U.are.U® Integrator Gold Software Development Kit

DigitalPersona's U.are.U Integrator Gold Software Development Kit (SDK) enables developers to add the power of fingerprint authentication security to their Windows applications. The toolkit includes header files that define the API, sample code for Visual C, Java, C++ 6.0, and the Fingerprint Recognition Engine runtime. For Visual Basic developers it will be necessary to use the U.are.U Integrator Platinum SDK or write a wrapper around the Gold DLLs. The SDK does not come with a U.are.U Fingerprint Sensor or license to the DigitalPersona Fingerprint Engine. You will need to purchase a sensor and license separately.

Who it is for?

System Integrators - The SDK can be used to develop custom applications for a wide variety of security use related to PC or client/server access. Basically, any application that runs on a PC or is controlled by a PC that needs user authentication can use the U.are.U Integrator Gold SDK.

Application Developers – Anyone who is developing an application to be distributed widely can include links to U.are.U for user administration and authentication. If your customer uses a U.are.U Sensor, your application will take advantage of it.

What is the SDK not for?

The SDK is designed to develop applications that run on the Windows platform. If you have an application where a PC running Windows will not be present, please contact us for additional information. Also, the standard shipping version of the SDK will work with all DigitalPersona sensors.

What is the architecture of the SDK and the DigitalPersona Fingerprint Engine?

There are several components to the DigitalPersona Fingerprint Engine, as exposed by the SDK. The application developer is provided with several levels of APIs, from the low-level interface to high-level authentication functions.

The Fingerprint Engine interacts directly with the U.are.U Sensor COM Server. The Server handles all sensors connected to the USB ports and dispatches notification of fingerprint capture to all U.are.U-enabled applications running on the system. There can be multiple sensors attached to the system as allowed by the USB configuration on your computer. The Server sets up a challenge/response encrypted link with the sensor to securely transfer the image from the sensor.

Fingerprint Engine Components

The Feature Extraction Module
The feature extraction module extracts a template from the fingerprint image that comes from the sensor. The standard feature extraction module works with fingerprint images produced with the DigitalPersona sensors. The feature extraction module supports two types of templates for fingerprint registration, namely BASIC and GREATS. The size of the BASIC template is *approximately* 350 bytes. The size of the enhanced composite GREATS template is *approximately* 1,250 bytes. Template size is subject to change with SDK upgrades. Except in unusual situations where storage space is extremely limited, we recommend the use of GREATS registration template as it offers significantly higher recognition accuracy. The feature extraction process takes approximately 0.22 seconds on a Pentium® 4 2.0GHz processor.

The Matching Module
The matching module takes two fingerprint templates, performs a match, and verifies that the fingerprints come from the same finger. The match process takes approximately 0.02 seconds on a Pentium 4 2.0GHz processor. The application can set the security level (False Accept Rate) to be used for matches. The default security setting is 0.01% False Accept Rate. At this setting, the False Reject Rate on the U.are.U 4000 Sensor using BASIC registration template is approximately 0.6%[1]. If a match is confirmed, the

matching module returns a 128-bit string, which can be used as a unique, reproducible key for that user. The matching module is also able to perform learning upon a successful match, which results in an update of the registration template. Learning requires extra computation and can be switched on and off by the application.

The Database Module

The Database Module can be used to store and manage a user database for fingerprint templates and user attributes. The user record contains multiple fingerprints from the user, and a protected storage area where data such as passwords or cryptographic keys can be securely stored for each user – only accessible by the user through a correct fingerprint match. The Database Module is included as a convenience for developers who wish to create a standalone application. However, fingerprint templates and user records can be stored in any location the developer chooses, such as within a LDAP directory or SQL database.

The High Level Interface Module

There are high level calls for registration, verification and sensor control. DigitalPersona does not display its own user interface. The Engine will perform a callback to user interface functions that are provided by the developer, so the developer can maintain a consistency of interface in the developed application.

Security and privacy measures

For all of the above modules, DigitalPersona has given paramount consideration to security and user privacy issues. For instance, at no time are the unencrypted templates or user records passed across library interface functions, exported or stored in a database. Furthermore, registration templates cannot be matched against themselves. At the time of installation, a security key is entered by the user and it is used internally as part of the encryption schema of the Fingerprint Engine. Templates that are created on different computers using different security keys are not compatible.

[1] A Transaction consists of three consecutive attempts of verification. Confidence interval of 90% was estimated to be [0.2, 1.0]% by taking the 5% and 95% quantiles of the nonparametric subset bootstrap estimate of the False Reject Rate distribution. A detailed report of the recognition engine performance evaluation and testing protocols is available from DigitalPersona.

DigitalPersona, 805 Veterans Blvd., Suite 301, Redwood City, CA 94063 USA, 877-378-2738, www.digitalpersona.com