|  |  |
| --- | --- |
| Dokumentation |  |

|  |  |
| --- | --- |
|  | PDF-AS Webanwendung Dokumentation |
|  | Dokumentation zur PDF-AS Webanwendung ab Version 4 |
|  | Version 0.3, 15.07.2014 |
|  | Andreas Fitzek – [andreas.fitzek@egiz.gv.at](mailto:andreas.fitzek@egiz.gv.at) |
|  | Tobias Kellner – [tobias.kellner@egiz.gv.at](mailto:tobias.kellner@egiz.gv.at) |

**Zusammenfassung:** Dieses Dokument beschreibt die Konfiguration der PDF-AS Webanwendung. Die PDF-AS Webanwendung erlaubt es, PDF Dokumente über ein Web Interface zu unterschreiben. Des Weiteren ermöglicht die PDF-AS Webanwendung externen Webanwendungen PDF Dokumente zu signieren.

Inhaltsverzeichnis

[1 Deployment 3](#_Toc393119355)

[1.1 Konfigurationsparameter 3](#_Toc393119356)

[1.2 SOAP-Schnittstelle 3](#_Toc393119357)

[1.3 PDF-AS Web Clusterbetrieb 4](#_Toc393119358)

[1.4 PDF-AS Web Konfigurationsdatei 5](#_Toc393119359)

[2 Beispiele 8](#_Toc393119360)

# Deployment

## Konfigurationsparameter

Im Java Anwendungsserver, zum Beispiel dem Apache Tomcat Server, muss eine Java Umgebungsvariable „pdf-as-web.conf“ definiert sein. Der Wert dieser Umgebungsvariablen ist der Dateipfad zur PDF-AS Web Konfigurationsdatei. Ein Beispielparameter für den Apache Tomcat Server:

-Dpdf-as-web.conf=“/…/pdf-as-web.properties“

## SOAP-Schnittstelle

PDF-AS Web bietet zwei SOAP-Schnittstellen um Dokumente zu unterschreiben bzw. zu verifizieren.

Die SOAP-Schnittstelle um Signaturen zu erzeugen ist definiert durch eine WSDL Datei. Die WSDL Datei kann unter *„{pdf-as-web-url}/wssign?wsdl“* abgerufen werden. Anwendungen können die SOAP-Schnittstelle nutzen um PDF-Dokumente direkt an PDF-AS Web hochzuladen. Bei diesem Request können diverse Signaturoptionen, wie beispielsweise der „Connector“, übergeben werden. Mit Hilfe der „Connector“ Option wird bestimmt womit die Signaturerzeugt werden soll. Hier können serverbasierte Signaturen, wie „JKS“ oder „MOA“ verwendet werden, oder clientbasierte Signaturen, wie „BKU“, „MOBILEBKU“ oder „ONLINEBKU“. Wird eine serverbasierte Signatur verwendet, ist das signierte Dokument in der Antwort enthalten. Wird eine clientbasierte Signatur verwendet, benötigt PDF-AS Web eine Benutzerschnittstelle um direkt mit dem Benutzer zu kommunizieren. In diesem Fall ist eine URL in der Antwort enthalten, auf die der Benutzer weitergeleitet werden muss. Das signierte Dokument wird dann entweder direkt an den Benutzer übermittelt oder die aufrufende Anwendung kann per „invoke-url“ informiert werden. „Abbildung 1.: Ablauf einer Signatur über die SOAP-Schnittstelle“ zeigt den Ablauf einer clientbasierten Signatur mit Hilfe der SOAP-Schnittstelle.

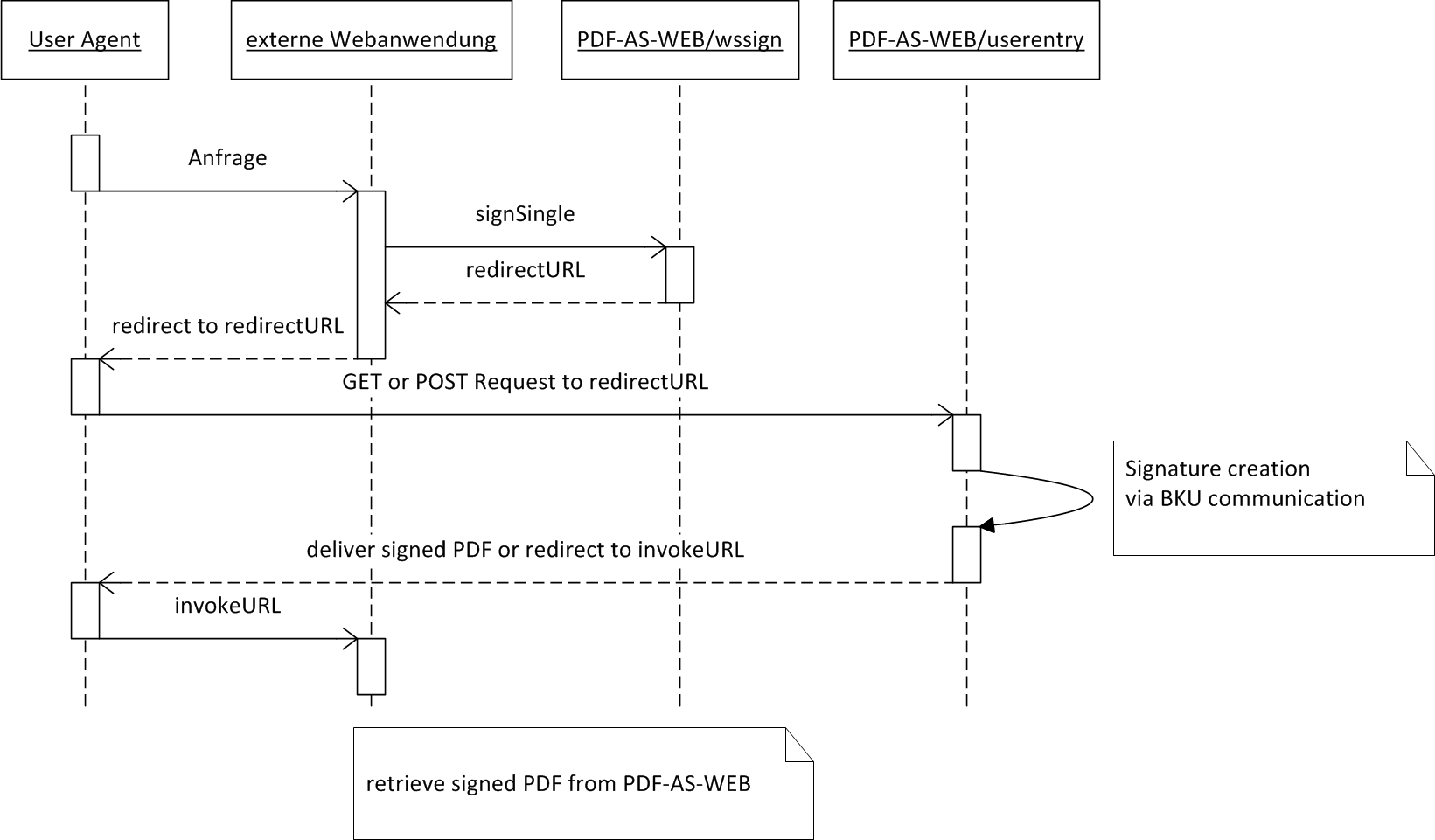


Abbildung 1.: Ablauf einer Signatur über die SOAP-Schnittstelle

Die SOAP-Schnittstelle bietet zwei Methoden „signSingle“ und „signBulk“. Mit der Methode „signSingle“ lässt sich ein Dokument signieren. Mit der Methode „signBulk“ lassen sich mehrere Signaturanfragen im Bulk erstellen.

Die SOAP-Schnittstelle um Dokumente zu verifizieren ist definiert durch eine WSDL Datei. Die WSDL Datei kann unter *„{pdf-as-web-url}/wsverify?wsdl“* abgerufen werden. Die SOAP-Schnittstelle bietet eine Methode „verify“ an. Diese Methode verifiziert ein Dokument und antwortet mit einer Liste von Signaturergebnissen. Für jede Signatur im Dokument wird ein Signaturergebnis gelistet.

## PDF-AS Web Clusterbetrieb

PDF-AS Web lässt sich in einem Cluster betreiben. Vorrausetzung für die korrekte Funktion von PDF-AS Web im Cluster ist, dass der Lastverteiler bestehende Sitzungen immer zur selben Instanz weiterleitet. Es muss also eine Session Fixation im Load Balancer geschehen. Ein Beispiel dafür mit zwei Tomcat Instanzen als Anwendungsserver und einem Apache Webserver.

In den beiden Tomcat Instanzen muss der Parameter jvmRoute für die Catalina engine festgelegt werden. Der Wert dieses Parameters muss sich in beiden Instanzen unterscheiden. In unserem Beispiel ist die „node1“ und „node2“

Dazu wird in der der conf/server.xml die Zeile „<Engine name=“Catalina“ defaultHost=“localhost“>“ geändert zu „<Engine name=“Catalina“ defaultHost=“localhost“ jvmRoute=“node1“>“ bzw. „<Engine name=“Catalina“ defaultHost=“localhost“ jvmRoute=“node2“>“.

Wenn beide Tomcat Instanz auf demselben Server ausgeführt werden, müssen auch die AJP Ports unterschiedlich sein. In unserem Beispiel sind diese auf 8009 und 8029 festgelegt.

Im Apache Webserver müssen die Module „proxy\_ajp“ und „proxy\_balancer“ aktiviert sein. Als erstes wird eine Balancer definiert:

<Proxy balancer://testcluster stickysession=JSESSIONID|jsessionid scolonpathdelim=On>

BalancerMember ajp://127.0.0.1:8009 min=10 max=100 route=node1 loadfactor=1

BalancerMember ajp://127.0.0.1:8029 min=10 max=100 route=node2 loadfactor=1

</Proxy>

Als letzer Schritt muss noch ein ProxyPass konfiguriert werden, welcher auf den Balancer zeigt:

ProxyPass /pdf-as-web balancer://testcluster/pdf-as-web

Wenn PDF-AS Web im Clusterbetrieb verwendet wird und mittels SOAP-Schnittstelle clientbasierte Signaturen erzeugt werden, benötigt PDF-AS Web eine Datenbank um die Clusterfähigkeit sicherzustellen. Nur in diesem Fall ist es zu empfehlen eine Datenbank für PDF-AS Web zu konfigurieren.

## PDF-AS Web Konfigurationsdatei

Die PDF-AS Web Konfigurationsdatei ist eine simple Java Properties Datei mit folgenden Einträgen:

|  |  |  |
| --- | --- | --- |
| Name | Werteberiech | Beschreibung |
| pdfas.dir | *Verzeichnis* | Das Basisverzeichnis für die PDF-AS Konfiguration |
| error.showdetails | *true | false* | Legt fest ob PDF-AS im Fehlerfall eine detaillierte Fehlermeldung liefern soll. |
| bku.local.url | *URL* | Die URL die PDF-AS für die lokale Bürgerkartenumgebung verwenden soll. Ist diese nicht definiert, erlaubt PDF-AS die Nutzung der lokalen Bürgerkartenumgebung nicht. |
| bku.online.url | *URL* | Die URL die PDF-AS für die online Bürgerkartenumgebung verwenden soll. Ist diese nicht definiert, erlaubt PDF-AS die Nutzung der online Bürgerkartenumgebung nicht. |
| bku.mobile.url | *URL* | Die URL die PDF-AS für die Handy Signatur verwenden soll. Ist diese nicht definiert, erlaubt PDF-AS die Nutzung der Handy Signatur nicht. |
| public.url | *URL* | Legt den öffentlichen Zugangspunkt für PDF-AS Web fest. (optional) |
| moa.enabled | *true | false* | Legt fest ob PDF-AS die Signatur mit einem MOA-SS Server zulassen soll. Der MOA-SS Server wird in der Basiskonfiguration von PDF-AS konfiguriert. |
| ks.enabled | *true | false* | Legt fest ob PDF-AS die Signatur mit einem KeyStore am Server zulassen soll. |
| ks.file | *Dateipfad* | Die bei einer Signatur mit einem Keystore zu verwendende KeyStore Datei. |
| ks.type | *JKS | PKCS12* | Die Art der Keystore Datei |
| ks.pass | *Passwort* | Das Passwort für die Keystore Datei |
| ks.key.alias |  | Der Bezeichner des Schlüssels in der KeyStore Datei mit dem die Signatur durchgeführt werden soll. |
| ks.key.pass | *Passwort* | Das Passwort für den Schlüssel in der KeyStore Datei. |
| soap.sign.enabled | *true | false* | Aktiviert oder Deaktiviert die SOAP-Schnittstelle. Standardmäßig ist die SOAP-Schnittstelle deaktiviert. |
| Soap.verify.enabled | *true | false* | Aktiviert oder Deaktiviert die SOAP-Schnittstelle für Verifikation. Standardmäßig ist die SOAP-Schnittstelle deaktiviert. |
| whitelist.enabled | *true | false* | Legt fest ob PDF-AS externe URLS mit der Whitelist vergleicht. |
| whitelist.url.\* | *JavaRegularExpression* | Eine Liste von Regular Expressions die eine Whitelist für externe URLS in PDF-AS festlegen. |
| request.store | *at.gv.egiz.pdfas.web.store.InMemoryRequestStore | at.gv.egiz.pdfas.web.store.DBRequestStore* | Legt die Implementierung des Requeststores fest. Nur wenn PDF-AS im Cluster verwendet wird und per SOAP-Schnittstelle eine clientbasierte Signatur erstellt werden soll, sollte dieser Parameter vom InMemoryRequestStore auf den DBRequestStore gestellt werden. Wenn hier der DBReqeustStore verwendet wird, speichert PDF-AS Web Signaturrequests, die per SOAP-Schnittstelle kommen und vom Benutzer bearbeitet werden müssen in eine Datenbank. In diesem Fall müssen die Eigenschaften hibernate.props.\* entsprechenden festgelegt werden. |
| request.db.timeout | *Number* | Gibt die Anzahl der Sekunden an, die ein Signaturrequest in der Datenbank gespeichert wird. |
| hibernate.props.\* | *Sammlung von Eigenschaften* | Alle Eigenschaften die unter diesem Prefix eingetragen sind dienen der Konfiguration von Hibernate für die Datenbankverbindung des DBRequestStore. Wenn dieser nicht konfiguriert ist, benötigt PDF-AS Web keine Datenbank. Ein komplettes Beispiel für diese Parameter ist in der Beispielkonfiguration in diesem Dokument zu finden. |
| reload.pwd | *Text* | Passwort um die Konfiguration neu zu laden. |
| reload.enabled | *true | false* | Aktiviert bzw. Deaktiviert das Servlet um die Konfiguration neu zu laden. |

Die Konfiguration kann zur Laufzeit neu geladen werden. Dies betrifft die Webkonfiguration und die Basiskonfiguration der PDF-AS-Bibliothek. Um die Konfiguration neu zu laden muss das Servlet /Reload mit der GET-Methode aufgerufen werden. Diesem Servlet muss der GET-Parameter „PASSWD“ übergeben werden. Der Wert dieses Parameters muss dem konfigurierten Wert in „reload.pwd“ entsprechen.

## Kommunikation

PDF-AS Web hat eingehende Verbindungen nur über den Anwendungsserver.

Ausgehende Verbindungen von PDF-AS Web sind Aufrufe wenn PDF-AS Web ein zu signierendes PDF-Dokument an einer URL abholt. Um Beispielsweise Portscans des internen Netzwerks zu verhindern, können diese URLs mit Hilfe einer Whitelist gefiltert werden.

# Beispiele

PDF-AS Web Konfigurationsdatei Beispiel:

# PDF-AS Basis Konfiguration

pdfas.dir=/config/.pdfas

# Oeffentliche URL

public.url=https://pdfas.egiz.gv.at/pdfas

# Show error details in PDF-AS

error.showdetails=false

# MOA-SS Signatur

moa.enabled=false

# Lokale BKU URL

bku.local.url=http://127.0.0.1:3495/http-security-layer-request

# Online BKU URL

bku.online.url=http://192.168.1.1/bkuonline/http-security-layer-request

# Handy Signatur URL

#bku.mobile.url=

ks.enabled=true

ks.file=/config/test.p12

ks.type=PKCS12

ks.pass=123abc

ks.key.alias=test

ks.key.pass=123abc

soap.sign.enabled=true

soap.verify.enabled=true

reload.pwd=123456

reload.enabled=true

# Whitelist

whitelist.enabled=true

# Matches everything

whitelist.url.01=^.\*$

#whitelist.url.02=^http://.\*$

#Request Store

# Default In Memory Store

#request.store=at.gv.egiz.pdfas.web.store.InMemoryRequestStore

# DB Request Store for cluster

#request.store=at.gv.egiz.pdfas.web.store.DBRequestStore

# seconds Requests are kept in Database (default 600)

#request.db.timeout=600

#Hibernate Properties for DB Store

#hibernate.props.hibernate.dialect=org.hibernate.dialect.MySQLDialect

#hibernate.props.hibernate.connection.driver\_class=com.mysql.jdbc.Driver

#hibernate.props.hibernate.connection.url=jdbc:mysql://localhost/pdfasweb

#hibernate.props.hibernate.connection.username=pdfasweb

#hibernate.props.hibernate.connection.password=pdfasweb

#hibernate.props.hibernate.connection.pool\_size=5

#hibernate.props.hibernate.connection.autocommit=false

#hibernate.props.hibernate.show\_sql=true

#hibernate.props.hibernate.hbm2ddl.auto=update

Dokumentenhistorie

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Datum | Autor(en) | Anmerkung |
| 0.1 | 06.02.2014 | Andreas Fitzek | Initiale Version |
| 0.2 | 19.02.2014 | Christian Maierhofer | Review |
| 0.3 | 15.07.2014 | Andreas Fitzek | SOAP-Schnittstelle, Clusterbetrieb |

Referenzen

|  |  |
| --- | --- |
|  |  |
|  |  |