

UbiQPKGen™



High Volume RSA Key Pair Generation

UbiQPKGen™ is a utility designed to provide a cost-effective way to generate large volumes of public key pairs. The primary purpose of UbiQPKGen™ is to generate and warehouse a number of key pairs before they are needed for other operations. For example, the dynamic data authentication (DDA) configuration for VSDC and M/Chip requires a key pair to be generated for each card issued.

Generating these keys at the time of personalization, or even at the time of data preparation, can adversely affect the efficiency of operations. However, the UbiQPKGen™ allows you to generate keys in advance and securely warehouse them until they are consumed – consumption occurs only when the data preparation personalization file is created.

The UbiQPKGen™ utility may co-reside in the same server as UbiQDataPrep™ and run in attended mode during low utilization hours, or may operate independently.

The design of UbiQPKGen™ provides for simultaneous access to multiple (1 to 4) HSM boards physically installed in a single server in order to optimize the rate of key pair generation on that server.

Types of On-Card Keys and Certificates

Current EMV compliant applications may require the use of many cryptographic keys and certificates to ensure the proper operation of the authentication, data integrity, and data confidentiality functions of the card. An understanding of the different sources, processing and life cycle management of these keys and certificates is essential to the proper use of personalization solution components such as UbiQKeyMaster™, UbiQDataPrep™ and UbiQPKGen™.

For this purpose, the on-card keys and certificates may be grouped into the following three categories:

Category 1 **Card Scheme Keys / Certificates**

Those that are entered into the card early in the card life cycle by the IC manufacturer, card manufacturer, or card enabler through interaction with the Card Scheme CA, or are included within files (i.e., application load certificates) generated directly by the Card Scheme CA for entry to the card during personalization. They may be an input to UbiQDataPrep™, but they are mainly managed by the Card Scheme CA.

Category 2 **Issuer Keys / Certificates**

Those card configuration keys / certificates that are generated and managed within the personalization solution using components such as UbiQKeyMaster™. The Card Issuer's key pair and Issuer PK certificate are examples. A set of these keys and certificates is typically used in all cards issued by an Issuer for an application.

Category 3 **Card / Cardholder Specific Keys / Certificates**

Those that are required in large volumes (one for each card). From the standpoint of the personalization solution, these keys are considered consumables, generated and logged by UbiQPKGen™ and consumed by UbiQDataPrep™, but not managed beyond that operation. Examples of these keys are the ICC PK pair (used for DDA) and the Enciphered PIN PK pair.

Adding Value Everyday

The UbiQPKGen™ Utility

Highlights of the UbiQPKGen™ Utility are as follows:

- Utilizes one to four host security modules (HSMs) of the Eracom Protect Server Orange Model 50, 220 or 450 type, depending on the volume of key pairs to be generated, and the desired rate of generation. Each thread uses a separate HSM board.
- Generates key pairs in the RSA algorithm (specified by EMV).
- Generates key pairs with public key modulus lengths of 512 / 1024 / 2048 bits and other lengths (multiple of 64 bits) on request.
- Generates and warehouses up to 2 million key pairs in an encrypted PK database.
- Consumes key pairs directly from the PK database or from a secondary file.
- Maintains a log of key pairs generated and key pairs used in its database.

Key Generation Performance

The generation of RSA public key pairs involves a process of generating and testing prime numbers, which are variable in time. Therefore it should be understood that any stated performance numbers are average numbers. The generation time is also a function of the key (public key modulus) length and varies somewhat with the exponent length.

Keys / Certificates for Static Data Authentication (SDA) in VSDC and M/Chip Cards

In advanced applications, such as those that perform debit and credit transactions with the use of off-line card authentication, the public key of the Card Issuer must be certified by the certification authority of the card scheme on the card. The preparation for this requirement - i.e., generating of the Issuer key pair, self-certifying the public key, submitting to the CA, and storing the resultant

certificate in a key vault - are all normal functions of UbiQKeyMaster™. This is an infrequent occurrence, is done well in advance of personalization, and there is no impact on performance.

The availability of the Issuer public key certificate in the card facilitates the use of Static Data Authentication (SDA) with the terminal during a debit or credit transaction. SDA is capable of verifying the integrity of data written to the card during personalization.

Keys / Certificates for Dynamic Data Authentication (DDA) in VSDC and M/Chip Cards

If the smart card platform selected for the application is capable of performing RSA public key operations and the transaction terminals are appropriately equipped, the Card Issuer may also choose to employ Dynamic Data Authentication (DDA). DDA allows the card to generate a digital signature over card data, terminal data, and transaction data and allows the terminal to verify that signature.

DDA requires the generation of an additional public key pair - the ICC key pair which is unique to the card. Actually, the ICC private key and the ICC public key (certified by the Issuer) are both written to the card.

This key pair and certificate should also be generated in advance of personalization, so that the time the card spends under the head of the personalization device can be minimized.

The same rationale applies if the Issuer chooses to use the Enciphered PIN public key pair, which is also unique to the card.

*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

T: + 952.912.9400
F: + 952.912.9439
Website: www.ubiqinc.com
Email: info@ubiqinc.com



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.