Bundesamt
für Sicherheit in der
Informationstechnik

Deutschland
Digital•Sicher•BSI•

Übergangsregelungen für die Zertifizierung von eID-Clients nach TR-03124-2

Version 2024-01

Datum: 6. Dezember 2023

1 Einleitung

Dieses Dokument definiert Übergangsregelungen für die Zertifizierung von eID-Clients nach TR-03124-2 [1]. Die Regelungen können innerhalb des Jahres 2024 im Rahmen der Zertifizierung zur Anwendung kommen, sofern diese zur Sicherstellung der Interoperabilität mit nicht-konformen Dienstanbietern notwendig sind. Die Übergangsregelungen werden regelmäßig aktualisiert.

Die Notwendigkeit der angewendeten Abweichung ist vom Antragsteller jeweils bei der Beantragung der Zertifizierung nachzuweisen.

2 Übergangsregelungen

2.1 TLS

2.1.1 Schlüssellängen in X.509-Zertifikaten

Abweichend von den Vorgaben der TR-03116-4 [2] darf ein eID-Client übergangsweise auch X.509-Zertifikate mit öffentlichen RSA-Schlüsseln mit einer der folgenden Schlüssellängen akzeptieren, falls dies zur Sicherstellung der Interoperabilität mit nicht-konformen Diensteanbietern, eID-Servern oder Remote-IFD Komponenten notwendig ist:

(2024-01.A1) Mindestens 2048 Bit.

2.2 Konformitätsprüfung

Die anzuwendenden Übergangsregelungen sind vom Antragsteller im Zertifizierungsantrag darzulegen und entsprechende Nachweise über die Notwendigkeit der Maßnahmen beizufügen.

Wird die Notwendigkeit von Abweichungen im Zertifizierungsantrag nachgewiesen, so ist dies von der Prüfstelle im Prüfbericht entsprechend zu vermerken. Die Konformitätstests sind basierend auf dem zugehörigen ICS durchzuführen.

Literaturverzeichnis

[1] BSI, „TR-01324 eID-Client - Part 2: Conformance Test Specification, Version 1.3“.

[2] BSI, „TR-03116 Kryptographische Vorgabe für Projekte der Bundesregierung - Teil 4: Kommunikationsverfahren in Anwendungen“.