

Certicom[™] **KeyInject**[™]

trusted key injection platform for anti-cloning

Certicom® KeyInject™, a trusted key injection platform for anti-cloning, enables device producers to track contract manufacturer production by controlling access to keying information; metering the use of this information and then reporting the results to the producer. KeyInject uses industry standard protocols and techniques based on elliptic curve cryptography (ECC) and AES for the strongest, most-efficient security.

Certicom Keylnject is part of the Certicom Trust Infrastructure that allows smart device vendors to securely manufacture and upgrade their devices with a cost-effective, off-the-shelf platform that offers flexibility, reliability and strong security.

proven, strong anti-cloning

Certicom Keylnject meets the stringent requirements of device producers that need to inject keying data during the vulnerable manufacturing process. Keylnject offers hardware-based protection of internal or third-party keys that is crucial to the security of the system. By controlling and reporting the volume of keyed devices, producers can eliminate the manufacture of black market devices.

cost-effective factory provisioning

Certicom Keylnject automates the process to key a device before it gets to the user which makes the system more secure while keeping costs lower in the manufacturing process. These flexible remote administration capabilities ensure that the producer can view the entire system with minimal effort which also leads to decreased costs.

complements conditional access and DRM systems

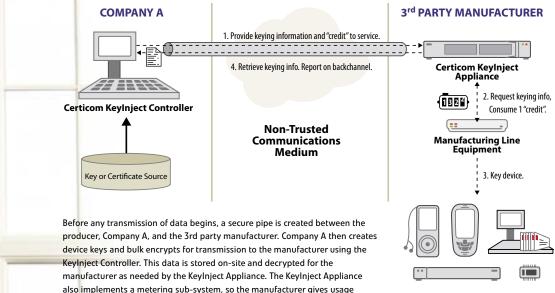
Certicom Keylnject can be used to transport and inject keys and certificates in conditional access and digital rights management (DRM) schemes such as HDCP (High-bandwidth Digital Content Protection), CPRM (Content Protection for Recordable Media), and other emerging consumer electronics standards. In these situations, unique keying material is embedded in a device to control access to streaming media and the usage of downloaded electronic files.

reports in exchange for "credit" to continue device production.

highly configurable

The ability to customize the interface and integrate it with the manufacturing line system enables Certicom Keylnject to address multiple deployment options. This flexibility also enables enhanced capabilities.





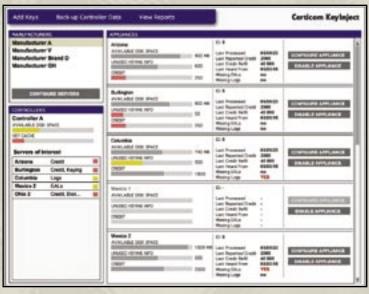
Certicom Keylnject Modules

The key components in the Certicom Keylnject offering include:

- Certicom Keylnject Controller Trusted key management and reporting system for producer site
- Certicom Keylnject Appliance Trusted key injection and metering for manufacturer site
- Key Source Custom key generation or load third-party keys
- Customization Services Interface to manufacturing line equipment

Cipher Suites	Transport	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
	Bulk storage	AES_128_WITH_SHA_256
Cryptographic Service Provider	Certicom Security Builder Crypto running within an Eracom ProtectServer Orange HSM.	
Hardware Security Module	Eracom ProtectServer Orange, Model PL-50.	
Key Protection Modes of Operation	Addressable cryptographic identity transport. Sequenced 3rd-party key transport. On-device cryptographic identity generation and binding.	
Transport Modes of Operation	Networked - Network Transport using TLS. Offline – Secure file based transport using DVD-RAM.	
Supported Third-Party Key Types	HDCP, CPRM, OMA DRM 2.0, ECC, Point-Compressed ECC, AES and other legacy key types.	

Quickly view status of your system with Certicom Keylnject



The simplified web interface makes it easy for you to configure an appliance, view the status of an appliance, or meter a specific manufacturer and request reports.

about certicom

Certicom protects the value of your content, applications and devices with security offerings based on Elliptic Curve Cryptography (ECC). Adopted by the National Security Agency (NSA) for classified and sensitive but unclassified government communications, ECC provides the most security per bit of any known public-key scheme. Visit www.certicom.com.

