Angaben des BSI zur Verwendung der Hashfunktion SHA-1 für qualifizierte Zertifikate
(zur für den 6.12.2006 anberaumten, dann aber ausgefallenen Expertenanhörung zum Algorithmenkatalog 2007)

Ausschnitt aus einer Mail des BSI vom 4.12.2006 an die Bundesnetzagentur:

„Kollisionsangriffe gegen die Zertifikaterstellung mit SHA-1
können von vornherein verhindert werden, wenn folgendes gilt:

1) Es wird das X.509v3 Format gemäß ISIS-MTT verwendet.
2) Die Seriennummer ("serialNumber") des Zertifikats hat eine genügend hohe Entropie h für den Angreifer. D.h. die Unsicherheit des Angreifers über die Seriennummer eines zu erstellenden Zertifikats ist mindestens h Bits.

Es wurden drei mögliche Wege identifiziert, wie eine solche Entropie sicher gewährleistet werden kann:

a) In die Generierung der Seriennummer gehen effektiv mindestens h Bit Entropie eines Zufallsgenerators ein.
b) Es wird ein Counter mit einem ausreichend sicheren Verfahren (z.B. 3DES) unter Verwendung eines geheimzuhaltenden Schlüssels verschlüsselt. Mindestens h Bits des Chiffrats gehen effektiv in die Generierung der Seriennummer ein.
c) Mindestens h Bit Entropie des zufällig auf der Karte generierten öffentlichen Schlüssels gehen effektiv in die Seriennummer ein. Notwendige Voraussetzung dafür ist allerdings, dass ein Angreifer den öffentlichen Schlüssel vor der Zertifikaterstellung nicht kennen kann. Insbesondere muss also gewährleistet sein, dass der öffentliche Schlüssel zufällig generiert wird und durch organisatorische Maßnahmen ausgeschlossen ist, dass ein Angreifer ihn vor der Zertifikaterstellung auslesen kann.

Die Mindestentropie h sollte ab Anfang 2010 20 Bit betragen.

Wir werden bei der Expertenanhörung bezüglich SHA-1 als vorläufige Angaben folgendes erklären:

'SHA-1 kann zur Zertifikaterstellung als bis Ende 2009 geeignet angesehen werden, sofern das X.509 Format gemäß ISIS-MTT verwendet wird. Dabei wird davon ausgegangen, dass ein Angreifer die Seriennummer nicht vorgeben kann und dass durch den organisatorischen Ablauf beim Zertifikaterstellungsvorgang in der Praxis ein Angreifer die Seriennummer höchstens bis auf mehrere Bits vorhersehen kann.
Eine Eignung für die Zertifikaterstellung bis Ende 2010 ist gegeben, falls gewährleistet ist, dass für einen Angreifer vor der Zertifikaterstellung mindestens 20 Bit Unsicherheit über die Seriennummer gegeben sind. Zur Gewährleistung dieser Anforderung gibt es die oben beschriebenen Möglichkeiten.' “