Anleitung zur Überprüfung der Signatur von Elektronischen Kontoauszügen

Zur Prüfung, ob die qualifizierte Signatur eines elektronischen Kontoauszugs gültig ist, können verschiedene Softwarelösungen genutzt werden. Entsprechend zertifizierte Signaturanwendungskomponenten bzw. Signatur-Viewer werden auf den Internetseiten der Bundesnetzagentur bekanntgegeben. Bekannte Lösungen sind bspw.

- Sign Live! der Firma Intarsys
- OpenLimit Reader

Diese Lösungen erlauben u.a. die Erstellung gesetzeskonformer Signaturprüfprotokolle im für die Langzeitarchivierung geeigneten Format PDF/A.

1 Validierung einer Signatur mit dem Sign Live! CC Validation Client

Die Software kann unter folgendem Link geladen werden:
https://www.intarsys.de/SignLiveCC-SparkassenEdition

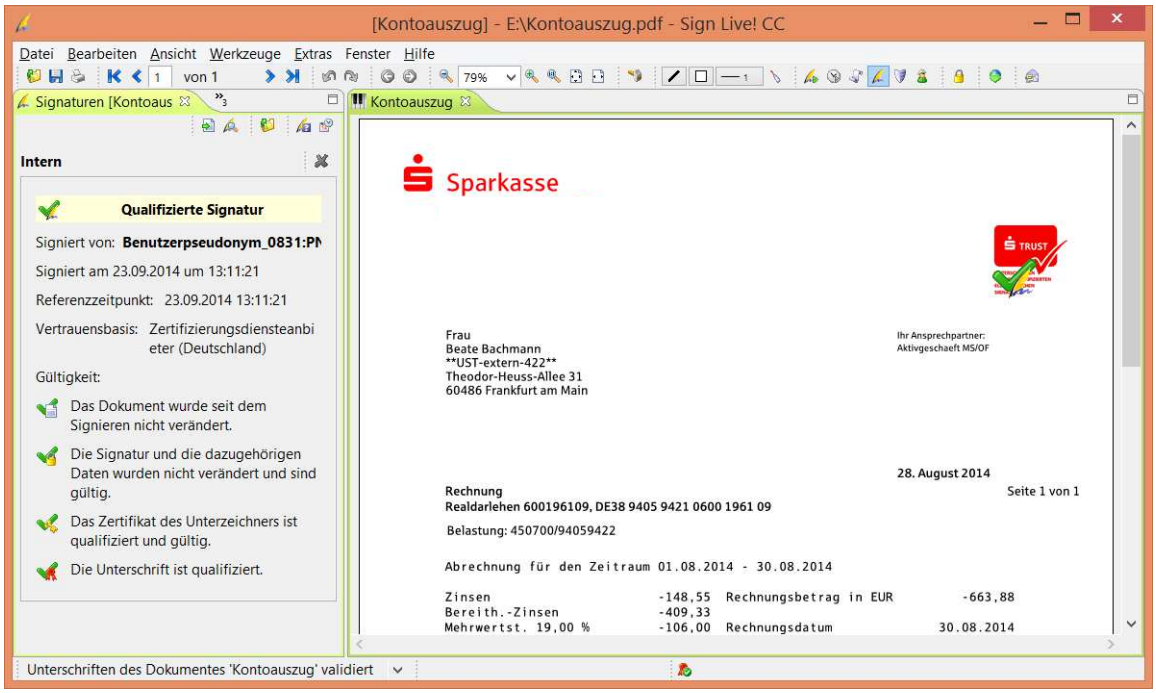
Die Nutzung der Software ist kostenfrei. Die Software erlaubt die Erstellung von maximal 10 Prüfprotokollen pro Tag. Dies sollte auch für geschäftliche Anwender ausreichend sein.

Es ist zu beachten, dass für die Installation der Software eine Java VM erforderlich ist. Ist diese noch nicht auf dem PC vorhanden, kann diese während des Installationsprozesses zusätzlich installiert werden.

Nach der Installation muss zunächst im Einstellungsdialog (Menüpunkt "Extras > Einstellungen") eine Parametrisierung erfolgen. Navigieren Sie zur Seite "Signaturen > Signaturvalidierung > Zertifikatsvalidierung" und beantworten Sie die Frage "Welche Zertifikate sollen mittels OCSP geprüft werden?" mit "Alle Zertifikate".

Zunächst wird die Software gestartet und über das Menü *Öffnen* die betreffende PDF-Kontoauszugsdatei geladen oder per Drag and Drop in das Fenster gezogen werden.

Der Prüfprozess der Signatur wird nach dem Öffnen automatisch gestartet. Dieser Prozess benötigt ggf. einige Sekunden. Anschließend wird im linken Fensterbereich der Status der Signatur angezeigt (s. Abbildung). Falls nicht, kann das entsprechende Fenster über das Menü *Ansicht -> Seitenleiste -> Signaturübersicht* eingeblendet werden.



Die Prüfung ist erfolgreich, wenn alle vier Einzelprüfungen erfolgreich und mit einem grünen Häkchen versehen sind:

- Das Dokument wurde seit dem Signieren nicht verändert.
- Die Signatur und die dazugehörigen Daten wurden nicht verändert und sind gültig.
- Das Zertifikat des Unterzeichners ist qualifiziert und gültig.[1]
- Die Unterschrift ist qualifiziert.

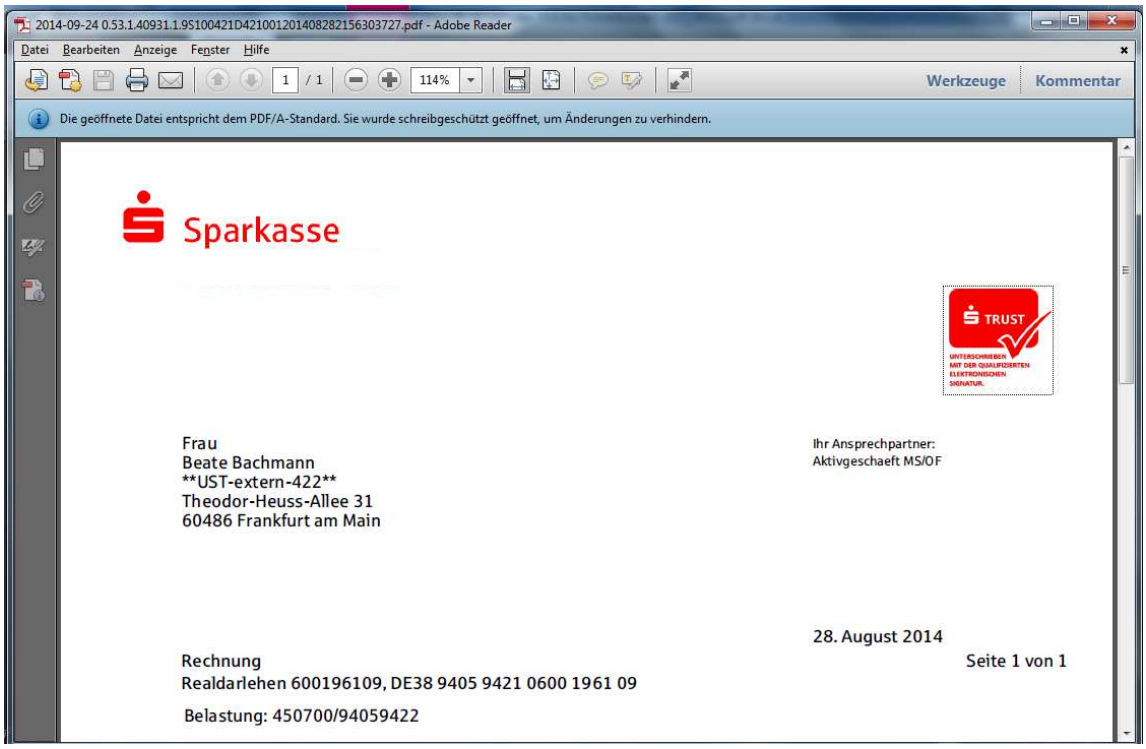
2 Validierung einer Signatur mit dem Adobe Reader

Der Adobe Reader erkennt beim Öffnen, ob ein Dokument eine Signatur beinhaltet. Hierzu muss mindestens die Version 6.0 des Adobe (Acrobat) Readers verwendet werden, da frühere Versionen keine signierten Dokumente unterstützen. Enthält das Dokument eine Signatur, wird die Signaturprüfung gestartet und das Ergebnis der Prüfung in einer blau unterlegten Zeile unterhalb des Menüs angezeigt. Diese Anzeige wird jedoch bei elektronischen Kontoauszügen i.d.R. von einer weiteren Meldung

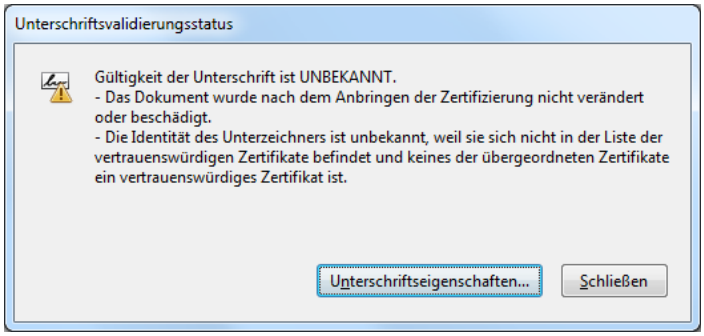
[1] Hinweis: Diese Prüfung ist nur bei bestehender Internetverbindung möglich, da die Software die Sperrlisten des Zertifikatanbieters S-TRUST laden muss. In Firmennetzwerken kann dieser Download u.U. durch die Firewall verhindert werden.

überlagert, die darauf hinweist, dass es sich im eine Datei gemäß PDF/A-Standard handelt (s. Abbildung).

Daher sollten nach dem Öffnen eines signierten Kontoauszugs mit dem Adobe Reader mit einem Klick auf das S-TRUST-Symbol rechts oben im Kontoauszug die Signatureigenschaften geöffnet werden.



In der Regel erscheint in den Signatureigenschaften die Meldung *„Gültigkeit der Unterschrift ist unbekannt“ (s. Abbildung).* Es wird zwar erkannt, dass das Dokument nach dem Unterzeichnen nicht mehr geändert oder beschädigt wurde, allerdings kann die Identität des Unterzeichners nicht verifiziert werden, da die Zertifikatshierarchien für qualifizierte Signaturen gemäß dem deutschen Signaturgesetz nicht standardmäßig im Acrobat Reader hinterlegt sind.



Das Zertifikat muss daher einmalig als vertrauenswürdig akzeptiert und hinterlegt werden. Hierzu ist wie folgt vorzugehen (Je nach Version des Adobe Readers können die Vorgehensweise und die Feldbeschriftungen leicht abweichen):

1. Auf „Unterschriftseigenschaften“ klicken
2. Anschließend im Fenster „Übersicht“ "Zertifikat anzeigen" wählen.
3. In der Zertifikatanzeige auf den Reiter "Vertrauenswürdigkeit" klicken und anschließend auf "Den vertrauenswürdigen Identitäten hinzufügen". Die anschließende Sicherheitsabfrage mit "OK" bestätigen.
4. In der Box "Kontakteinstellungen importieren" sicherstellen, dass die Option "Dieses Zertifikat als vertrauenswürdigen Stamm verwenden" ausgewählt ist.
5. Auf "OK" klicken und erneut mit „OK“ bestätigen.

Der beschriebene Vorgang ist nur einmalig erforderlich. Wenn das Dokument anschließend nochmal geöffnet wird, erscheint nach kurzer Prüfung die Meldung „Unterschrieben und alle Unterschriften sind gültig.“. Hierzu ist eine bestehende Internetverbindung erforderlich, da der Signaturviewer die aktuelle Sperrliste von S-TRUST laden muss.

Es sei jedoch wie oben bereits erwähnt darauf hingewiesen, dass die Validierung der Signatur mit dem Adobe Reader nicht denselben Stellenwert hat, wie die Prüfung mit einer zugelassenen Signaturanwendungskomponente, wie bspw. Sign Live!. Denn diese führt neben der Integritätsprüfung, also der Verifizierung der kryptographischen Gültigkeit der Signatur, auch die folgenden Prüfungen durch:

- *Gültigkeit der Zertifikatskette*: Qualifizierte Signaturen nach dem deutschen Signaturgesetz lassen sich lückenlos zurückverfolgen bis zu einem vertrauenswürdigen Wurzelzertifikat (bspw. der Bundesnetzagentur). Diese Wurzelzertifikate sind bereits in die Software integriert. Im Falle eines S-TRUST-Zertifikats ist dies das Wurzelzertifikat „S-TRUST Qualified Root CA“. Durch die Validierung ist sichergestellt, dass der Zertifizierungspfad bis zum Wurzelzertifikat mathematisch korrekt und lückenlos ist.
- *Prüfung auf eventuelle Zertifikatssperren*: Die Trust-Center geben sogenannte Sperrlisten mit Informationen über gesperrte und nicht mehr gültige Zertifikate heraus. Der Signaturviewer lädt diese Listen herunter und vergleicht die zu prüfenden Zertifikate mit den Sperrlisten. So wird eindeutig festgestellt, ob die

zu prüfende Signatur gültig ist und wirklich von dem Absender stammt. Auch eine Online-Prüfung von Signaturzertifikaten ist möglich.

Für eine aussagekräftige Prüfung der Signatur ist daher von der Verwendung des Adobe Readers abzuraten.