Securing RFID

ECPVS enables decentralized product authentication and consumer privacy

A Certicom White Paper
February 2007

certicom™

Table of Contents

certicom™

Executive Summary

Driven by government legislative requirements aimed at securing the integrity of the US healthcare system, the pharmaceutical industry has been piloting trials of Radio Frequency Identification (RFID) tag technology as a way to secure the prescription drug supply chain. Beyond meeting emerging legislative requirements, like the California e-Pedigree certification needed starting on January 1st 2009, RFID track and trace trials have strong commercial promise to reduce counterfeit drugs and boost supply chain efficiency.

It is widely believed that the pharmaceutical pilots will lead the way to widespread deployment of Item-Level Tagging (ILT), with the technology diffusing to other industries where product authentication and privacy are important.

As these pilots progress, it is becoming increasingly clear that e-Pedigree efforts suffer from two fundamental flaws. First, implementation of this method will be very costly and it will take several years to build the needed infrastructure. Second, the e-Pedigree method does not secure the entire supply chain. For instance, the secondary wholesale distributor level remains vulnerable to counterfeiting.[1]

For this reason, leading companies are exploring proven product authentication solutions that rely on digital signatures. Product authentication solutions secure the entire supply chain and can be deployed immediately, without requiring a significant change to existing infrastructure.

The crux of the matter is this: a centralized, always-on network based authentication scheme adds significant cost and complexity to RFID authentication. Also, even an always-on network scheme needs a trusted back-up system for when the network fails and applications are offline.

For these reasons, organizations may want to consider a cost-effective approach that provides both item-level authentication and privacy in real-time, without requiring full-time access to a centralized tag database.

This whitepaper describes how a decentralized approach, based on Elliptic Curve Pintsov-Vanstone Signatures (ECPVS), extends the benefits of item-level tagging where online access is not possible or is cost-prohibitive. In addition, this paper will demonstrate how a decentralized approach augments online systems, increases flexibility, and boosts ROI.

[1] http://www.eweek.com/article2/0,1895,2072311,00.asp

http://news.zdnet.com/2100-3513_22-6143979.html

certicom™

Why Global Trade is Driving RFID Standardization

The US Department of Defense and Wal-Mart have both been early adopters of RFID tagging technology, championing RFID's role in supply chain management. And GS1, a leading global organization dedicated to the design and implementation of global standards and solutions to improve the efficiency of supply and demand chains, has established a group, EPCglobal[2], which is working to achieve worldwide adoption of electronic product codes (EPC). With a board of governors that includes representatives from leading manufacturers like Proctor & Gamble, Wal-Mart, Hewlett-Packard, Johnson & Johnson, and Dow Chemical, EPCglobal is trying to enable the supply chain to reap the benefits of RFID.

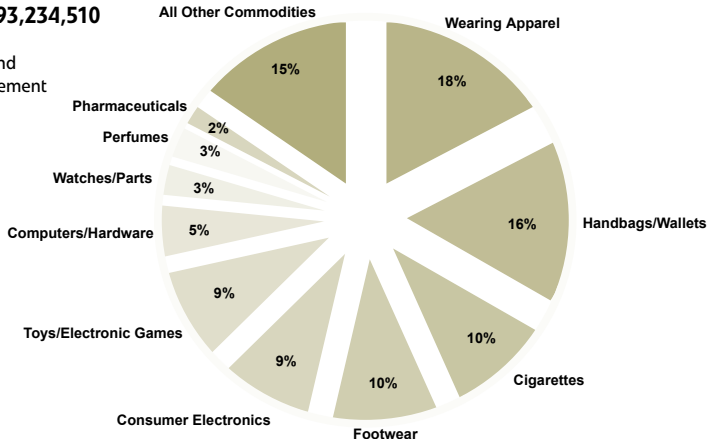
The EPCglobal Network system enables electronic supply chain management – track and trace of shipments at the container and pallet level, with a uniform electronic product code that can be used by OEMs, shippers, distributors, and retailers alike to manage the flow of product inventory.[3]

Challenges Posed by Global Piracy

Besides improving logistics and supply chain management, one of the major problems that EPCglobal has set out to address is the growing impact of counterfeit products. In 2005, the US Department of Homeland Security seized over $93 million dollars worth of products. It is assumed that this is merely a fraction of the total amount. Some research suggests that US companies lose more than $200 billion in revenue each year.[4]

For the most part, counterfeit products mainly impact a manufacturer's profitability by creating low-cost alternatives that consumers purchase in lieu of the genuine products. From the chart below, it's clear that this can cost a manufacturer millions in lost potential revenue. Worse, counterfeiters are not held to the same manufacturing standards as legitimate suppliers. As a result, they are a common source of shoddy, unreliable, and dangerous products that can damage a manufacturer's brand. Moreover, these counterfeit products pose a very real public safety risk -with pharmaceuticals a special concern.[5]

Total FY 05 Domestic Value: $93,234,510
Department of Homeland Security
U.S. Customs and Border Protection and
U.S. Immigration and Customs Enforcement



[2] To learn more about EPCGlobal, visit: http://www.epcglobalinc.org/about/faqs#8

[3] http://www.gs1.org/productssolutions/

[4] http://www.dnatecaus.com/counterfeit.htm

[5] For more details, http://www.usatoday.com/news/nation/2007-01-11-counterfeit-seizures_x.htm

certicom™

Mitigating Risk with RFID-Based Product Authentication

RFID tags mitigate the risk of counterfeit products in a fairly straight-forward manner, with a tag used to verify a product's origin. The unfortunate problem with RFID tags on their own is that data can easily be copied from one tag and written onto another tag. The good news is that copied data can be detected with an authentication system – a means to distinguish authentic tags and reject invalid copies. A couple of methods have been proposed for authenticating individual tags – one a centralized approach based on electronic databases, the other a decentralized approach based on digital signatures.

RFID Tagging and Privacy

In addition to product authentication, privacy is also an important issue to be addressed. It's a concern for the consumer, who may not wish to broadcast their Viagra purchases via the item-level tag. It's also an issue for the manufacturer, since they may want to prevent the detection and subsequent theft or product substitution with counterfeits somewhere in the supply chain. An RFID tag authentication system must ensure that only authorized devices can identify products.

Benefits and Limitations of a Centralized Approach

The centralized approach is quite simple in concept. It uses an on-line database such as the EPCglobal Network to provide an item-level tag pedigree service. The data from every product to be authenticated would be registered in a secure online database tying the unique tag ID to the product's unique 96-bit EPCglobal product identifier. Each item to be processed or authenticated could be found by accessing the online database to match the tag ID and EPC Number.

The major limitation of this methodology is that all tag readers and writers need to have online access to the centralized database. The additional equipment and effort required to build the needed infrastructure will necessitate an enormous - and unnecessary - drain on resources. Also, online access at the individual reader level adds significant cost to any pharmacy or retail authentication system. Retailers put business continuity at risk if they rely on Internet access for item-level tagging. For a large company such as Wal-Mart, with several thousand stores, even a small percentage of downtime can have a significant impact on the bottomline.

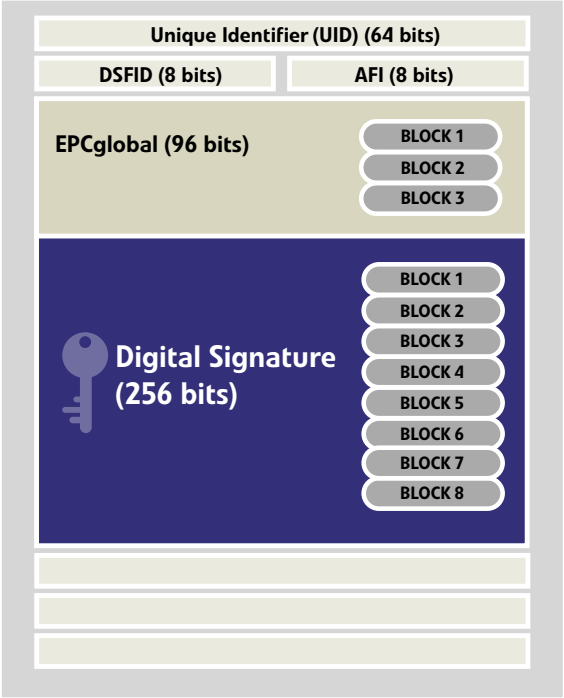
Privacy can certainly be addressed using the online database approach. In the pharmaceutical case, where the patient doesn't want their prescription broadcast, there's a simple solution. Rather than writing an EPC Product Class ID or National Drug Code (NDC) that can be read by any reader, the EPCglobal 96-bit Serialized Global Trade Identification Number (SGTIN) written on the RFID tag can be used to retrieve data from the online database. The SGTIN specification can be used to track the item type right down to a specific serial number. Once again, the infrastructure requirements for online access add cost, since the item must be first registered in the database, and then later the RFID reader must go online to retrieve it.

Aside from cost constraints, accessing online information is sometimes itself undesirable because the act leaks information. If RFID tags are used to authenticate weapons systems components, for instance, accessing a pubic database may cause security vulnerabilities.

certicom™

The Benefits of a Decentralized Approach

The decentralized alternative to RFID-based product authentication involves the use of digital signatures such as the signatures used to sign SSL certificates for web servers. Digital signatures are akin to unique, certified data fingerprints – they allow each tag, and hence each item-level product, to be authenticated. All that's needed to authenticate any tag is the public key from the signing key pair.



This diagram illustrates how digital signatures can be applied to a 2048-bit RFID tag - a typical device used for data storage.

The digital signature is generated on the concatenation of the UID and the EPCglobal number. Though the signature on such a tag can be read from a genuine tag and programmed into another one, the copy cannot be verified successfully, since the UIDs of the tags are unique and cannot be reprogrammed. Thus the digital signature serves as proof of an authentic product.

The benefit of the digital signature approach to authentication is that verification is an off-line process. It requires only that each reader has possession of the verification key – i.e. the public key corresponding to the tag's signature.

RSA signature size makes them impractical for product authentication. The signature size prevents multiple signatures from being used on the same tag. In some instances, being able to add multiple signatures can help ensure authentication throughout the supply chain.

The Elliptic Curve Pintsov-Vanstone Signature (ECPVS) scheme is a digital signature scheme with message recovery. That is, part of the message that was signed can be recovered from the signature verification process. An ECPVS signature is significantly smaller than a comparable RSA signature – about 1/3rd the size and signs 3 times as fast. It is also about half the size of an Elliptic Curve Digital Signature Algorithm (ECDSA). The message recovery feature can be used in an item-level tag because ECPVS can provide both authentication and privacy in a single off-line operation.

ECPVS can be used sign an RFID tag and verify it using a reader with the corresponding public "verification" key. At the same time it can hide the Product Class ID from unauthorized readers without a verification key.

Strong and efficient, ECPVS is ideal for RFID item-level tagging. A tag requiring the same security level as one signed with a 1024 bit RSA signature requires only 352 bits of storage, including the 96 bit EPCglobal ID and the 20 bit Product Class ID that the ECPVS operation is encrypting. Since memory size impacts die size, saving memory reduces the cost of the RFID tag. Further, the faster signature operation of ECPVS increases the signing speed by a factor of three! Scaling to higher security levels give ECPVS an even more impressive advantage.

	EPC Number (bits)	Digital Signature (bits)	Total (bits/Memory)
RSA – 1024 bits	**96**	**1024**	**1120**
ECPVS – 160 bits (part of IEEE 1363a)	**96**	**256**	**352**

- ECC based security for EPC saves 2/3 the space of RSA
- Other applications may save up to 3/4 the space
- Also offers encryption above and beyond RSA to hide the Product Class ID

Using ECPVS, distributors and pharmacies can realize process efficiencies by having sensitive product data available on the tag for smart-shelf inventory management, without needing to access a centralized information system.

In addition, because of the reduced storage requirements, it is also feasible to use ECPVS to concatenate multiple signatures on the same tag. This feature can be used, for example, to authenticate the chain of custody for products such as sensitive equipment which might be handled in an arena where on-line access is not available.

A 2k tag using ECPVS could hold up to 7 signatures. This would enable individuals and organizations throughout the supply chain to verify authenticity and confirm their responsibility for the e-pedigree at any stage of distribution. This would enable trace capabilities at any stage of the supply chain. And it could be done directly from the tag, as opposed to having to acquire and review variety of shipping documents.

THE KEY BENEFITS OF ECPVS

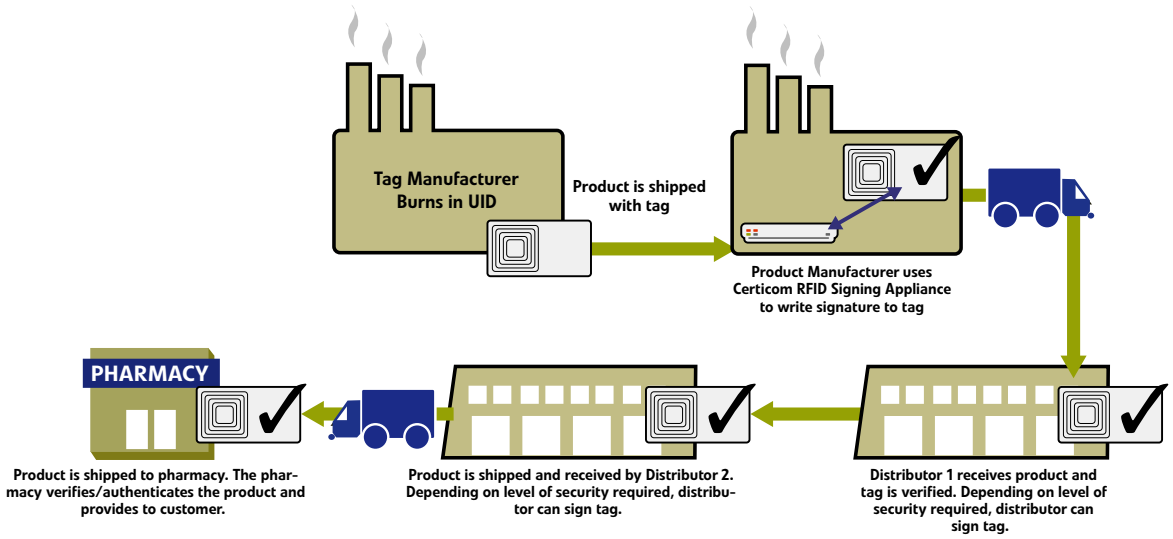
- 1/3 the size of a 1024 bit RSA signatures for product authentication
- 3 X faster signing speed
- Off-line operation enables functionality, like smart-shelves, for off-line product interrogation
- Privacy: hides Product Class ID from unauthorized readers
- Multiple signatures can be applied to one another. allows each node in supply chain to sign tag
- Standards-based
- Proven technology already used to secure the postal system

Certicom Security for RFID Product Authentication

Certicom Security for RFID Product Authentication uses standards-based and proven cryptographic protocols for its RFID appliance, including a standardized public-key cryptography scheme, ECPVS. This efficient ECC-based digital signature scheme enables a high level of security to be added to a RFID tag or reader without requiring a lot of computing power and storage. In fact, a 160-bit ECC key provides the same level of protection as a 1024-bit RSA key, but its digital signature is approximately 1/4th the size – and when it is used to provide security for EPCGlobal, ECC saves 2/3rd the space as compared to RSA at comparable strength.

Certicom Security for RFID Product Authentication includes an Authentication Agent and an RFID signing appliance.

The Certicom Security for RFID Product Authentication Architecture



Certicom RFID Signing Appliance

Digital signature schemes rely on keeping the private key of a public/private key pair secret and sharing the public key. In the item-level tagging scheme this requires drug manufacturers to maintain control over their private signing keys and how they are used. Doing so prevents unauthorized production of authentic tags. An authentic tag is an authentic product.

Item-level tag signing in a high speed production environment requires a robust security design. An appropriate high-assurance solution requires a chain of trust and custody for the signing key and appropriate control and monitoring of its use. Best practice indicates the use of a FIPS 140-2 level 3 Hardware Security Module (HSM) as part of the tag signing system. The HSM, in turn, needs to interface with both the RFID printers which are writing the actual tags, and with the manufacturing workflow. In essence, what is required is a secure tag signing station that can operate at production line speeds.

certicom™

Certicom RFID Authentication Agent

In order to authenticate the RFID tags, readers need to employ an authentication agent that can verify each ECPVS signature and recover the encrypted Product Class ID. The agent needs access to a copy of the verification keys–the public keys linked to the signing process. Of course, in order to ensure that privacy is maintained, only authorized agents should have access to verification keys and the keys should be securely managed.

Each authentication agent is able to read the tag signature and select the appropriate verification key from its internal database using a cleartext portion of the EPCglobal number. In compressed form, each key occupies 22 bytes, so a reader can store 5000 keys in only 110KB of memory.

While it's simple to think of the agent as part of a standalone reader, an agent is in fact middleware which can readily be integrated into IT infrastructure or in a standalone device.

To learn more about Certicom Security for RFID PRoduct Authentication**, watch the multimedia presentation or read the following articles.**[6]

Conclusion

Commercial industries and government agencies face a number of issues – anti-counterfeiting, theft, grey market competition, brand integrity, liability, inventory control, supply chain inefficiencies, privacy concerns, and government mandates – that can be solved with a RFID solution that guarantees product authenticity and keeps unauthorized individuals from viewing product information.

Two methods have been proposed for authenticating individual tags – one a centralized approach based on electronic databases and a decentralized approach based on digital signatures. The primary limitation of a centralized approach is the significant costs to implement and the lack of a back-up system for when connectivity is lost. By contrast, a decentralized approach that uses ECPVS enables distributors and pharmacies to realize process efficiencies that bridge the gap between pallet level supply chain management and item-level authentication. By making sensitive product data available on the tag inventory management can take place without the need to access a centralized information system. As a result, authentication and verification can be done with low cost, portable readers that can work off-line - thereby speeding up operation, ensuring product authenticity, and protecting end-user privacy with a cost-effective system that won't require significant changes to existing IT infrastructure.

Certicom Security for RFID Product Authentication enables both on-network as well as off-network functionality, while addressing critical infrastructure, privacy, security, and efficiency requirements for the pharmaceutical, medical supply, cosmetics, machine peripherals, document management, and collectables industries.

[6] Video Presentation:
http://www.certicom.com/rfiddemo

RFID Journal:
http://www.rfidjournal.com/article/articleview/2816/1/1/

Supply & Chain Executive:
http://www.sdcexec.com/online/article.jsp?id=8893&siteSection=29

certicom™

References

http://www.dnatecaus.com/counterfeit.htm

http://www.cbp.gov/linkhandler/cgov/import/commercial_enforcement/ipr/seizure/fy05_midyear_stats.ctt/fy05_ipr_midyear.pdf

Combating Counterfeit Drugs: A Report of the Food and Drug Administration Annual Update, May 18, 2005, page 1. Available at http://www.fda.gov/bbs/topics/NEWS/2005/NEW01179.html

Securing the Pharmaceutical Supply Chain with RFID and Public-key infrastructure (PKI) Technologies; By Joseph Pearson; Texas Instruments RFid Systems

http://www.informationweek.com/story/showArticle.jhtml?articleID=60402017

"Authenticated RFID Reference Guide", Texas Instruments, 3M and VeriSign, Draft ver.4.0, August 2005.

"Guide to Elliptic Curve Cryptography", D. Hankerson, A. Menezes and S. Vanstone, Springer-Verlag, 2004.

"Recommendation for Key Management – Part 1: General Revised", NIST Special Publication 800-57, National Institute of Standards and Technology, May 2006.

"Digital Signature Standard (DSS)", FIPS PUB 186-2, U.S. Department of Commerce/National Institute of Standards and Technology, January 2000.

"Annex A: Approved Security Functions for FIPS PUB 140-2, Security Requirements for Cryptographic Modules", FIPS PUB 140-2 Annex A, National Institute of Standards and Technology, April 2006.

"Public Key Cryptography for the Financial Services Industry - The Elliptic Curve Digital Signature Algorithm (ECDSA)", ANSI X9.62, American National Standards Institute, 2005.

"IEEE Standard Specifications for Public Key Cryptography – Amendment 1: Additional Techniques", IEEE Standard 1363a-2004, The Institute of Electrical and Electronic Engineers, March 2004.

certicom™

Additional Certicom White Papers

To read other Certicom white papers, visit www.certicom.com/whitepapers.

Sum Total: Determining the True Cost of Security
Sourcing Security: Five Arguments in Favour of Commercial Security Solutions

Government

Making the Grade: Meeting Government Security Requirements (Suite B)
Meeting Government Security Requirements: The Difference Between Selling to the Government and Not
FAQ: The National Security Agency's ECC License Agreement with Certicom Corp.

Mobility

The Inside Story
Many Happy Returns: The ROI of Embedded Security
Welcome to the Real World: Embedded Security in Action

Sensor Networks

Securing Sensor Networks

DRM & Conditional Access

Injecting Trust to Protect Revenue and Reputation: A Key Injection System for Anti-Cloning, Conditional Access and DRM Schemes
Achieving DRM Robustness: Securing the Device from the Silicon Up to the Application(PDF)

Enterprise Software

Using Digital Signatures to cut down on Bank Fraud Loss

ECC

An Elliptic Curve Cryptography Primer
ECC in Action: Real World Applications of Elliptic Curve Cryptography
Using ECC for Enhanced Embedded Security (PDF)

certicom™

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.

Contact Certicom

Corporate Headquarters

5520 Explorer Drive, 4th Floor
Mississauga, Ontario L4W 5L1
CANADA
Tel: +1-905-507-4220
Fax: +1-905-507-4230
info@certicom.com

Sales Offices

Worldwide Sales Headquarters
1800 Alexander Bell Dr., Suite 400
Reston, Virginia 20190
USA
Tel: 703-234-2357
Fax: 703-234-2356
sales@certicom.com

Ottawa
349 Terry Fox Drive
Kanata, ON K2K 2V6
CANADA
Tel: 613-254-9270
Fax: 613-254-9275
sales@certicom.com

U.S. Western Regional Office
393 Vintage Park Drive, Suite 260
Foster City, CA 94404
USA
Tel: 650-655-3950
Fax: 650-655-3951
sales@certicom.com

Europe
Golden Cross House
8 Duncannon Street
London WC2N 4JF
UK
Tel: +44 20 7484 5025
Fax: +44 (0)870 7606778
mwersall@certicom.com

Engelska Huset
Trappv 9
13242 Saltsjo-Boo
SWEDEN
Tel: +46 8 747 17 41
Mobile: +46 733 100 900
Fax: +46 708 74 41 61
jgardelius@certicom.com

Israel
Atidim, POB 58019
Tel-Aviv 61580
ISRAEL
Tel: +972-3-648-4121
Fax: +972-3-647-8365
Mobile: +972-52-356-7478
gglazer@certicom.com

APAC
6-4-11-401 Minami Shinagawa
Shinagawa-ku
Tokyo 140-0004
JAPAN
sales@certicom.com

DongMyoung Bldg.
#202, 2nd Floor 165-7
SeokChong-Dong
Songpa-Gu
Seoul, Korea 138-844
KOREA
sales@certicom.com

www.certicom.com