SECANDA

AUTHENTIFIZIERUNG
PC UND NETZWERK SCHÜTZEN

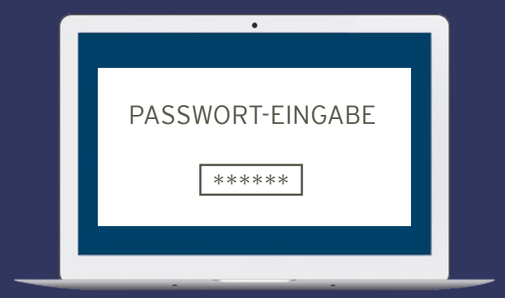
Die Passwort-Anmeldung um Chipkarte oder App ergänzen und mit nur einer Anmeldung auf alle Daten zugreifen

SECANDA

secanda.com

1 Mit der Chipkarte anmelden: Authentifizierung Faktor 1

2 Passwort eingeben: Authentifizierung Faktor 2



3 Personalisierter Zugriff auf alle Daten und Systeme: Single Sign-on

MIT CHIPKARTE UND PASSWORT SICHER AM PC ANMELDEN UND AUF DATEN ZUGREIFEN

Für das Entsperren von Computern oder den Zugang zu Netzwerken bietet das einfache Passwort häufig keinen ausreichenden Schutz.

Wird zusätzlich zur Eingabe des Passworts auch die persönliche Chipkarte des Nutzers eingelesen, erhöht sich die Sicherheit erheblich. Hierzu muss lediglich ein Chipkartenleser per USB angeschlossen oder ein bereits vorhandener Leser genutzt werden.

Das bedeutet: Ohne den physischen Besitz der Chipkarte ist der Zugang zu vertraulichen Daten ausgeschlossen.

VORHANDENE CHIPKARTE NUTZEN

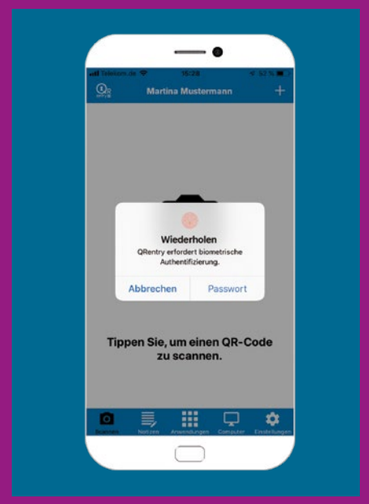
Wer seine Chipkarte heute bereits als Zutrittskarte zu Räumen oder als Bezahlkarte für Mensa oder Kantine nutzt, erhält mit der gleichen Chipkarte zukünftig auch Zugang zu Netzwerken und Daten: von jedem PC aus mit individuell festgelegten Rechten.

Mitarbeiter- oder Dienstausweise und Studierenden- oder Mitgliedsausweise erhalten so eine weitere Funktion im bestehenden Chipkartensystem.

ZUGANGSRECHTE ZU DATEN INDIVIDUELL VERWALTEN

Durch das Single Sign-on Verfahren haben Nutzer die Möglichkeit, mit nur einer Anmeldung durch Passwort und Chipkarte Zugang zu allen Daten und Servern zu erhalten, ohne sich für jeden Datenserver neu anmelden zu müssen. Diese Rechte können sogar einer Urlaubsvertretung übertragen werden, ohne dass Passwörter offengelegt oder gemeinsam genutzt werden müssen.

DOPPELTE SICHERHEIT DURCH AUTHENTIFIZIERUNG MIT ZWEI FAKTOREN



2-FAKTOR-AUTHENTIFIZIERUNG: PASSWORT UND CHIPKARTE, APP ODER USB-TOKEN

Der Zugang zu einem Netzwerk oder zu sensiblen Daten gilt erst als sicher geschützt, wenn zusätzlich zum einfachen Passwort weitere Faktoren abgefragt werden. Ein zweites Passwort birgt dabei das Risiko, dass Nutzer ihre Passwörter lediglich wiederholen, aufschreiben oder sogar liegen lassen.

Mit der Chipkarte, der App, einem USB-Token oder biometrischen Merkmalen lässt sich die Authentifizierung mit beliebig vielen Faktoren zuverlässig absichern, ohne weitere Passwörter abfragen zu müssen.

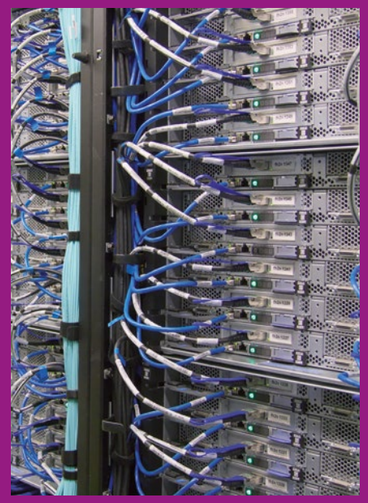
DIE GLEICHEN ZUGANGSRECHTE AN JEDEN ARBEITSPLATZ MITNEHMEN

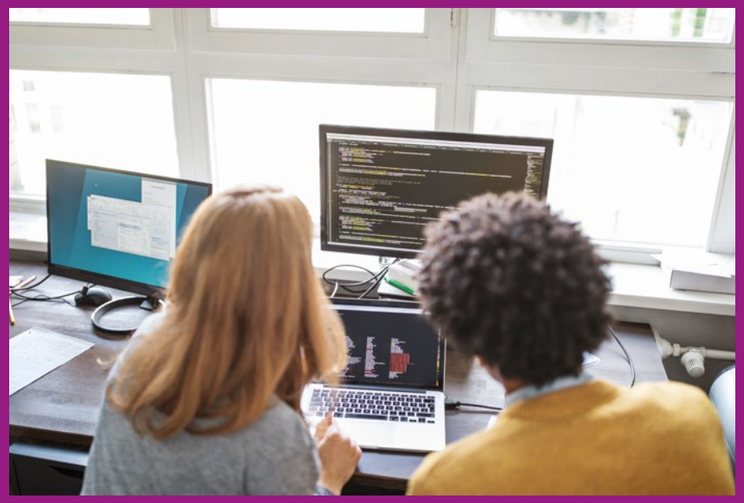
Wer an einem Arbeitsplatz innerhalb einer Organisation Zugangsberechtigungen zu klar definierten Daten und Systemen hat, kann diese Rechte mit der gleichen Authentifizierung auch an anderen Arbeitsplätzen nutzen. Wer das Terminal oder den Arbeitsplatz wechselt, nimmt seine Zugriffsrechte für Daten und Systeme also automatisch mit.

Eingesetzt werden kann das Verfahren auch an öffentlichen Terminals, wo Studierende überall auf dem Campus ein gemeinsames System nutzen, aber jeweils nur ihre personalisierten Daten abrufen können.

So hat der Nutzer an jedem Ort auf dem Campus oder in der Organisation die gleichen Zugriffrechte – oder eben auch nicht.

ZUGANGSBERECHTIGUNGEN ZU DATEN ZENTRAL VERWALTEN





SINGLE SIGN-ON: NUR EINE ANMELDUNG FÜR ALLE DATEN UND PROGRAMME

Mit Single Sign-on reicht eine einzige Anmeldung am persönlichen Computer aus, um Zugriff auf verschiedenste Daten und Server gleichzeitig und ohne Eingabe weiterer Zugangsdaten zu ermöglichen. So muss sich der Nutzer nur noch ein einziges Passwort merken.

Welche Daten der Nutzer einsehen und welche Programme er wie nutzen darf, wird durch die individuell vergebenen Zugangsrechte klar geregelt.

Das hohe Sicherheitsniveau bleibt auch bei Single Sign-on bestehen, wenn diese zentrale Zugangsberechtigung zu allen Daten sicher durch die 2-Faktor-Authentifizierung mit der Chipkarte geschützt ist.

SYSTEMNUTZER EINDEUTIG ZUORDNEN

Sicherer Zugang zu Daten und Anwendungen bedeutet umgekehrt auch Sicherheit bei der Zuordnung von Vorgängen zu Personen. Wer sich beispielsweise in der Universität als Studierender zu Prüfungen oder zu einem neuen Semester anmeldet, oder wer als Arzt Systeme und Daten nutzt, lässt sich damit sicher zuordnen. Bei Haftungsfällen oder Daten-Leaks kann so der einzelne Nutzer exakt bestimmt werden.

BERECHTIGUNGEN ZEITWEISE ÜBERTRAGEN

Durch ein zentrales Management der Berechtigungen kann der Zugang zu persönlichen Daten und Verzeichnissen übertragen werden, ohne dass Passwörter offengelegt oder gemeinsam genutzt werden müssen. So kann beispielsweise bei Urlaubsvertretungen die Zugangsberechtigung vorübergehend gewährt und später wieder entzogen werden.

SECANDA

NEHMEN SIE KONTAKT MIT UNS AUF

SECANDA Systems AG
Marienstraße 10
78054 Villingen-Schwenningen

T +49 (0)7720 99 45 0
F +49 (0)7720 99 45 10
E info@secanda.com

secanda.com