

ICS 35.030; 35.240.50

Anforderungen und Referenzarchitektur eines Security Gateways zum Austausch von Industriedaten und Diensten

Requirements and reference architecture of a security gateway for the exchange of industry data and services

Architecture de référence pour un portail de sécurité pour l'échange de données et de services relatifs à l'industrie

Zur Erstellung einer DIN SPEC können verschiedene Verfahrensweisen herangezogen werden:
Das vorliegende Dokument wurde nach den Verfahrensregeln einer PAS erstellt.

Gesamtumfang 26 Seiten

Koordinierung DIN SPEC

Inhalt

	Seite
Vorwort	3
Einleitung	5
1 Anwendungsbereich.....	6
2 Normative Verweisungen	6
3 Begriffe	6
4 Security-Gateway-Zielarchitektur und Kommunikationsstruktur	8
4.1 Allgemeines	8
4.2 Architekturen für den Datenaustausch.....	8
4.3 Infrastruktur, in die das Security Gateway eingebettet sein soll.....	9
4.4 Architektur des Security Gateway.....	11
4.5 Security-Gateway-Profil.....	12
5 Das Konzept der Security-Level nach IEC 62443	12
5.1 Allgemeines	12
5.2 Sicherheitslevel und Sicherheitsprofile	13
5.3 Struktur der Sicherheitsanforderungen nach IEC 62443	13
6 Anforderungen an das Security Gateway.....	14
6.1 Allgemeines	14
6.2 Anforderungen an den Entwicklungsprozess	15
6.3 Anforderungen an das Security Gateway nach IEC 62443.....	16
6.4 Zusätzliche Anforderungen	19
6.4.1 Allgemeines	19
6.4.2 Kommunikationssicherheit.....	20
6.4.3 Kontrolle über Datenflüsse.....	21
6.4.4 Unterstützung eines gemeinsamen Informationsmodells	22
6.4.5 Identitäts- und Zugriffsmanagement	23
6.4.6 Anbindung an einen Brokerdienst.....	23
6.4.7 Betriebssystemsisicherheit.....	24
6.4.8 Apps und Anbindung an einen App Store	25
6.4.9 Nachvollziehbarkeit von Datennutzung.....	26

Vorwort

Diese DIN SPEC wurde nach dem PAS-Verfahren erarbeitet. Die Erarbeitung von DIN SPEC nach dem PAS-Verfahren erfolgt in DIN SPEC (PAS)-Konsortien und nicht zwingend unter Einbeziehung aller interessierten Kreise.

Die Erarbeitung und Verabschiedung des Dokuments erfolgten durch die nachfolgend genannten Initiator(en) und Verfasser:

Andreas Teuscher, SICK AG

Gerd Brost, Fraunhofer AISEC

Uwe Brettner, nicos AG

Martin Böhmer, Fraunhofer IML

Bastian Fraune, Hochschule Bremen

Christian Haas, Fraunhofer IOSB

Tina Hardt, AREND Prozessautomation GmbH

Benjamin Heidenreich, GESIS Gesellschaft für Informationssysteme mbH

Christian Jung, Fraunhofer IESE

Lutz Jänicke, Phoenix Contact Deutschland GmbH

Markus Ketterl, msg systems AG

Jörg Langkau, nicos AG

Nadja Menz, Fraunhofer FOKUS

Mykolai Protsenko, Fraunhofer AISEC

Christoph Sanders, admeritia GmbH

Marius Schmeding, Cybus GmbH

Florian Schönberg, GESIS Gesellschaft für Informationssysteme mbH

Richard Sethmann, Hochschule Bremen

Sebastian Steinbuß, International Data Spaces Association

Sascha Wessel, Fraunhofer AISEC

Für dieses Thema bestehen derzeit keine Normen im Deutschen Normenwerk. DIN SPEC (PAS) sind nicht Teil des Deutschen Normenwerks.

Für diese DIN SPEC (PAS) wurde kein Entwurf veröffentlicht

Trotz großer Anstrengungen zur Sicherstellung der Korrektheit, Verlässlichkeit und Präzision technischer und nicht-technischer Beschreibungen kann das DIN SPEC (PAS)-Konsortium weder eine explizite noch eine implizite Gewährleistung für die Korrektheit des Dokuments übernehmen. Die Anwendung dieses Dokuments geschieht in dem Bewusstsein, dass das DIN SPEC (PAS)-Konsortium für Schäden oder Verluste jeglicher Art nicht haftbar gemacht werden kann. Die Anwendung der vorliegenden DIN SPEC (PAS) entbindet den Nutzer nicht von der Verantwortung für eigenes Handeln und geschieht damit auf eigene Gefahr.

Es wird auf die Möglichkeit hingewiesen, dass einige Elemente dieses Dokuments Patentrechte berühren können. DIN ist nicht dafür verantwortlich, einige oder alle diesbezüglichen Patentrechte zu identifizieren.

Die kostenfreie Bereitstellung dieses Dokuments als PDF-Version über den Beuth WebShop wurde im Vorfeld finanziert.

Einleitung

Durch die zunehmende Digitalisierung und die Transformation von rein physischen Produkten zu virtuellen Produkten und Dienstleistungen erschließen sich Unternehmen neue Geschäftsmodelle, in denen Daten als Wirtschaftsgut verwertet werden. Bei einem Datenaustausch in einem unternehmensübergreifenden Daten- und Diensteraum, wie beispielsweise dem International Data Space (IDS), haben die Datensicherheit und Datensouveränität eine hohe Priorität. Das Security Gateway, welches als Einstiegspunkt in einen sicheren, unternehmensübergreifenden Daten- und Diensteraum dient, unterstützt einen sicheren Datenaustausch mit anderen Security Gateways sowie Datendiensten (Apps), um eine vertrauenswürdige Verarbeitung von Daten zu ermöglichen. Mit der Architektur kann die Verlässlichkeit erhöht werden, dass die von einem Datenbereitsteller festgelegten Nutzungsbedingungen eingehalten werden (Datensouveränität) und dass IT-Sicherheitsfunktionen wie Isolation (Datendienste können sich nicht unzulässig gegenseitig beeinflussen), Attestation (Bestätigung eines sicheren, vertrauenswürdigen Zustands), Authentisierung sowie sichere Verarbeitung und Kommunikation aufeinander abgestimmt realisiert sind.

1 Anwendungsbereich

Dieses Dokument definiert drei Profile von Anforderungen an Security Gateways für einen unternehmensübergreifenden Daten- und Diensteraum. Diese ermöglichen einen geschützten Austausch von Industriedaten unter Einhaltung der Datensouveränität und die Realisierung von vertrauenswürdigen Datendiensten auf einem Security Gateway.

Das Security Gateway für einen unternehmensübergreifenden Daten- und Diensteraum adressiert Industrien aus unterschiedlichen vertikalen Domänen wie Finanzindustrie, Gesundheitsindustrie, IT-Industrie, Telekommunikationsindustrie, Logistik und Industrie 4.0 / Industrial Internet.

Anforderungen an andere Elemente der vorausgesetzten Kommunikationsarchitektur, d. h. den unternehmensübergreifenden Daten- und Diensteraum, wie App Store, Clearingstelle oder Broker werden in diesem Dokument nicht gestellt. Die in diesem Dokument definierten Anforderungen betreffen technische Eigenschaften eines Security Gateways für einen unternehmensübergreifenden Daten- und Diensteraum, nicht jedoch Anforderungen an den Entwicklungsprozess, die Herstellung oder den sicheren Betrieb.

2 Normative Verweisungen

Die folgenden Dokumente werden im Text in solcher Weise in Bezug genommen, dass einige Teile davon oder ihr gesamter Inhalt Anforderungen des vorliegenden Dokuments darstellen. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

DIN EN IEC 62443-4-2:2019-12, *IT-Sicherheit für industrielle Automatisierungssysteme — Teil 4-2: Technische Sicherheitsanforderungen an Komponenten industrieller Automatisierungssysteme (IACS)*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

DIN und DKE stellen terminologische Datenbanken für die Verwendung in der Normung unter den folgenden Adressen bereit:

- DIN-TERMinologieportal: verfügbar unter <https://www.din.de/go/din-term>
- DKE-IEV: verfügbar unter <http://www.dke.de/DKE-IEV>

3.1

Security-Level

Schutzstufe, nach der eine Komponente ausgelegt ist

Anmerkung 1 zum Begriff: Aus den Security-Leveln leiten sich auch die Angreifergruppen ab, gegen die eine Komponente abgesichert ist.

3.2

Sicherheitsprofil

Festlegung der Sicherheitsmerkmale eines Security Gateways in mehreren Dimensionen

Anmerkung 1 zum Begriff: Dies sind zum Beispiel Isolation der Komponenten untereinander, sichere Datenübertragung oder die Fähigkeiten zum manipulationssicheren Audit Logging.

3.3

Gateway

Netzwerkkomponente, welche die Verbindung zwischen verschiedenen Netzwerksegmenten herstellt

Anmerkung 1 zum Begriff: Es befindet sich typischerweise an der Unternehmensgrenze nach außen und definiert damit die Schnittstellen nach außen. Die Unternehmensgrenze ist hier logisch zu verstehen, das heißt, das Security Gateway kann sowohl in Räumen des Unternehmens als auch in Räumen oder Anlagen eines Dienstleisters implementiert sein.

3.4

Security Gateway

Gateway, das Security-Funktionalitäten bereitstellt

Anmerkung 1 zum Begriff: Dieses Dokument stellt 3 verschiedene Profile für ein solches Security Gateway zur Verfügung.

3.5

Broker

Dienst zum Auffinden von Datenquellen

Anmerkung 1 zum Begriff: Während bei vielen nachrichtenbasierten Systemen ein Broker die Nutzdaten verteilt, dient der Broker im Verständnis dieses Dokumentes zur Vermittlung von Metadaten über angebotene Dienste.

3.6

Identity Provider

Dienst, der die Identitätsattribute einer Entität beglaubigt

Anmerkung 1 zum Begriff: Damit belegt dieser die Identität von Komponenten und Diensten und deren Eigenschaften. Dies kann beispielsweise durch eine klassische Certification Authority (CA) erfolgen und durch einen Dienst zur Beglaubigung dynamischer Attribute erweitert werden.

3.7

App Store

Vertriebsplattform für digitale Softwarekomponenten, die in Form von Containern zum Herunterladen zur Verfügung stehen

3.8

App

Anwendung, die digitale Dienste bereitstellt, die in einem Container mit allen notwendigen Abhängigkeiten und Metadaten verpackt ist

Anmerkung 1 zum Begriff: Diese Anwendung bietet in der Regel Datendienste an, um beispielsweise Datenströme zu verarbeiten.

3.9

Container

Getrennt auslieferbares, in einem Security Gateway installierbares und lauffähiges Softwareartefakt

Anmerkung 1 zum Begriff: Durch den Einsatz von Containern ist ein Security Gateway in der Lage, die Prozesse und den Datenverkehr zu isolieren und diese unabhängig voneinander zu betreiben. Dieser mandantenfähige Ansatz unterbindet unbefugten Zugriff auf Funktionen und Daten von anderen Apps.

4 Security-Gateway-Zielarchitektur und Kommunikationsstruktur

4.1 Allgemeines

In diesem Abschnitt wird die angedachte Datenaustauscharchitektur beschrieben, die Datenaustauschinfrastruktur und die Zielarchitektur des Security Gateways selbst. Detaillierte Entscheidungen über Feinstrukturen der Architektur bzw. die spätere Implementierung ergeben sich aus den in Abschnitt 5 definierten Anforderungen und sollen hier nicht vorgegeben werden.

Die Datenaustauscharchitektur beschreibt die Topologie der kommunizierenden Knoten. Die Infrastruktur beschreibt notwendige zentrale Komponenten. Die Zielarchitektur beschreibt das Security Gateway selbst. Die später definierten Anforderungen dienen dazu, um bei Anbietern und Konsumenten Mindestsicherheitsanforderungen wie z. B. die Authentizität der Teilnehmer, eine verschlüsselte und integritätsgeschützte Kommunikation und Kontrolle über die Nutzung der Daten sicherzustellen.

4.2 Architekturen für den Datenaustausch

Konzeptionell unterstützen Security Gateways den Datenaustausch in unterschiedlichen Netzwerktopologien oder Infrastrukturen.

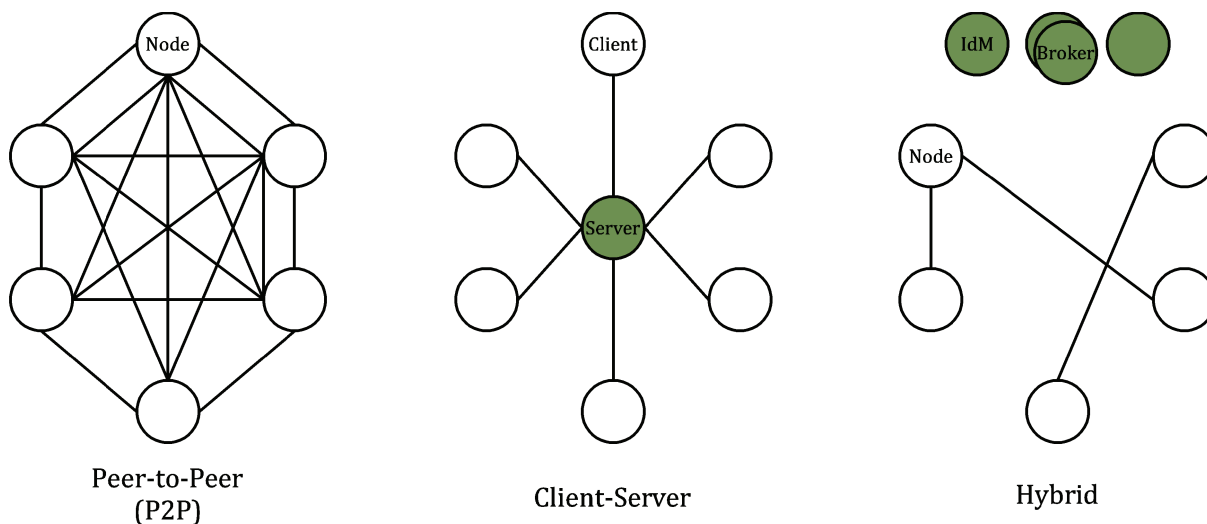


Bild 1 — Schema für Datenaustauschstrukturen

Bei reinen Peer-to-Peer-Architekturen finden sich mitunter voll vermaschte Netzstrukturen. Clients sind untereinander gleichgestellt und dienen sowohl als Client als auch Server. In reinen Peer-to-Peer-Netzen ist keine zentrale Infrastruktur notwendig. In der klassischen Client-Server-Topologie sind die Rollen strikt getrennt und es kommunizieren alle Clients mit zentralen Servern. In hybriden Infrastrukturen können alle Netzknoten sowohl Server als auch Client sein. Es wird hier allerdings auf zentrale Infrastrukturkomponenten zurückgegriffen. Die später beschriebenen Konzepte wie Broker, Identity Provider und App Store sind solche Komponenten. Diese können zwar von unterschiedlichen Betreibern angeboten werden und parallel existieren, doch sind sie für den Betrieb notwendig und üben eine gewisse Kontrolle aus.