

DigitalPersona® Pro SDK



DigitalPersona SDKs provide the tools for developers to create a new generation of commercial and internal use applications delivering the convenience, security and biometric assurance of fingerprint authentication. From time and attendance, process control, point of sale to business applications, the DigitalPersona SDKs allow developers to quickly integrate fingerprint authentication into their software and hardware designs.

Easy, fast way to integrate biometrics into applications for commercial and internal uses:

- **Authenticate users reliably and conveniently.**
- **Simplify and enhance security.**
- **Streamline business processes.**
- **Address compliancy concerns.**
- **Reduce password management costs.**

DigitalPersona Software Development Kits (SDK) enable integrators and developers to quickly add the power of fingerprint-based authentication to their Microsoft® Windows-based applications.

DigitalPersona offers several SDKs from which to choose. Developers select the SDK best fitting their development environment, the preferred programming language, the level of customization required, and the type of application.

Easy to Use Toolkits

In only a few hours, developers easily integrate fingerprint authentication within their application and have access to a full range of authentication services for their solution. The high-level interface frees developers from the burden of programming many time consuming tasks such as networking, user interface and reader handling.

Programming Options

DigitalPersona SDKs support several development environments and interfaces including Visual Studio C++, ASP, .NET, C#/VB.NET and Delphi.

The SDKs provide a proprietary database or developers may use their preferred database.

With the appropriate SDK, choose from our DigitalPersona® Pro Workstation user interface, develop your own customer interface or use an ActiveX built-in user interface for easy integration.

Fingerprint Recognition Engine

The DigitalPersona Fingerprint Recognition Engine provides the basic functionalities

of fingerprint feature extraction, registration and matching. Verified by third parties, the DigitalPersona Engine combined with DigitalPersona U.are.U® readers, offers highly accurate fingerprint recognition and fast execution time.

Security and Privacy

DigitalPersona has given much consideration to security and user privacy issues. Fingerprint data is encrypted and/or signed, offering protection from tampering and maintaining user's privacy.

Supported Fingerprint Readers

The DigitalPersona Pro SDK supports the standalone U.are.U Reader, the U.are.U Module designed for integration with OEM equipment and the ergonomic U.are.U Fingerprint Keyboard which includes an embedded U.are.U 4000B Reader.

Proven Technology

DigitalPersona is the trusted leader in biometrics. DigitalPersona's proven fingerprint authentication technology can be found in custom applications around the world. Examples include banking applications in Mexico, point of sale terminals in US retail chains and restaurants, and health care industries.



digitalPersona.

System Requirements

Operating System Windows® Vista, XP Pro, 2000, Server 2003 and 2000
 Hardware Pentium-class processor (or better), CD-ROM drive, USB Port

Development Environment

Visual Studio C++
 Visual Basic
 .NET, C# / VB.NET

Programming Interface

C, C++

User Interface

Pro Workstation user interface

Fingerprint Registration

Pro attended or self-registration

Database

Pro Server - Active Directory database

Fingerprint Readers

DigitalPersona U.are.U Reader, U.are.U Module and U.are.U Fingerprint Keyboard

Security

- Fingerprint templates are encrypted by the engine.
- The fingerprint reader sets up a challenge-response encrypted link with the driver to securely transfer the image.
- Signs fingerprint registration templates together with the GUID of the user using "RSA public-key signature algorithm" (1024-bit key).
- Uses RSA public-key exchange algorithm (1024-bit key) for key exchange and "RC4 stream encryption algorithm" (128-bit key) for data encryption to secure the client-server communication channel.
- For the Pro SDK only, uses RC4 (128-bit key) to encrypt applications' protected storage.

Performance

Tested by third parties, the SDKs offer highly accurate recognition and fast execution time. Please request a white paper for details.

Application Deployment

DigitalPersona Pro Workstation required and available separately. U.are.U Readers are not included with SDK purchase.

Authentication Server Support

Pro Server Support

