FSP
SOFTWARE & CONSULTING
Wettbewerbsvorteile aus einer Hand.

Zukunftsoffene nPA/eID Lösung

Kundenregistrierung und -zugang per nPA/eID zukunftsoffen für weitere Verfahren z.B. Fido, biometrische Verfahren und mTan

AusweisApp 2

1 Inhalt

2 Einleitung

Ausgangslage:

Die Zugangsdaten für das Kundenlogin werden häufig noch über einen PIN-Brief postalisch zugestellt. Dieses Identifizierungsverfahren kann z.B. um ein schnelleres, auf der eID-Funktion des neuen Personalausweises basierendes, Verfahren ergänzt werden.

Dem Kunden eröffnet dies die Möglichkeit, innerhalb von wenigen Minuten seine Registrierung **komfortabel, einfach und sicher** durchzuführen und so den Zugriff auf seinen persönlichen Kundenbereich zu erlangen.

Der Kunde benötigt:

- Neuen Personalausweis (nPA) mit freigeschalteter eID-Funktion
- Die für jedes aktuelle Android-Smartphone und iPhone mit NFC-Funktion

  (ab Version 7) verfügbare Ausweis-App2
- Internetverbindung

Der Kunde kann nach einem Online-Vertragsabschluss über alle verfügbaren Kanäle auf dieses Verfahren hingewiesen werden. Ergänzend sollte auf der Website bzw. in der APP des Unternehmens eine Informationsseite angeboten werden, auf der das Verfahren erläutert wird. Es ist sinnvoll dort auch eine Einwilligung zur Datenspeicherung zu implementieren. Die Einwilligung ist Voraussetzung für die Fortführung des Identifizierungsprozesses. Ein Button auf der Informationsseite startet dann den nPA-Identifizierungsdialog.

Der Kunde öffnet nach Aufforderung die Ausweis-App2 auf seinem Smartphone und folgt den Anweisungen. Mittels NFC werden die Ausweisdaten ausgelesen und der Transfer der fachlich relevanten Ausweis-Daten und der notwendigen technischen Daten durchgeführt:

- Name, Vorname (aus nPA ausgelesen)
- Adresse (aus nPA ausgelesen)
- Geburtsdatum (aus nPA ausgelesen)
- Pseudonym (aus nPA ausgelesen)

und zusätzlich optional

- eMail-Adresse (vom Kunden im Dialog eingegeben)
- Mobilfunk-Nr . (vom Kunden im Dialog eingegeben)

Anschließend müssen die Ausweis-Daten im Vertrags-Bestand abgeglichen werden. Falls der Kunde gefunden wird, werden diese Daten dem Kunden angezeigt. Nach Bestätigung per Checkbox erhält der Kunde Zugang zu seinem persönlichen Kundenbereich.

Kann der Kunde nicht im Bestand gefunden werden, ist ein Clearing über die Vertragsabteilung herzustellen (z.B. Rückruf beim Kunden).

Optional können die E-Mail-Adresse und Mobilfunknummer in den Clearing-Prozess z.B. per mTAN bzw. Double-Opt-in integriert werden.

Die vom Kunden erhobenen Daten, sowie die Metadaten (Datum, Uhrzeit, ID-Art) und weitere technisch notwendige Daten (Zertifikats-ID, Token, Credentials etc.) sind im entsprechenden Unternehmens-System abzuspeichern.

Für den nachfolgenden immer wieder kehrenden Zugang zum persönlichen Kundenbereich per nPA (Authentifizierung) kann der nPA neben Benutzername/Passwort eine Option sein aber auch andere Verfahren wie z.B. mTan oder moderne auf dem Fido Standard basierende Anmeldeprozesse per Fingerprint oder FaceID.

Sowohl die Identifizierung als auch die Authentifizierung durch den nPA erfüllen die Voraussetzug für eine 24/7-Verfügbarkeit.

FSP stellt mittels der im Folgenden beschriebenen Lösung die nPA-Anbindung für die Kunden Website/APP und den Zugang zum eID-Server des Bundes inkl. Zertifikatshosting sowie die notwendigen technisch-fachlichen Informationen zur Verfügung.

3 Lösungsskizze

3.1 Prämissen der Lösung

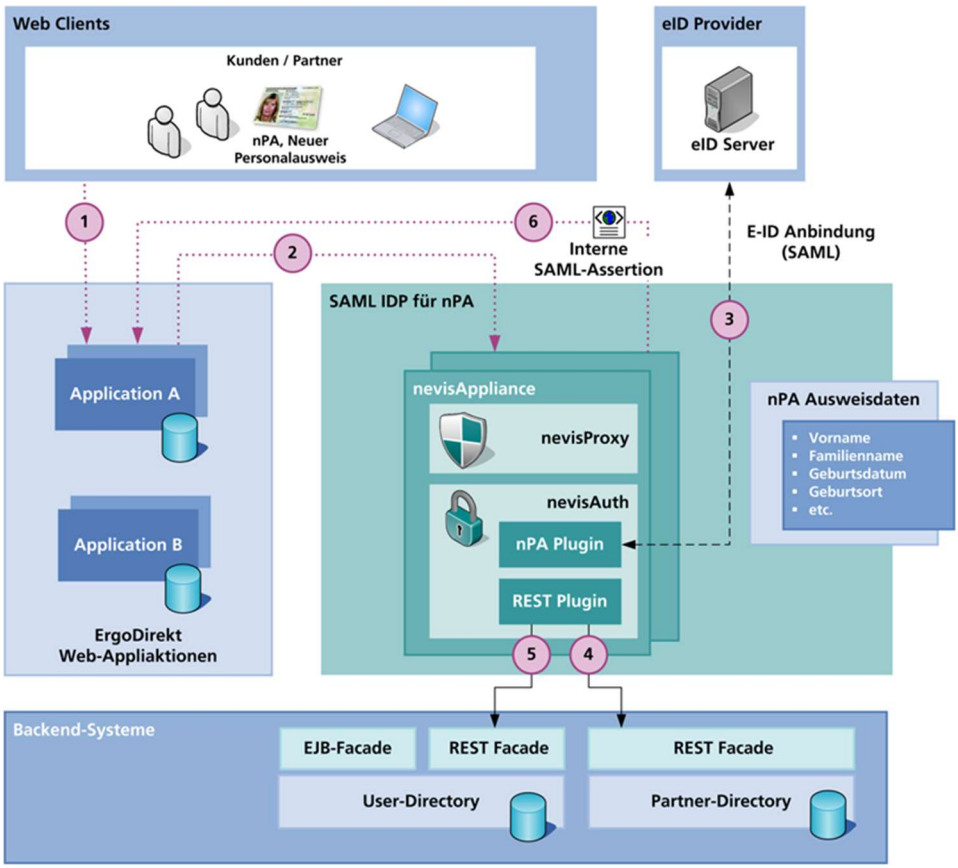
Die angebotene Lösung realisiert eine optimale Kosten-Nutzen-Relation.

Die Umsetzung ist kurzfristig möglich.

Die Lösung gewährleistet die notwendige Flexibilität für zukünftige Entwicklungen.

Diese Anforderungen werden durch die Verwendung von bereits verfügbaren Standardkomponenten in der Lösung erreicht.

3.2 Architekturüberblick



Für die Realisierung der nPA-Integration in die Unternehmens-Web-Umgebung wird ein auf der NEVIS Security Suite basierter SAML-IDP (Identity Provider) aufgebaut, welcher die Funktionalität für die nPA-Registrierung und die nPA-Authentisierung vollständig kapselt. In einer NEVIS Software-Appliance (nevisAppliance) stehen die beiden Komponenten nevisProxy und nevisAuth zur Verfügung. Die nevisAppliance, als bootbares Linux-Image geliefert, kann problemlos in virtualisierten Umgebungen (ESX oder Hyper-V) betrieben werden.

Die nevisAppliance beinhaltet alle notwendigen NEVIS-Komponenten für die Realisierung der Lösung.

Das Herzstück der NEVIS Authentisierungslösung bildet der Authentisierungsservice nevisAuth. Dieser besteht im Kern aus einer konfigurierbaren „Authentication-Engine“,

welche es ermöglicht, sog. Authentication-Plugins flexibel miteinander zu kombinieren. Diese Architektur ermöglicht die Unterstützung einer großen Anzahl von Authentisierungsmechanismen und stellt darüber hinaus sicher, dass die Lösung sehr einfach um kundenspezifische Plugins erweitert werden kann. Für die Authentisierung mittels nPA stellt der nevisAuth bereits „out-of-the-Box“ ein Standard-Plugin zur Verfügung.

3.3 Integration in das Unternehmens-Kundenportal

Die NEVIS-basierte nPA-Infrastruktur wird lose mittels SAML (Security Assertion Markup Languge) mit der bestehenden Unternehmens-Web-Infrastruktur gekoppelt. Bei SAML (http://saml.xml.org/wiki/saml-introduction) handelt es sich um ein standardisiertes Protokoll für die Föderierung von Identitäten über System- und Organisationsgrenzen hinweg.

Der Ablauf einer Registrierung mittels nPA sieht wie folgt aus:

1. Der Benutzer wählt die Funktion „Registrieren mittels nPA“ auf der Unternehmens-Login-Seite/APP und wird damit auf den NEVIS-basierten SAML IDP umgeleitet. (HTTP Redirect)
2. Der Schritt 2 in der obenstehenden Grafik entspricht dem erwähnten HTTP Redirect.
3. Das nPA-Plugin des nevisAuth stößt anschließend den nPA Authentisierungsvorgang an, der Benutzer wird in dessen Verlauf nach dem nPA-PIN gefragt. Nach erfolgter Authentisierung mittels nPA stehen die abgefragten User-Attribute wie z.B. Vorname, Familienname, Geburtsdatum, etc. zur Verfügung.
4. Im nächsten Schritt überprüft ein nevisAuth REST-Plugin, ob der nPA Benutzer bereits Kunde ist. Dazu werden die identifizierenden Attribute (z.B. Vorname, Familienname, Geburtsdatum, Geburtsort) an das unternehmensspezifische REST-API des Partner-Directory weitergeleitet. Falls das API keinen eindeutigen Treffer liefert, so wird der Benutzer auf eine Fehlerseite geleitet. Die Fehlerseite beinhaltet z.B. die Telefon-Nummer des Helpdesks sowie die Aufforderung, sich dort zu melden.
5. Falls der Benutzer im unternehmensspezifischen Partner-Directory gefunden wird, so wird mittels API-Call auf das unternehmensspezifische User-Directory sichergestellt, dass dort ebenfalls eine Identität angelegt ist und der Benutzer bei Folge-Identifizierungen mittels nPA wiedergefunden werden kann. Beispielsweise durch eine eindeutige Pseudonym-Kennung im User-Directory. Falls bereits ein Account besteht, so wird die Pseudonym-Kennung als zusätzliches Benutzer-Attribut gespeichert. Der Benutzer hat nun die Möglichkeit, sich alternativ zum bisherigen Username / Passwort z.B. mittels nPA anzumelden. Falls noch keine Identität vorhanden ist, so wird eine neue erstellt. Als Basis-Informationen stehen die nPA-Attribute sowie sämtliche Attribute aus dem Partner-Directory zur Verfügung. Eine mittels nPA-Registrierung angelegte Identität verfügt über kein Passwort und kann sich daher auch zukünftig nur mittels nPA oder anderer passwortloser Athentifizierungsverfahren, z.B. Fido basiertem Fingerprint oder FaceID, anmelden.
6. Im letzten Schritt erstellt der nevisAuth eine SAML-Assertion und leitet den Benutzer zurück an die Applikation. Die SAML-Assertion wird von der Applikation konsumiert und verifiziert. Der Benutzer ist damit direkt in der Applikation angemeldet. Das Mapping des Benutzers innerhalb des User-Directory erfolgt anhand der zuvor hinterlegten Pseudonym-Kennung.

Der Ablauf einer Folge-Identifizierung unter Nutzung des nPA ist prinzipiell gleich mit der Ausnahme, dass der Schritt 4 (Mapping im Partner-Directory) übersprungen wird. Der Anmeldevorgang ist nur erfolgreich, wenn der nevisAuth über die REST-Schnittstelle des User-Directorys das hinterlegte nPA Pseudonym findet. Sollte dies nicht der Fall sein, so wird dem Benutzer eine Fehlerseite dargestellt mit dem Hinweis, dass er sich zuerst für die Authentisierung mittels nPA registrieren muss. Um den Registrationsprozess starten zu können, enthält die Fehlerseite direkt einen Link auf den Registrationsprozess.

Das nachfolgende Sequenz-Diagramm zeigt den kompletten Ablauf der Registrierung mittels nPA nochmals im Detail: