

SECURITY: Design for Secure Manufacturing



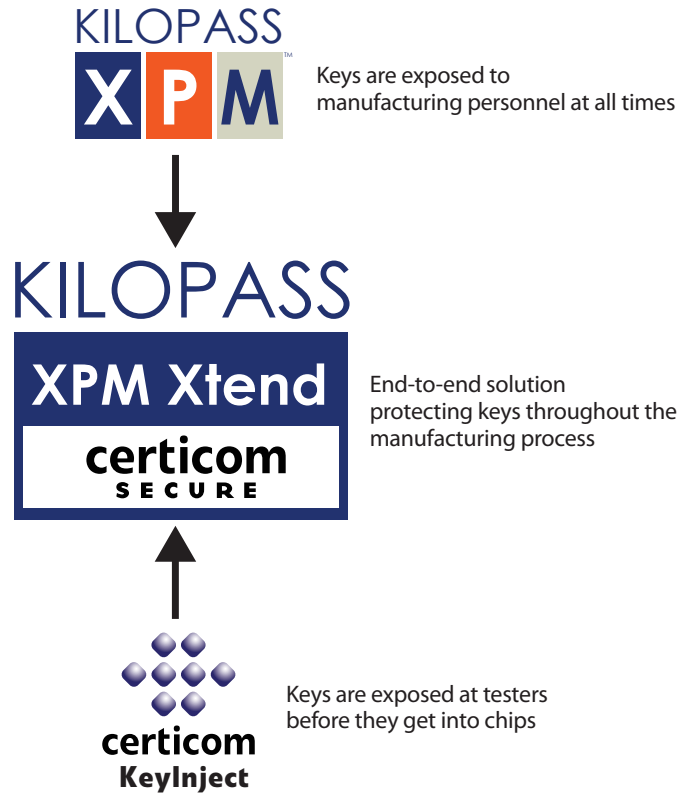
Kilopass XPM Xtend

XPM Xtend protects chip designs from IP theft and shields your company from liability claims. This is increasingly important for HDMI, DisplayPort, HD-DVD, and Blu-Ray licensees who are now liable for \$8 million for each licensed HDCP key exposed.

The likelihood of intentional theft or accidental exposure due to human error is high because so many people are involved in the manufacturing process. Whether intentional or not, a company is still held responsible and liable for any key exposed.

By seamlessly integrating hardware RTL with Kilopass XPM in the chip design and Certicom KeyInject on the factory floor, Kilopass delivers a comprehensive solution that protects keys at every phase of the manufacturing process.

XPM Xtend encrypts content protection licensed key data throughout the outsourced manufacturing process. As a result, no one can read protected keys, except the chip itself. Decryption of an HDCP key stored in XPM memory is accomplished by a static key that is embedded in the chip design. Certicom KeyInject, automates key distribution and further eliminates risk associated with manufacturing personnel. Keys are no longer visible or touched by anyone, at any time, or anywhere in the manufacturing process.



XPM Xtend Virtually Eliminates Concerns Relating To:

Key Theft By:

- Inside Employees
- Outsourced Test Sites
- Intermediaries
- Untrusted Chip Testers

Human Error By:

- Accidental Key Re-Use
- Lost Key Files

Liability Due To:

- Flaws in Cryptographic Design and Implementation
- Flaws in Proprietary Secure Key Storage Schemes
- Claims You Didn't Follow Best Practice

XPM Xtend integrates seamlessly with Certicom KeyInject infrastructure that automates and secures manufacturing of HDCP keyed chips. For more information, see Certicom KeyInject product sheet.

XPM Xtend - Designed For Secure Manufacturing

Given the \$8 million per key liability for HDCP licensees, companies are re-evaluating whether an in-house key management system provides sufficient protection. Not only does building a reasonably secure tracking system consume valuable NRE and operations capacity, most still include manual processes like FTP sites and email that make costly mistakes more likely than a fully automated solution that is tightly integrated with existing systems.

XPM Xtend is able to solve this problem on the factory line because Certicom KeyInject automatically protects and delivers keys to chips with embedded XPM Xtend technology.

Whether HDCP or other key types are being sent, XPM Xtend keeps keys private, even from shared ATE resources.

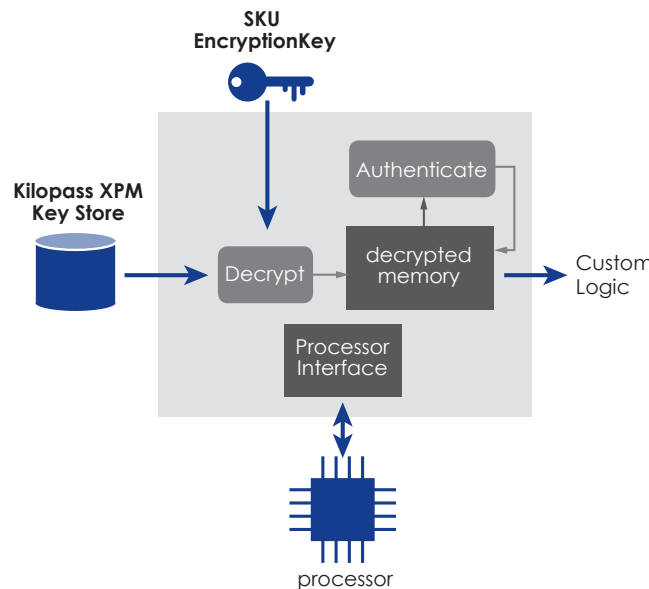
As a result, liability issues relating to key management and company secrets are protected down to the firmware - from company headquarters right to the chips being produced at offshore locations around the world.

Proven Technology - Greater Than The Sum of Their Parts

The world's leading chip manufacturers already rely on Certicom technology to automate key logistics, diminish liability, improve tracking, and reduce costs relating to offshore chip manufacturing and silicon testing. Likewise, many of Kilopass' customers are using XPM non-volatile memory technology to securely store HDCP and other encryption key information. By pre-integrating Certicom technology into Kilopass XPM, a new product - XPM Xtend - emerges to provide Kilopass customers an additional layer of security not available previously. XPM Xtend offers security conscious customers significant ROI within the first year of production.

Kilopass XPM Xtend Key Features:

- Enabled on power-up or via external processor control
- Customizable memory and processor bus widths
- Works with various system clock frequencies
- 35K gates and 200MHz (TSMC 90nm G)
- Key encryption cipher: AES-128
- Key authentication algorithm: CMAC using AES-128
- Supported by Certicom KeyInject for automated key logistics



What customers are saying -

"After evaluating a number of alternatives, we chose Kilopass' XPM memory technology since it provides the best standard logic CMOS solution for our secure software storage."

— Rudy Bruce, EVP of Marketing and Sales, BITMICRO Networks