COLUMBITECH

Columbitech Mobile VPN – CJIS-compliant mobile access for smartphones and tablets

Mobile Security in Public Safety

FIPS VALIDATED 140-2 ™

ADVANCED AUTHENTICATION CJIS BE COMPLIANT

Mobile Security in Public Safety

Columbitech Mobile VPN – CJIS-compliant mobile access for smartphones and tablets

911 calls
Warrants
Vehicle registration
Driver's license information
Surveillance cameras
Streaming video
Fire hydrants maps
Hazmat maps

FIPS 140-2 Inside

** The Columbitech FIPS 140-2 certificate can be found on the NIST website under certificate number #307.*

Thanks to powerful smartphones and tablets, first responders are no longer tethered to their vehicles to access criminal history, vehicle registration records and dispatch information. Mobile technologies put mission-critical information at their finger tips, helping them to fight crimes and save lives while staying safe and alert.

Potential but more risk

However, these new technologies expose the information systems to new security threats. The FBI Criminal Justice Information Services Policy and the Health Insurance Portability and Accountability Act (HIPAA) address these threats and call for the use of FIPS 140-2-validated encryption for wirelessly transmitted data and advanced two-factor authentication.

Public safety agencies are facing the challenge of securing a diverse range of computing devices with an increased pressure to support the bring-your-own-device trend.

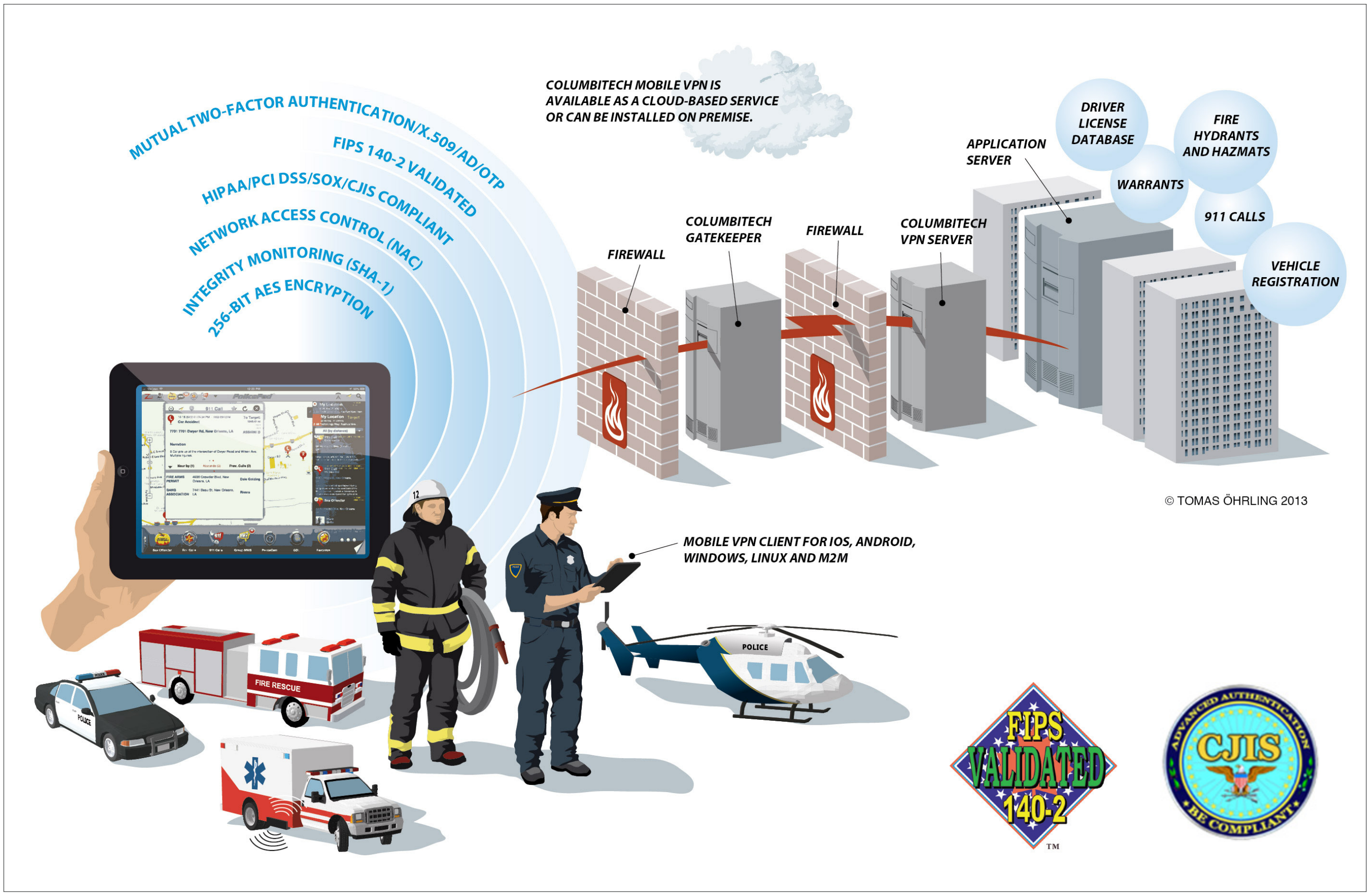
FIPS 140-2 validation and CJIS-compliant

Columbitech Mobile VPN is a security software solution especially developed for wireless networks. It creates a secure tunnel between a mobile device and the agency's network by using FIPS 140-2 validated end-to-end encryption in compliance with the CJIS policy for law enforcement agencies using wireless technology to connect to federal systems.

In addition, the implementation of the approved security protocols and algorithms has been validated by the National Institute of Standards and Technology (NIST). The use of a validated product with approved security components guarantees best practice and ensures regulatory compliance.

Support for advanced authentication

Columbitech Mobile VPN supports advanced two-factor and multi-factor single-sign-on authentication with unique client certificates, user-based public key infrastructure, one-time passwords (OTPs), smartcards, biometric systems, and software and hardware tokens.


MUTUAL TWO-FACTOR AUTHENTICATION/X.509/AD/OTP
FIPS 140-2 VALIDATED
HIPAA/PCI DSS/SOX/CJIS COMPLIANT
NETWORK ACCESS CONTROL (NAC)
INTEGRITY MONITORING (SHA-1)
256-BIT AES ENCRYPTION
COLUMBITECH MOBILE VPN IS AVAILABLE AS A CLOUD-BASED SERVICE OR CAN BE INSTALLED ON PREMISE.
FIREWALL
COLUMBITECH GATEKEEPER
FIREWALL
COLUMBITECH VPN SERVER
APPLICATION SERVER
DRIVER LICENSE DATABASE
WARRANTS
FIRE HYDRANTS AND HAZMATS
911 CALLS
VEHICLE REGISTRATION
MOBILE VPN CLIENT FOR IOS, ANDROID, WINDOWS, LINUX AND M2M
POLICE
FIRE RESCUE
FIPS VALIDATED 140-2
CJIS
ADVANCED AUTHENTICATION
BE COMPLIANT

© TOMAS ÖHRLING 2013

In addition, Columbitech offers a split certificate solution, which leverages QR codes to store a piece of a certificate.

Columbitech Mobile VPN provides integrity monitoring (SHA-1) of all data in motion as well as support for Network Access Control (NAC), which enables enforcement of the agency's IT policy.

Multi-platform support

Columbitech Mobile VPN offers multi-platform support, including Apple iOS and Mac OS, Android, Windows and Linux, and can be deployed for any IP-based network for seamless roaming between cellular, Wi-Fi and satellite networks.

Advanced mobility features

Police and other first responders move around and sometimes work in remote areas with poor cellular coverage, causing mobile devices to lose coverage with negative impact on productivity. Many public safety agencies rely on multiple cellular carriers as well as Wi-Fi and satellite services to provide the best possible network coverage. Roaming between networks is therefore a challenge.

Session persistence and automatic roaming

Columbitech Mobile VPN enables automatic roaming between networks and creates a persistent connection between the mobile device and the company's server as utility workers move around and roam between different cellular carriers and Wi-Fi and satellite networks, or temporarily lose coverage. The mobile VPN automatically reestablishes the connection so that users do not lose data or have to reauthenticate and restart applications when the connection is reestablished.

Data compression

Adaptive data compression provides up to 100 percent faster throughput than do SSL and IPSec VPNs. This improves the application performance in networks with limited bandwidth.

Cloud-based or on premises

Columbitech Mobile VPN solution is a client-server-based VPN software product and does not require any additional hardware. The VPN server supports virtualization and can be installed on a server computer on premises but is also available as a cloud-based service.

The VPN server can handle up to 10,000 concurrent users and can cluster as many as 255 mobile VPN servers in one server group. Columbitech offers a Gatekeeper that further strengthens the protection and handles load balancing and failover between the VPN servers in larger deployments.

SDK for app integration

The Columbitech App software development kit (SDK) provides tools for building apps with built-in mobile VPN functionality for Android, iOS and Windows Phone 8 apps.

Provisioning

Columbitech Mobile VPN leverages existing tools for deploying software such as Windows MSI packages or leading mobile device management solutions.

It also provides built-in support for version updates and distribution of security credentials such as digital certificates. Mobile devices using Android or iOS are easy to deploy directly from the iTunes App Store (iOS) or Google Play (Android) and are configured by simply scanning a QR code.

Pricing

The software is available as life-time perpetual licensing or software-as-a-service with monthly licensing.

Mobile devices using Android or iOS are configured by simply scanning a QR code. This oode provides access to the Columbitech demo server.

TECHNICAL SPECIFICATION

CLIENT SUPPORT

Apple iOS 5.0 and up
Apple Mac OS Snow Leopard 10.6 and up
Android 4.0 and up
Android 2.2/2.3 (rooted)
Windows XP/Vista/7/8
Windows Mobile 2002/2003/5.x/6.x
Windows CE 3.x/4.x/5.x
MS-DOS and DR-DOS
Embedded systems

For any other platforms, the Columbitech embedded SDK can be used to create a custom VPN client.

SERVER SUPPORT

Windows 2003/2008/2012
Linux (kernel 2.6.8 or higher)

NETWORKS

Ethernet (fixed)
Wi-Fi (private and public)
Mesh networks
Cellular networks (WiMAX, 2G, 3G, and 4G)
Dial-up
Satellite

ENCRYPTION

Up to 256-bit AES encryption (FIPS 140-2 validated)

AUTHENTICATION

Client certificates (PKI x.509)
Windows Active Directory
Common access cards
Smart cards
Biometrics
Radius
Google authenticator
Verizon Universal Identity Services (UIS)
OTP (e.g. SMS, RSA SecurID, Yubico, Verizon Universal Identity Services (UIS)

About Columbitech

Columbitech protects the entire workforce with one FIPS-validated VPN solution. With more than two million users, customers include three of the top 10 U.S. retailers, public safety agencies, telecom providers and U.S. military branches. Columbitech is privately held, with offices in Stockholm and New York. Visit www.columbitech.com for more information.