



plusID

Using the plusID™ biometric device for logon in a Microsoft® domain environment

Introduction

plusID biometric devices can be used to log users onto a domain via two or three-factor authentication. The plusID device is ISO 7816 Part 3 smart card compliant, and as such enumerates itself to a computer exactly like a smart card, allowing for rapid enterprise integration of plusID devices across Microsoft® systems that support smart cards.

System requirements

The following are the smart card related system requirements for deploying Privaris plusID biometric devices into a Microsoft® environment for user authentication/logon (via USB or via Bluetooth):

1. Microsoft Windows 2000 Server (or later) domain environment

Microsoft Windows 2000 Server, and later, natively support smart card authentication as a means of logging users onto a domain environment. In a domain environment, users and their access permissions are stored and managed in a central location, referred to as the Active Directory.

Once a server is configured to act as a domain controller, smart card authentication via plusID biometric devices is automatically enabled on all client machines that are a member of the domain. For details on server configuration, see “Additional Information” below.

2. Microsoft certificate services

Smart card authentication relies on the public key infrastructure (PKI) to authenticate users to the domain. The Microsoft Certificate Services are the server component that provides the infrastructure to support PKI and is responsible for issuing credentials (certificates) that can be used for a variety of purposes, including secure email and user authentication.

In security-conscious environments, these credentials are stored on a secure device such as the Privaris plusID so that they may not be tampered with or used without authorization. The Microsoft Certificate Services include a web-based interface through which an administrator can generate credentials for a user and securely store them on the user's plusID. Certificate services can be installed anywhere, as long as it is trusted by the server. For details on downloading certificates, see “Additional Information” below.

3. USB port

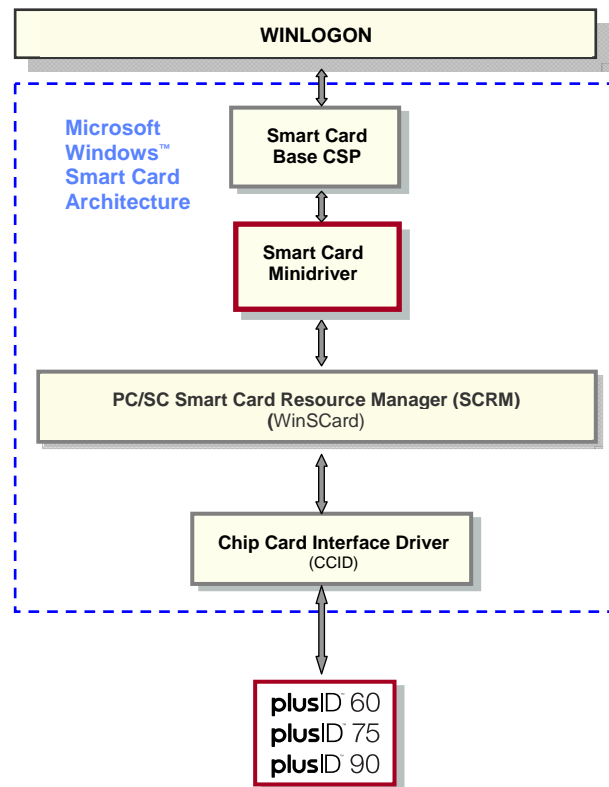
The plusID device connects to the client machine using the Universal Serial Bus (USB). Each client machine must have at least one USB port available in order to connect to the device. The plusID device works with both high-power and low-power USB ports, though a high-power port is recommended in order to recharge the plusID's internal battery.

4. Device driver software

Client machines must be configured before they are able to make use of a plusID. This includes the installation of device driver software, which consists of a CCID driver and a plusID device minidriver. The CCID driver is a standard driver provided by Microsoft for working with smart card devices such as the plusID and can be obtained via Windows Update when the plusID is first connected to the client. The device minidriver is a small software library provided by Privaris that allows Windows to interact with the plusID. The minidriver is included in the Logical Access Software Package which is an option during installation of the plusID Manager software (used for enrolling and configuring devices).

How plusID Interfaces with Microsoft's Smart Card Architecture for Logon

Blocks in red supplied by Privaris. Yellow = Microsoft software White = hardware



Additional information

The Microsoft "Smart Card Deployment Cookbook" covers all aspects of smart card deployment, from general information to detailed installation and configuration information: <http://www.microsoft.com/technet/security/guidance/identitymanagement/smrtdcb/default.mspx>