Certified By GS1 – PKI

Inhalt

Certified By GS1 USP

Bei der ID Vergabe teilt GS1 einem Unternehmen mit der Basisnummer ("Company Prefix") einen Namensraum zu, in welchem das Unternehmen dann selbst IDs vergeben kann. Parallel hierzu ermöglicht ein Unternehmenszertifikat mit Basisnummer Certified By GS1 dem Unternehmen selbst Zertifikate für die eigenen IDs zu erstellen. Diese grundlegende Idee ist in Bild 1 dargestellt.

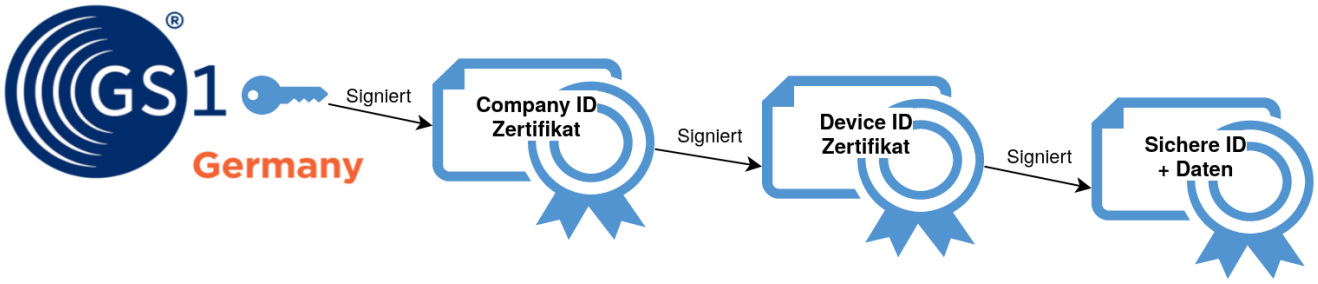

Bild 1. Die Vertrauenswürdigkeit von Zertifikatsketten kann ausgehend vom Wurzelzertifikat überprüft werden

Mit dem Unternehmenszertifikat kann die Echtheit der eigenen IDs fälschungssicher nachgewiesen und offline überprüft werden, d.h. es kann z.B. überprüft werden, dass eine SGTIN tatsächlich von dem Unternehmen erzeugt wurde, dem die zugehörige Basisnummer gehört, ohne das ein online Lookup in einer entsprechenden Datenbank nötig wäre. Auch Eigenschaften des mit der ID gekennzeichneten Assets können z.B. über die GS1 Standards in z.B. einen 2d Code wie die Datamatrix kodiert und deren Vertrauenswürdigkeit offline verifiziert werden.

Abgeleitete ID-spezifische Zertifikate sind besonders im IoT Kontext interessant, da Maschinen sich mit einer solchen ID Certified By GS1 selbst ausweisen können. Mittels etablierter kryptografischer Verfahren können Maschinen sich basierend auf dem Certified by GS1 System gegenseitig überprüfen und so eine gesicherte Verbindung untereinander oder auch über das Internet z.B. zu Cloud Diensten herstellen, wie in Bild 2 dargestellt.

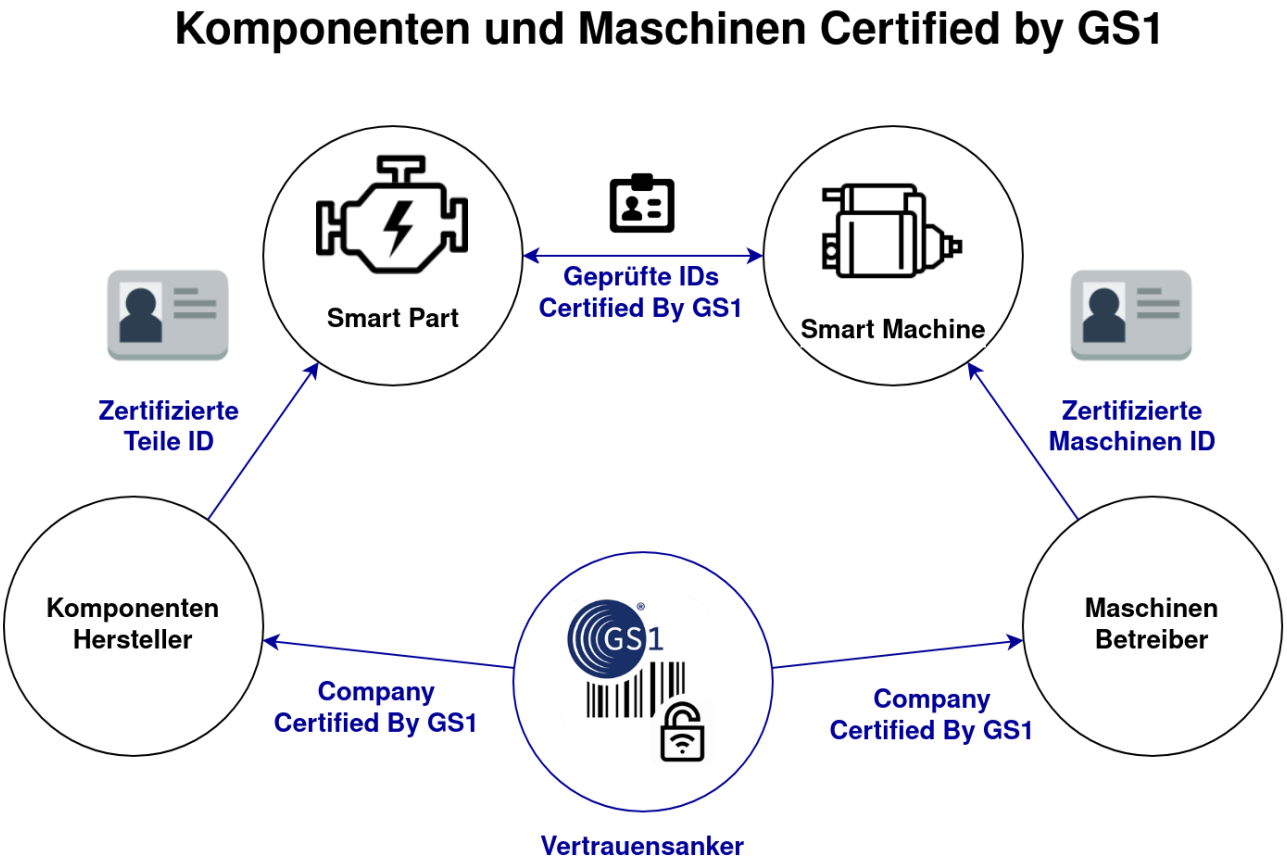

Bild 2. Vertrauen in IDs certified by GS1 ermöglicht M2M authentifizierung und den Aufbau gesicherter Kommunikationskanäle

Basierend auf digital zertifizierten Identitäten kann, genau wie bei der gängigen Verschlüsselung der Kommunikation über das Internet, ein gesicherter Kommunikationskanal aufgebaut werden. So können z.B. Messdaten oder Steuerbefehle übertragen werden, ohne dass diese von dritten gefälscht werden können.

Umsetzung

Arbeitspakete

Use Case:

- Angriffszenarios/Mehrwerte klar darstellen
- Vorteile von Certified
- Vergleich mit existierenden Lösungen

Technisch:

- X.509 Zertifikatsstruktur (Welche Key/Values genau werden verwendet)
- GS1 Wurzelzertifikat Prototyp: Handling/Prozesse/Sicherheitsfragen für Demo Phase definieren
- Prozesse (digital/analog)

Demonstrator:

- Was genau kann innerhalb der Projektlaufzeit fertig gestellt und gezeigt werden?
- Mock Up von Teilen?
- Weiterführung zum Prototyp, evtl. sogar MVP?

Umsetzung mit EKU Power Drives

- https://www.ekupd.com

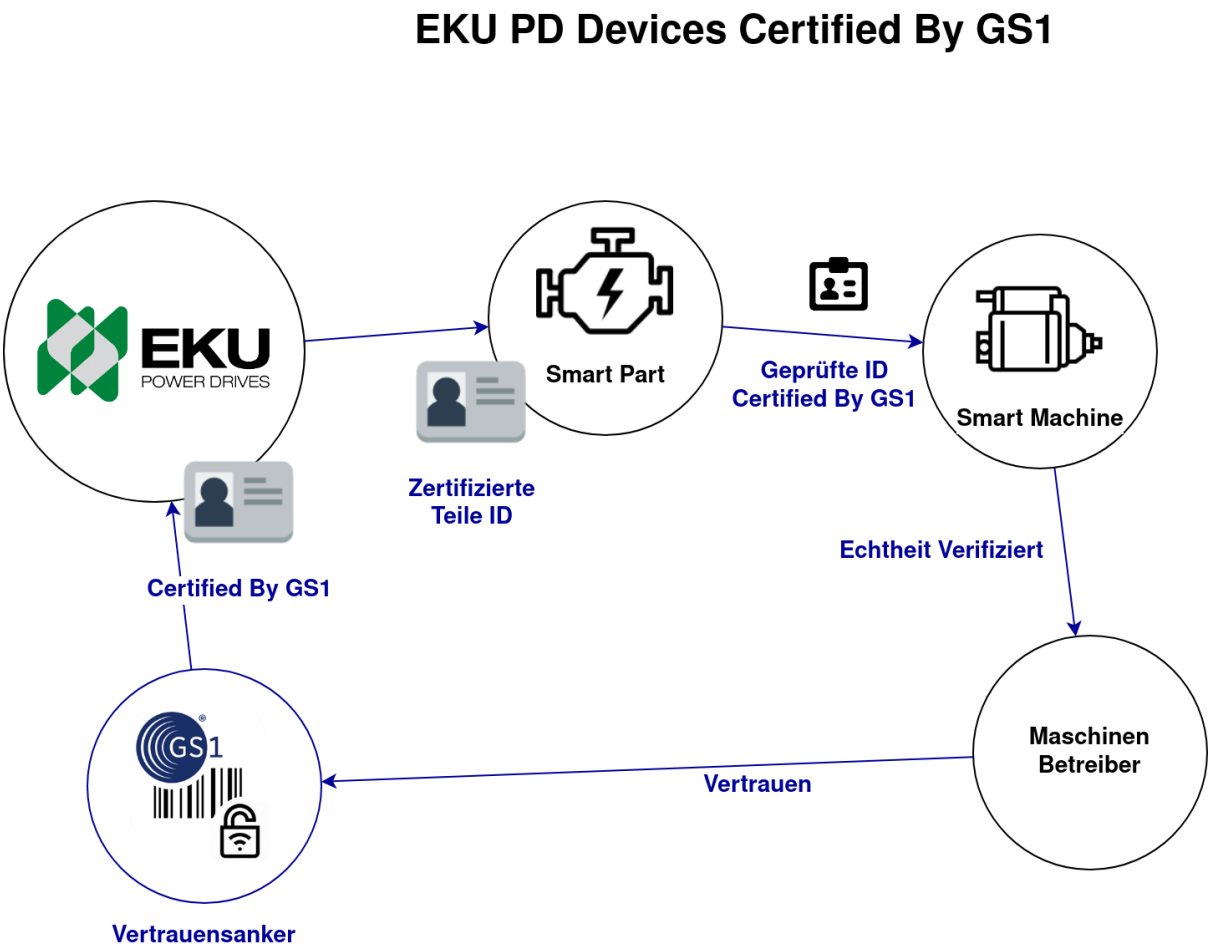

Bild 3. Concreter EKU PD Use Case