Signierte PDF-Dateien - Signatur wird als ungültig bewertet

PDF-Anzeigeprogramme können bestimmte qualifizierte Signaturen nicht validieren

Viele aktuelle PDF-Anzeigeprogramme können qualifizierte elektronische Signaturen nicht prüfen, die mit dem Signaturalgorithmus ECDSA (Elliptic Curve Digital Signature Algorithm) erstellt wurden, wenn spezielle elliptische Kurven, wie zum Beispiel die Brainpool-Kurven verwendet wurden.

Konformität zum Deutschen Signaturgesetz

Gemäß aktuellem Algorithmenkatalog für 2014 ist die Verwendung der elliptischen Brainpool-Kurven für ECDSA in Deutschland für qualifizierte Signaturen durch die Bundesnetzagentur vorgeschrieben. Andere Kurven dürfen nicht verwendet werden. Die Bundesnetzagentur ist, laut Deutschem Signaturgesetz, die Aufsichtsbehörde, die jedes Jahr festlegt, welche Signaturalgorithmen für qualifizierte elektronische Signaturen für wie lange verwendet werden dürfen.

Der Governikus Signer und der Web-basierte Governikus Verification Service erkennen qualifizierte Signaturen, die mit dem Signaturalgorithmus ECDSA unter der Verwendung von Brainpool-Kurven erstellt wurden und können diese Signaturen auch validieren.

Technischer Hintergrund

Die PDF-Anzeigeprogramme erkennen zwar, dass die PDF-Datei signiert ist. Die Signaturen werden allerdings als ungültig bewertet. Wir haben dies mit den folgenden PDF-Anzeigeprogrammen getestet, die eine Komponente zur Validierung von Signaturen enthalten(Stand Dezember 2014): Adobe Reader (Version 11.0.0.9), Foxit Reader, Nitro Reader, PDF-XChange Viewer; dabei benutzen viele PDF-Anzeigeprogramme zum Validieren von Signaturen denselben Security Handler Adobe.PPKLite. Dieser Security Handler unterstützt die elliptischen Kurven NIST P256, P384 und P521, die vom National Institute of Standards and Technology, U.S. Department of Commerce. empfohlen werden. Die Brainpool-Kurven werden nicht unterstützt. Brainpool-Kurven werden zurzeit durch die folgenden qualifizierten Signaturkarten angewendet:

- TeleSec PKS-ECC-Signaturkarte
- Neuer Personalausweis mit einem nachgeladenen qualifizierten Zertifikat.

Die Brainpool-Kurven wurden durch eine Arbeitsgruppe von Firmen und Institutionen spezifiziert und sind im RFC 5639 der IETF standardisiert.

Beispiel Adobe Reader

Die folgende Abbildung zeigt die Meldung, die der Adobe Reader ausgibt, wenn er eine qualifiziert signierte PDF-Datei anzeigt, die mit dem Signaturalgorithmus ECDSA unter Verwendung einer Brainpool-Kurve signiert wurde. Korrekterweise sollte die Fehlermeldung des Adobe Readers hier lauten, dass der benutzte Signaturalgorithmus nicht unterstützt wird und der Status der Signatur daher unbekannt ist.

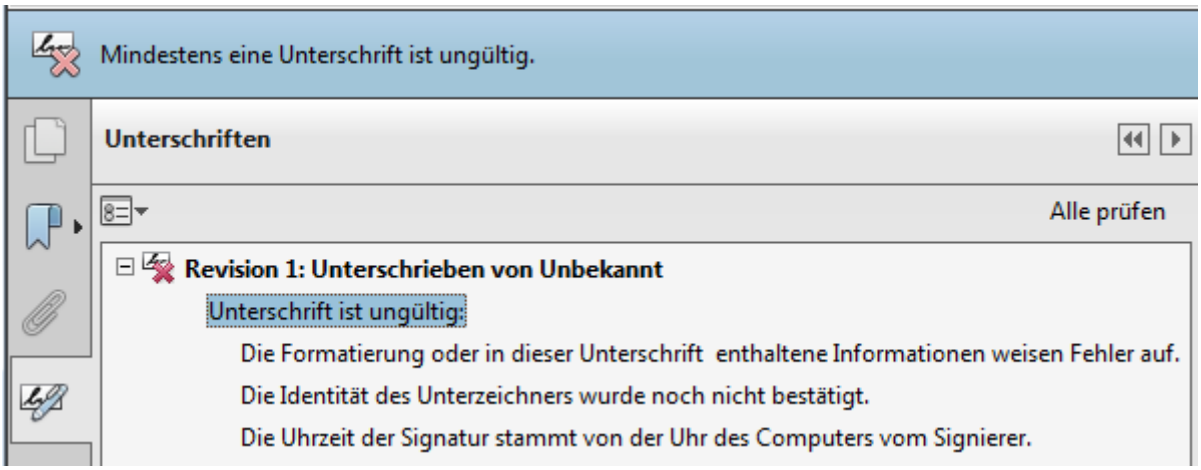

Abbildung 1: Beispiel Adobe PDF-Reader - Unterschrift ungültig

Quellenhinweise

	**Bezugsquellen**: Hier finden Sie das Dokument von Adobe Systems zu unterstützen ECC-Algorithmen: Document security algorithms - Adobe Systems

	**Bezugsquellen**: Hier finden Sie den Algorithmenkatalog für 2014, veröffentlicht von der Bundesnetzagentur.

Hinweis

Zu Demonstrationszwecken ist diese PDF-Datei signiert. Für die Erstellung der Signatur wurde eine deutsche, qualifizierte Signaturkarte verwendet, die die genannten Brainpool-Kurven benutzt.