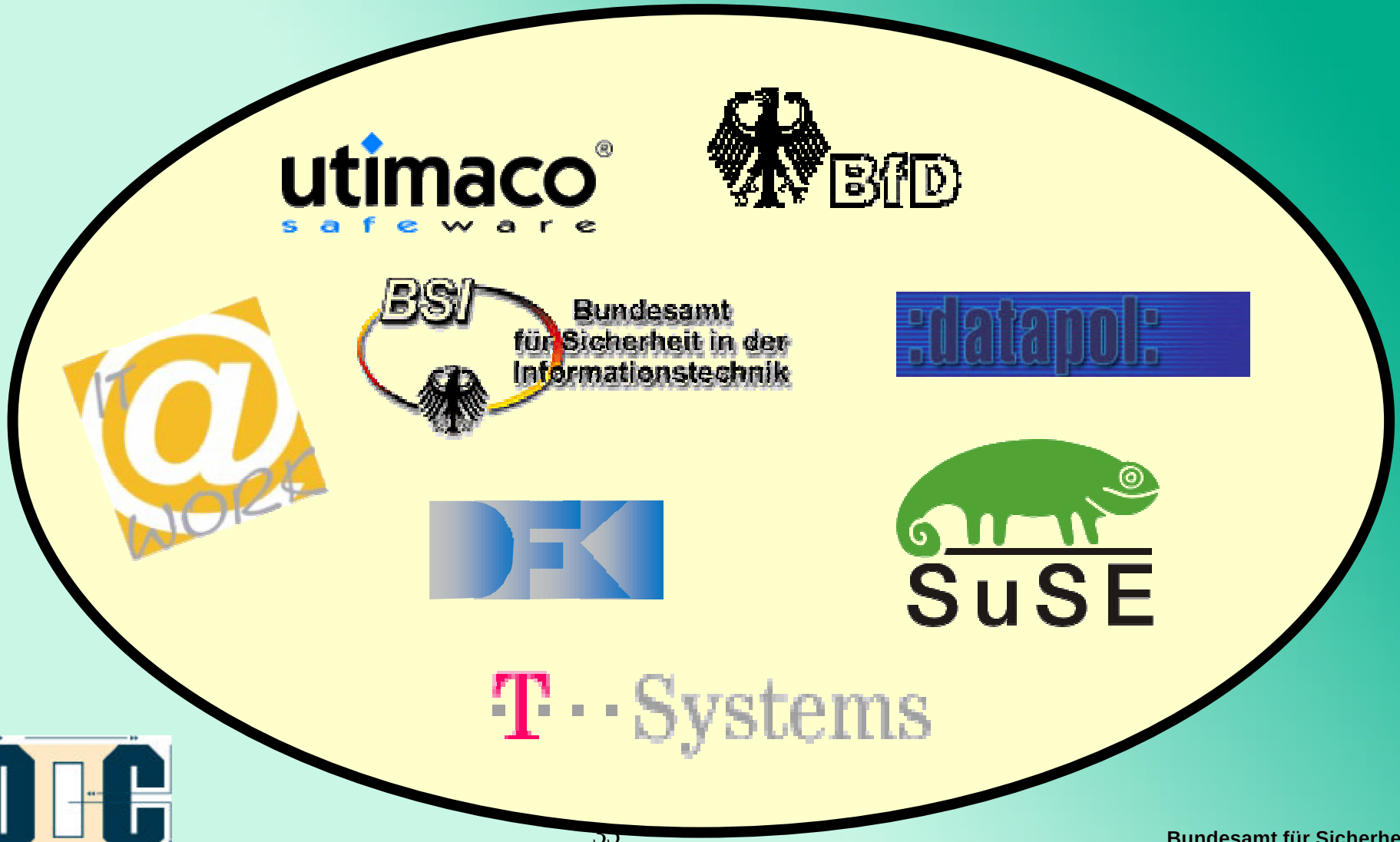
- Kompromisslose Orientierung an der dem IT-Nutzer bekannten Schnittstelle: der Applikation
  - Nur aus dieser Perspektive sind die Informationswerte bekannt
- Gleichartige Administrationsoberfläche verschiedener Sicherheitstechniken
  - Umsetzung der Sicherheitsleistung kann technisch völlig unterschiedlich sein

Discretionary Information Flow Control

Status

- Fertigstellung: 4. Sept. 2002
- Zertifizierung: 27. Sept. 2002
- Registrierung (http://www.bsi.bund.de/)
  - BSI-PP-0007-2002
  - BSI-PP-0008-2002
- Überreichung der Zertifikate an den Bundesbeauftragten für den Datenschutz: 12. Nov. 2002

Beteiligte Partner



Wer kann von BISS profitieren?

- E-Government
  - Steuererklärung, Antragswesen, ...
- Gesundheitswesen
  - Patientenakte, Telemedizin, ...
- Telekommunikation
  - Mobile Dienste, Personalisierung, ...
- Private Finance
  - Versicherungs-, Bankdienstleistungen, ...

Einige konkrete Anforderungen des BISS-PP´s

- Eine Informationsflussregel besteht aus
  - einem Operator (read/write)
  - einer Menge von Subjekten
  - einer Menge von Datenorten
  - einem Control Flag CF
  - einem Trust Flag TF
  - einem Protocol Flag PF
  - einer Liste von Informationsflussvorschriften

Security Principles

(P1) Protokollierung

(P2) Datensicherheit

(P3) Zweckbindung

(P4) Informationsflusskontrolle

(P5) Benutzerbestimmbarkeit

(P1) Protokollierung

Entscheidungen über die Erlaubnis bzw. Verweigerung von Informationsflüssen werden protokolliert, wenn dies gemäß der Informationsflussregeln erforderlich ist.

- Rückkopplung für den EVG-Administrator
- Revisionsfähigkeit erst mit Zusatzanforderungen

(P2) Datensicherheit

Erlaubte Informationsflüsse finden immer in Übereinstimmung mit den in den Informationsflussregeln genannten Informationsflussvorschriften statt.

- Verschlüsselte Aufbewahrung
- Verschlüsselte Übertragung
- Signierte Übertragung
- Algorithmen: AES, 3DES, RSA, SHA-1
- Kompatibilität zu SPHINX
- Offen für weitere Funktionen (wie Datenvermeidung, Pseudonymisierung usw.)

Discretionary Information Flow Control

(P3) Zweckbindung

Ist der Kontrollstatus eines Objektes C(O) = strong, so werden die das Objekt O betreffenden Informationsflüsse nur erlaubt, falls sie von einem Subjekt S angefordert werden, welches hierzu gemäß der Informationsflussregeln autorisiert ist.

- Einschränkung der Verarbeitung
- Lose Kopplung mit Informationsflusskontrolle

(P4) Informationsflusskontrolle

Ist der Kontrollstatus eines Objektes C(O) = strong, so kann eine Information I, die vom Objekt O stammt, nicht in ein Objekt O‘ mit C(O') = weak gelangen, es sei denn, das diesen Informationsfluss auslösende Subjekt S ist gemäß der Informationsflussregeln dazu autorisiert.

- Kontrolle durch Referenzmonitor
- Einfache Informationsflusskontrolle
- Entscheidungsverantwortung beim Benutzer* für Eingabe aller Regeln (Benutzerbestimmbarkeit)

*Benutzer im Sinne von verantwortlichem IT-Betreiber

(P5) Benutzerbestimmbarkeit

Alle IF-Regeln werden vom Benutzer (mindestens EVG-Administrator) vorgegeben. Als Ausnahme zu Prinzip (P4 – Informationsflusskontrolle) kann mind. der EVG-Administrator den Informationsfluss explizit autorisieren, d.h. eine Information I, die von einem Objekt O mit C(O) = strong stammt, kann dann in ein Objekt O' mit C(O') = weak gelangen.

- Entscheidungsverantwortung beim Benutzer* - auch für Außerkraftsetzung von Regeln
- Erweiterbar um Rechte für andere Benutzer**

*Benutzer: verantwortlicher IT-Betreiber
** andere Benutzer: delegieren von Verantwortlichkeiten

Security Characteristics

Auswahlfunktion liefert	keine Regel	Regel R für den Datenort	
Objekt hat Kontrollstatus		weak	strong
Subjekt S wird in Regel R			genannt / nicht genannt
read	GO	GO P1 P2	GO P1 P2 P3 / STOP P1 P2 P3

Security Characteristics

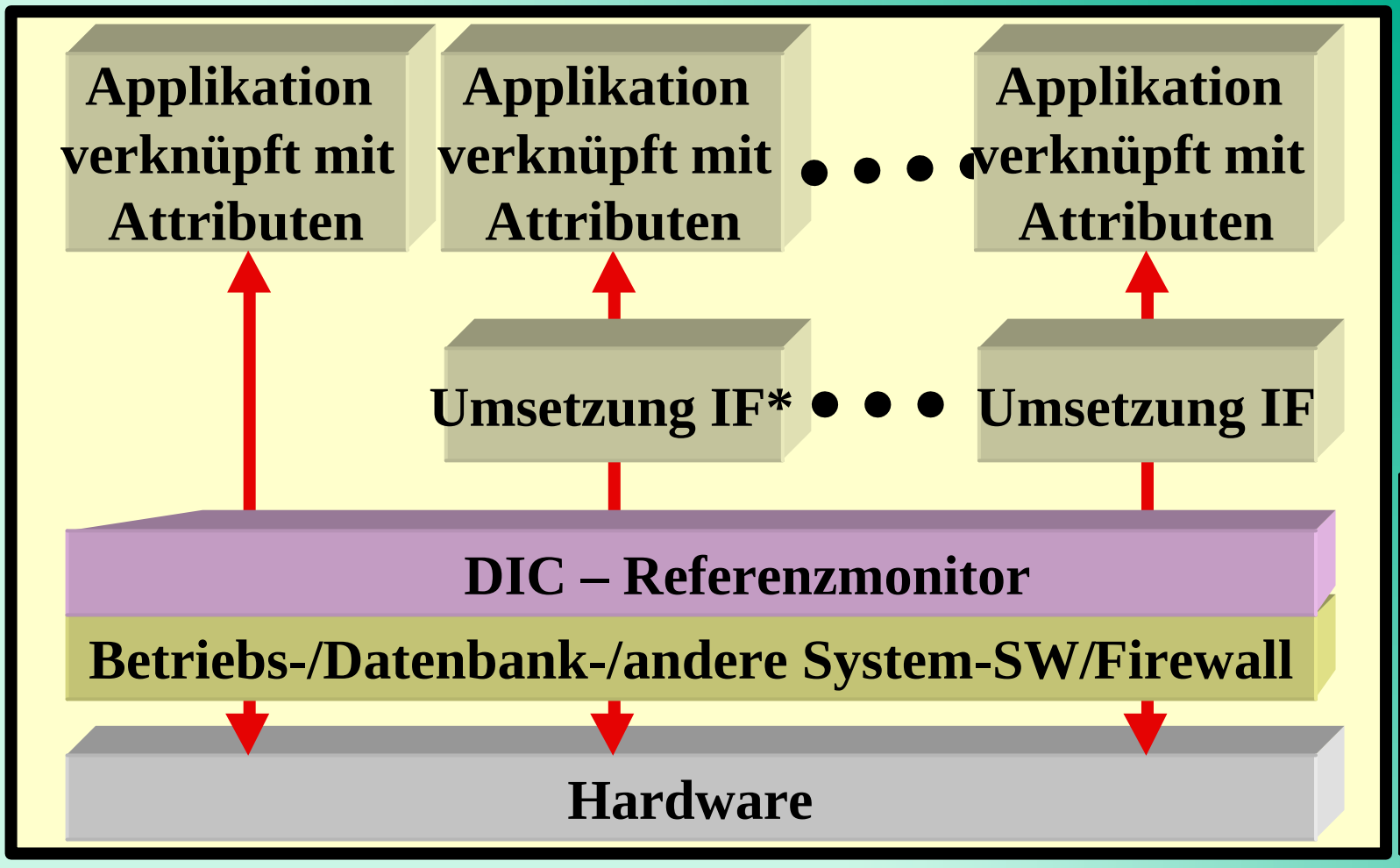
Auswahlfunktion liefert		keine Regel	Regel R für den Datenort		
Objekt hat Kontrollstatus			weak	strong	
Subjekt S wird in Regel R				genannt	nicht genannt
read		GO	GO P1 P2	GO P1 P2 P3	STOP P1 P2 P3
write	L(S) = low	GO P4	GO P1 P2 P4	GO P1 P2 P3	STOP P1 P2 P3

Discretionary Information Flow Control

Security Characteristics

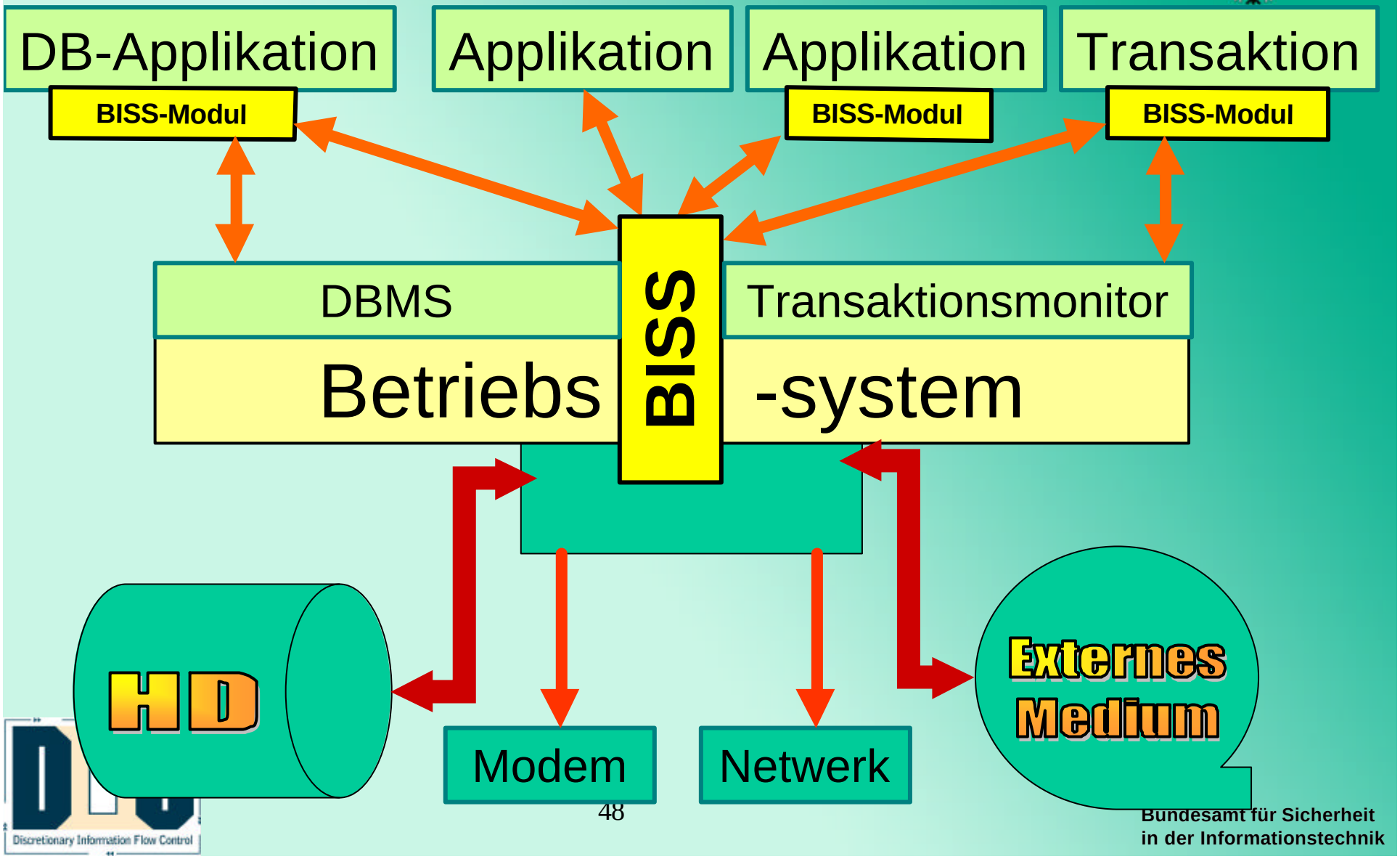
Auswahlfunktion liefert		keine Regel	Regel R für den Datenort		
Objekt hat Kontrollstatus			weak	strong	
Subjekt S wird in Regel R				genannt	nicht genannt
read		GO	GO P1 P2	GO P1 P2 P3	STOP P1 P2 P3
write	L(S) = low	GO P4	GO P1 P2 P4	GO P1 P2 P3	STOP P1 P2 P3
	L(S) = high	STOP P4 P5	STOP P1 P4 P5	GO P1 P2 P3	STOP P1 P2 P3

Struktur



*IF=Informationsflussregel

Wie kann BISS realisiert werden?



BISS-Integration in bestehende Systeme möglich

- Vorhandene Sicherheitstechniken anderer Systeme sind weiterhin nutzbar
- BISS kann diese ersetzen und ermöglicht zusätzliche Sicherheitspolitiken
- Widersprüche in der Administration nur möglich, wenn in BISS entsprechende Plausibilitätsprüfungen vorhanden sind
- Sicherheitsfunktionen anderer Systeme sind u.U. von BISS nutzbar

Qualitative Mindestanforderung der BISS-Schutzprofile

- Stufe der Vertrauenswürdigkeit: EAL2
  - Augmentierung zur Verbesserung der Sicherheit der Administration
  - Schutz gegen geringes Angriffspotential
- Zwei Varianten
  - Single-user Umgebung (SU)
  - Multi-user Umgebung (MU)

Einige Perspektiven zur Weiterentwicklung von BISS

Discretionary Information Flow Control

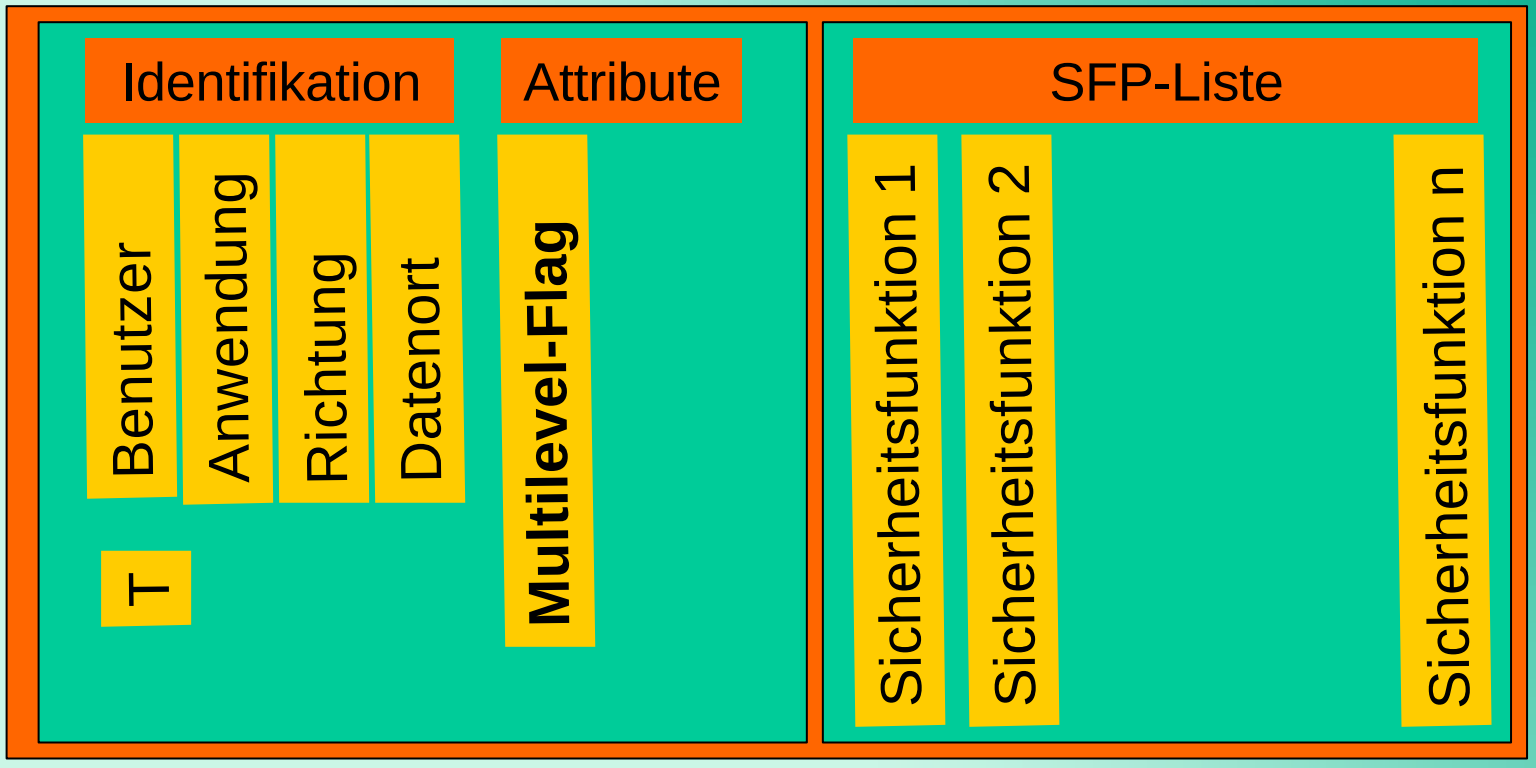
Perspektiven
Höhere Vertrauenswürdigkeitsstufen

- EAL2 in BISS-PP gefordert
- bis EAL4 möglich, wenn...
  - entsprechende Implementierung
    - höherwertige Schwachstellenanalyse
  - weitere unterstützende Sicherheitsfunktionalität
    - Authentifizierung der Applikationen
- bis EAL7 möglich, wenn...
  - wenn Konzept formales Sicherheitsmodell erfüllt
  - Entwicklungsspezifikation teilweise formal ist

Perspektiven: Multilevel-Security

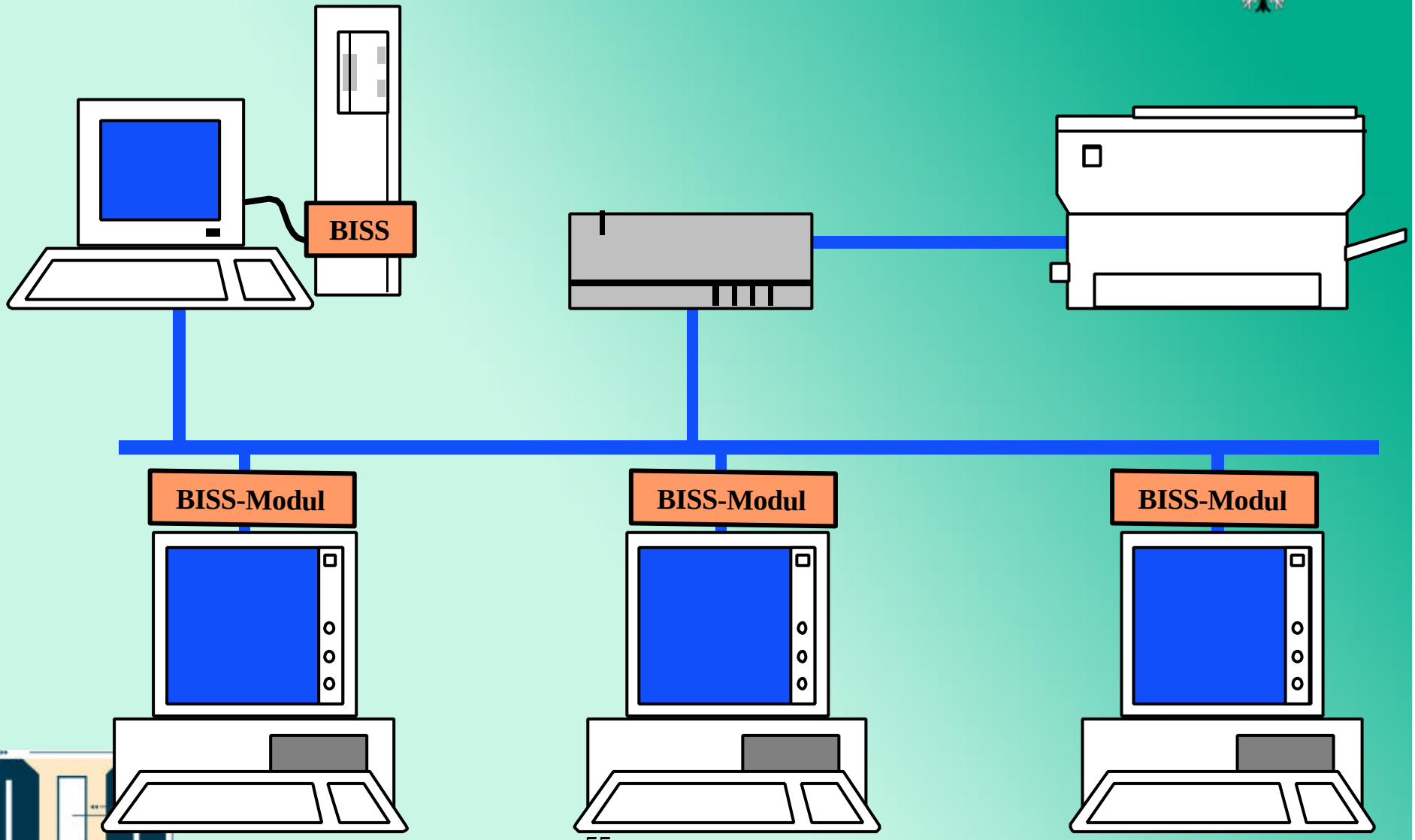
- Das „C“-Flag kann zu einem Sicherheitslevel erweitert werden
  - Repräsentation einer Vertraulichkeitsstufe (Vertraulich, Geheim, Streng geheim)
- Sicherheitslevel vererbbar - auch bei Interprozesskommunikation
- Aufrechthaltung des Sicherheitslevels über unterschiedliche Sicherheitstechniken

Perspektiven: Multilevel-Security

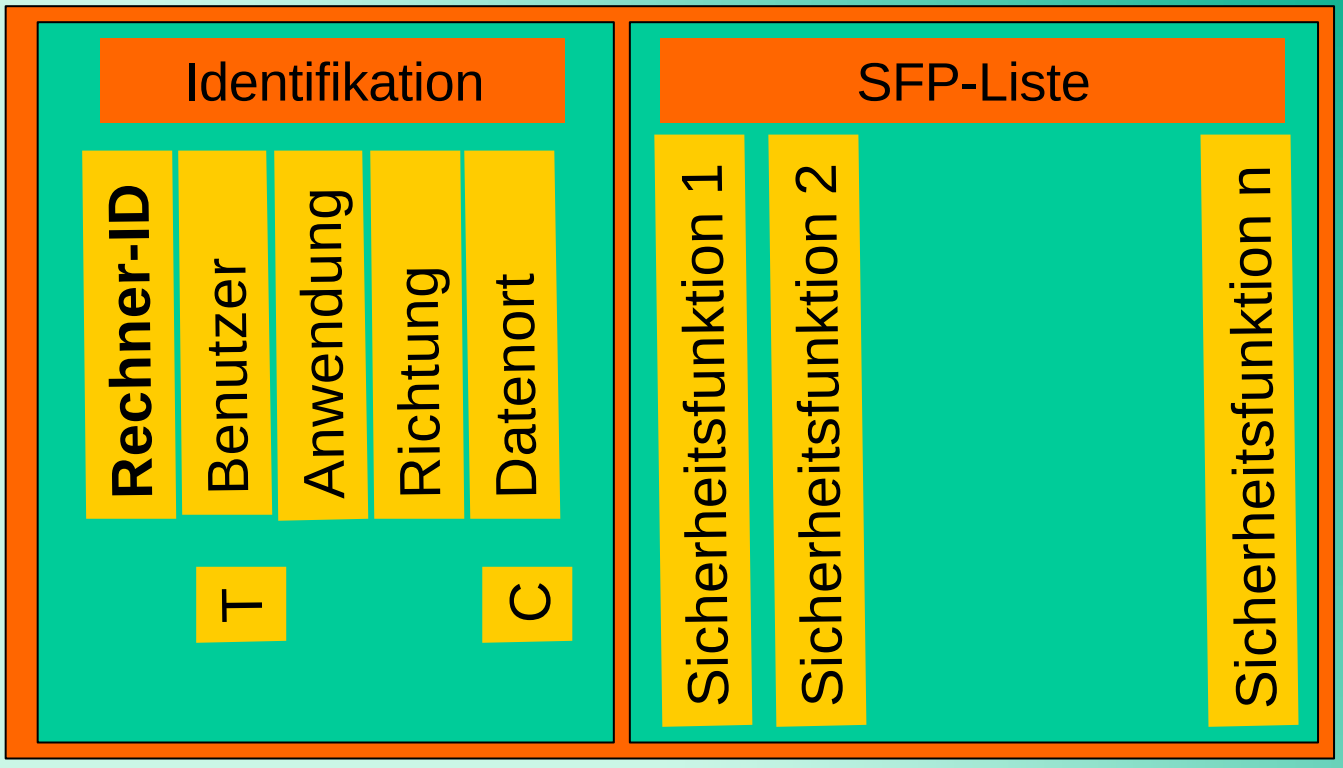


DIG Discretionary Information Flow Control

Perspektiven:
BISS in verteilten Systemen



Perspektiven:
BISS in verteilten Systemen



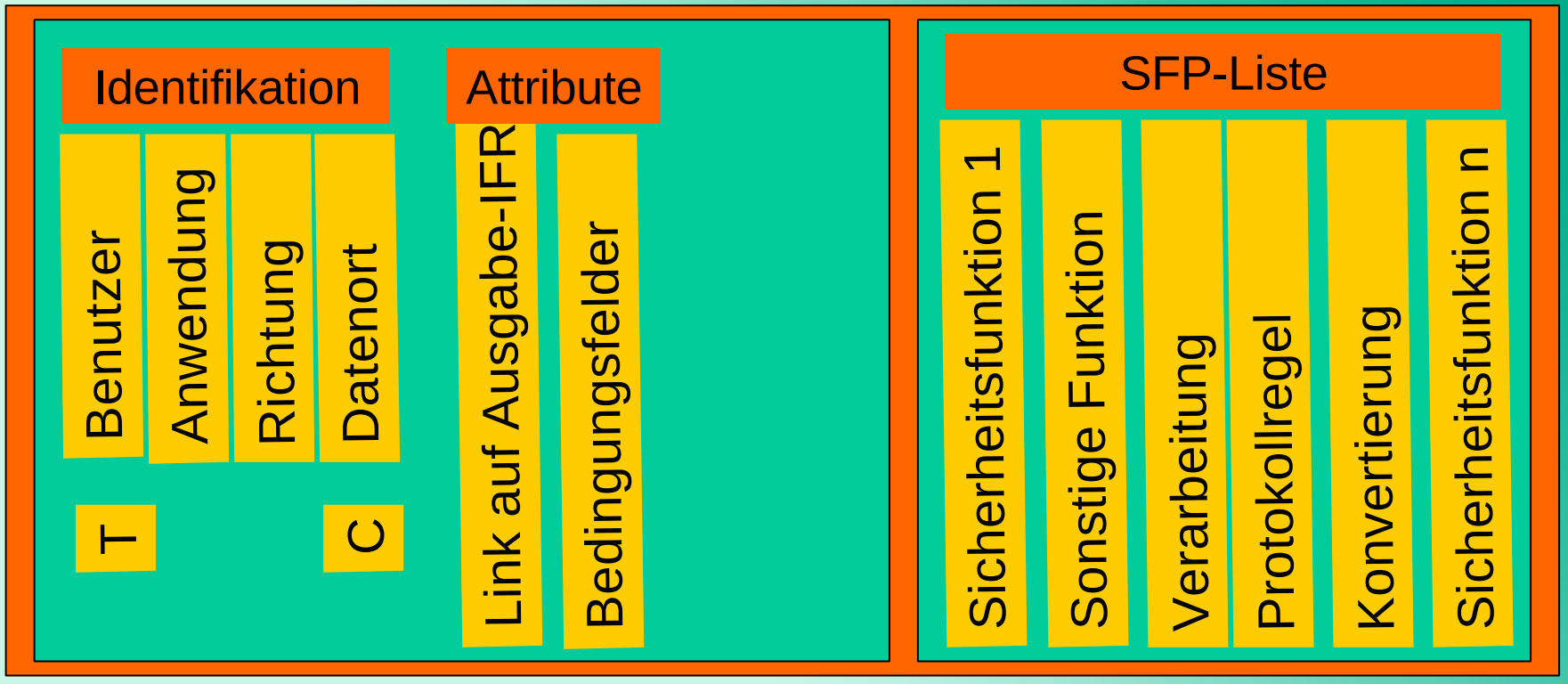
Perspektiven Workflow-Sicherheit

Unterstützung von Workfloweigenschaften

- Prozessattribut wird zur vollständigen Informationsflussregel erweitert
- Dynamisierung von IF-Regeln durch Regeltabelle
  - Einhaltung definierter Geschäftprozesse wird erzwungen
  - ermöglicht die Vorgangskontrolle

Erweiterung des Begriffes auf regelbasierte Informationsflusssteuerung

Perspektiven
Workflow-Sicherheit

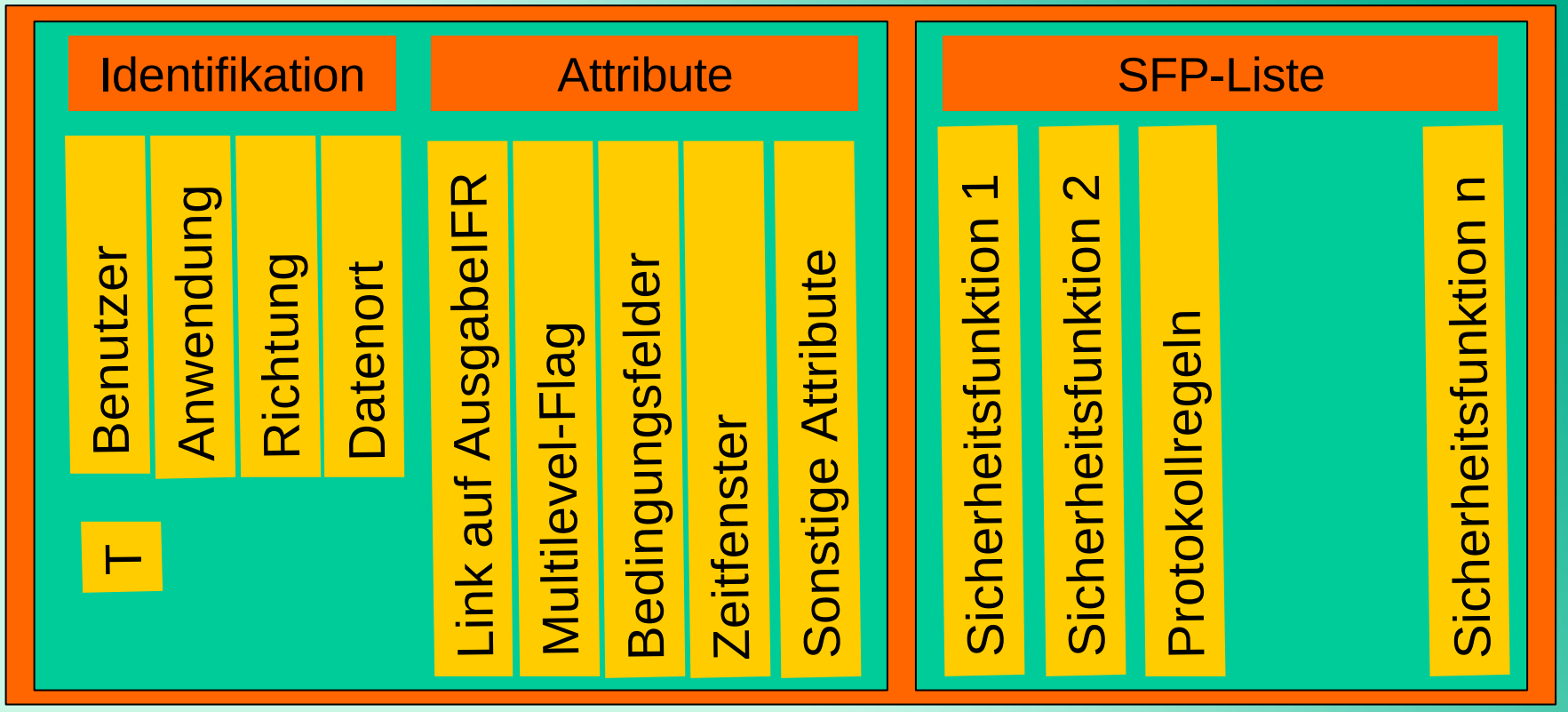


Discretionary Information Flow Control

Perspektiven
weitere Attribute gemäß Anwenderbedarf

- Attribut „Bedingungsfeld“
  - ermöglicht zusätzliche Berechtigungsprüfung anhand sonstiger Bedingungen
    - Beispiel: Unterschriftsberechtigung bis zu bestimmten Grenzwerten
- Attribut „Zeitangabe“
  - ermöglicht Angabe von Gültigkeitsbereichen
    - ermöglicht automatisiertes Löschen nach gesetzlichen Vorgaben
    - verhindert Arbeiten mit ungültigen Informationen
  - ermöglicht Priorisierung zur Termineinhaltung
- usw.

Perspektiven
weitere Attribute gemäß Anwenderbedarf



Discretionary Information Flow Control

Perspektive
Weitere Variante von BISS:
nur regelbasierte Informationsflüsse erlaubt

- erlaubt Informationsflüsse ausschließlich gemäß IF-Regeln (hohe Sicherheit)
  - Alle nicht definierten IF werden unterbunden
- Sicherheitsfunktionalität frei gestaltbar
  - dadurch ist TPM-konforme BISS-Lösung realisierbar

Discretionary Information Flow Control

Trusted Platform Module TPM und BISS

(TCPA=Trusted Computing Platform Allianz)

TPM:

- Listenorientierte Dateikontrolle
  - Liste gesperrter Dateien
  - Verarbeitungsliste
  - Liste zugelassener/verbotener SW/HW
- Zugriffskontrolle nur dateiorientiert
- Schutz vor Softwarepiraterie
- Schutz vor Viren/Würmern durch Schutz der Software
- Realisierung vorgegeben
  - Externe SRL, DRL und HCL-Server kontrollieren PC
- Entweder TPM oder nicht
- Alle müssen TPM konform sein

BISS-Konzept:

- Informationsflusskontrolle
  - Objekttyp offen (Datei, Feld, ...)
- Datenflussssicherheit parametrisiert
- Zweckbindung für alle Objekttypen
  - Wahrung von Geschäftsprozessen
- Sicherheitsfunktionalität erweiterbar (Virenschutz, SW-Authentisierung, ...)
- Sicherheit nur an Information gebunden
- Verarbeitungsfunktionen möglich
- Realisierung offen
- Benutzer bestimmt Umfang der Sicherheit
- Schrittweise Konstruktion sicherer Netzwerke

Anstehende Aufgaben

- Algorithmen zur Konsistenzwahrung von Regeln
- Algorithmen zum Finden der spezifischsten Regel
- PP für Multilevelsecurity (Sicherheitsmodell)
- Erstellung eines PP für LAN-Variante
- Erstellung eines PP mit VPN-Funktion
- Funktionale Spezifikation und Grobarchitektur für Open Source Implementierung
- Prototyprealisierungen
- Strategien zur Marktakzeptanz
- verschiedene Grundlagenarbeiten wie
  - BISS mit herkömmlichen Sicherheitstechniken
  - Vorteile- Nachteile- Grenzen dieser Architektur

Zusammenfassung

- Regelbasierte Informationsflusssteuerung ist das Modell einer neuen Sicherheitsarchitektur
- Die vorliegenden Schutzprofile sind nur eine erste Instantiierung dieser Architektur
- Wesentlichste Merkmale dieser Architekur sind:
  - die Sicherheit ist regelbasiert
  - Sicherheitsattribute werden mit den Prozessen verknüpft
  - Sicherheit wird über Sytemgrenzen hinweg gewahrt
  - Einheitliche Administrationsoberfläche für alle Systeme (Betriebssystem, Datenbank, Firewall usw.)
  - regelbasierter Ansatz ist auch für automatisierte Verarbeitungsabläufe nutzbar
  - BISS ist in bestehende Systeme integrierbar

Common Criteria Schutzprofil

Benutzerbestimmbare Informationsflusssicherheit BISS / DIC

Vielen Dank für Ihre Aufmerksamkeit

Bundesamt für Sicherheit in der Informationstechnik

Marcel.Weinand@bsi.bund.de
Tel.: 018889582-152

http://www.bsi.bund.de/zertifiz
http://www.commoncriteria.org