

TeleTrust-EBCA "PKI-Workshop" 2026

Berlin, 08.10.2026

Agentic AI braucht mehr als IAM: Warum PKI der erste Schritt zu einer echten Vertrauensinfrastruktur ist

Andreas Philipp, Dietmar Kopp, SITS

Agenda

- **Ausgangslage**

Digitale Identität im Kontext Agentic AI

Wir behandeln ein Vertrauensproblem wie ein Berechtigungsproblem

- **Identitätsmodell**

Rolle und Grenzen von X.509 im Kontext Agentic AI

Vier Ebenen der Agentenidentität

Wie bekommen KI Agenten eine sicherer kryptografische Identität?

Signierte Agent Cards und Tool-Manifeste

A2A, MCP und ACP lösen die Vertrauensfrage nicht allein

- **Einordnung nach kryptografischer Funktion**

- **ANS · AGENT NAME SERVICE**

- **Zusammenfassung**

Digitale Identität im Kontext Agentic AI

Autonome Agenten handeln über APIs, Clouds und Tools. Statische Secrets liefern dafür zu wenig Sicherheit und Verantwortlichkeit.

1

Autonomes Handeln

Agenten greifen selbstständig auf kritische Systeme und Ressourcen zu.

2

Kurzlebige Instanzen

Auch ein Agent für nur eine Aktion braucht eine eindeutige Identität.

3

Vertrauen

Wie kann ich dem Agenten Vertrauen, kann der Agent der Quelle Vertrauen,

4

Delegiertes Handeln

Agenten handeln im Namen eines Benutzers, Dienstes oder Principals.

4

Multi-Agent-Ketten

Vertrauen und Autorisierungen müssen über mehrere Delegationsstufen erhalten bleiben.

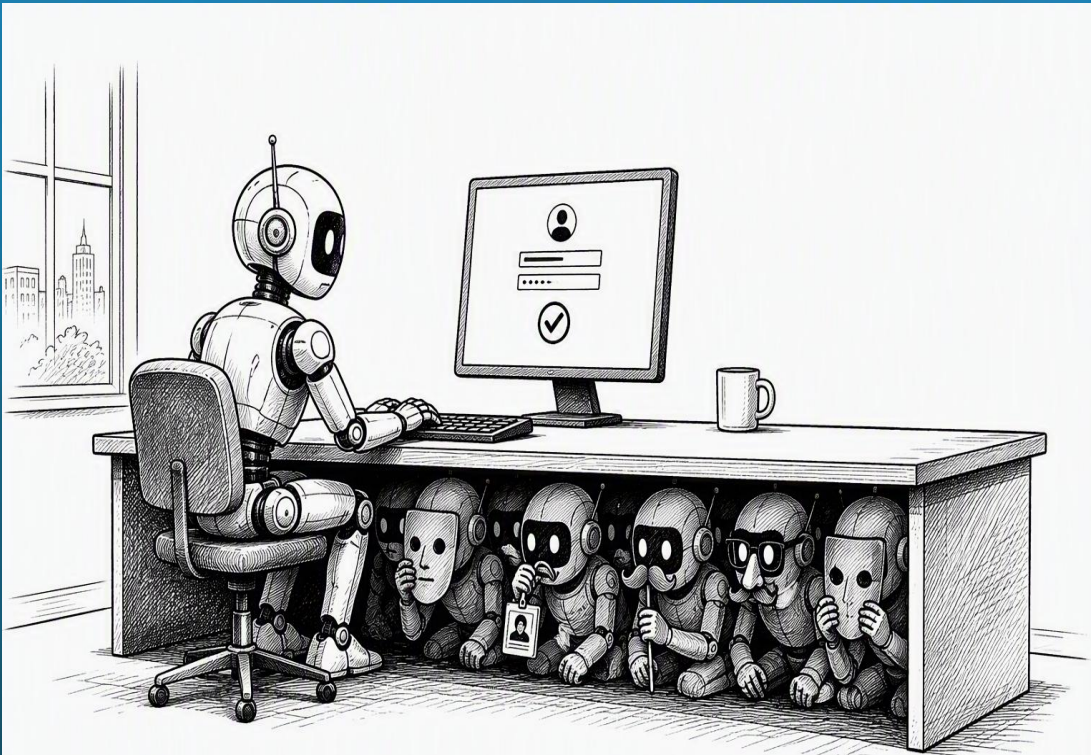


Wie wird jede Aktion eindeutig einem Agenten zugeordnet?

Wir behandeln ein Vertrauensproblem wie ein Berechtigungsproblem

IAM kontrolliert Zugriff.

Ohne verifizierbare Identität, Herkunft und Integrität kann es jedoch nicht entscheiden, wem es diese Rechte tatsächlich anvertraut.



"On the Internet, nobody knows if you're an AI agent."

- 1 Agent bekommt Berechtigung**
Rolle, Scope, token und Policy sind vorhanden
- 2 Vertrauen bleibt implizit**
Agente, Tool, Herkunft, und Laufzeit werden nicht belastbar verifiziert
- 3 Legitime Rechte werden missbraucht**
Prompt injection, kompromittierte Tools, kopierte Credentials täuschen gültige Berechtigungen vor.

Aktuelle Verweise:

- ISACA: White Papers 2026 Cybersecurity Recommendations for Securing AI Agents
- Mandiant-Report: Prompt Injection bleibt ein zentraler Angriffsvektor; gefordert werden klar identifizierte und adaptive Identitätskontrollen.

Ein Vertrauenslayer für Agentic AI entsteht

Erste Initiativen, Konzepte arbeiten daran, Identität, Herkunft und Vertrauensnachweise für autonome KI-Agenten interoperabel zu machen.

01

Verifizierbare
Agentenidentität

02

Nachweisbare
Herkunft &
Integrität

03

Interoperable
Vertrauenssignale



Rolle und Grenzen von X.509 im Kontext Agentic AI

Ein Zertifikats-Subject oder ein Agentenname darf nicht mit der vollständigen fachlichen Autorisierung gleichgesetzt werden. Discovery, Authentisierung und Autorisierung bleiben getrennte Funktionen.

Was X.509 leistet

Authentisierung der Gegenstelle

Schutz und Authentisierung des Transportkanals über mTLS

Bindung von Public Key, Name und Attributen im Zertifikat

Vertrauenskettens und kryptographisch prüfbare Signaturen

Automatisierte kurzlebige Maschinenidentitäten

Was X.509 nicht alleine leistet

Feststellung des Fachlichen Auftraggebers

Entscheidung welche Tools, Daten und Aktionen erlaubt sind

Bewertung der Software-, Modell- oder Laufzeitintegrität ohne Attestation

Steuerung von Delegation und Subdelegation

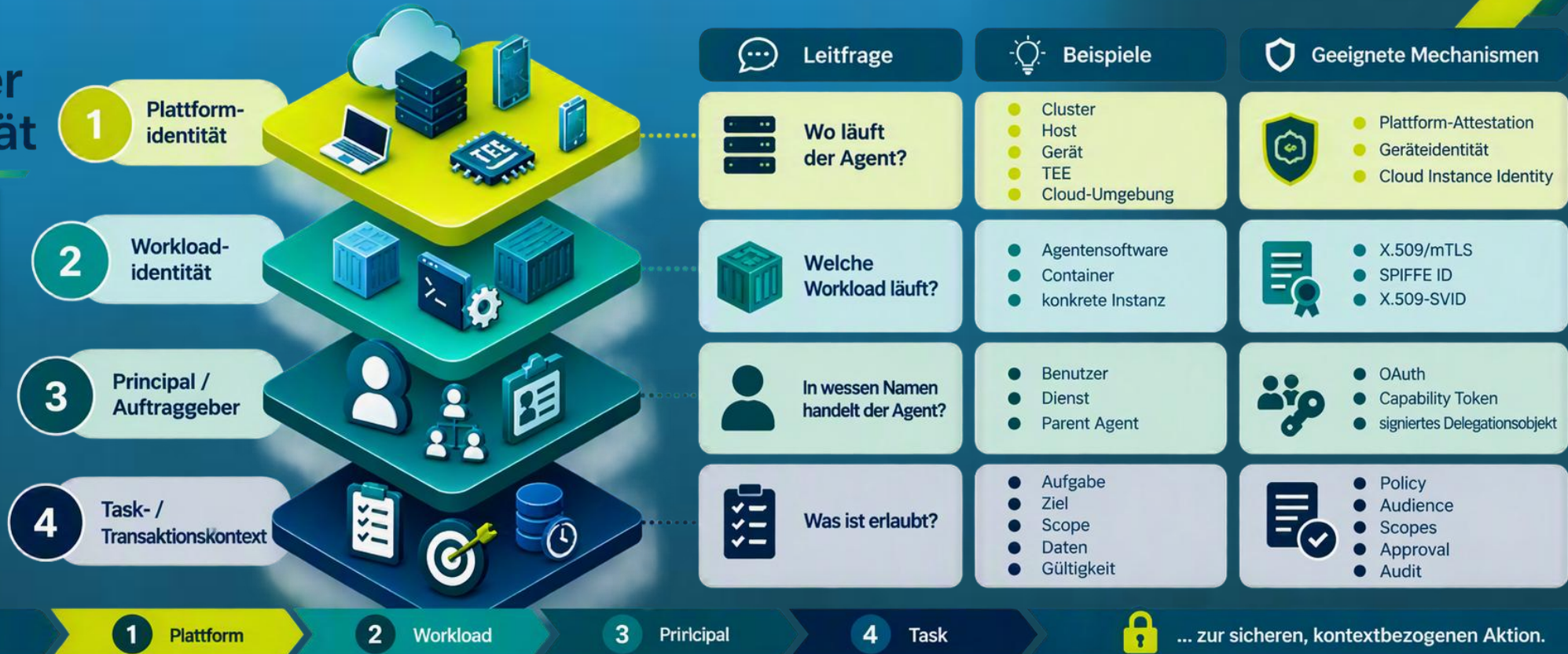
Vollständige Transaktions- und Auditkontext

Vier Ebenen der Agentenidentität

Vier Ebenen der Agentenidentität

Ein Agent hat nicht nur eine Identität – sondern vier Ebenen.

Jede Ebene beantwortet eine andere Frage und ermöglicht es, Agenten eindeutig zu identifizieren, zu verwalten und sicher zu steuern.



Vom Untergrund ...

Wie bekommen KI Agenten eine sicherer kryptografische Identität?



Signierte Agent Cards und Tool-Manifeste

Digitale Signaturen binden maschinenlesbare Beschreibungen an einen überprüfbaren Herausgeber.



A2A, MCP und ACP lösen die Vertrauensfrage nicht allein

Discovery, Authentisierung und Autorisierung bleiben getrennte technische Funktionen.



Ein Agentenname oder ein Zertifikat darf diese drei Funktionen nicht semantisch vermischen.

Einordnung nach kryptografischer Funktion

Die Ansätze liegen auf unterschiedlichen Ebenen und sind deshalb nicht direkt austauschbar.

Kryptografische Funktion	Mechanismus / Technologie	Einsatz bei Agentic AI
Kanal authentisieren	X.509 + mTLS	Agent↔Agent, Agent↔Tool und Agent↔API
Schlüsselbesitz nachweisen	Digitale Signatur / Proof of Possession	Request- und Token-Bindung
Zertifikate ausstellen und rotieren	ACME, EST oder CMP	Dynamische Agenten- und Plattformidentitäten
Workloadidentität bereitstellen	SPIFFE/SPIRE und X.509-SVID	Kurzlebige, attestierte Agenteninstanzen
Auftrag delegieren	Schlüsselgebundene OAuth- oder Capability-Token	Handeln im Namen eines Principals
Metadaten sichern	Signierte Agent Card / Tool-Manifest	Herkunft, Fähigkeiten und Endpunkte
Namen und Zertifikat binden	DNSSEC / DANE; ANS als Beispiel	Organisationsübergreifende Discovery
Lebenszyklus nachweisen	Transparency Log	Registrierung, Historie und Versionierung

Agent Name Service

Vertrauen auf dem Daten-Highway



ANS
Agent Name Service
Identität · Discovery · Vertrauen

Vertrauensschicht
Identität prüfen

Daten-Highway
Sicher · Offen · Standardisiert

Gemeinsam unterwegs
Menschen & Agenten

APIs
↑

Daten
↑

Services
↓

Ich kenne dich.
Du darfst.

Mensch
Mara Hoffmann ✓
 Mitarbeiterin
 Projektleiterin

Agent
DataAnalyst-01 ✓
 Analyse
 Reporting
 API-Zugriff

Agent
CustomerSupport-02 ✓
 Support
 Kommunikation
 Datenabruf



ANS • AGENT NAME SERVICE

Ein offener, DNS-inspirierter Infrastruktur-Standard, der KI-Agenten eine überprüfbare, kryptografisch gesicherte Identität verleiht,



ANS • AGENT NAME SERVICE

Agenten müssen organisationsübergreifend auffindbar sein und veröffentlichte Metadaten überprüfbar an eine Identität binden.



Rollen und kryptografische Prüfpunkte

Die Architektur verbindet Registry, Registration Authority, Certificate Authority und Protokolladapter.



Mehrschichtige Verifikation

Die Vertrauensstufen kombinieren die CA-basierte Prüfung mit DNS- und Transparency-Nachweis.



ZUSAMMENFASSUNG UND EINSCHÄTZUNG



Fazit

Sicherheit, die mitdenkt.

Vom automatisierten Zertifikat zur kontinuierlich attestierten, kurzlebigen und auftragsgebundenen Agentenidentität.



Vertrauenswürdig



Automatisiert



Skalierbar



Zukunftssicher

Kontakt Daten:



Dietmar Kopp

Product Manager & Senior Solution Architect



dietmar.kopp@sits.com



+41 55 220 64 32



Andreas Philipp

Head of Applied Crypto – Business Development



andreas.philipp@sits.com



+49 241 4468801