



# **TLS VPN - Overview of compliance requirements for Federal, State, and Local Agencies**

# Background

## History of Compliance Directives

The landscape for agencies and different bodies within the Department of Defense (DoD) has been challenging and shifting over the last seven years. It has equally challenged suppliers who try to be in compliance and offer good products and services for increased security. For a long time, the international initiative called Common Criteria was the highest priority. Together with FIPS 140-2, this was the direction for the future of compliance. This initiative was based upon many similar and overlapping policies, creating a difficult situation for everyone involved, and it slowed down the utilization of any wireless network implementation.

Around 2003 there was a policy drafted calling for all wireless 802.11 networks to use IPSec VPN security. However, this policy changed with regard to this specific requirement, before getting ratified. This was due to usability limitations of the IPSec VPN, which include slow transactions and high memory consumption for mobile devices—and thus negatively impacted wireless networking’s core purpose: secure mobility. The final policy simply demanded VPN-class security without defining a specific protocol.

Soon there were rumors of a new wireless security policy now demanding so-called Layer 2 security, whereas the flawed rationale claimed it to be “more” secure than security applied higher up in the TCP/IP stack. (To delve into this in greater detail is a different discussion and it is not within the scope of this document.) This policy later became 802.11i while the IEEE body was still ratifying its specifications. For wireless devices, including access points and handheld devices, the WPA standard was formed by the Wi-Fi Alliance and soon became the WPA, and later, the WPA2 standard.

The combination of 802.1x with EAP-TLS mutual authentication using x.509 certificates, together with WPA2-class devices using AES encryption, is the collection of moving parts and together they create the described 802.11i security at its highest level.

The latest DoD directive issued as a supplement to the previous Layer 2 requirements concerning wireless networks came out in June 2006, and is named 8100.2. It specifies how to secure 802.11 networks with 802.11i security only. This policy was created with the intention of establishing a common ground and more heterogeneous wireless networks with interoperability among different agencies within DoD. However, the next update of this directive will soon be released and will ease

the requirements of EAP-TLS, simply allowing for a lower level of authentication and the potentially increased risk for unauthorized access to government networks.

## Current Situation

### Compliance challenges

The difficult challenges of 802.11i and EAP-TLS are many, but the interoperability among different hardware vendors has been, to say the least, disappointing — and is best explained by stating that there are as many implementations as there are vendors. It furthermore requires an authentication server communication with the RADIUS protocol between wireless devices and access points. This creates many architectural headaches and increases costs.

Today, most equipment installed does not support these security features at all and in the best of worlds an upgrade can do the trick, but more often, there is simply no option available and a complete “rip-and-replace” scenario from a single vendor is the best bet — but this then obviously becomes cost-prohibitive. The only thing worse than weak security is a security strategy that is impossible to implement in reality. These painful realities will bring the next release of the 802.11 network security back to square one. The same problem is also facing retailers and the Payment Card Industry initiative, where IT is focused more on compliance on paper than on protecting their valuable assets. 802.11i security, using so-called pre-shared secrets, is no longer a secure network and can be easily compromised because there is one secret password that does not change very often. It is a nightmare to administer, which historically always mean that shortcuts will be taken and the secret is out.

The overarching challenge with any of these directives seems to exist when they are tied to hardware. This puts everybody involved constantly behind the curve. Evolving radio technologies with new user patterns such as 3G, WiMax and ZigBee, to mention a few, will entirely disrupt the slower-working bodies of standardization followed by an “always too late” vendor adaptation. Computing power is the other factor challenging the landscape of security measures.

Now there are other DoD directives named 8500.1 and 8500.2 that are intended for Information Assurance (IA) and do not go into specific details, such as in the case of the described 8100.2. Instead, these call for numerous initiatives to maintain a high level of security and are aimed at mobile computing devices (8500.1 -2.1.2.7), as well as many others. It furthermore calls for PKI and

uses language such as that of section 4.2 of 8500.1: All DoD information systems shall maintain an appropriate level of confidentiality, integrity, authentication, non-repudiation, and availability that reflect a balance among the importance and sensitivity of the information and information assets.

## **FIPS 140-2**

The single compliance requirement that has kept its inherent sanity over the last seven years is FIPS 140-2, a North American compliance initiative and requirement for any IT supplier selling software or hardware. Its issuing organization is the National Institute of Standards and Technology (NIST).

It is important to understand that products claiming FIPS compliance need to be fully reviewed. This means that the entire solution, including both client and server implementations, has to be evaluated and tested by NIST. It is the product itself that requires the FIPS 140-2 compliance. Consequently, the use of certified 3rd party components is not sufficient to claim FIPS 140-2 compliance.

Attempts to try to take a shortcut into selling to the DoD are often made by simply using the FIPS-compliant AES encryption; this is, however, not an adequate take on the overall purpose of FIPS 140-2 certifications and information assurance.

The other goal of FIPS-140-2 is to make sure that agencies use security standards that can be reviewed and that are publicly available. This is to ensure the highest quality of security and to not risk flaws with proprietary security implementations, lacking the necessary insight and improvements if necessary.

## **Conclusions: Things to Look Out For**

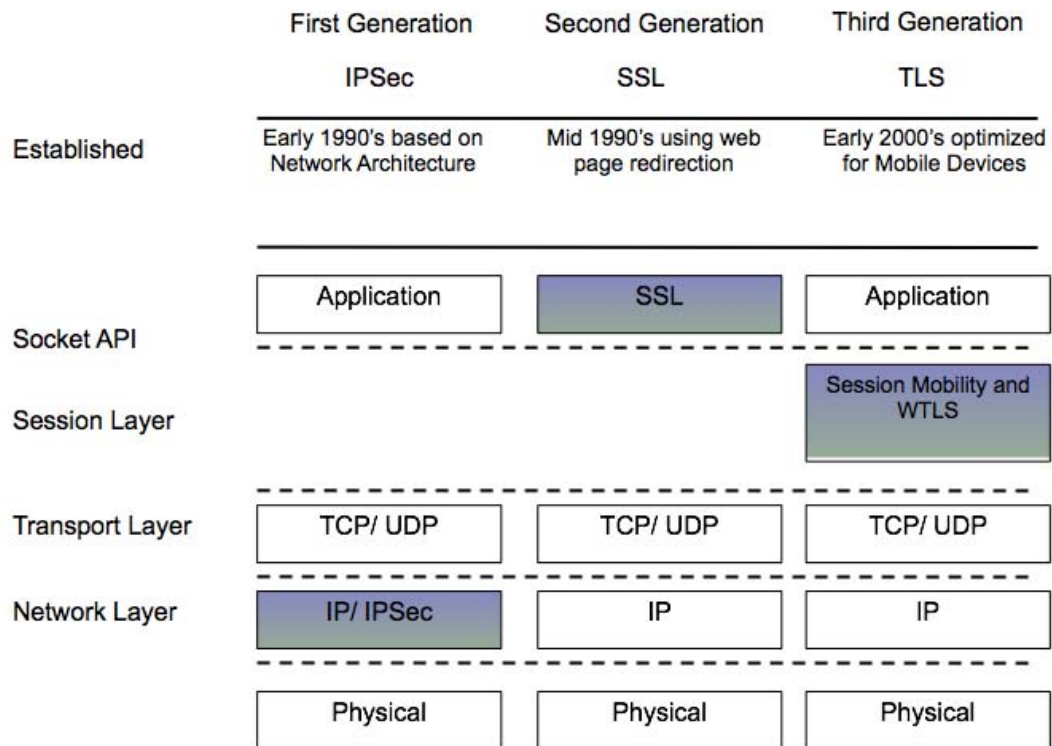
- Make sure the product uses a standard security protocol such as TLS or IPsec.
- Make sure that it is the actual product, and not just components, that has been thoroughly tested.
- Download the product's security policy document from NIST and verify the above.

# TLS VPN

## Overview

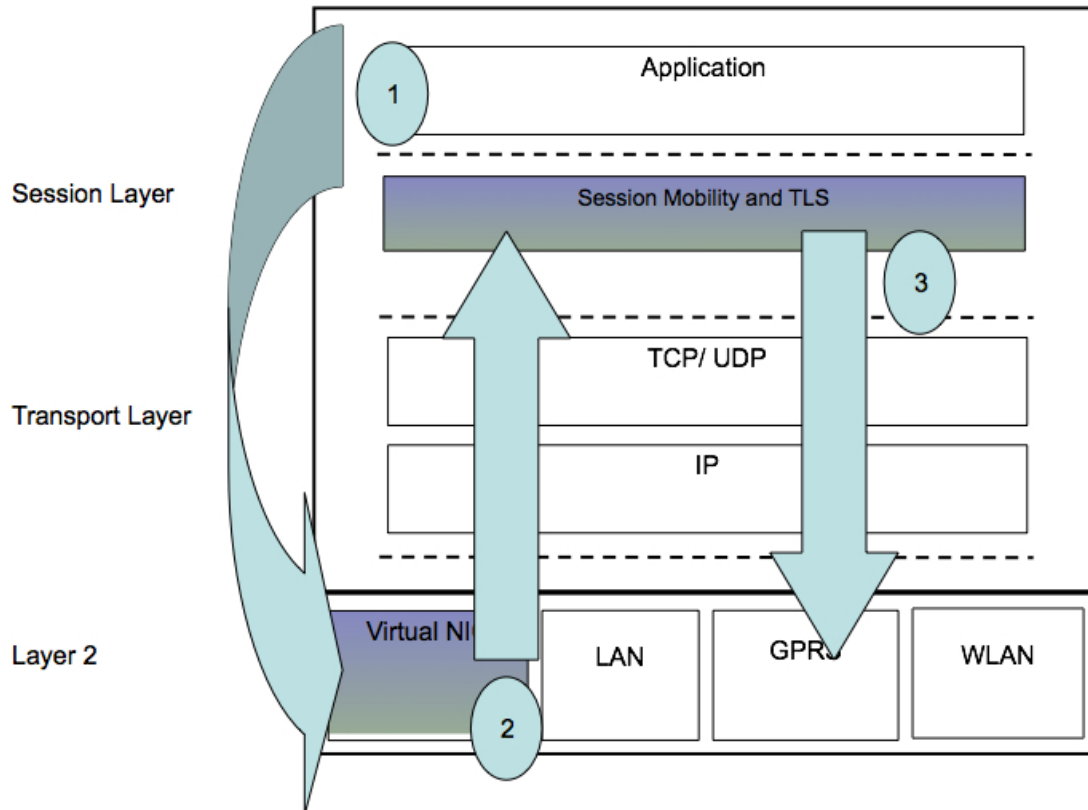
A TLS VPN is a software technology using an IEEE-standardized security protocol. The benefits of using a standardized security protocol such as TLS are many:

- The protocol and its design are publically available
- It's lightweight compared to IPSec
- It is routable over different network technologies such as 802.11, 3G, EV-DO, ZigBee and WiMax.
- It can be used in combination with any hardware, OS, or TCP/IP implementation.
- It instantly secures any application without any changes.



## Layer 2 and TLS

A TLS VPN is hooked into the TCP/IP stack at layer 2 but effectively processes the payload at the session layer to achieve the most efficient mobility experience. The payload is then put into a secure end-to-end tunnel and sent over the active network.



*1. Application request. 2. TLS VPN middleware captures all application requests at layer 2 using a virtual network interface— VNIC. 3. All data packets are compressed and sent off through the currently active physical network card.*

## Description of a Typical TLS VPN Log-On

Here is a short and simplified explanation of what happens when a computer and its user access the private network:

1. The user enters his username and password.
2. The process of mutual authentication is initiated using PKI and x.509 certificates, verifying that the server is really what it claims to be, and the server verifies the incoming client's identity.

3. The RSA keys using 4096-bit encryption are then exchanged to establish a safe passage for the payload encryption and the key exchange with AES 256-bit keys.
4. Now we can safely exchange sensitive information that will be integrity-checked using SHA-1 (to prevent any unauthorized alterations), and we have the constant change of the AES keys to prevent any replay attacks.
5. The TLS security protocol can be implemented to support session resume. If radio coverage is poor, or the need to roam to another available technology arises, the security credentials are automatically exchanged again, which is referred to as secure roaming. This means that all applications will be maintained even when a voice call comes through, and the ongoing data transactions will be picked up where they were left off. This is all seamless and combines strong security with high usability and productivity.

### **TLS vs. IPSec**

IPSec has become the de facto standard for IP VPNs. IPSec operates on the network layer and its security mechanisms are tightly connected to the IP address of the connecting host, an unfortunate characteristic that prevents smooth operation in a fragmented network environment with different networks hosted by different providers.

One of the most serious problems with IPSec is that the protocol does not support network address translation, a technology that virtually every enterprise and service provider uses in order to increase its public address space. NAT servers expect transport-level information rather than IPSec headers following the IP header. The common solution is to append a transport protocol header between the IP header and the IPSec header on each data packet. One problem has been solved, but unfortunately, by introducing another: The extra transport protocol header introduces additional overhead to the data transmission. Using IPSec together with Mobile IP will lead to a substantial performance degradation related to extensive protocol overhead.

Another serious shortcoming of IPSec is its lack of session resume functionality. In a fixed network environment, connections are rarely dropped, which is why session resume was never an issue when designing the protocol. A wireless connection, on the other hand, presents a much higher demand on the protocols used. Wireless networks are unstable and connections will be dropped. Without session resume, the user will have to log on again every time a connection is lost, including for heavyweight functions, such as key exchange and user authentication.

# Conclusions

## Requirements to Sell to 802.11 Network (Wi-Fi) Customers

A TLS VPN can replace 802.11i security, but it can also ride on top of any 802.11 security implementation. Whether it is WEP or static keys, there is no difference because it creates a secure end-to-end tunnel, and together with a firewall, will create maximum security using TLS with certificates, AES for encryption, and SHA-1 for integrity. It uses the same security for any other network and can even route packets between different technologies without compromising the security or integrity of any IP communication.

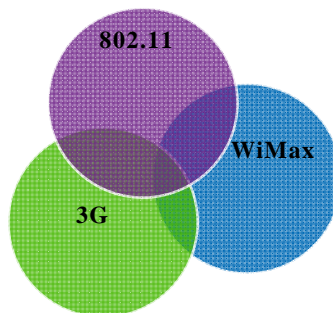
The 8100.2 directive, however, also leaves room for exceptions that need to be justified and documented with DoD Information Assurance Certification and Accreditation Process (DIACAP), which, in particular, must explain the impact of the loss of interoperability.

One would in this case argue an increased level of interoperability with its hardware, platform, network, and application independence. We should not forget that the job at hand is to provide proven and adequate security in the best interests of DoD. I have attached the latest version of this policy for a full review.

## Requirements to sell to Wireless WAN customers

The use of any other technology such as UMTS-3G, CDMA-EV-DO, WiMax, or the combination of any of them with WiFi makes the discussions earlier in this document obsolete. The only existing requirement is a full FIPS 140-2-certified product.

The future requirements for compliance will be mainly influenced by the Defense Information Systems Agency (DISA), and the existing draft named SP800-113 that calls for TLS VPN security.



*The combination of wireless networks imposes new challenges and requires better management of secure connectivity.*

## Growing From WLAN to Also Include WWAN

There are mainly two types of situations when federal entities consider adding WWAN to their applications to increase the level of access to applications.

1. With no WLAN-compliant solution in place, they would consider using a TLS VPN solution that would address compliance across their networks, pointing to the IA 8500.1 policy for overall network security and the drafted SP800-113 for WWAN. In this case one would also anticipate a discussion of the relevance of the amended 8100.2 policy that specifically requires an 802.11i solution using TLS on layer 2 for the WLAN. This scenario would probably have to be discussed with DIACAP and DISA.
2. With an existing solution in place, and adhering to the 8100.2 policy using an 802.11i solution, and when the time and money are already invested, the situation changes. The 8100.2 policy is completely obsolete with a WWAN network; and the question then is what to do, and this is where the federal marketplace becomes confused. From a policy perspective, there is only the IA 8500.1 for overall network security and the drafted SP800-113 for WWAN available, and the choice of a TLS VPN the only option. However, cross-communication between the networks becomes a problem.

What would make the most sense in the latter case is to not change a thing for the existing WLAN. Once an agency moves beyond those boundaries to utilize WWAN, they could set up a TLS VPN server behind a firewall connected to the Internet, run the TLS VPN on top of their 802.11i-secured WLAN, and have the TLS VPN protect over WWAN, as well as also add an additional layer of end-to-end security for the WLAN.

The benefits are a seamless integration of existing networks, with the possibility of utilizing WWAN and maintaining compliance using any FIPS 140-2 TLS VPN.