TeleTrusT
Pioneers in IT security.

TeleTrusT-interner Workshop

Nürnberg, 21./22.06.2012

Michael Gröne

Sirrix AG security technologies

IT-Sicherheitsaspekte des "digitalen Unternehmens" und der dort genutzten Komposition von Software ("Emergente Software")

Software-Cluster

Der Software-Cluster und das Projekt EMERGENT

Michael Gröne

Nürnberg, 22.6.2012

INVENTED IN GERMANY

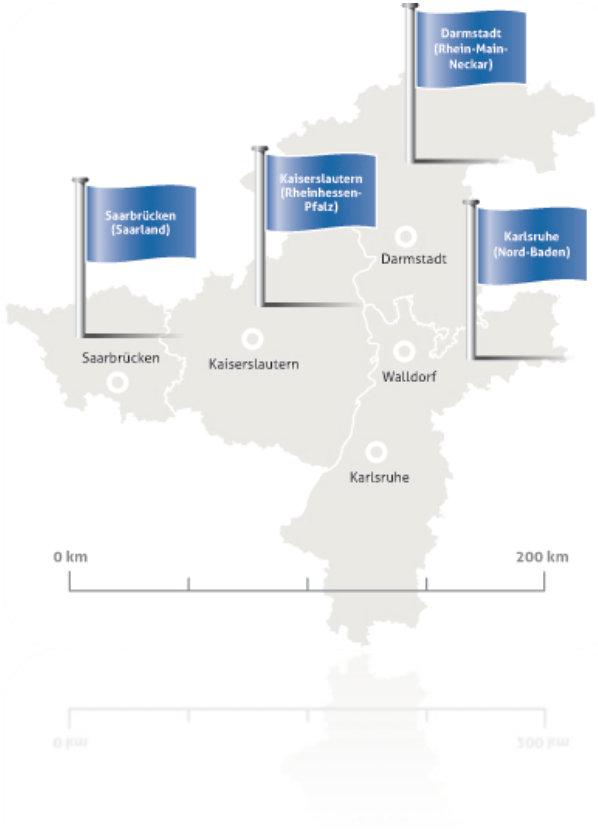
GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung

Agenda

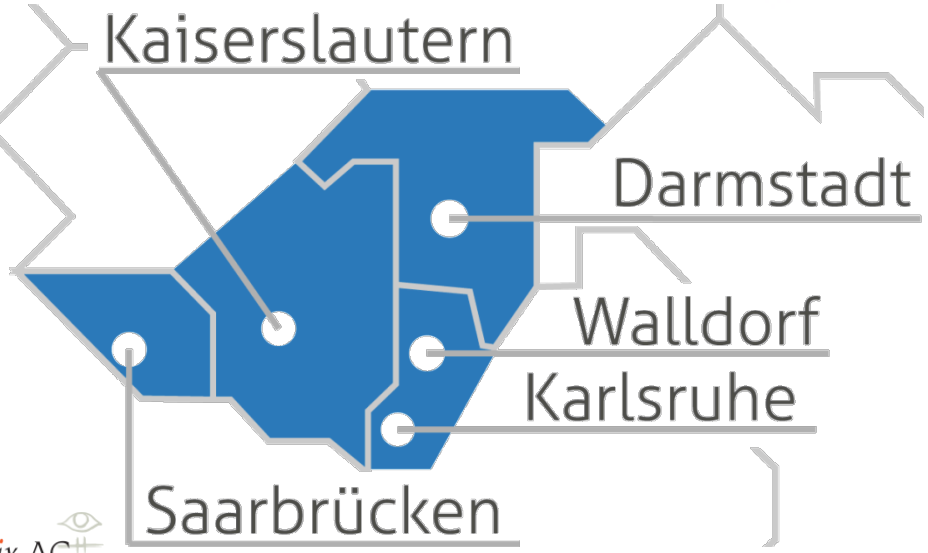
Software-Cluster

- Eckdaten zum Software-Cluster
- Das Projekt EMERGENT
  - Randbedingungen und Herausforderungen
  - Emergente Software & Schwerpunkte
- Forschungsschwerpunkt Sicherheit
  - Ziele, Schwerpunkte, Nutzen
  - Ausgewählte Highlights
  - Ausblick



Was ist der Software Cluster?

Software-Cluster



Software-Cluster statt IT-Cluster

- IT-Cluster gibt es wie Sand am Meer (umfasst auch Hardware und Telekommunikation)

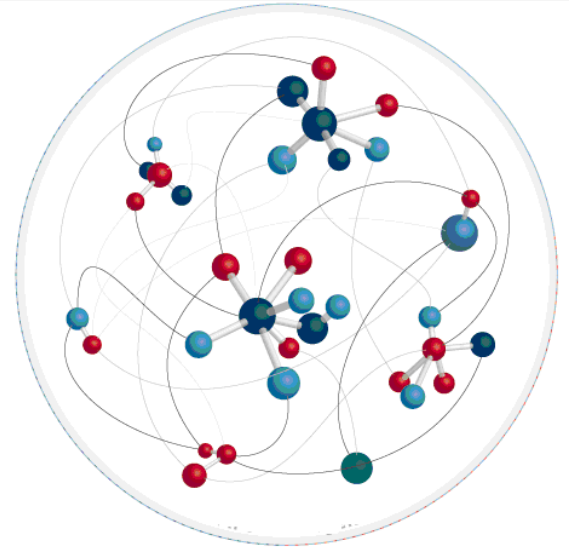
- Die überragende Stärke der Region, in der sie weltweit wettbewerbsfähig ist, liegt im Bereich Unternehmenssoftware bzw. Software für das Management von Geschäftsprozessen

- **Vision**
  Der Software-Cluster ist das Zentrum für Unternehmenssoftware in Europa und gehört zu den Top-Technologie-Regionen in der Welt.

Ziel des Software Clusters

Software-Cluster

Software ist eine wesentliche Grundlage für den Wohlstand in Deutschland – vor allem in der zunehmend globalisierten Wirtschaft. Software stärkt die Wettbewerbsfähigkeit von deutschen Unternehmen.



Der Software-Cluster entwickelt Konzepte, Software und Standards für „Digitale Unternehmen“.

Diese führen zu einer völlig neuen Qualität der Geschäftsmodelle und -abläufe bei Anbietern und Anwendern.

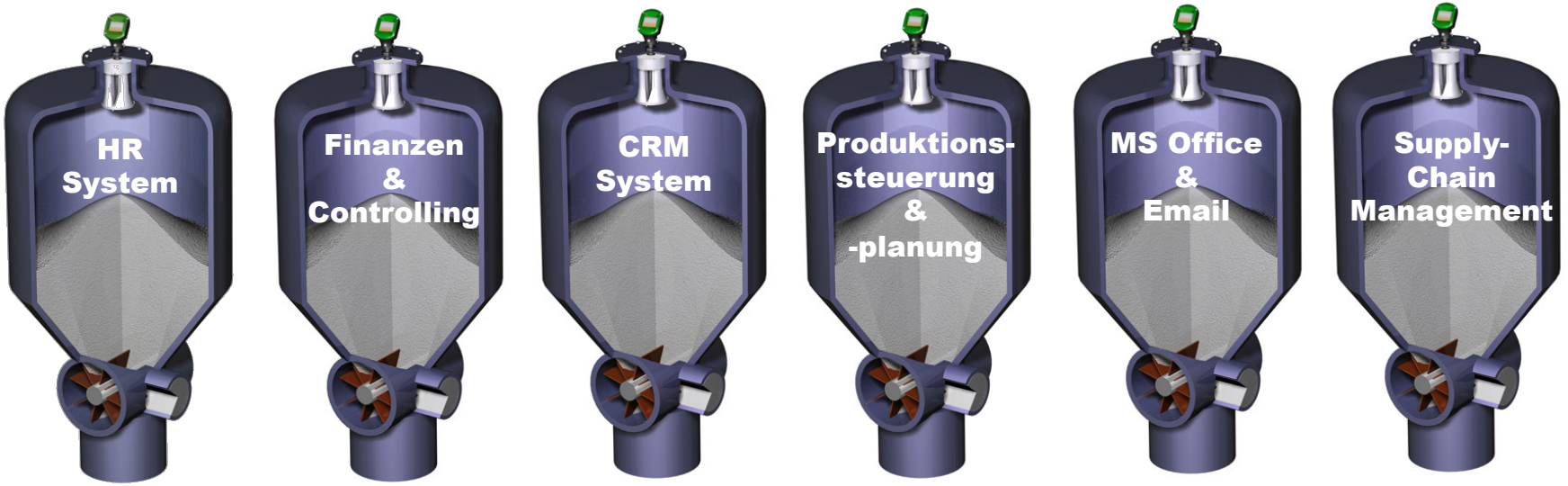
Herausforderung:
Die Unternehmensprozesse in „IT-Silos“

Software-Cluster





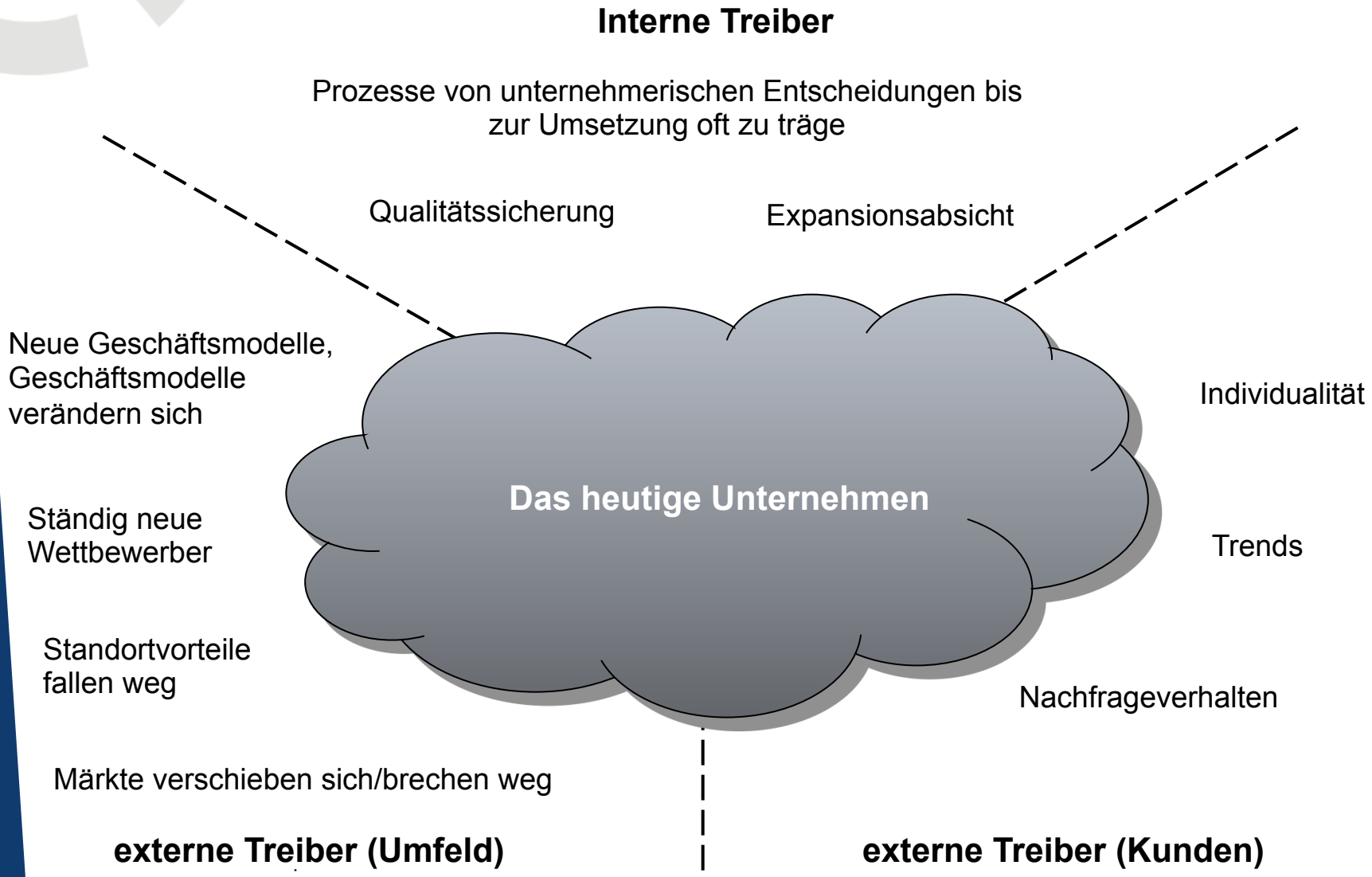

Personalwesen	Buchhaltung	Vertrieb	Produktion	Dokumentation & Kommunikation	Logistik



Das Projekt EMERGENT

Software-Cluster

Neue Randbedingungen



Neue Herausforderungen

Software-Cluster

Neue oder veränderte Anforderungen

Unternehmensübergreifende Dienstleistungen

Bedarfgerechte Sicherheit

Echtzeitreaktionen

Adaptive Prozesse

Erfassung des Kontext

Auswertung von Kontextinformationen

Agilität und Flexibilität

Proaktivität statt Reaktivität

Ad-hoc Vernetzung von Unternehmen

Individuelle Anpassung von Prozesse

Foren und Community-Plattformen

Probleme im Unternehmensumfeld

Mangelnde Transparenz in der Wertschöpfungskette

gleichbleibende Qualität bei Routineaufgaben

Größerer Wettbewerb

Akzeptanz

Vertrauen in die neuen Dienstleitungen

Komplexität in der Bindung zwischen Unternehmen

Echtzeitfähigkeit bei der unternehmerischen Entscheidung

Emergenz als Schlüssel

Software-Cluster

Neue oder veränderte Anforderungen

Unternehmensübergreifende Dienstleistungen

Bedarfgerechte Sicherheit

Echtzeitreaktionen

Adaptive Prozesse

Erfassung des Kontext

Auswertung von Kontextinformationen

Agilität und Flexibilität

Proaktivität statt Reaktivität

Ad-hoc Vernetzung von Unternehmen

Individuelle Anpassung von Prozesse

Foren und Community-Plattformen

Probleme im Unternehmensumfeld

Mangelnde Transparenz in der Wertschöpfungskette

gleichbleibende Qualität bei Routineaufgaben

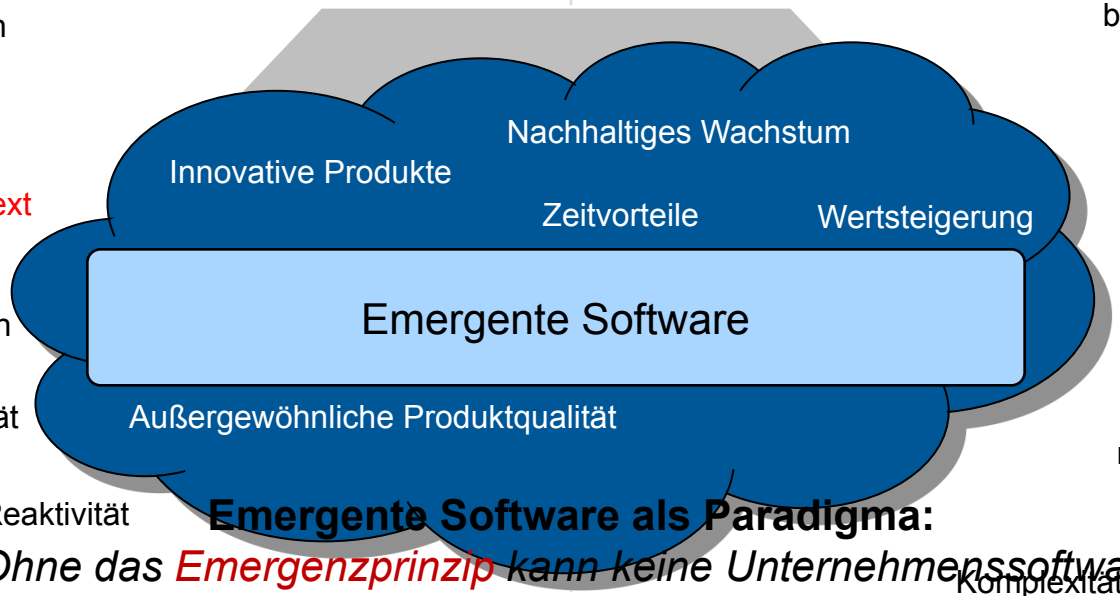
Größerer Wettbewerb

Akzeptanz

Vertrauen in die neuen Dienstleitungen

Komplexität in der Bindung [illegible] Unternehmen

Echtzeitfähigkeit bei der unternehmerischen Entscheidung



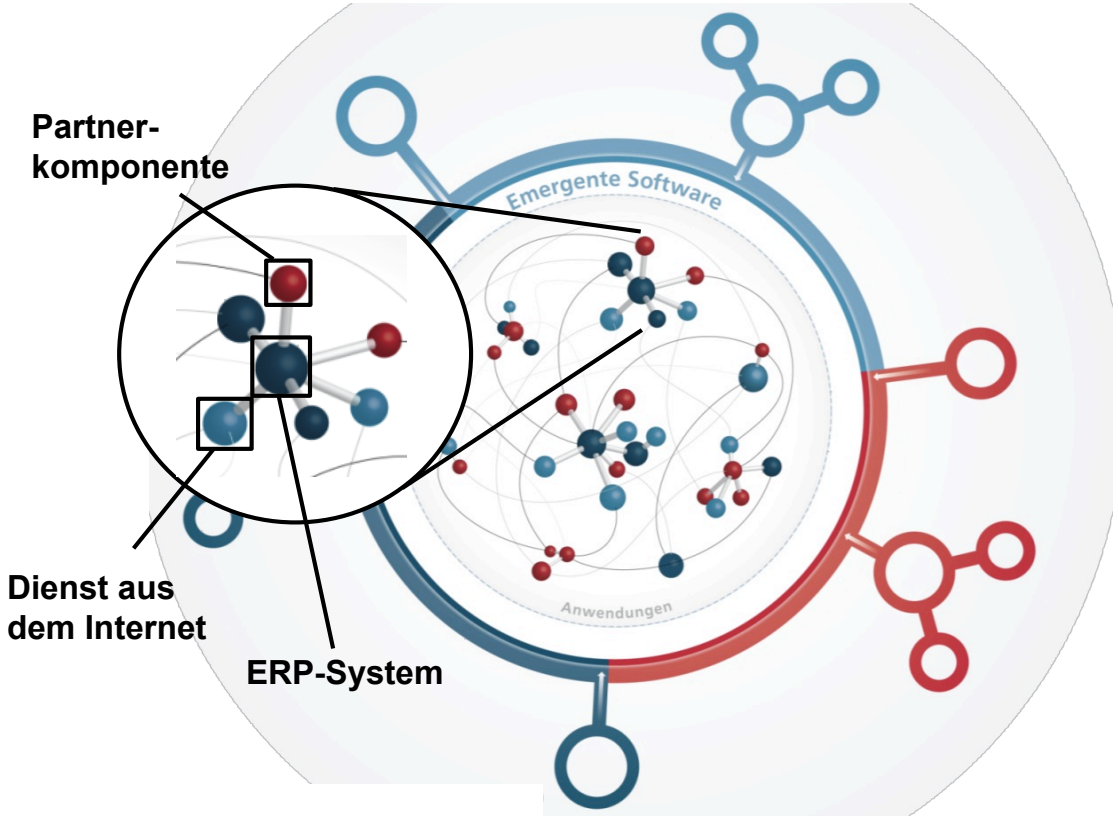
Emergente Software als Paradigma:

Ohne das Emergenzprinzip kann keine Unternehmenssoftware entwickelt werden, die es Unternehmen in Zukunft ermöglicht als „digitale Unternehmen“ in einer global vernetzten Welt erfolgreich Wertschöpfung zu generieren!

Innovationssprung

Emergenz ist das Auftreten neuer Eigenschaften auf einer höheren Komplexitätsstufe, die sich auf der vorangehenden Stufe nicht vorhersehen lassen haben.

- Der Begriff beschreibt das aus dem Zusammenspiel der einzelnen Komponenten im Internet der Dinge und Dienste entstehende Gesamtsystem
- Das führt zu einem Quantensprung in der Wertschöpfung.



Emergente Software & Schwerpunkte

Software-Cluster

Software ist emergent, wenn sie in unternehmensübergreifenden Prozessen möglichst **ohne weitere Anpassung** auf **sichere** Weise **flexibel integriert** und sofort durch den **Endanwender genutzt werden** kann.

→ Sie ist somit adaptiv, sicher, interoperabel und nutzerfreundlich.

Adaptivität

- adaptive Geschäftsprozesse
- organisationsübergreifendes Systemverhalten
- dynamische Anpassung mit QoS-Garantien

Sicherheit

- Schutz von Daten der Benutzer und Firmen
- Vertrauen durch aktive Sicherheit

Interoperabilität

- durchgängige Software-Engineering-Methodik
- abgestimmte technische Schnittstellen
- Skalierbarkeit durch Clouds

Nutzerfreundlichkeit

- Situations-sensitive Präsentation von Informationen
- Benutzerführung in integrierten Nutzerschnittstellen

Positive ökonomische Effekte

Software-Cluster

- **Intelligente Kombination** führt zu **neuen Angeboten bei Anwendern**
  - neue Geschäftsmodelle auf Seite der Anwender

  und bei den Anbietern
  - Entwicklungs- und Wartungsaufwand drastisch reduziert
  - adressierbarer Markt erweitert durch Kombinationsfähigkeit
  - Time-to-Market reduziert durch abgestimmte Lösungen
  - neue Geschäftsmodelle auf Anbieterseite

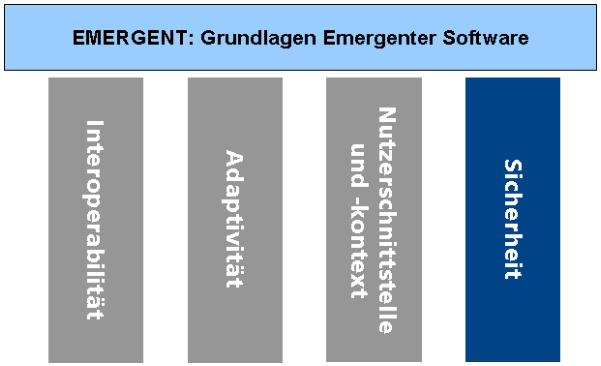
- **Cloud-Computing**: Lösungen skalierbar, wartungsarm und mit geringen Investitionen

Software-Cluster

Forschungsschwerpunkt Sicherheit

Forschungsschwerpunkt Sicherheit

Software-Cluster



Ziel

- Sichere Unternehmenssoftware für das Digitale Unternehmen

Motivation

- Innovative Geschäftsmodelle erfordern den **garantierten Schutz** von Daten der **Benutzer sowie der beteiligten Firmen** in nahtlos verwebten Prozessen und Diensten über Unternehmensgrenzen hinweg
- Dies erfordert **Mechanismen zum aktiven Schutz von Benutzer- und Firmendaten** – unter Einbeziehung von Clouds
- Aktive Sicherheit sensitiver Daten als **Schlüssel für Akzeptanz von Innovation**

Sirrix AG security technologies

Fraunhofer IESE

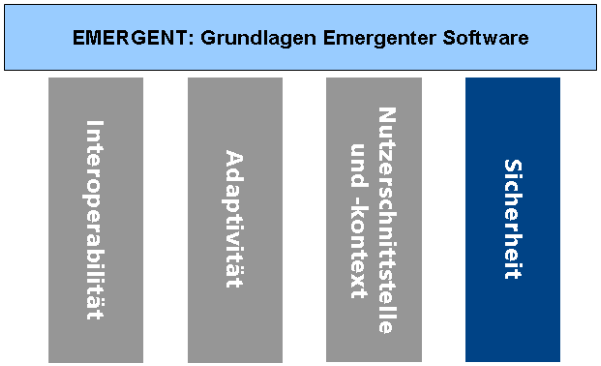
KOBIL secure your identity

TECHNISCHE UNIVERSITÄT DARMSTADT

SAP

Forschungsschwerpunkt Sicherheit

Software-Cluster



Schwerpunkte

- Systematische Analyse der Sicherheits-anforderungen Emergenter Software
- Entwicklung grundlegender Sicherheitskonzepte als Grundlage für
  - Fehlertolerante Softwarekomponenten
  - Bedarfsorientiertes, dynamisches Sicherheitsmanagement
  - Datensicherheit und Nutzungskontrolle

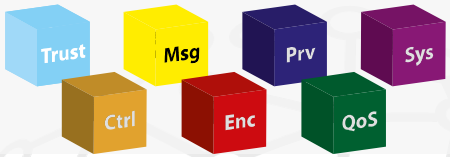
Neuartigkeit durch

- **Garantierte Systemsicherheit** im Internet der Dinge
- **Bedarfsgerechte Sicherheit** für Dienste und Geschäftsprozesse
- Sicherheitsrichtlinien im **Internet der Dienste**

Policies, Ziele, Durchsetzung

Software-Cluster

Policy-Baukasten



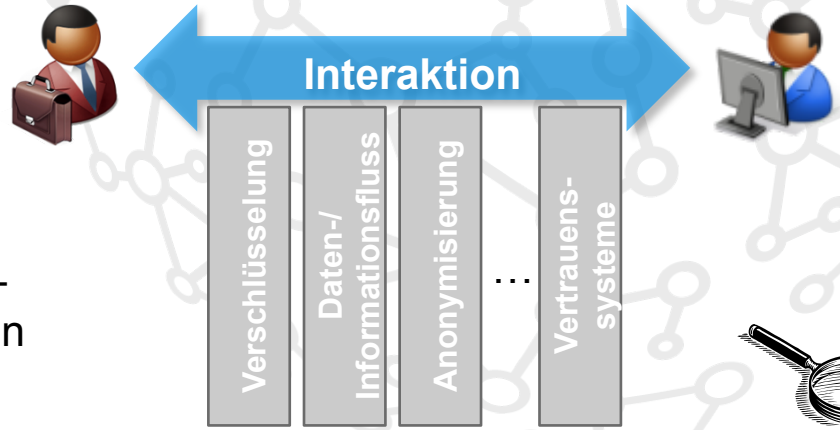
Einzelne Sprachkonstrukte

Policy-Sprache

Ausgewählte & kombinierte Sprachkonstrukte

Policy

Instanz der Sprache



Sicherheits-technologien

Sicherheitsziele

C I A & beyond

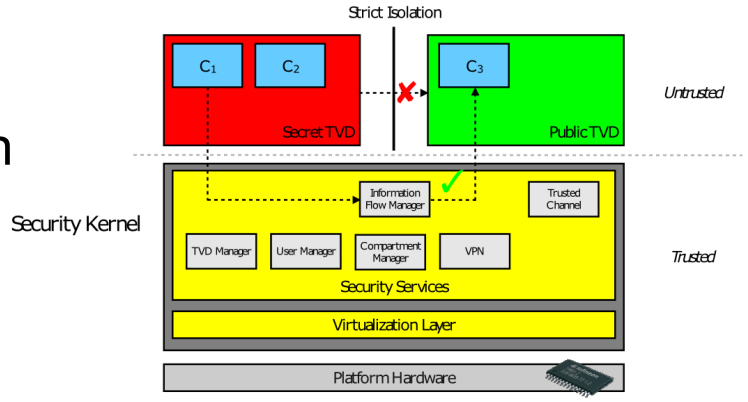
Spezifikation, Verhandlung, Umsetzung und Durchsetzung der Policy (bzw. deren Ziele)

Highlight 1 - Demonstrator
Policy-based Information Flow Control between Trusted Virtual Domains

Software-Cluster

Ziel:

- TVD-Konzept forciert strikte Isolation von virtuellen Rechenumgebungen
- Autorisierte Informationsflüsse zwischen TVDs sollen zugelassen werden



Lösungskonzept:

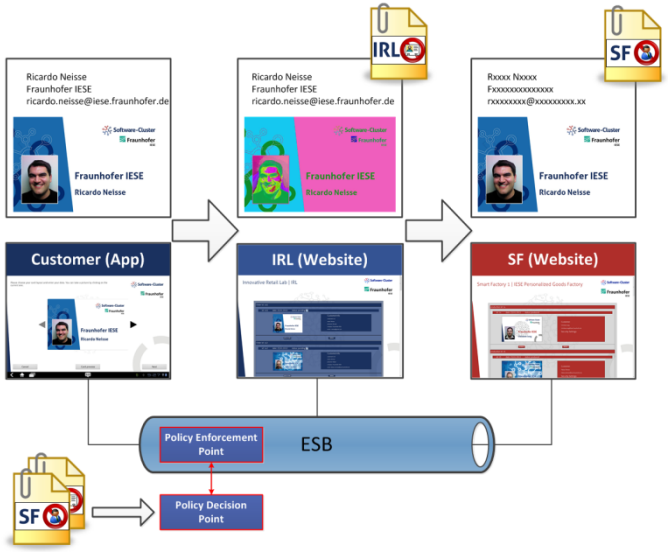
- „Information Flow Manager“-Komponente innerhalb des vertrauenswürdigen Security-Kernels
- Policy-basierte Autorisierung mit einem PDP und einem PEP
- Dynamische Änderungen an Policies werden unterstützt und direkt umgesetzt
- Zentrales Management und Offline-Fähigkeit

Sirrix AG security technologies

SecurITy made in Germany

Highlight 2 - Demonstrator
Next Generation Data Usage Control

Software-Cluster



Ziel:

- Erzwingung von Zugriffs-und Nutzungskontrolle in emergenten Dienstekompositionen

Lösungskonzept:

- Policy-Enforcement auf Bus-Ebene
- Spezifikation von Nutzungskontrolle via Obligation Specification Language (OSL)
- Vision: Top-Level Policy-Definition wird auf unterschiedlichen Ebenen des Systemstacks umgesetzt

Fraunhofer IESE

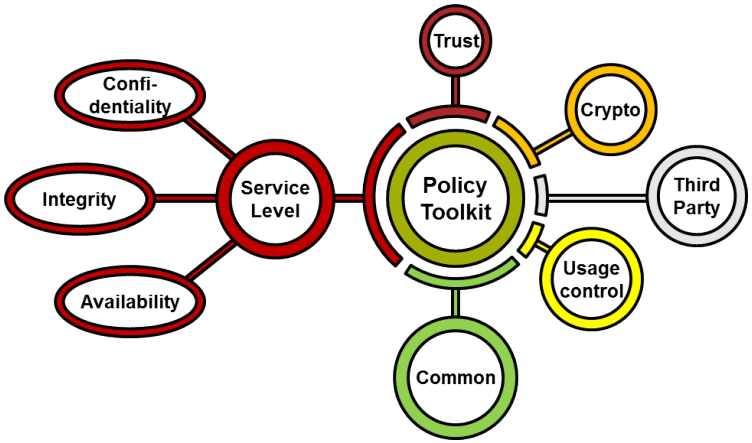
- Unterstützend: Trust-basierte Anbieterselektion implementiert „Soft Security“-Aspekte

TECHNISCHE UNIVERSITÄT DARMSTADT

Theorie und Ausblick

Software-Cluster

Systematische Entwicklung eines Baukastens für Sicherheitspolicies für emergente Software



- **Neue Konzepte** für Policy-Sprachen
  - Unterstützung verschiedenster Sprachkonstrukte heutiger Policy-Sprachen
  - Sprachkonstrukte für Nicht-binäre Policies
  - Polymorphie für Policies in unterschiedlichen Kontexten
  - Einschränkung der Gültigkeit einer Policy auf einen bestimmten Kontext
- **Entwicklung eines Kataloges von Plug-Ins** für die benötigten Sprachkonstrukte

Theorie und Ausblick

Software-Cluster

Systematische Entwicklung von fehlenden Sicherheitstechnolgien zur Durchsetzung von Policies

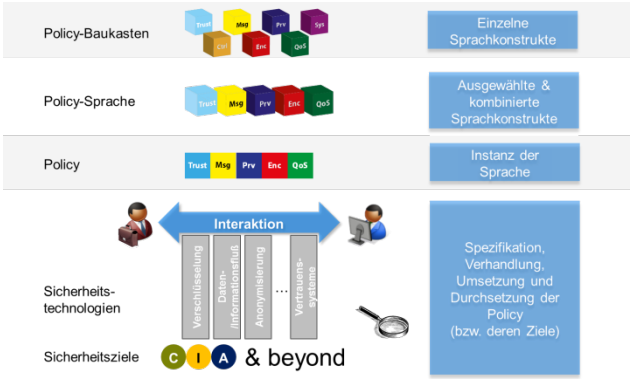
Neue Konzepte für identifizierte relevante Bereiche

- **Überwachung** von Prozessen in emergenter Geschäftssoftware
- **Informations-** und **Datenflusskontrolle** in unternehmensübergreifenden emergenten Prozessen
- **Leichtgewichtige Kryptographie** für robuste Interaktion
- **Vertrauens- und Reputationsmodelle** zur reliablen Komponentenauswahl in emergenten Diensten

- **Überführung der Konzepte in Technologien**
  - **Prototypen und Demonstratoren** zur Evaluation

Fortführung EMERGENT in InDiNet und SInDiUm

Software-Cluster



Ziele des AP Sicherheit in **EMERGENT**:

- Gewährleistung von Sicherheit in emergenter Unternehmenssoftware:
  - **Spezifikation**, **Refinement** und **Durchsetzung** von **Security-Policies** für emergente Software
  - Umfassendes **Monitoring**, **Enforcement** und **Management** (Secure Lifecycle)
  - Entwicklung von noch **fehlenden grundlegenden Sicherheitskonzepten** und –**technologien** zum Einsatz in emergenten Umgebungen

Fortführung in den Projekten InDiNet und SInDiUm

- **Praxisnahe Umsetzung** von Security-Policy-Durchsetzungsmechanismen
  - Geräteübergreifend (insb. Mobile Devices),
  - nutzbar,
  - flexibel und skalierbar im Vordergrund (‘as-a-Service’ und ‘pay-per-use’)

Software-Cluster

Vielen Dank!

GEFÖRDERT VOM

Bundesministerium
für Bildung
und Forschung