Exposé

Trust-Engineering

Methodik zur Entwicklung vertrauenswürdiger IT-Systeme und Geschäftsprozesse

TrustKBB GmbH

Version 02/2022

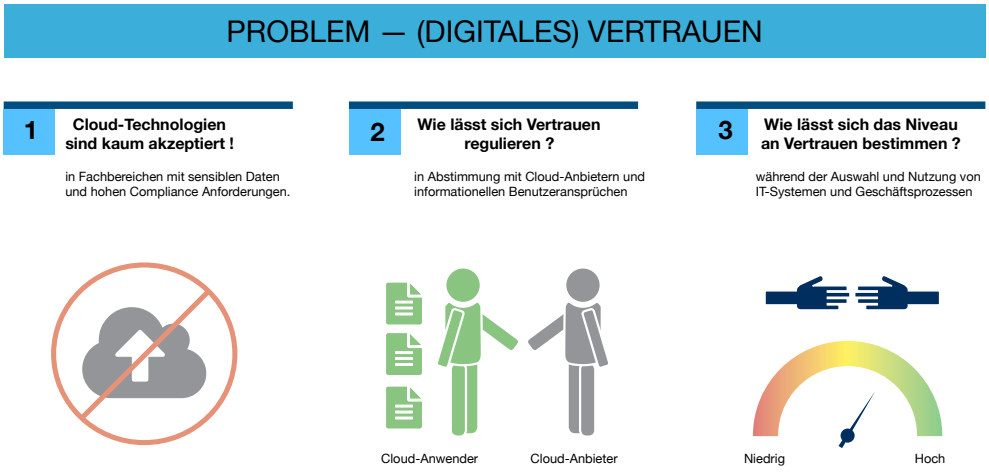
Trust K|B|B

Trust-Engineering

TrustEngineering beschreibt ein strukturiertes Vorgehensmodell, das sich als Spezialisierung aus dem Bereich der IT-Sicherheit herausgebildet hat. *Trust-Engineering* erweitert Sicherheitsarchitekturen um vertrauensbildende Konzepte überprüfbarer Zusicherungen (*TrustAssurance*) von Systemeigenschaften.

Vertrauen – Problem der Digitalisierung:

Das Thema IT-Sicherheit (*Cyber-Security*) wird als grundlegende Voraussetzung für vertrauenswürdige IT-Lösungen angesehen. Jedoch wird der Frage nach dem Grad an Vertrauen (*Trust*), wie IT-Sicherheit ganzheitlich und zuverlässig wirksam die gesetzten Ziele erfüllt, weniger Beachtung eingeräumt. Es besteht oft eine nicht ausgesprochene Annahme, dass mehr Sicherheit zwangsläufig die Bereitschaft zu mehr Vertrauen im Bereich digitaler Lösungen nach sich zieht.



Im Bereich sensibler Geschäftsprozesse zeigt sich immer noch eine große Zurückhaltung und auch Misstrauen, die Verarbeitung von Unternehmens-Assets, z.B. über Cloud- oder ähnliche digitale Technologien, abwickeln zu lassen.
Eines der großen Herausforderungen der Digitalisierung besteht darin, dass Anwender von Geschäftsprozessen in die Lage versetzt werden, um selbstbestimmt technische, sicherheits- und verhaltensbezogene Ansprüche auf digitale Prozessräume übertragen zu können. Gleichermaßen benötigen solche Strukturen vertrauensbildende Architekturelemente, um die zweifelsfreie und konforme Umsetzung solcher Ansprüche authentisch zu attestieren.

Vertrauen in digitale Identitäten:

Vertrauen in das Verhalten und die Qualität digitaler Identitäten ist Ausgangspunkt und zugleich Gegenstand von Trust-Engineering. Vertrauenswürdige digitale Identitäten legen den Grundstein für das Trust-Management komplexer digitaler Geschäftsprozesse. Identitäten, z. B. für natürliche Personen, unterteilen sich in:

- Attribute einer Person (z. B. persönliche, soziale, berufliche Eigenschaften)
- Biometrische Eigenschaften (z. B. Fingerbadruck, DNA-Muster, Iris- Merkmale)
- Besitz kryptographischer Schlüssel, die einer Person, z. B. für die vertrauliche Kommunikation, eindeutig zugeordnet sind

Wie lässt sich das Verhalten einer digitalen Identität zweifelsfrei einer natürlichen Person zuordnen?
Während der Ausführung digitaler Transaktionen $T(doc)$ attestiert ein Trustworthy-Assurance-Service (TAS) die sichere Bindung digitaler Identitätsmerkmale $ID(z)$ an eine natürliche Person *PA*. Digitale Transaktionen werden mit vertrauenswürdigen Identitäten in Form einer überprüfbaren Zusicherung kryptographisch verknüpft.

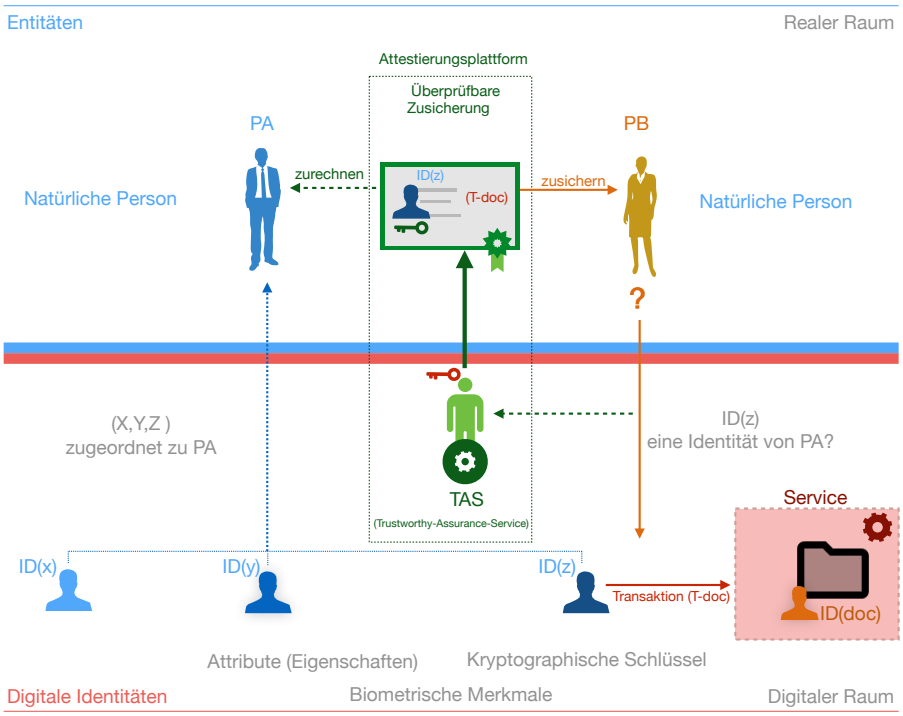


Abbildung 1: Prinzip einer überprüfbaren Zusicherung

Überprüfbare Zusicherungen führen z. B. bei der Person *PB* zur Gewissheit, dass eine konkrete digitale Identität $ID(z)$ fest an die natürlichen Person *PA* gebunden ist und eine identifizierte Transaktion dieser Person zweifelsfrei zugerechnet werden kann.

Formen vertrauenswürdiger Zusicherungen:

Für Entitäten aus unterschiedlichen Gesellschaftsbereichen (Sektoren) ist die Nutzung einer digitalen Identität als Repräsentant der eigenen Objektklasse gemeinsam. Natürliche Personen bilden nur eine Teilmenge. Ob Fahrzeuge, technische Systeme, Industrieprozesse, Informationen, jeder Objektbegriff repräsentiert sich über eine eigenständige digitale Identität.

Vertrauenswürdige Zusicherungen:

- sind überprüfbar, können im Nachgang nicht unerkannt verändert werden,
- schaffen für die Person *PB* Transparenz und Beweiskraft,
- Identitäten werden nicht-abstreitbar einer natürlichen Person *PA* zugeordnet,
- Die Zurechenbarkeit ausgeführter Transaktionen setzt einen Wert an Vertrauenswürdigkeit für die darin enthaltenen Aussagen

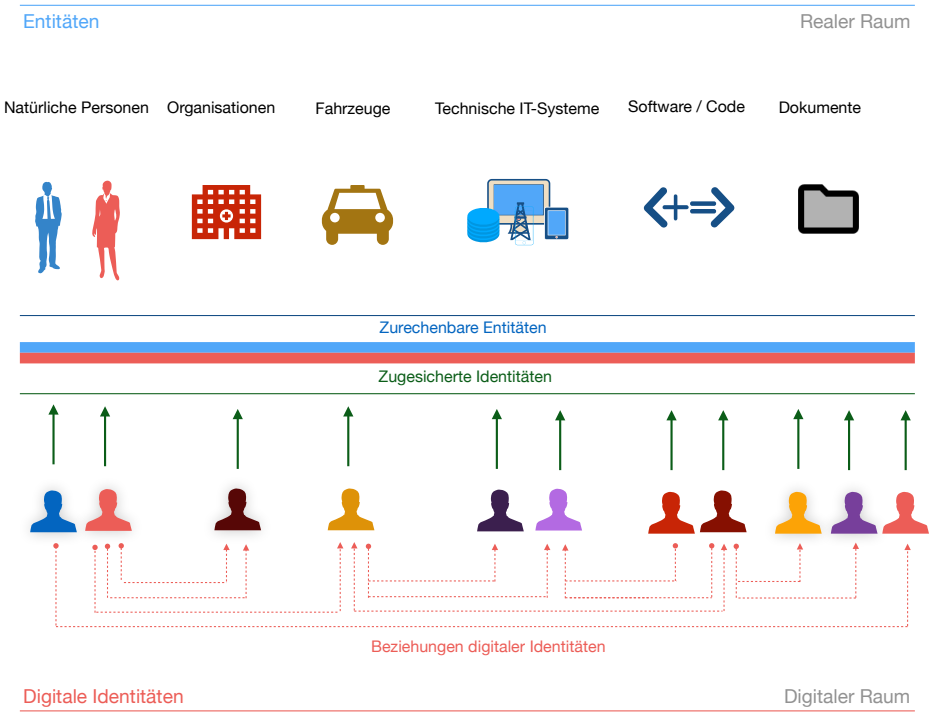


Abbildung 2: Digitale Identitäten repräsentieren Objekte der realen Welt

Trust-Engineering entwickelt Methoden, um Zusicherungen über digitale Identitäten, z. B. während der Ausführung sensibler Transaktionen, mit einem geforderten Vertrauensniveau

zu erzeugen und bereitzustellen.
Trust-Engineering setzt sich mit sektorspezifischen Zielen von Zusicherung auseinander und entwickelt integrierte Plattformen zur Attestierung gegenüber dem Anwender. Nachfolgend werden unterschiedliche Formen an Zusicherungen vorgestellt.

Autoindustrie: Erzeugung von Zusicherungen, dass Fahrzeuge (Fahrzeug-Identität) mit Systemkomponenten (Baugruppen-Identität) mit vorgegebenen Releaseversionen (Software-Identität) ausgestattet sind.

Die Zusicherungen attestieren die Bindung von Baustein- und Softwareeigenschaften an identifizierbare Systemkomponenten eines Fahrzeugs. Gleichzeitig erfolgt eine Bindung von technischen Identitäten an Prozessidentitäten (z. B. Testprozesse als Digitaler Twin), um eine UNECE Compliance nachzuweisen.

Technische Cloud-Client- und Serversysteme: Erzeugung von Zusicherungen darüber, dass z. B. Hardwarekomponenten von Client- und Serversystemen, bestehend aus Teilkomponenten und Softwarebausteinen der Firmware, Virtualisierungstechnologien, Betriebssystem und digitaler Applikationen mit vorgegebenen Sicherheits- und Technologieeigenschaften bestehen.

Die Zusicherungen attestieren die Vertrauenswürdigkeit von z. B. operativen Serversystemen in einem Rechenzentrum.

Organisationen: Vertrauenswürdige Zusicherungen kennzeichnen Bindungen einer Juristischen Person (z. B. einer GmbH) mit anderen juristischen Einheiten (Aufbaustruktur) und Identitäten natürlicher Personen (z. B. Mitarbeiter, Personal).

Entscheidungen: Im Bereich digitaler Geschäftsprozesse einer Organisation werden digitale Entscheidungen im Form nicht-abstreitbarer Zusicherungen eingebunden. Sie enthalten eine überprüfbare Bindung zwischen der verantwortlichen Akteursidentität und der Entscheidung selbst.

Software-Code: Die Authentizität, Aktualität und Unversehrtheit konkreter Softwarebausteine (Workloads) steht im Mittelpunkt der Zusicherung. Im Rahmen souveräner Cloud-Prozesse bilden vertrauenswürdigen Zusicherungen den Rahmen einer regulierter Software- bzw. Service- Life-Cycle-Prozesse.

Digitales Schriftgutobjekte: Im behördlichen, ressortübergreifenden Informationsaustausch kennzeichnen Zusicherungen die Bindungen von Schriftgut-Identitäten an konkrete digitale Informationen (Content). Die Bindungen von Schriftgutobjekten an vertrauenswürdige Identitäten einer Organisation ist Aufgabe von spezifischen Zusicherungen über des Bestand einer Organisationen (z. B. Bindung einer E-Akte-an eine Organisation).

Vertrauensanker (Root-of-Trust)

Die Entwicklung von Vertrauen benötigt als Grundlage einen unveränderlichen und eindeutig identifizierbaren Zustand (*Root-of-Trust*). Aufbauend auf einer *Root-of-Trust* leiten sich weitere vertrauenswürdige Zustände ab, die zu einer einer Zustandskette (*Chain-of-Trust*) kryptographisch verknüpft werden.

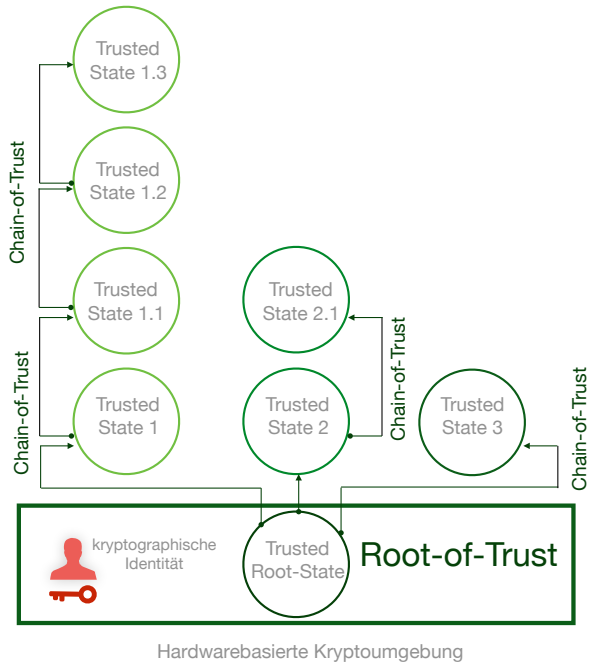


Abbildung 3: Prinzip einer Root-of-Trust

Eine *Root-of-Trust* für digitale Systeme wird technisch über hardwaregebundene Kryptographie erzeugt. Die Bindung an Hardware garantiert die Erzeugung einer eindeutigen, nicht kopierbaren, kryptographischen Identität. Gegen äußere Kompromittierungen dieser Identität bietet die Hardwareumgebung einen definierten Schutz.
In Bezug auf die Attestierung von Eigenschaften entsteht in horizontaler Richtung mit jeder weiteren Zusicherung ein neuer verlinkter *Trusted State* (z. B. State1, State2, State3). Werden bereits vollzogene Zusicherungen (Zustände) in eine neue Zusicherung mit eingebunden, so entwickelt sich eine Vertrauenskette in vertikaler Richtung (z. B. State2, State2.1).

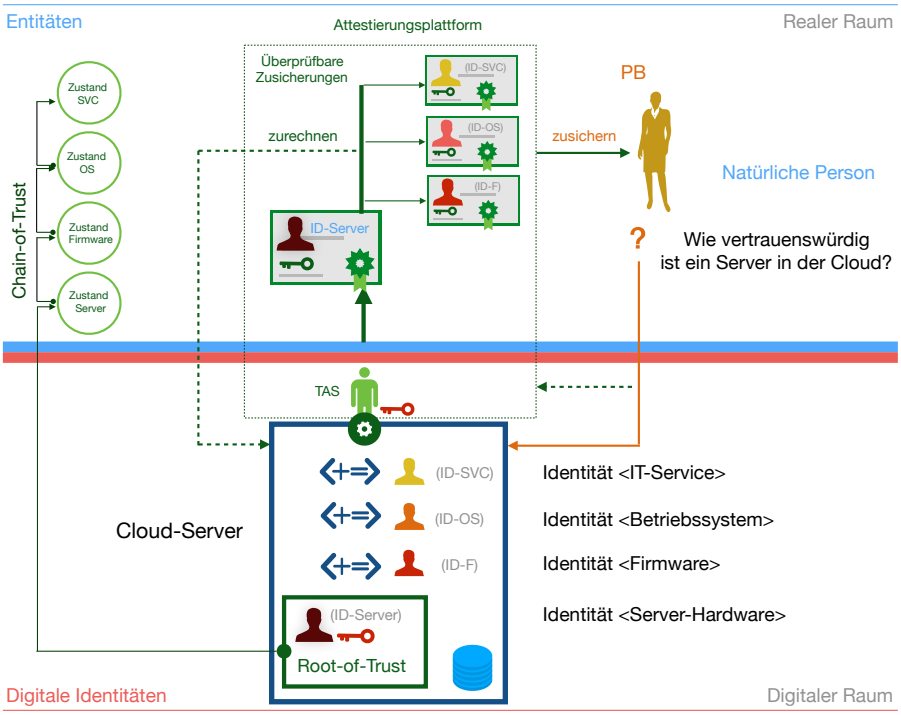
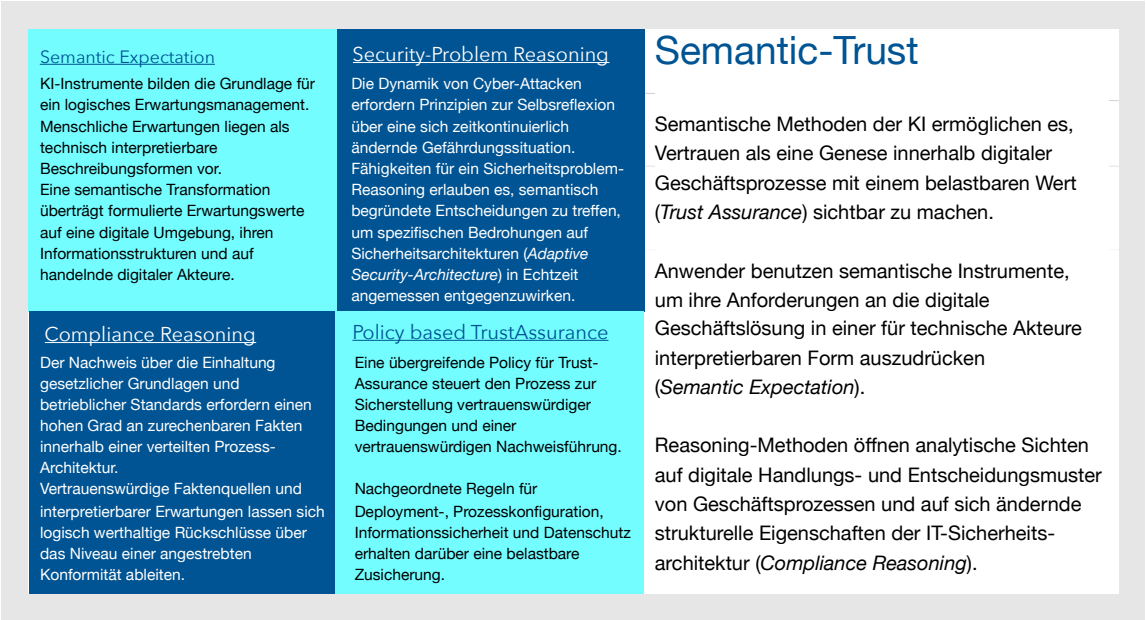


Abbildung 4: Zusicherung vertrauenswürdger Server-Eigenschaftesn

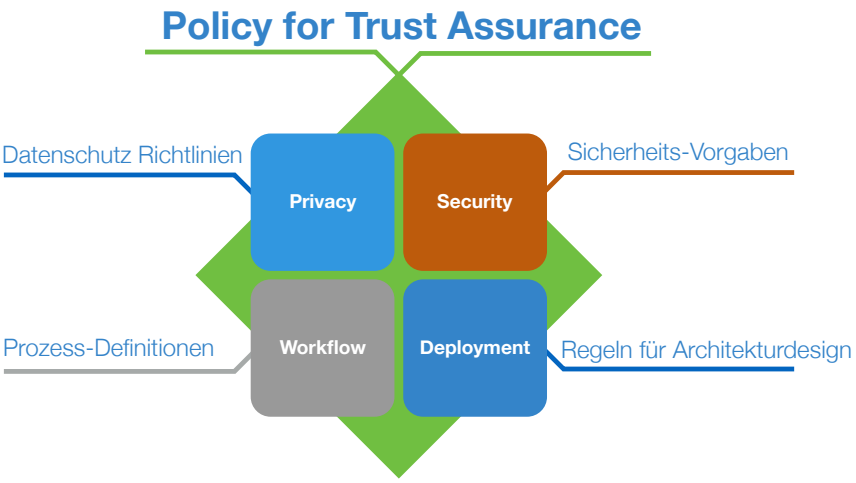
Im Prozess der Attestierung von Grundeigenschaften eines Cloud-Servers entwickelt sich eine Vertrauenskette bestehend aus verknüpften Zuständen erhobener Systemeigenschaften. Ein Zustand wird kryptographisch aus den zum Zeitpunkt gemessenen Systemeigenschaften, z. B. einer identifizierten Systemkomponente, berechnet und in einer *Chain-of-Trust* verlinkt.
Die Authentizität einer Zusicherung führt auf den TAS zurück und ist überprüfbar.
Jedes identifizierbare Teilsystem lässt sich einer Entität, z. B. Softwareversion der Firmware (ID-F) zuordnen. Die Vertrauenskette beginnt mit der *Root-of-Trust*. Ein TAS übernimmt Messungen der integrierten Einzelidentitäten und überträgt eine vertrauenswürdige Zusicherung an die Attestierungsplattform.

SemanticTrust – Regulierungsinstrument für digitales Vertrauen

KI-basierte Methoden (*SemanticTrust*) erweitern Infrastrukturen für Geschäftsprozesse für die Nutzung eines durchgehenden *Trust-Engineerings*. Erwartungen der Anwender (*Requirements*) an Lösungen und die Gewissheit ihrer Umsetzung (*Confidence*) sind aus der sozialen Welt abgeleitete Grundprinzipien für die Entwicklung von Vertrauen.



SemanticTrust transformiert diese Grundprinzipien auf die Entwicklung von digitalen Geschäftsprozessen. Jede Ebene zur Bereitstellung von Prozessbedingungen (z.B. Workflow, Deployment, Security) wird in Bezug auf gesetzte Erwartungswerte analysiert und über vertrauenswürdige Elemente sichergestellt und rückgespiegelt.



Für eine ganzheitliche regulative Erzeugung und Bereitstellung vertrauenswürdiger Grundbedingungen (*Policy of TrustAssurance*) stellt *SemanticTrust*, als ein KI-basiertes methodisches Framework, die notwendigen Methoden und Infrastrukturerweiterungen bereit.

Erweiterte Eigenschaften von Sicherheitsarchitekturen:

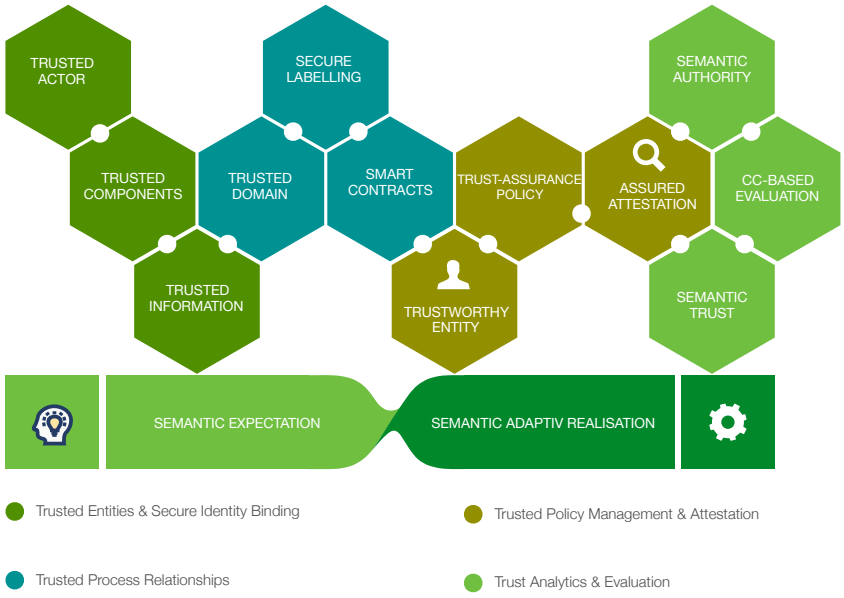
vertrauenswürdig

Die Zusicherung, dass komplexe Geschäftsprozesse konform ausgeführt werden, stützt sich auf ein erweitertes Konzept digitaler Vertrauenspunkte. Sämtliche Nachweise von

Aktivitäten sowohl zur Prozessbereitstellung als auch ihrer schrittweisen Ausführung (*Audit*) stützen sich auf eine zurechenbare Faktenbereitstellung.

semantisch-analytisch
Geschäftsprozesse sind auf Grundlage zurechenbarer Fakten einer kontinuierlichen Analyse unterzogen (*SIEM*). Semantische KI-Bausteine erlauben eine kontinuierliche Schlussfolgerungsfähigkeit und Bewertung in Bezug auf gesetzte Erwartungswerte (*Policies*).

Beratungsgegenstand und Leistungsbausteine: Trust-Engineering berücksichtigt alle Elemente einer Sicherheitsarchitektur. Die Leistungsbausteine beschäftigen sich mit der vertrauensbildenden Zusicherung, das Eigenschaften und Verhaltensformen erfüllt sind.



Semantic Expectation
Mit Methoden von SemanticTrust entwickelt sich eine neue Form zur vollständigen Beschreibung von Anforderungen. Es bildet das strategische Element zur Ausrichtung und qualifizierten Ausprägung von digitalen Lösungen.

Semantic Adaptiv Realisation
SemanticTrust mit seinem KI-gestützten Infrastrukturrahmen überführt logikbasierte Erwartungen über einen Transformationsprozess in reale, vertrauenswürdige IT-Infrastrukturen und Prozesslösungen.