certicom™

The Benefits of Digital Signatures for Reducing Bank Fraud Losses

An Overview of the Certicom Security Architecture for Check 21

February 2005

Introduction

Check 21 has the potential to save financial institutions over 2 billion dollars annually and to reduce the exposure to unexpected transportation disruptions. It eliminates the dependency on physical shipment of checks between financial institutions and accelerates clearing cycles.

However, replacing physical checks with electronic and physical reproductions of images raises a number of security concerns. How do you know the image is genuine? How do you know it has not been tampered with? What other problems are introduced when banks and their customers have to deal with substitute checks? How do you protect images that are archived temporarily or permanently (up to seven years) on various servers during the check process? How do you protect these images so that they will stand up to any internal or external malicious attempts to alter check images?

The method that solves these problems is digital signatures. Digital signatures have been used for several years in other areas of e-commerce to provide message and data integrity, authentication, and non-repudiation. Without digital signatures on a check images – all parties involved in the transaction do not have any proof of authenticity of the image, without comparing it physically to original document.

Digital signatures are recognized as legal equivalents to handwritten signatures in all 50 states, and most industrialized nations including Canada, UK, Australia, France, Germany, Singapore, and Japan. In the US, financial services organizations such as the American Bankers Association, BAI, VISA, and the Electronic Payments Forum have been encouraging the adoption of digital signatures within electronic transactions.

The ANSI[1] *DSTU X9.37-2003 Specifications for an Electronic Exchange of Check & Image Data* standard provides the guidance for conformance for Check 21 images. X9.37 establishes the file sequences, record types, and field formats to be used for the electronic exchange of check MICR (Magnetic Ink Character Recognition) line, associated check processing data and check images in the form of cash letters. X9.37 includes fields for digital signatures, quality flags, and usability flags. The digital signature fields that are applied to a check image at the time of image capture provides indisputable authentication and non-repudiation of the original document, thus ensuring that all parties within the check processing system can rely and ultimately trust these electronic images.

This white paper will demonstrate why digital signatures should be applied to all check images at the time of image capture, how they reduce fraud and improve ROI, why and how elliptic curve cryptography is the best overall cryptosystem for digital signatures for Check 21, and how the Certicom Security Architecture for Check 21 provides the foundation to ensure security within the check processing system.

[1] The administration and conformity around standards in the United States is handled by the American National Standards Institute (ANSI). Within ANSI, there is a specific Accredited Standards Committee known as X9. The Accredited Standards Committee X9 (ASC X9) has the mission to develop, establish, maintain, and promote standards for the Financial Services Industry in order to facilitate delivery of financial services and products.

Risk in the Check 21 Process

The first basic exposure to risk is when both the paper item and its IRD are being processed through the system. Fraud filters already look for duplicate items between the IRD and original check document. However fraud filters usually have dollar review thresholds to control the volume of suspects that must be further examined. Duplicate items under that dollar amount will not appear on the report unless the filters are specifically tuned for duplicates to lower amount.

Typically, small IRDs that do not process cleanly are charged off without research. It is less expensive to charge an item off as a "miscellaneous operating loss" that it is to invest the time and energy to find the correct accounts to apply it to or even to return it.

Of greater concern is the risk that altered or completely fictitious IRDs will be introduced into the processing stream. Specifics on exactly how to create an IRD are readily available to the public, so producing legitimate looking IRDs is not difficult.[2] The software needed to modify check images is also readily available. The duplicate filters would not even catch these.

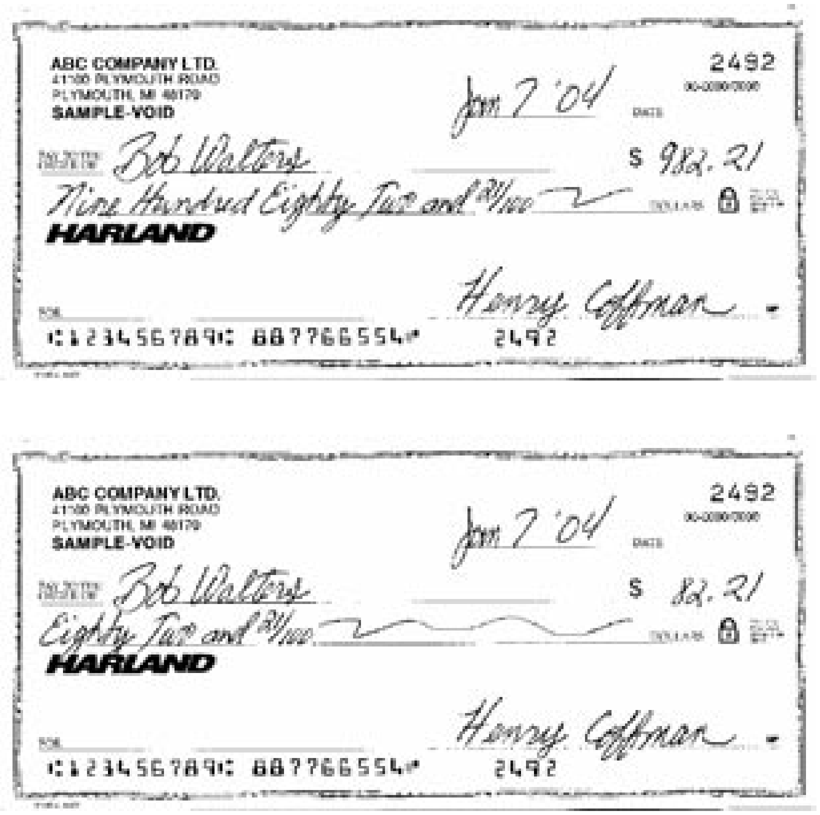
Not having access to the original item also creates several areas of risk for the bank. For corporate checks, the biggest risks involve counterfeiting, forgery, and alterations. Once checks have been converted to an image, unless a company uses a means of authenticating the check prior to acceptance, it will be very difficult to determine a counterfeit check from an authentic one, or even an altered check from a counterfeit.

Specific examples of these internal and external risks include:

[2] Check image files are created and stored in JPEG (Joint Photographic Expert Group) or TIFF (Tagged Image File Format) image formats. These image files can easily be altered using commercially available software.

Diminishing the Debit

This is when the X9.37 fields for the check amount are changed to a lower dollar value. This results in the payor being debited for less than the original check amount. The payor's bank is defrauded of the difference.



ABC COMPANY LTD.
41100 PLYMOUTH ROAD
PLYMOUTH, MI 48170
SAMPLE-VOID

2492
[illegible]

Jan 7 '04 DATE

PAY TO THE ORDER OF Bob Walters $ 982.21

Nine Hundred Eighty Two and 21/100 DOLLARS

HARLAND

FOR

Henry Coffman

⑆123456789⑆ 887766554⑈ 2492

ABC COMPANY LTD.
41100 PLYMOUTH ROAD
PLYMOUTH, MI 48170
SAMPLE-VOID

2492
[illegible]

Jan 7 '04 DATE

PAY TO THE ORDER OF Bob Walters $ 82.21

Eighty Two and 21/100 DOLLARS

HARLAND

FOR

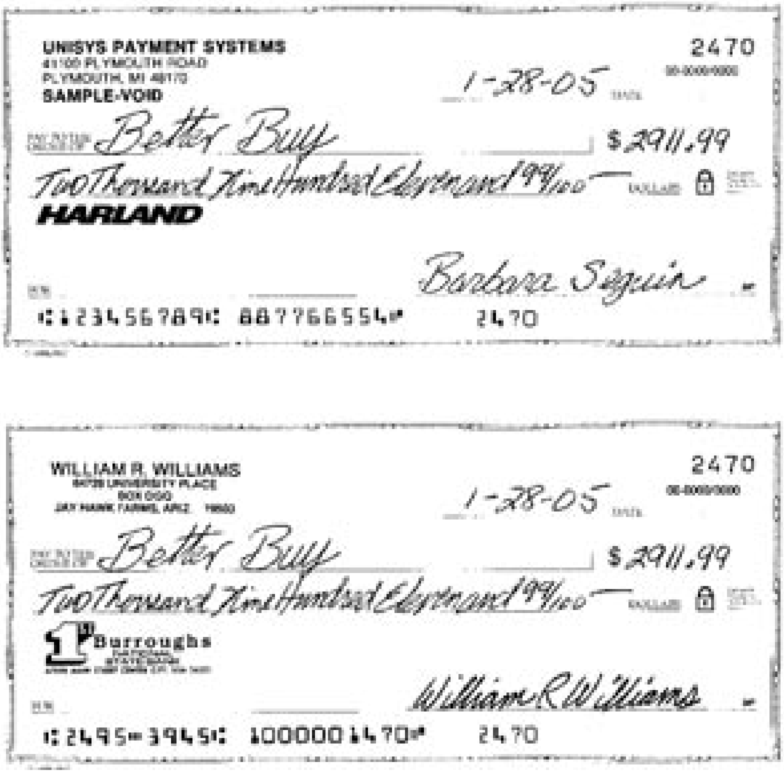
Henry Coffman

⑆123456789⑆ 887766554⑈ 2492

Figure 1

Redirecting the Debit

This is when the X9.37 fields for the MICR bank information are altered so that the check is debited from another account. This results in a third bank being defrauded for the entire amount of the altered check.



UNISYS PAYMENT SYSTEMS
41100 PLYMOUTH ROAD
PLYMOUTH, MI 48170
SAMPLE-VOID

2470

1-28-05

Better Buy $ 2911.99

Two Thousand Nine Hundred Eleven and 99/100

HARLAND

Barbara Seguin

123456789 887766554 2470

WILLIAM R. WILLIAMS
UNIVERSITY PLACE
BOX
JAY HAWK FARMS, ARIZ

2470

1-28-05

Better Buy $ 2911.99

Two Thousand Nine Hundred Eleven and 99/100

Burroughs

William R Williams

2495-3945 1000001470 2470

Figure 2

Without a method to verify these images, fraud filters within the check processing system cannot catch the alterations – and in many cases, if a dispute arises, depending on the amount in question, many banks simply charge off the fraud since it is less costly than initiating an investigation. Over time, these small amounts can add up to millions of dollars in losses for a bank.

Another example of external risk has to do with image capture at a customer site. Banks are finding ways to minimize the costs with customers making deposits at local branches. Check transport vendors are coming up with new tabletop check imaging equipment that can be deployed at retail sites. When a consumer wishes to purchase goods by check at a retail outlet, the retail outlet may now have a check transport attached to the cash register. A store clerk can then scan the check at the cash register and have the image transmitted directly to the Bank of First Deposit (BOFD) for processing. The greatest risk with this type of deployment is that the check image is stored within an insecure environment, presenting the opportunity for an employee to modify images prior to transmission to the BOFD.

How Digital Signatures Mitigate Risk

Since the check payment process has several points where images are stored and archived either temporarily (i.e. prior to a retail customer transmitting their nightly batch of checks from their customers), or permanently (i.e. at the Bank of First Deposit or payor bank for seven years), a security mechanism is required to protect these images at every point during the process. Digital signatures offer the security required.

A comparison can be made to e-commerce sites processing credit card transactions via SSL (Secure Sockets Layer). SSL provides the confidentiality needed to encrypt customer and credit card information during transmission from the customer's computer to the retail web site, and then from the retailer to their credit card processor. However there has been no evidence of a malicious attack on credit card information during transmission. Rather the risk has always resided in the weak security surrounding the storage and archiving of private information. Why try to attack the sending and receiving of information for a single transaction when you can just go to the where the information is all stored on thousands of customers? The same analogy can be applied to check images – the point of risk is going to be where the images are stored.

Check 21 makes a substitute check the legal equivalent of the original. A substitute check—or Image Replacement Document [IRD] —is a paper item that carries images of the front and rear of the original check, the MICR code line for the original check, legal legends, and endorsements. IRDs may be machine readable and compatible with current standards and check processing equipment. While ANSI X9.37 describes the necessary quality and usability fields that must be present during image capture, it leaves banks exposed to the opportunity for images to be modified—unless digital signatures are applied to the image.

A digital signature is applied to a hash of the image data. The result is called a 'message digest'. Every image has a unique message digest. If an image is tampered with, even right down to a single pixel, the result will be an entirely unique message digest. This is why when an image is received, its message digest is processed again, and compared to the original message digest to verify the image. If both digests match, then the image has not been tampered with during transmission. However, if the two message digests do not match, then the verifying party will know that the image has been tampered with. The digital signature also provides authentication information on the identity of the Bank of First Deposit.

The use of digital signatures, regardless of the check amount, will mean that all parties can be assured of the authenticity of the check. This reduces fraud even on the small amount checks, which means that banks will no longer have to charge off small dollar amounts, further reducing losses.

If the image is signed at the time of capture at the retail level, an employee would no longer be able to alter the image prior to transmission. Banks would also be able verify if the image has been tampered with upon receipt. Applying digital signatures at the time of deposit – and optionally verifying the image prior or during transmission will result in a fraudulent image being caught before it enters the payment system.

A hash function is an algorithm that condenses a message into quantitative result that yields an identical result every time same the algorithm is executed using the same message. The message cannot be derived from the result produced by the algorithm and two different messages cannot produce the same result by using the same algorithm. The output of a hash function is called a hash, hash value, hash code, message digest, or sometimes fingerprint.

The Importance of ECC for Check 21

Applying digital signatures at the time of image capture solves the problem of authentication, data integrity, and non-repudiation and reduces the risk of fraudulent transactions that must be written off. But security is only economically feasible if it does not impact performance and the overall throughput of the check processing system. Everyday, millions and millions of checks are processed in US. If security is paramount and digital signatures are to be applied and verified on each of those images, then the digital signature scheme needs to provide strong security that:

- **delivers optimal performance**
- **scales with a key strength that matches the archiving period (the signature has to be valid for at least seven years)**
- **matches the equivalent symmetric key strength if encryption of these images is desired**

Performance

While ANSI X9.37 describes 5 digital schemes that can be used for the security flags, they are actually based on three ANSI approved digital signature algorithms – RSA, DSA, and ECDSA. All three algorithms provide equivalent and very strong digital signatures. ECDSA, however, has smaller key sizes and provide a higher security per bit over RSA and DSA. Smaller keys result in greater efficiency and performance. This means that more checks can be processed which results in faster payment and settlement for both banks and their customers. ECDSA also allows software vendors to provide greater performance without needing to invest in additional hardware acceleration or upgrading existing equipment. In the case of Unisys' check transports, existing equipment just required a software update to support over 10,000 signatures per minute, which is a target benchmark they want to maintain as they move to larger key sizes. This could not be achieved with 2048-bit RSA or DSA.

The following table demonstrates the performance of ECDSA over RSA for signing.[3] The ECC and RSA signatures compared at each level are of equivalent strength, despite the difference in signature size. The chart measures the number of digital signatures applied to a data block per second.

ECDSA Signature	ECDSA Speed (sigs/minute)	RSA Signature	RSA Speed (sigs/minute)	ECC Benefit
163 bit	170640	1024 bit	25380	672 %
224 bit	105840	2048 bit	2940	3600 %
256 bit	54000	3072 bit	480	11250 %

Figure 3: Signing Performance of ECDSA versus RSA

ECDSA provides better performance and throughput without requiring additional hardware to accelerate digital signatures. This results in lower capital costs, higher margins, and a higher ROI.

[3] The performance was measured on Windows XP with an Intel 3.00 GHz Pentium 4 processor, and 512KB of memory. Your actual performance will vary based on the platform and operating system and the application that is integrated with Certicom Security Architecture for Check 21. This raw performance data was measured by Certicom own internal benchmarks using Security Builder toolkits.

The following chart demonstrates the proof points for protection lifetime and encryption requirements.[4]

CRYPTOGRAPHIC STRENGTH	KEY SIZE RATIO	HASH ALGORITHM	ELLIPTIC CURVE ASYMMETRIC ALGORITHMS	RSA/DSA/DH ASYMMETRIC ALGORITHMS	EXPECTED LIFETIME EXPIRY
56 bits	DES	–	–	–	expired
80 bits	3DES (2 key)	SHA-1	160 bits	1024 bits	2010
112 bits	3DES (3 key)	SHA-224	224 bits	2048 bits	2030
128 bits *	AES-128	SHA-256	256 bits	3072 bits	2031+
192 bits	AES-192	SHA-384	384 bits	7680 bits	2031+
256 bits *	AES-256	SHA-512	512 bits	15360 bits	2031+

Figure 4: Expected Lifetime Expiry and Encryption Requirements Comparison

Protection Lifetime

Federal regulations require financial institutions to archive the image files for up to seven years from the time of image capture. Therefore the digital signature applied to the image needs to be not only strong enough at the time of image capture – but also be strong enough to be tamper resistant seven years later.

An image captured today would need to be archived until 2012. In order to be valid, a 2048-bit RSA or equivalent 224-bit ECDSA signature would need to be applied. From the performance chart above you can see that the ECDSA signature would deliver 3600% faster processing, and would also take up less storage footprint because of the smaller signature key size.

Encryption

The ANSI X9.37 standard deals primarily with the signing of images. If check images are going to be transmitted over the Internet, then financial institutions and payment processors should additionally encrypt the images using very fast FIPS approved symmetric encryption algorithms such as 3DES and AES. To ensure strong security, the encryption of these images should match the signature that has been applied. For example, at 128 bit AES symmetric encryption, the corresponding public key size required for digital signatures would be 256 bits for ECDSA or 3,072 bits for RSA. Again, because of size and performance requirements, ECDSA is the logical choice.

Using ECDSA also frees up additional CPU resources, so that more features that provide better usability and robustness can be added. For example, better image quality.

For performance, adequate cryptographic lifetime and an overall strong cryptosystem that matches data encryption strength with digital signature strength, ECDSA is the most practical choice for digital signatures for Check 21. ECDSA is a key algorithm supported within the Certicom Security Architecture for Check 21.

[4] All comparisons are based on ECC and RSA equivalent keys sizes as per NIST Special Publications 800-56 and 800-57 and RSA Labs.

http://csrc.nist.gov/CryptoToolkit/kms/keyschemes-Jan03.pdf

http://csrc.nist.gov/CryptoToolkit/kms/guideline-1-Jan03.pdf

http://www.rsasecurity.com/rsalabs/node.asp?id=2004#table1, May 6, 2003 Publication by Burt Kaliski

The Certicom Security Architecture for Check 21

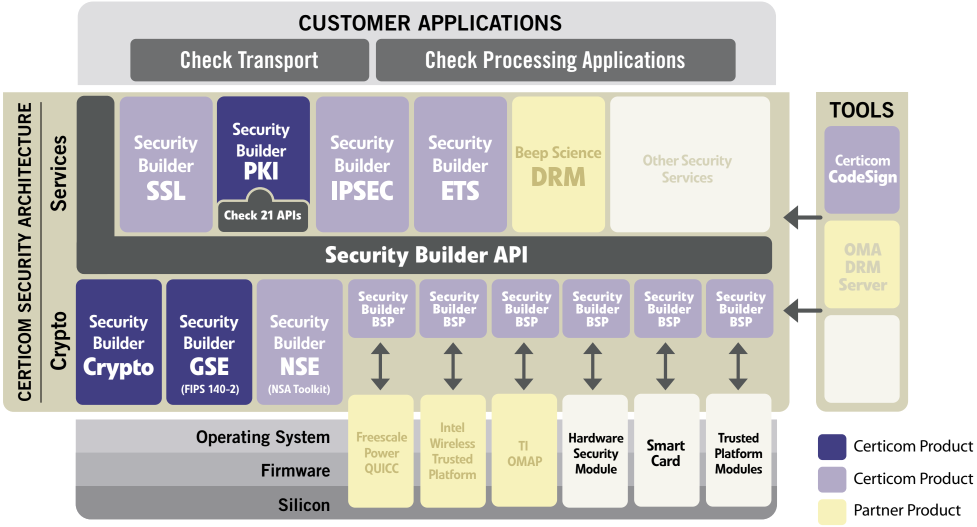


Figure 5: The Certicom Security Architecture for Check 21

The Certicom Security Architecture for Check 21 enables check transport vendors and check application vendors to quickly and cost effectively implement digital signatures and digital signature verification. It provides full support of the ANSI X9.37 security flags and ECDSA. The solution contains the following components:

- **Security Builder® PKI™** *digital certificate management toolkit*
- **Check 21 Check Verification APIs**
- **a choice of software cryptographic providers**
  - **Security Builder® Crypto™** *cross-platform cryptographic module*
  - **Security Builder® GSE™** *FIPS 140-2 Validated cryptographic module*
  - **matches the equivalent symmetric key strength if encryption of these images is desired.**

All components of the Certicom Security Architecture for Check 21 are unified by a single common API—Security Builder® API™—that sits between the protocols and cryptographic providers, enabling developers to quickly migrate their Check 21 applications to whichever cryptographic module is required.

The Components of Certicom Security Architecture for Check 21

Security Builder PKI

Security Builder PKI is a complete digital certificate management toolkit that supports the X.509 v3 certificates used to identify the check transport that captured the image. Security Builder PKI provides a common cross-platform API for generating certificate requests, importing and exporting certificates and password protected keys, and binding a digital signature to a certificate and public key. Security Builder PKI also includes PKCS #11.

Check 21 Check Verification APIs

Three function calls specifically developed for Certicom Security Architecture for Check 21 enable check image verification to be quickly added to any application in a matter of minutes. These functions provide:

- digital signature verification
- chain validation to a trusted Check 21 root certificates
- Certificate Revocation List verification

Security Builder Crypto

Security Builder Crypto offers highly efficient implementations of the most widely used cryptographic operations. Available on more than 30 different platforms, it provides a complete suite of cryptographic algorithms for developers to easily integrate additional encryption algorithms such as AES, 3DES, ECC and RSA.

Security Builder GSE

Security Builder GSE is a FIPS 140-2 Validated cryptographic module that is available for leading client and server side platforms, enabling end-to-end security. Validated platforms include: AIX, HP-UX, Palm, Red Hat Linux, Sun Solaris, Windows 98, Windows CE and Windows 2003

Using Security Builder GSE as the software cryptographic provider within the Certicom Security Architecture for Check 21 allows vendors to run Security Builder PKI in FIPS approved mode of operation.

Both Security Builder Crypto and Security Builder GSE provide Certicom Security Architecture for Check 21 with the necessary cryptographic algorithms to perform the signing and/or verification of check images. This includes support for all 5 digital signature methods in X9.37:

- ECDSA with SHA-1 (ANSI X9.62)
- DSA with SHA-1 (ANSI X9.30)
- RSA with MD5 (ANSI X9.31)
- RSA with MDC2 (ANSI X9.31)
- RSA with SHA-1 (ANSI X9.31)

Advantages of the Certicom Security Architecture for Check 21

The Certicom Security Architecture for Check 21 provides check transport vendors and check application vendors a number of advantages:

Comprehensive solution for the addition of standards-based digital signatures:

Central to the interoperability and longevity of the Certicom Security Architecture is its standards-based design. Certicom Security Architecture for Check 21 supports all the digital signature methods recommended in ANSI X9.37 and can also provide a FIPS 140-2 validated cryptographic module for use in applications that require a high level of security. The Certicom Security Architecture for Check 21 supports both legacy RSA and today's new standard ECC, ensuring a bridge to the future.

Lower total cost of development and improved time-to-market

The concise and intuitive API reduces your need for crypto and PKI expertise, shortening the developer learning curve and allows you to add image signature verification to new or existing applications within minutes. Support for a wide range of platforms further reduces porting requirements and minimizes the expense of embedding security.

Fast performance

Strong, efficient ECC-based signatures allow the signing and verification of thousands of images per second, without the addition of any hardware acceleration. The relatively small size of ECDSA signatures allows you to add strong security and meet the application performance requirements of your customers.

Security strategy partner

Certicom is a dedicated security organization with a core competency in providing security for companies focused on financial services and digital imaging for financial applications, including BEA, ImageNow, NCR, Sterling Commerce, and Unisys. Certicom is an active contributor to the ANSI X9 standards and authored ANSI X9.63, one of the approved signature standards in X9.37. Partnering with Certicom allows check transport and check application vendors to avoid investing in security R&D while still achieving the future-proof security strategy the market demands.

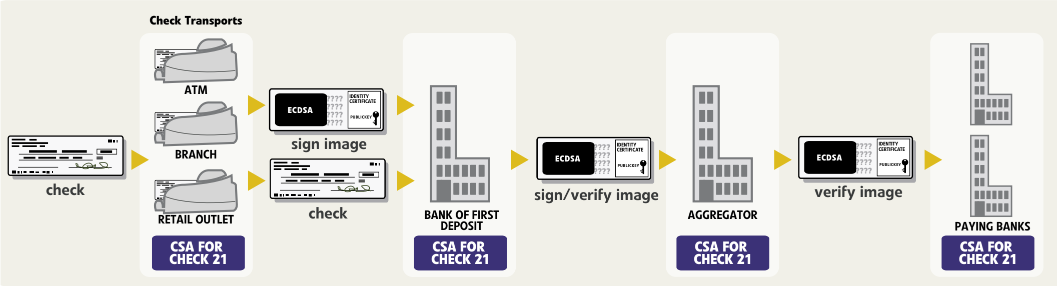


Figure 6: Check Process Flow

This diagram demonstrates where the Certicom Security Architecture for Check 21 would be used in the check payment process. Physical checks are collected at an ATM, a branch, or a retail outlet. The check image is captured by a check transport at these locations. Certicom Security Architecture for Check 21 resides with the application that performs the signing of the image – it may also optionally verify the image prior to transmission to the Bank of First Deposit [BOFD]. If the check image is not captured at these initial locations, then the physical check is sent to the BOFD where the image will be captured on the check transports. The images are then transmitted to a Payment Aggregator who will verify the images upon receipt. The check images are sorted according to the paying bank based on the MICR encoded information captured in the image. The Aggregator then sends the check images to the paying banks for payment. The Paying Banks then in turn will verify the check images prior to payment.

There are obviously many technical details to make the above process happen, but the Certicom Security Architecture for Check 21 removes much of the complexity, meaning that check verification can be added to an application in a matter of minutes, and requires no Public Key Infrastructure expertise. For more detail on the steps of Check 21 verification, including public key management see Appendix A.

Conclusion

Using digital signatures in combination with Check 21 may significantly help reduce check fraud, because it allows for quick detection of any fraudulent activity. This in turn lowers banking losses and improves overall operational costs, while enabling financial institutions to leverage the digital signatures for value added services for their customers even after the images are archived.

The Certicom Security Architecture for Check 21 allows check transport vendors and check application vendors to differentiate their offering and quickly and cost effectively implement digital signatures and digital signature verification, without needing to be a PKI expert.

Certicom Security Architecture for Check 21 also provides the ability for vendors to scale their security for protecting the image files over the archival period with the least amount of impact on resources and eliminates investing in additional hardware to accelerate digital signatures. This of course can only be achieved by the use of ECDSA signatures, and the availability of a trusted Check 21 Root Certificate Authority from VeriSign.

About Certicom

Certicom Corp. (TSX: CIC) is the authority for strong, efficient cryptography required by software vendors and device manufacturers to embed security in their products. Adopted by the US government's National Security Agency (NSA), Certicom technologies for Elliptic Curve Cryptography (ECC) provide the most security per bit of any known public key scheme, making it ideal for constrained environments. Certicom products and services are currently licensed to more than 300 customers including Motorola, Oracle, Research In Motion, Terayon, Texas Instruments and Unisys. Founded in 1985, Certicom is headquartered in Mississauga, ON, Canada, with offices in Ottawa, ON; Reston, VA; San Mateo, CA; and London, England. Visit www.certicom.com.

Appendix A:
A Detailed Look at Check 21 verification using Certicom Security Architecture for Check 21

The first step for a bank is to create their X.509 Version 3 certificate request. The PKCS #10 function included with the Certicom Security Architecture for Check 21 enables this to be completed rapidly. This process will create the public/private key pair that will be used to the sign the check images. The PKCS #10 certificate request contains information about the entity requesting the certificate, including the name of the financial institutions, its geographic location, along with the public key. The certificate request is then submitted to a Check 21 Certificate Authority (CA), like VeriSign via a secure website. A security officer at the CA will verify the certificate request, after performing a background check on the entity requesting the certificate. Once validated, the CA will generate a X.509 v3 certificate and will sign the public key that is contained within the certificate. The CA will also send the root certificate that is associated with the private root key that signed the financial institution's certificate. The certificates are sent in a PKCS #7 file format.

Once the root and financial institution's certificates are received, usually via e-mail, the certificates can now be installed into the Certicom Security Architecture for Check 21 trusted database. This database is where trusted keys, certificates, and Certificate Revocation Lists are stored for signing and verifying check images.

The private key that was generated during the certificate request process is securely stored within the trusted database of the Certicom Security Architecture for Check 21. It is password protected and encrypted using AES and SHA-1. The private key is used to sign and hash the images with ECDSA with SHA-1 (ANSI X9.62). The signed hash and certificate is appended to the corresponding check image. The image is now ready to be truncated to the corresponding paying bank for settlement.

The paying bank, which has an agreement in place with the payor bank prior to exchanging images, must first download and install a Check 21 Root Certificate from the CA and Certificate Revocation List. By installing a Check 21 Root Certificate and the Certificate Revocation List –which is a file that contains a list of any certificate that have been revoked by the CA–the paying bank is able to validate the images to trusted Certificate Authority that will authenticate the identity of the payor bank. The CRL also notifies if the paying bank can still trust the digital signature that has been appended to the check image.

The next step is to validate the check image. This is accomplished by using the second function contained within Check 21 Validation APIs in the Certicom Security Architecture for Check 21. Three pieces of information are necessary for validation: the image data that was signed, the certificate that corresponds with the private key that signed the image, and the signature.

Once the first two functions are completed, the image either passes or fails.

The third and final function of the Check 21 APIs ends the batch processing of the check images.

Certicom White Papers

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

The Inside Story

Many Happy Returns: The ROI of Embedded Security

Wireless Security Inside Out (authored by Texas Instruments and Certicom)

Welcome to the Real World: Embedded Security in Action

Sum Total: Determining the True Cost of Security

The Elliptic Curve Cryptosystem for Smart Cards

Elliptic Curve DSA (ECDSA): An Enhanced DSA

Formal Security Proofs for a Signature Scheme with Partial Message Recovery

Postal Revenue Collection in the Digital Age

An Elliptic Curve Cryptography Primer

ECC in Action: Real World Applications of Elliptic Curve Cryptography

Using ECC for Enhanced Embedded Security: Financial Advantages of ECC over RSA or Diffie-Hellman

Good Things Come in Small Packages: Certicom Security Architecture for Mobility

Meeting Government Security Requirements: An overview of the Certicom Security Architecture for Government

The Benefits of Digital Signatures for Cutting Bank Fraud Losses: A Technical Overview of The Certicom Security Architecture for Check 21 certicom™

Contact Certicom

Corporate Headquarters

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

Sales Offices

Worldwide Sales Headquarters

1800 Alexander Bell Dr., Suite 400
Herndon, Virginia 20190
Tel: 703-234-2357
Fax: 703-234-2356
E-mail: sales@certicom.com

Canada

5520 Explorer Drive
Mississauga, Ontario
L4W 5L1
Tel: 905-507-4220
Fax: 905-507-4230
E-mail: info@certicom.com

Ottawa

84 Hines Road
Suite 210
Ottawa, Ontario
K2K 3G3
Tel: 613-254-9270
Fax: 613-254-9275

U.S. Western Regional Office

1810 Gateway Drive, Suite 220
San Mateo, CA 94404
Tel: 650-655-3950
Fax: 650-655-3951
E-mail: sales@certicom.com

Europe

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

Engelska Huset
Trappv 9
13242 Saltsjo-Boo
SWEDEN
Tel: +46 8 747 17 41
Mobile: +46 70 712 41 61
Fax: +46 708 74 41 61

www.certicom.com