Produktinformation ArmorToken™

1 Anwendungshinweise

Allen Personen (z.B. Unternehmen, Kanzleien aber auch Privatpersonen), die höchste IT-Datensicherheit bei einfacher Anwendung verlangen, bietet der neuartige ArmorToken™ der Firma ArmorSolutions die richtige und kostengünstige Lösung.

Es handelt sich dabei um ein USB-Token mit einer Smart Card (vergleichbar dem Chip auf einer Bankkarte), in dem ein Sicherheitsschlüssel (ECC) gespeichert ist.

Mit seiner Hilfe werden die sensiblen Daten eines Unternehmens wirkungsvoll vor unerlaubtem Zugang sowohl von außen als auch durch unberechtigte Mitarbeiter geschützt.

Zum Verschlüsseln von beliebigen Dateien wird der ArmorToken™ in den USB-Anschluss des PC gesteckt. Nach Eingabe der zum ArmorToken™ gehörigen individuellen PIN verschlüsselt die mitgelieferte PC-Anwendung ArmorToken™ die ausgewählten Dateien. Jede Datei wird dabei mit einem anderen Schlüssel (AES) verschlüsselt. Der Vorgang ist sehr einfach mit Hilfe des Kontextmenüs oder durch Drag&Drop durchzuführen.

Die verschlüsselten Dateien können sich auf allen üblichen Speichermedien befinden (lokaler PC, Server, Cloud, USB-Flash etc.) und lassen sich auch als E-Mail Anhang versenden.

Eine sichere Datenspeicherung (z.B. bei Dienstreise oder Kundenbesuch) ist auch im ArmorToken™ selbst möglich durch den Einsatz eines optionalen Micro-SD Flash Speichers bis 32 GB.

Die Speicherung des Sicherheitsschlüssels auf einen ArmorToken™, die Personalisierung, kann vom Kunden selbst durchgeführt werden. Er verwendet dazu die mitgelieferte PC-Anwendung ArmorToken Admin. Dabei lassen sich Benutzergruppen in einer frei wählbaren, individuellen Hierarchie (vergleichbar einem Gebäude-Schlüsselmanagement) einrichten und damit gegeneinander geschützte Gruppen definieren.

Durch die 2-Faktor-Authentisierung (ArmorToken™ plus PIN), die Verwendung hochsicherer Kryptologieverfahren (ECC, AES), die Anwendung auf alle Dateiarten und Speicherorte sowie die leichte Bedienbarkeit ist mit dem ArmorToken™ ein Produkt verfügbar, das hinsichtlich der Sicherheit und Bedienbarkeit höchsten Ansprüchen genügt.

Beim Kauf mindestens eines ArmorToken™ werden die PC-Anwendungen ArmorToken Admin und ArmorToken kostenlos mitgeliefert.

Unser Motto:

ArmorToken™: Datensicherheit immer dabei

2 FAQ – Häufig gestellte Fragen

2.1 Warum bleibt der PC beim Hochfahren hängen?

Verhalten: Nach dem Starten des PC bleibt dieser hängen, der Bildschirm bleibt schwarz.

Ursache: Ein ArmorToken™ ist eingesteckt und auf diesen greift die PC-SW als erstes zu.

Abhilfe: ArmorToken™ ausstecken und erneut hochfahren und dann erst ArmorToken™ einstecken.

2.2 Warum zählt der PIN-Versuchszähler herunter?

Verhalten: Nach Eingabe und Bestätigen der PIN zählt der PIN-Zähler herunter.

Ursache: Falsche PIN-Eingabe.

Abhilfe:

1. Überprüfen Sie, ob die Shift-Lock-Taste gedrückt ist
2. Vergewissern Sie sich, dass die PIN zu dem eingesteckten ArmorToken™ passt.
3. Verwechseln Sie nicht die PIN mit dem Kennwort.
   Bei Verwendung eines Root-Token zum Rücksetzen einer gesperrten PIN von einem Benutzer-Token wird die **PIN** des Root-Token (nicht das Kennwort) benötigt!

Sie können Ihre PIN in einem Texteditor eingeben und mit Copy-Paste in das Feld für die PIN-Eingabe kopieren. Damit haben Sie die vollständige Kontrolle über Ihre Eingabe.

Bitte denken Sie daran, die PIN aus dem Editor wieder zu löschen!

2.3 Wie viele Hierarchiestufen kann ich einrichten?

Mit jeder tieferen Hierarchiestufe, die mit der PC-Anwendung ArmorToken Admin eingerichtet und für die ein Benutzer personalisiert wird, wird ein Schlüsselpaar auf der SmartCard gespeichert. Da dieser Speicher begrenzt ist, gibt es tatsächlich eine maximale Anzahl der Hierarchiestufen. Sie wird in der Praxis mit Sicherheit nicht erreicht werden, da sie über 100 liegt.

2.4 Warum kommt die Meldung „ArmorToken: Token einstecken“?

Verhalten: Beim Start des Vorgangs *Verschlüsseln* oder *Entschlüsseln* kommt die Meldung:

ArmorToken: Token einstecken

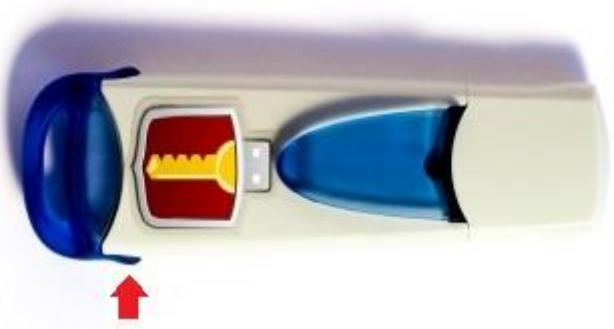
Ursache: ArmorToken™ ist nicht gesteckt, wird nicht erkannt oder die PIN ist gesperrt.

Abhilfe:

1. Überprüfen Sie, ob überhaupt ein ArmorToken™ in einem PC-USB-Steckplatz steckt, evtl. vermeiden Sie einen USB-HUB.
2. Schließen Sie die PC-Anwendung ArmorToken, ziehen Sie den ArmorToken™, starten Sie wieder die Anwendung und stecken den ArmorToken™ erneut. Diesen Vorgang sollten Sie auf jeden Fall ausführen wenn Sie einen anderen ArmorToken™ verwenden wollen.
3. Lassen Sie vom Administrator (Geschäftsführer) die PIN rücksetzen.
4. Prüfen Sie, ob der PC-USB-Eingang am PC funktioniert.
   Wenn Sie den Steckplatz im USB-Token für einen Flash-Speicher bestückt haben, sollte z.B. bei Windows ein Explorer für dieses Laufwerk automatisch öffnen.

2.5 Wie setzt man einen Micro-SD Flash Speicher ein?

Um einen Micro-SD Flash Speicher einzustecken müssen Sie die blauen Verschlusskappe öffnen. Dazu drücken Sie die blaue Verschlusskappe an einer Seite z.B. mit dem Fingernagel ein (siehe roten Pfeil) und ziehen nun die Verschlusskappe **einseitig** ein wenig heraus.



Die Halterung auf der anderen Seite löst sich jetzt leicht. Ziehen Sie die Verschlusskappe nur soweit aus dem USB-Token, wie es das schmale Halteband zulässt.

Zum Einsatz einer MicroSD Karte drehen Sie den USB-Token auf die andere Seite und führen die MicroSD Karte ein.
Dann schieben Sie die Verschlusskappe wieder in den USB-Token.

3 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-2048 oder RSA-4096 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.
6. Schlüsselsicherheit, Backdoor Möglichkeit
   - Es besteht keine Backdoor Möglichkeit, das bedeutet, weder Kunde noch Hersteller haben die Möglichkeit, irgendwelche Schlüssel auszulesen oder wiederherzustellen. Es besteht also keine Möglichkeit, die Herausgabe der Schlüssel zu erzwingen.
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 (VolksToken).
   - 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.

4 Stichworte

4.1 Gruppenhierarchie

Mit Hilfe der leicht zu bedienenden mitgelieferten PC-Anwendung ArmorToken Admin werden in einer Datenbank Berechtigungsgruppen in einer Gruppenhierarchie eingerichtet. So können kritische Sicherheitsbereiche wirkungsvoll gegen Ausspähen auch durch nicht berechtigte eigene Mitarbeiter abgesichert werden. Die höchste Hierarchiegruppe, die der Geschäftsführer, ist z.B. gegen alle anderen Gruppen wirkungsvoll geschützt. In der nächst tieferen Hierarchieebene könnten z.B. die Finanz- und die Personalabteilung sowie die Administration eigene Gruppen darstellen.
Grundsätzlich kann eine übergeordnete Gruppe die Dateien aller Untergruppen lesen. Die Geschäftsführung hat damit Zugang zu allen verschlüsselten Dateien.
Mitglieder einer Gruppe erhalten denselben Sicherheitsschlüssel und können nur deren Dateien uneingeschränkt lesen und bearbeiten.

4.2 Personalisierung

Vor der Verwendung eines ArmorToken™ wird er mit Hilfe der PC-Anwendung ArmorToken Admin und der erstellten Datenbank vom Kunden selber personalisiert.
Er kann auch vom Lieferanten als fertig einsetzbarer VolksToken bezogen werden.

4.3 Ver- und Entschlüsseln

Nach Einstecken eines ArmorToken™, Eingabe der persönlichen PIN und unter Verwendung der mitgelieferten PC-Anwendung ArmorToken können Dateien beliebiger Größe und Art ver- und entschlüsselt werden. Es können auch Verzeichnisse ausgewählt werden, dann werden die Dateien sämtlicher Unterverzeichnisse ebenfalls abgearbeitet.
Der Vorgang kann auf einfache Weise mit Hilfe des Kontextmenüs, per Drag&Drop und auch per Menü gestartet werden.

4.4 Dateinamen

Alle verschlüsselten Dateien behalten ihren Namen, es wird lediglich die Endung „.ate“ angefügt.
Die Größe der zu verschlüsselnden Dateien ist nicht begrenzt.

4.5 PIN-Falscheingabe

Nach 3-maliger PIN Falscheingabe wird der ArmorToken™ gesperrt.
Er kann dann mit Hilfe eines ArmorToken™ irgendeiner höheren Hierarchiegruppe unter Verwendung der PC-Anwendung ArmorToken Admin wieder entsperrt werden.

4.6 Diebstahl

Der Diebstahl eines ArmorToken™ allein bedeutet kein Sicherheitsproblem. Dem Dieb müsste dazu noch die PIN bekannt sein. Nach 3-maliger Falscheingabe wird der ArmorToken™ gesperrt. Die PIN kann vom Benutzer jederzeit geändert werden.

4.7 Totalverlust von Daten

Bei einer verschlüsselten Festplatte besteht die Gefahr des Totalverlustes. Diese Gefahr ist bei unserem Verfahren, jede Datei einzeln zu verschlüsseln, deutlich geringer.

4.8 2-Faktor-Authentisierung

Bedeutet „Haben“ (ArmorToken™) plus „Wissen“ (persönliche PIN).
Der Verlust nur eines der Teile führt noch zu keinem Sicherheitsproblem.

4.9 Backdoor

Unter Backdoor versteht man die Möglichkeit, ein Sicherheitssystem durch eine geheime Hintertüre zu umgehen. Bei einem ArmorToken™ besteht keine Backdoor Möglichkeit. Das bedeutet, dass keiner, weder der Kunde noch der Hersteller, die Möglichkeit hat, irgendwelche Schlüssel auszulesen oder wiederherzustellen. Die Herausgabe der Schlüssel kann auch nicht erpresst oder erzwungen werden.