

Information

# oneclick™ + Identitäts- und Rechtmanagement FIDES

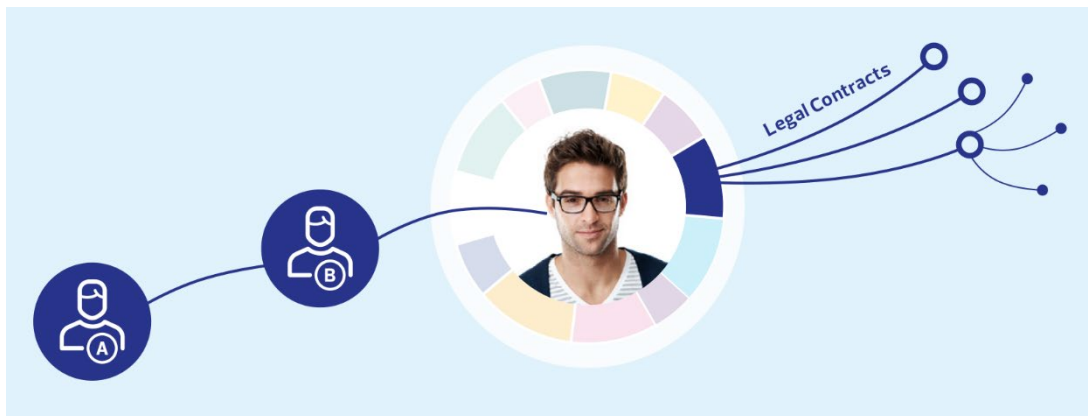
Stand 30. Jul. 2020

Mit dem Identitäts- und Rechtmanagement FIDES erhalten Nutzer Selbstbestimmung über ihre Daten mittels digitaler Berechtigungsketten. Die oneclick™ Plattform hat FIDES für die Bereitstellung digitaler Arbeitsplätze integriert.

## Inhaltsverzeichnis

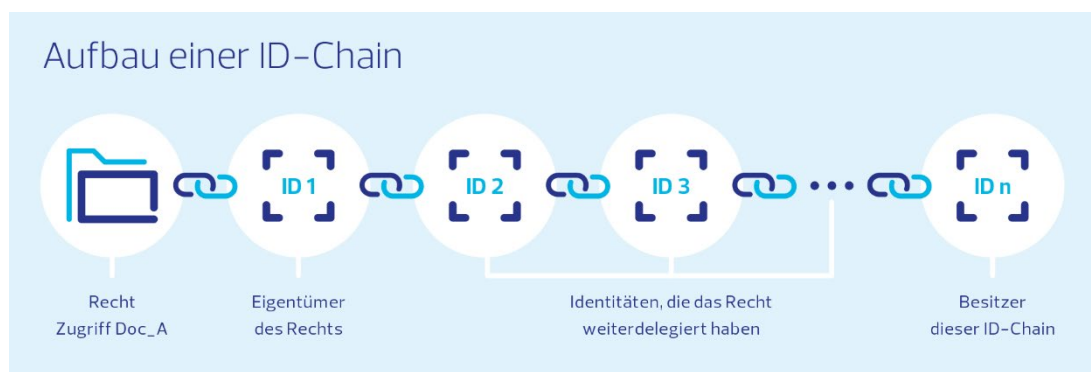
|   |    |
|---|----|
| Erfüllung hoher Anforderungen an den Datenschutz .....  | 3  |
| Compliance-konform und rückverfolgbar .....   | 4  |
| Die „Business-Chain“ für Unternehmen und andere Organisationen.....   | 5  |
| Sicherheit steht bei oneclick™ an erster Stelle .....   | 6  |
| Von „Zero Trust“ zu „Zero Knowledge“ .....  | 7  |
| Kontrolle über das System aber nicht über benutzerbezogene Daten .....  | 8  |
| Vereinfachte Bedienung und gleichzeitige Bereinigung des Active Directory .....   | 8  |
| Einzigartig: Ein abgesicherter Unified Workspace für die Verwaltung des Active Directory<br>und den Zugriff auf sämtliche Applikationen und Daten ..... | 9  |
| Sichere Authentifizierung und Single Sign-On.....   | 10 |
| Starke Passwörter einfach handhaben .....   | 11 |
| Über die Bundesdruckerei .....  | 11 |
| Haben Sie Fragen oder brauchen Sie weitere Informationen? .....   | 12 |

Klassische Identitäts- und Rechtemanagementsysteme erfüllen das Bedürfnis der Nutzer nach Datenhoheit und Sicherheit nur unzureichend. Deshalb hat das Innovationslabor der Bundesdruckerei mit FIDES einen revolutionären Ansatz entwickelt, der die individuelle Datensouveränität bereits in der Basistechnologie verankert. Kern des Identitäts- und Rechtemanagements FIDES sind verknüpfte Berechtigungen, sogenannte ID-Chains, die auf der Blockchain-Technologie basieren. Die Idee dahinter: Mit FIDES hat allein der Nutzer die Kontrolle über seine digitalen Berechtigungen, wie etwa den Zugriff auf seine persönlichen Daten. Befugnisse kann er an andere weitergeben oder wieder entziehen. Im Zentrum steht das Selbstbestimmungsrecht des individuellen Nutzers, jederzeit souverän über seine Daten und deren Weitergabe zu entscheiden.



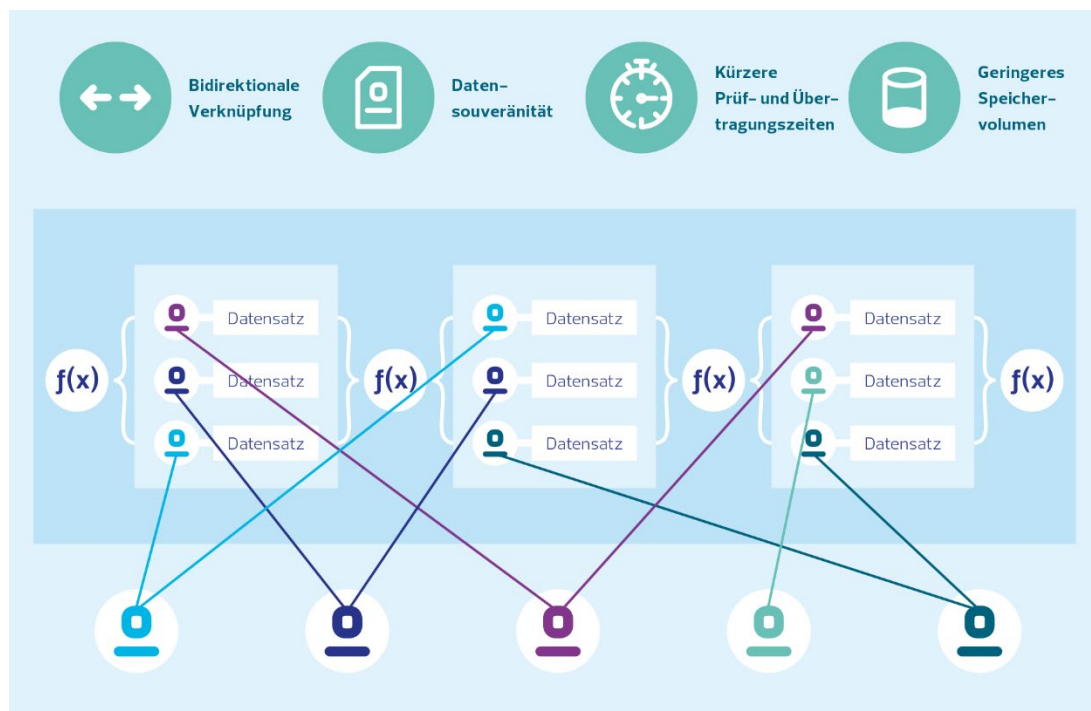
## Erfüllung hoher Anforderungen an den Datenschutz

Mit dem Konzept der ID-Chains gibt FIDES eine konsequent anwenderfreundliche Antwort auf gestiegene Erwartungen an Datenschutz und -sicherheit, die den hohen Anforderungen der Datenschutz-Grundverordnung der Europäischen Union entspricht. Diese sieht unter anderem das Recht auf Vergessenwerden und den Privacy-by-Design-Ansatz bei der Verarbeitung personenbezogener Daten vor. Bei diesen Forderungen stößt beispielsweise eine öffentliche Blockchain auf Probleme. In der Kette gespeicherte Informationen können dort nicht gelöscht werden und sind für die Teilnehmer der Blockchain einsehbar.



## Compliance-konform und rückverfolgbar

Mit FIDES kann jeder Nutzer nur das sehen, wofür er Berechtigungen besitzt. Innerhalb des Systems hat er keine Möglichkeit herauszufinden, welche weiteren Identitäten und Berechtigungen vorhanden sind. Die Folge: Jeder sieht nur, was er sehen darf. Datenhoheit besitzen allein diejenigen, zu denen die Daten in fachlicher oder persönlicher Hinsicht gehören. Durch die eindeutige Vergabe von Rechten existiert eine klare Verantwortlichkeit zu jedem Recht. Das System protokolliert alle Rechte und Identitäten mit. Zudem dokumentiert es jede Delegation von Berechtigungen sowie alle Zugriffe. Das garantiert die Integrität der Nutzerdaten, Transparenz und Manipulationssicherheit. Ein Nutzer kann jederzeit nachverfolgen, was mit seinen Rechten geschieht. Insbesondere bei Audits ist für Prüfer stets nachvollziehbar, wer wann mit welchen Berechtigungen auf welche Daten oder Systeme zugegriffen hat und woher diese Berechtigungen stammen. Eine Transaktionshistorie in Form einer Timeline wird regelmäßig systemseitig gespeichert.



## Die „Business-Chain“ für Unternehmen und andere Organisationen

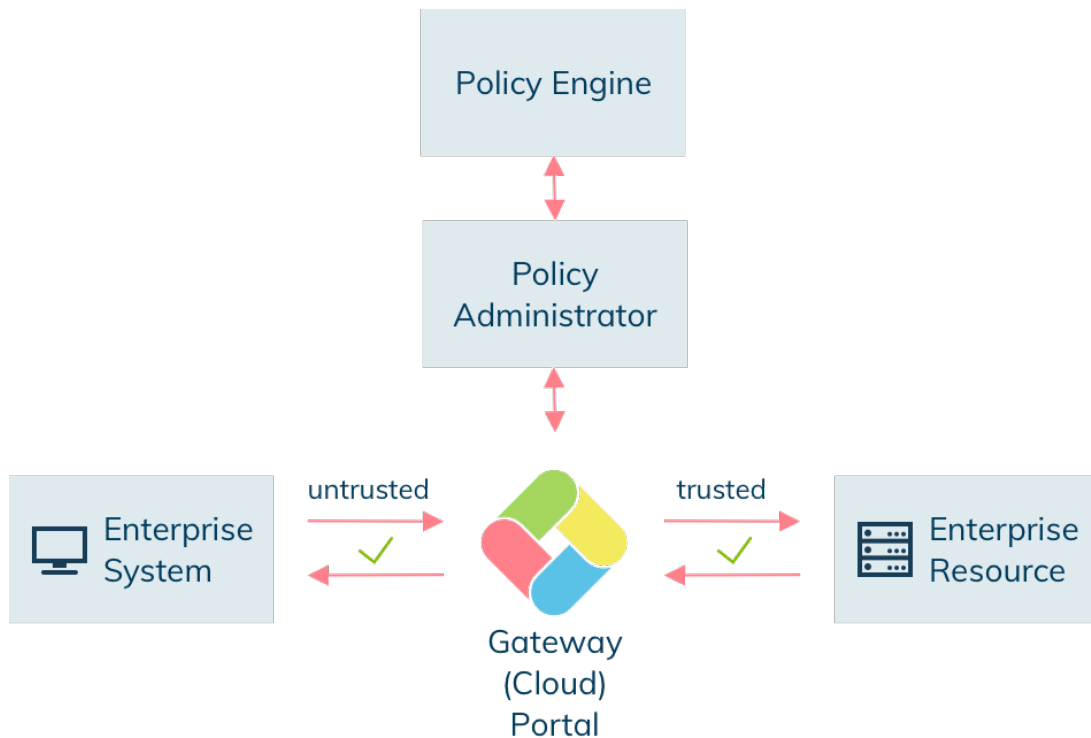
„  
Mit oneclick™ haben wir einen Partner gefunden, FIDES im Unternehmensumfeld als Business-Chain einzusetzen. Unser FIDES-Konzept ermöglicht im Zusammenspiel mit der oneclick™ Plattform eine effiziente und sichere Vergabe sowie die Pflege von Rechten für den Zugriff auf sämtliche Anwendungen, Daten und weitere Unternehmensressourcen. Dank FIDES kann ein neuer Mitarbeiter alle wichtigen Berechtigungen direkt durch den Teamleiter oder einen dafür zuständigen Kollegen erhalten. FIDES gibt den Verantwortlichen in der Organisation die Gestaltungshoheit und die technischen Werkzeuge, ihre jeweiligen Rechte zu verteilen und zu pflegen. Jeder Rechteeigentümer sowie jede weiterdelegierende Instanz in der Kette übernehmen die Verantwortung dafür, dass nur diejenigen Identitäten eine Berechtigung erhalten, die diese tatsächlich brauchen. Ändert sich beispielsweise das Aufgabengebiet einer Person, werden ihr die nicht mehr benötigten Rechte unmittelbar entzogen.



Dr. Manfred Paeschke, Chief Visionary Officer der Bundesdruckerei

## Sicherheit steht bei oneclick™ an erster Stelle

Die oneclick™ Plattform, unter anderem Gewinnerin der renommierten eco und Enterprise Workspace Awards, orientiert sich für die Anwendungsbereitstellung an Best Practices der IT-Sicherheit, nämlich an den Prinzipien einer [Zero Trust Architektur](#) (ZTA).



Dabei wird jeder Zugriff auf dedizierte Unternehmensressourcen individuell authentifiziert und der Vertrauensstatus fortlaufend überprüft. Unerlaubte Seitwärtsbewegungen in einem Unternehmensnetzwerk oder innerhalb größerer und verteilter hybrider Strukturen werden zuverlässig unterbunden. oneclick™ trägt als vertrauenswürdiger Cloud Service das Trusted Cloud Label. Eine Überprüfung von Capgemini im Auftrag des Bundesministeriums für Wirtschaft und Energie bestätigt, dass oneclick™ alle Anforderungen im Hinblick auf Transparenz, Sicherheit, Qualität und Rechtskonformität erfüllt. Zudem ist oneclick™ aktives Mitglied bei TeleTrust, dem größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa.



## Von „Zero Trust“ zu „Zero Knowledge“

“

*Mit unseren digitalen Arbeitsplätzen im Browser verbinden wir Nutzer auf sichere Art und Weise mit allen Unternehmensanwendungen und Daten. Als zentrale Orchestrierungsplattform ermöglicht oneclick™ beispielsweise den Fernzugriff auf On-Premises-Umgebungen, automatisiert über Schnittstellen die Bereitstellung von Cloud-Infrastruktur, und authentifiziert die Benutzer an eingesetzten SaaS-Applikationen. Dabei verfolgen wir bei oneclick zwei Paradigmen: Consumerization of IT und Democratization of Innovation. Bei beiden Zielen unterstützt uns FIDES, indem der einzelne Nutzer im Mittelpunkt steht. Wir gehen aber noch einen Schritt weiter: durch den Einsatz des Pseudonymisierungsdienstes von FIDES werden in oneclick™ keine personenbezogenen Daten mehr erkennbar gespeichert und unsere Zero Trust Architektur wird ergänzt um einen Zero Knowledge Ansatz. Aus visionärer Sicht entwickeln wir uns dank der Integration von FIDES vom bereits unterstützten Bring-your-own-Device (BYOD) in Richtung Bring-your-own-Application und noch einen Schritt weiter gedacht in Richtung Bring-your-own-Data. Mit oneclick™ und FIDES haben Unternehmen und Administratoren jetzt die Möglichkeit, sich als absolut führend zum Thema Datenschutz zu positionieren und damit Wettbewerbsvorteile zu erzielen.*

”



Dominik Birgelen, CEO der oneclick AG

## Kontrolle über das System aber nicht über benutzerbezogene Daten

Wo das Identitätsmanagementsystem von FIDES betrieben wird, kann ein Unternehmen frei entscheiden. Der Betrieb ist im Rechenzentrum der Bundesdruckerei, bei oneclick™ oder im eigenen Rechenzentrum möglich. Die Daten werden in jedem Szenario mittels der hochsicheren Algorithmen der Bundesdruckerei verschlüsselt. Die Lösung unterscheidet sich grundlegend von klassischen Identitätsmanagementsystemen, in denen der Administrator jeder Identität bestimmte Rollen und Rechte zuordnet. Insbesondere in größeren Organisationen lässt sich häufig nicht mehr nachvollziehen, welche Rechte eine gewählte Person zu einem bestimmten Zeitpunkt besaß oder besitzt. Zudem erfährt der Administrator oft nicht rechtzeitig von Änderungen beim Personal oder bei Zuständigkeiten. Im schlimmsten Fall können Mitarbeiter auf die Daten einer Abteilung zugreifen, obwohl sie diese schon vor Monaten verlassen haben. Während in den meisten bestehenden Systemen ein Administrator alle Dateiberechtigungen besitzt, sind bei FIDES die Rechte den jeweiligen Verantwortlichkeiten zugeordnet. Der Administrator hat somit zwar weiter die Kontrolle über das System aber nicht mehr über die benutzerbezogenen Daten.



**Untrennbare Verknüpfung  
zwischen Identitäten und  
Rechten**



**Atomare  
Rechtevergabe,  
keine Rollen**

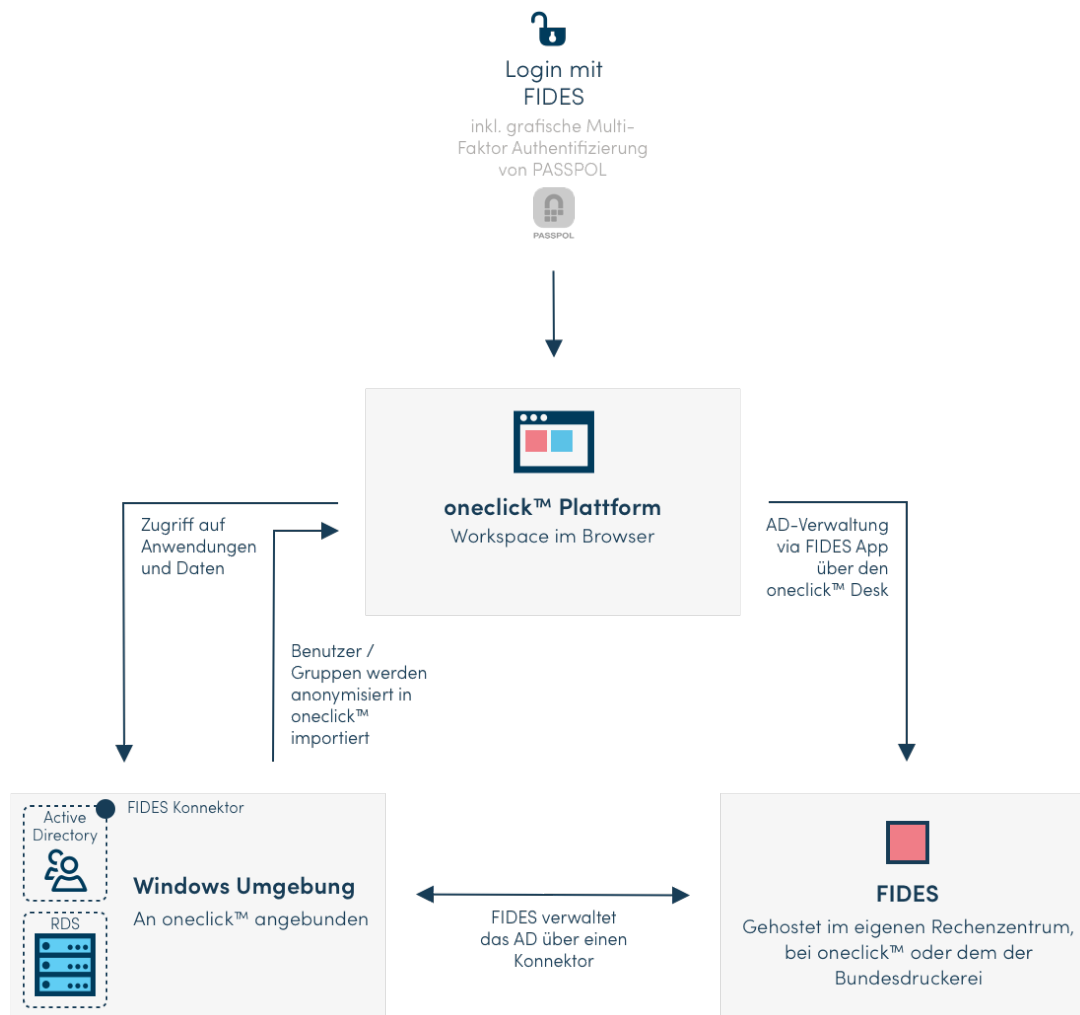


**Nachvollziehbarkeit  
der Rechtevergabe**

## Vereinfachte Bedienung und gleichzeitige Bereinigung des Active Directory

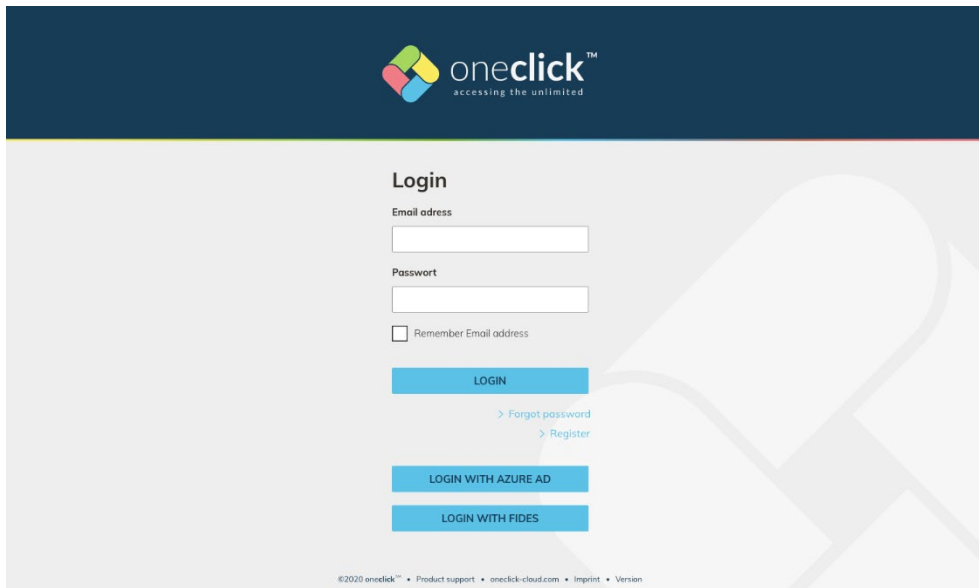
Die Verwaltung eines Unternehmens-Active Directory kann bei größeren und verteilten Unternehmensstrukturen schnell eine komplexe Angelegenheit werden. Neu werden die Benutzer übersichtlich und einfach in FIDES angelegt und das Active Directory über einen Konnektor bedient. Dabei wird das Active Directory des Kunden gleichzeitig aufgeräumt, denn FIDES erkennt bei der Einrichtung sofort alle Redundanzen und Konflikte, die sich über die Zeit angesammelt haben, zum Beispiel indem Benutzer mehreren Gruppen mit überschneidenden Rechten zugeordnet wurden. FIDES spielt dem Administrator solche Ungereimtheiten zurück, so dass er das Active Directory bereinigen kann. Auch eine Synchronisation mit mehreren Systemen ist möglich, wie zum Beispiel die Kombination eines Active Directory und SAP.





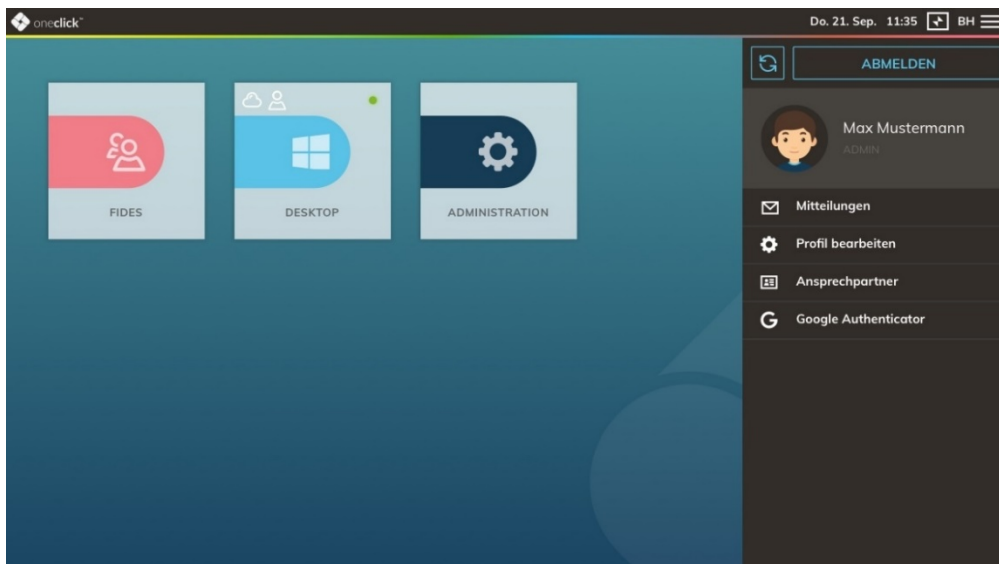
## Einzigartig: Ein abgesicherter Unified Workspace für die Verwaltung des Active Directory und den Zugriff auf sämtliche Applikationen und Daten

Die Kombination von oneclick™ und FIDES macht es erstmals möglich, sowohl die Verwaltung des gesamten Active Directory als auch den Zugriff auf Applikationen und Daten über eine einheitliche Oberfläche im Browser zu bewerkstelligen. Mit der FIDES-App im oneclick™ Workspace kann jeder Benutzer seine Active Directory-Berechtigungen verwalten und delegieren. Sämtliche für den täglichen Arbeitsalltag notwendigen Anwendungen lassen sich ebenfalls direkt über den oneclick™ Workspace öffnen und bedienen. Daten werden über das sogenannte Hybrid Drive anwendungsübergreifend und mittels modernster Streaming-Technologie bereitgestellt, ohne dass diese den definierten Speicherort verlassen. Eine Installation zusätzlicher Client- oder Server-Dienste entfällt.



## Sichere Authentifizierung und Single Sign-On

Um mit oneclick™ und dem FIDES Identitäts- und Rechtemanagement zu arbeiten, müssen Nutzer sich nur einmal an der Plattform anmelden. Grundlage für den Zugang ist ein vertrauenswürdiger Identity Provider, der Identitäten anlegt und bestätigt. Die oneclick™ Plattform und FIDES unterstützen dabei den Standard OpenID Connect. Ein Rechteeigentümer kann für bestimmte Rechte verschiedene Vertrauenslevel definieren. So kann für den Zugang zu weniger kritischen Dokumenten nur die Eingabe eines Passworts erforderlich sein oder bei besonders sensiblen Informationen ein zweiter oder dritter Faktor abfragt werden.



## Starke Passwörter einfach handhaben

Um starke Passwörter einfach zu handhaben, setzen die Partner auf PASSPOL, eine patentierte, grafische Multi-Faktor Authentifizierung, die eine schnelle, bequeme und hochsichere Alternative für textuelle Passwörter, PINs oder biometrische Verfahren darstellt. Personalisierbare Bilder, die gleichzeitig als kryptografische Keyfiles dienen, werden in einer bestimmten Reihenfolge auf einer Matrix verschoben. Diese Sequenz, in Verbindung mit den richtigen Bildern, dient zur Verifikation, ist sehr leicht merkbar und nahezu unvergesslich. PASSPOL macht sich hierzu drei bewährte psychologische Phänomene zunutze: den Pictorial Superiority Effekt, den Dual-Code-Effekt und die hohe Merkfähigkeit von Bewegungsmustern.



## Über die Bundesdruckerei

Die Bundesdruckerei GmbH ist ein führendes deutsches Hightech-Sicherheitsunternehmen. Ihre Produkte und Dienste sind „Made in Germany“, sie basieren auf der zuverlässigen Identifikation von Personen und Institutionen. Als Sicherheitsunternehmen des Bundes ebnet das Unternehmen den Weg in eine sichere digitale Zukunft. Weitere Infos unter [www.bundesdruckerei.de](http://www.bundesdruckerei.de).



Bildquellen:

Bundesdruckerei GmbH (2018): Whitepaper: Vom allmächtigen Administrator zum selbstbestimmten Nutzer. Online unter <https://www.bundesdruckerei.de/de/whitepaper/download/2835/Whitepaper-Fides.pdf> (besucht am 28.07.2020)

# Haben Sie Fragen oder brauchen Sie weitere Informationen?

Wir helfen Ihnen gerne weiter!

Herr Dominik Birgelen

Tel.: +41 44 578 88 93

E-Mail: [dominik.birgelen@oneclick-cloud.com](mailto:dominik.birgelen@oneclick-cloud.com)

## oneclick™ - die Everything-as-a-Service-Plattform

Als zentrale Zugriffs- und Verteilplattform in der Cloud ermöglicht oneclick™ das Management des ganzen Technologie-Stacks für die Anwendungsbereitstellung. oneclick™ vereint Software-, Plattform- und Infrastruktur-as-a-Service aus beliebigen On-Premises und Cloud-Umgebungen hinter einem Webportal. Everything-as-a-Service (XaaS) bedeutet, dass Sie all dies als Service konsumieren können.



oneclick AG  
Zollikerstraße 27  
CH-8008 Zürich

T (+41) 44 578 88 93  
[info@oneclick-cloud.com](mailto:info@oneclick-cloud.com)  
<https://oneclick-cloud.com>

Copyright © 2020 oneclick AG. All rights reserved.  
oneclick and the oneclick logo are trademarks or registered trademarks of oneclick AG