D 14749 F

BARCODE
DRUCKER
RFID / NFC
MOBILE IT
SENSORIK
KENNZEICHNUNG
LOGISTIKSOFTWARE

31. Jahrgang
Nr. 3/2026

ident

Das Magazin für Automatische Identifikation & Digitalisierung

Zukunftsfähigkeit sichern

So modernisieren Sie Ihre Zutrittskontrolle ohne Betriebsunterbrechungen

ident.de

Zukunftsfähigkeit sichern: So modernisieren Sie Ihre Zutrittskontrolle ohne Betriebsunterbrechungen

Jason Ouellette
VP, Innovation and Tech Partnerships

ELATEC GmbH
Zeppelinstr. 1
82178 Puchheim
www.elatec-rfid.com

In Logistik- und Distributionszentren sowie Produktionsstätten verrichten Zugangssysteme meist unbemerkt ihren Dienst – bis es zu Ausfällen kommt. Seit Jahrzehnten ist die 125-kHz-Karte (Low-Frequency-Karte) das Herzstück der industriellen Zugangsberechtigung: kostengünstig, zuverlässig und allgemein etabliert. Diese Beständigkeit hat vielen Unternehmen gute Dienste geleistet, auch wenn sich die Sicherheitsanforderungen und Erwartungen an die Credentials (Berechtigungsnachweise) ständig weiterentwickelt haben.

Die gleiche Kartentechnologie, die 2005 das Lagertor öffnete, öffnet es auch heute noch. Während Betriebsteams in der Zwischenzeit Förderbänder, ERP-Systeme und Lagerverwaltungsplattformen modernisiert haben, basiert die Zutrittskontrolle häufig noch auf einer völlig veralteten Technologie. Woran liegt das? Selten mangelt es an Problembewusstsein. Vielmehr wägen Unternehmen Kosten, Zeitaufwand und Betriebsrisiken sorgfältig ab. In einer Anlage, die rund um die Uhr läuft, wirkt eine systemweite Modernisierung weniger wie ein Routineprojekt und mehr wie ein massiver betrieblicher Einschnitt. Der Weg in die Zukunft liegt daher in der kontinuierlichen Modernisierung: Ziel ist es, eine agile Ebene für die Zutrittskontrolle zu schaffen, die sich im Laufe der Zeit an neue Sicherheitsanforderungen, Credentials und Authentifizierungstechnologien anpassen lässt, anstatt das gesamte System auf einen Schlag auszutauschen. Universelle Lesegeräte machen genau das möglich und ersparen Unternehmen einen radikalen Umbruch.

Was moderne Zutrittskontrolle blockiert

Eine herkömmliche Modernisierung der Zutrittskontrolle ist mehr als nur ein Technologiewechsel. Sie erfordert neue Lesegeräte an jeder Tür, neue Credentials für alle Mitarbeitenden und Dienstleister, eine Neukonfiguration der Plattform sowie Installationsarbeiten – und das in Anlagen, die sich keinen Stillstand leisten können. Vor diesem Hintergrund erscheint es oft als die sicherste Entscheidung, vorerst nichts zu unternehmen. Gleichzeitig sehen sich Sicherheitsteams mit einer wachsenden Bedrohungslandschaft und strengeren Compliance-Anforderungen konfrontiert,

die zwingend verschlüsselte Credentials erfordern. Da zudem Apple Wallet-Firmenausweise und BLE-Mobile-Credentials zunehmend zum Standard werden, erwarten Nutzer künftig, ihr Smartphone als Ausweis nutzen zu können – zumindest als Alternative, wenn nicht gar als primäres Identifikationsmittel.

„Modernisierung muss als fortlaufender Prozess und nicht als einmaliges Ereignis verstanden werden. Ein schrittweiser Plan ist sowohl einfacher als auch kostengünstiger als ein radikales „Rip-and-Replace"-Projekt"

Es gibt vier konkrete Hürden, die Unternehmen oft von einer Modernisierung abhalten:

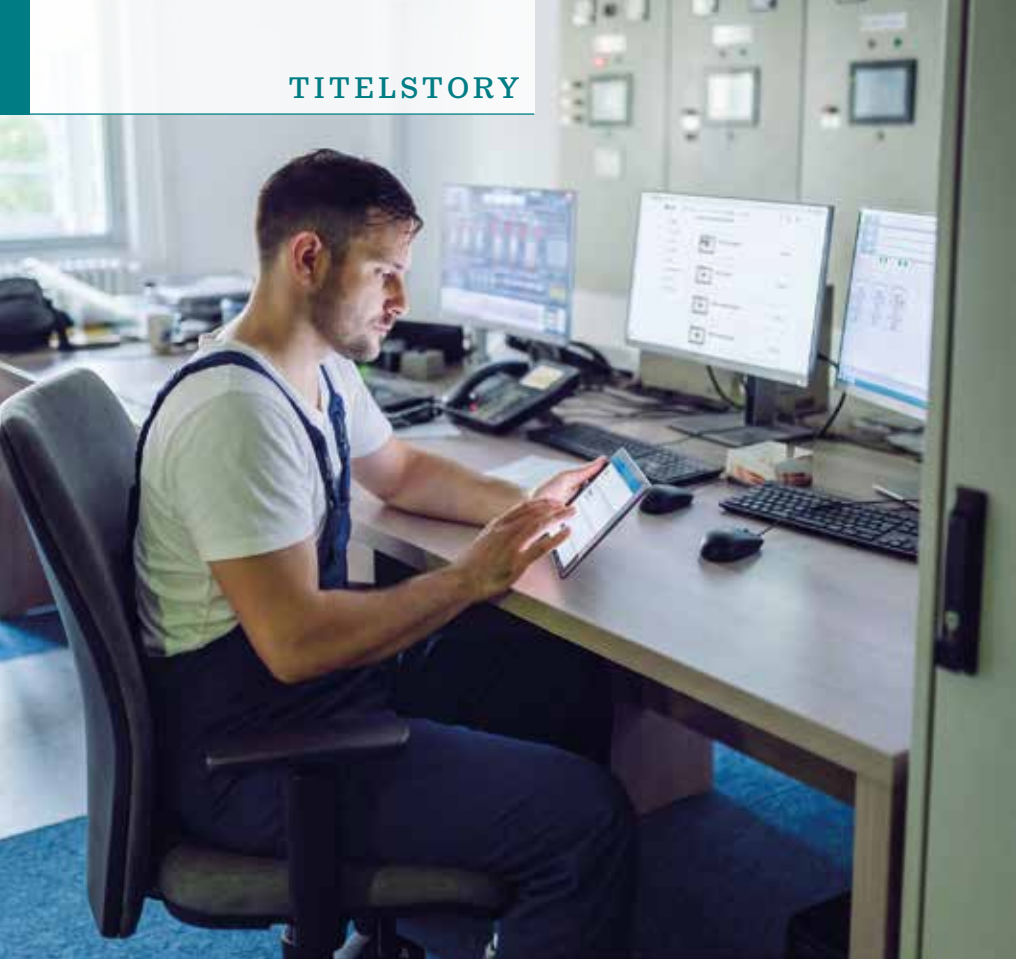
1. Der logistische Engpass: Der Austausch eines Low-Frequency-basierten Systems bedeutete traditionell einen harten Schnitt: neue Lesegeräte, neue Ausweise, eine neue Plattformkonfiguration und die Neuregistrierung aller Mitarbeitenden und Dienstleister vor dem Stichtag. Für einen Standort, der rund um die Uhr in Betrieb ist und über zahlreiche Mitarbeiter sowie wechselnde Auftragnehmer verfügt, ist das ein logistischer Albtraum, der oft eine vollständige Abschaltung erfordert. Allein die Neuausstellung der Credentials für Hunderte oder Tausende Personen in einem engen Zeitfenster kann die Personal- und Sicherheitsabteilungen wochenlang binden.

2. Der Credential-Dschungel: In den meisten Logistikunternehmen gibt es keine einheitliche Credential-Struktur. Oft sind drei oder vier verschiedene Systeme parallel im Einsatz: ein altes 125-kHz-System für die Stammbelegschaft, ein anderes Format aus einer Firmenübernahme, ein fremdverwaltetes System für Dienstleister und ein mobiles Pilotprojekt, das nie flächendeckend ausgerollt wurde. Diese Systeme kommunizieren nicht miteinander und kein einzelnes Lesegerät unterstützt alle Formate.

Warum ältere Systeme an ihre Grenzen stoßen

Die 125-kHz-Karte (Low-Frequency) hat lange Zeit den Standard für Benutzerfreundlichkeit und breite Kompatibilität definiert. Heute prüfen jedoch viele Organisationen, wie sie ihr Sicherheitsmodell durch moderne Alternativen verbessern können:

- **Erhöhter kryptografischer Schutz:** Herkömmliche Low-Frequency-Credentials übertragen lediglich eine unverschlüsselte Identifikationsnummer. Dies wird den heutigen Anforderungen an eine verschlüsselte und dynamische Authentifizierung nicht mehr gerecht.
- **Verbesserte Validierung:** Herkömmliche 125-kHz-Systeme bieten keine gegenseitige Authentifizierung (Mutual Authentication) oder Challenge-Response-Mechanismen, wie sie bei modernen Credential-Plattformen zunehmend üblich sind.
- **Besserer Schutz vor Duplizierung:** Aufgrund ihrer einfachen Datenstruktur sind Low-Frequency-Karten leicht zu kopieren. Moderne, verschlüsselte Credentials sind hingegen gezielt darauf ausgelegt, autorisierte Nutzer zuverlässig von geklonten Ausweisen zu unterscheiden.
- **Absicherung der gesamten Kommunikationskette:** Viele ältere Installationen nutzen noch das unverschlüsselte Wiegand-Protokoll für die Kommunikation zwischen Lesegerät und Controller. Eine Modernisierung auf verschlüsselte und überwachte Protokolle (wie OSDP) ist geboten, um die Credentials auch während der Datenübertragung zu schützen.
- **Interoperabilität bewahren:** Moderne offene Standards bieten dieselben Vorteile bei der Interoperabilität wie die bewährte Low-Frequency-Technik, gewährleisten dabei aber ein deutlich höheres Sicherheitsniveau.



3. Veraltete Infrastruktur: Statische Lesegeräte unterstützen oft nur die Ausweisformate, mit denen sie ursprünglich ausgeliefert wurden, oder bieten kaum Update-Möglichkeiten. Wird eine neue Sicherheitslücke entdeckt oder ein neuer Mobile-Standard eingeführt, lässt sich die Hardware nicht anpassen. Die einzige Lösung ist dann der physische Austausch, was unweigerlich zu neuen Investitionen, Installationsaufwand und erneuten Betriebsunterbrechungen führt.

4. Die cyber-physische Lücke: IT-Abteilungen setzen auf Zero-Trust-Architekturen und verschlüsseln den gesamten Netzwerkverkehr. Gleichzeitig sichert dieselbe Organisation ihren Serverraum mit einem Wiegand-Lesegerät ab, das Credentials im Klartext überträgt. Der IT-Sicherheitsperimeter endet am Netzwerkrand – die physische Eingangstür wird oft als separates Thema betrachtet und bei der Budgetierung vernachlässigt.

Der Weg nach vorn: Kontinuierliche Modernisierung

Die Lösung für dieses Mammutprojekt ist kein noch größerer Kraftakt. Vielmehr bedarf es eines grundlegend neuen Ansatzes für die Zutrittskontroll-Infrastruktur: Modernisierung muss als fortlaufender Prozess und nicht als einmaliges Ereignis verstanden werden. Ein schrittweiser Plan ist sowohl einfacher als auch kostengünstiger als ein radikales „Rip-and-Replace"-Projekt (Austausch des kompletten Systems). Durch eine sanfte Migration werden Arbeits- und Logistikkosten deutlich gesenkt und erzwungene Ausfallzeiten komplett vermieden. Unternehmen können die Modernisierung etappenweise durchführen – etwa nach Standort, Abteilung oder beim regulären Ablaufdatum der Credentials. So bleibt der Betrieb ungestört und die Kosten verteilen sich über einen längeren Zeitraum. Dank zukunftssicherer, universeller Lesegerätetechnologie wird das Lesegerät von einem starren Anlagegut zu einer flexiblen Plattform, die mit den Anforderungen mitwächst.

Beginnen Sie mit einer universellen Infrastruktur

Die Grundlage für eine kontinuierliche Modernisierung ist ein universelles Lesegerät, das alle bereits im Gebäude vorhandenen Credentials verarbeiten kann (ältere 125-kHz-Karten, moderne Smartcards, Mobile Credentials) und gleichzeitig für künftige Entwicklungen gerüstet ist. Da sich Zutrittstechnologien stetig weiterentwickeln, sollte die Unterstützung für neue Formate und Sicherheitsstandards einfach per Firmware-Update hinzugefügt werden können, ohne die Hardware austauschen zu müssen.

Lassen Sie alte und neue Credentials koexistieren

Mit Multi-Technologie-Lesegeräten wird die Umstellung zu einem fließenden Übergang. Neue Mitarbeitende erhalten vom ersten Tag an moderne Credentials. Die bestehende Belegschaft wird nach und nach umgestellt. Legacy-Karten (Alt-Systeme) funktionieren parallel weiter, bis das Unternehmen bereit ist, sie endgültig aus dem Verkehr zu ziehen. Schließlich kann die Unterstützung für Low-Frequency-Karten oder unsichere Credentials gezielt über ein Remote-Firmware-Update deaktiviert werden – ohne Ausfallzeiten oder Chaos an den Drehkreuzen.

Sichern Sie die gesamte Kette, nicht nur die Karte

Die bloße Aufrüstung der Credentials ohne Berücksichtigung der Kommunikationsebene greift zu kurz. Der Wechsel vom Wiegand-Protokoll zu OSDP Secure Channel (einem bidirektionalen, mit AES-128 verschlüsselten Protokoll) schließt Sicherheitslücken wie Replay-Angriffe und bietet eine Manipulationserkennung zwischen Lesegerät und Controller. Moderne Credentials und eine sichere Kommunikationsebene schützen die gesamte Authentifizierungskette – von der Karte oder dem Smartphone bis hin zur Zutrittskontrollplattform.

Wählen Sie eine Infrastruktur, die Sie nicht einschränkt

Interoperabilität ist kein reines Komfortmerkmal, sondern ein entscheidender strategischer Vorteil. Eine Infrastruktur auf Basis universeller Lesegeräte, die mit den meisten Transpondertechnologien und Ausweisformaten – ob physisch oder mobil – kompatibel sind, schützt effektiv vor Herstellerabhängigkeit (Vendor Lock-in) und teuren Systemwechseln. Zudem erweisen sich universelle Lesege-

räte als wertvolle Absicherung bei Fusionen und Übernahmen: Übernimmt ein Unternehmen einen Standort mit einem abweichenden Ausweissystem oder bringt ein neuer Dienstleister ein unbekanntes Kartenformat mit, lassen sich die vorhandenen Lesegeräte einfach umkonfigurieren. So werden die neuen Credentials vom ersten Tag an problemlos akzeptiert. Da sich Zutrittssysteme und Ausweisstandards kontinuierlich weiterentwickeln, können Unternehmen mit einer flexiblen Lesegeräte-Infrastruktur diesen Wandel bequem per Firmware-Update vollziehen. Wer hingegen auf starre Hardware setzt, steht unweigerlich vor dem nächsten kostenintensiven Investitionsprojekt.

Sicherheit, die skaliert

Diese Prinzipien gelten für einen einzelnen Standort ebenso wie für einen Logistikkonzern mit 5.000 Mitarbeitenden an Dutzenden Standorten. Da kein harter Stichtag für die Umstellung nötig ist, wird das operative Risiko, das ein traditionelles Groß-Upgrade oft undenkbar macht, beherrschbar. Der Übergang verläuft für die Nutzer an den Türen völlig unsichtbar. Der Handlungsdruck steigt: Asymmetrische Smartcard-Optionen, Apple Wallet-Firmenausweise und Mobile Credentials via BLE-Technologie werden in den kommenden Jahren im Unternehmensumfeld – auch in Logistik und Fertigung – flächendeckend Einzug halten. Unternehmen, die bereits in eine universelle, per Firmware aktualisierbare und mobilfähige Lesegeräte-Infrastruktur investiert haben, werden diesen Wandel mühelos bewältigen. Alle anderen stehen spätestens dann vor der nächsten teuren „Rip-and-Replace"-Entscheidung. Kontinuierliche Modernisierung ist kein abgeschlossenes Projekt, sondern eine dauerhafte strategische Fähigkeit: Es ist die Möglichkeit, die Sicherheitsinfrastruktur im eigenen Tempo weiterzuentwickeln – ohne Ausfallzeiten und ohne Abhängigkeit von bestimmten Ausweistechnologien. Wer diese Flexibilität heute aufbaut, löst nicht nur ein Sicherheitsproblem, sondern sichert die Zukunftsfähigkeit seiner gesamten Betriebsabläufe. ■

Ein Markt im Wandel – Jenseits herkömmlicher Credentials

Sowohl neue offene Standards (die die Herstellerabhängigkeit verringern) als auch weitverbreitete proprietäre Plattformen treiben den Markt in Richtung einer immer stärkeren Kryptografie. Diese modernen Credentials lassen sich auf Smartcards, mobilen Endgeräten oder kombiniert bereitstellen. Unternehmen, die sich heute für eine neue Lesegeräte-Infrastruktur entscheiden, sollten sicherstellen, dass die Hardware für diesen Technologiewandel gerüstet ist, um künftige und teure Austauschaktionen zu vermeiden.

Folgende Initiativen und Standards gewinnen dabei zunehmend an Bedeutung:

- **LEAF Identity:** Ein interoperables Rahmenwerk für Credentials auf Basis starker symmetrischer Verschlüsselung, das bereits in zahlreichen Installationen zum Einsatz kommt und sich als zuverlässiger Ersatz für veraltete Systeme bewährt hat.
- **LEAF Verified:** Eine Zutrittskontrollplattform der nächsten Generation auf Basis von NXP MIFARE DESFire (bzw. DUOX), die auf Public-Key-Kryptografie setzt. Dies macht die klassische Verwaltung gemeinsamer Schlüssel (Shared Keys) überflüssig und ermöglicht eine interoperable, herstellerneutrale Zutrittskontrolle.
- **PKOC (Public Key Open Credential):** Eine offene, herstellerunabhängige Credential-Spezifikation der Physical Security Interoperability Alliance (PSIA). Sie nutzt asymmetrische Public-Key-Kryptografie, bei der der private Schlüssel das Endgerät nie verlässt und eine Ableitung des öffentlichen Schlüssels als Credential fungiert.
- **Aliro:** Ein offener, auf mobile Anwendungen ausgerichteter Identifikationsstandard, der voraussichtlich 2026 von der Connectivity Standards Alliance (CSA) veröffentlicht wird. Unterstützt von Apple, Google, Samsung und über 220 Branchenmitgliedern, bietet Aliro neben asymmetrischer Public-Key-Kryptografie auch native Wallet-Integration, Offline-Geräteunterstützung und Mailbox-Funktionen.
- **HID Seos:** Eine weitverbreitete proprietäre Credential-Plattform, die sich als sichere, auf symmetrischer Verschlüsselung basierende Lösung für Installationen jeder Größenordnung bewährt hat – von kleinen Betrieben bis hin zu Großkonzernen. Sie unterstützt sowohl physische Smartcards als auch mobile Anwendungen, einschließlich Wallet-Integration.

Universeller Zugang mit ELATEC

Die Lesegeräte der TWN4-Serie von ELATEC basieren auf einem plattformunabhängigen Konzept: Sie sind multitechnologisch, multifrequenzfähig und flexibel per Software konfigurierbar. Dadurch stellen Unternehmen sicher, dass sie sich weder an eine spezifische Credential-Technologie noch an einen einzelnen Anbieter binden.

Wichtige Merkmale der TWN4-Familie:

- Umfassende Kompatibilität: Unterstützung von mehr als 100 physischen und mobilen Credentials sowie über 60 Transpondertechnologien.
- Vereint RFID, NFC und BLE in einem einzigen Lesegerät.
- Das System ist mit ELATEC DevPack vollständig softwarekonfigurierbar. Credentials, Verschlüsselungseinstellungen und Sicherheitsprotokolle lassen sich bequem per Fernzugriff (Remote-Update) aktualisieren – ein physischer Hardware-Austausch entfällt.
- Gewährleistet sowohl Rückwärtskompatibilität zu bestehenden Legacy-Systemen als auch Zukunftsfähigkeit bei der Einführung neuer Standards.
- Erhältlich in unterschiedlichsten Formfaktoren für zahlreiche Authentifizierungsanwendungen. Von der Zutrittskontrolle an Türen und Drehkreuzen, über die Desktop-Registrierung, bis hin zur Maschinenauthentifizierung.

ident Das Magazin für Automatische Identifikation & Digitalisierung

A B O N N E M E N T

Sichern Sie sich ihre Vorteile!

Bitte liefern Sie mir ab sofort die ident (6x ident Magazin, ident PRODUKTE und das ident JAHRBUCH pro Jahr) zum Bezugspreis von € 90,- inkl. 7% MwSt. zuzüglich Versandkosten (Inland € 10,-/Ausland € 20,-). Das Abonnement verlängert sich jeweils um ein weiteres Jahr, wenn es nicht 8 Wochen vor Ablauf des Bezugsjahres gekündigt wird.

1. Unkomplizierte Lieferung
Wir liefern Ihnen alle Ausgaben der ident direkt an Ihre Adresse. So sind Sie immer aktuell informiert.

2. Aktuelle Informationen
Sie erhalten praxisorientierte Anwendungsberichte, aktuelle Fachinformationen, Produktmeldungen und Branchennews aus dem Themenfeld der Auto-ID und Digitalisierung.

3. Vernetzter Wissensaustausch
Die ident verbindet branchenübergreifend Informationen aus Wissenschaft, Industrie und Anwendung.

4. *ident* Anbieterverzeichnis
Das Anbieterverzeichnis ist der direkte Weg zu Unternehmen, Lösungen und Produkten aus der Branche.

Firma: .....

Name: .....

Vorname: .....

Position: .....

Branche: .....

E-Mail: .....

Straße/Postfach: .....

PLZ/Ort: .....

Land: .....

IBAN: .....

Bankinstitut: .....

Datum/Unterschift: .....

Ident Verlag & Service GmbH
LESERSERVICE: Durchstraße 75, 44265 Dortmund
Tel.: +49 231 72546092, E-Mail: verlag@ident.de

ident.de

IMPRESSUM

ident
Das Magazin für Automatische Identifikation & Digitalisierung

Jährlich erscheinen 6 Magazine, ein Produkte Heft und ein Jahrbuch.

Website & Informationsportal: www.ident.de

Offizielles Organ der AIM-D e. V.

Herausgeber:
Ident Verlag & Service GmbH
Durchstraße 75, 44265 Dortmund, Germany
Tel.: +49 231 72546092
E-Mail: verlag@ident.de

Chefredakteur:
Dipl.-Ing. Thorsten Aha (verantwortlich)
Durchstr. 75, 44265 Dortmund, Germany
Tel.: +49 231 72546090
E-Mail: aha@ident.de

Redaktionsteam:
Tim Rösner
Prof. Dr.-Ing. Klaus Krämer

Anzeigenleiter:
Bernd Pohl
Tel.: +49 6182 9607890
E-Mail: pohl@ident.de

Abo/Leserservice/Verlag:
Tel.: +49 231 72546092
E-Mail: verlag@ident.de

Redaktionsbeirat:
Prof. Dr. Michael ten Hompel, Fraunhofer IML
Peter Altes, Geschäftsführer AIM-D e.V.
Frithjof Walk, Schneider Kennzeichnung GmbH
Heinrich Oehlmann, Eurodata Council
Bernhard Lenk

Gestaltung und Umsetzung:
RAUM X – Agentur für kreative Medien
Ranja Ristea-Makdisi, Stefan Ristea GbR
Huckarder Str. 12, 44147 Dortmund
Tel.: +49 231 847960-35,
E-Mail: mail@raum-x.de

Herstellung:
Strube OHG, Stimmerswiesen 3, 34587 Felsberg

Bezugsbedingungen:
Jahresabonnement € 90,- inkl. 7% MwSt. zzgl. Versandkosten (Inland € 10,-/Ausland € 20,-) und Einzelheft € 14,- inkl. 7% MwSt. zzgl. Versandkosten. Das Abonnement verlängert sich jeweils um ein weiteres Jahr, wenn es nicht 8 Wochen vor Ablauf des Bezugsjahres gekündigt wird. Bestellungen über den Buch- und Zeitschriftenhandel oder direkt beim Verlag: ISSN 1432-3559 ident MAGAZIN, ISSN 1614-046X ident JAHRBUCH.

Rechtliche Angaben:
Erfüllungsort und Gerichtsstand ist Dortmund, USt-IdNr. DE230967205
Amtsgericht Dortmund HRB 23359, Geschäftsführer Thorsten Aha

ident & ident.de sind eingetragene Marken der Ident Verlag & Service GmbH.