***SSO - Single Sign On***

*Ein konzeptioneller Überblick für*

ckg-logo.png

****

*Matthias Jenzen, CKG Entwicklung, November 2014*

Inhalt

[1 Über dieses Dokument 3](#_Toc402446121)

[2 Einführung in Single Sign On 3](#_Toc402446122)

[2.1 Definition 3](#_Toc402446123)

[2.2 „Einmal anmelden, alles nutzen“ 4](#_Toc402446124)

[2.3 Pro: Nutzen von SSO 4](#_Toc402446125)

[2.4 Contra: Stolpersteine beim SSO 4](#_Toc402446126)

[3 Externe SSO Plattformen 5](#_Toc402446127)

[3.1 Die Suche auf dem SSO-Markt 5](#_Toc402446128)

[3.1.1 Kriterium 1: Schnittstellen 6](#_Toc402446129)

[3.1.2 Kriterium 2: Sicherheit 6](#_Toc402446130)

[3.1.3 Kriterium 2: Nutzerfreundlichkeit 7](#_Toc402446131)

[4 Multi-Faktor-Authentifizierung 8](#_Toc402446132)

[4.1 Sinn und Zweck 8](#_Toc402446133)

[4.2 Definition 8](#_Toc402446134)

[4.3 Die 3 Authentifizierungs-Methoden 9](#_Toc402446135)

[4.3.1 Methode 1 (Etwas, das man weiß) 9](#_Toc402446136)

[4.3.2 Methode 2 (Etwas, das man besitzt) 9](#_Toc402446137)

[4.3.3 Methode 3 (Etwas, das man ist, ein persönliches Attribut) 10](#_Toc402446138)

[4.4 Fazit 11](#_Toc402446139)

[5 Social Media SSO mit Facebook, Twitter & Co. 12](#_Toc402446140)

[5.1 Technischer Ablauf 12](#_Toc402446141)

[5.2 Implementierungslösungen für CKG/ DAD 13](#_Toc402446142)

[5.2.1 Anbindung über externe Social-Connect Provider 13](#_Toc402446143)

[5.2.2 Eigenprogrammierung 14](#_Toc402446144)

[6 CKG/DAD spezifische Anforderungen 15](#_Toc402446145)

[6.1 Welche Lösungen haben wir schon? 15](#_Toc402446146)

[6.1.1 URL Remote Login 15](#_Toc402446147)

[6.1.2 Sepia-Integration in alle DAD Web Portale 16](#_Toc402446148)

[6.1.3 Fazit zu unseren bestehenden Lösungen 18](#_Toc402446149)

[6.2 Welche Lösungen im erweiterten SSO Kontext können wir künftig anbieten? 19](#_Toc402446150)

[6.2.1 Benutzer-individuelle Downloadressourcen 19](#_Toc402446151)

[6.2.2 Zeitlich begrenzte Anwendungs-Sets 20](#_Toc402446152)

# 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 CKG/DAD Portalen umgesetzt sind.

# Einführung in Single Sign On

## Definition

Single Sign-On (Abkürzung „SSO“) bezeichnet die Möglichkeit, dass sich ein Nutzer nach einer einmaligen Identifizierung bei einem SSO Anbieter auf verschiedenen Portalen im Internet mit dieser SSO Kennung anmelden kann. Hierfür muss der Betreiber des Internetportals mit einem oder mehreren der SSO Dienste zusammenarbeiten, um eine Registrierung auf diese Art zu gewährleisten.

Während sich der Nutzer auf einer Portalseite über einen SSO Dienst anmeldet, muss er zur Bestätigung die Anmeldung des Portals manuell authentifizieren. Nach diesem Schritt ist sein SSO Konto mit demjenigen der Portalseite verbunden und er kann sich mit dem SSO Konto einloggen, bzw. bleibt stets eingeloggt sofern er dies wünscht.

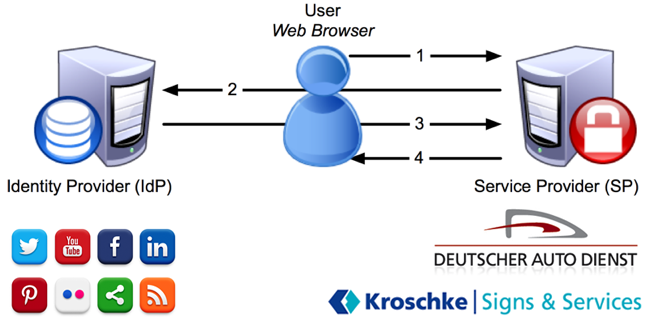


Abbildung 1: Der "Single Sign On" Workflow

Der Vorteil für den Nutzer besteht darin, dass er sich nicht auf jeder Portalseite, auf der er ein Konto anlegen möchte, mit neuen Benutzernamen und Passwörtern anmelden muss. Durch sein Konto beim SSO Dienst hat er einen einmaligen Schlüssel, dessen Zugangsdaten er sich merken muss. Zusätzlich kann er beim SSO Anbieter einsehen, welche Dienste er bereits authentifiziert hat.

## „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 [[1]](#footnote-1) oder Enterprise-SSO [[2]](#footnote-2) 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 **[[3]](#footnote-3)**.

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.



***Empfehlung an CKG / DAD***

*Die externen SSO Lösungen seien hier nur der Vollständigkeit erwähnt.  
Sie kommen meist mit hohen Investitionskosten für Software und Server Hardware einher, gefolgt von einem nicht zu unterschätzenden Administrations- und Schulungsaufwand.*

# 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.*“

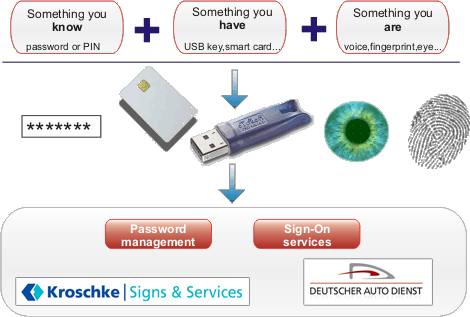


Abbildung 2: Die 3 Prüfmethoden zur Authentifizierung

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.



***Empfehlung an CKG / DAD***

*Aufgrund des nicht zu unerheblichen 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.*

# foto-social-media.jpgSocial Media SSO mit Facebook, Twitter & Co.

Social Media Portale wie Facebook, Google+ oder Twitter bieten die praktische Möglichkeit einer Benutzer Authentifizierung für eigene Web Portale.

Der Vorteil für den Web Benutzer besteht darin, dass er sich nicht auf jeder Portalseite, auf der er ein Konto anlegen möchte, mit neuen Benutzernamen und Passwörtern anmelden muss.

Durch sein Konto beim SSO Dienst hat er einen einmaligen Schlüssel, dessen Zugangsdaten er sich merken muss. Zusätzlich kann er beim SSO Anbieter einsehen, welche Dienste er bereits authentifiziert hat.

## Technischer Ablauf

Während sich der User auf einer Portalseite über einen Social Media Portal wie Facebook, Google+ oder Twitter anmeldet, muss er zur Bestätigung die Anmeldung des Portals manuell authentifizieren. Nach diesem Schritt ist sein SSO Konto mit demjenigen der Portalseite verbunden und er kann sich mit dem SSO Konto einloggen, bzw. bleibt stets eingeloggt sofern er dies wünscht.

Für CKG/DAD besteht der Vorteil darin, den Usern den Zugang zum den eigenen Portalen zu vereinfachen.

Durch die Verbreitung der SSO Dienste bietet es sich für Portalseiten an, SSO als Anmeldeverfahren zu verwenden. Auf der anderen Seite muss ein Portal beachten, dass es potenzielle Nutzer verliert, wenn es sich lediglich auf einen SSO Dienst beschränkt und keine zusätzliche Möglichkeit anbietet, sich auf der Seite anzumelden. Alle Besucher, die kein Konto beim eingesetzten SSO Dienst besitzen, könnten sich nicht registrieren.

Die Social Media SSO Dienste, die am meisten eingesetzt werden, sind

* Facebook Connect / Open Graph (SSO Dienst von Facebook)
* OAuth **[[4]](#footnote-4)**
* OpenSocial (SSO Dienst von Google) **[[5]](#footnote-5)**
* OpenID **[[6]](#footnote-6)**

## Implementierungslösungen für CKG/ DAD

Für die so genannte “Social Connect” Anbindung der eigenen Portale stehen 2 Varianten zur Verfügung:

* Anbindung über externe Social-Connect Provider
* Eigenprogrammierung, Integration der SSO Social Media Dienste über deren API

### Anbindung über externe Social-Connect Provider

Externe Service Dienstleister wie [www.ca.com](http://www.ca.com) bieten erweiterte Authentifizierung und Single Sign-On (SSO) und helfen Portalbetreibern wie den DAD, sicheren Zugriff auf seine Web-Anwendungen zu ermöglichen, ohne seine End User zu behindern.

Mit einer zentralen Plattform für SSO, Zugriffsmanagement und Authentifizierung können sich die hauseigenen Entwickler auf die eigene Geschäftslogik konzentrieren und neue Anwendungen schneller fertig stellen.

Vorteil:

* Geringer Implementierungsaufwand bezüglich Eigenentwicklung,   
  hier sind nur Schnittstellenanbindungen bezüglich User Account Informationen umzusetzen.

Nachteile:

* Monatliche Gebühren für die Nutzung des externen SSO Services
* Ein Hacker-Angriff auf den Social-Connect-Provider bedeutet auch den ungewollten Zugriff auf alle angeschlossenen Netzwerke/Seiten,   
  => also auch auf die CKG/DAD Portale.
* Der Social-Connect-Provider des Vertrauens kann von einer unseriösen Firma übernommen werden.
* Der Social-Connect-Provider kann ggfls. seinen Dienst einstellen.   
  => Interner Umstellungsaufwand ggfls. zu unpassendem Zeitpunkt wäre die Folge.



***Empfehlung an CKG / DAD***

*Die Wahl eines potenziellen externen SSO Dienstes sollte sehr genau abgewogen werden - immer vor dem Hintergrund, dass man sich in eine potentielle Abhängigkeit von einem externen Software Dienstleister begibt.*

*Da die Nachteile klar den Vorteilen überwiegen, empfehlen wir hier mit Bedacht vorzugehen.*

### Eigenprogrammierung

Bei dieser Variante erfolgt die Integration der SSO Social Media Dienste über deren Programmier API.

Die hauseigenen Entwickler programmieren die SSO API der Social Media Netzwerke in Form einer Schnittstelle direkt an und bekommen Informationen über die eigenen Portal User bereits in authentifizierter Form übergeben.

Die Verknüpfung zwischen Social Media Account und CKG/DAD Portal Account erfolgt über eindeutige Benutzer Merkmale wie E-Mail in Kombination mit Vor- und Nachnamen.  
Bei Bedarf können bestimmte Kunden oder Benutzer für diesen Social Media Connect Service in der Kunden bzw. User Administration der CKG/DAD Portale frei geschaltet werden.

Für jeden Social Media Dienst muss diese Schnittstelle separat, aber nur einmalig programmiert werden.

Den Implementierungsaufwand pro Schnittstelle schätzen wir auf durchschnittlich 2 Manntage.  
Am Beispiel des Google+ Netzwerks haben wir innerhalb der CKG Entwicklung bereits Erfahrung gesammelt.

Zusätzlich fällt ein einmaliger Aufwand von ca. 2 Manntagen für die generelle Erweiterung der Kunden- und User-Verwaltung an, wie z. B. Administrations-Masken und Social Login Buttons.



Vorteile:

* Unabhängigkeit von externer Software / Dienstleistern.
* Volle Flexibilität bei der Authentifizierung über die bestimmte User Merkmale
* Möglichkeit der gezielten „Scharfschaltung“ ggfls. nur bestimmter Social Media Connectoren pro Kunde.

Nachteil:

* Für jedes neu entstehendes Social Media Netzwerk muss einmalig eine eigene Schnittstelle zu den CKG/DAD Portalen programmiert werden.  
  Der Aufwand pro Schnittstelle fällt aber nur einmalig an und ist mit ca. 2 Manntagen zudem überschaubar.



***Empfehlung an CKG / DAD***

*Aufgrund der Unabhängigkeit von externen Dienstleistern sowie der großen Flexibilität bei der SSO Authentifizierung gepaart mit überschaubarem und zudem nur einmalig anfallenden Implementierungsaufwandes für die SSO Schnittstellen   
=> ist die Lösung „Eigenprogrammierung“ unser klarer Favorit!*

# CKG/DAD spezifische Anforderungen

## Welche Lösungen haben wir schon?

### URL Remote Login

Auf Kundenanforderung (Kunde ANAG) haben wir im Jahr 2013 speziell in 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.

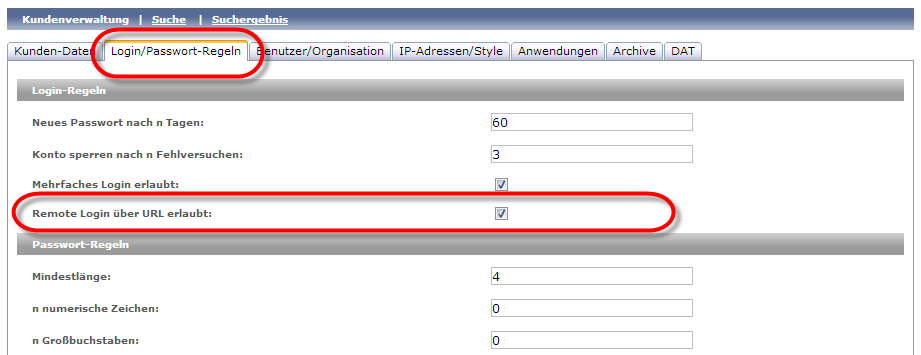
*Screenshots, Services Portal / Admin Section:*

Abbildung 3: Screenshot „Customer Management”

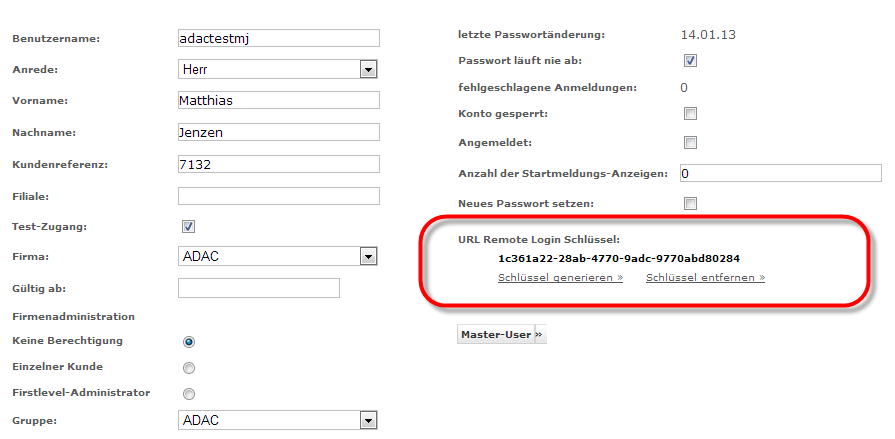


Abbildung 4: Screenshot „User Management“

### Sepia-Integration in alle DAD Web Portale

Die 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.

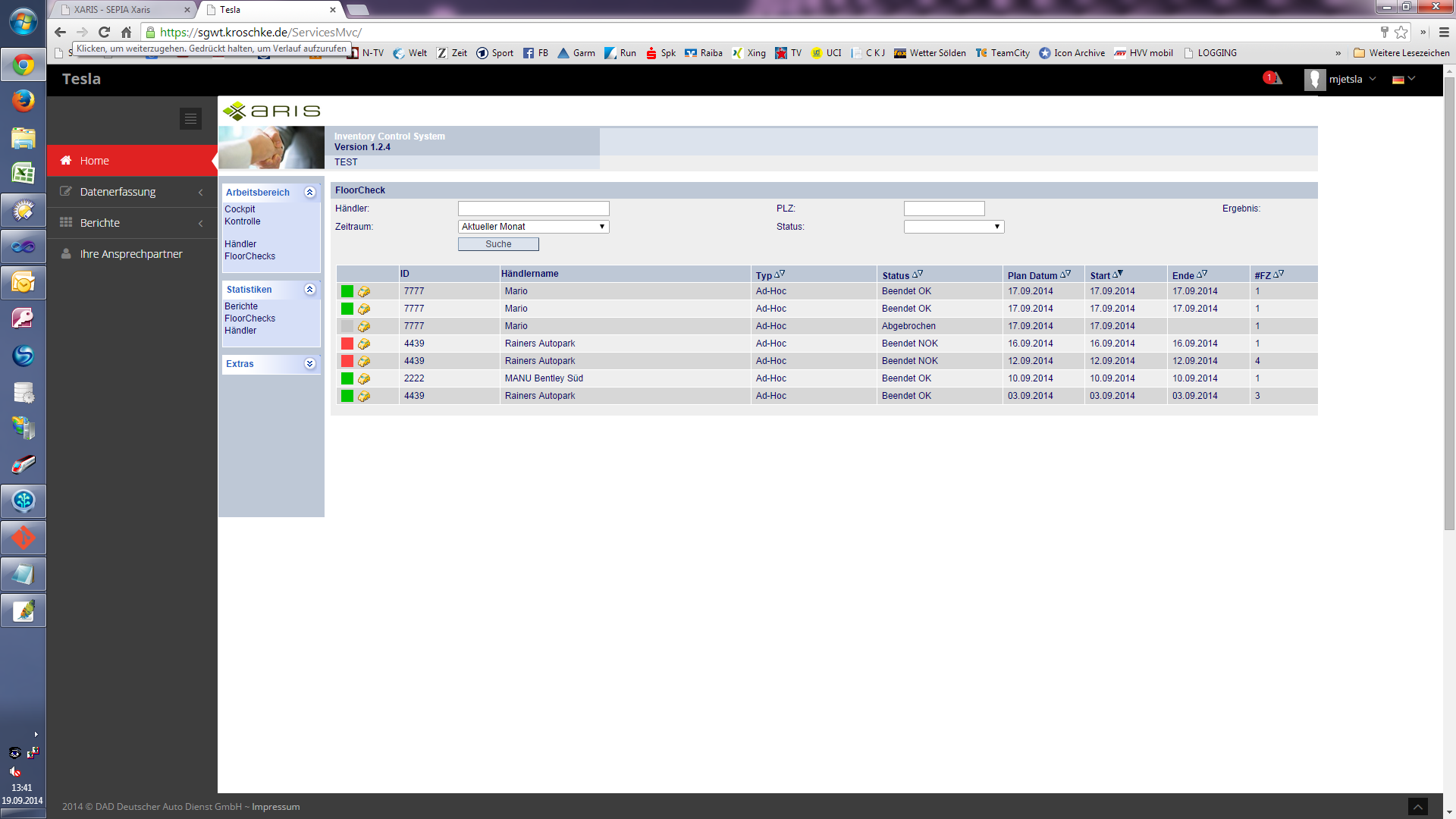


Abbildung 5: Integration Xaris ⬄ DAD Metronic Portal

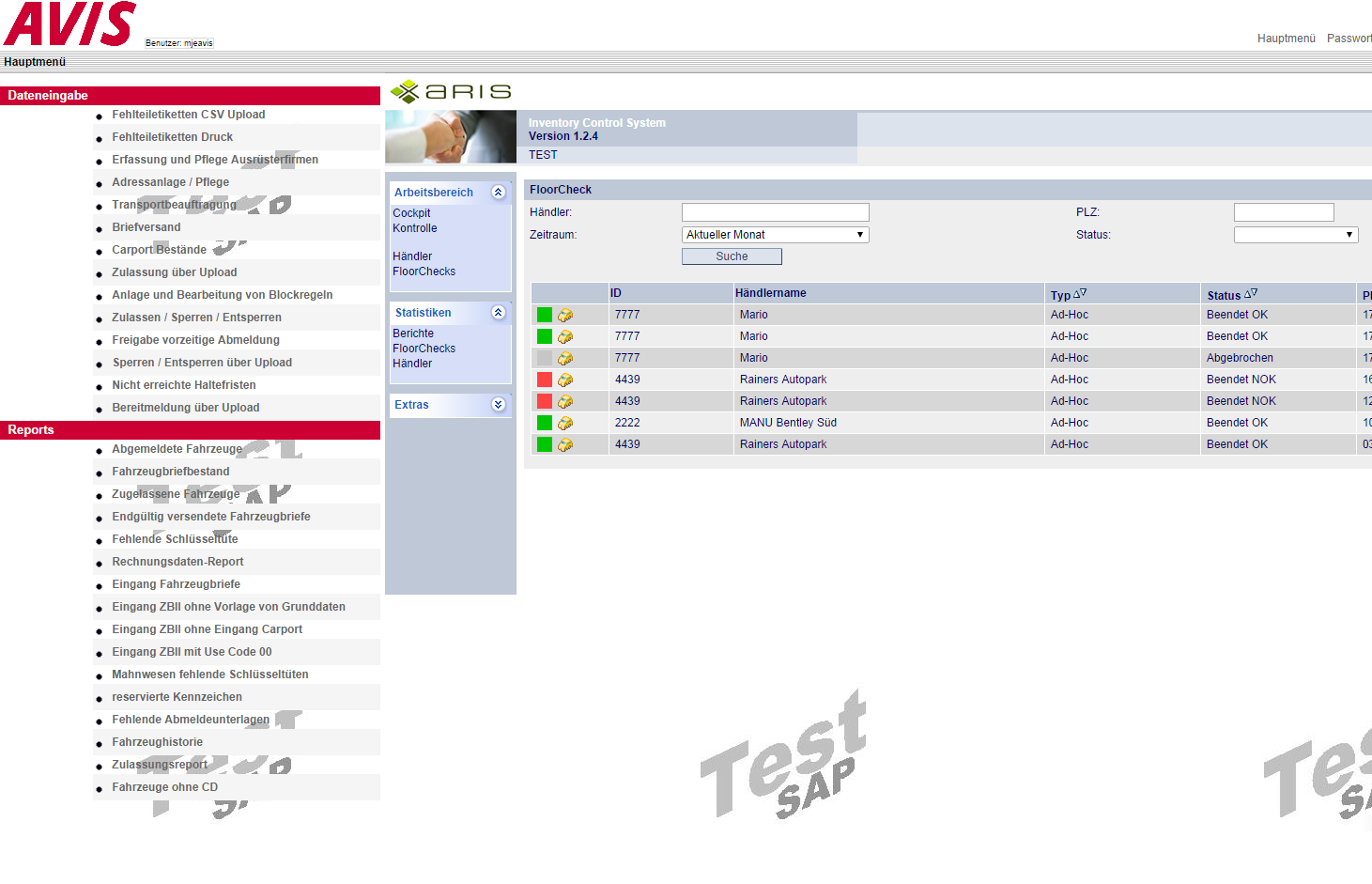


Abbildung 6: Integration Xaris ⬄ klassisches DAD Portal

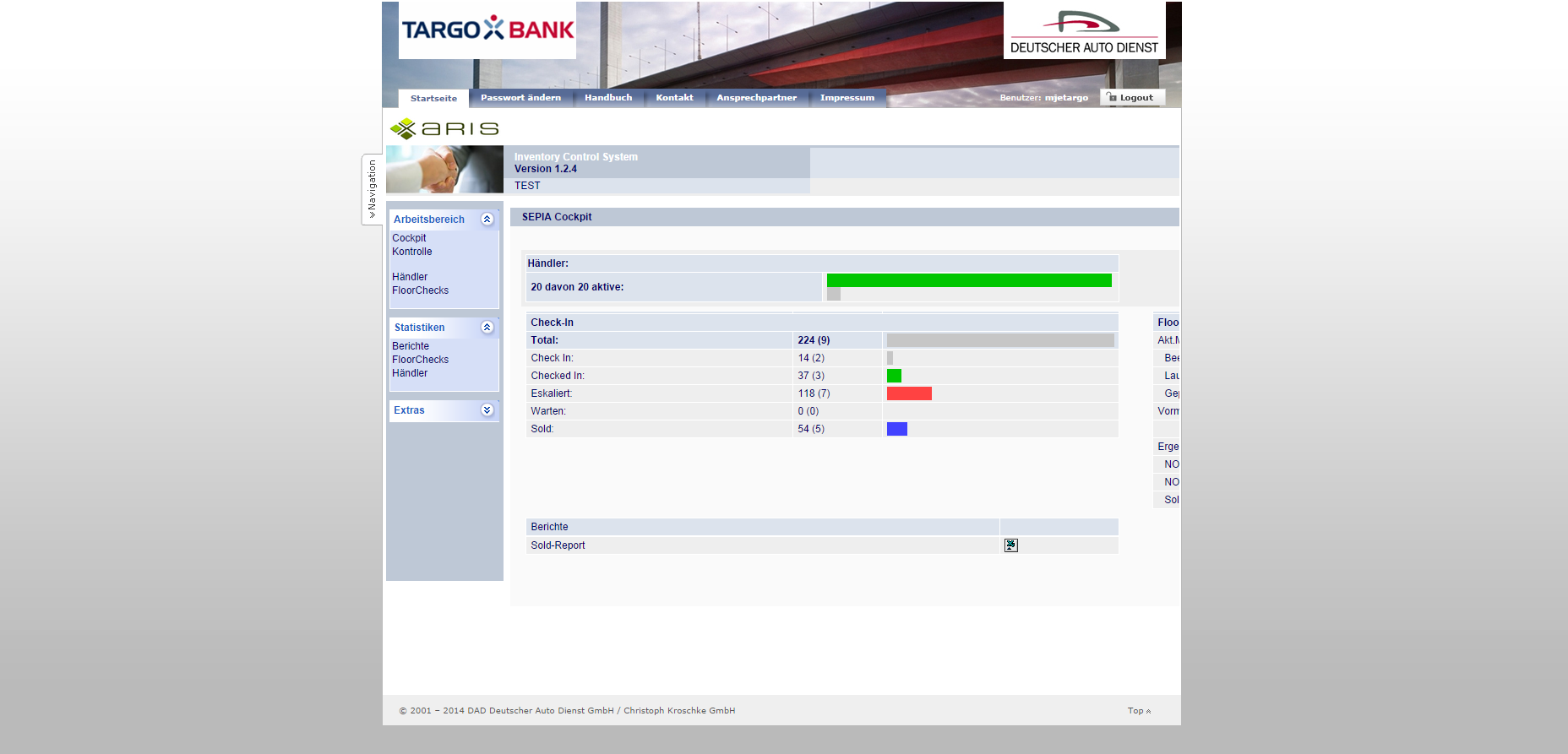


Abbildung 7: Integration Xaris ⬄ DAD Services Portal

### Fazit zu unseren bestehenden Lösungen

Unsere bestehenden Lösungen bedurften einerseits nur eines geringen Implementierungsaufwandes und warten zudem noch mit hoher Flexibilität für künftige Erweiterungen auf, da wir über den kompletten Quellcode verfügen.

Alle bestehenden Lösungen sind maßgeschneidert für alle 3 DDA Web Portale.

***Empfehlung an CKG / DAD***

*Unsere bestehenden Lösungen haben sich bewährt!*

*Sie warten mit folgenden Vorteilen auf:*

* **Geringer Implementierungsaufwand**
* **Hohe Flexibilität für künftige Erweiterungen**
* **Maßgeschneiderte Lösung für alle 3 DAD Portale**

## Welche Lösungen im erweiterten SSO Kontext können wir künftig anbieten?

### Benutzer-individuelle Downloadressourcen

Den CKG/DAD Web-Portal Usern könnten künftig individuelle Ressourcen wie Dokumente oder Bilder zum Download angeboten werden. Diese könnten entweder auf Kunden- bzw. auf Gruppen-Ebene oder User individuell autorisiert werden.

|  |  |
| --- | --- |
| time-limit.png | Zudem könnten diese Ressourcen mit einem Verfallsdatum individuell zeitlich  begrenzt werden. |

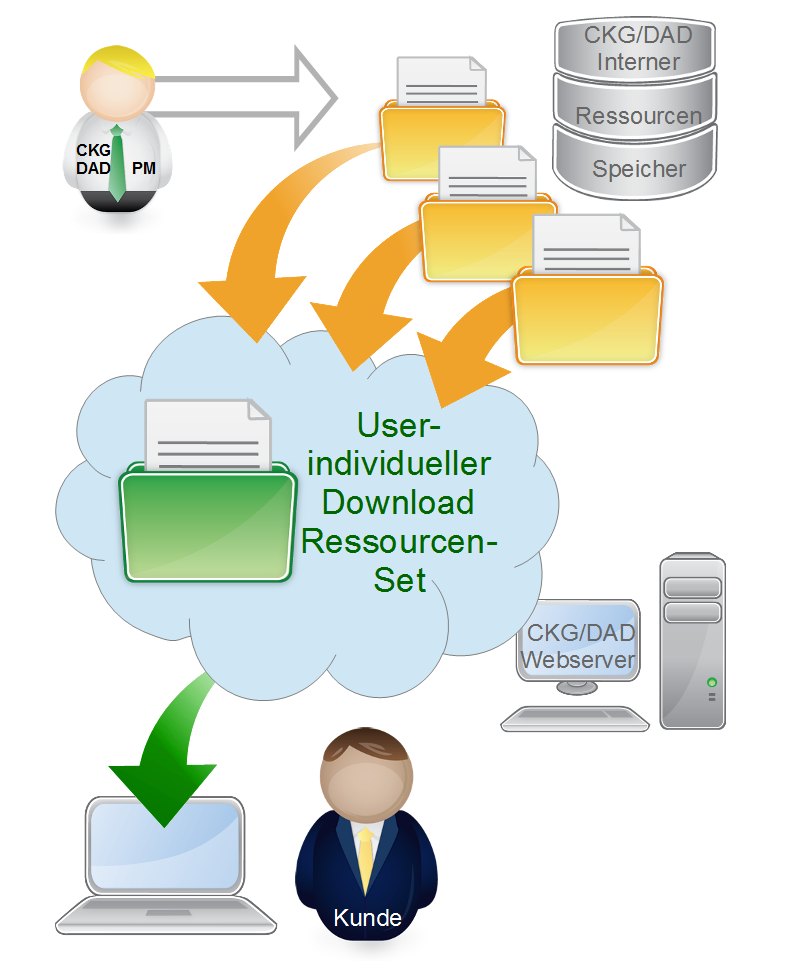


Abbildung 8: Die CKG/DAD-Portal könnte künftig individuelle Ressourcen-Sets zum Download anbieten.

### Zeitlich begrenzte Anwendungs-Sets

Einzelnen Portal Benutzern könnten zeitlich begrenzte Sets aus bestehenden Anwendungen zur Verfügung gestellt werden.  
Der User würde auf seine verfügbaren Anwendungen über ein individuelles Menü oder direkt über eine speziell für den Anwendungs-Set (automatisch) generierten Homepage zugreifen können.

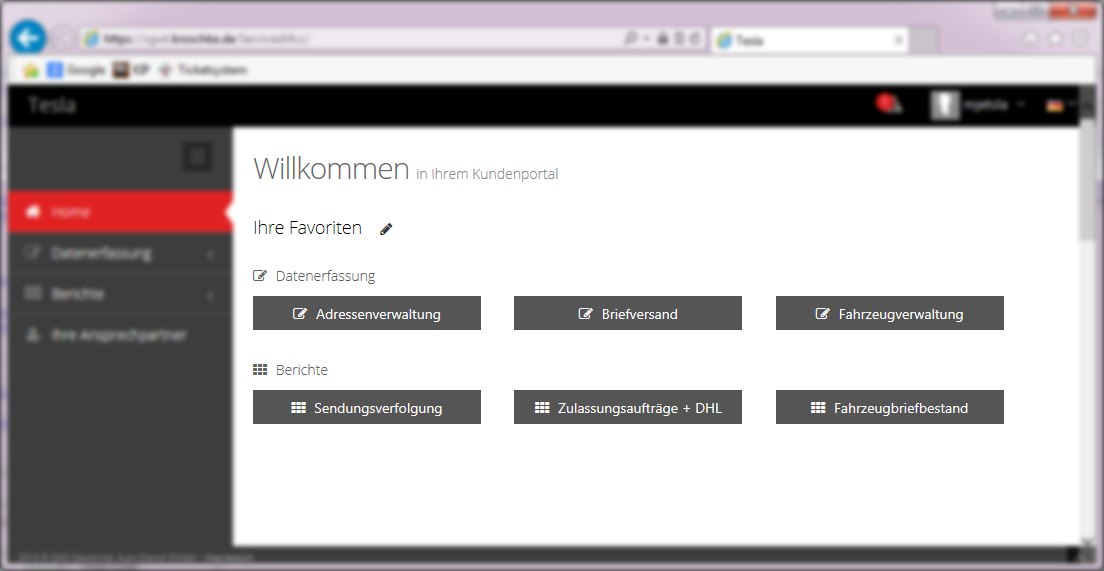


Abbildung 9: Automatisch generierte Homepages für individuelle, zeitlich begrenzte Anwendungs-Sets

Die Pflege der Anwendungs-Sets würde über eine entsprechende Administrations-Maske gesteuert werden.   
Pro Set werden die Anwendungen, Zeit-Limits sowie die User definiert, die Zugriffsberechtigung auf den Set erhalten sollen.  
Zudem könnte hieraus ein Link-Versand per E-Mail an die User gesteuert werden, wahlweise individuell pro User oder als Batch-Versand.

1. WebSSO heißt der Vorschlag des Red-Hat-Ingenieurs Nathaniel McCallum, um Anwendern mehrmaliges Anmelden in Intranet, Web und Cloud zu ersparen.  
    [↑](#footnote-ref-1)
2. Unter Enterprise-SSO versteht man umfassende Software-Lösungen für das Identitätsmanagement.   
   Beispiele: Sun OpenSSO Enterprise, Oracle Enterprise Single Sign-on [↑](#footnote-ref-2)
3. 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-3)
4. [OAuth](http://en.wikipedia.org/wiki/OAuth) ist ein offenes Protokoll, das eine standardisierte, sichere API-Autorisierung für Desktop-, Web- und Mobile-Applikationen erlaubt. OAuth wird u.a. genutzt von Twitter ( <http://en.wikipedia.org/wiki/OAuth> )  
    [↑](#footnote-ref-4)
5. [OpenSocial](http://de.wikipedia.org/wiki/OpenSocial) ist eine Sammlung an Programmierschnittstellen für Anwendungen in webbasierten sozialen Netzwerken. OpenSocial wird von Google entwickelt und wurde am 1. November 2007 veröffentlicht.  
   (<http://de.wikipedia.org/wiki/OpenSocial> )  
    [↑](#footnote-ref-5)
6. [OpenID](http://de.wikipedia.org/wiki/OpenID) (englisch für offene Identifikation) ist ein dezentrales Authentifizierungssystem für webbasierte Dienste (<http://de.wikipedia.org/wiki/OpenID> ) [↑](#footnote-ref-6)