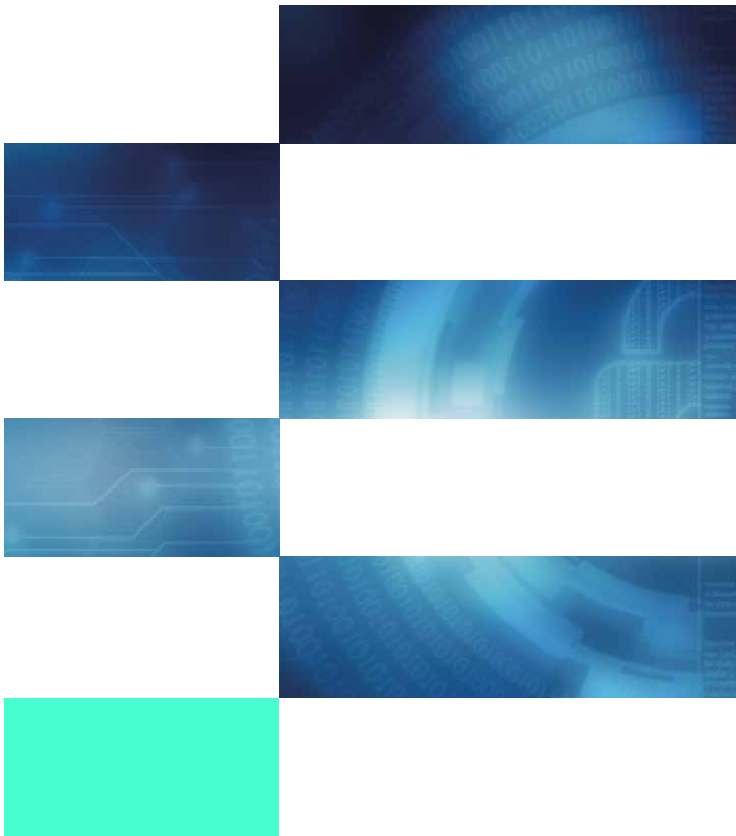
esatus

Neue Chancen für die Digitalisierung.

Ausstellung und Prüfung von digitalen Credentials leichtgemacht.



02
22

Dieses Whitepaper ist die Fortsetzung unserer Schriftenreihe „Vertrauen im Internet“. Wir empfehlen, mit der Lektüre des ersten Whitepapers zu starten, das den Prozess der Credentialausstellung aus Sicht des Nutzers schildert.

Credentials mit Self-Sovereign Identity: Der Schlüssel zur digitalen Transformation

Ein Auto mieten, einen Kredit beantragen, Bewerbungsunterlagen einreichen oder den Impfstatus nachweisen – für all das müssen wir uns identifizieren und eindeutig belegen, dass wir über die erforderlichen Eigenschaften, Qualifikationen oder Berechtigungen (wie z.B. eine Fahrerlaubnis) verfügen. Diese Identifizierungs- und Nachweisprozesse zu vereinfachen und zu beschleunigen, ist eine der großen Herausforderungen für eine erfolgreiche digitale Transformation.

Die Technologie der Self-Sovereign Identity (Selbstbestimmte Identität bzw. SSI) mit digitalen Nachweisen (sog. Credentials) eröffnet in dieser Hinsicht ganz neue Möglichkeiten: Fälschungssicherheit, Überprüfbarkeit und der Widerruf von bereits ausgestellten Credentials werden sichergestellt und sind einfach umsetzbar. Credentials können für viele Anwendungsbeispiele bedarfsgerecht und individuell konzipiert werden: als Ausweisdokument, Gutschein, Ticket, Garantiebescheinigung, Zugangsberechtigung und vieles mehr. Auch die Bestimmungen des Datenschutzes werden unterstützt, denn der Nutzer behält die Kontrolle und kann selbstbestimmt entscheiden, welche persönlichen Daten wann er mit wem teilt. Und das alles, ohne eine Brieftasche mit Ausweispapieren oder einen Ordner voller Dokumente mit sich zu führen, denn die digitalen Credentials sind für den Endanwender jederzeit griffbereit auf dem eigenen Smartphone verfügbar.

Die SSI-Technologie basiert auf einem Vertrauensverhältnis zwischen den beteiligten Rollen:

- dem Aussteller des digitalen Credentials,
- dem Inhaber, der die Nachweise auf seinem Smartphone mit sich führt
- und der prüfenden Partei, die verifiziert, ob die gezeigten Informationen aus den Credentials echt und gültig sind.

Weiterführende Informationen zu den Grundlagen der SSI-Technologie finden Sie im esatus-Whitepaper „Vertrauen im Internet“.

Im Folgenden wird Schritt für Schritt erläutert, wie digitale Credentials auf Basis von SSI ausgestellt und durch die prüfende Partei verifiziert werden können. Dafür haben wir ein aktuelles Beispiel gewählt: den digitalen Corona-Testnachweis[1].

Credentialausstellung am Beispiel eines Testzentrums

Ein Covid-19-Testzentrum möchte seinen Kunden Testergebnisse in Form von digitalen Credentials zur Verfügung stellen. Diese Credentials sollen durch Dritte, bspw. eine Fluggesellschaft, ein Restaurant oder eine Behörde, einfach und mit möglichst geringem Aufwand geprüft werden können.

Was benötigt das Testzentrum?

- Einen PC oder ein mobiles Endgerät (Tablet)
- Eine Software zur Ausstellung der Credentials auf Basis von SSI (von verschiedenen Anbietern erhältlich z.B. SOWL - esatus AG).

Beim Erwerb der Software ist die Registrierung auf einer dezentralen Datenbank und dadurch die Berechtigung zur Ausstellung von Credentials mit inbegriffen.

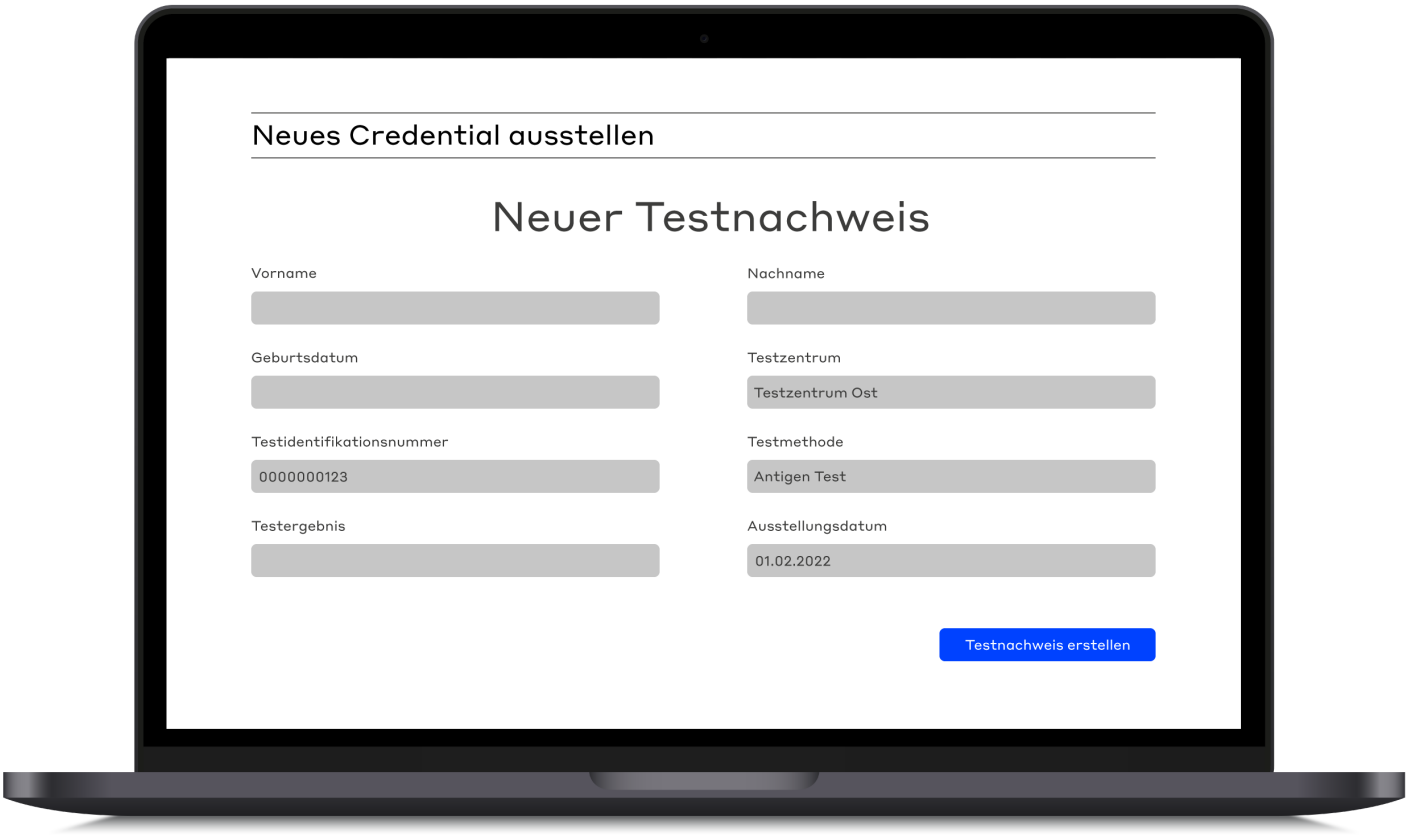
Was benötigt der Kunde?

- Eine Wallet App auf einem Smartphone (von verschiedenen Anbietern erhältlich, z.B. esatus Wallet App, kostenfrei im Apple App-Store oder im Google Play-Store erhältlich)

[1] Bei dem hier beschriebenen Anwendungsfall handelt es sich um ein beispielhaftes Szenario, um den Nutzen und die Funktionsweise von digitalen Credentials zu erläutern. Es stellt weder eine Empfehlung für Verhaltensweisen während der Corona-Pandemie dar, noch soll damit eine Lockerung von derzeit geltenden Corona-Maßnahmen befürwortet werden.

Nachdem ein Kunde den Schnelltest absolviert hat, findet er sich bei der Credentialausgabe ein. Ein Mitarbeiter des Testzentrums ruft den Menüpunkt „Neues Credential ausstellen“ auf. Es erscheint eine Eingabemaske mit den notwendigen Feldern für die Ausstellung des Testnachweises.

Ausstellung eines Credentials



Eingabemaske für den Ausstellungsprozess eines Testnachweises

Die Felder Ausstellungsdatum, Testidentifikationsnummer, Testzentrum und Testmethode sind bereits vorausgefüllt. Der Mitarbeiter gibt nun die persönlichen Daten des Kunden ein (Vorname, Nachname, Geburtsdatum) sowie das Testergebnis (positiv, negativ). Das Testzentrum könnte weitere Sicherheitsmerkmale integrieren, z.B. die getestete Person fotografieren und das Foto dem digitalen Testnachweis beifügen. Mit Klick auf „Testnachweis erstellen“ wird ein QR-Code generiert, worin eine Anfrage zum Verbindungsaufbau zwischen der Software des Testzentrums und der Wallet App des Kunden hinterlegt ist.

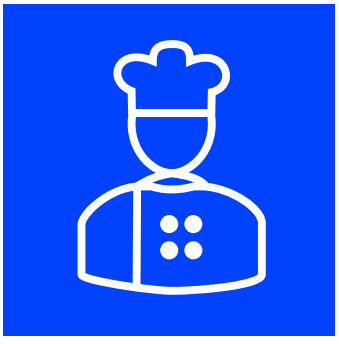
Übermittlung des Testnachweises als Credential

Der Mitarbeiter bittet den Kunden, den QR-Code mit seinem Smartphone zu scannen und anschließend den Aufbau einer Verbindung zwischen dem Smartphone und dem Testzentrum zu bestätigen. Über diese sichere und private Verbindung wird der digitale Testnachweis automatisch an die Wallet App des Kunden übermittelt. Der Kunde empfängt auf seinem Smartphone eine push-Nachricht: „Sie haben ein neues Credential“. Jetzt muss er nur noch dem Erhalt des Testnachweises zustimmen und diesen auf seinem Smartphone speichern.

Digitaler Testnachweis auf dem Smartphone des Getesteten

Prüfung eines Credentials am Beispiel eines Restaurants

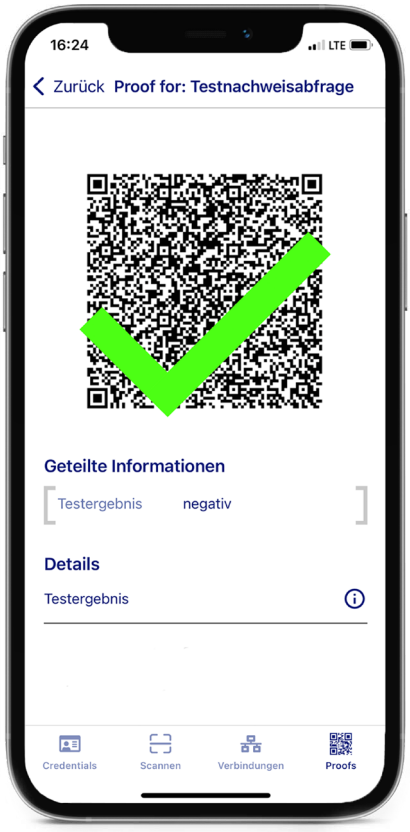
Die getestete Person möchte ihren Nachweis am gleichen Tag zum Besuch eines Restaurants nutzen.



Was benötigt das Restaurant, um die Echtheit und Gültigkeit des digitalen Testnachweises verifizieren zu können?

- Einen PC oder ein mobiles Endgerät (Smartphone oder Tablet)
- Eine Software für die Verifizierung der Information auf dem Credential (von verschiedenen Anbietern erhältlich z.B. SOWL - esatus AG)

Beim Eintreffen des Gastes klickt ein Restaurantmitarbeiter auf „Erstellen“ und generiert damit einen QR-Code; diesen scannt der Gast mit seinem Smartphone. Im Display erscheint die Anfrage, einen gültigen, negativen Corona-Test nachzuweisen. Weitere persönliche Daten werden nicht abgefragt. Durch Klick auf „Bestätigen“ wird das Testergebnis übermittelt. Im Hintergrund überprüft die Software des Restaurants die Authentizität und Gültigkeit der übermittelten Informationen. Sobald das Testergebnis verifiziert ist, erscheint ein grünes Häkchen, das den Gast zum Betreten des Restaurants berechtigt. Eine zusätzlich gewünschte Identifizierung des Gastes erfolgt entweder über das bei der Credentialausstellung hinterlegte Foto oder über einen Abgleich des Namens mit dem Personalausweis.



Appansicht des Restaurants nach erfolgreicher Verifikation des Testergebnisses

An diesem Beispiel wird deutlich, wie unkompliziert und effizient solche Prozesse mit digitalen SSI Credentials abgebildet werden können. Mit minimalem Aufwand können alle Beteiligten sich darauf verlassen, dass die Credentials gültig und echt sind, und dass die Privatsphäre des Endanwenders zu jedem Zeitpunkt gewahrt wird.

Digitale Credentials auf Basis von SSI können einen wesentlichen Beitrag zur Beschleunigung der Digitalisierung in allen Lebensbereichen leisten. Die Technologie ist ohne spezielle IT-Kenntnisse für jedermann einfach anwendbar. In Anbetracht ihrer vielfältigen Einsatzmöglichkeiten können digitale Credentials die Basis für viele Geschäftsprozesse sein, unabhängig von Branche und Größe des Unternehmens oder der Institution. Eine Anbindung an eigene, bereits vorhandene IT-Systeme ist einfach möglich.

Wollen Sie erfahren, wie Sie digitale Credentials effizient zum Einsatz bringen können? Kontaktieren Sie uns. Wir unterstützen Sie gerne.

In Kontakt treten

Herausgeber: esatus AG

Copyright Fotos: jijomathai/ Adobe Stock; Creefty/ Adobe Stock; NEO/Adobe Stock;

Version 1.0

Neue Chancen für die Digitalisierung.

esatus steht für eine sichere, freiheitliche, am Menschen orientierte digitale Zukunft. Wir sind Brückenbauer zwischen dem Heute und Morgen.

Digitalisierungsprozesse gestalten wir zukunftsorientiert und bieten Lösungen aus einer Hand – von der Konzeption über die individuelle Software-Entwicklung bis hin zur Betriebsführung. Weiterhin steht bei uns das Thema Information Security (InfoSec) im Fokus. Wir beraten Unternehmen aus einer ganzheitlichen Perspektive rund um das Thema Identity & Access Management und unterstützen bei der Umsetzung von Compliance und Datenschutzanforderungen (GRC).

Seit 2015 sind wir passionierter Treiber von Self-Sovereign Identity (SSI) in Deutschland und einer der globalen Technologieführer. SSI setzt den Menschen in den Mittelpunkt des digitalen Ökosystems und sorgt für nutzerfreundliche, selbstbestimmte Verwaltung der eigenen Daten.

esatus