BG ETEM Intranet Präventionswerkzeuge

Schnittstellenkontrakte

Version	1.2
Stand:	11.07.2014 17:18:00
Autor:	Achim.Mueller@msg-systems.com
Ablage:	80_Schnittstellenkontrakte.docx
Umfang:	9 Seiten

Versionshistorie

Version	Beschreibung	Autor	Datum
0.9	Initiale Version erstellt	Achim Müller	22.05.2014
1.0	Freigabe zur Abnahme	Stefan Hofmaier	26.05.2014
1.1	Anmerkungen BG ETEM eingearbeitet	Stefan Hofmaier	27.05.2014
1.1	Dokument von BG ETEM abgenommen	BG ETEM	10.06.2014

BG ETEM Intranet Präventionswerkzeuge
Schnittstellenkontrakte

Review

Version	Datum	Teilnehmer

0.9	26.05.2014	Stefan Hofmaier

1 Inhaltsverzeichnis

2 Einleitung

2.1 Zweck

Das Dokument beschreibt die Schnittstellen, die zwischen der Anwendung „Intranet Präventionswerkzeuge“ und externen IT-Systemen existieren. Es handelt sich hierbei um die Schnittstellen zum Verzeichnisdienst LDAP und zu Mail-Programmen für das Versenden von E-Mails und das Erstellen von Terminen.

2.2 Referenzen

Die Schnittstellenkontrakte wurden auf Basis der folgenden von BG ETEM im Rahmen der Ausschreibung zur Verfügung gestellten Dokumente konzipiert:

- Intranet Präventionswerkzeuge - Grob-Konzept
- Intranet Präventionswerkzeuge – Konzeptergänzung

Die Informationen aus den genannten Dokumenten wurden in Workshops mit BG ETEM und dem Pilotpartner Rohde & Schwarz konkretisiert.

2.3 Abgrenzung

Die Schnittstellenkontrakte beschreiben lediglich die Schnittstellen zu den relevanten externen Systemen. Die Funktionsweise der externen Systeme wird nicht beschrieben.

3 Schnittstellenbeschreibungen

3.1 Überblick

Die Anwendung "Intranet Präventionswerkzeuge" kommuniziert mit folgenden externen IT-Systemen

- LDAP-Server
- Terminverwaltung
- E-Mail-Server

3.2 LDAP-Server

Der LDAP-Server erfüllt zwei Funktionen für Intranet Präventionswerkzeuge:

- Authentifizierung der Benutzer
- Übernahme der Benutzerdaten, wie z. B. Name, Vorname, Organisationseinheit und E-Mail Adresse aus dem Verzeichnisdienst

3.2.1 Authentifizierung der Benutzer

Die Authentifizierung von Benutzern in Intranet Präventionswerkzeuge erfolgt gegen einen unternehmensweiten LDAP-Server. In Intranet Präventionswerkzeuge selbst erfolgt keine Passwortverwaltung.

Damit ein Benutzer aus dem LDAP Zugriffsberechtigung auf Module, Funktionen oder Knoten in der Unternehmensstruktur von Intranet Präventionswerkzeuge erhalten kann, muss der Benutzer in der Anwendung angelegt werden.

Die Erfassung und Pflege der Rollen und Anwendungsberechtigungen erfolgt ausschließlich in Intranet Präventionswerkzeuge. Der Verzeichnisdienst LDAP dient nur zur Authentifizierung des Benutzers und zur Synchronisierung der Benutzerinformationen.

Die Authentifizierung gegen LDAP erfolgt immer in 2 Schritten:

- Eintrag des Benutzers im LDAP suchen
- Benutzer/Passwort gegen seinen Eintrag im LDAP authentifizieren

Je nachdem in welcher Reihenfolge diese Schritte durchgeführt werden, gibt es grundsätzlich 2 Verfahren:

1. Search-first (Zuerst suchen)
2. Authentication-first (Zuerst authentifizieren)

Das Verfahren 1 ist nur möglich, wenn das LDAP so konfiguriert ist, das anonymer Lesezugriff erlaubt ist. Andernfalls muss Verfahren 2 verwendet werden.

Verfahren 2 setzt voraus, dass ein technischer Benutzer für den Zugriff auf das LDAP konfiguriert und bekannt ist und ein anonymer Zugriff verboten wurde.

Da nicht bekannt ist, wie das LDAP in den Mitgliedsunternehmen konfiguriert ist, müssen beide Verfahren unterstützt werden. Dies wird durch die Konfiguration folgender Parameter ermöglicht:

Parameter	Beschreibung	Beispiel
userProvider	LDAP-Server-URL mit Base DN (Einstiegsverzeichnis)	ldap://ldap-rohde-schwarz,dc=de
authIdentityFilter	Technischer Benutzername, wie er zum Login beim LDAP benutzt werden soll	{USERNAME}

authIdentity Username	Kennung des technischen Benutzers	IPW_LDAPUSER
authIdentity Password	Passwort des technischen Benutzers, BASE64 codiert	GHJKT342HJK
userFilter	Suchfilter, um den Eintrag des Benutzers im LDAP zu finden	(&(|(samAccountName={USERNAME}) (userPrincipalName={USERNAME}) (cn={USERNAME}))(objectClass=user))
useSSL	Schalter, ob die Kommunikation mit SSL (Secure Socket Layer) erfolgen soll	true

Die Konfiguration der Parameter erfolgt über die zentrale Konfigurationsdatei „ipw.properties“.

Ist der Parameter "authIdentityFilter" leer, wird Verfahren 1 angewendet, andernfalls Verfahren 2.

3.2.2 Übernahme von Benutzerdaten

Damit Benutzer Zugriff auf Intranet Präventionswerkzeuge erhalten, muss für jeden Benutzer ein Benutzereintrag in der Anwendungsdatenbank vorhanden sein. Benutzer können über eine Pflegeoberfläche erfasst werden. Zu den Benutzerdaten gehören insbesondere Benutzername, Name, Vorname und E-Mail-Adresse.

Bei jedem erfolgreichem Login eines Benutzers gegen den LDAP-Server werden die Benutzerdaten aus dem LDAP-Verzeichnis ausgelesen und mit den Daten in Intranet Präventionswerkzeuge synchronisiert.

Hierfür dienen die folgende konfigurierbaren Filter Parameter, die beschreiben an welcher Stelle im LDAP-Verzeichnis die entsprechenden Attribute zu finden sind:

Parameter	Beschreibung
nameFilter	Findet den Namen des Benutzers
vornameFilter	Findet den Vornamen des Benutzers
emailFilter	Findet die E-Mail-Adresse des Benutzers

Ist ein Parameter leer, so wird das zugehörige Attribut nicht synchronisiert.

Die Konfiguration der Parameter erfolgt über die zentrale Konfigurationsdatei „ipw.properties“.

3.2.3 Terminverwaltung

Der Eintrag von Terminen lässt sich mittels Versand einer E-Mail mit einer .ics Datei als Anhang bewerkstelligen. Das .ics Dateiformat wird von den gängigen E-Mail-Programmen insbesondere auch von Lotus Notes unterstützt und bietet die Möglichkeit Serientermine einzustellen.

Beispiel einer ICS-Datei:

```
BEGIN:VCALENDAR
VERSION:2.0
METHOD:PUBLISH
BEGIN:VTIMEZONE
TZID:W. Europe Standard Time
BEGIN:STANDARD
DTSTART:16011028T030000
```

```
RRULE:FREQ=YEARLY;BYDAY=-1SU;BYMONTH=10
TZOFFSETFROM:+0200
TZOFFSETTO:+0100
END:STANDARD
BEGIN:DAYLIGHT
DTSTART:16010325T020000
RRULE:FREQ=YEARLY;BYDAY=-1SU;BYMONTH=3
TZOFFSETFROM:+0100
TZOFFSETTO:+0200
END:DAYLIGHT
END:VTIMEZONE
BEGIN:VEVENT
CLASS:PUBLIC
CREATED:20140521T120121Z
DESCRIPTION:Dies ist der Text zum Termin.\n
DTEND;TZID="W. Europe Standard Time":20140520T130000
DTSTAMP:20140521T120122Z
DTSTART;TZID="W. Europe Standard Time":20140520T123000
LAST-MODIFIED:20140521T120121Z
LOCATION:München
PRIORITY:5
RRULE:FREQ=WEEKLY;BYDAY=MO,TU,WE,TH,FR
SEQUENCE:0
SUMMARY;LANGUAGE=de:Beispieltermin
TRANSP:OPAQUE
UID:040000008200E00074C5B7101A82E00800000000203ECE1CFD74CF01000000000000000
      0100000005BBB420AB7D5E54CB2F0DD9CBD161A55
END:VEVENT
END:VCALENDAR
```

Um eine ICS-Datei zu generieren, sind folgende Parameter erforderlich:

Parameter	Beschreibung	Beispiel
SUMMARY	Betreff	`Beispieltermin`
DESCRIPTION	Text des Kalendereintrags	`Dies ist der Text zum Termin`
LOCATION	Ort	`Köln`
DTSTART	Start des Termins (12:30)	`20140520T123000`
DTEND	Ende des Termins (13:00)	`20140520T130000`
RRULE	Wiederholungsregel bei Serienterminen	`WEEKLY;BYDAY=MO,TU,WE,TH,FR`

Zum Versand des Kalendereintrags gelten die Parameter wie unter 3.2.4 beschrieben.

3.2.4 E-Mail-Server

Intranet Präventionswerkzeuge versendet E-Mails an ausgewählte Benutzer. Hierfür muss Zugriff auf einen SMTP-Server bestehen, der die E-Mails versendet. Hierfür sind folgende Schnittstellenparameter erforderlich:

Parameter	ipw.properti	Beschreibung	Beispiel

	es[1]		
smtpserver	X	Adresse und Port des SMTP-Servers	mail.rohde-schwarz.de:587
smtpusername	X	Benutzername zur Anmeldung an dem SMTP-Server	ipw_user
smtppassword	X	Passwort zur Anmeldung an dem SMTP-Server (BASE64-codiert)	A9768FR96
senderemail		E-Mail-Adresse des Absenders	benutzer123@rohde-schwarz.de
recepientemail		E-Mail-Adresse des Empfängers	Benutzer456@rohde-schwarz.de
defaultsenderemail	X	E-Mail-Adresse des Senders, falls es fachlich keinen Absender gibt (Systemmails)	ipw-anwendung@rohde-schwarz.de
adminemail	X	E-Mail-Adresse des Empfängers für Systemnachrichten	admin@rohde-schwarz.de

Ist der Parameter "smtpusername" leer, so wird ein anonymer Versand durchgeführt.

Die Konfiguration der smtp-Parameter erfolgt über die zentrale Konfigurationsdatei „ipw.properties". Dort kann auch eine Absender-E-Mail-Adresse konfiguriert werden, sofern es fachlich keinen Absender gibt, z. B. bei Systemmeldungen, bzw. die E-Mail-Adresse eines Systemadministrators für den Empfang von Systemnachrichten.

[1] Ein ‚X' gibt an, dass der Parameter über ipw.properties konfiguriert werden muss

4 Offene Punkte

Nr.	Beschreibung	Verantwortlich