Bundesverband der Deutschen Volksbanken und Raiffeisenbanken e. V.
Bundesverband deutscher Banken e. V.
Bundesverband Öffentlicher Banken Deutschlands e. V.
Deutscher Sparkassen- und Giroverband e. V.
Verband deutscher Pfandbriefbanken e. V.

Die Deutsche Kreditwirtschaft

Krypto LifeCycle EBICS

Version 1.4 vom 09.07.2025

Endfassung

Krypto LifeCycle

Die im EBICS-Verfahren zur Anwendung kommenden kryptografischen Komponenten werden unter Berücksichtigung der Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) regelmäßig überprüft und bei Bedarf an die aktuellen Sicherheitsanforderungen angepasst. Dabei ist es aber umgekehrt ebenso wichtig, ältere kryptografische Komponenten und/oder als nicht mehr angemessen sicher geltende Schlüssellängen, die von Kunden verwendet werden, nicht mehr zu unterstützen. Daher wird der für das DFÜ-Abkommen zuständige Arbeitsstab „DFÜ mit Kunden“ der Deutschen Kreditwirtschaft (kurz: Ast DFÜ) zukünftig unter Berücksichtigung angemessener Migrationsfristen in einem Krypto LifeCycle folgende Termine setzen:

1. Termin, ab wann neue oder angepasste kryptografische Komponenten und/oder Schlüssellängen bankseitig von allen Kreditinstituten zu unterstützen sind
2. Termin, ab wann bestimmte ältere kryptografische Komponenten und/oder Schlüssellängen bankseitig von Kreditinstituten nicht mehr akzeptiert werden

Der hier vorliegende initiale „Krypto LifeCycle“ umfasst die Regelungen zu unter EBICS unterstützten TLS-Versionen sowie Vorgaben zu Mindestschlüssellängen für RSA-Schlüssel über einen mittelfristigen Zeithorizont (Authentifikationssignatur, Anwendungsverschlüsselung und Elektronische Unterschrift). Dies wird laufend aktualisiert, um aktuelle Empfehlungen, so zum Beispiel des BSI, und langfristige Entwicklungen, wie zum Beispiel aus der perspektivischen Bedrohung des Quantencomputing, berücksichtigen zu können.
Weiterhin können perspektivisch auch technisch-organistorische Hilfestellungen für die Migration sicherheitstechnisch relevanter Komponenten ergänzt werden. Hierzu wird ein Austausch mit Marktteilnehmern, das heißt Zahlungsdienstleistern und Softwareherstellern, angestrebt.

Im EBICS-Verfahren zu verwendende TLS-Versionen (Transportverschlüsselung):

TLS-Version **mit den vom BSI jeweils dazu empfohlenen Ciphersuiten[1]**	**LifeCycle**
V 1.2 oder höher	
Kleiner V 1.2	Ausgelaufen seit 11/2020

[1] https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Technische-Richtlinien/TR-nach-Thema-sortiert/tr02102/tr02102_node.html

Im EBICS-Verfahren zu verwendende Mindestlängen für RSA-Schlüssel
(Authentifikationssignatur, Anwendungsverschlüsselung, Elektronische Unterschrift):

RSA-Schlüssellänge (für alle verwendeten Schlüsselpaare A00x, X00x, E00x)	LifeCycle
Mindestens 4.096 Bit	Ab 11/2027[2]
Mindestens 2.048 Bit	Läuft aus zu 11/2027
Kleiner 2.048 Bit	Ausgelaufen seit 11/2021

EBICS LifeCycle

Da kryptografische Komponenten und/oder Schlüssellängen zum Teil direkt mit einzelnen EBICS-Versionen verknüpft sind, ergeben sich aus den Vorgaben des Krypto LifeCycles Konsequenzen für den EBICS LifeCycle.

LifeCycle für EBICS-Versionen:

EBICS-Version	LifeCycle	Bemerkung
V 3.0		
V 2.5		Hier sind Schlüssellängen von mindestens 2.048 Bit erforderlich (siehe entsprechende Tabelle oben im Abschnitt Krypto LifeCycle)
V 2.4	Ausgelaufen seit 11/2023.	

[2] Für Chipkarten gilt ab November 2027 die Mindestschlüssellänge von 3.072 Bit