CASE STUDY

LOGISTIK

SEKTOR

DIE HERAUSFORDERUNG

Mobile Endgeräte spielen eine wichtige Rolle bei der Datenübermittlung. Angesichts des Datenschutzes ist es unerlässlich, geeignete Maßnahmen zur Verschlüsselung einzusetzen. Bei der Entscheidung für eine verschlüsselte E-Mail-Kommunikation ist in diesem Case Study die Wahl auf S/MIME gefallen.

Die stetig steigende Nutzung von Mobilgeräten erfordert dringend eine Verschlüsselungslösung. Dieser Logistik-Konzern bevorzugt für die Bereitstellung der Zertifikate eine maßgeschneiderte Lösung. Hierbei wird das Zertifikat verschlüsselt und per E-Mail an den Empfänger versendet. Das Passwort zur Entschlüsselung des Zertifikats wird an die App übermittelt. Dieses Vorgehen gewährleistet, dass der private Schlüssel der Zertifikate ausschließlich auf dem Endgerät gespeichert wird.

Eine Public Key Infrastructure (PKI) zur Generierung von Zertifikaten war vorhanden. Es sind jedoch wichtige Anpassungen notwendig, damit die neue Lösung für mobile Endgeräte reibungslos funktioniert.

TECHNOLOGIE & METHODEN

SPRING BOOT · KOTLIN · OPENAPI · INTELLI-J IDEA · JUNIT SPRING SECURITY · OIDC · JWT · OAUTH2 · GITLAB CI/CD · DOCKER · KUBERNETES · OPENSHIFT · POSTMAN · JMETER

DIE LÖSUNG

Die Middleware wurde als Spring Boot Projekt umgesetzt. Wichtig bei der Umsetzung ist die Validierung des Authentifizierung Tokens. Nur ein authentifizierter Nutzer soll in der Lage sein, ein Zertifikat für die Verschlüsselung zu beantragen. Nach Abschluss der Entwicklung der grundlegenden Funktionalität des S/MIME Brokers für die Beantragung von E-Mail-Zertifikaten wurde ein umfassender Penetrationstest (PEN-Test) durch ein externes Unternehmen durchgeführt. Das Ziel des PEN-Tests bestand darin, potenzielle Sicherheitslücken oder Schwach-stellen in der Middleware aufzudecken. Bereits im ersten Durchlauf des PEN-Tests wurde der S/MIME Broker ohne jegliche Be-funde als sicher eingestuft. Dies ist ein Zeugnis für die sorgfältige Entwicklung und Implementierung der Middleware, bei der Sicherheitsaspekte von Anfang an berücksichtigt wurden. In einer späteren Phase wurden Optimierungen eingeführt, um die Leistung der Middleware zu verbessern. Dazu gehören Maßnahmen wie die Parallelisierung sowie Minimierung der Anfragen an die PKI sowie externe APIs, um die Netzwerk-belastung zu reduzieren und die Antwort-zeiten zu optimieren. Zudem wurden Optimierungen für spezielle Anwendungsfälle implementiert, um die Effizienz und Zuverlässigkeit der Middleware in verschiedenen Szenarien zu gewährleisten.

STARKRAFT

TECHNOLOGY | CONSULTING | ENGINEERING