certicom™
securing innovation

Certicom Security for Silicon Design Protection

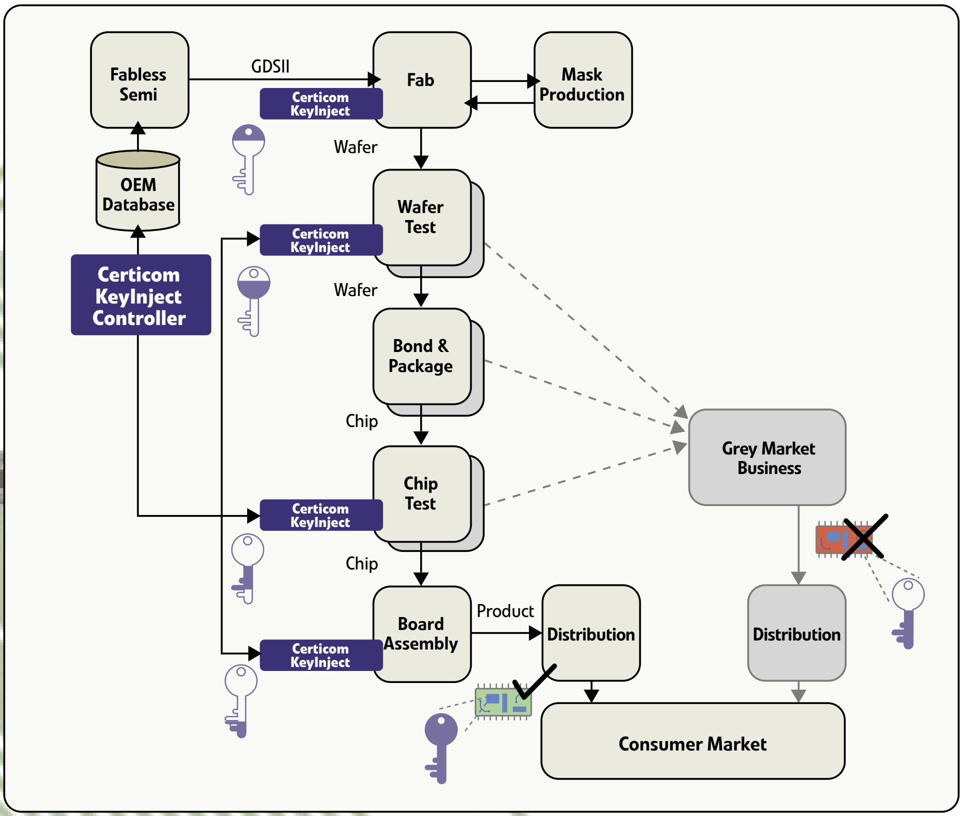
making low-cost silicon foundries as reliable as high-priced alternatives

Semiconductor companies increasingly outsource manufacturing in order to improve bottom line profitability and to remain focused on core competencies. Since manufacturing costs make up the largest part of chip production expenses, fabless semiconductor design companies can save millions of dollars per chip design by using low-cost foundries overseas. Unfortunately, concerns about exposure to fraud make it risky.

Certicom Security for Silicon Design Protection enables fabless semiconductor design companies to protect valuable IP at every stage of the production process. By adding a manufacturing security system with sophisticated hardware blocks to chip designs, fabless design companies can defeat gray markets and make low-cost foundries as reliable as high-priced alternatives.

protect your IP

By combining software-based Certicom KeyInject with hardware-based IP cores, security is extended right to the silicon. Additionally, Certicom uses government-rated, tamper resistant Hardware Security Modules (HSMs) to protect key and logging data every step of the way, so designs are protected even in the most hostile environments.



Certicom Security for Silicon Design Protection can be used at every touch point to provide the highest level of security in the chip production process.

eliminate gray market threats

Gray market sales cost IT manufacturers up to $5 billion in lost profits. Certicom Security for Silicon Design Protection forces checks and balances throughout the silicon manufacturing process. Chips produced outside the established path simply won't work, eliminating the gray market profit motive for overproduction or yield misrepresentation.

gain control over the production process

Certicom Security for Silicon Design Protection facilitates the monitoring of third party manufacturing by embedding a unique, valid encryption key into each chipset. This allows tracking of remote production through metering and retrieval of traceable audit trails from each subcontractor.

increase bottom-line profitability

Knowing that Certicom technology provides the security needed to instill trust, fabless semiconductor manufacturers can choose less expensive contract manufacturers, thereby lowering product costs.

Features

The key components of Certicom Security for Silicon Design Protection:

- **Certicom KeyInject Controller** – Trusted key management and reporting system for producer site
- **Certicom KeyInject Appliance** - Trusted key injection and metering for manufacturer site
- **Customization Services** - Interface to manufacturing line equipment
- **Production Control Core (PCC) –** locks and unlocks chip design

Certicom KeyInject Specifications

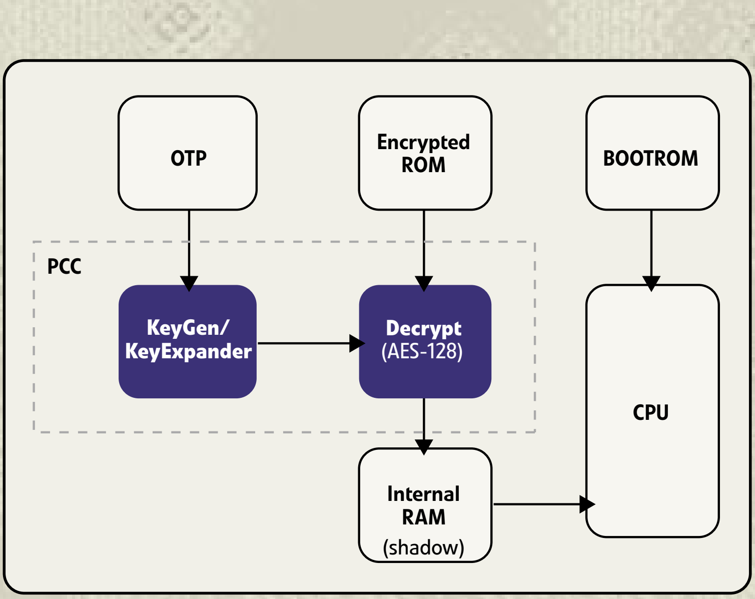
Cipher Suites	Transport	TLS_ECDH_ECDSA_WITH_AES_128_CBC_SHA, TLS_ECDH_ECDSA_WITH_AES_256_CBC_SHA
	Bulk storage	AES_128_WITH_SHA_256
Cryptographic Service Provider	Security Builder® Crypto™ running within a FIPS 140 rated HSM.	
Hardware Security Module	a FIPS 140 rated HSM	
Transport Modes of Operation	Networked - Network Transport using TLS. Offline – Secure file based transport using DVD-RAM.	

Production Control Core Specifications

At each step in the chip manufacturing process, Certicom KeyInject is used to inject key information into the OTP (One Time programmable memory). At power on reset, the KeyGen/KeyExpander combines this keying information to derive a single key, which is then fed into the AES decryption block and used to decrypt data and instructions from encrypted ROM. If the chip has followed the defined manufacturing process, it will function correctly, otherwise it will be crippled.

For More Information

For more information on the Certicom Security for Silicon Design Protection solution, visit www.certicom.com/fabless.



Note: Certicom PCC Core adds 20k gates (2 input NAND equivalent)

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.