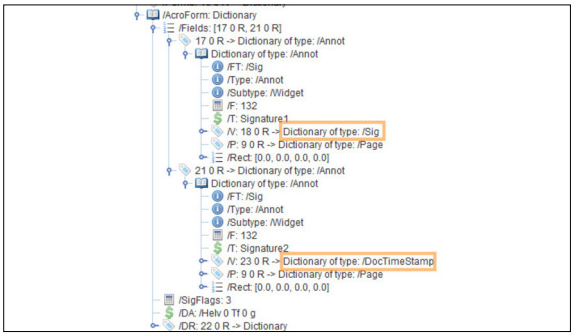
Alexis
Thomas Cyrill
Suter

Diplomand	Alexis Thomas Cyrill Suter
Examinator	Prof. Dr. Andreas Steffen
Experte	Dr. Ralf Hauser, PrivaSphere AG, Zürich
Themengebiet	Sicherheit

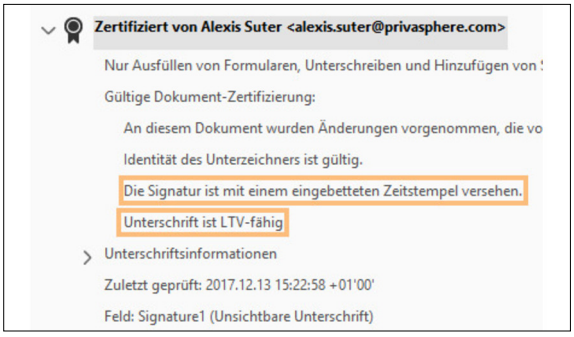
Long-Term Validation für PDF Signaturen (LTV)

```
/ExtensionLevel 5
>>
>>
/Version /1.7
>>
endobj
21 0 obj
<<
/Font 23 0 R
>>
endobj
22 0 obj
<<
/VRI 24 0 R
/OCSPs [25 0 R 26 0 R 27 0 R]
/CRLs [28 0 R 29 0 R]
/Certs [30 0 R 31 0 R 32 0 R 33 0 R 34 0 R 35 0 R 36 0 R 37 0 R 38 0 R]
>>
endobj
23 0 obj
<<
/Helv 39 0 R
/ZaDb 40 0 R
>>
endobj
24 0 obj
<<
/53699A368EB8807822CA228A116F838B44091636 41 0 R
>>
endobj
```

Einbindung strukturierter Daten in ein PDF Dokument.



Ein PDF-Dokument kann mehrere Signaturen enthalten. Die äussere überlappt die innere und sichert diese ab.



Die LTV-Fähigkeit des Dokumente wird im Adobe Acrobat Reader angezeigt.

Ausgangslage: Aktuell ist die Verlagerung von der Papierwelt in die digitale Welt voll im Gange. Deshalb werden diverse Prinzipien auf das Digitale übertragen. Dazu gehört natürlich auch das Unterschreiben. Es gibt bereits sehr gute Standards für das sogenannte Signieren von Dokumenten. Doch ist die Akzeptanz und Verbreitung noch sehr klein. Der Schweizer Bund hat hierzu Regelungen für die digitale Signatur aufgestellt, die auf den detaillierten Spezifikationen des ETSI basieren. Diese geben vor, wie Signaturen erweitert werden sollen, um für längere Zeit gültig (valide) zu sein – genauer, weit über die Gültigkeit eines signierenden Zertifikats.

Problemstellung: Optimalerweise werden diese Validierungs-Informationen direkt in das signierte Dokument eingebunden. Dies ist aber ein komplexer Prozess, denn der Inhalt eines signierten Dokuments darf und kann nicht verändert werden. Doch um das Problem zu umgehen wurde zumindest für PDF-Dokumente ein Ausweg gefunden. Die Validierung kann dem Dokument angehängt werden, ohne dabei den Inhalt zu verändern.

Vorgehen: Um die Validierung für einen grösseren Zeitraum zu ermöglichen (LTV – Long Term Validation), werden zusätzliche Daten in ein Dokument eingebunden. Es sind vereinfacht zweierlei.

- Ein extern signierter Zeitstempel ist da um die Existenz einer Signatur zu einem Zeitpunkt zu beweisen und einzufrieren.
- Validierungsdaten zu allen benutzten Zertifikaten werden dem Dokument angehängt. Es werden die aktuellen Daten abgefragt (OCSP), die bezeugen, dass das entsprechende Zertifikat zum Zeitpunkt der Signatur war.

Die Arbeit hatte zum Ziel den LTV Standard zu verstehen, umzusetzen und in das Open Source Projekt "Apache PDFBox" zu integrieren. Somit ist die Implementation von LTV öffentlich zugänglich und kann dank des realisierten Beispiels auch in anderen Projekten eingesetzt werden.

Für die Umsetzung wurden diverse Standards herangezogen. Zu den wichtigsten gehören:

- PDF/A – Standard für PDF Dokumente, über den auch LTV definiert ist
- CMS – Cryptographic Message Syntax, mit ASN.1 Encoding
- OCSP – Online Certificate Status Protocol, Valdierungs Informationen