



certicom

securing innovation

**protect your content,
applications and devices**

with government-approved security



Enhanced Protection of HDCP Keys in Manufacturing

Bill Lattin
Chief Technology Officer

About Certicom

- Founded in 1985 by Dr. Scott Vanstone, University of Waterloo
- 120+ employees
- Offices in Toronto, San Francisco, Washington DC, Ottawa & London (UK)
 - New sales presence in Asia Pacific and Israel
- 350+ Patents/Patents Pending based on Elliptic Curve Cryptography (ECC)
- License software products, patents & services to OEMs who require secure solutions

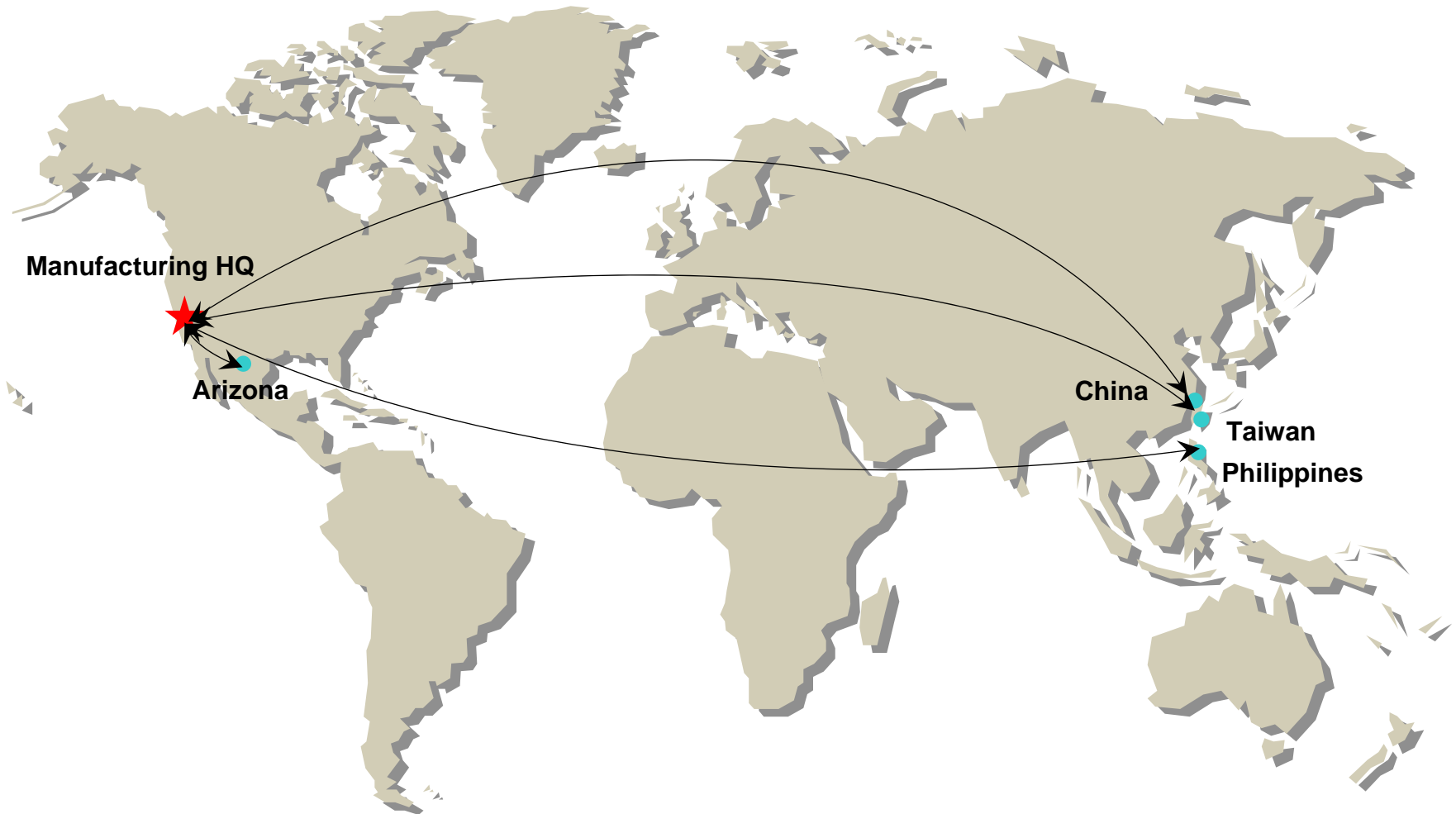
Importance of Security for Keys

- Keys need to stay secret, if not then:
 - Digital media can be stolen
 - Confidential messages can be read
 - People can pretend to be someone they are not
 - Products can be **copied or counterfeited**
- If secret keys are being sent to outsiders and contractors
 - Does the contract company operate in another country?
 - Are the other country's laws adequate to protect the keys/enforce contracts?
 - How easy is it to **bribe** contractor's employees, given the country's economic conditions and infrastructure?
- Secret keys can also be compromised/misused by accident
 - I.e. Same key programmed twice by accident - very common

Manufacturing Risk to HDCP Security

- Secrecy of HDCP keys at risk due to poor security during manufacturing
 - Content protection specifications (HDCP, DPCP) are requiring secure manufacturing
 - No specific guidance on how secure manufacturing is to be performed
 - Key reuse
 - Hackers
 - Storage of key data
 - HDCP \$1M-\$8M **Liquidated Damages**, not covered by traditional insurance policies for insecure manufacturing

How to Secure Global Manufacturing?



Steps to Mitigate the Manufacturing Stage Risk

- Protect contents of key CD while still under your control
- Never expose keys until they are burned into the chip or device
- Collect and protect records of every key consumed
- No impact to existing manufacturing throughput
- Coordinate distribution of keys to all of your manufacturing sites

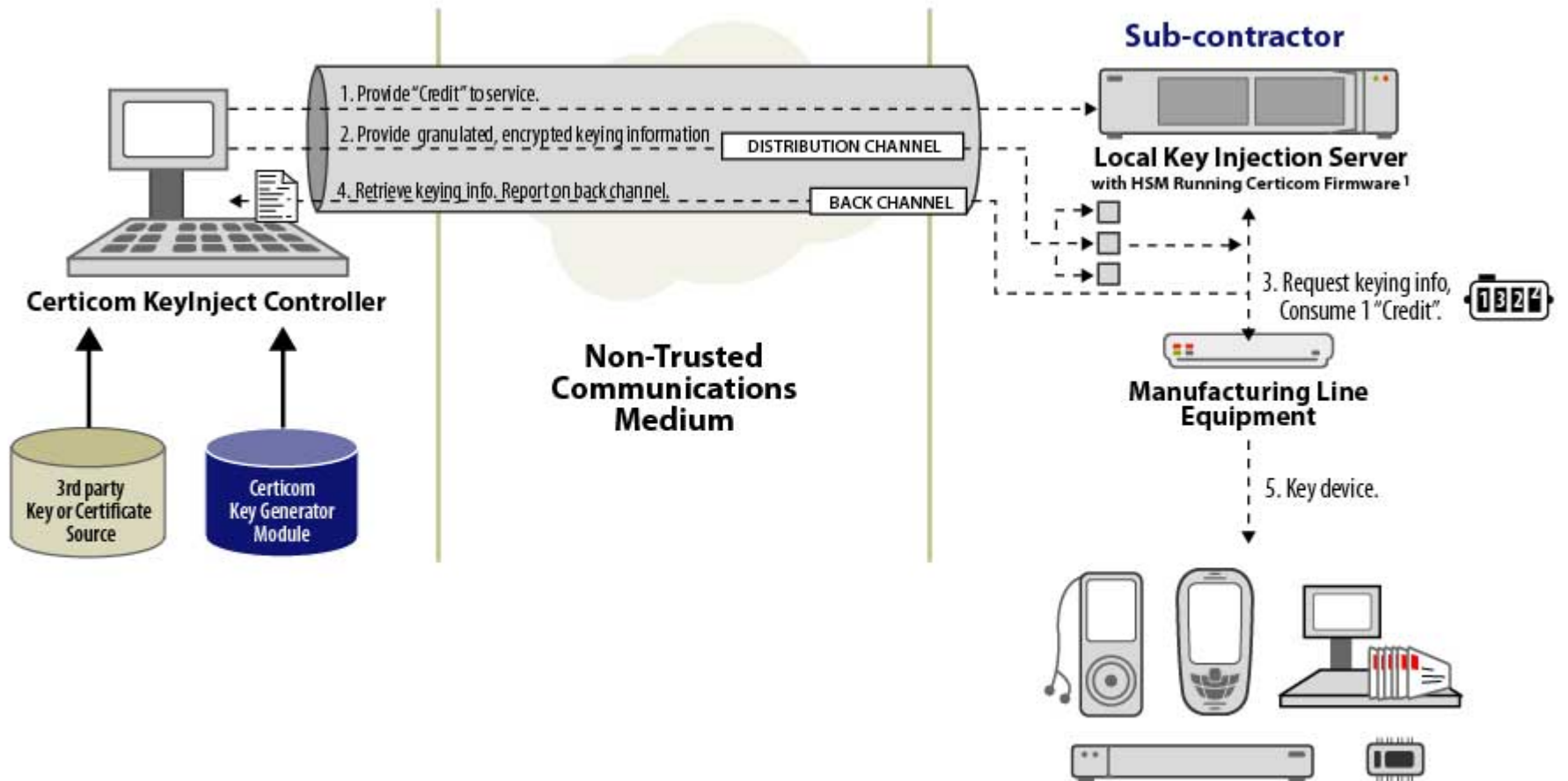
What is KeyInject?

- A cryptographic key distribution system for device manufacturers
 - Device manufacturing factories
 - Silicon foundries
- Value Propositions:
 - **DRM & CAS Protection** – Protects DRM and Conditional Access System keys during vulnerable manufacturing stage
 - **Logistics/Automation** – Getting factory workers to put unique data into mass produced parts is *really painful*, mistakes are often made!
 - **Gray Market Protection** – Need to watch and audit outsourced contract manufacturers

How Certicom KeyInject Works

1. Creates a secure pipe between producer and contract manufacturer
2. Producer holds device keys and bulk encrypts for transmission to the manufacturer
3. Bulk encrypted data is *stored on-site* and decrypted for the manufacture as needed
4. Hardware security module (HSM) used to protect decryption keys on-site and force usage reports
5. HSM implements metering sub-system, so manufacturer gives usage reports in exchange for "credit" to continue device production

KeyInject System Architecture



¹ equipment supplied by producer

KeyInject FDP Package

The KeyInject Factory Deployment Package is a turnkey drop-in offering high availability in a rugged mobile rack.



Certicom KeyInject – Proven Control

- Built using government strength cryptographic ciphers and tools
 - ECC and AES based solution
 - FIPS 140-2 Level 3 rated HSMs
 - Tamper reactive cryptographic hardware for factory floor
- Currently deployed by
 - ATI to protect HDCP keys
 - Used in multiple global factories
 - Plans for other protection standards
 - Other customers using for various proprietary media protection schemes

Contact Certicom

Bill Lattin

CTO

Certicom Corp.

650-242-8719

blattin@certicom.com

Brian Neill, CISSP

Product Manager

Certicom Corp.

905-501-3865

bneill@certicom.com



**protect your content,
software and devices**

with government-approved security