



# Vertrauenswürdige Digitale Identitäten sind der Schlüssel für die zukünftige Digitalisierung.

Alfred Dietel und Christian von Staudt im Interview mit Karsten Treiber

**Steinbeis M&A, vertreten durch Alfred Dietel und Christian von Staudt, begleiteten das mySaveID-Team der targens GmbH über 18 Monate von der Verifizierung bzw. Optimierung des Business Plans über die Geschäftsbereichsausgründung bis zum Verkauf an msg im April dieses Jahres. Welche Bedeutung dezentrale, Digitale Identitäten (Self-Sovereign Identity = SSI) für die fortschreitende Digitalisierung vieler Geschäftsbereiche in nahezu allen Branchen zukommt, das beleuchten Karsten Treiber, Geschäftsführer mySaveID bei msg, und Steinbeis M&A im Interview.**

## **Ganzheitliche Transaktionsberatung von Unternehmern für Unternehmer!**

Steinbeis M&A [www.steinbeis-finance.de](http://www.steinbeis-finance.de) bietet seinen Kunden ein umfangreiches und professionelles Beratungs- bzw. Dienstleistungsspektrum in den Bereichen (1) Mergers & Acquisitions (2) Buy-and-Build, (3) Strategy und (4) Capital Advisory, über alle Branchen hinweg. Mandanten sind insbesondere mittelständische Unternehmer, Unternehmen und Unternehmensgruppen im In- und Ausland, aber auch internationale Konzerne, die sich auf dem Mittelstandsmarkt etablieren wollen. Aktuell sind 13 Partner bei Steinbeis M&A tätig, die weit über 200 erfolgreiche Transaktionen in den letzten Jahren abgeschlossen haben. Steinbeis M&A mit Büros in Frankfurt, Stuttgart, Hamburg, Köln, Berlin, München, Karlsruhe, Wien (A), Zürich (CH), Palma (ES) und London (UK) ist eine unabhängige Beratungsgesellschaft der Steinbeis-Gruppe [www.steinbeis.de](http://www.steinbeis.de).

### **Alfred Dietel:**

Warum sind vertrauenswürdige digitale Identitäten so (immens) wichtig?

### **Karsten Treiber:**

Bis heute sind der Umsetzung von Digitalisierungsvorhaben oftmals juristische, gesellschaftliche und insbesondere gesetzliche Grenzen gesetzt, sodass die digitale Transformation an der Unternehmensgrenze endet. Dabei bieten gerade die unternehmensübergreifenden Prozesse ein hohes Optimierungspotenzial. Besonders das Management von Unternehmensberechtigungen und -daten im Außenverhältnis ist mit hohem Zeitaufwand verbunden. Durch vertrauenswürdige Autorisierungen können digitalisierte Prozesse angestoßen werden, die Anpassungen von Verwaltungsaufgaben und Kompetenzen in Unternehmensstrukturen deutlich leichter, schneller sowie kostengünstiger ermöglichen.

### **Christian von Staudt:**

Wie können wir uns das Thema der Digitalen Identität bildlich vorstellen?

### **Karsten Treiber:**

Mittels einer Digitalen Identität lässt sich ein Unternehmen, eine Person oder ein Objekt in der virtuellen Welt genauso wie im realen Leben eindeutig identifizieren. Im realen Leben läuft dies oft



Christian von Staudt  
Steinbeis M&A



Alfred Dietel  
Partner Steinbeis M&A

mit einem Ausweis oder anhand einer Urkunde. Typische Merkmale der realen Identität einer Person sind dabei etwa der Name, die Adresse und das Geburtsdatum oder auch ein Fingerabdruck, ein Bild des Gesichts sowie die Körpergröße. Die bekanntesten Attribute einer bisherigen Digitalen Identität bestehen oft nur aus Benutzernamen und Passwort und sind entsprechend (hoch) risikobehaftet. Genau das wollen wir ändern.

### **Alfred Dietel:**

Mittlerweile sind ständig Cyberattacken auf staatliche Stellen sowie Hackerangriffe auf Firmen in den Nachrichten. Wie können wir uns davor schützen und welche Entwicklungen helfen uns dabei?

**Karsten Treiber:**

Um Missbrauch auszuschließen muss sichergestellt werden, dass der Zugang nur durch eine eindeutig identifizierbare Datenform einer digitalen Abbildung einer realen Person, eines Unternehmens oder eines Objekts vorliegt. Seit geraumer Zeit erhalten reale Personen ihre Digitale Identität in der virtuellen Welt mittels Datenverarbeitung und -verschlüsselung. Einige Verfahren sind wenig gesichert, wie z.B. die einfache Registrierung von Nutzernamen und Passwörtern auf einer Webseite. Andere Verfahren erfordern eine erhöhte Sicherheit. So wurden zusätzliche PIN-Prozesse von Chipkarten oder TAN-Generatoren eingeführt oder etwa die Zwei-Faktor-Authentisierung sowie biometrische Erkennungsdaten. Die Kontoeröffnung durch ein Video-Identifizierungsverfahren nutzt beispielweise reale Identifizierungsmerkmale der natürlichen Person anhand des vorliegenden Personalausweises zur Erstellung der digitalen Identität des Kontoinhabers.

**Christian von Stadt:**

Das hört sich doch bereits sehr sicher und ausgereift an. Wo liegen die Probleme dieser Verfahren bzw. warum werden diese nicht überall schon eingesetzt?

**Karsten Treiber:**

Der Nachweis der eigenen Digitalen Identität muss schnell, komfortabel und sicher sein, um von einer breiten Masse angewendet zu werden. Dies ist heute oftmals noch nicht der Fall. Die erwähnten verbesserten Zugangsverfahren sind für die meisten Anwender äußerst umständlich, zeitaufwendig und zudem fehleranfällig. Auch eignen sich diese Verfahren bestenfalls für die korrekte Identifizierung von Personen bzw. deren Transaktionen, jedoch nicht für Objekte. Zudem sollten vorzugsweise nur wenige Identifizierungsdaten an Orten gespeichert werden, auf die der Nutzer keinen Einfluss hat. Wichtig ist ebenfalls, dass sich eine Person gegenüber einer Stelle ausweisen kann, ohne dass Dritte davon erfahren. Die heutigen Verfahren erfüllen diese Sicherheitsmerkmale leider nicht und sind zudem wenig anwenderfreundlich. Dies führt dazu, dass viele Unternehmen bei der Anmeldung über Firmen Log-Ins weiterhin auf hauptsächlich klassische, oftmals nur auf einen Anwendungsfall beschränkte Verfahren setzen. Doch

kann man sich sicher sein, dass es sich wirklich um die berechnete Person handelt und nicht um einen Angriff? Unberechtigte Dritte könnten nicht nur in das interne Firmennetz gelangen und Informationen einsehen, sondern auch Transaktionen veranlassen oder E-Mails manipulieren.

**Alfred Dietel:**

Wie sehen in der nahen Zukunft die Lösungen für die fortschreitende Digitalisierung von Transaktionen aus?

**Karsten Treiber:**

Im Mittelpunkt steht der Wunsch nach einer dezentralen Nutzung vertrauenswürdiger Identitätsdaten, einer vertrauenswürdigen Digitalen Identität. Ein Treiber dieser Art der Datennutzung stammt aus den Anforderungen der Distributed Ledger Technology (DLT), eines der bekanntesten Beispiele ist die Blockchain-Technologie, welche beispielsweise für die Schaffung (Mining) der Bitcoins verwendet wird. Hier lassen sich schon heute Transaktionen und Objekte unveränderbar prozessieren und protokollieren. Ausgangspunkt dieses Verfahrens sind IT-Algorithmen, die Daten dezentral, transparent und sicher verschlüsseln. Der englische Begriff „Ledger“ bedeutet ein Journal bzw. Hauptbuch zwecks Nachweisführung. Das Vertrauen und die Transparenz der DLT besteht darin, dass eine Kopie des Ledger an jeden berechtigten Teilnehmer (node) im Netzwerk verteilt wird und jeder node den Ledger einsieht, überprüft und Eingriffe oder Betrugsversuche im Transaktionsverlauf aufdeckt und verwirft (Abbildung 1).

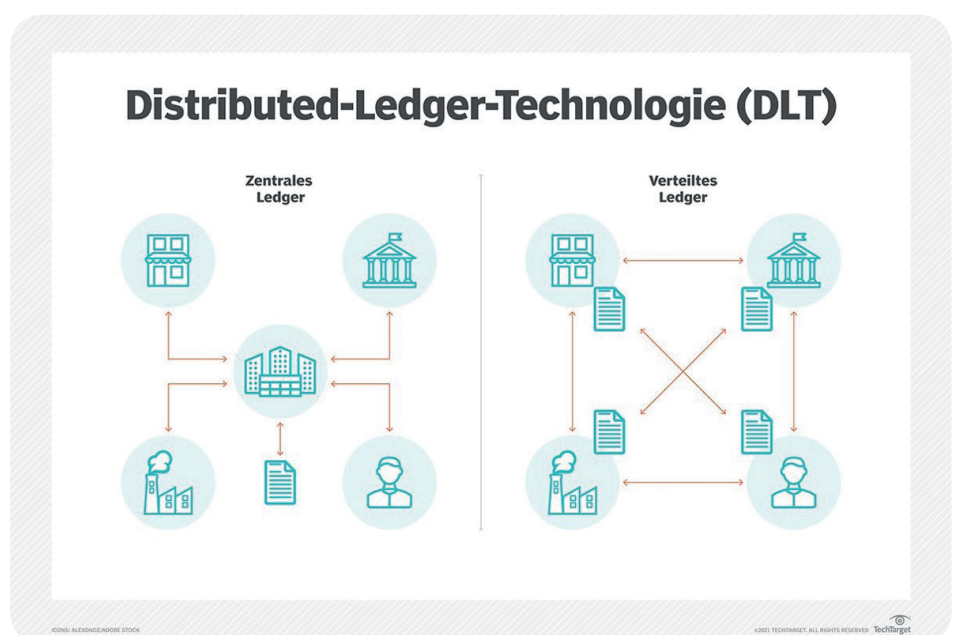


Abbildung 1: Illustration: [www.techtarget.com](http://www.techtarget.com)



biniert die für einen Geschäftsprozess nötige Funktionalität in einem vertrauenswürdigen, beaufsichtigten Service und schafft einen medienbruchfreien Mehrwert für Anwender und Netzwerke (Abbildung 4).

Zu den wesentlichen Produkten des Leistungsportfolios nach J.)&BJMWJSINJVZFN\*NJWYJQJPWTSNMJNLSFZWIFJ- gel und der Zeitstempel, welche in den digitalen Prozessen unserer Kunden nahtlos integrier- und nutzbar sind.

Der mySaveID Service ist technologieunabhängig konzipiert und kann über standardisierte Schnittstellen in bestehende Anwendungen, Plattformen oder Netzwerke integriert werden. Darüber hinaus ist er mit verschiedensten Distributed-Ledger-Technologien kompatibel.

Alfred Dietel:

Vielen Dank, dass Sie uns diese Einblicke in die Voraussetzungen zu weiteren Fortschritten in der digitalen Transformation gegeben haben. Zusammenfassend können wir festhalten, dass ohne vertrauenswürdige, digitale Identitäten jeglicher Fortschritt NSMHMZSLFZYSTRJWTJXKFXSRLQNHMGNSJK\*NJSY verläuft oder erhebliche Sicherheitsmängel aufweist. Die Notwendigkeit von digitalen Vertrauensdienstleistern, wie z.B. mySaveID von msg und deren Produkte, rückt in den Vordergrund der digitalen Transformation.

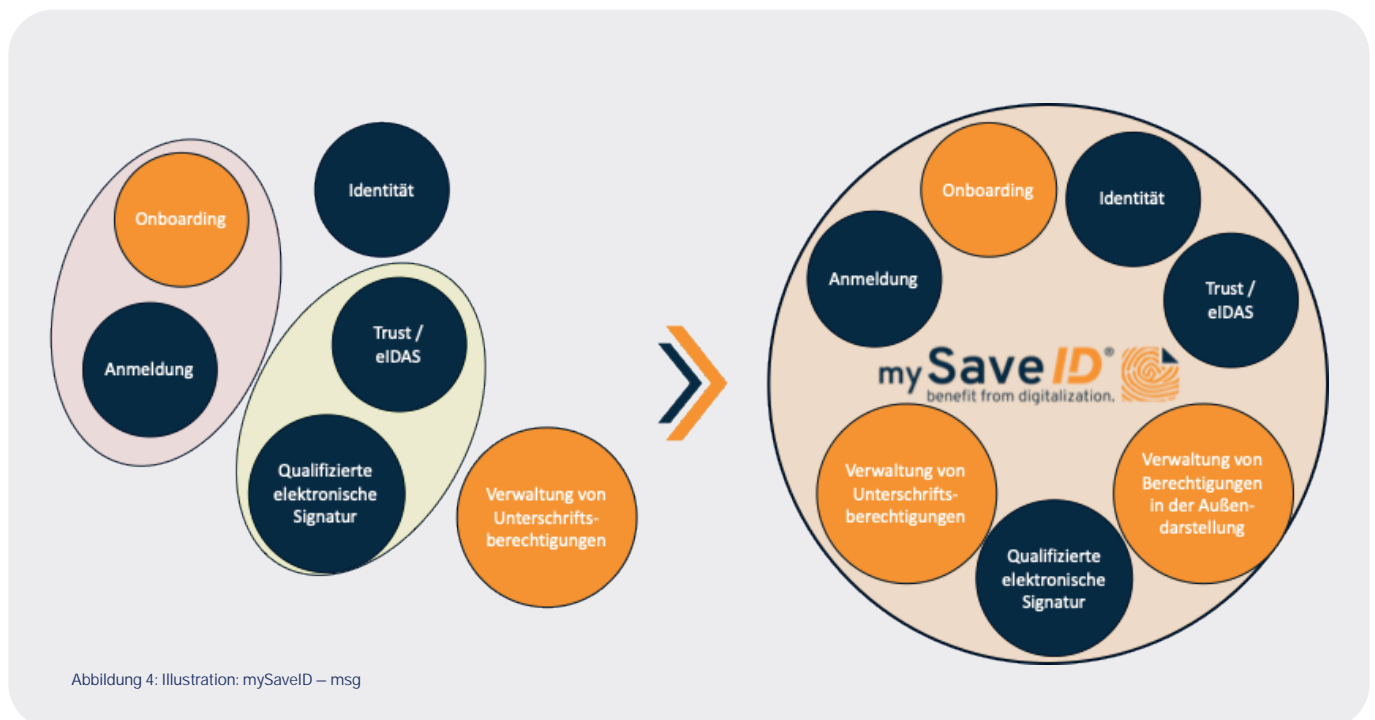


Abbildung 4: Illustration: mySaveID – msg