

Authentifikation

Mit der Version 6.5 wurde die Authentifikations- und das Autorisierungs-Verfahren für das ITREXS-Web-Frontend auf eine neue Technologie SAE von RSA angepasst.

Im Rahmen dieser technologischen Umstellung wurde auch die Integration der User-Verwaltung und zusätzliche Authentifizierungs-Varianten eingeführt.

Die Produktionseinführung auf die neue Version sollte bis zum 30.06.2010 abgeschlossen sein.

Künftig soll es grundsätzlich drei unterschiedliche Authentifizierungs-Profile geben:

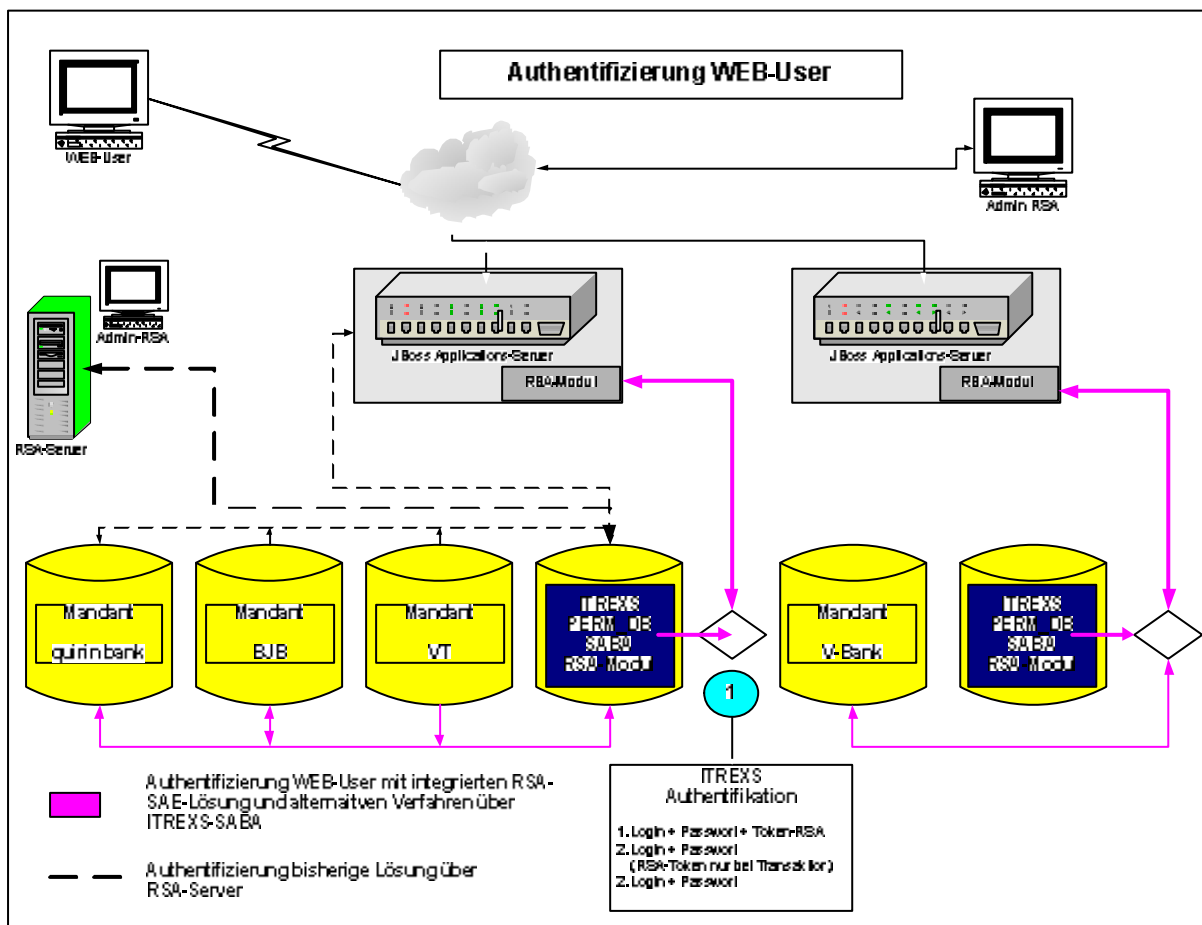
- Authentifizierung über Login + Passwort (SABA)
- Authentifizierung über RSA-Login + PIN + Token-cod
- Authentifizierung über RSA-Login + Passwort, (bei Transaktionen zusätzlich über Tokencode (SABA + RSA ohne PIN))

Bisher wurde die Authentifikation über einen eigenständigen RSA-Server durchgeführt. Die Administration erfolgte ausschließlich über den RSA-Server, ohne Integration in ITREXS-Datenstruktur.

Durch die Ablösung des RSA-Servers und durch Einbindung der RSA-SAE-Komponente besteht weiterhin das gleiche Authentifizierungsverfahren auf höchstem Sicherheitsniveau für den ITREXS -Web-User.

Wesentliche Vorteile bestehen durch die integrierte Verwaltung der Web-User, der Token und die automatische Erstellung von Kunden-Anschreiben.

Das Schaubild zeigt die alte und neue Architektur in Verbindung mit den verschiedenen Mandanten-Datenbanken. Die Umstellung auf das neue Konzept erfolgt für die Mandanten jeweils gemeinsam, sofern ein gemeinsamer JBoss Applications-Server genutzt wird.

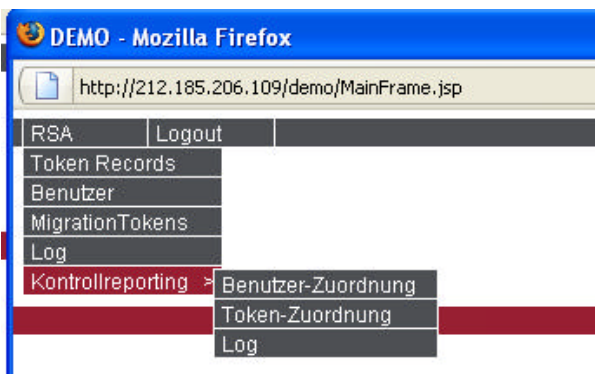


Die Authentifikation des Web-Users erfolgt zunächst über die Permissions-DB in SABA (Sachbearbeiter-Berechtigungs-System). Hier wird geprüft, welche Authentifikation für den User hinterlegt ist. Nach Eingabe

des Login, entsprechend der definierten Methode, wird der User der jeweiligen Mandanten-DB zugeordnet. Gleichzeitig wird dem System die Autorisierung für die freigegebenen Funktionen übergeben.

Funktionserweiterungen:

- Einbindung und Administration der SAE-Software (JAVA) gemäß Spezifikation von RSA in die ITREXS-WEB-Anwendung. Die Funktionen sind über das ITREXS-Menü Administrator verfügbar.
- Verwaltungsfunktion für die RSA-Tokens über JSF-Technologie
- WEB-User-Anlage über die Stammdaten und gleichzeitige Registrierung – abhängig vom Profil – als RSA-User
- Erstellung von Brief-Anschreiben für den Kunden und für den Administrator für den Versand der Token, Passwort und User-Login
- Erstellung von Kundenanschreiben vor Ablauf der Gültigkeit des Tokens.



RSA-Secure-ID www.rsa.com

Securing Your Future with Two-Factor Authentication



RSA SecurID® **two-factor authentication is based on something you know (a password or PIN) and something you have (an authenticator)—providing a**

much more reliable level of user authentication than reusable passwords.

The only solution that automatically changes your password every 60 seconds
20-year history of outstanding performance and innovation

To access resources protected by the RSA SecurID system, users simply combine their secret Personal Identification Numbers (PIN's) (something they alone know) with the token codes generated by their authenticators (something they have). The result is a unique, one-time-use passcode that is used to positively identify, or authenticate, the user. If the code is validated by the RSA SecurID system, the user is granted access to the protected resource. If it is not recognized, the user is denied access.

- Aufzeichnung der Zugriffe der User, Anzahl, IP-Adresse, Fehlversuche
- Auswertung des Zugriffsverhaltens der User
- Behandlung von Fehlversuchen. Nach drei Fehlversuchen zeitliche Sperre
- Temporäre Umschaltung der Zugangsberechtigungen, wenn Token außer Funktion, z. B. Kunde hat Token verloren

Authentifizierung ohne RSA

Alternativ zu dem RSA-Verfahren kann auch für z.B. nur lesende Zugriffe das Authentifizierungsverfahren für Kunden mit Login und Passwort gewählt werden. Dies sollte jedoch nur dann gewählt werden, wenn der Kunde diese Art wünscht und keine aktiven Funktionen im Zahlungsverkehr und für das Wertpapiergeschäft ausführen will.

In diesem Fall prüft ITREXS das Login und das Passwort des Kunden. Die RSA-SAE-Funktionalität wird in diesem Fall nicht genutzt.

Administrations-Funktionen

Die Verwaltung der RSA-Tokens bzw. Passwörter erfolgt über den Administrations-User im ITREXS-Web-Frontend. Im Web-Frontend über den Menüpunkt RSA. Die jeweiligen Berechtigungen werden über SABA den autorisierten Personen zugeordnet.

Damit kann die Administration und die Analyse der Web-User von unterschiedlichen Personen und Standorten ausgeführt werden.

Die Funktionen werden unterteilt nach:

- Veralterung und Zuordnung der Berechtigungen und Token
- Die Zuordnung von Token und Usern und die Erstellung von Token-Versandanschreiben.
- Auswertungen von Web-Usern, Zugriffen, Fehlversuchen
- Kontrolle und Dokumentation der User-Rechte für Kunden und Mitarbeiter der Bank

Parametersteuerung

Über die Parameterisierung können unterschiedliche Verhalten und Verfahren definiert werden.

Bei Neuanlage kann über die Checkbox „Enabled“ des jeweiligen Tokens bzw. Passworts dieses aktiviert oder deaktiviert werden. Ist das Token / Passwort deaktiviert, ist eine Anmeldung mit diesem nicht möglich. Eine Deaktivierung des Tokens / Passworts erfolgt automatisch nach mehreren erfolglosen Anmeldungen. Nach der Zuordnung eines neuen Tokens bzw. Passworts ist dieses automatisch Enabled. Wurde die Checkbox geändert, so wird die Änderung erst nach der Speicherung wirksam.

New PIN / Passwort Mode

Wird die Checkbox „New PIN / Passwort Mode“ aktiviert, muss der Benutzer nach der nächsten erfolgreichen Anmeldung eine neue PIN für sein Token bzw. ein neues Passwort vergeben. Die Änderung der Checkbox wird erst nach der Speicherung wirksam.

PIN LÖSCHEN

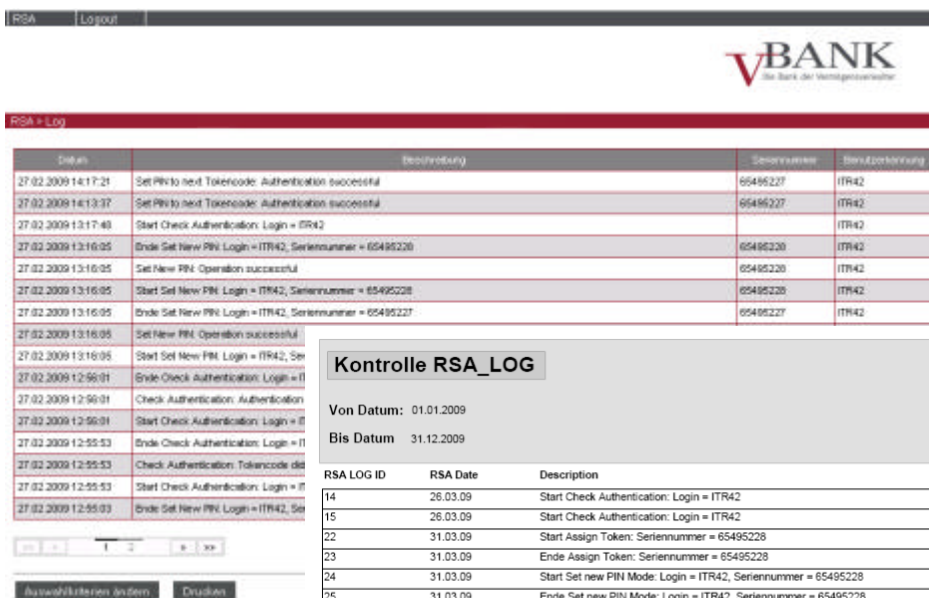
Mit dem Button „PIN des ausgewählten Tokens löschen“ kann die PIN eines Tokens gelöscht werden. Wurde die PIN gelöscht, muss der Benutzer des To-

kens bei der nächsten Anmeldung eine neue PIN vergeben. Für die Anmeldung sind nur das Login und der aktuelle Tokencode erforderlich.

Auswertungen LOG

Alle Aktionen, die im Zusammenhang mit RSA stehen, werden im System protokolliert. Das heißt, im Log werden alle Aktionen festgehalten, die durch die Administration entstehen. Hierzu gehören z.B. Import einer Datei mit Informationen zu Tokens, Zuordnung eines Tokens zu einem Benutzer etc.

Weiterhin werden auch Aktionen der Web-Benutzer, die im Zusammenhang mit den RSA-Tokens stehen protokolliert, z.B. Anmeldung, Änderung PIN etc. Das Log kann nach verschiedenen Kriterien gefiltert werden.



Kontrolle RSA_LOG

Von Datum: 01.01.2009
Bis Datum: 31.12.2009

Datum	Beschreibung	Seriennummer	Benutzerkennung
27.02.2009 14:17:21	Set PIN to next Tokencode: Authentication successful	65495227	ITR42
27.02.2009 14:13:37	Set PIN to next Tokencode: Authentication successful	65495227	ITR42
27.02.2009 13:17:49	Start Check Authentication: Login = ITR42		ITR42
27.02.2009 13:16:05	Ende Set New PIN Login = ITR42, Seriennummer = 65495228	65495228	ITR42
27.02.2009 13:16:05	Set New PIN: Operation successful	65495228	ITR42
27.02.2009 13:16:05	Start Set New PIN Login = ITR42, Seriennummer = 65495228	65495228	ITR42
27.02.2009 13:16:05	Ende Set New PIN Login = ITR42, Seriennummer = 65495227	65495227	ITR42
27.02.2009 13:16:05	Set New PIN: Operation successful		
27.02.2009 13:16:05	Start Set New PIN Login = ITR42, Ser		
27.02.2009 12:56:01	Ende Check Authentication: Login = IT		
27.02.2009 12:56:01	Check Authentication: Authentication		
27.02.2009 12:56:01	Start Check Authentication: Login = IT		
27.02.2009 12:55:53	Ende Check Authentication: Login = IT		
27.02.2009 12:55:53	Check Authentication: Tokencode did		
27.02.2009 12:55:53	Start Check Authentication: Login = IT		
27.02.2009 12:55:03	Ende Set New PIN Login = ITR42, Ser		

Kontrollreport RSA-User-Zuordnung

Datum: 06.04.09
Seite: 1 von 1

Assign: 1
Domäne

WEB-User	Seriennummer	Name	Domäne	Assign	Datum	Authentifikation	Tok-Beginn	Tok-Ende	Enabled	Status	Bemerkungen
ITR42	65495228		ITREXS ³ -GmbH	1	31.03.09	Login + PIN + Token	21.05.07	30.09.10	0	NORMAL	
ITR42	65495227		ITREXS ³ -GmbH	1	25.03.09	Login + PIN + Token	21.05.07	30.09.10	0	NORMAL	

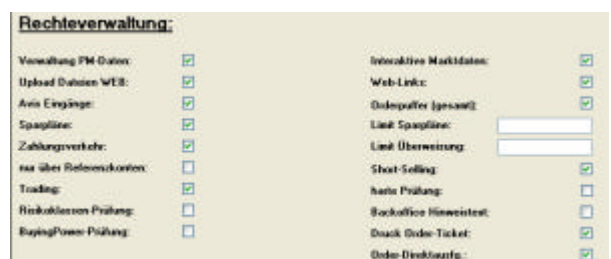
Kundenanschriften

Kundenanschriften werden direkt bei der Web-User-Anlage Konto-/Depoteröffnung geniert. Die Anschreibentexte sind als Textbausteine hinterlegt. Abhängig von dem Authentifizierungs-Verfahren werden die Anschreiben unterschiedlich erstellt und den Kunden bzw. den Beratern zugestellt. Die Anschreiben und Versandwege sind abhängig vom Authentifizierungsverfahren:

- Benutzerkennung
- RSA-Tokenversand
- SABA-Web-User

Web-Usergruppe

Jeder Web-User wird einer User-Gruppe zugeordnet. Für jede Gruppe können unterschiedliche Rechte vergeben werden. Die Rechte steuern Funktionen und Limite.



Rechteverwaltung:

- Verwaltung PM Daten:
- Upload Dateien WEB:
- Avis Eingänge:
- Spaßline:
- Zahlungsverkehr:
- Trading:
- Rückkäufe Prüfung:
- BuyingPower Prüfung:
- Interaktive Marktdata:
- Web-Link:
- Orderpuffer (gesamt):
- Limit Spießline:
- Limit Überweisung:
- Short-Selling:
- Arbitr. Prüfung:
- Backoffice Hinweislast:
- Quick Order-Ticket:
- Order Direktaufg.:

Benutzerrechte Reporting

Benutzerrechte für WEB-User und ITREXS -Client

Über die Report-Funktion können die Benutzerrechte nach verschiedenen Bereichen ausgewählt werden. Zunächst werden die verschiedenen User-Gruppen mit der Anzahl der Benutzer und Aktionen ausgewiesen.

Unter Restriktionen werden die Funktionen dargestellt, für die die Gruppe bzw. der User nicht berechtigt ist.

QUIRIN SABA Benutzerrechte

- * Cognos BI Benutzerkreis
- ITREXS-Client-Anwendung
- ITREXS-WEB
- Reuters-Kursubnahme
- System Administration Module

[Alles auswählen](#) [Auswahl aufheben](#)

Das Beispiel zeigt einen Auszug der Rechteverwaltung für der ITREXS-Client-Anwendung.

Benutzergruppe	Benutzer	Module	Masken	Aktionen	Alle Aktionen	Restriktionen	Freigaben
Abwicklung für SPOOL	19	1	428	814	124.545	1.463	190
Administrator	16	1	428	880	106.096	16	
Pflege WM Daten POOL	8	1	428	881	53.056		8
Test	7	1	428	881	46.424		
Admin SDV-Operative	6	1	428	778	39.150	642	
Kursflecke	2	1	428	881	13.264		2
				811	13.104	160	4
				820	6.558	21	
				881	6.632		

Administrator	Benutzer	Module	Masken	Aktionen	Alle Aktionen	Restriktionen	Freigaben
ADMIN	1	1	428	880	6.631	1	
KKOWALSK	1	1	428	880	6.631	1	
URUECKER	1	1	428	880	6.631	1	
HRESTLE	1	1	428	880	6.631	1	
CDAHMS	1	1	428	880	6.631	1	
LSATTLER	1	1	428	880	6.631	1	
SFRINGEL	1	1	428	880	6.631	1	
MKRETSCH	1	1	428	880	6.631	1	
MSHEFAAT	1	1	428	880	6.631	1	
DTEES	1	1	428	880	6.631	1	
CROEMER	1	1	428	880	6.631	1	
MSTANJOR	1	1	428	880	6.631	1	
ASCHNEIDER	1	1	428	880	6.631	1	
QOSYAGIN	1	1	428	880	6.631	1	
KIAKUBIT	1	1	428	880	6.631	1	
SSEIFERT	1	1	428	880	6.631	1	

Benutzergruppe	Benutzer	Modul	Maske	Aktion	Restriktionen
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Stammdaten/Produkte/Übersicht	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Stammdaten/Produkte/Produktz	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Stammdaten/Produkte/Produktz	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	Pflegemaske für Börsen	Daten/Neu	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Systempflege/Value at Risk	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Systempflege/Schnittstellen/Out	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Systempflege/Abschluss	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Systempflege/Bewertungen	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Systempflege/Parameter	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Zahlungsverkehr/Kontoabschluss	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Stammdaten/WP-Reports	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Systempflege/Batch	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Stammdaten/Produkte/Produktz	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Stammdaten/Partner/Geschäftsp	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Auswertungen/Übersicht	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Zahlungsverkehr/Zahlungsausgar	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Stammdaten/Partner/Adressan	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Stammdaten/Partner/Businesssg	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Auswertungen/Portfolio	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Stammdaten/Produkte/Produktz	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Zahlungsverkehr/Zahlungseingang	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Stammdaten/Produkte/Steuersun	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Stammdaten/Zinsen/Indizes	1
Abwicklung für SPOOL	KWORMS	ITREXS-Client-Anwends	IRIS-Hauptfenster	Geschäfte/Zinsderivate	1

Das ad hoc-Reporting dient zur Kontrolle der aktuellen Berechtigungen für die einzelnen User. Über Drill-Down kann von der User-Gruppe auf den einzelnen User bzw. von der Funktion auf die User verzweigt werden.

So ist es möglich mit einigen Klicks die Rechte eines Users festzustellen bzw. für eine Funktion alle berechtigten Users darzustellen.

Das Reporting erfolgt unter **Cognos 8 (BI)**.

Die Detaillisten werden in Excel ausgegeben und können für die Dokumentation oder für Änderungen der User-Gruppen-Rechte genutzt werden.