MakoSi

Management komplexer Sicherheitsmechanismen

MakoSi

MakoSi - Projektpartner

- **FhG IGD Darmstadt**
  Fraunhofer Institut für Graphische Datenverarbeitung
- **FhG IPK Berlin**
  Fraunhofer Institut für Produktionsanlagen und Konstruktionstechnik
- **FhG SIT Darmstadt**
  Fraunhofer Institut für Sichere Telekooperation
- **DiK TU Darmstadt**
  Datenverarbeitung in der Konstruktion
- **ZGDV e.V. Rostock**
  Zentrum für Graphische Datenverarbeitung

Ausgangssituation

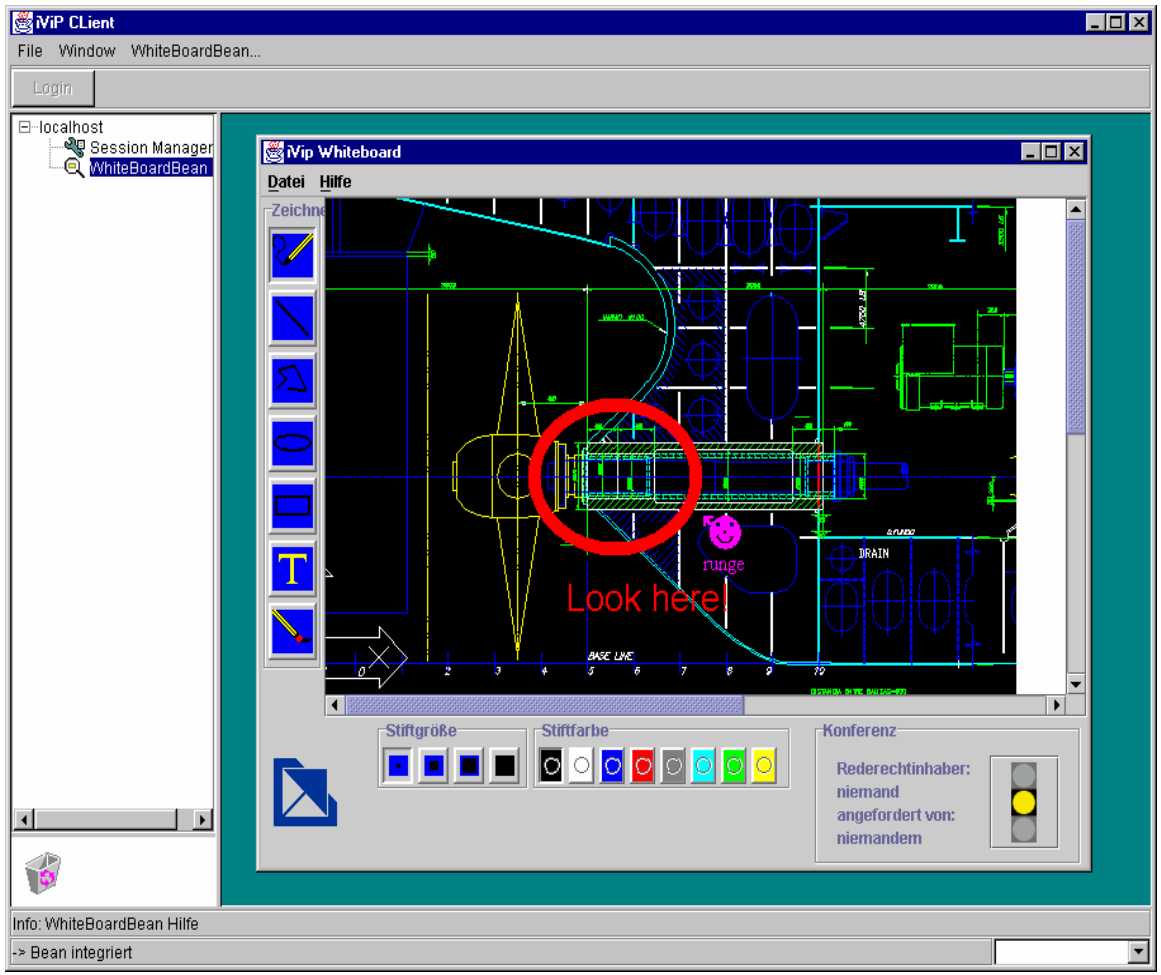
- Zunehmende Kooperation und Vernetzung von Unternehmen
- Steigendes Bedrohungs-potential beim elektronischen Informationsaustausch
- Unzureichende Nachvollziehbarkeit der Sicherheitsmaßnahmen trotz hohen Aufwands
- Fehlendes Handwerkszeug zur strukturierten Unterstützung von Sicherheitskonzepten
- Fehlende Ausdrucksmöglichkeiten **heterogener** Sicherheitsbedürfnisse

Beispielszenario: Das IVIP-Whiteboard

Verteilte Konstruktionsumgebung für Anwendungen im Automotive-Bereich

Entwickelt im Rahmen des BMBF-Leitprojektes virtuelle, integrierte Produktentstehung

Sicherheitsanforderungen von **Zulieferern** und **Automobilherstellern** sind häufig stark asymmetrisch, geprägt durch ökonomische Machtverhältnisse, Schutzrechte und Vertragsbeziehungen



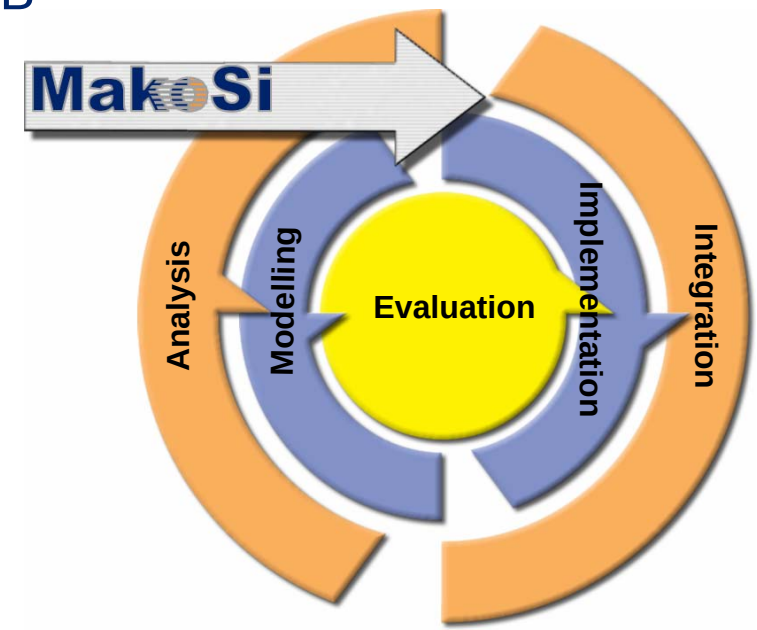
Zielstellung MakoSi

- Schutz sensitiver Daten bei der unternehmensübergreifenden Zusammenarbeit
- Geschäftsprozessorientierung, ohne Vernachlässigung der Sicherheitsrisiken
- Kompromiss zwischen IT-Sicherheit und Kosten, Performanz sowie Funktionalität und Usability
- Weitgehende Formalisierung und Automatisierung
- Berücksichtugung etablierter Standards (CC, BS77/99, Grundschutzhandbuch, ...)
- Vision: Policy Driven System

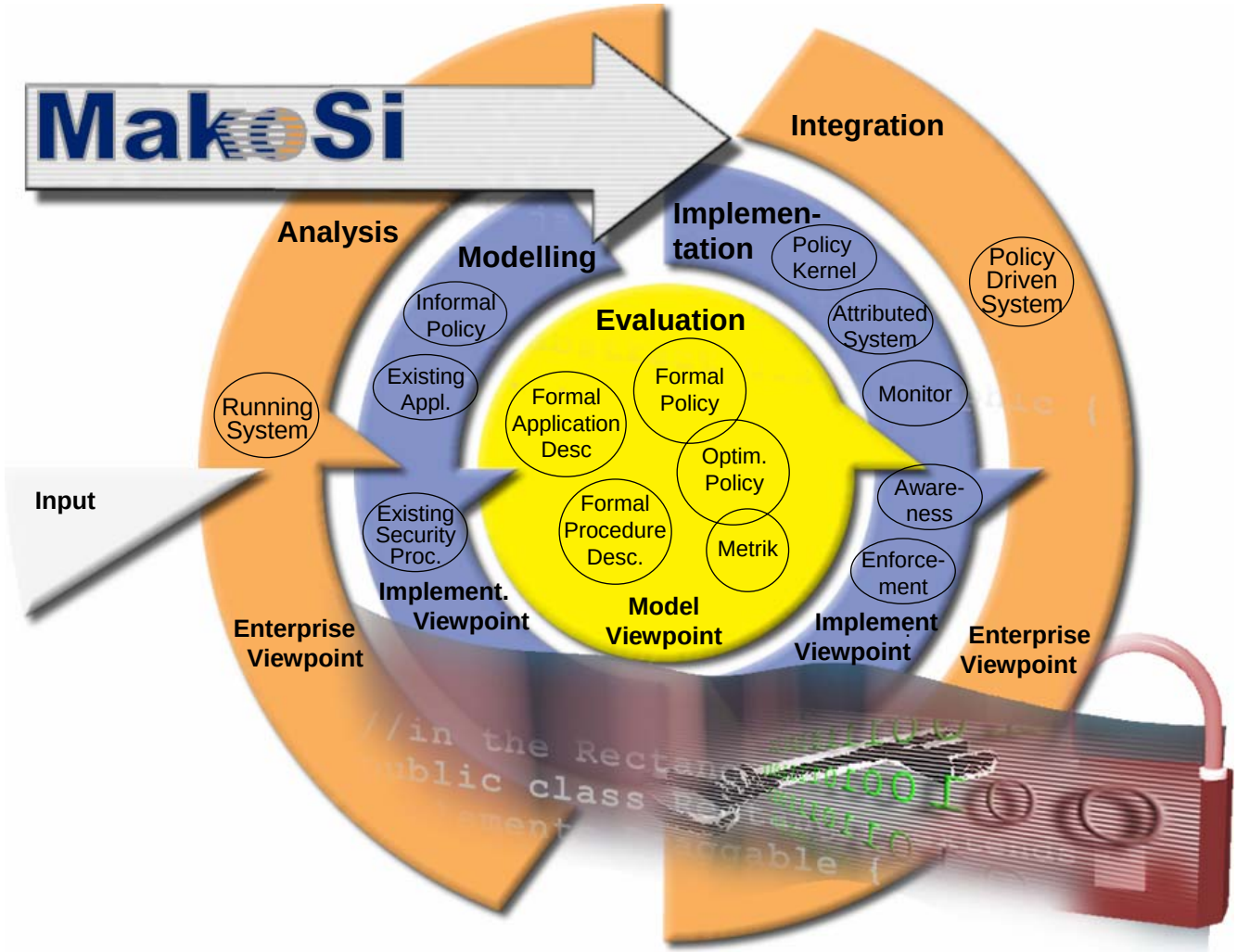
Beispiel: Sicherheitsrichtlinien nach BS 7799-2

Ansatz

- Verwendung und Integration von Security-Policies
- Gleichberechtigte Unterstützung von **Risk-Awareness** und **Security-Enforcement**
- Pilothafte Umsetzung der Konzepte am Beispiel einer Shared Whiteboard-Konferenz, dem ivip WB
- Forschung adressiert unterschiedliche Ebenen
  - Analyse von Geschäftsprozessen
  - Komponenten zur technischen Lösung
  - Evaluation am formalen Modell
- Ableitung eines mehrstufigen Vorgehensmodells zur Abdeckung des Integrationsprozesses



Der Weg zu einem „Policy Driven System“



Schwerpunkte in MakoSi

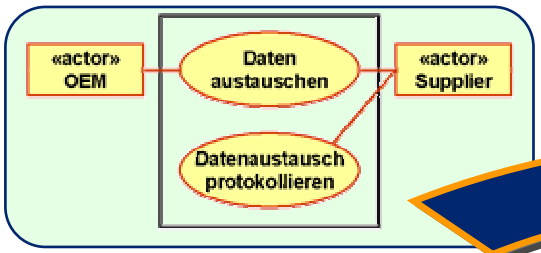
- Vorgehensmodell: nachvollziehbare Schritte von der Spezifikation bis zur Implementierung
- Datenmodell zur Beschreibung von Kooperations-systemen, das MakoSi Basis-Datenmodell (MBDM)
- Policy Enforcement auf Basis der WBEM Services von Sun und dem Common Information Model (CIM) – leicht wiederverwendbare Standardkomponenten
- Abgleich von Laufzeitinformationen, durch eigenständige Komponenten (RTI)
- Risikovermittlung beim Benutzer durch den Security-Awareness Enginge (SAE)

MakoSi-Vorgehensmodell

Das MakoSi-Vorgehensmodell zielt auf:

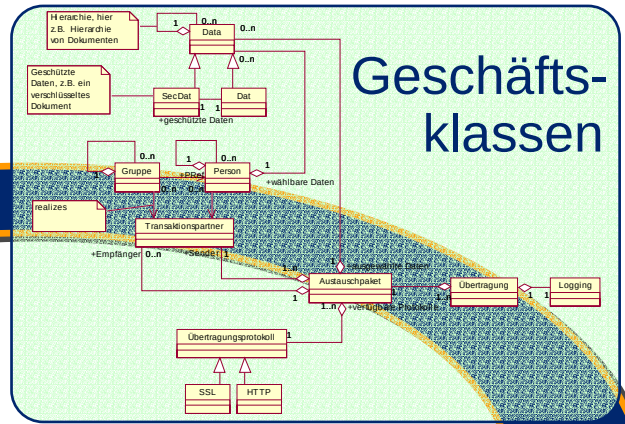
- Handhabbarer, vollständiger und fehlerfreier Vergleich von Sicherheitsrichtlinien bei Domänen-übergreifender Zusammenarbeit
- Methodenbasierte Unterstützung aller Beteiligten von der Spezifikation bis hin zur Implementierung
- Effektive, effiziente und für alle Beteiligten nachvollziehbare Implementierungen von Sicherheitsrichtlinien

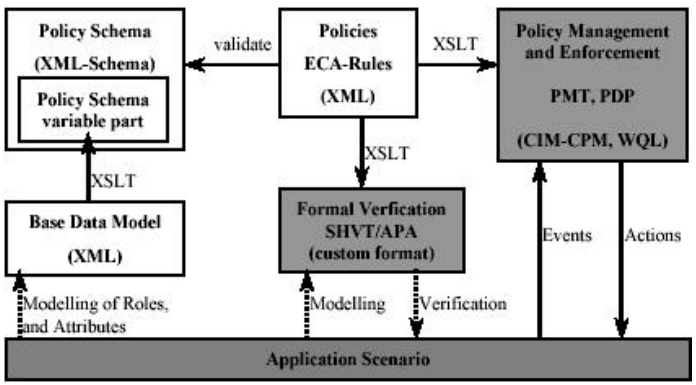
MakoSi-Vorgehensmodell



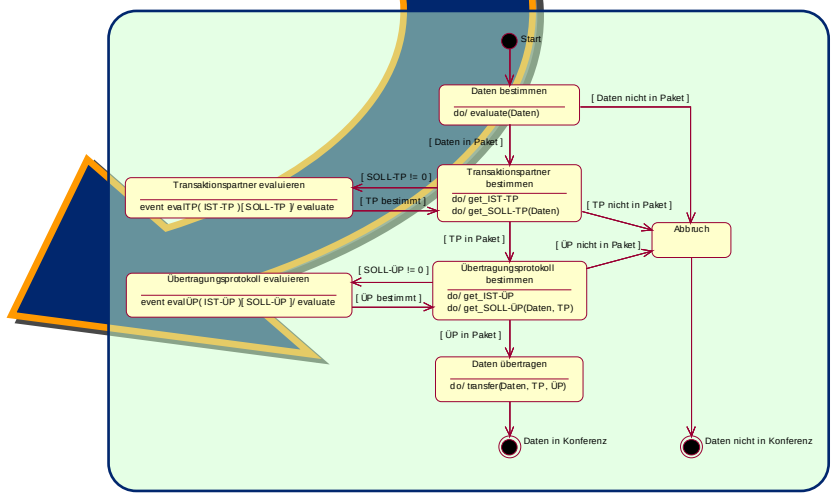
Risiko-Analyse

Verbale Spezifikation



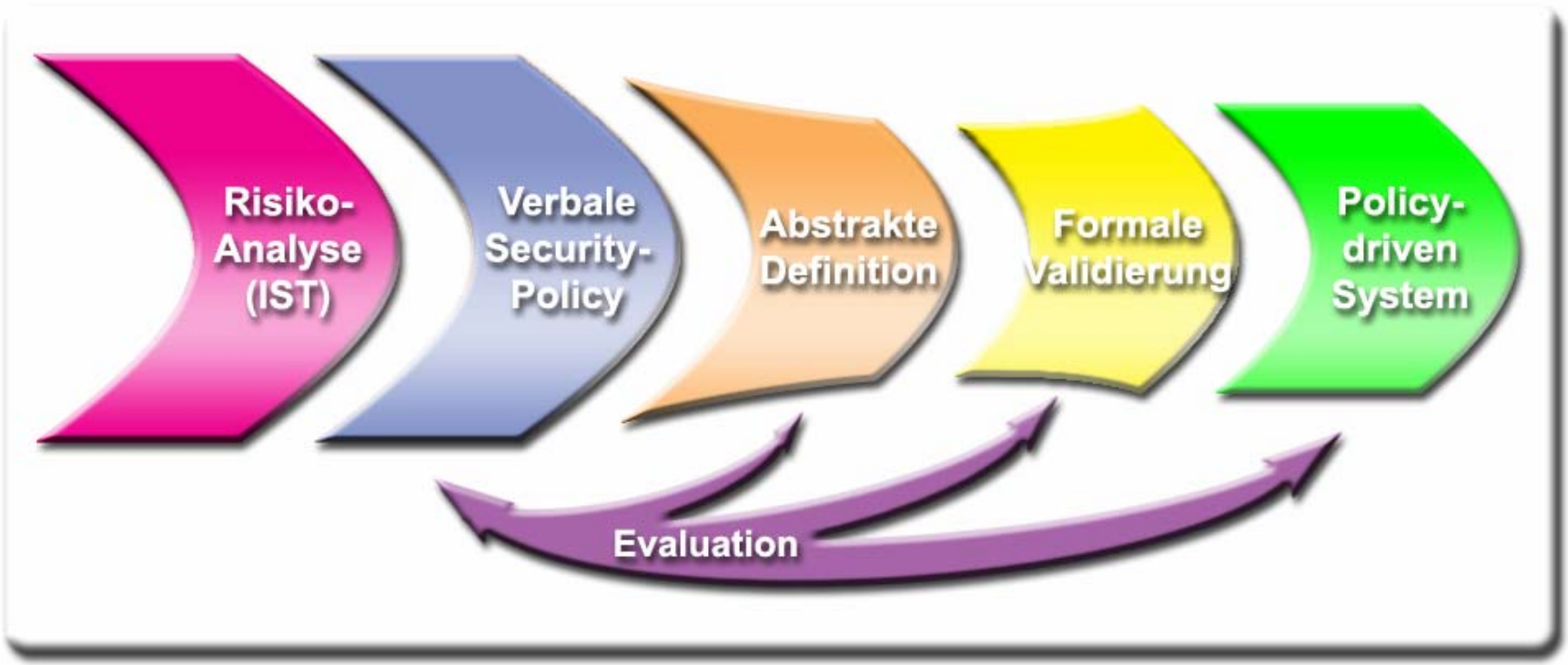


Implementierung



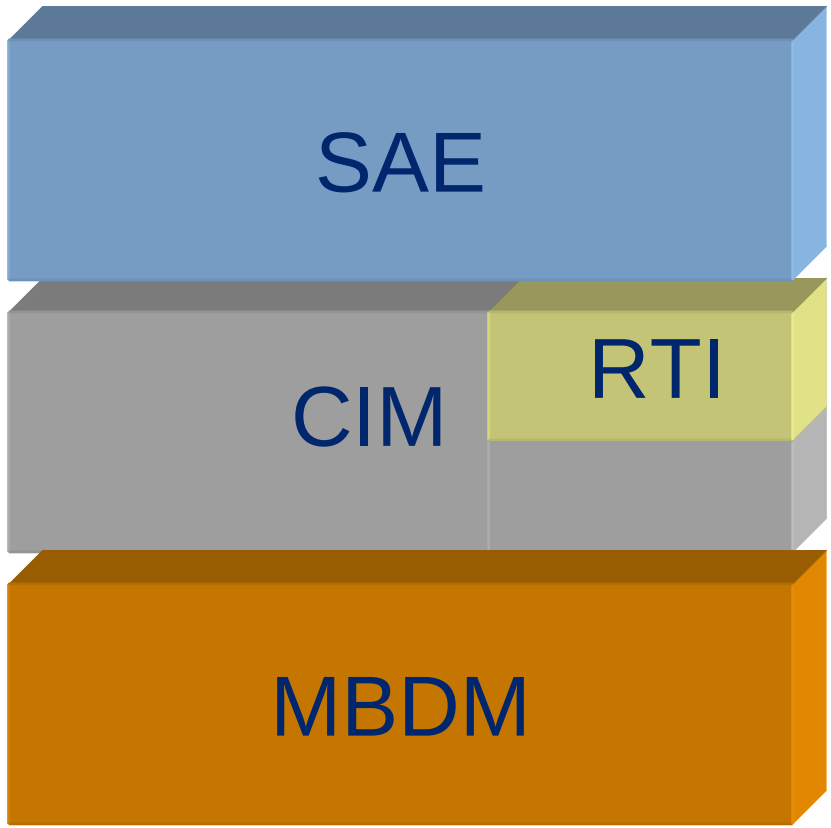
Zustandsmodellierung & Formale Analyse

Meilensteine des MakoSi-Vorgehensmodells



Bausteine des „Policy Driven System“

- Risikovermittlung beim Benutzer (SAE)
- Abgleich von Laufzeitinformationen (RTI)
- Policy Enforcement auf Basis der WBEM Services (CIM)
- MBDM

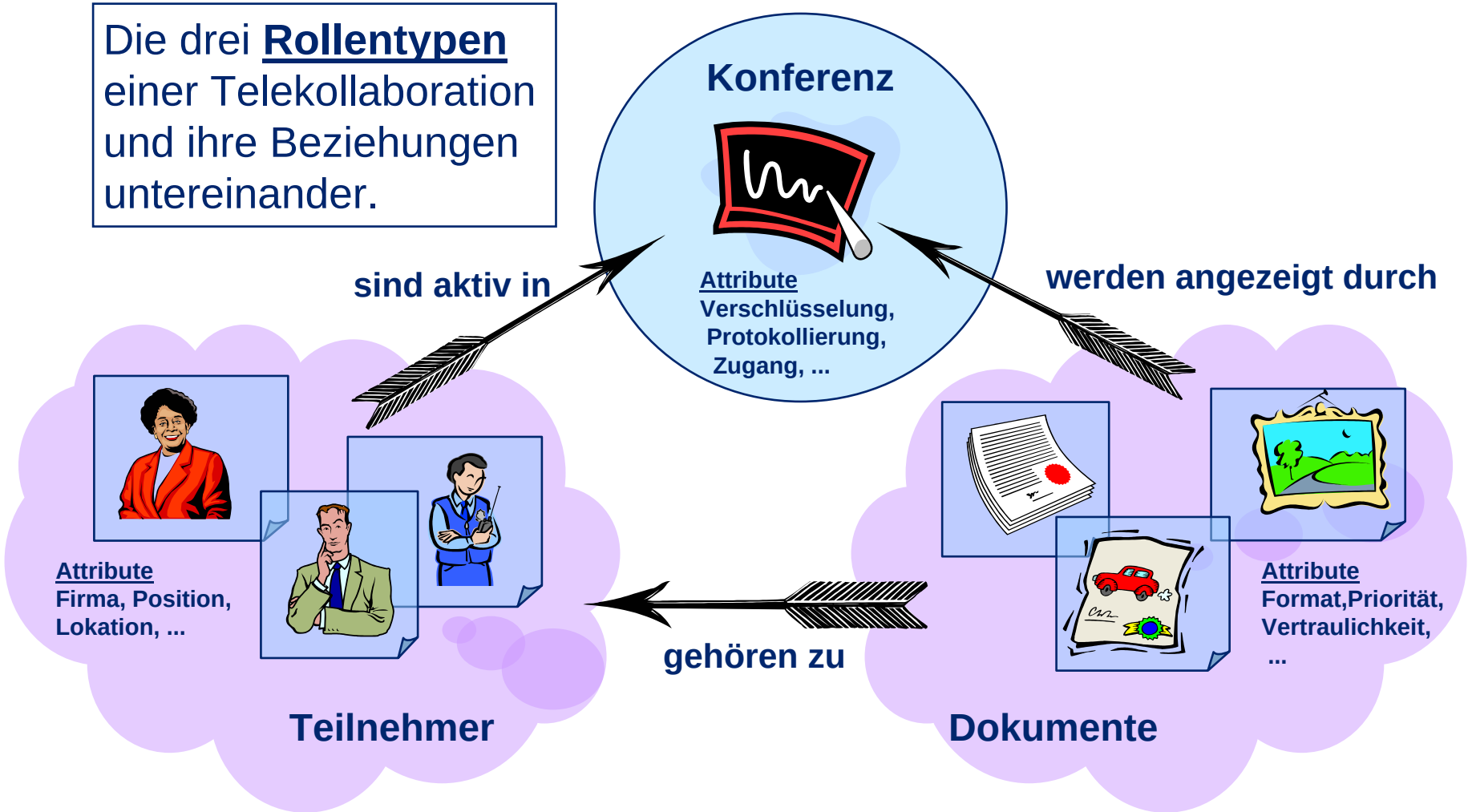


MakoSi-Basis-Datenmodell (MBDM)

- Einfaches Datenmodell zur Beschreibung von Kooperationssystemen auf der Basis von Rollen
- Aufbau von einfachen Sicherheitsmodellen für die Formulierung von Sicherheitspolitiken und deren Verifikation
- Bereitstellung von „Standardmodellen“ für gängige Kooperationsszenarien
- XML Repräsentation für einfachen Austausch und Transformation der Modelle bzw. Szenarien
- Ziel: Einheitliches Vokabular und Ontologie die die Konsistenz zwischen formaler Evaluation und Implementierung sichern

Ein MBDM-Profil: Rollentypen einer Telekollaboration

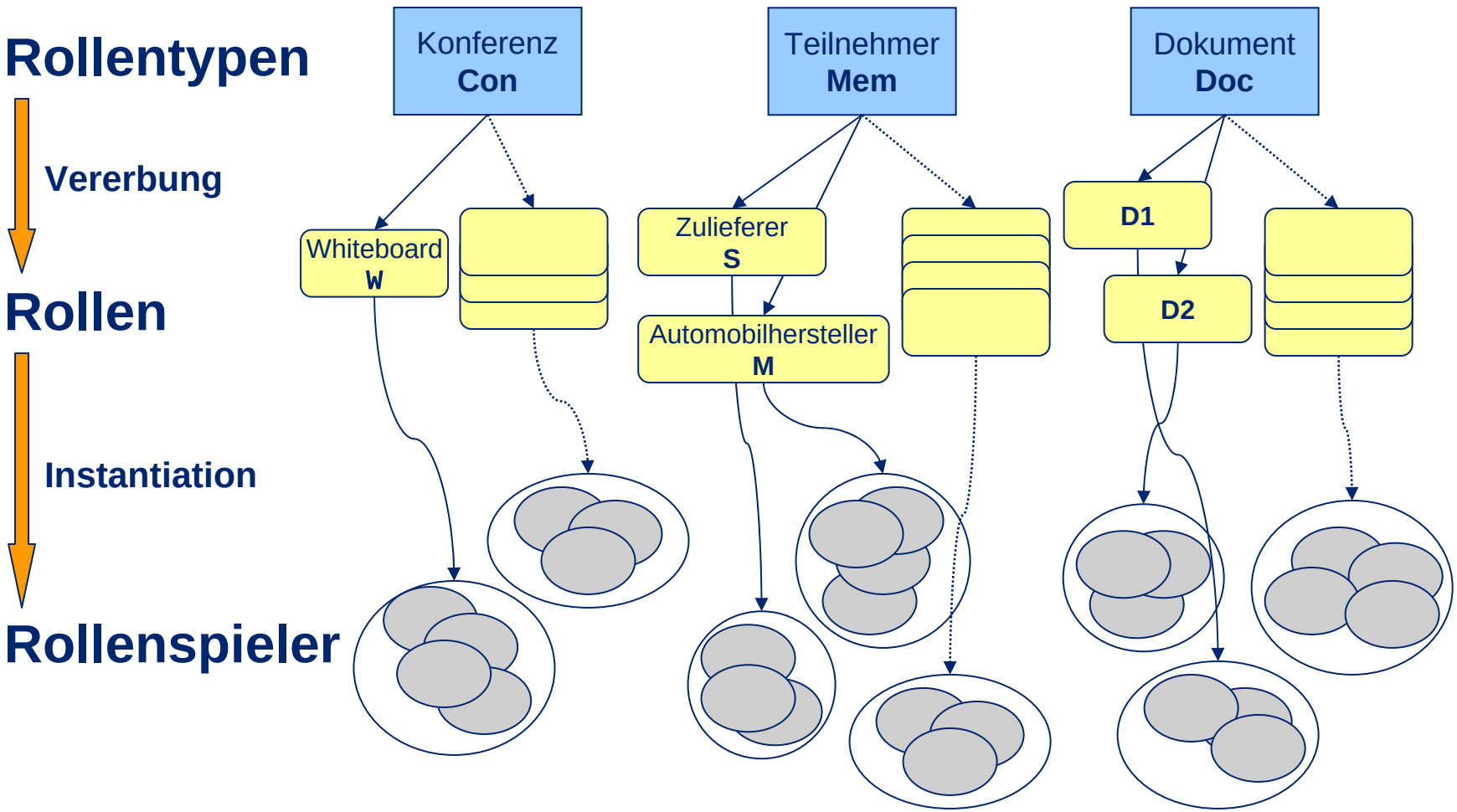
Die drei **Rollentypen** einer Telekollaboration und ihre Beziehungen untereinander.



Telekollaboration – Funktionale Grundcharakteristik

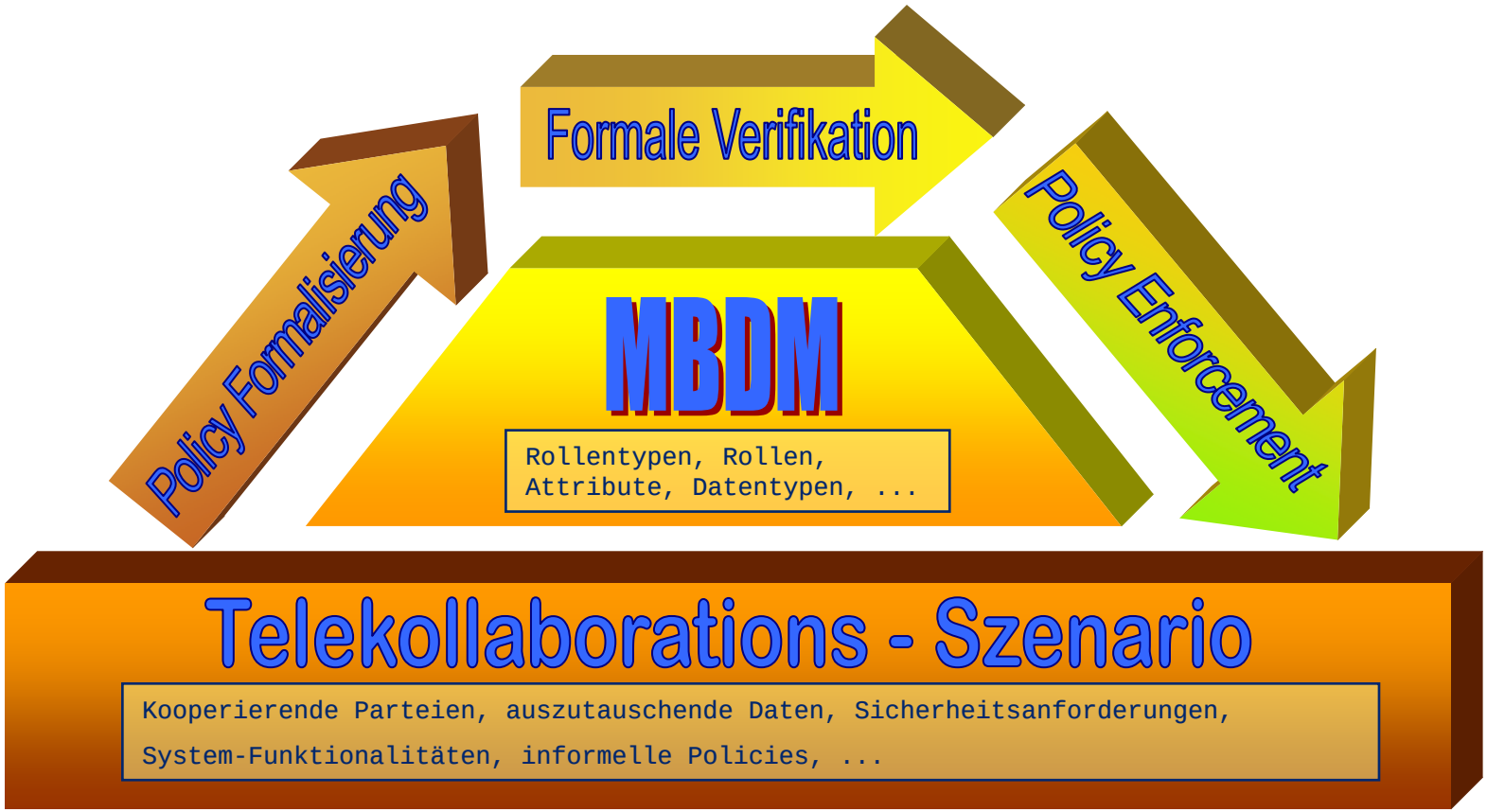
- Sicherheitsrelevante Grundcharakteristik einer Telekollaboration ist:
  - Dokumente in einer Konferenz sind unmittelbar allen Teilnehmern zugänglich
- Policies sind Event-Condition-Action (ECA) Regeln, die ausgelöst durch einen (versuchten) Zustandsübergang, d.h. eine Änderung von Attributswerten, Bedingungen auswerten und im Erfolgsfall Aktionen durchführen

MBDM – Rollenhierarchie

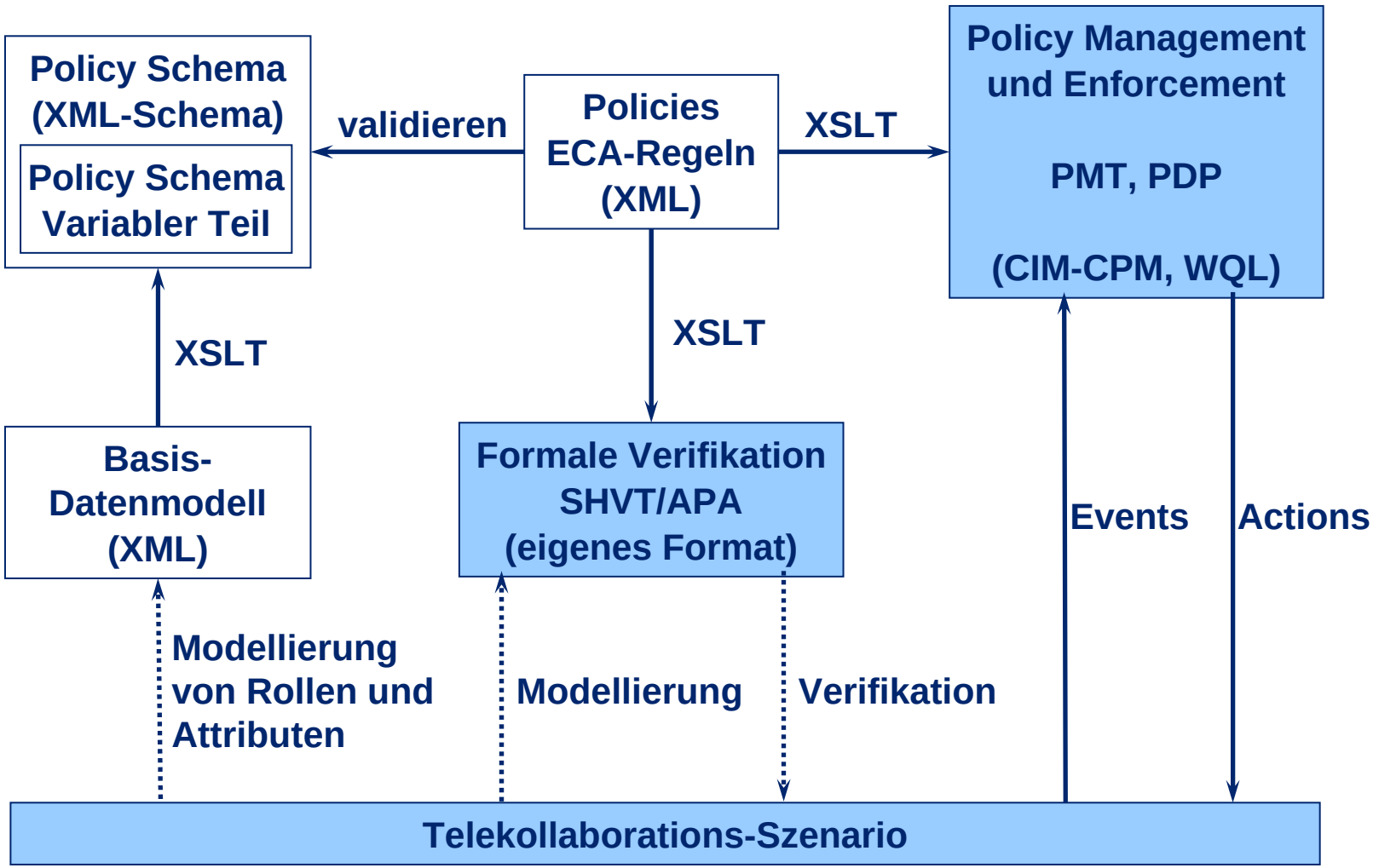


Die Funktion des MBDM in MakoSi

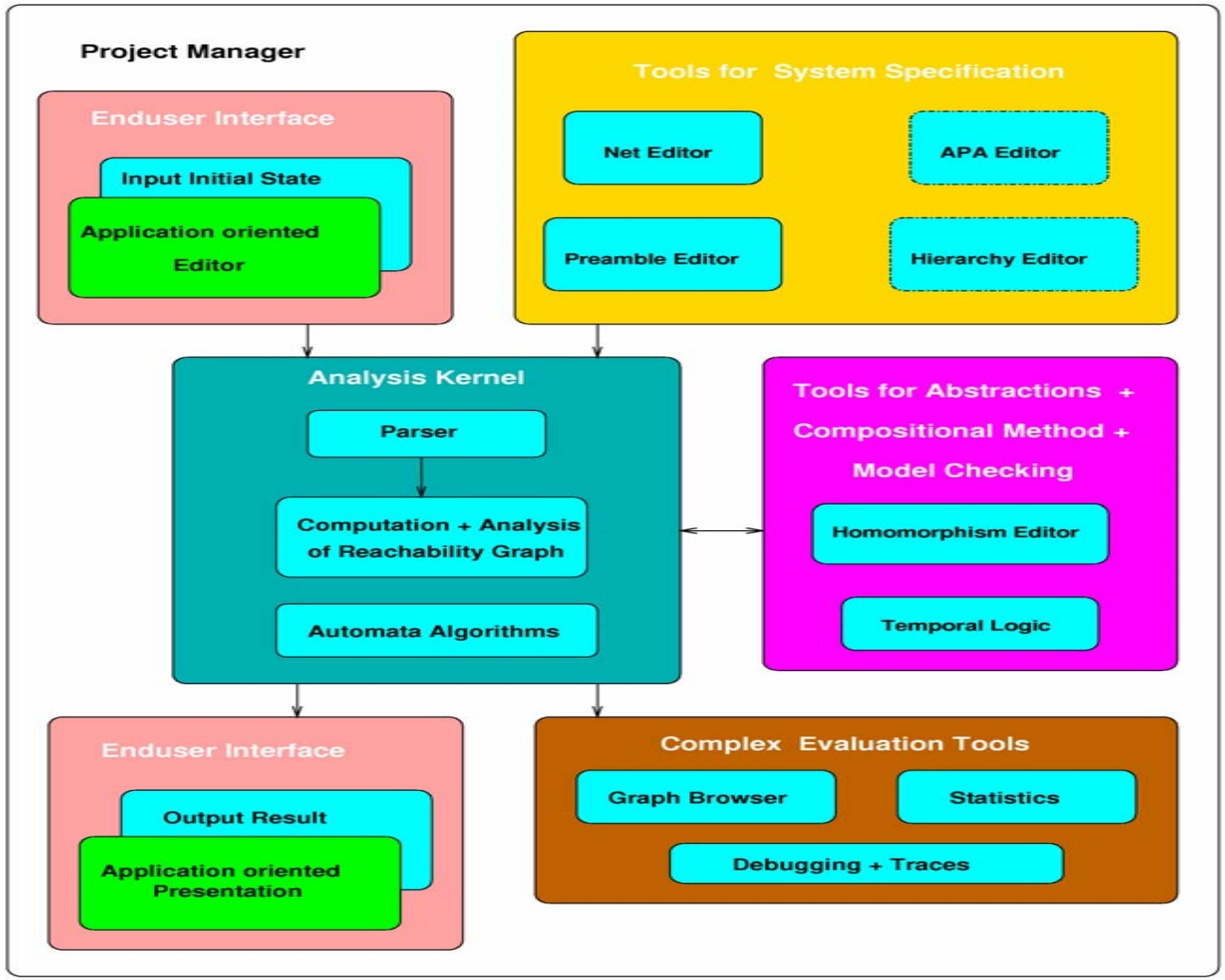
Das MakoSi-Basis-Datenmodell ist die grundlegende Datenstruktur für die zentralen Prozessschritte von MakoSi.



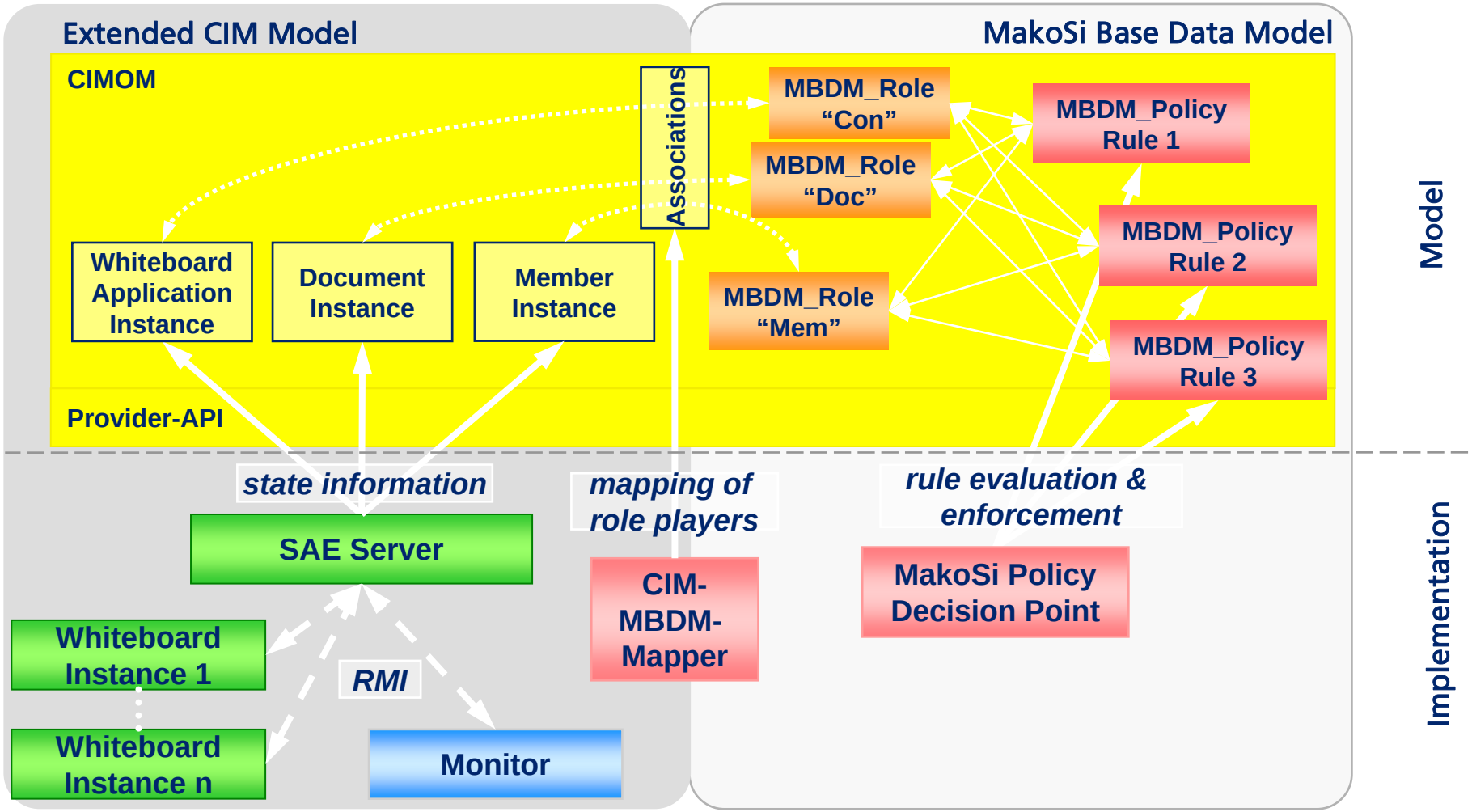
MBDM als Basis-Infrastruktur



Formale Verifikation – Das SHVT

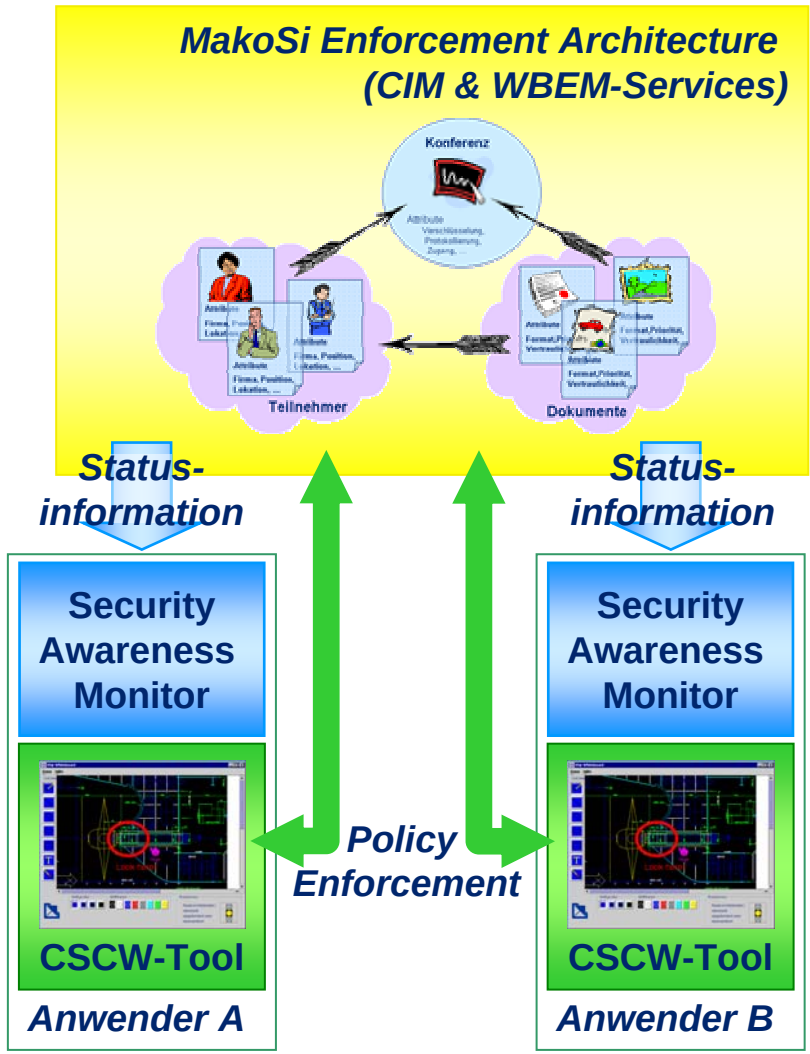


MBDM-CIM Modell Architektur



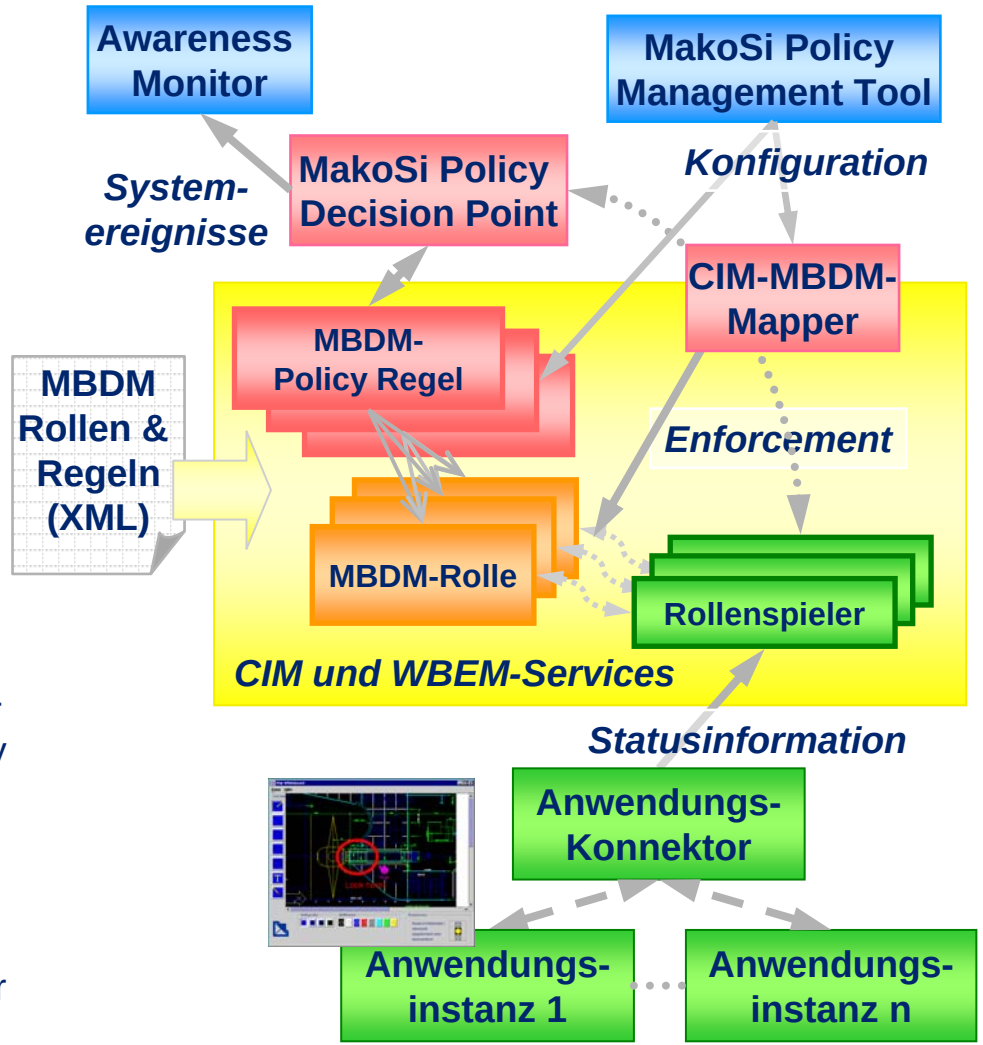
Policy Driven System auf Basis von WBEM-Services (1)

- Laufzeitarchitektur auf der Basis des des CIM-Standards und der WBEM-Services
- Integration der MBDM-Szenarien und Regeln
- Zuordnung zu realen „Rollenspielern“ im CIM
- Einfache Anwendung und Wiederverwendung von einmal erstellten und validierten Regelsätzen



Policy Driven System auf Basis von WBEM-Services (2)

- Policy Management Tool:
  - Editor für Policy Regeln
  - Zuordnung zwischen MBDM-Rollen und Rollenspieler
  - Im- & Export von MBDM-Rollen & Policy Regeln
- CIM-MBDM-Mapper:
  - Update der MBDM-Rollen-Instanzen in Abhängigkeit vom Systemzustand der Rollenspieler-Objekte
- MakoSi Policy Decision Point:
  - Auswertung & Durchsetzung der Policy Regeln im MBDM
- Awareness Generator:
  - Security awareness Informationen für den Endbenutzer auf Basis der Policy Entscheidungen u./o. anderer Systemereignisse
- Anwendungskonnektor:
  - Anbindung von Telekooperationsan-wendungen an die WBEM-Architektur

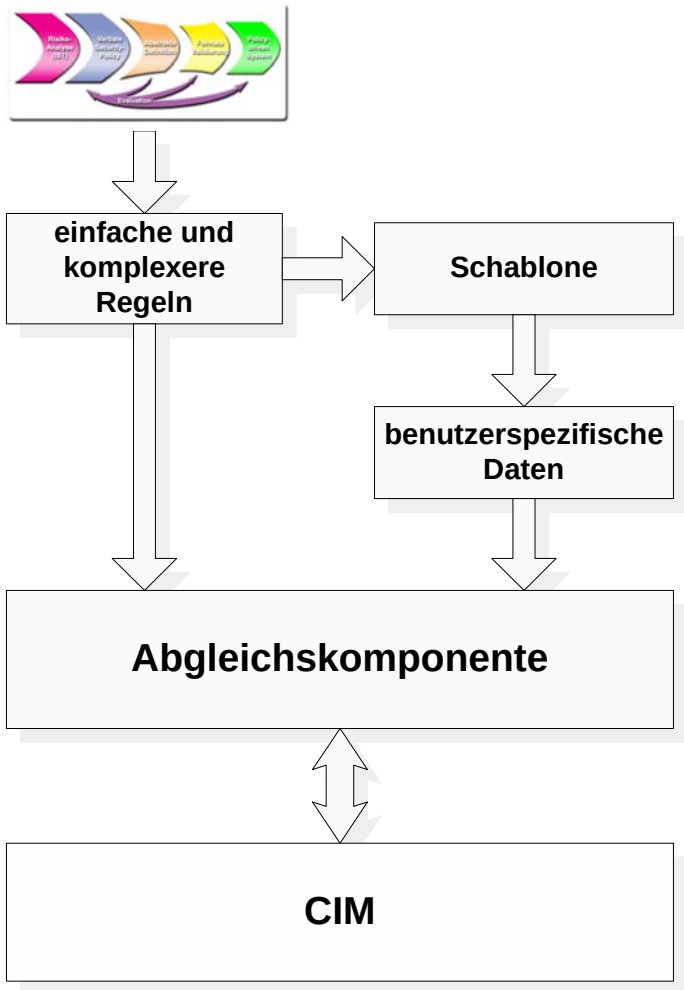


Abgleich von Laufzeitinformation

- Hintergrund:
  - aus Komplexitätsgründen kann laufzeitrelevante Detailinformation bei der formalen Verifikation nicht berücksichtigt werden
  - Sie wird deshalb abstrahiert (z.B. Zusammenfassung von verschiedenen Verschlüsselungstypen in Klassen)
- Detailinformation ist aber ein wichtiger Faktor im implementierten System
- Ziel:
  - ✓ Erleichterung der Erfassung relevanter Detailinformation für Administratoren und Endbenutzer
  - ✓ Automatisierter Abgleich

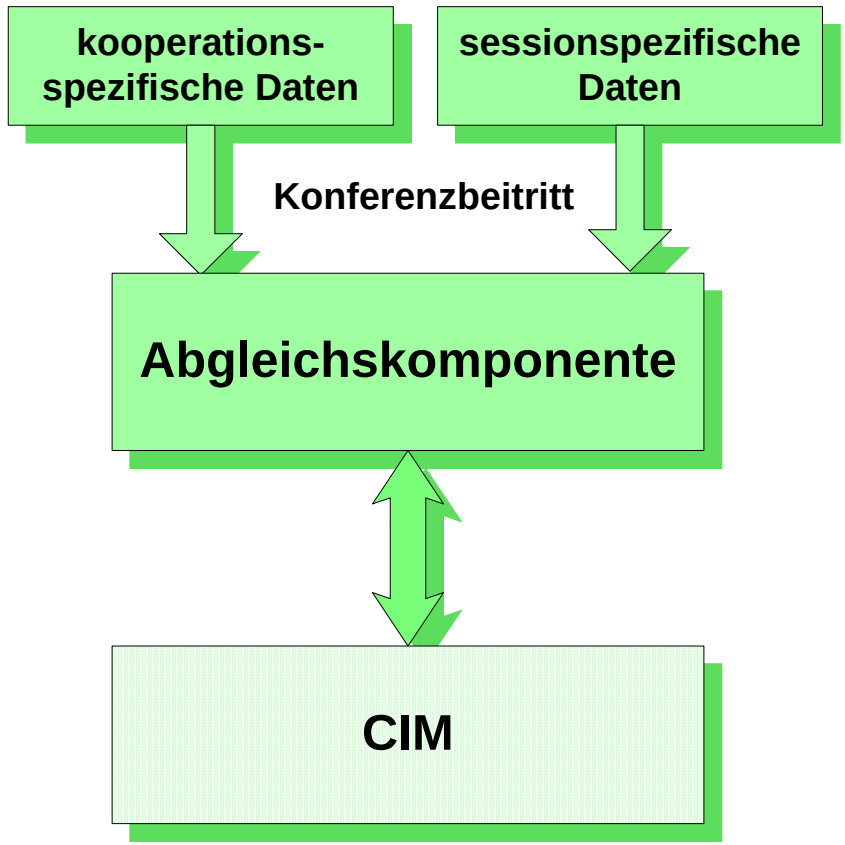
Abgleich der Laufzeitinformation

- Identifikation der laufzeit-relevanten Information mit Hilfe des MakoSi-Vorgehensmodell
- Administrator kann Zusammenhänge in der laufzeitrelevanten Information berücksichtigen
- Der Benutzer erhält eine Schablone und ergänzt die Regeln um individuelle benutzerspezifische Daten
- Die Abgleichskomponente führt den Abgleich durch



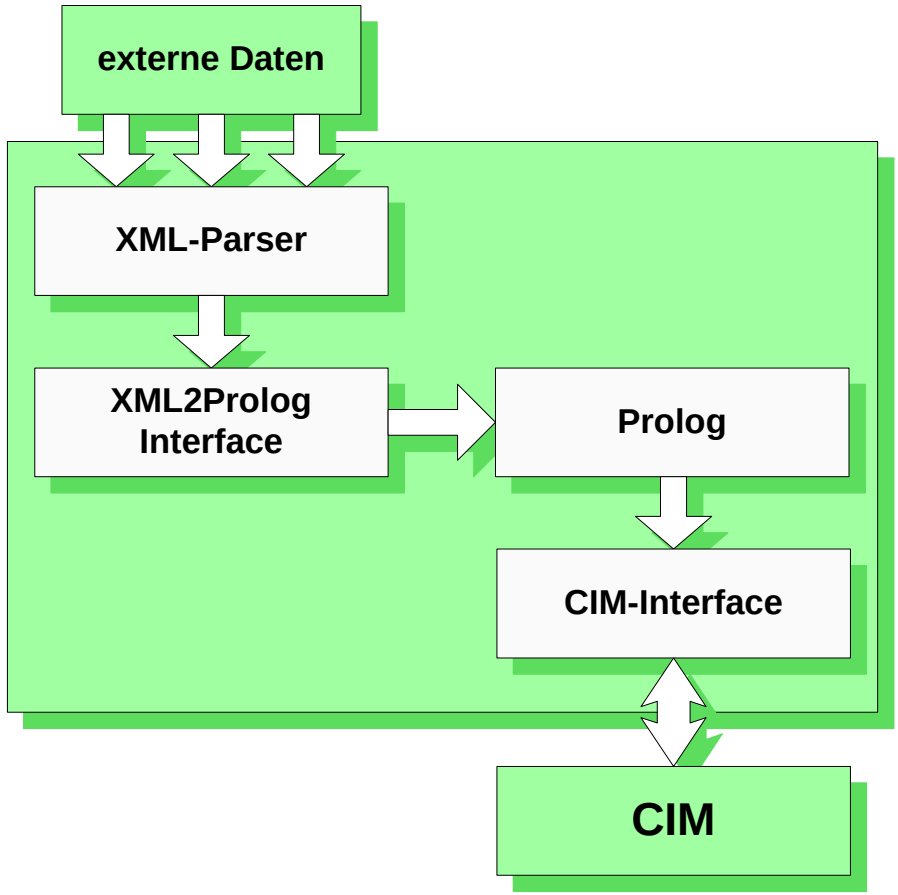
Integration der Abgleichskomponente

- Regeln werden für die jeweilige Kooperation erstellt
- Session-spezifische Daten werden von den Benutzer geliefert
- Abgleichskomponente verarbeitet Regeln und Daten
- Interaktion mit CIM stellt Integrität sicher



Funktionsweise der Abgleichskomponente

- Prolog-Kern zur dynamischen Regelauswertung
- Regeln und sitzungsspezifische (externe) Daten werden in XML beschrieben
- Kommunikation mit der CIM-Komponente zur Laufzeit

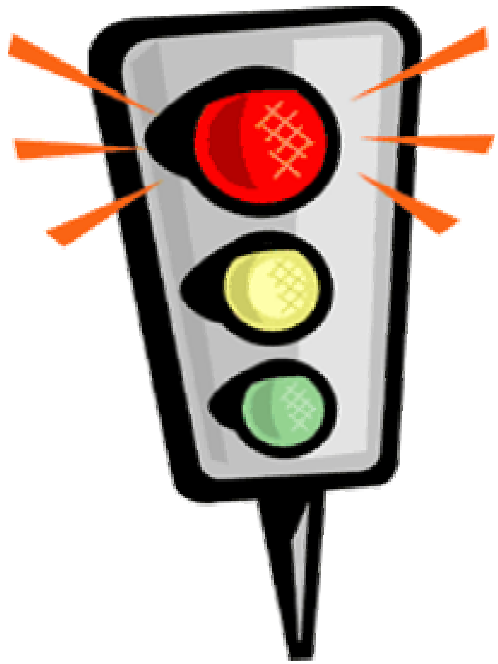


Security Awareness and Enforcement (SAE)

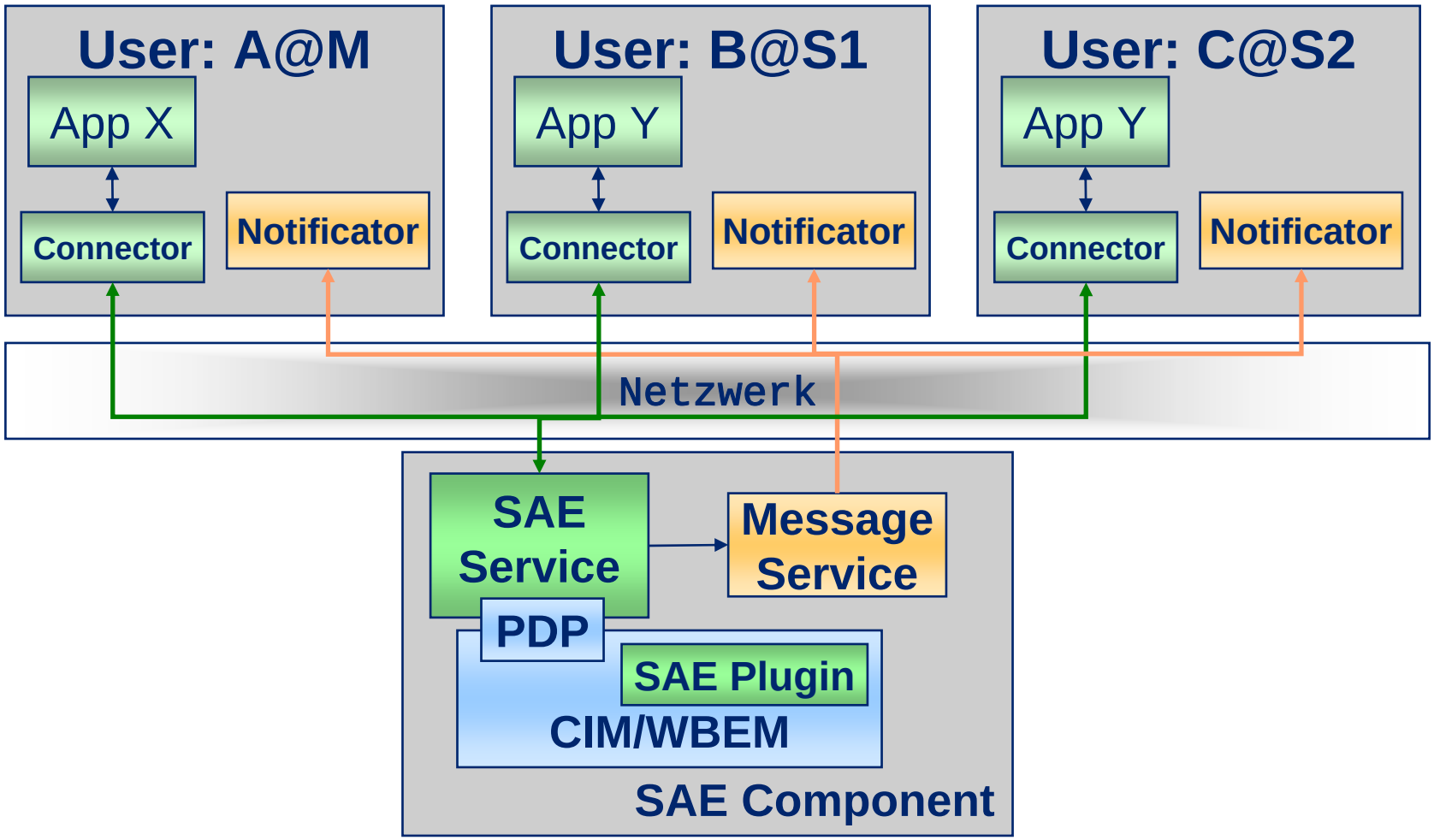
- Effektive Durchsetzung von Sicherheitsrichtlinien erfordert Sensibilisierung der Benutzer
- Methoden
  - Nachvollziehbares Enforcement

    Unterstützung der Benutzers bei der Einhaltung von Sicherheitsrichtlinien
  - Risikovermittlung

    Verbesserung der Wahrnehmung von Sicherheitsrisiken durch den Anwender

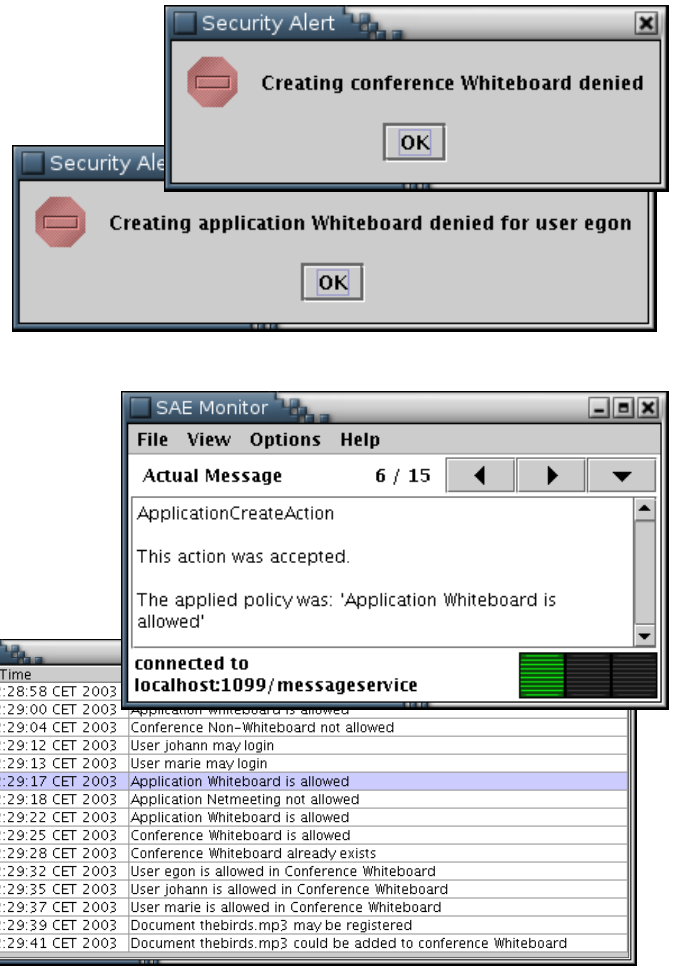


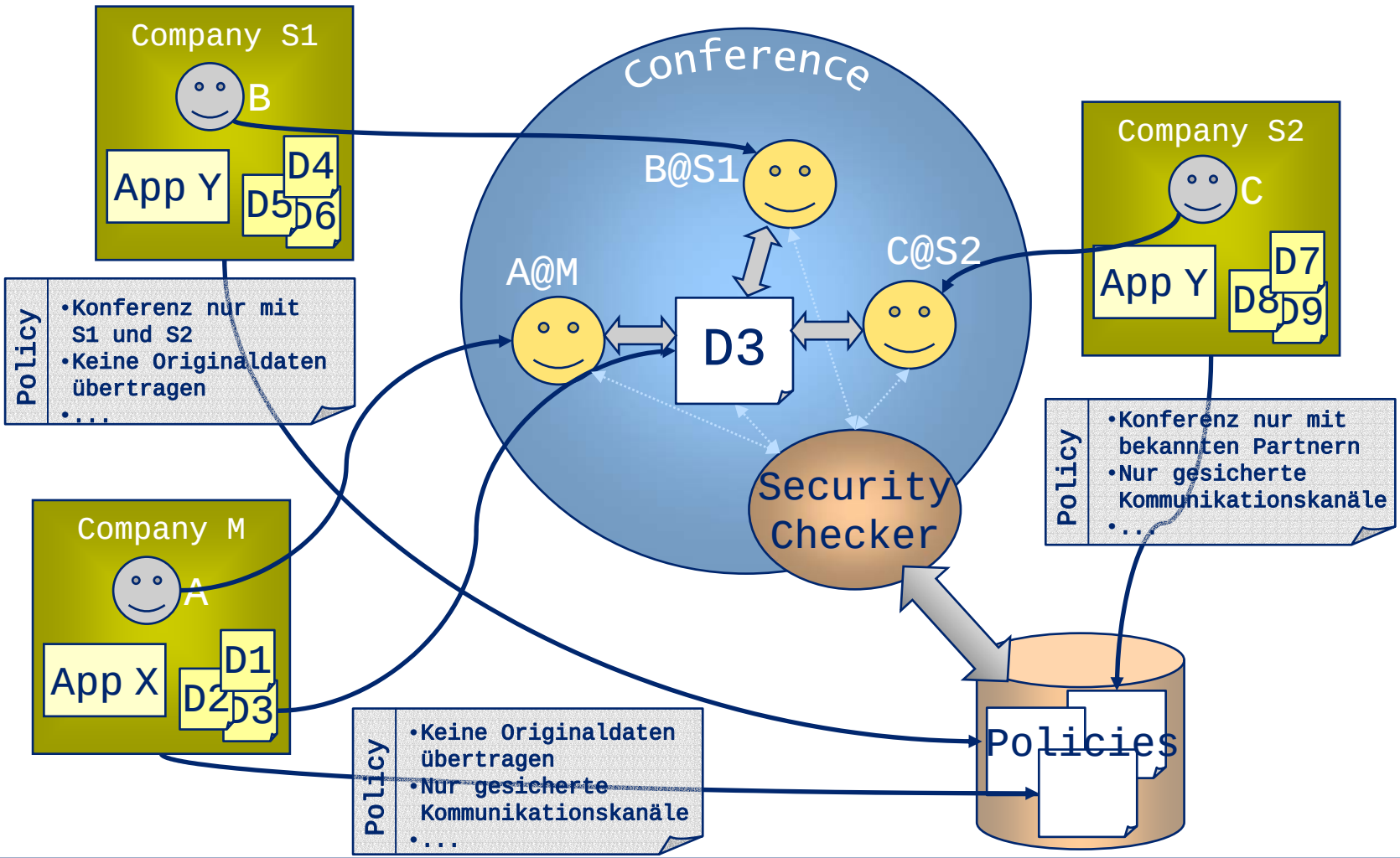
SAE Architektur



Security Awareness and Enforcement (SAE)

- Maßnahmen zur Awareness-Vermittlung
  - Applikation erfragt Durchführbarkeit bei sicherheitsrelevanten Aktionen.
  - Sicherheitskritische Aktionen werden signalisiert
  - Nur unbedenkliche Operationen dürfen durchgeführt werden
  - In einem Monitor werden die geprüften Aktionen und das Ergebnis angezeigt.
  - Der Benutzer wird damit für sicherheits-kritische Aktionen sensibilisiert.
- Existierende Applikationen können flexibel in diese Infrastruktur integriert werden



Nachfolgende Folien enthalten ergänzende Informationen

Anwendungsszenario: Virtual Design Review