CERTIFICATE ON DEVICE

Higher Assurance Security for Mobile Devices

Authenticating devices that attempt to access your network and resources provides a greater level of information assurance beyond a username and password, and enables levels of access to be assigned to users based on the device they're using.

As IT infrastructures extend beyond traditional boundaries into the Cloud and the number and variety of mobile devices continues to proliferate, organizations increasingly struggle with securely managing access and protecting data.

At the same time, employees want to use their personal mobile devices to work whenever they want, wherever they are—and accommodating that successfully can pay off with increased productivity and more motivated employees.

Identify the User and the Device

Today's goal for end-user computing to "Go Anywhere, Stay Connected, and Be Productive" can only be achieved by allowing any authorized user, using any authorized device, to connect to any authorized network, and authenticate to any authorized service or capability.

A Solution For All Mobile Devices

Given the ever-changing diversity, connectivity, and computing power of mobile devices, it is critical for the content of these devices to be properly identified and secured, and the integrity of the transmissions to be protected.

Because Certificate-on-Device can be implemented on a variety of form factors, including SD and MicroSD cards, SIM chips, and USB drives, you have a long-term, flexible solution—even as devices evolve and become more powerful.

- Ensure that the only devices accessing your network are authorized and protected
- Manage what users can access and download based on whether they are using their personal or corporate-owned device
- Ensure your compliance with regulations related to accessing restricted data
- Enable a secure connection between mobile devices and your corporate network
- Revoke certificates of devices that were lost or stolen, or belong to an employee who has left your organization

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

WYY-401502

CERTIFICATE ON DEVICE

Higher Assurance Security for Mobile Devices

WidePoint's Certificate-on Device brings higher levels assurance to mobile devices

Identify a device on the network

- Provides the capability to establish secure communication between the device and the application before the individual authenticates to the application.
- Provides the capability to digitally sign and encrypt transactions on an organization's network. As the device is identified to the network, the user will be able to use the device to sign and encrypt documents before sending them over the network. Other users within the organization who also possess digital certificates will be able to verify the digital signature and decrypt the document.

Authenticate the user to other apps

- Provides more capabilities of primary credentials (CAC/ PIV and derivatives) for federal government employees, contractors and trading partners. As individuals need their CAC/ PIV functionality to authenticate to cloud services in a mobile environment, the credentialed device will invoke WidePoint's derived credentials to access applications.
- Provides a level of assurance that is higher than Level Of Assurance 2 or 3[1] non-crypto.
- Use a derived credential for access into e-authenticated servers and applications.

Use the device as a strong identity token

- As strong identity credentials are issued to devices at Levels Of Assurance 3 and 4, the device will become the primary token and replace a smart card or other hand-held token, thus freeing individuals to carry a single mobile device containing multiple smartcards or tokens.

Ready For Your Environment

WidePoint solutions accommodate today's wide variety of mobile devices and security containers because we design our digital identity solutions using standards-based technologies and readily available commercial, off-the-shelf (COTS) products.

We can accommodate a variety of storage form factors, issuing digital certificates via secure cloud services, including:

- SD and MicroSD cards
- Trusted Platform Module (TPM)
- SIM cards
- USB drives
- UICC tokens
- Smart cards
- Software containers

A Solution With Federated Validation Services

WidePoint Certificate-on-Device digital certificates are trusted worldwide. They are available for both government and commercial use, and we provide global federated validation services for all your mobile devices as an authorized Certificate Authority (CA) for:

- Department of Defense External Certificate Authority (ECA)
- GSA Access Certificates for Electronic Services (ACES)
- Transportation Workers Identification Card (TWIC)
- Federated Identity Cross Credentialing (FiXs)
- GSA Shared Service Provider (SSP) Program

We provide the Trust Behind Your Digital Identity.

[1] US Federal Government describes four identity authentication assurance levels for e-government transactions. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential in this context) that refers to his or her identity. In this context, assurance is defined as (1) the degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and (2) the degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.