

# CASE STUDY

## Single Sign On

Swisscom Mobile benötigte ein Single Sign On System für ein einheitliches Login auf Web-Applikationen. Für dieses Vorhaben hat Intersys AG gemeinsam mit der SUN Microsystems eine umfassende Lösung bereitgestellt.

### Die Ausgangslage

Swisscom stellt ihren Kunden eine ständig wachsende Anzahl von Web-Applikationen zur Verfügung, wobei diese Applikationen teils von Swisscom und teils auch von externen Partnern betrieben werden. Da die Benutzerfreundlichkeit direkt mit der Akzeptanz und damit dem Nutzungsgrad der Web-Applikationen in Verbindung steht, entstand das Bedürfnis, alle Applikationen mit einem einzigen Login schützen zu können und damit die Handhabung für den Anwender zu vereinfachen. Der Schutzmechanismus sollte einem Anwender nach einmaligem Login (Username/Passwort) erlauben, alle Applikationen zu nutzen, für welche er Zugriffsrechte besitzt, und zwar unabhängig davon, ob die betreffende Applikation direkt von der Swisscom oder von einer Partnerfirma der Swisscom betrieben wird.

Der Schutz der Web-Applikationen durch ein einmaliges Login ist Hauptzweck des sogenannten Single Sign On Systems (SSO), das gleichzeitig als Authentifizierungs- und Autorisierungsplattform (AA) eingesetzt wird. Intersys erhielt den Auftrag, Komponenten für ein Single Sign On System auf Basis des SUN Access Managers zu implementieren und verschiedene Swisscom Systeme zu integrieren.



Bridging the gap



### Die Anforderungen

Das Projekt SSO Live hatte anspruchsvolle Anforderungen zu erfüllen. Die SSO Plattform ...

- ... muss auf dem Access Manager SUN Microsystems basieren
- ... muss interne Web-Applikationen durch ein einmaliges Login schützen und somit das sogenannte Intra-Domain SSO bereitstellen
- ... muss externe Web-Applikationen durch ein einmaliges Login schützen und somit das so genannte Cross-Domain SSO bereitstellen
- ... muss den Übergang zwischen internen und externen Applikationen nach einem einmaligen Login ermöglichen
- ... muss die Authentifizierung und Autorisierung des Zugriffs auf die zu schützenden Applikationen im Hintergrund und für den Anwender unsichtbar abwickeln
- ... muss für Authentifizierung und Autorisierung bestehende Kundendaten verwenden, d.h. die bereits vorhandenen Swisscom Systeme müssen in den SUN Access Manager integriert werden
- ... muss die Sicherheit des Selbstregistrierungsprozesses durch das Versenden eines temporär gültigen Passworts per SMS erhöhen.

## Die Lösung

Intersys hat im Rahmen des Projekts SSO Live folgende Aufgaben erfüllt:

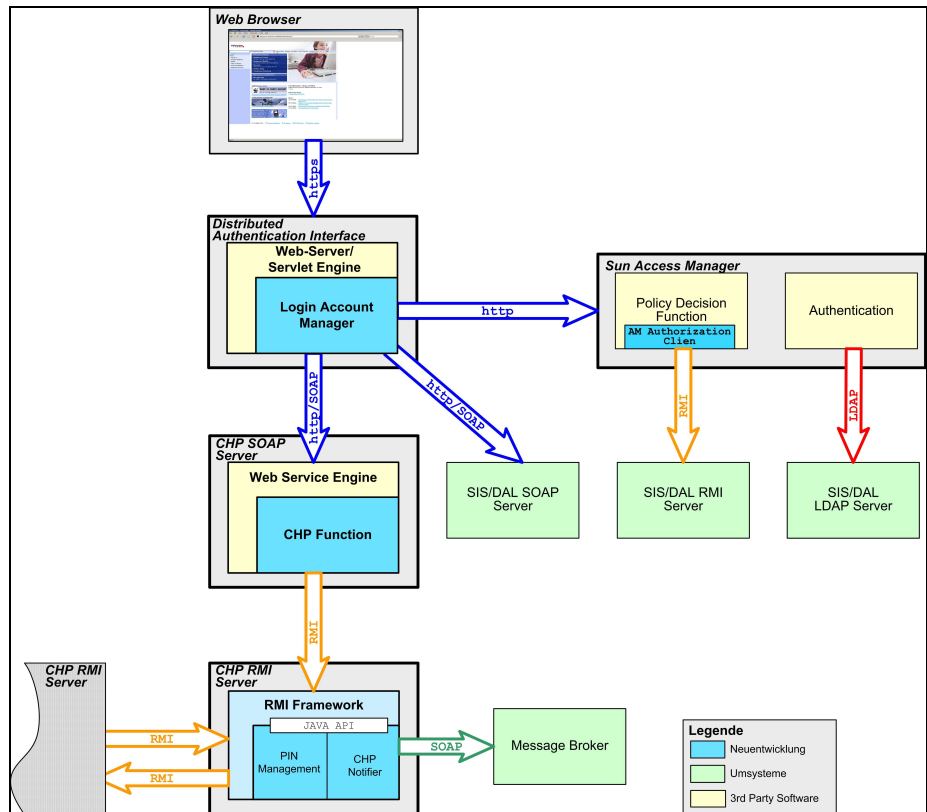
### SUN Access Manager – Unterstützung bei der Installation und der Inbetriebnahme:

Der SUN Access Manager ist ein kommerzielles Produkt, das den Kern des ganzen Systems bildet und Mechanismen beinhaltet, die sowohl Single Sign On wie auch Authentifizierung und Autorisierung ermöglichen. Zu diesem Zweck interagiert der Access Manager mit den Umsystemen und weiteren Access Manager-eigenen Komponenten, die auf den zu schützenden Web-Servern installiert werden müssen. Intersys hat bei der Installation und der Integration der Swisscom-Systeme eng mit SUN Microsystem zusammengearbeitet und sich massgebend am Aufbau des ganzen Systems mitbeteiligt. Eigens für dieses Projekt nahm Intersys auf eigener Hardware den Access Manager inhouse in Betrieb. Diese Installation diente einerseits als Entwicklungsumgebung und andererseits als willkommenes Testsystem für Swisscom.

### Policy Agent – Installation und Inbetriebnahme:

Der Policy Agent ist eine Access Manager Komponente, die auf jedem Web-Server mit den zu schützenden Web-Applikationen installiert werden muss. Der Policy Agent sorgt für das Überprüfen eines erfolgreichen Logins und falls nötig für das Weiterleiten des Anwenders auf eine Login-Seite. Weiter initiiert der Policy Agent die Autorisierung und Authentifizierung unter Einbezug des Access Managers. Intersys war verantwortlich für die Installation und Inbetriebnahme des Policy Agents auf den eingebundenen Web-Servern.

Bridging the gap



**Distributed Authentication Service Interface – Customizing, Installation und Inbetriebnahme:** Distributed Authentication Service Interface ist ebenfalls eine Access Manager-eigene Komponente, die beim ersten Login zum Einsatz kommt. Diese Komponente wird in der sogenannten demilitarized Zone (DMZ) installiert und schützt somit den im internen Subnetz installierten Access Manager vor unerlaubten Zugriffen. Intersys hat in enger Zusammenarbeit mit SUN und nach Vorgaben von Swisscom das Customizing des Distributed Authentication Service Interface ausgeführt.

**Login Account Manager - Neuentwicklung:** Login Account Manager ist eine Web-Applikation, die den Kunden der Swisscom die Verwaltung ihrer Accounts ermöglicht. Mit dieser Applikation können sich die Kunden selber registrieren, ein neues Passwort anfordern sowie ihre Accounts sperren. Zu diesem Zweck agiert der Login Account Manager als ein SOAP Client, um die spezifische Autorisierungs- und Authentifizierungsplattform von Swisscom einzubinden.

**Check of Handy Possession – Neuentwicklung:** Der Check of Handy Possession (CHP) Server kommt während des Selbstregistrierungsprozesses zum Einsatz. Diese Applikation stellt SOAP Services zur Verfügung, die das Erstellen und das Versenden von Passwörtern per SMS mit einer zeitlich beschränkten Gültigkeit ermöglichen. Diese Passwörter müssen während der Selbstregistrierung von Swisscom Kunden im Login Account Manager eingegeben und vom CHP Server auf ihre Gültigkeit überprüft werden.

**Customer Condition – Neuentwicklung:** Die Customer Condition ist ein neu entwickeltes Modul, zur Integration der eigenen Authentifizierungs- und Autorisierungsplattform von Swisscom. Mit Hilfe von Customer Condition wurden Kundendaten von Swisscom in den SUN Access Manager integriert und als Basis für die Authentifizierungs- und Autorisierungsprozesse verwendet.

### Das Resultat

Seit Abschluss des Projekts steht dem Kunden eine effektive Single Sign On Plattform zur Verfügung, welche für die Authentifizierung und Autorisierung des Zugriffs auf eigene und auch auf fremdbetriebene externe Web-Applikationen genutzt werden kann. Damit bildet diese SSO-Applikation eine solide Grundlage für künftige Erweiterungen und vor allem für eine einfache und effiziente Einbindung von kommerziellen Web-Applikationen.

In diesem Projekt hat Intersys sehr eng mit SUN Microsystems zusammengearbeitet. Diese erfolgreiche Kooperation ist der Grundstein für die seither bestehende vertiefte Partnerschaft zwischen SUN und Intersys, vornehmlich im Bereich Identity Management.

### Intersys schlägt Brücken – Stellen Sie uns auf die Probe!

Den Erfolg unserer Kunden verbessern ist das Merkmal unserer ICT-Lösungen (Information and Communication Technology). Sie sind auf die jeweilige Aufgabe zugeschnitten und holen das Beste aus dem Vorhandenen. Dabei zeichnen wir uns durch Zuverlässigkeit und Termintreue, grosses Verständnis für die Prozesse und Abläufe unserer Kunden und das Wahrnehmen der Verantwortung über die gesamte Lebenszeit unserer Arbeit aus.