Sign Live! CC und Long Term Validation

(Kurzanleitung)

Inhaltsverzeichnis

1 Einführung

Auf Grund gesetzlicher Vorschriften müssen Dokumente unterschiedlich lang archiviert werden. Dies gilt auch für digitale Dokumente, einschließlich der sich auf dem Dokument befindlichen Signaturen.

Ob die Signatur valide, also gültig ist, sollte auch nach Jahren – vorzugsweise auch ohne Verbindung zum Internet – möglich sein.

Die Lösung ist, die Validierungsdaten direkt in das Dokument einzubetten. Somit gelingt der Nachweis, dass die Signatur zum Signaturzeitpunkt gültig war.

Die Voraussetzung für den Nachweis einer gültigen Validierung ist, dass bestimmte Normen eingehalten werden. Um diese Normierung kümmert sich ETSI[1] (***E****uropean* ***T****elekommunications* ***S****tandards* ***I****nstitute*). ETSI hat für die Signaturformate verschiedener Dokumentenarten die Standards PAdES[2], CAdES[3] und XAdES[4] entwickelt. Diese Profile tragen dem Umstand Rechnung, dass digital signierte Dokumente oft viele Jahre archiviert werden und es zu jedem Zeitpunkt in der Zukunft möglich sein muss, die Signatur des Dokuments zu prüfen. Dieses Konzept nennt man Long-Term Validation (LTV).

2 Validierung in Sign Live! CC

Sign Live! CC prüft beim Öffnen eines Dokuments automatisch, ob das Dokument signiert wurde[5]. Wenn ja, wird die Signatur sofort validiert.

Das Validierungsergebnis kann jederzeit in das Dokument eingefügt werden.

Hinweis:
Es werden nur gültige Sperrinformationen in das Dokument eingebettet.

[1] ETSI ist eine gemeinnützige Organisation und verfolgt das Ziel, weltweit anerkannte Standards für Informations- und Telekommunikationstechnologien zu schafften. ETSI ist von der Europäischen Union offiziell anerkannt.
[2] PAdES (engl.: (***P****DF* ***Ad****vanced* ***E****lectronic* ***S****ignatures*) für PDF-Dokumente
[3] CAdES (engl.: ***C****MS* ***Ad****vanced* ***E****lectronic* ***S****ignatures*) für CMS-Dokumente
[4] XAdES (engl.: ***X****ML* ***Ad****vanced* ***E****lectronic* ***S****ignatures*) für XML-Dokumente
[5] Die automatische Prüfung kann über Menüpunkt *Extras* > *Einstellungen* > *Signaturen* > *Signaturvalidierung* ein- und ausgeschaltet werden.

3 Einstellungen für LTV

Bei der LTV wird unterschieden, ob die Daten bereits während der Signaturerstellung eingebettet werden sollen oder erst nachträglich, also nach der Validierung. Dabei werden sowohl die Einstellungen zur Zertifikatsvalidierung, als auch Einstellungen aus der Signaturerstellung herangezogen. Aus diesem Grund lohnt sich ein genauerer Blick auf die Einstellungen, wobei hier nur die für die LTV relevanten Einstellungen beleuchtet werden.

3.1 Einstellungen Zertifikatsvalidierung

Die Validierung von Signaturen kann über Sperrlisten oder online per OCSP erfolgen. Sind beide Einstellungen aktiv, prüft *Sign Live! CC* die Signatur zuerst über OCSP. War die OCSP-Prüfung erfolgreich, werden die Sperrlisten nicht mehr herangezogen.

Ist die OCSP-Prüfung nicht aktiviert oder fehlgeschlagen – zum Beispiel weil keine Online-Verbindung vorhanden – werden die Sperrlisten herangezogen, da diese lokal zur Verfügung stehen.

Hier erfolgen die Einstellungen, die während der Signaturvalidierung herangezogen werden.

1. Starten Sie *Sign Live! CC*
2. Wählen Sie Menüpunkt *Extras* > *Einstellungen*.

Scrollen Sie bis zu *Signaturvalidierung* und markieren Sie den Eintrag *Zertifikatsvalidierung*.

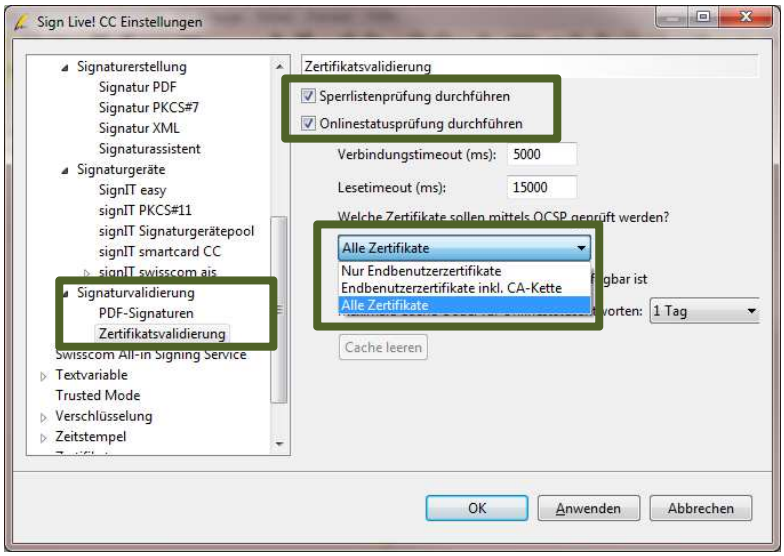


Abbildung 1 - Einstellungen Zertifikatsvalidierung

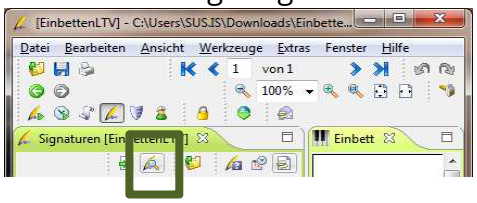
Welche Art der Prüfung?
Obwohl einige TrustCenter die Sperrlistenprüfung abgeschafft haben kann diese Einstellung aktiv bleiben.

Die Onlinestatusprüfung sollte nach Möglichkeit aktiviert bleiben.

Welche Zertifikate sollen geprüft werden?
Standardmäßig werden alle Zertifikate geprüft. Wir empfehlen diese Einstellung beizubehalten.

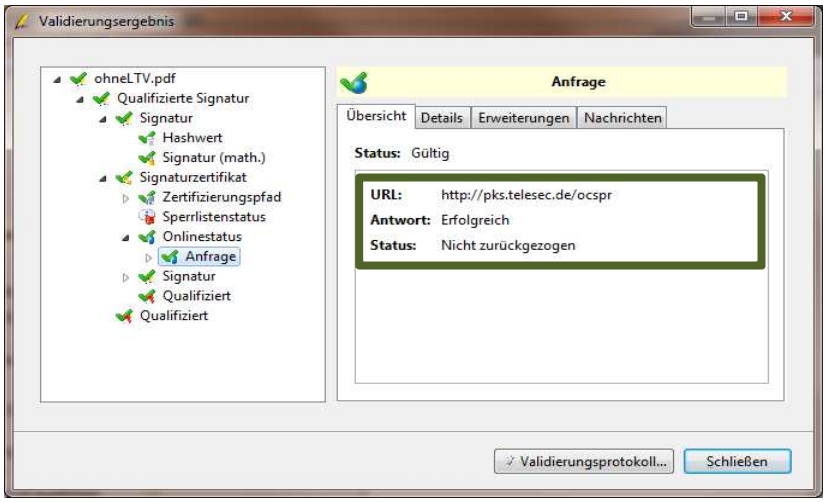
3.1.1 Anzeige Validierungsergebnis mit/ohne eingebetteter OCSP-Prüfung

Nach der Validierung der Signatur wird das Validierungsergebnis in der Seitenleiste „Signaturübersicht“[6] angezeigt.



Ob die Validierungsdaten eingebettet wurden ist in der Übersicht sichtbar. Öffnen Sie dazu das Fenster Validierungsergebnis über das zweite Symbol auf der Seitenleiste.

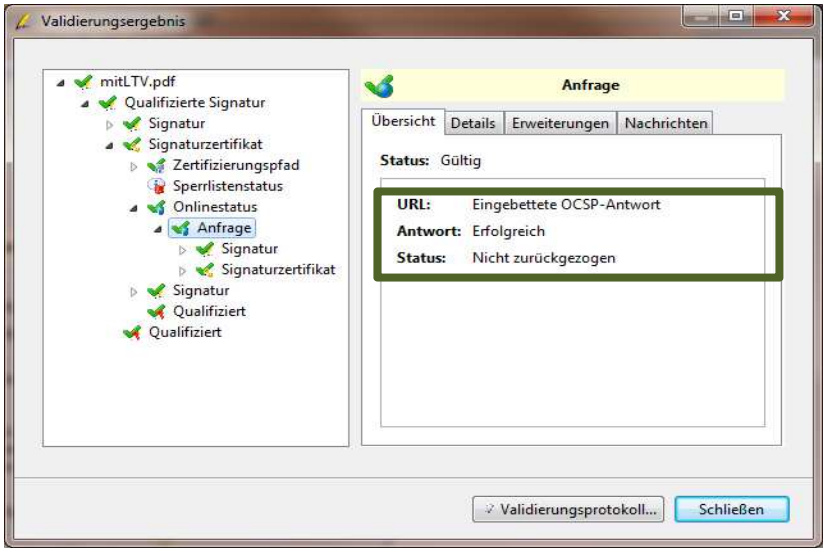
Ohne eingebettete OCSP-Anfrage wird die URL der Anfrage angezeigt.



Hinweis zum Sperrlistenstatus:
Da die OCSP-Abfrage erfolgreich war, werden Informationen aus Sperrlisten nicht mehr herangezogen.

Abbildung 2 - Anzeige des Validierungsergebnisses ohne LTV

Mit eingebetteter OCSP-Anfrage wird auf die Einbettung hingewiesen.



URL:
In der URL-Anzeige erfolgt der Hinweis auf die eingebettete OCSP-Antwort.

Abbildung 3 - Anzeige des Validierungsergebnisses mit LTV

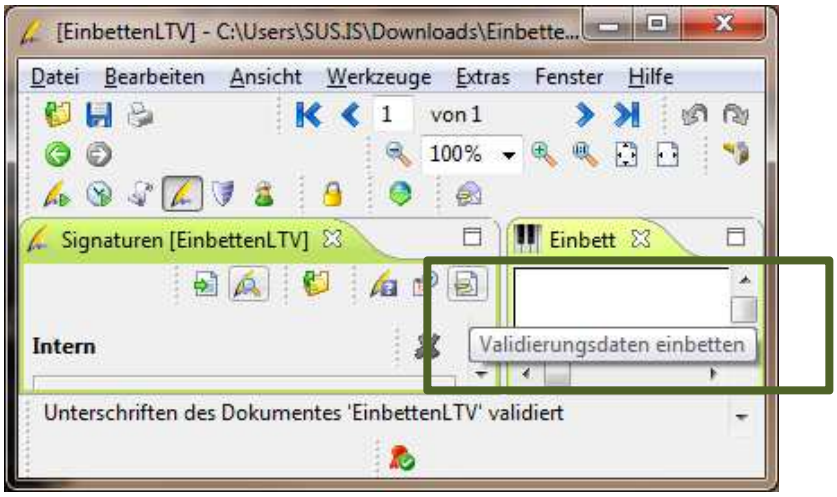
[6] Die Seitenleiste kann im Menüpunkt *Ansicht* > *Seitenleiste* > *Signaturübersicht* eingeschaltet werden.

3.1.2 Validierungsdaten nachträglich einbetten

Sind die Validierungsdaten nicht eingebettet, kann dies bei Bedarf nachgeholt werden.

Um die Validierungsdaten einzubetten, öffnen Sie das Dokument und warten Sie, bis die Validierung abgeschlossen ist.

Die Validierung wird auf Grundlage der aktuellen Einstellungen durchgeführt. Sollten Sie die Einstellungen geändert haben, führen Sie die Validierung nochmals aus[7].



Nutzen Sie dieses Symbols aus der Seitenleiste Signaturübersicht um die aktuellen Validierungsdaten einzubetten.

Abbildung 4 - Validierungsdaten einbetten

3.2 Einbetten der LTV-Informationen während der Signaturerstellung

Für das Einbetten der LTV-Informationen während der Signaturerstellung muss zum Zeitpunkt der Signaturerzeugung der OCSP- Dienst und/oder Sperrlisten zur Verfügung stehen. Durch die eingebetteten Daten kann die spätere Prüfung offline erfolgen.

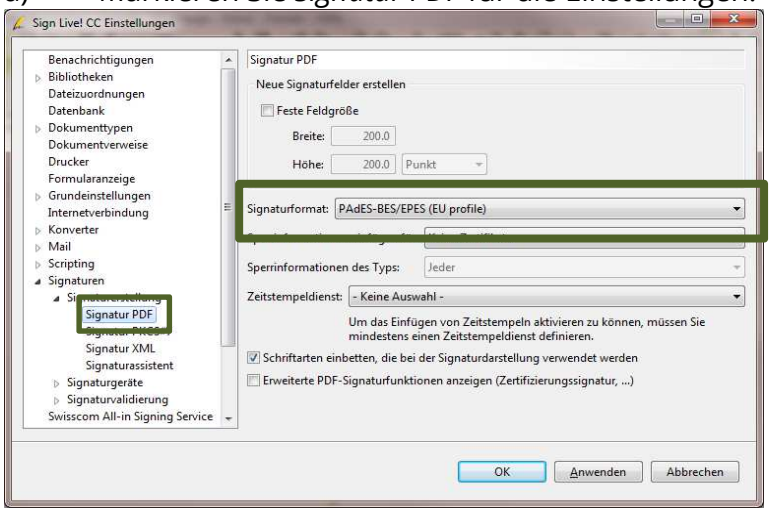
Werden alle Zertifikate - von Herausgeber inklusive aller Zwischenzertifikate bis zum Endbenutzerzertifikat - eingefügt, bilden diese eine Vertrauenskette, *Trusted Chain* genannt.

Welche Validierungsinformationen (Sperrinformationen) sofort eingebettet werden, wird in den Einstellungen für jedes Signaturformat separat festgelegt.

Wählen Sie Menüpunkt *Extras* > *Einstellungen*.
Scrollen Sie bei Bedarf hinunter bis zum Punkt *Signaturen* und öffnen Sie das Verzeichnis *Signaturerstellung*.

[7] Validierung über Menüpunkt *Werkzeuge* > *Signaturfunktionen* > *Dokument validieren*.

a) Markieren Sie *Signatur PDF* für die Einstellungen:



Signaturformat:
Da es sich um eine PDF-Signatur handelt ist als Signaturformat das PAdES-BES/EPES (EU profil) eingestellt. Auf Wunsch können Sie nach PAdES-Basic wechseln.

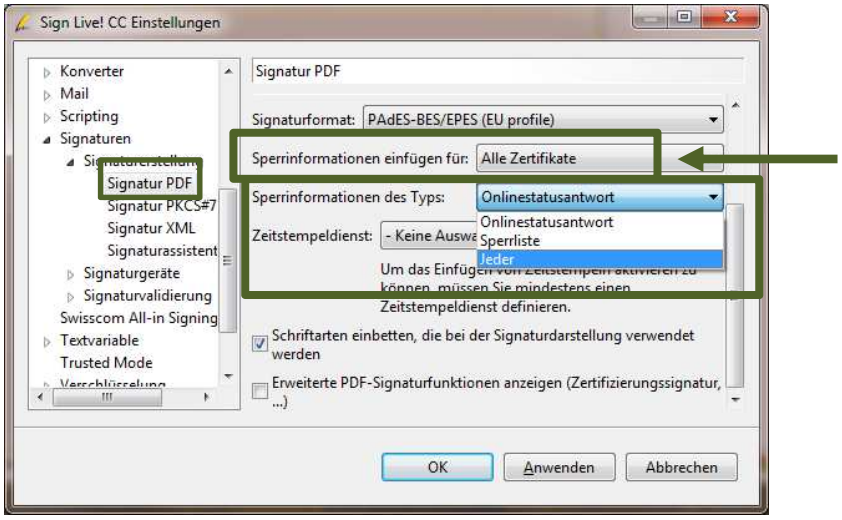
Abbildung 5 - Einstellung Signaturerstellung PDF

Einstellung für sofortiges Einfügen der LTV-Daten für PDF-Signatur

Sollen die Sperrinformationen sofort eingefügt werden, wird dies durch die Einstellung „Alle Zertifikate“ erreicht.

Beim Typ der Sperrinformationen legen Sie fest, welche Informationen eingebettet werden. Es empfiehlt sich die Auswahl von **„Jeder“**, da diverse TrustCender nicht mehr mit Sperrlisten arbeiten.

Es können auch nur die **OCSP-Abfrage** (Onlinestatusantwort) oder der **Sperrliste** eingebettet werden.
Bitte beachten Sie, dass durch die OCSP-Abfrage die Signaturerstellung etwas länger dauert, da das Signaturzertifikat online geprüft wird.



Sperrinformationen für Zertifikate:
Es empfiehlt sich, die Sperrinformationen für **„Alle Zertifikate“** einzustellen.

Sperrinformationen des Typs:
Bei der Einstellung **„Jeder“** ist es unerheblich, welche gültige Sperrinformation eingebettet wird.

Abbildung 6 - Einstellung zur sofortigen Einbettung der Validierungsdaten bei PDF-Signatur

Sind **Zeitstempel** eingerichtet, können auch diese Daten eingebettet werden.

Der Vollständigkeit halber werden hier noch die Einstellungen für das Einfügen der Sperrinformationen für die PKCS#7-Signatur und die Signatur einer XML-Datei angezeigt.

b) Markieren Sie *Signatur PKCS#7* für Grundeinstellungen zu PKCS#7-Signaturen:

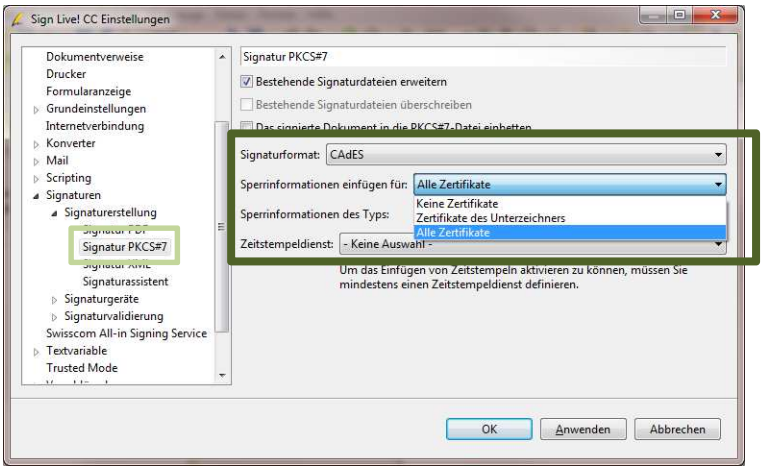


Abbildung 7 - Einstellung Sperrinformationen für PKCS#7

Signaturformat:
Für PKCS#7-Signatur auf verschiedenen Dokumente (z. B. TXT-Dateien) wird das Signaturformat CAdES verwendet. Auf Wunsch können Sie auf das Signaturformat CMS wechseln.

Sperrinformationen:
Analog zu PDF-Signaturen empfiehlt es sich **„Alle Zertifikate"** während der Signatur einzubetten.

c) Signatur XML:

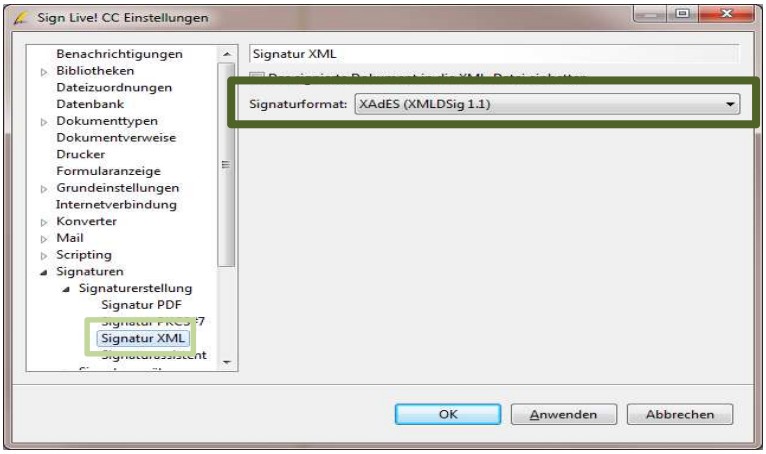


Abbildung 8 - Einstellung Sperrinformationen für XML

Signaturformat:
Für die Signatur einer XML-Datei wird das Signaturformat XAdES verwendet.