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

Empfehlungen zu EBICS-Sicherheitsverfahren und Schlüssellängen

Die in der EBICS-Spezifikation definierten Sicherheitsverfahren entsprechen dem aktuellen Stand von Wissenschaft und Technik und bieten ein sehr hohes Sicherheitsniveau. Dies zeigt sich u. a. darin, dass seit Einführung des EBICS-Verfahrens keine erfolgreichen Angriffe auf die EBICS-Sicherheitsverfahren bekannt sind. Gleichwohl erlaubt die EBICS-Spezifikation für die Kundenseite eine gewisse Variabilität, was z. B. Schlüssellängen und Versions-Ausprägungen der Verfahren betrifft. Es ist hier unbedingt zu empfehlen, dass Kunden bzw. Hersteller von Kundensystemen die Parameter wählen, die den Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI) entsprechen.
Folgende Empfehlungen für die EBICS-Sicherheitsverfahren entsprechen den Empfehlungen des BSI[1]:

- Verwendung von TLS 1.2 für die EBICS-Transportverschlüsselung mit den im Rahmen von TLS 1.2 unterstützten und empfohlenen[1] „Cipher-Suiten“
- Verwendung der Schlüssellänge von mindestens 2048 Bit für RSA-Schlüssel im Rahmen der EBICS-Sicherheitsverfahren Elektronische Unterschrift (A006), Authentifikationssignatur (X002) und Verschlüsselung (E002)

Die oben angeführten Schlüssellängen und Ausprägungen der EBICS-Sicherheitsverfahren sind konform zur EBICS-Versionen 2.5 und werden von allen Banken und Sparkassen in Deutschland bankseitig unterstützt. Generell ist zu empfehlen, die EBICS-Version 2.5 und keine älteren EBICS-Versionen zu nutzen.

Sofern Kunden nicht bereits die oben angeführten Schlüssellängen und Verfahrensausprägungen mit der EBICS-Version 2.5 nutzen, ist ein entsprechendes Update der EBICS-Kundensoftware zu empfehlen, ggf. sollten Firmenkunden hierzu den Hersteller ihres Softwareproduktes ansprechen.

In der EBICS-Version 3.0 sind die oben angeführten Schlüssellängen und Ausprägungen der EBICS-Sicherheitsverfahren die Mindestanforderungen. Folglich ist die Verwendung der Versionen A004 (hier: feste Schlüssellänge 1024 Bit) ab EBICS V3.0 technisch gar nicht mehr möglich und ein entsprechendes Update wird mit Wechsel auf EBICS V 3.0 unumgänglich.

Es ist insgesamt zu empfehlen, die oben angeführten Schlüssellängen und Verfahrensausprägungen bereits in der EBICS Version 2.5 zu verwenden. Insbesondere raten wir, gemäß BSI-Empfehlungen direkt auf die Unterschriftsversion A006 zu wechseln, auch wenn A005 die empfohlene Mindestschlüssellänge ebenfalls unterstützen könnte.

---

[1] Die Empfehlungen des BSI sind unter folgender URL veröffentlicht:
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_htm.html

- BSI TR-02102 Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Version 2018-02
- TR-02102-2, Kryptographische Verfahren: Empfehlungen und Schlüssellängen, Teil 2 – Verwendung von Transport Layer Security (TLS), Version 2018-01