**Presseinformation**

Stand: September 2018

**Unternehmensportrait**

Die Digitalisierung erfordert neue Technologien, um die Identitäten, der an einer Transaktion beteiligten Parteien bzw. der Vertragspartner, zuverlässig zu verifizieren. In Anlehnung an die Blockchain-Technologie entwickelt Keyp ein Identitäts-Terminal mit einem eigenen Protokoll zum Austausch von Identifikationsmerkmalen wie Passwörtern oder biometrischen Daten. Datensicherheit, Datenschutz, Offenheit und Agilität bilden die Grundlage für die Entwicklung des Keyp Identity Terminals. Keyp verbindet sichere und offene Austauschplattform-Dienstleister, die einzelne Identitätsmerkmale verifizieren, mit den Betreibern digitaler Angebote und ermöglicht es Unternehmen, ihre eigenen Whitelabel-Plattformen zu erstellen. Einmal verifiziert und gespeichert, werden Identitätsmerkmale zu Identitätsfaktoren. Diese bleiben dabei stets in der Verfügungsgewalt ihrer Besitzer.

**Wie funktioniert Keyp?**

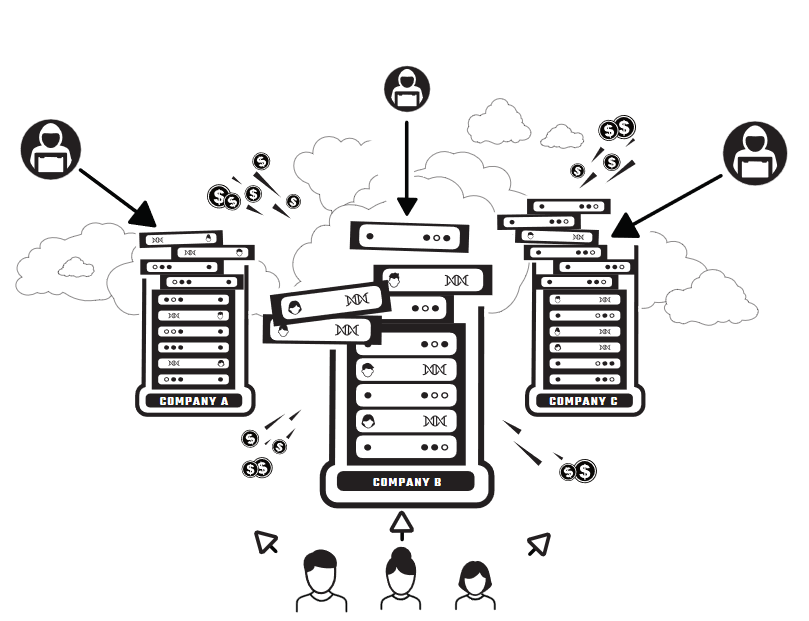
Nutzer von Keyp erhalten eine App auf ihrem Smartphone, in der all ihre Identitätsfaktoren gespeichert sind – ähnlich wie bei einem Passwortmanager oder einem digitalen „Wallet“. Die App – Keyp Wallet – erlaubt es, sich bei den jeweils genutzten Diensten automatisch einzuloggen und zu identifizieren. Dabei funktioniert sie vergleichbar mit Apps über die die Anmeldung automatisch über den persönlichen Facebook-Account erfolgen kann – ebenso mit nur einem Klick. Nur, dass die persönlichen Daten beim Nutzer der App bleiben und nicht im Datenkosmos der Unternehmen verschwinden – die Verfügungsgewalt über die vollständigen Daten und somit die eigene digitale Identität verbleibt exklusiv beim Anwender. Jeder User gibt an seinen Vertragspartner somit nur die Identifikations-Zugangsdaten heraus, die für die jeweilige Transaktion benötigt werden. Heißt: ausschließlich die für eine Transaktion.

Die notwendigen Identitätsmerkmale, die auf der App des Nutzers verwaltet werden, werden ähnlich wie bei einem App-Store abgefragt, ohne dass Unternehmen sich nochmals die Identität von Dritten verifizieren lassen müssen. Die verwalteten Merkmale wurden von bereits vorhandenen, vertrauenswürdigen Instanzen verifiziert – beispielsweise kann die Post die Anschrift und die Bank die Kreditkartendaten bestätigen. So kann sich ein Webseiten-Betreiber darauf verlassen, dass die übermittelten Identitätsdaten echt und aktuell sind. Dieser Ansatz der zweckgebundenen Verarbeitung personenbezogener Daten ist mit Blick auf die im Mai 2018 in Kraft getretene EU-Datenschutz-Grundverordnung (EU-DSGVO) ein wichtiger Schritt in Richtung persönliche Datenhoheit und Verbraucherschutz.

***Das Problem digitaler Identitäten:***

Digitale Identitäten sind der Schlüssel für eine Vielzahl von Online-Anwendungen und Geschäftsmodellen. Zwischen zwei Geschäftspartnern muss stets eine Vertrauensbeziehung hergestellt werden, indem sich beide Beteiligten gegenseitig ihre Identität beweisen. Daher gibt es heute wohl Millionen von Identitätslösungen – jede von einem Unternehmen genutzte Kundendatenbank stellt eine solche Individuallösung dar. In Folge dessen erkennen viele Marktteilnehmer, dass ein standardisiertes Ökosystem zur Nutzung und Verwaltung digitaler Identitäten diesem Wildwuchs vorzuziehen ist. Daher erleben wir aktuell, wie unterschiedliche Konglomerate aus Unternehmen für ihren Bedarf Standards definieren und versuchen, diese im Markt durchzusetzen.

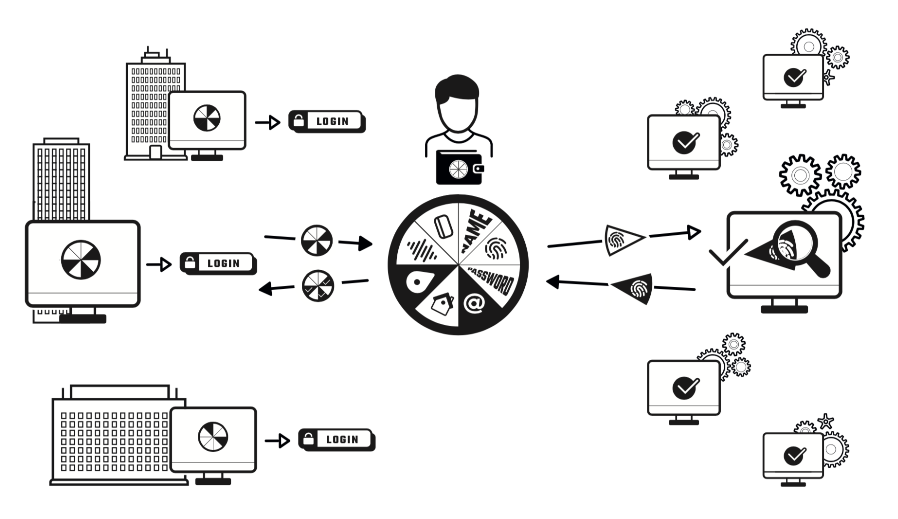
Doch diese Versuche, Industriestandards zu etablieren, stoßen auf unterschiedliche nationale Regulationen – selbst im EU-Raum setzen die einzelnen Mitgliedsstaaten die europäische Datenschutzgrundverordnung unterschiedlich um. Hinzu kommen branchenspezifisch definierte Anforderungen wie im Bankensektor oder in der Automobilindustrie. Von einzelnen Unternehmen nach ihrem eigenen Bedarf geformte Identitätslösungen können die Menge an Anforderungen nicht umfassend erfüllen. Hinzu kommt, dass die meisten Nutzer in der digitalen Welt mehrere Accounts bei unterschiedlichsten Anbietern besitzen – und diese zumeist nur über Passwörter schützen. Dies führt automatisch zu einem strukturellen und lästigen Dilemma: Dadurch, dass Nutzer sich meist bei jeder Transaktion erneut anmelden beziehungsweise verifizieren müssen, zahlen Unternehmen häufig enorme Kosten für die Aktualisierung sowie Authentifizierung ihrer Datenbanken und Nutzerprofile. Hinzu kommen immense Investitionen in Cyber-Security-Software, um sich vor Hacker-Angriffen zu schützen.



***Keyps Lösung:***

Keyp wirkt diesem Dilemma entgegen, indem es die Online-Identifikation für alle Teilnehmer vereinfacht und noch sicherer macht. Digitale Zugänge sind kontext-spezifisch und erfordern komplexe Authentifizierungs- und Verifizierungsprozesse. Das Kartenlesegerät beim Einkauf im Supermarkt benötigt beispielsweise andere Identitätsdaten als das Zugangsportal zum Ebay-Account. Nutzer benötigen demnach unterschiedliche Karten, Log-Ins bzw. Identitätsmerkmale, um unterschiedliche Dienste in Anspruch nehmen zu können. Auf der anderen Seite müssen sich Unternehmen die Echtheit der Daten von Dritten bestätigen lassen. Ebay muss sich folglich beim Verkauf eines Produkts die Kreditkartendaten des Käufers vom Kreditkarteninstitut bestätigen lassen, um die Transaktion abzuschließen. Keyps Identity Terminal – vergleichbar mit einem Karten-Terminal im Geschäft – verbindet nun alle digitalen Geschäftspartner einer Transaktion miteinander und garantiert dem Nutzer dabei vollkommene Datenhoheit. Der Nutzer braucht sich keine Passwörter zu merken und muss keine Profile mehr aktualisieren. Für Unternehmen wird es wiederum sicherer und kostengünstiger, ihre Services anzubieten, da sie sich darauf verlassen können, es mit verifizierten Kunden zu tun zu haben.

Keyp als sichere und offene Austauschplattform ermöglicht Unternehmen und Anbietern folglich, selbst auszuwählen, welche Identitätsfaktoren von welcher bereitstellenden beziehungsweise verifizierenden Stelle sie nutzen. Dadurch können Keyp-Nutzer eigene unternehmensspezifische Identitätsplattformen erstellen, nutzen und verwalten. Dies wird weitestgehend ohne eigenen Entwicklungsaufwand und nahezu in Echtzeit möglich. Das reduziert sowohl Implementierungskosten als auch -zeiten erheblich.



Dieser konsequent dezentrale Ansatz von Keyp bietet deutliche Vorteile gegenüber der gängigen zentralistischen Speicherung von Identitätsdaten durch einzelne Wirtschaftsunternehmen und ist zudem EU-DSGVO konform. Zentralistische Lösungen wälzen Risiken überwiegend auf die Verbraucher ab: Bei Hackerangriffen oder Datenmissbrauch wird die persönliche, digitale Identität jedes betroffenen Kunden in Mitleidenschaft gezogen. Zu einem möglichen wirtschaftlichen Schaden kommt dann oft noch das Problem, dass Betroffene auf Jahre hinaus Einschränkungen an der Teilnahme am digitalen Wirtschaftsleben erleiden.

**Wie kam es zur Gründung von Keyp?**

Die Gründer des Unternehmens erkannten als Start-up-Profis schon früh, dass dezentrale Identifikationstechnologien ein enormes Potenzial für das digitale Leben bieten. Mit Hilfe eines Features aus einer früheren Geschäftsidee entwickelten sie den Ansatz einer sicheren und digitalen Authentifizierungslösung weiter und gründeten Keyp. Das von Keyp entwickelte Identity Terminal für digitale Identitäten löst dabei ein grundlegendes Problem des Internets: die Herstellung von Vertrauen zwischen einander fremden Geschäftspartnern durch sicheren und offenen Austausch von Identitätsfaktoren. Die Gründer plädieren für ein offenes Ökosystem als zukunftssichere Lösung. Keyps föderiertes System soll zu einem marktübergreifenden Wachstum führen und nicht nur bestimmte Identitätssilos schärfen. Das Start-up versteht sich als alternatives und flexibles Angebot für Unternehmen, die digitale Identitäten für ihre Online-Services nutzen müssen. Die Plattform erhebt keinen Exklusivitätsanspruch –  kann von ihren B2B-Nutzern also auch zusätzlich zu anderen Identitätslösungen eingesetzt werden. Das Keyp-Ökosystem ist leistungsfähig genug, um auch komplexe Anforderungen und Use Cases zu erfüllen und gleichzeitig so einfach, dass es auch für Kleinstunternehmen attraktiv und nutzbar ist. Keyp verbindet damit Convenience mit Security: Einmalig hinterlegte User-Daten werden mit höchsten Sicherheitsstandards, etwa biometrischen Daten, verbunden. Es ist zudem der schnellste und unkomplizierteste Weg, um gesetzeskonforme Identitätsprüfungen wie etwa die Verifikation des Alters eines Kunden oder des Besitzes eines gültigen Führerscheins durchzuführen. Einzelne, geschlossene Lösungen für bestimmte Anwendungsfälle werden in Zukunft nicht ausreichen, da Transaktionen zwischen verschiedensten Parteien, beispielsweise auch zwischen Mensch und Maschine, möglich sein müssen. Folglich muss es einen gemeinsamen strukturellen Standard geben, um die Validität und den Identitätsnachweis unter allen Parteien zu ermöglichen.