

## SUCCESS STORY:

### ZWEITER AUTHENTIFIZIERUNGSFAKTOR SCHÜTZT DIGITALE LOGINS BEI SCANIA

#### Sicherheit auf dem neuesten Stand der Technik – Scania erweitert Identity- und Access-Management für Mitarbeiter

Scania gehört zu den weltweit führenden Anbietern von Transportlösungen. Das über 125 Jahre alte Traditionsunternehmen mit Sitz im schwedischen Södertälje produziert Lkw und Busse, die für unterschiedliche Transportaufgaben genutzt werden. Des Weiteren umfasst das Angebot von Scania Industrie- und Schiffsmotoren, die in zahlreichen Transport- und Industrieanwendungen im Einsatz sind, von Radladern über Patrouillenbooten bis hin zu Notstromaggregaten. Zusätzlich zu seinen hochentwickelten Transport- und Motorenlösungen bietet Scania seine Kunden ein umfangreiches Serviceangebot, das unter anderem Werkstattleistungen, Finanzierungs- und Versicherungslösungen sowie Fahrtrainings und Support-Dienstleistungen umfasst. Im Rahmen seines weltweiten Vertriebs- und Servicenetzes ist Scania mit rund 46.000 Mitarbeitern in 100 Ländern präsent.

Ergänzend zu seinem Kerngeschäft engagiert sich Scania für die Entwicklung nachhaltiger Transportsysteme und zukunftsweisender Mobilitätslösungen. So arbeitet der Fahrzeugspezialist eng mit strategischen Partnern zusammen, um das Transportwesen durch innovative Technologien wie Fahrzeugvernetzung oder die Optimierung der Energieeffizienz smarter und umweltfreundlicher zu machen.

**SCANIA**

- **Einsatzbereich:**  
Authentifizierung von Mitarbeitern im Außendienst und im Homeoffice
- **Lösung:**  
KeyIdentity MFA-Plattform
- **Token:**  
SMS- und Software-Token
- **Implementierung:**  
Erstimplementierung im Mai 2015, Erweiterung in 2017
- **Vorteile:**  
höhere Sicherheit, Bedienungsfreundlichkeit, Skalierbarkeit, reibungslose Erweiterung, Kosteneffizienz; Erfüllung von Compliance-Standards

## Einhaltung strenger Compliance-Vorgaben

Für Scania stehen stets die Kunden und ihre Sicherheit im Vordergrund: Dies bedeutet zum einen, dass alle Scania Fahrzeuge und Transportlösungen höchste Standards in Sachen Verkehrssicherheit und Zuverlässigkeit erfüllen müssen. Zum anderen hat es sich das Unternehmen zum Ziel gesetzt, alle Compliance-Vorgaben und insbesondere Datenschutz-Regularien wie die EU-Datenschutz-Grundverordnung (EU-DSGVO) einzuhalten. Um dies zu gewährleisten, überprüft und aktualisiert Scania regelmäßig all seine IT-Sicherheitsmechanismen inklusive seines Identity- und Access-Managements (IAM). Die Identitäts- und Zugriffsverwaltung sorgt dafür, dass nur die berechtigten User durch eine strenge Authentifizierungs- und Autorisierungskontrolle auf die Applikationen und Systeme im Unternehmen zugreifen können. Im Zuge ihres Security-Updates hat die Scania Deutschland GmbH am Standort Koblenz unter anderem auch ihre Multi-Faktor-Authentifizierung (MFA) ausgeweitet, mit der das Unternehmen den Zugriff auf seine Virtual Private Networks (VPNs) schützt.

## Sicherer Zugriff auf VPN-Verbindungen

Die VPN-Verbindungen ermöglichen es den Scania Mitarbeitern im vertrieblichen oder technischen Außendienst sowie im Homeoffice, jederzeit sicher über webbasierte Anwendungen auf Kunden- und Unternehmensdaten zuzugreifen. Damit die VPN-Nutzung stets unter Einhaltung der strengen Compliance-Vorgaben geschieht, hat sich Scania entschieden, den Einsatz seiner MFA-Lösung von KeyIdentity auszubauen.

## Zweiter Authentifizierungsfaktor schützt digitale Logins

Die SMS- und App-basierten Token fungieren im Rahmen der MFA-Lösung als jeweils zweite Faktoren. Damit muss der Nutzer einen zusätzlichen Berechtigungsnachweis unabhängig vom ersten Faktor – dem Passwort oder dem Login-Code – erbringen, bevor eine VPN-Verbindung aufgebaut werden kann. Denn Passwörter allein schützen digitale Identitäten heute nicht mehr ausreichend. Dem „Data Breach Investigations Report“ von Verizon zufolge waren gestohlene oder verlorene Passwörter im Jahre 2017 sogar in 80 Prozent aller Fälle die Ursache für Datendiebstähle oder Hacks. Durch die Multi-Faktor-Authentifizierung wird dieses Risiko ausgeschlossen. Denn selbst wenn potenzielle Angreifer ein Passwort erbeutet haben, befindet sich der zweite Faktor ausschließlich im Besitz des berechtigten Nutzers.

”

„Wir setzen bereits seit 2015 die Multi-Faktor-Authentifizierungslösung von KeyIdentity erfolgreich ein. Aufgrund von Compliance-Vorgaben haben wir uns dazu entschlossen, die Anzahl unserer User deutlich zu erweitern – von etwa 50 auf über 1.000. Wir setzen dabei zu etwa 98 Prozent auf eine Authentifizierung per SMS und zu zwei Prozent auf eine App-basierte Ausgabe des Einmal-Passworts“

**Michael Zimmer**  
Teamleiter IT Operations  
Scania Deutschland GmbH

Aufgrund des hohen Sicherheitsniveaus empfehlen sowohl das Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch der Bundesverband IT-Sicherheit e.V. (TeleTrust) die Technologie. Wenn sie sich für den Aufbau der VPN-Verbindung einloggen, erhalten die Scania Mitarbeiter automatisch ein sogenanntes Einmal-Passwort – oder auch One-Time-Password (OTP) – per SMS oder App-Benachrichtigung auf ihr Smartphone. Sie müssen dieses nur noch als zusätzliche Komponente innerhalb des Authentifizierungsvorgangs eingeben und erhalten dadurch Zugang zur VPN-Verbindung.

## Einfach zu nutzen und flexibel erweiterbar

„Unsere Mitarbeiter konnten die Multi-Faktor-Authentifizierung reibungslos in ihre Arbeitsabläufe integrieren. Sie agieren damit bei jedem Login deutlich sicherer als zuvor und ermöglichen uns, die strengen Compliance-Vorgaben auch wirklich einzuhalten. Dafür müssen sie sich kein zusätzliches Passwort merken und können sich somit voll und ganz auf ihre Aufgaben konzentrieren. Dies war uns besonders wichtig, denn für höchstmöglichen Datenschutz und IT-Sicherheit müssen wir mit unseren Kolleginnen und Kollegen an einem Strang ziehen. Daher wollten wir ihnen den Einsatz der MFA-Lösung auch so einfach wie möglich machen“, so Michael Zimmer von Scania weiter. „Die MFA-Lösung ließ sich dank des API-first-Ansatzes von KeyIdentity schnell und einfach erweitern. Durch die Smart-Features der Lösung wie ein Auto-Assignment der Token oder eine Auto-Synchronisierung wird der Aufwand in unserem User-Helpdesk erheblich reduziert. Gleichzeitig steigt damit einmal mehr die Gesamtakzeptanz und die Zufriedenheit der Nutzer.“

Die MFA-Technologie von KeyIdentity erfüllt nicht nur alle aktuell geltenden Sicherheitsstandards und ist einfach einsetzbar. Sie lässt sich darüber hinaus flexibel skalieren und problemlos erweitern. Auch das Rollout weiterer Token-Typen wie Push-, OR- oder Hardware-Token ist damit ohne großen Zusatzaufwand denkbar. Ein weiterer Vorteil: KeyIdentity entwickelt und aktualisiert seine Security-Technologie von Anfang bis Ende in Deutschland. Damit ist gewährleistet, dass der gesamte Einsatz und Support nach strengem deutschen Datenschutz geschieht und selbst neueste Regularien wie die EU- DSGVO eingehalten werden. Scania ist damit in der Lage, die hohen Sicherheitsanforderungen für seine Kunden optimal und auf dem neuesten Stand der Technik umzusetzen.

”

*„Die MFA-Lösung ließ sich dank des API-first-Ansatzes von KeyIdentity schnell und einfach erweitern. Gleichzeitig haben wir durch die Smart-Features des IAM-Systems kaum Support-Aufwand für die Verwaltung der sicheren Login-Lösung auf MFA-Basis.“*

**Michael Zimmer**  
Teamleiter IT Operations  
Scania Deutschland GmbH

### Über KeyIdentity

KeyIdentity ist ein führender Anbieter von hoch skalierbaren, einfach einsetzbaren Identity- und Access-Management-Lösungen (IAM) auf Open-Source-Basis für die Absicherung und Verwaltung digitaler Identitäten über Netzwerk- und Cloud-Umgebungen. Der Fokus von KeyIdentity liegt auf den Bereichen Transaktionssicherheit, Identitätsmanagement und der starken Authentifizierung mittels Multi-Faktor-Authentifizierung (MFA).

Die IAM-Lösungen von KeyIdentity werden von Anfang bis Ende in Deutschland entwickelt und bereitgestellt und erfüllen höchste Sicherheitsstandards nach deutschem Recht. Durch den Open-Source-Ansatz lassen sich zudem kryptografische Backdoors ausschließen. KeyIdentity bietet seit 2002 „Security made in Germany“ und hat seinen Sitz in Weiterstadt bei Darmstadt.

[www.keyidentity.com](http://www.keyidentity.com)