

Anlage 2 zu den

Besondere Bedingungen der Deutschen Bundesbank für die Datenfernübertragung via EBICS für sonstige Kontoinhaber ohne Bankleitzahl (EBICS-Bedingungen)

(Sicherheitsanforderungen an das EBICS-Kundensystem)

Stand: 14. September 2019

(Keine inhaltlichen Änderungen ggü. 18. November 2018,
sondern Anpassung des Dokumentenstands an den der EBICS-Bedingungen nebst Anlage 1)

Sicherheitsanforderungen an das EBICS-Kundensystem

Über die in Anlage 1 beschriebenen Sicherheitsmaßnahmen hinaus sind durch den Kunden folgende Anforderungen zu berücksichtigen:

- Die vom Kunden für das EBICS-Verfahren eingesetzte Software muss die in Anlage 1 beschriebenen Anforderungen erfüllen.
- EBICS-Kundensysteme dürfen nicht ohne Firewall eingesetzt werden. Eine Firewall ist eine Einrichtung, die den gesamten ein- und ausgehenden Nachrichtenverkehr überwacht und nur bekannte oder autorisierte Verbindungen zulässt.
- Es ist ein Virenschanner zu installieren, der regelmäßig mit den neuesten Virendefinitionsdateien auszustatten ist.
- Das EBICS-Kundensystem ist so einzurichten, dass sich der EBICS-Teilnehmer vor dessen Nutzung anmelden muss. Die Anmeldung hat als normaler Benutzer und nicht als Administrator, der z. B. berechtigt ist, die Installation von Programmen vorzunehmen, zu erfolgen.
- Die internen IT-Kommunikationswege für unverschlüsselte bankfachliche Daten oder für unverschlüsselte EBICS-Nachrichten sind gegen Abhören und Manipulationen zu schützen.
- Wenn sicherheitsrelevante Updates für das jeweils eingesetzte Betriebssystem und weiterer installierter sicherheitsrelevanter Software-Programme vorliegen, sollten die eingesetzten EBICS-Kundensysteme mit diesen aktualisiert werden.
- Entsprechend einer Empfehlung des Bundesamtes für Sicherheit in der Informationstechnik (BSI)¹ ist zu verwenden:
 - a) ausschließlich die aktuelle Verschlüsselungsversion TLS 1.2 mit den im Rahmen von TLS 1.2 unterstützten und empfohlenen „Cipher-Suiten“,
 - b) eine Schlüssellänge von mindestens 2048 Bit für RSA-Schlüssel im Rahmen der EBICS-Sicherheitsverfahren Elektronische Unterschrift (A006), Authentifikationssignatur (X002) und Verschlüsselung (E002)
 - c) Version A006 für die Elektronische Unterschrift mit mindestens 2048 Bit Schlüssellänge (s. oben) für die Elektronische Unterschrift.

Ferner sind die von der Deutschen Kreditwirtschaft herausgegebenen EBICS-Sicherheitsempfehlungen für Firmenkunden zu beachten. Auf Änderungen wird die Deutsche Bundesbank schriftlich oder auf elektronischem Wege hinweisen. Des Weiteren können die vorgenannten EBICS-Sicherheitsempfehlungen über den zuständigen Kundenbetreuungs-service angefordert werden.

Die Umsetzung dieser Anforderungen liegt ausschließlich in der Verantwortung des Kunden.

¹ BSI TR-02102-2 (https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr02102/index_html.html)