

UbiQCardIssue™ Application



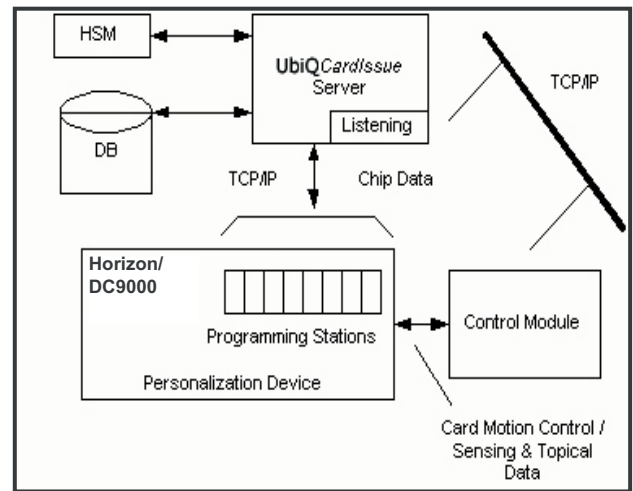
The final step in the personalization lifecycle is the actual issuance of the cards. The UbiQCardIssue™ application runs on a computer attached to your issuing device of choice and manages the smart card personalization process.

It incorporates an open system architecture, providing the Issuer with a single application that can support all products defined by UbiQCardPlan™ and all data prepared by UbiQDataPrep™. In addition, the application supports a library of personalization devices and chip operating systems.

As a result, the Issuer has greater freedom in selecting or changing all the components in its personalization system with minimal impact. In some cases, UbiQCardIssue™ enhances personalization device performance. Additionally, UbiQCardIssue™ can increase issuing speed and capacity by networking multiple lower-cost, low-volume personalization devices, thereby saving both time and cost.

A Sample Card Production Configuration

The diagram illustrates the card production configuration, using the UbiQCardIssue™ application, working with the NBS Horizon™, CIM or Datacard 9000™ personalization device. These devices are complex, high-volume card production machines, and may have modules for embossing, magnetic stripe encoding, topical image and data printing, as well as multiple chip-writing stations.



UbiQCardIssue™ Server Interfaces

UbiQDataPrep™ Application

Not shown in the illustration above is the UbiQDataPrep™ application. However, it is the primary source of input to UbiQCardIssue™. This input is a single production file, resulting from the key generation and data mapping operations, and is held in the database.

Personalization Device / Control Module

The UbiQCardIssue™ Server interfaces with the Personalization Device / Control Module in several ways. This interface varies with the device and its functionality. The UbiQCardIssue™ Application has the capability to interact with a variety of personalization devices by virtue of its UbiQLink® libraries. In the instance of the more complex NBS Horizon™ or Datacard 9000™, UbiQCardIssue™ is capable of communicating with the individual IC programming stations.

Adding Value Everyday



UbiQCardIssue™ Application

Another interface between these two card production system components is required for synchronization. The Horizon or DC9000 control module controls the movement of cards from station to station, and the arrival of a card at a particular programming station is sensed, resulting in a signal on the TCP/IP network connection. A 'listening module' within the UbiQCardIssue™ server detects the signal and begins a thread by which data flows to that particular programming station. The NBS Horizon™ or Datacard 9000™ contains multiple chip programming stations, which normally receive data simultaneously in a multi-threaded process.

Library of Personalization Devices supported by UbiQCardIssue™

UbiQCardIssue™ is closely linked with UbiQLink® technology, smart card issuing technology that provides a solution for dealing with the complex requirements of multiple applications, card operating systems, and key management systems. Through its multiplicity of built-in libraries, UbiQLink® also provides UbiQCardIssue™ with the capability to issue cards on a wide variety of card personalization devices.

Host Security Modules (HSM)

Though most of the cryptographic key generation / derivation and certificate preparation is performed in advance by the UbiQDataPrep™ application, an HSM associated directly with the UbiQCardIssue™ server is required to perform keytranslation operations and key derivation based on data retrieved from the target card. Keys loaded to the card during the personalization process are encrypted under a session key.

UbiQCardIssue™ Functions

Receipt / Utilization of Production File

The production file output from the UbiQDataPrep™ application is received by the UbiQCardIssue™ server and the personalization device control module.

The production file contains data used in embossing, mag stripe personalization, and for image printing on the card. These are portions of the personalization that are controlled directly by the device module and not required in the UbiQCardIssue™ application. When the designated personalization device is the Datacard 9000™, the device

control module also receives a T9k file. The T9k file is simply the Datacard 9000™ input file. The production file is based on the Card Program originally created in the UbiQCardPlan™ and processed by the UbiQDataPrep™ application and is supported by Issuer-supplied cardholder data, application code and data supplied by the Application Provider, and keys / certificates to support the card and application profiles. Associated with MULTOS cards are application load units (ALUs) delete certificates (ALCs and ADCs) provided by the MULTOS certification authority (CA).

Library Reference

In the card and application templates are pointers to the libraries of card operating systems and personalization devices contained within the UbiQCardIssue™ Server. This ensures that the card issue operation can accommodate production data for new card batches without reconfiguration, as long as the libraries contain the correct operating system.

Synchronism With the Personalization Device

Based on the production file and T9k files it receives, the Datacard 9000™ control module controls movement of cards throughout the device feed and provides the personalization data to the emboss, magnetic stripe and printing stations. When a card reaches one of the IC programming stations, the control module signals the 'listening function' of the UbiQCardIssue™ Server via the TCP/IP link that the IC programming station is ready to receive data. At this point a thread is opened between UbiQCardIssue™ and the IC programming station, and the thread is held open until IC personalization of that card is complete.

Security for Loading Sensitive Data

The production file developed by the UbiQDataPrep™ application is normally encrypted under a KEK shared with UbiQCardIssue™.

The production file is decrypted from under the shared KEK by UbiQCardIssue™ and a DES session key, derived from the card manager's encryption key, is used to securely transport cryptographic keys and other sensitive data to the card. At no time are any keys exposed outside of the HSM in the clear in the communication process.

U.S. Patent #5,684,742, #5,889,941, #6,014,748.

Other Patents Pending.

UbiQ Inc.
10925 Bren Road East
Minneapolis, Minnesota 55343
USA

Website: www.ubiqinc.com
Email: info@ubiqinc.com

T: + 952.912.9400
F: + 952.912.9439



UbiQ Inc. is a division of NBS Technologies Inc.
Specifications are subject to change without notice.

© 17-April-06 UbiQ Inc. All rights Reserved. All brand and product names are the trademarks or registered trademarks of their respective holders.