Certicom Security for Printer OEMs

preserving after market printer cartridge revenue

THE PROBLEM

A well-known sales and marketing rule is that existing satisfied clients are the easiest and cheapest market to pursue. With this thought in mind, companies designing and manufacturing printers have an opportunity to create an ongoing revenue stream that lasts a printer's lifetime by providing replacement ink cartridges to their established clientele. Over the span of several years, the replacement cartridge sales can easily eclipse the initial sale price of the printer itself.

An obstacle to realizing the full revenue potential for cartridge revenue stream is competition from aftermarket cartridge suppliers. Although patent protection provides some relief, aftermarket suppliers ingeniously circumvent copyrights and patents, leaving the original company significantly short of expected revenue.

Policy	Solution
Provide enhanced user experience through reliability	*Code-sign firmware and preclude malicious alteration*
Provide enhanced ecological material reuse through licenced remanufacturing	*Users receive significant monetary incentive to recycle cartridges which can be controlled through licenced remanufacturing creating a profitable ecosystem*
Provide branded Quality Assurance of remanufactured cartidges	*Authenticate remanufactured cartridges*
Support Intellectual Rights and Patent enforcement of technology through the application of security to preclude cloning	*Even if third party cloner is willing to risk infringement, security will close the gap.*
Secure available printer features to legitimate customers	*A printer core may have a superset of features, not all of which may be enabled for all markets. Printers can be "feature upgradeable" through ordering, paying for and received digital keys that enable conditional access to enhanced features.*
Some combination of the above example policies	*Protect the revenue eco-system and investments, provide a mechanism to enact regulatory policies, and allow flexibility to achieve price/feature point flexibility with common printer core engines.*

Potential security solutions to common problems facing printer OEMs.

THE SOLUTION

Due to price points required by the market, cartridges are necessarily tightly cost-controlled, especially as there is an expectation to license 3rd party manufacturers to mass produce the devices. Therefore, any potential solution must carefully balance production unit cost parameters against the level of difficulty of cloning cartridges.

An optimal solution must balance several design considerations:

- **What is the incremental unit cost of cartridge?**
- **Should there be one appropriate security model, or a gradated solution depending on hardware resources and revenue stream to be protected?**
- **How feasible is the design including integration with manufacturing partners, specialty IC manufacturers and 3rd party cartridge manufacturing licensees?**

In balancing production unit costs against the level of difficulty of cloning cartridges, achieving "perfect security" is economically infeasible – the optimal solution must provide "enough" security at an acceptable incremental unit manufacturing cost.

Certicom has significant experience developing anti-cloning and conditional access systems. Using public key technology, you can make the life of an aftermarket copycat very difficult by creating software mechanisms to:

- **provision a unique manufacturer's digital signature for each cartridge**
- **have the printer authenticate the cartridge's unique digital signature**
- **have the printer optionally challenge a "smart" tamper-proof cartridge for validity**
- **provide for other means of intelligence in the printer to ascertain illegitimate print cartridges**

Certicom uses innovative cryptography techniques that:

- **minimize the digital signature size (less than 200 bits)**
- **maximize the signature strength and prevent "cracking" of the secret manufacturer's key**
- **protect secret keying material through tamper resistance**
- **minimize performance impacts**

Certicom tools integrate into the manufacturing environment, offering:

- **a streamlined process that generates keys and serial numbers, signs information with a certificate, injects the information into ROM or silicon**
- **a system for protecting the key generation process from insiders and licensed third parties**
- **a system to allow manufacturers and licensed third parties to re-authorize refurbished cartridges**

THE IMPLEMENTATION

Our industry-leading Security Builder® developer toolkits can be used to create an anti-cloning solution, by examining the capability of the printer and cartridge to incorporate the following behavior:

The printer cartridge must be capable of holding some cryptographic data (ideally in the dozens of bytes)

- Certicom's ECC-based public key and digital signatures can be as small as 20 bytes.

The printer will have to contain appropriate software that can interrogate the cartridge and ascertain if

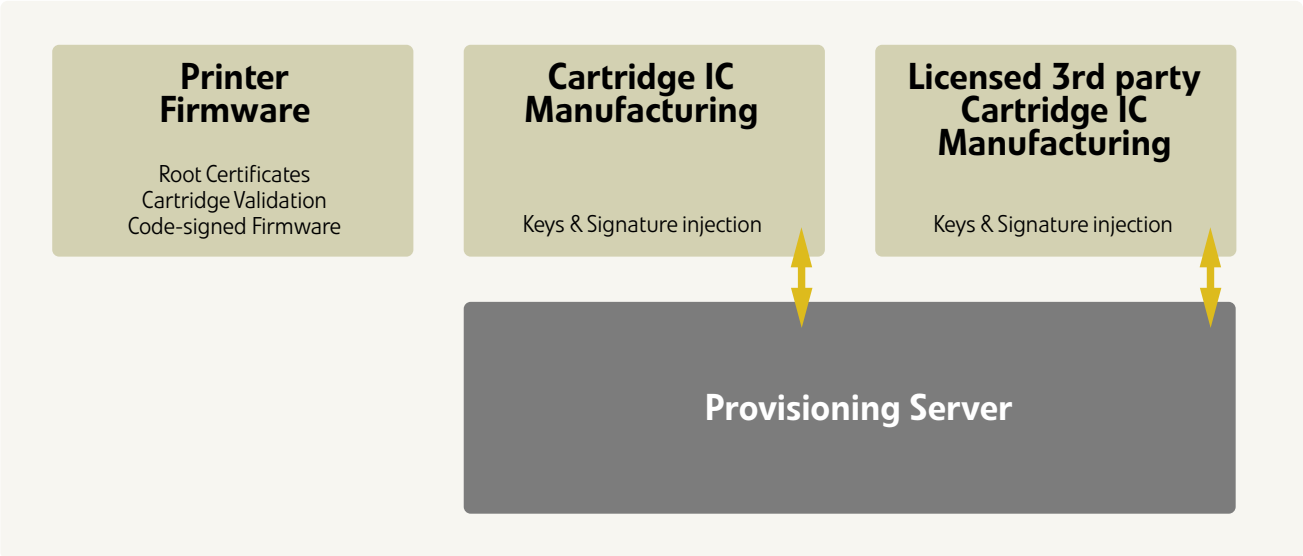
- a digital signature exists and;
- the digital signature maps to the information data within the cartridge (i.e. is a valid signature).
- Alternatively, "smart" cartridges could digitally sign challenges from the printer.

The cartridge includes irreversible (i.e. one-time programmable) bits that can be used as "state" information, and be programmed by the printer, for example:

- The manufacturer denotes the print cartridge as refill number "n". If "n" is zero, the print cartridge is marked as "new".
- When the printer examines the cartridge, it reads the "new" bit and other information bits, then marks the cartridge as "in use".
- The cartridge bits are irreversibly marked to reflect the state of the cartridge becoming empty.
- Refurbished cartridges can only be re-authorized by licensed third parties.

The printer firmware software contains

- The manufacturers root certificate and certificate chain for the cartridge.
- The ability to validate a digital signature directly or through a challenge response.
- A code-signed image to protect against malicious firmware upgrades.



Printer Anti-cloning Manufacturing Process

Given the print cartridge and printer's suitability for anti-cloning capability, Certicom can adapt its Security Builder developer toolkits into a solution that provides software libraries featuring:

- **a signing function for inclusion in the manufacturing systems that can accept data from the cartridge, sign it, and output for programming into the cartridge**
- **the ability for smart printer cartridges to sign challenges from the printer in a tamper resistant IC module**
- **a signature validation function for placement in the printers**
- **the optimal cryptographic functionality given the constraints of the printer and cartridge system**
- **code-signing for the printer firmware**
- **threat and risk assessment for different anti-cloning solutions based on cost**

SUMMARY

Certicom offers the OEM printer manufacturer a means to significantly increase revenue by employing Certicom's industry-leading technology to shut out aftermarket companies or legitimately license them.

In a broader sense, Certicom has the tools and expertise to enact and enforce policy decisions of the printer manufacturer.

---

about certicom

Founded in 1985 with a long-term focus on Elliptic Curve Cryptography, Certicom has been awarded over 500 patents. As a leader in applied cryptography and key management, Certicom provides managed PKI, key management and provisioning technology that helps to protect customers' device firmware, applications, and long-lived assets. Certicom is a critical element of the Blackberry cybersecurity portfolio deploying the first and best in class end-to-end security solutions used in preventing product counterfeiting, re-manufacturing, and rogue network access. Blackberry Certicom's secure key provisioning, code signing and identity management solutions are field- proven to protect next-generation connected cars, critical infrastructure and IoT deployments.