Inhalt

[1 Über dieses Dokument 2](#_Toc401143559)

[2 Einführung in Single Sign On 2](#_Toc401143560)

[2.1 „Einmal anmelden, alles nutzen“ 2](#_Toc401143561)

[2.2 Pro: Nutzen von SSO 2](#_Toc401143562)

[2.3 Contra: Stolpersteine beim SSO 2](#_Toc401143563)

[3 Externe SSO Plattformen 3](#_Toc401143564)

[3.1 Die Suche auf dem SSO-Markt 3](#_Toc401143565)

[3.1.1 Kriterium 1: Schnittstellen 4](#_Toc401143566)

[3.1.2 Kriterium 2: Sicherheit 4](#_Toc401143567)

[3.1.3 Kriterium 2: Nutzerfreundlichkeit 5](#_Toc401143568)

[4 Multi-Faktor-Authentifizierung 6](#_Toc401143569)

[4.1 Sinn und Zweck 6](#_Toc401143570)

[4.2 Definition 6](#_Toc401143571)

[4.3 Die 3 Authentifizierungs-Methoden 6](#_Toc401143572)

[4.3.1 Methode 1 (Etwas, das man weiß) 6](#_Toc401143573)

[4.3.2 Methode 2 (Etwas, das man besitzt) 7](#_Toc401143574)

[4.3.3 Methode 3 (Etwas, das man ist, ein persönliches Attribut) 7](#_Toc401143575)

[4.4 Fazit 8](#_Toc401143576)

[5 Social Media Sign On 9](#_Toc401143577)

[6 DAD spezifische Anforderungen 10](#_Toc401143578)

[6.1 Welche Lösungen haben wir schon? 10](#_Toc401143579)

[6.1.1 URL Remote Login 10](#_Toc401143580)

[6.1.2 Sepia-Integration in alle DAD Web Portale 11](#_Toc401143581)

# Über dieses Dokument

Dieses Dokument bietet einen konzeptionellen Überblick rund um das Thema Single Sign-On.

Es werden Lösungsansätze vorgeschlagen, die auch realistisch in die Systeme des DAD und der Christoph Kroschke GmbH eingebunden werden können.

Zudem bietet es einen Überblick über die Lösungen die bereits in den DAD Portalen umgesetzt sind.

# Einführung in Single Sign On

## „Einmal anmelden, alles nutzen“

Mit einem Single Sign-On (SSO) müssen sich Mitarbeiter nur noch einmal anmelden (primär authentifizieren) und das SSO übernimmt das Anmeldeverfahren bei eingebundenen Applikationen nach hinterlegten Regeln. Dies erspart den Usern nicht nur Tipparbeit, sondern auch die lästige Suche nach Passwörtern. Darüber hinaus lässt sich die Sicherheit durch Verschärfung der Passwortregeln erhöhen und die Anmeldung z.B. mit einer Smartcard oder einem Biometrie-Verfahren kombinieren.

Bei der Gesamt-Abmeldung “Single Log-Out” (SLO) kann sich der Benutzer durch einmaliges “Ausloggen” aus allen genutzten Diensten und Applikationen abmelden. So kann niemand den Account missbrauchen, wenn der Anwender z.B. seinen Arbeitsplatz verlässt.

Mit Ergänzungen wie Passwort-Synchronisation, Web-SSO oder Enterprise-SSO lässt sich das vereinfachte und sichere Anmeldeverfahren auf alle Applikationen ausdehnen.

Das “Simplified Sign-On” ist dagegen ein weniger komfortables und nicht besonders sicheres Verfahren. Es vereinfacht die Anmeldung an mehreren Systemen mit den gleichen Anmeldeinformationen durch den Abgleich der Systeme (Synchronisation von User-Name und Passwort untereinander).

## Pro: Nutzen von SSO

* Zugriff auf alle angebundenen Dienste und Anwendungen ohne erneute Anmeldung.
* Zeitersparnis durch Wegfall von Log-In’s (evtl. verbunden mit Suche nach Passwort).
* Weniger Helpdeskanfragen wegen vergessener Passwörter, da sich der Anwender weniger Passwörter merken muss. Und weniger Anfragen bedeuten geringere Auwände.
* Sicherheitssteigerung durch Wegfall der Merkzettel und durch die Ermöglichung strengerer Passwortrichtlinien.
* Besserer Benutzerkomfort und somit höhere Zufriedenheit.

## Contra: Stolpersteine beim SSO

* Nicht alle SSO Systeme unterstützen den gleichen Umfang an Applikationen und Systemen.   
  Es ist sorgfältig zu prüfen, ob wirklich sämtliche Applikationen   
  (z.B. Unix Applikationen im x-Window, Web Applikationen, Applikationen mit Kerberos Unterstützung, Apps, etc.) vollständig von allen SSO Funktionen unterstützt werden. Dazu zählen nicht nur der Anmeldevorgang sondern auch der automatische Passwort-Reset und der automatische zyklische Tausch der Passwörter im Hintergrund.
* Oft wird das SSO nur für eine Auswahl an Applikationen umgesetzt, weil sich die technische Komplexität der vielfältigen Systeme (AD, LINUX, HOST, SAP, Mobile-Devices, Web-Applikationen, gehostete Systeme) und deren Vielzahl kaum beherrschen lässt.
* Die Wenigsten konzipieren das SSO als Zwei-Faktor Authentifizierung zusammen mit Smartcard, Biometrie oder anderen Verfahren. Das ist aber ratsam, da bei SSO das Passwort extrem mächtig ist (möglicher Komplettzugang!) und ein Ausspähen fatale Folgen hätte. Viele übersehen, dass die meisten SSO Produkte keine Managementkomponente besitzen   
  (“Wer darf SSO nutzen?”, “Welche Applikationen darf ein User nutzen?”, etc).
* Häufig werden wesentliche Aspekte des Passwortspeichers übersehen:   
  Ist der Passwortspeicherverschlüsselt? Wo ist er abgelegt? Ist er auch offline verfügbar?   
  Wie wird er synchronisiert? Werden Verzeichnisse als Repository unterstützt?

# Externe SSO Plattformen

## Die Suche auf dem SSO-Markt

Betrachtet man den Markt für SSO-Lösungen, sind gerade in der jüngsten Zeit viele neue Anbieter hinzugekommen. Der SSO-Markt ist in Bewegung, auch wegen der stetigen Zunahme an betrieblich genutzten Smartphones und Tablets, der steigenden Nutzung von Cloud-Diensten und der zunehmenden Bedeutung von Social Media im Unternehmen.

Die Vielfalt an unterstützten Anwendungen ist bei solchen SSO-Lösungen in der Regel groß. Verschiedene SSO-Plattformen berücksichtigen auch Identitätsdienste wie OpenID, CloudMinder zum Beispiel auch die Verwendung der Facebook- oder Google-Zugangsdaten bei Websites, die diese Art der Anmeldung unterstützen.

Einer der führenden Identitätsdienste im Internet ist OpenID.  
SSO Plattformen, die z. B. OpenID als Identitätsanbieter und Anmeldeverfahren vorsehen, können nach einmaligem Login des Nutzers die Anmeldung an allen Webseiten vornehmen, die den Identitätsdienst OpenID integriert haben. Welche dies sind, findet man unter anderem in einem OpenID-Verzeichnis.

Soziale Netzwerke wie Facebook, Twitter und Google+ bieten sich inzwischen ebenfalls als Identitätsdienst an. Man spricht auch von Social-Log-In-Diensten.

Die Lösung NetIQ Social Access zum Beispiel ermöglicht es Unternehmen, ihren Kunden oder Partnern eine Anmeldung mit einem der Social Log-Ins anzubieten, also für die Anmeldung die Zugangsdaten eines bestimmten sozialen Netzwerkes zu verwenden.

Unternehmensanwendungen, Mobile und Cloud Neben Anwendungen, die im internen Netzwerk betrieben oder aus einer Cloud bezogen werden, sind es die mobilen Apps, die für den betrieblichen Einsatz zunehmend wichtig werden.

IBM Security Access Manager for Cloud and Mobile zum Beispiel vereinheitlicht den Zugang zu verschiedenen Cloud-Diensten und die Anmeldung für bestimmte mobile Apps.

Lösungen wie SecureAuth IdP bieten für mehrere mobile Plattformen spezielle Apps an, die die Nutzer auf ihr Smartphone oder Tablet laden, um das Single-Sign-On mobil nutzen zu können.

CloudAccess SaaS SSO, Symplified, Symantec O3 oder PingOne bieten eine zentrale Nutzeranmeldung für zahlreiche, unterstützte Cloud-Dienste, darunter Google Apps, Salesforce.com oder MS SharePoint.

Für die SSO-Plattform MyAccessLive gibt es mobile Zugriffsmöglichkeiten, mit denen Administratoren Nutzeranfragen zu neuen oder geänderten Zugängen mobil bearbeiten können.

### Kriterium 1: Schnittstellen

Grundlegend für jedes SSO-Verfahren ist dessen Integrierbarkeit - genauer gesagt die Vielfalt an Schnittstellen-, die darüber entscheidet, ob man wirklich von einer einheitlichen, zentralen Anmeldung sprechen kann, oder ob gleich mehrere Anwendungen, die das Unternehmen einsetzt, nicht unterstützt werden.

Ein SSO-Verfahren, das tatsächlich alle eingesetzten Anwendungen einbinden kann, ist kaum zu finden. Doch die entscheidenden Anwendungen eines Unternehmens sollten durch die SSO-Lösung der Wahl unterstützt werden.

Zu beachten sind dabei insbesondere die von der jeweiligen SSO-Lösung unterstützten Standards, Verzeichnisdienste (wie Active Directory oder OpenLDAP), Identitätsdienste und Anwendungen im Netzwerk und in der Cloud, zudem mobile Anwendungen und Social-Media-Plattformen.

Unterstützte Standards und Identitätsdienste Lösungen wie CA CloudMinder, SurePassID oder IBM Tivoli Federated Identity Manager unterstützen Autorisierungsstandards für Web-, Desktop- und mobile Applikationen wie OAuth, die Web-Spezifikation WS-Federation und das SAML-Framework **[[1]](#footnote-1)**.

Damit sind wichtige technische Voraussetzungen für den standardisierten Austausch von Zugangsdaten mit zahlreichen Applikationen gegeben.

### Kriterium 2: Sicherheit

Bei einem SSO-Verfahren sollten Vorgaben für komplexe Passwörter und verschlüsselte Anmeldeverfahren Standard sein. Gelänge es einem Unbefugten, den zentralen Zugang zu knacken, hätte er in der Regel Zugang zu allen angebundenen Anwendungen.

Abhängig vom jeweiligen Schutzbedarf, den internen Richtlinien und den für das Unternehmen geltenden Compliance-Vorgaben sollten deshalb auch Mehr-Faktor-Authentifizierungen möglich sein. Bei Identity and Management Plattformen (IAM) wie Aveksa MyAccessLive oder SecureAuth IdP zum Beispiel kann das SSO-Passwort richtlinienabhängig um weitere Faktoren wie einem Einmal-Passwort (OTP) ergänzt werden.

Ob eine einfache Passwortanmeldung für die SSO-Anmeldung reicht oder nicht, entscheidet beispielsweise CA CloudMinder auf Basis des aktuellen Risk Score. Dieser hängt unter anderem davon ab, wo sich der Nutzer aktuell befindet, welches Gerät für die Anmeldung genutzt wird, welche Aktionen der Nutzer vornehmen möchte und ob die geplanten Aktionen des Nutzers mit seinen Aktivitäten in der Vergangenheit zusammen passen.

### Kriterium 2: Nutzerfreundlichkeit

Eine SSO-Lösung sollte sich auch durch ihre Nutzerfreundlichkeit auszeichnen - sowohl für Standardanwender als auch für Administratoren.

Bei Cloud-basierten Lösungen wie Aveksa MyAccessLive, CloudAccess SaaS SSO, OneLogin, McAfee Cloud Single Sign On (SaaS Edition) oder PingOne entfallen Installationsaufwände, denn die zentrale Administration und die SSO-Anmeldung durch die Nutzer erfolgen über den Webbrowser.   
Allerdings ist bei Cloud-basierten SSO-Lösungen die hohe Verfügbarkeit des Dienstes von zentraler Bedeutung, ebenso die Betreibersicherheit, da die Identitätsdaten vor Unbefugten geschützt sein müssen.

Mobile Administrationszugriffe sind bei vielen Lösungen möglich.   
So können Administratoren und Entscheider mit der Android- oder iPhone-App MyAccessMobile Nutzeranfragen zu neuen oder geänderten Zugängen und Berechtigungen mobil bearbeiten.

CA CloudMinder, SecureAuth IdP oder IBM Tivoli Federated Identity Manager ermöglichen unter anderem das Zurücksetzen des Nutzerpasswortes als Self-Service.

Solche Funktionen, mit denen Nutzer bestimmte Zugangsprobleme wie ein vergessenes Passwort selbst lösen können, erhöhen die Nutzerakzeptanz und entlasten die Administratoren.

# Multi-Faktor-Authentifizierung

## Sinn und Zweck

Die Multi-Faktor-Authentifizierung bietet eine weitaus höhere Sicherheit bei der Anmeldung von Usern an Softwaresystemen als Standard Authentifizierungen mit ausschließlich User und Passwort.

Z. B. könnte der DAD speziell seinen Kunden mit erhöhten Sicherheitsanforderungen (wie z. B. der FORD Bank) diese Art der Authentifizierung zusätzlich anbieten.

## Definition

Um den Begriff der Multi-Faktor-Authentifizierung zu erklären, muss man zunächst die verschiedenen Arten der Authentifizierung beschreiben. Hier also zunächst einige notwendige, wenn auch etwas langwierige Erläuterung:

„*Die Authentifizierung ist ein Vorgang, bei dem eine Person oder eine Computersoftware ihre Identität nachweist, um Zugriff auf Informationen zu erhalten. Die Identität der Person ist eine einfache Aussage, z. B. die Login-ID für eine bestimmte Computeranwendung. Der zu erbringende Nachweis spielt bei dem Begriff die wichtigste Rolle.*“

In dieser Definition ist bereits das größte Problem im Hinblick auf die Authentifizierung enthalten: Wie kann man sicherstellen, dass die Person an der Tür wirklich diejenige ist, die sie zu sein vorgibt? Ihre wahre Identität muss mithilfe einer Frage an diese Person überprüft werden. Es gibt verschiedene Fragekategorien für einen solchen Fall. Dabei handelt es sich um die folgenden Prüfmethoden:

1. Etwas, das man weiß (Wissen)
2. Etwas, das man besitzt
3. Etwas, das man ist (persönliches Attribut)

Im Folgenden werden die 3 Methoden beschrieben:

## Die 3 Authentifizierungs-Methoden

### Methode 1 *(Etwas, das man weiß)*

Methode 1 ist recht klar:   
Hier ist sowohl ein Benutzername als auch ein Kennwort erforderlich. Diese Angaben muss sich der Benutzer merken, und diese Angaben bleiben zumindest eine Zeit lang unverändert. Um also auf das Account einer Person zugreifen zu können, reicht es aus, sich diese Angaben vom rechtmäßigen Eigentümer auf welche Weise auch immer zu beschaffen.

Vorteile:

* Für jeden einfach zu nutzen
* Relativ kostengünstige Implementierung

Nachteile:

* Sichere Kennwörter müssen notwendigerweise komplex sein.
* Kennwörter werden manchmal vergessen.

Es gibt keine weiteren Sicherheitsstufen, sodass es recht einfach ist, das Kennwort zu knacken (z. B. Wörterbuchangriff, Spyware, Social Engineering, Phishing).

### Methode 2 *(Etwas, das man besitzt)*

Zum Erläutern der zweiten Methode müssen wir etwas weiter ausholen:   
Diese Kategorie beschreibt z. B. Geräte im Besitz des Account-Eigentümers, wie etwa einen TAN-Generator, ein Mobiltelefon für den Empfang von mTANs, einen speziellen Token-Generator o. Ä. In den meisten Fällen sind die Codes, die mit solchen Geräten generiert werden, nur ein Mal verwendbare Kennwörter, die sich bei jeder Anmeldung ändern.   
Das ist im Hinblick auf die Sicherheit natürlich sinnvoll.

Das Ausspähen eines nur einmal verwendbaren Kennworts mithilfe eines Keyloggers oder einer Spyware nützt einem Unbefugten nicht unbedingt, um sich Zugang zum Account des Opfers verschaffen zu können (es sei denn, er ist in der Lage, den Browser zu kompromittieren, nachdem er den Computer mit einem speziellen Trojaner infiziert hat, doch das ist wieder eine ganz andere Geschichte).   
Schlauer wäre es hingegen, das betreffende Gerät zu stehlen, zumindest dann, wenn diese Authentifizierungsmethode nicht mit einer weiteren Methode kombiniert wird.

Vorteile:

* Die Bandbreite möglicher Authentifizierungsgeräte ist groß.
* Zusätzliche Einführung einer Sicherheitsstufe.

Nachteile:

* Das Authentifizierungsgerät kann verloren gehen oder gestohlen werden.
* Die Methode schafft ein falsches Gefühl der Sicherheit, wenn die Authentifizierung auf dem Anmeldegerät (z. B. Mobiltelefon) erfolgt.

### Methode 3 *(Etwas, das man ist, ein persönliches Attribut)*

Die dritte Methode ist ebenfalls schnell erklärt:   
Zu dieser Kategorie zählen Fingerabdruck-, Iris-, DNA- und Spracherkennung sowie einige weitere persönliche Merkmale, kurz gesagt: biometrische Daten. Diese Merkmale gelten gemeinhin als diebstahlsicher, doch auch das ist nicht ganz richtig. Nicht immer ist es nötig, so wie in manchen Hollywood-Filmen dargestellt, mit dem Löffel einen Augapfel aus der Augenhöhle des Opfers zu entfernen, um sich illegalen Zugang zu dessen Accounts zu verschaffen. Oft reicht es schon aus, sich den mithilfe der Iris ermittelten Hashwert zu verschaffen, einen eindeutigen, errechneten Wert. Ebenso ist es durchaus möglich, eine Kopie eines Fingerabdrucks anzufertigen, die ihren Zweck aufs Beste erfüllt. Natürlich ist es in den meisten Fällen ziemlich aufwendig, biometrische Daten zu entwenden oder zu kopieren. Daher ist es ziemlich unwahrscheinlich, dass sich jemand auf diese Art und Weise beispielsweise unbefugten Zugriff auf eine Online-Spiele-Community verschafft. Diese Methode wird derzeit vorwiegend für ausgereifte Authentifizierungszwecke als Ein-Faktor-Authentifizierung oder als Teil einer Multi-Faktor-Authentifizierung genutzt.

Vorteile:

* Höhere Sicherheitsstufe.
* Es gibt keine Kennwörter, die man vergessen könnte.
* Idealerweise können biometrische Identifizierungsmerkmale (Finger, Augen, usw.) nicht verloren gehen oder gar gestohlen werden.

Nachteile:

* Höhere Implementierungskosten.
* Wie jede andere Sicherheitslösung ist auch diese Methode nicht hundertprozentig sicher.
* Es besteht die Gefahr, dass Dritte ein eindeutiges Bewegungsprofil der betreffenden Person erstellen könnten.
* Wenn der errechnete Hashwert gestohlen wird, kann er nicht ersetzt werden.

Damit eine Zwei-Faktor-Authentifizierung vorliegt, muss eine Kombination von zwei verschiedenen, voneinander völlig unabhängigen Authentifizierungsmethoden eingesetzt werden.

Eine Kombination aus Benutzername und Kennwort reicht nicht aus, da beide Merkmale Teil der ersten Authentifizierungsmethode sind.

Für eine Zwei-Faktor-Authentifizierung muss mindestens ein nur einmal verwendbares Kennwort an ein unabhängiges Gerät versendet werden, z. B. an ein Mobiltelefon.   
Im Regelfall ist eine Zwei-Faktor-Authentifizierung auch eine Zwei-Wege-Authentifizierung.   
Dies ist aber nicht der Fall, wenn das Anmeldegerät und das Empfangsgerät für das nur ein Mal verwendbare Kennwort identisch sind.   
In diesem Szenario fehlt das zweite, unabhängige Element. Man denke nur an eine Spyware auf dem betreffenden Smartphone, die in der Lage wäre, alle erforderlichen Anmeldedaten (Benutzername, Kennwort und das ein Mal verwendbare Kennwort) von nur einem einzigen Gerät auszuspionieren. Praktische Probleme mit der digitalen Multi-Faktor-Authentifizierung auf Mobilgeräten Im Folgenden geht es um die Probleme, mit denen sich viele Banken heutzutage konfrontiert sehen.

## Fazit

Zweifelsohne sind Multi-Faktor-Authentifizierung und Mehrwege-Authentifizierung sicherer als Ein-Faktor- und Ein-Wege-Authentifizierung.

Der Bedarf an sicheren, wirkungsvollen Authentifizierungsmethoden wird immer größer, insbesondere angesichts der ständigen Verfügbarkeit des Internets auf Mobilgeräten und der dadurch fast rund um die Uhr bestehenden Zugriffsmöglichkeit.

Bei alldem muss jedoch für ein individuell ausgewogenes Verhältnis zwischen Benutzerfreundlichkeit und Sicherheitsanforderungen gesorgt werden.

***DAD Empfehlung:  
Aufgrund des hohen Implementierungs- sowie Wartungs-Aufwands empfehlen wir dem DAD die Multi-Faktor-Authentifizierung nur für „zahlungskräftige“ Kunden mit erhöhten Sicherheitsanforderungen, wie z. B. Banken und Leasinggesellschaften.***

# Social Media Sign On

# DAD spezifische Anforderungen

## Welche Lösungen haben wir schon?

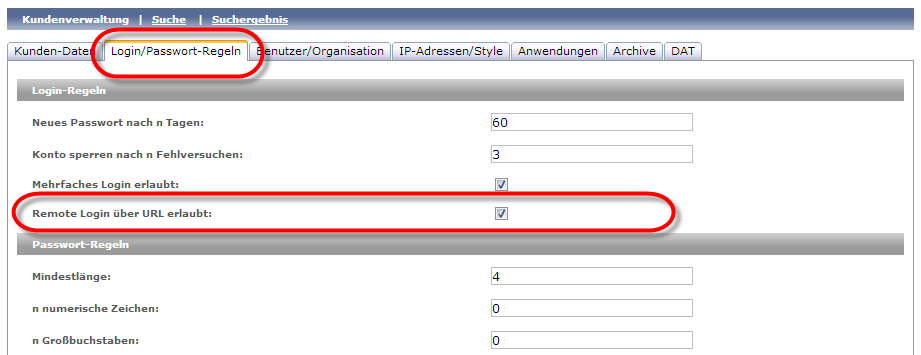
### URL Remote Login

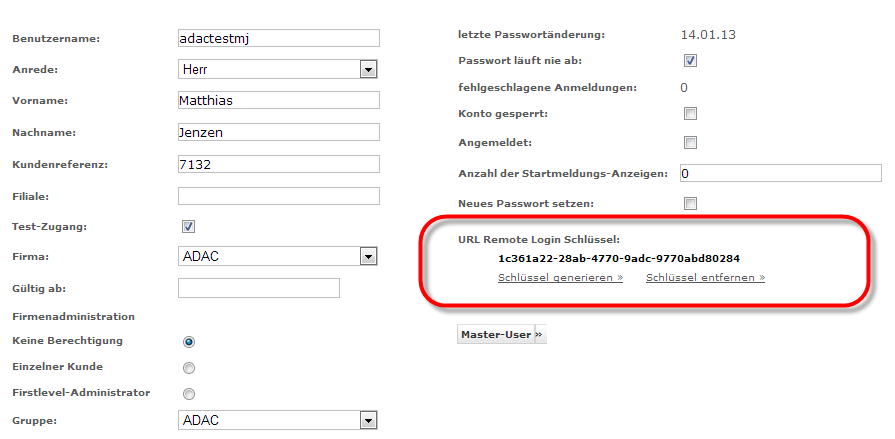
Auf Kundenanforderung (Kunde ANAG) haben wir im Jahr 2013 die DAD Portale mit einem so genannten URL Remote Login Verfahren erweitert.

Über dieses Verfahren sind Kunden in der Lage, über ihre eigene Software (temporär) gültige Login Links zu erzeugen und ihre eigenen User automatisiert über diese Links in die DAD Portale einzuloggen.

Aus Sicherheitsgründen haben die Login Links nur eine kurze Gültigkeit.

Zudem stellten wir dem Kunden einen Algorithmus bereit, über den sichergestellt ist, dass nur er und wir er diese Links generieren + interpretieren können.

*Screenshots, Services Portal / Admin Section:   
1. Customer Management:*

*2. User Management:*

### Sepia-Integration in alle DAD Web Portale

Das Applikationen „Inventory Management“ und „Floorcheck“ werden im DAD Netzwerk auf einem hauseigenen DAD Server über ein separates Web Portal gehostet.  
Dieses Web Portal mit dem Namen „Xaris“ wurde von einem externen Dienstleister programmiert.

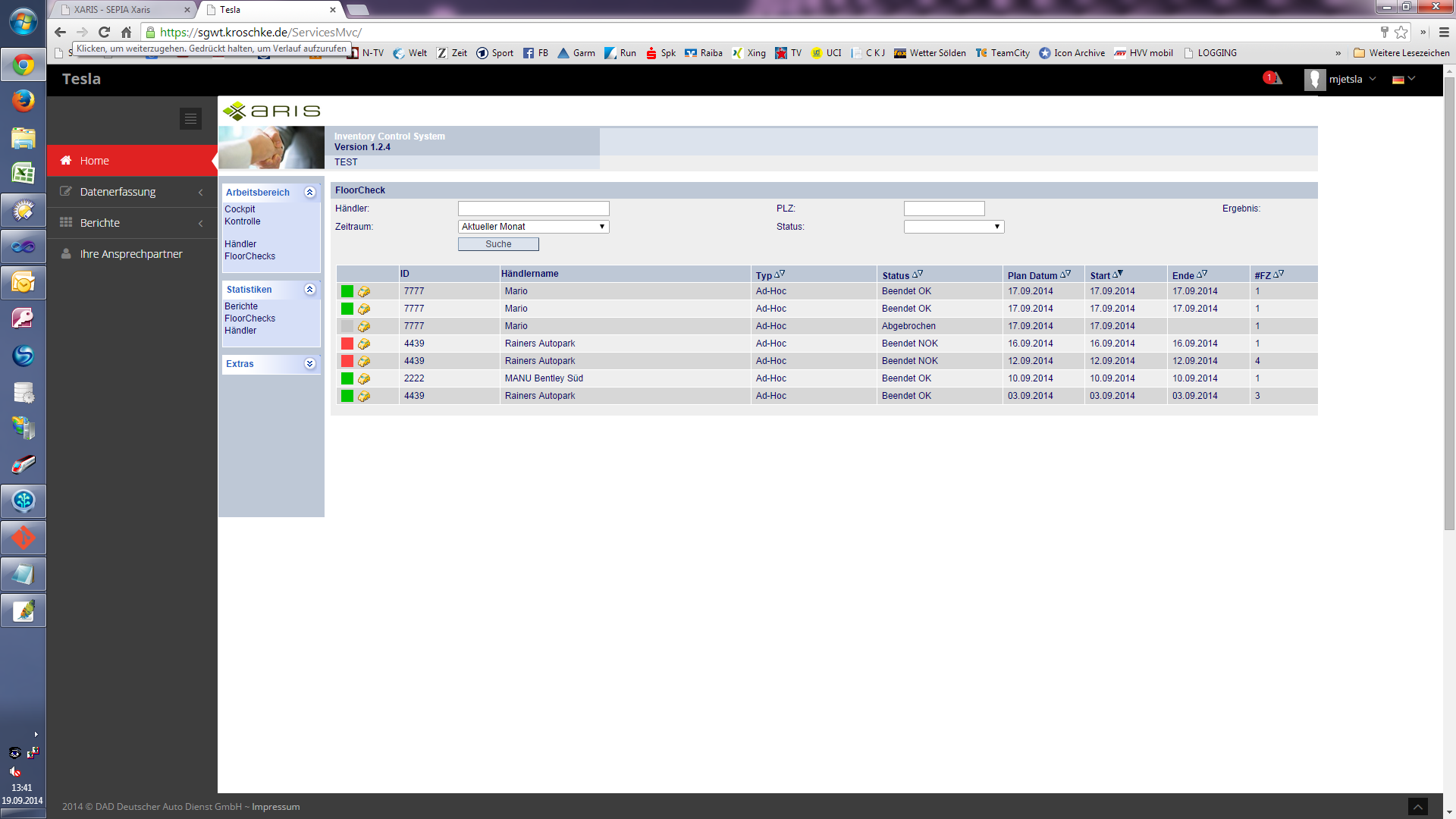
Nachteile:

* Unsere Portal User benötigen für das Xaris Systems ein separates Login.  
  Die Folge sind lästige doppelte Login Prozeduren.
* Paralleles Arbeiten einerseits in den DAD Portalen und andererseits im Xaris System funktioniert nur über separate Browser Fenster.  
  Eine nahtlose Integration wäre hier wünschenswert.

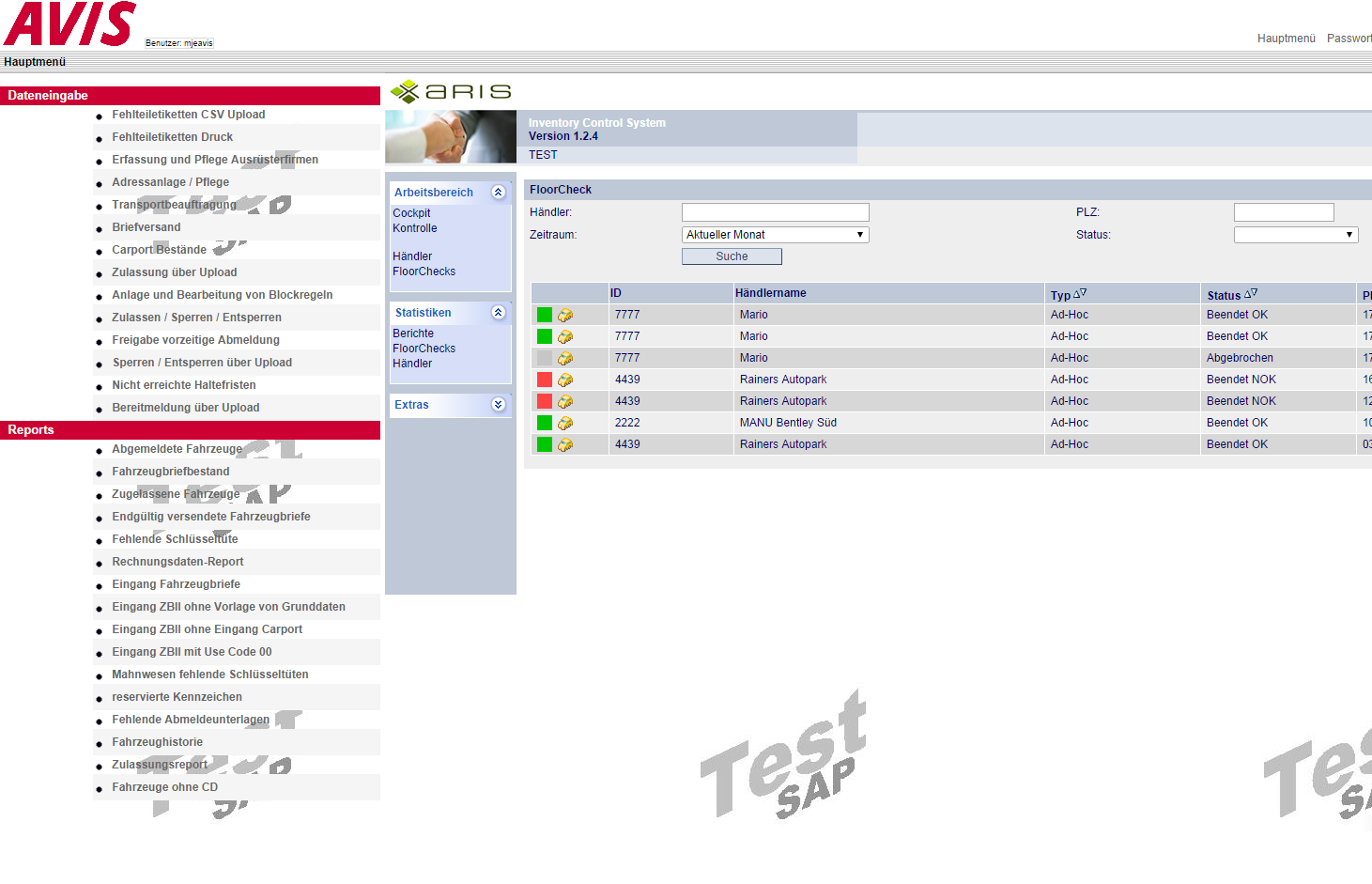
Lösung:  
Mit dem Hersteller des Xaris Systems wurde die Implementierung einer individuellen SSO Lösung vereinbart, über das

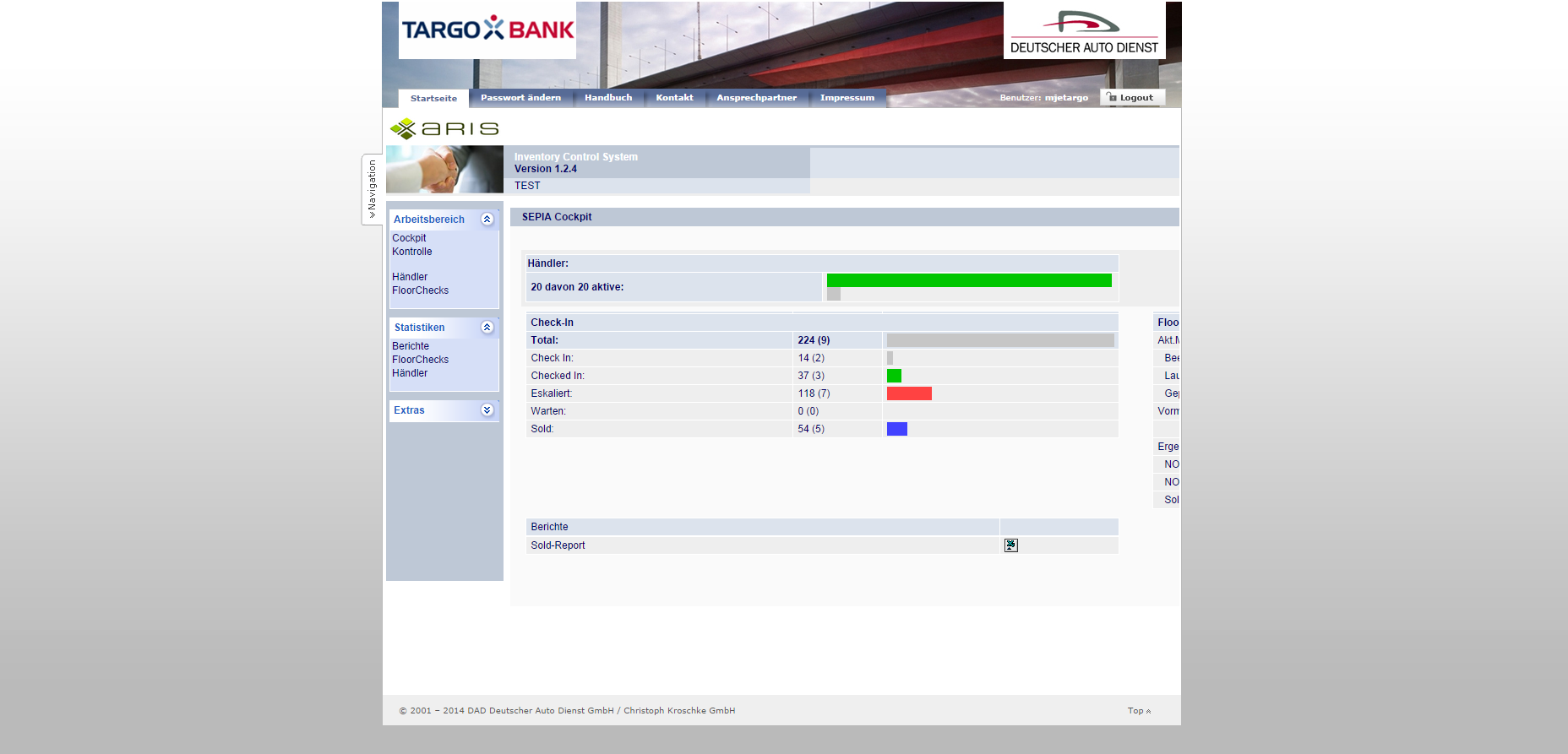
* die Xaris Website nahtlos in die alle 3 DAD Kundenportale integriert wird
* nur noch eine User Verwaltung notwendig ist, die zudem eine reibungslose automatisierte Synchronisation der Benutzerdaten zwischen den beiden Systemdatenbanken sicherstellt.

*Screenshot, Integration Xaris⬄ DAD Metronic Portal*



*Screenshot, Integration Xaris ⬄ klassisches DAD Portal*



*Screenshot, Integration Xaris ⬄ DAD Services Portal*

1. Die Security Assertion Markup Language (kurz SAML) ist ein XML-Framework zum Austausch von Authentifizierungs- und Autorisierungsinformationen. Sie stellt Funktionen bereit, um sicherheitsbezogene Informationen zu beschreiben und zu übertragen. [↑](#footnote-ref-1)