MOBILE DEVICE SECURITY

Trusted Public Key Infrastructure (PKI)

The next generation in PKI ensures that only authorized devices connect to your infrastructure. Machine identity certificates cover the smart phones, tablets, and other mobile devices we use every day. Regardless of OS, whether it be Android, iOS, WinOS, etc., machine identity certificates can identify a machine to any Public or Private Cloud entity with which it interacts and provide a level of assured security beyond a simple username and password proprietary VPN solution. The machine identity certificates reside within the operating system's certificate store or on a hardware security module for each device. Certain unique attributes of the machine can be identified within the certificate—like the DNS name or the Globally Unique Identifier (GUID).

Imagine the Scenario

Your company has employees working with several different devices. A typical employee has at least two devices – a laptop and a handheld device – used to obtain information from your infrastructure. Access is usually via a Web-based application or a VPN solution requiring a username and password. The employee may also need access to company information from their home computer or other device that you have no way to control or to determine vulnerabilities. By assigning machine identity certificates to the devices and requiring these certificates to authenticate to your infrastructure, you can limit your exposure to privacy data and intellectual property vulnerabilities.

Machine identity certificates allow you to confidently identify critical assets necessary to maintain the level of security you need to run your business. Installing machine identity certificates is fast and easy.

Add Flexibility To Your Network and Secure Telecommuting

This technology allows your network to become truly virtual without major expense. The machine identity certificates enable network privileges, opening up opportunities for secure telecommuting within an organization. The enhanced key usage attribute of the certificate contains an object identifier that allows client/server authentication as well as various IPSec and VPN protocols. This means that once a certificate is installed on a machine, a secure VPN connection can be made between corporate mobile resources and the home office without a proprietary client. Machine identity certificates may also identify devices to Web servers that wish to verify the machine before allowing the user on that machine to download the data it protects.

WidePoint Corporation

Headquarters: 703.349.2577
7926 Jones Branch Dr., Ste 520
McLean, VA 22102

Cybersecurity: 703.273.0578
11250 Waples Mill Rd., S. Tower Ste 210
Fairfax, VA 22030

WidePoint.com

widepoint

MOBILE DEVICE SECURITY

Trusted Public Key Infrastructure (PKI)

Reduce Risk Within Your Network Infrastructure

Incorporating machine identity certificates into your network addresses vulnerabilities simple VPN solutions cannot. Employees can download sensitive information to only authorized, properly configured and protected computers and mobile devices. Since a device is identified and authenticated to your network at a high level of assurance, it puts up a barrier against rogue machines accessing data or the inadvertent download of sensitive data on non-authorized devices. The strongest security aspect is that if a machine is compromised and no longer under your control, revocation of that certificate will instantly prevent that machine from authenticating to your infrastructure.

Machine identity certificates allow you to confidently identify critical assets necessary to maintain the level of security you need to run your business. Installing machine identity certificates is fast and easy. It is simply loaded into the pre-existing architecture of your machines with no proprietary client required.

Visit www.widepoint.com to learn more about WidePoint's Mobile Device Security