Empfehlungen zur technischen Umsetzung von Signaturdiensten

1. Einleitung

Mit der Aufhebung des Signaturgesetzes und der Signaturverordnung entfällt die bisherige gesetzliche Grundlage für den Algorithmenkatalog, der letztmals am 30.12.2016 im Bundesanzeiger veröffentlicht wurde (Bundesnetzagentur, 2016). Eine Weiterentwicklung des Algorithmenkatalogs in Form eines unverbindlichen Dokuments, das die Vorgaben des Algorithmenkatalogs in Form unverbindlicher Empfehlungen zum Stand der Technik fortschreiben würde, wird als nicht sinnvoll angesehen. Stattdessen wird primär auf die Empfehlungen des SOGIS-Kryptokataloges (SOG-IS, 2016) verwiesen. Dies steht im Einklang zur bestehenden Konsensposition der eIDAS Expert Group, wie sie sich aus dem Sitzungsprotokoll zur Sitzung der Gruppe vom 12.5.2017 ergibt (eIDAS Expert Group, 2017). Dieser Konsens setzt die Aufforderung „die Mitgliedstaaten [sollten] zusammenarbeiten, um sich auf die zu verwendenden kryptografischen Algorithmen, Schlüssellängen und Hash-Funktionen in diesem Bereich zu einigen“ aus Erwägungsgrund (8) in Durchführungsbeschluss (EU) 2016/650 der Kommission vom 25. April 2016 um.

Das vorliegende Dokument stellt dementsprechend keine Fortführung des Algorithmenkatalogs dar, sondern soll Anwender, Hersteller und Nutzer von Vertrauensdiensten durch Verweise auf existierende Standards und Richtlinien bei der sicheren Implementierung digitaler Signaturverfahren im eIDAS-Rahmen unterstützen. Hierbei wird in erster Linie der SOGIS-Katalog als Referenz herangezogen, und nur für zusätzliche Aspekte der sicheren Implementierung auf andere Quellen verwiesen.

2. Empfohlene Algorithmen

Ein digitales Signaturverfahren besteht grundsätzlich aus einem kryptographischen Hashverfahren sowie aus einem asymmetrischen Algorithmus zur Signierung der Daten. Nach heutigem Kenntnisstand als sicher zu bewertende und im SOGIS-MRA konsentierte Verfahren sind im SOGIS-Kryptokatalog (SOG-IS, 2016) zu finden.

Der SOGIS-Katalog unterscheidet hierbei zwischen empfohlenen Verfahren und Legacy-Mechanismen. Die Nutzung der Legacy-Mechanismen wird nicht empfohlen, da sie nicht mehr in vollem Umfang dem kryptographischen Stand der Technik entsprechen. Ihr Einsatz genügt aber bis zu dem Zeitpunkt des Auslaufens ihrer Eignung den Anforderungen (siehe hierzu Abschnitt 1.1 von (SOG-IS, 2016)).

Die im SOGIS-Katalog empfohlenen Signaturverfahren basieren auf drei verschiedenen Grundmechanismen: RSA, diskreten Logarithmen in elliptischen Kurven, und diskreten Logarithmen in endlichen Körpern. Die empfohlenen Schlüssellängen hängen vom Typ des genutzten kryptographischen Primitivs ab. Die derzeit empfohlenen Schlüssellängen finden sich in den Abschnitten 4.1 bis 4.3 von (SOG-IS, 2016). Dort finden sich auch weitere Hinweise zur Schlüsselgenerierung und zur Auswahl geeigneter Nutzungsparameter, die für eine sichere Nutzung der Verfahren beachtet werden müssen. Eine Liste empfohlener Hashfunktionen findet sich dort in Abschnitt 2.3.

Die konkrete Festlegung empfohlener Signaturverfahren findet sich in (SOG-IS, 2016) Abschnitt 5.2.

Bei der Schlüsselerzeugung für die empfohlenen Signaturverfahren und auch bei der Erzeugung ephemerer Schlüssel für DSA- und EC-basierte Signaturverfahren wird die gleichverteilte Erzeugung von Zahlen aus einem festgelegten Intervall benötigt. Hierzu wird empfohlen, die Hinweise aus (SOG-IS, 2016) Abschnitt 6.3 zu beachten. Für die Erzeugung eines gleichverteilten Stroms von Zufallsbits werden in Abschnitt 6.2 des gleichen Dokuments drei Verfahren aufgelistet.

3. Sonstige Hinweise und Empfehlungen

Bei der Prüfung digitaler Signaturen etwa im Rahmen von Verfahren zur Langzeitarchivierung müssen unter Umständen einmal ausgestellte Signaturen noch beträchtliche Zeit nach dem Auslaufen ihrer Eignung geprüft werden. Hierbei kann insbesondere das Problem auftreten, dass festgestellt werden muss, ob eine Signatur zu dem Zeitpunkt der Aufbringung eines qualifizierten Zeitstempels noch den damaligen Anforderungen genügt hat. Bei dieser Prüfung ist es nicht einfach, einen gemeinsamen Test zu finden, der den Ansprüchen des digitalen Binnenmarktes gerecht wird. Es wird daher empfohlen, hierfür die Liste der Verfahren und Gültigkeitsperioden aus Abschnitt 6 von (Bundesnetzagentur, 2016) als Grundlage heranzuziehen und im Fall einer erfolglosen Prüfung ein Protokoll zu erzeugen, aus dem hervorgeht, welche innere Signatur oder welche inneren Signaturen aus welchem Grund nicht erfolgreich geprüft werden konnten.

Die Hinweise aus Abschnitt 5 von (Bundesnetzagentur, 2016) zur sicheren Langzeitarchivierung signierter Dokumente sind aus sicherheitstechnischer Sicht weiterhin sinnvoll.

Der SOGIS-Katalog beschränkt sich im Bereich der Zufallszahlenerzeugung auf die Beschreibung geeigneter Nachbearbeitungsmechanismen. Jeder Zufallsgenerator benötigt aber auch eine Quelle tatsächlich unvorhersagbarer Bits, also eine Entropiequelle. Der SOGIS-Katalog fordert hier für den Seed eines akzeptierten Zufallsgenerators eine Mindestentropie von 125 Bit, aber es wird offengelassen, wie das Vorliegen einer ausreichenden Seed-Entropie nachgewiesen werden kann. Es wird hier als grundsätzliche Sicherungsmaßnahme empfohlen, die Hinweise aus (Bundesamt für Sicherheit in der Informationstechnik, 2018) Abschnitt 9 zu beachten.

Für RSA-basierte Verfahren ist eine adäquate Methode zur Primzahlerzeugung unabdingbar als Voraussetzung der Sicherheit des Signaturverfahrens. Genauere Empfehlungen zu diesem Thema finden sich in Abschnitt B.5 von (Bundesamt für Sicherheit in der Informationstechnik, 2018).

Literaturverzeichnis

Bundesamt für Sicherheit in der Informationstechnik. (Januar 2018). BSI TR-02102-1: Kryptographische Verfahren, Empfehlungen und Schlüssellängen, Version 2018-01.

Bundesnetzagentur. (30. 12 2016). *www.bundesanzeiger.de.* Von Bundesanzeiger: https://www.bundesanzeiger.de/ebanzwww/wexsservlet?page.navid=official_starttoofficial_print&genericsearch_param.edition=BAnz+AT+30.12.2016&global_data.language= abgerufen

eIDAS Expert Group. (2017). Minutes 17th meeting of the eIDAS Expert Group (Trust Services). Brüssel.

SOG-IS. (2016, 05). *SOG-IS Crypto Evaluation Scheme: Agreed Cryptographic Mechanisms.* Retrieved from https://www.sogis.org/documents/cc/crypto/SOGIS-Agreed-Cryptographic-Mechanisms-1.0.pdf