MAGTEK®
THE TECHNOLOGY BEHIND THE TRANSACTION

The iDynamo is MagTek's secure card reader authenticator designed to work with the various Apple iOS devices. It comes in a modular design with the base secure reader and various adaptors to fit the Apple iTouch, iPhone 3, 3S, 4, 4S, iPad 1 and iPad 2.

There are two programming pieced that are required for these devices. The first is the Reverse DNS/Bundleseed ID required by Apple, and the second is the Secure Encryption Key required by MagTek to help make this a secure device.

Reverse DNS/Bundleseed ID is used by Apple to register an application on the iTunes App Store. When a developer registers an application with Apple, the developer and Apple assign these IDs to the application. The main purpose this ID is to "marry" the reader to the actual application. For example, QwickPay by MagTek has a unique ID matched to both the reader and in the app.The reader and the app must to have matching values to function properly. Apple is now allowing for shared values, so MagTek has values assigned to our products, which we share with our SDK* and encourage folks to use our values rather than individual, specific values related to just their product. This is a positive development for distributors and resellers, since there are fewer variants in the identification process and potential for shared inventories.

**Note: If a developer/integrator is writing to the iDynamo you will need MAGTEK's SDK. SDK is readily available and free from MAGTEK as an NDA document.*

The **encryption key** is used to "jumble" or secure the credit card data coming from the reader into the application and then onto a service provider. For developers, MagTek has the ANSI TEST KEY, a universal key with public data values used for developers and networks to test secure card transactions across the systems. The test key is never used in a live environment.

Many service providers, networks, integrators are sharing MagTek's key in securing their data. This **live key** is typically used when an application is connecting to the MagTek Magensa network for card decryption services. This could be a custom app, such as QwickPay, or MPPG. MagTek will waive a key load fee when the live key is used.

Service providers and end users may also have a **custom key**, loaded by MagTek at the factory, used in a closed environment to the service provider or the network. Some examples of custom keys include TGATE and Mercury. Both of these service providers offer secure card support and have their own encryption key.

Two columns can be mixed and matched specific to an end user when it comes to Appleseed and Encryption. It's important to match these to exactly what is needed, as the reader will not work if not programmed correctly and the readers are not returnable once there is a custom programming.

Pick one from each column:

Appleseed/Reverse DNS	Encryption Key
Magtek	Magtek
ShopKeep	Mercury
ISIS	TGATE
Merchant Warehouse	NMI
Gramercy	Gramercy
POSLAVU	????
????	????
Etc	Etc

For example, a reader could have a Magtek Appleseed and a Magtek Encryption key, or a Magtek Appleseed and a TGATE key. Or a Shopkeep Appleseed and a TGATE key, or Shopkeep Appleseed and a Mercury Key, etc. The combinations are endlessly customizable depending on individual needs.

In addition, relationships may require certain values and may also limit whose information can be used. Mercury currently requires any devices loaded with their keys to be purchased via Mercury. MagTek is working on opening that process up for future key loading.