

ZENTRALER KREDITAUSSCHUSS

MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN · BUNDESVERBAND DEUTSCHER BANKEN E.V. BERLIN
BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E.V. BERLIN · DEUTSCHER SPARKASSEN- UND GIROVERBAND E.V. BERLIN-BONN
VERBAND DEUTSCHER PFANDBRIEFBANKEN E.V. BERLIN

Utimaco Safeware AG
Herr Rainer Herbertz
Hohemarkstraße 22
61440 Oberursel

EINGEGANGEN

20. Nov. 2006

10785 Berlin, 17. November 2006
Lennéstraße 11
AP - AZ: utim-001-SB

electronic cash-System

hier: Sicherheitsuntersuchung der Hardware der S-Box „CryptoServer CS“

Sehr geehrter Herr Herbertz,

durch den Gutachter T-Systems GEI GmbH wurden am 31. Oktober 2006 im Arbeitsstab „Sicherheitsfragen“ im Zentralen Kreditausschuss (ZKA) die Ergebnisse der „Teilkomponente: Sicherheitsuntersuchung der Hardware sowie der Firmware des CryptoServer CS der Utimaco Safeware AG“ vom 13. Oktober 2006 vorgestellt.

Das Gutachten ist durch den Arbeitsstab Sicherheitsfragen zur Kenntnis genommen worden.

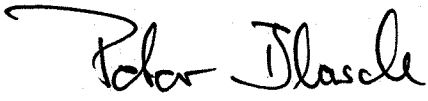
Wir können Ihnen mitteilen, dass als Voraussetzung für den Einsatz der überprüften Hardware der Sicherheitsbox „CryptoServer CS“ (HW-Version: CryptoServer CS, Version: 2.0.2.0 vom 10.03.2006) Folgendes sicherzustellen ist:


- Die SBox darf nur in einer sicheren Umgebung betrieben werden.
- Es darf nur die abgenommene Software in die SBox eingebracht werden. In Netzbetrieben darf ausschließlich das Master-Profil NET zum Einsatz kommen.
- Ein nachträglich unautorisiertes Einspielen von Software in die SBox muss ausgeschlossen sein.
- Die Transportschlüsselhälften sind in getrennten Tresoren bzw. Tresorfächern aufzubewahren.
- Das PIN-Pad zur Eingabe der Schlüssel muss verschlossen in einem der Tresore des Netzbetreibers aufbewahrt werden.
- Die Schlüsseltabellen müssen gelöscht werden, wenn die SBox zur Reparatur oder Wartung aus der sicheren Umgebung entfernt wird.
- Die SBox muss in einem eigenen Netzsegment betrieben werden.

Voraussetzung für die Erteilung einer Zulassung Ihrer S-Box in Netzbetrieben des Zahlungssystems electronic cash ist die Vorlage und positive Bewertung einer Sicherheitsuntersuchung der Anwendung nebst Integration, die seitens des Netzbetreibers bereitgestellt werden muss.

Für das oben genannte S-Box-Gutachten wurde im ZKA-Zulassungsverfahren die Nummer 1958 vergeben.

Mit freundlichen Grüßen
Für den
ZENTRALEN KREDITAUSSCHUSS
Bundesverband Öffentlicher
Banken Deutschlands e. V.


(Blasche)


(Pohl)