

# CRYPTOCard-Lösungen für VPNs

Mobile Anwender benötigen ein virtuelles privates Netzwerk (VPN), um auf Netzwerkressourcen und -dienste zuzugreifen. Wird Ihr VPN nur durch eine typische Passwortauthentifizierung geschützt, ist es jedoch nicht wirklich privat. Schützen Sie Ihr Unternehmen durch die sichere Zwei-Faktor-Authentifizierung mit der preisgekrönten Technologie von CRYPTOCard. Dank Passwörtern, die bei jeder Anmeldung neu erzeugt werden, entsteht eine sichere VPN-Verbindung.



## VPNs schützen wichtige Daten

Virtuelle private Netzwerke erlauben Unternehmen, von den Kostenvorteilen und grenzenlosen Möglichkeiten des Internets zu profitieren, indem sie Angestellten und Geschäftspartnern Zugriff auf vertrauliche Unternehmensdaten, -ressourcen und geschützte Anwendungen geben. VPNs schützen die Integrität der Datenübertragung; sie prüfen jedoch die Identität des Endbenutzers nicht genau. CRYPTO-Server stellt eine leistungsstarke Endbenutzer-Authentifizierungslösung bereit.

## Benutzerauthentifizierung – das schwächste Glied in der VPN-Sicherheit

VPNs authentifizieren Benutzer in der Regel mit einem statischen Benutzernamen und Passwort. Dieses Vorgehen bietet nur geringfügige Sicherheit, da Passwörter einfach geknackt werden können. Diese unzulänglichen Sicherheitsmethoden werden aus zwei Gründen verwendet: Kosten und Einfachheit. IT-Administratoren riskieren jeden Tag bewusst die Sicherheit ihres Netzwerks zugunsten einer Lösung, die billig und einfach

zu verwenden ist und deren Support-Kosten möglichst gering sind.

## Kosten der Sicherheit

Werden die Support-Kosten jedoch tatsächlich reduziert? Gemäß der GIGA Group beziehen sich über 30 % der Helpdesk-Anrufe auf Passwörter. Benutzer verlieren oder vergessen Passwörter, oder sie vergessen, die Passwörter zu ändern usw.

## Sichere Authentifizierung mit CRYPTOCard

Die preisgekrönte Technologie von CRYPTOCard verwendet Einmal-Passwörter, die über einen portablen Authentifizierungstoken generiert werden, der in verschiedenen Formaten erhältlich ist. So wird die Sicherheit erhöht und die Anzahl der Helpdesk-Anrufe verringert. Die statischen Passwörter, die so einfach zu knacken und zu vergessen sind, werden durch die vom CRYPTOCard-Token generierten Einmal-Passwörter ersetzt. Kombiniert mit einer einfachen PIN bietet dies eine sichere Authentifizierung.

## FUNKTIONEN UND VORTEILE

- Sichere VPNs mit der preisgekrönten Zwei-Faktor-Authentifizierung
- Bedeutend weniger Helpdesk-Anrufe dank der Eliminierung statischer Passwörter
- CRYPTO-Server kann in jedes VPN oder Netzwerkgerät integriert werden, das RADIUS unterstützt
- Tokens in verschiedenen Formaten für die unterschiedlichen Anforderungen einzelner Unternehmen

## Funktionsweise

Mit Ihrem VPN-Gerät wird ein verschlüsselter Tunnel zwischen der Host- und der VPN-Anwendung erstellt. Es kann den Zugriff auf LAN-Ressourcen steuern und aufgrund der Authentifizierungsinformationen, wie Benutzername und Passwort, lokale IP-Adressen zuweisen. Bei der Verwendung von CRYPTO-Server werden die statischen Passwörter über das VPN-Gerät durch eine sichere Zwei-Faktor-Authentifikation ersetzt. CRYPTO-Server verhindert so die Verwendung von verlorenen, gestohlenen oder einfach zu erratenden Passwörtern.

1. Der Benutzer erstellt über den VPN-Client eine Verbindung zum internen Netzwerk und verwendet den Anmeldenamen, die persönliche PIN sowie das mit dem CRYPTOCARD-Token generierte Einmal-Passwort.
2. Das VPN-Gerät gibt die Authentifizierungsinformationen (via RADIUS-Protokoll) an den CRYPTO-Server weiter.
3. Der Benutzername und das Passwort werden vom CRYPTO-Server authentifiziert und eine Access-Accept-Meldung wird an das VPN-Gerät zurückgegeben, wodurch der Benutzer Zugriff auf das Netzwerk erhält. CRYPTO-Shield enthält auch ein clientseitiges Plugin für verschiedene VPN-Client-Softwarepakete, das den Authentifizierungs- und Anmeldevorgang für Benutzer bei Verwendung der CRYPTOCARD ST-1-Software, einer CRYPTOCARD SC-1 Smart Card oder eines CRYPTOCARD UB-1 USB-Tokens automatisiert.

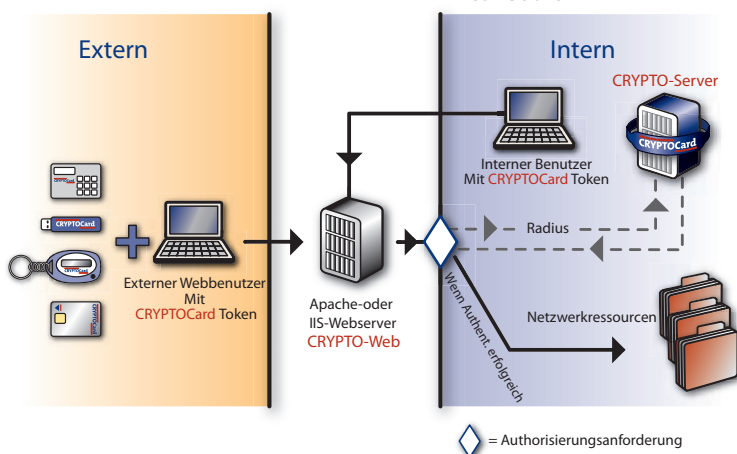
## Voraussetzungen

- CRYPTO-Server 6.x, einschließlich
- CRYPTO-Protocol Server-Modul.
  - RADIUS-Server: Der VPN Concentrator kann so konfiguriert werden, dass er die RADIUS-Server-Einrichtung des CRYPTO-Protocol Server-Moduls verwendet, das mit CRYPTO-Shield geliefert wird, oder er kann für die Verwendung des RADIUS-Servers eines Drittanbieters, wie Cisco Secure ACS, Funk Steel-Belted RADIUS oder IAS, konfiguriert werden. RADIUS-Server von Drittanbietern müssen fähig sein, für Anfragen an den RADIUS-Server im CRYPTO-Protocol Server-Modul die Proxyfunktion zu übernehmen.
  - CRYPTOCARD-Benutzerkonto und -Token: Damit sich ein Benutzer für das VPN-Gerät authentifizieren kann, muss er über ein Benutzerkonto auf dem CRYPTO-Server verfügen und es muss ihm ein Token zugewiesen sein.
  - VPN-Clientanwendung: Die VPN-Clientanwendungssoftware kann wahlweise auf dem Benutzercomputer installiert werden.

## Nahtlose VPN-Integration

Das CRYPTO-Shield-Netzwerkgerät von CRYPTOCARD kann in jedes VPN integriert werden, dass RADIUS unterstützt, einschließlich Lösungen von:

- Cisco
- Nortel
- Checkpoint
- Juniper
- WatchGuard
- SonicWave
- AEP
- Whale
- F5



### CRYPTOCARD North America

340 March Road  
Suite 600  
Ottawa, Ontario  
K2K 2E4 Canada

Toll Free: 800-307-7042  
Tel: +1-613-599-2441  
Fax: +1-613-599-2442  
E-mail: info@cryptocard.com

[www.cryptocard.com](http://www.cryptocard.com)

### CRYPTOCARD Europe

Eden Park, Ham Green  
Bristol BS20 0EB,  
United Kingdom

Tel: +44 870 7077 700  
Fax: +44 870 7077 711  
E-mail: info@cryptocard.com

[www.cryptocard.co.uk](http://www.cryptocard.co.uk)

CRYPTOCARD und CRYPTO-Server sind eingetragene Marken oder Marken von CRYPTOCARD Inc. in Kanada, den USA und/oder anderen Ländern. Microsoft und Windows sind eingetragene Marken oder Marken der Microsoft Corporation in den USA und/oder anderen Ländern. Alle anderen genannten Marken sind das Eigentum der jeweiligen Unternehmen. © 2006 CRYPTOCARD Inc. Alle Rechte vorbehalten

20061212