
Technische Daten

ArmorToken™



Datensicherheit Made in Germany

(Abbildung in Originalgröße)

ArmorSolutions

Mühlweg 5 • D-82008 Unterhaching
Telefon: +49 89 82079792 • Fax: +49 89 82079793
Internet: www.armorsolutions.de
E-Mail: info@armorsolutions.de

Ing.-Büro Hermann Ullenboom

Technische Daten:

1. ArmorToken
 - USB-Token mit Buchsen für Smart Card und Micro-SD Flash Speicher
 2. Smart Card
 - Java Card 2.2.2, Certification & Approvals: EMVCo (HW approval); Common Criteria (EAL) 5+
 3. Micro-SD Flash Speicher
 - Optional in ArmorToken einzustecken, bis 32 GB
 4. Sicherheitsschlüssel (ECC)
 - Schlüssel auf der Smart Card nach dem Verfahren der Elliptische-Kurven-Kryptographie ECC-256 Bit
Entspricht dem Sicherheitslevel RSA-15360 Bit, üblich sind RSA-1024 oder RSA-2048 Bit
 - Verwendet zur Benutzer-Authentisierung und zur Bildung der AES-Dateischlüssel
 5. Dateischlüssel (AES)
 - AES-256 Bit, für jede Datei wird ein anderer Schlüssel verwendet
 - Der AES Schlüssel wird mit Hilfe des Sicherheitsschlüssels (ECC) gebildet.
 - Das AES-256 Bit-Verfahren wird vom Bundesamt für Sicherheit in der Informationstechnik empfohlen.
 6. Schlüsselsicherheit, Backdoor Möglichkeit
 - Die AES Dateischlüssel verlassen niemals die Smart Card.
 - Es besteht keine Backdoor Möglichkeit, das bedeutet, auch der Hersteller hat keine Möglichkeit, irgendwelche Schlüssel auszulesen oder wiederherzustellen.
 7. Smart Card Applets
 - Bei der Smart Card handelt es sich um eine zertifizierte Java Card. Neben den schon gespeicherten Applets für die Schlüsselverwaltung und das Ver-/Entschlüsseln können weitere z.B. firmenspezifische Applets geladen werden.
 8. PC-Anwendung ArmorToken Admin
 - Anwendung für den Endbenutzer oder als Service vom Lieferanten.
 - Personalisieren der ArmorToken durch den Endbenutzer oder als Service durch den Lieferanten.
 - PC-Anwendung ist lauffähig auf den Betriebssystemen Windows, Mac-OS X, Linux.
 9. PC-Anwendung ArmorToken
 - Anwendung für den Endbenutzer zum Ver- und Entschlüsseln von beliebigen Dateien unter Verwendung eines ArmorToken mit zugehöriger PIN.
 - Änderung der persönlichen PIN des ArmorToken.
 - PC-Anwendung ist lauffähig auf den Betriebssystemen Windows, Mac-OS X, Linux.
-