ADVANCED PROVISIONING

- Issuer has total control
- Secure over any channel
- Eliminates the need for key exchange
The MULTOS application provisioning method has many advantages, especially when it comes to provisioning applications and application updates to MULTOS based devices already deployed in the field. At the heart of the process is the MULTOS Key Management Authority (KMA).

1. Each chip is injected at manufacture time with a **unique transport key** derived from a key held at the KMA. It is also injected with a **unique serial number** (unique across all manufactures). At this point the chips are truly generic stock items and can be used for any customer or use.

2. Once sold to a customer, the generic chips need to be **enabled** for use. This is done by sending the serial numbers to the KMA which returns enablement data encrypted by the unique transport key of each chip. The enablement data contains, amongst other items, an **owner ID number** (called the issuerID) and a unique, **signed asymmetric key pair**. This locks the chips to their owner and provides the key needed for the application provisioning.

3. **Personalised** applications are generated **off-line** (i.e. the chip does not need to be present) and **encrypted** using the **public key** of the target chip. If the public key is not known, then the chip can be asked to provide its public key certificate. The encrypted, personalised application can then only be read by the target chip and can be transmitted over any network, secure or not.

4. A **load certificate** from the KMA is required to **authorise** the loading of an application to a chip and is tied to the chip owner ID. The certificate also allows the chip to check that the application is **genuine** and unmodified. Likewise a **delete certificate** is required to delete an application.

5. One **standard script**, for any application, is all that is needed to load the application to the chip. The chip itself does all the cryptography required internally (no need for an external HSM or keys). This means that you can use a computer, mobile phone, tablet, ATM, POS Terminal and just about anything else you can think of as a post-issuance personalisation tool.

For more information about MULTOS visit [www.multos.com](http://www.multos.com)