

## Zusammenfassung der Sicherheitsuntersuchung zum System MCFT\_3DES der debis IT Security Services vom 22.12.1998

Das System MCFT\_3DES (MultiCash File Transfer – TripleDES Version 01/1999) der Firma Omikron dient der sicheren Kommunikation und Zahlungsverkehrsabwicklung zwischen Kunden und Bank via Internet.

MCFT\_3DES ist der Nachfolger des Systems MC-DFÜ, welches bereits einer Begutachtung durch die Firma debis IT Security Services unterzogen wurde. Dabei wurden einige Schwachstellen identifiziert, die durch das System MCFT\_3DES behoben werden sollen, und entsprechende Änderungen empfohlen.

Bei den empfohlenen Änderungen handelte es sich um

- die Ersetzung des einfachen DES-Algorithmus durch den Triple-DES-Algorithmus,
- die Ersetzung des schwachen MSR-Encryption-Verfahrens durch einen stärkeren Algorithmus (z.B. Triple-DES) und
- die Verwendung des Diffie-Hellmann-Verfahrens mit größeren Parametern.

Grundlage der Sicherheitsuntersuchung des neuen Systems MCFT\_3DES war die von der Firma Omikron erstellte Dokumentation „Functional Description of the MultiCash File Transfer Protocol – TripleDES Version 01/1999 (MCFT\_3DES)“, das „Sicherheitsgutachten zum System MC-DFÜ“ von debis IT Security Services sowie die Ergebnisse der „Sicherheitsuntersuchung der SCORE-Software der Firma Concord-Eracam“ von debis Systemhaus GEI. (Die SCORE-Software dient der Realisierung von Teilfunktionen des Systems MCFT\_3DES.)

Der Quellcode von MCFT\_3DES wurde im Rahmen der Sicherheitsuntersuchung nicht begutachtet.

Die Sicherheitsuntersuchung der MCFT\_3DES wurde bezüglich der Sicherheitsdienste

- **Vertraulichkeit** von Nachrichten und gespeicherten Daten,
- **Integrität** von Nachrichten,
- **Authentizität** von Nachrichten und
- **Non-Repudiation** („Proof of Origin“, „Proof of Delivery“)

durchgeführt.

Der Dienst **Vertraulichkeit** soll die zwischen Bank und Kunde ausgetauschten Nachrichten wie Zahlungsanweisungen, Kontoinformationen etc. vor Kenntnisnahme durch Dritte schützen.

Durch den Dienst **Integrität** von Nachrichten wird für den Empfänger einer Nachricht überprüfbar, ob diese während der Übertragung vom Sender zum Empfänger verändert wurden.

Der Dienst **Authentizität** von Nachrichten dient dem Nachweis gegenüber dem Empfänger, dass eine Nachricht wirklich von dem angegebenen Absender stammt und während der Übertragung nicht verändert wurde.

Durch den **Non-Repudiation** Dienst ist gegenüber Dritten nachweisbar, dass eine bestimmte Nachricht vom betreffenden Absender gesendet („Proof of Origin“) und/oder vom betreffenden Empfänger empfangen („Proof of Delivery“) wurde. Durch einen derartigen Nachweis ist es nicht möglich, dass die betreffenden Kommunikationspartner ihre Beteiligung an der Kommunikation leugnen können.

Zur Realisierung dieser Sicherheitsuntersuchung wurden die im System MCFT-3DES zur Realisierung der genannten Sicherheitsdienste eingesetzten Sicherheitsmechanismen identifiziert, untersucht und bewertet. Die zugrunde liegenden kryptographischen Algorithmen und Sicherheitsfunktionen sowie die Anwendungsprotokolle wurden ebenfalls analysiert.

Die Untersuchung erfolgte unter der Prämisse, dass Kundenvertragsbedingungen eingesetzt und eingehalten werden, um den Kunden auf seine Verantwortlichkeiten für

- die angemessene Handhabung der PINs (Geheimhaltung, Mindestlänge etc.), der einzugebenden Zufallswerte und der BPD-Diskette,
- die Integrität der eingesetzten MCFT\_3DES-Software auf seinem Rechner und
- das Verhindern unautorisierter Prozesse (z.B. Viren) auf seinem Rechner

zu verpflichten, und in welchen das Verfahren zur Reaktivierung blockierter Benutzer vereinbart wird (vgl. nachfolgende Empfehlung).

Die Sicherheitsmechanismen auf der Bankseite, die zur Sicherung der sensitiven Kunden- und Anwendungsdaten eingesetzt werden, waren nicht Gegenstand der vorliegenden Untersuchung. Es wird die Realisierung geeigneter Mechanismen in Verantwortung der Bank vorausgesetzt.

### ERGEBNIS

**Die im MCFT\_3DES System konzipierten Maßnahmen und Mechanismen sowie ihre Umsetzung sind nach dem heutigen Wissensstand geeignet, um die angestrebten Sicherheitsdienste zu realisieren.**

**Durch das System MCFT\_3DES kann auch dem heutigen Stand der Technik und unter Beachtung der zu erwartenden Entwicklung ein hinreichend hohes Sicherheitsniveau erreicht werden, wenn**

- **die Kundenvertragsbedingungen eingehalten werden,**
- **bankseitig geeignete Sicherheitsmechanismen zum Schutz sensitiver Kunden- und Anwendungsdaten Verwendung finden und**
- **eine korrekte Umsetzung des Konzepts unter Berücksichtigung sicherheitstechnischer Aspekte erfolgt.**

**Im System MCFT\_3DES wurden alle von debis IT Security Services empfohlenen Änderungen am System MC-DFÜ berücksichtigt.**

Unter Einhaltung der Kundenvertragsbedingungen und bei Einsatz geeigneter bankseitiger Sicherheitsmechanismen gilt für die Sicherheitsdienste im Einzelnen:

Durch den Mechanismus der elektronischen Signatur (RSA-Verfahren mit Hashfunktion RIPEMD-160) können entsprechend dem derzeitigen Stand der Technik

- **Integrität von Nachrichten** vom Kunden zur Bank,
- **Authentizität von Nachrichten** vom Kunden zur Bank und
- **Non-Repudiation** im Sinne eines „Proof of Origin“ für Nachrichten vom Kunden zur Bank

auf einem hinreichend hohen Niveau gewährleistet werden.

Insbesondere kann durch die digitale Signatur gewährleistet werden, dass Zahlungsverkehrsdaten manipulationsgeschützt und nur vom autorisierten Kunden an die Bank übertragen werden können.

Der Sicherheitsdienst **Vertraulichkeit** kann für alle **übertragenen Nachrichten** und die **DFÜ-PIN** des Kunden durch Triple-DES Verschlüsselung auf Basis von Sessionkeys (vereinbart mittels Diffie-Hellman-Verfahren) in allen Dialogen auf hinreichend hohem Niveau gewährleistet werden.

Die **Vertraulichkeit von gespeicherten sensiblen Daten** beim Kunden ist nach dem heutigen Standard der Technik aufgrund der Triple-DES Verschlüsselung unter Verwendung jederzeit änderbarer PINs als hinreichend sicher anzusehen.

## **EMPFEHLUNGEN**

Um eine optimale Sicherheit des MCFT\_3DES Systems zu erzielen, sollen die folgenden Empfehlungen eingehalten werden:

1. Das Widerfreischalten eines Kunden sollte immer durch die Ausgabe einer neuen BPD-Datei und einer neuen **Start-PIN** erfolgen und nicht per Fax.
2. Bankseitig sollte ein Vergleich aller Bytes des aus dem elektronisch übermittelten öffentlichen RSA-Teilnehmerschlüssel berechneten Hashwerte und des in Papierform übermittelten Hashwertes durchgeführt werden.

Die Auswahl des Verfahrens für das Widerfreischalten liegt in der Verantwortung der Bank und muss mit dem Kunden in den Kundenvertragsbedingungen entsprechend vereinbart werden.