certicom™

Certicom Security for Check 21

ensuring secure and efficient digital image interchange

THE PROBLEM

In the United States alone, the financial industry stands to save 2 billion dollars a year by eliminating paper-based financial instruments such as checks and moving to digital images or paper substitutes that are printed when and where needed. This process is commonly referred to as electronic image interchange or its subset – check truncation.

Recently, new legislation in the United States known as Check 21 encourages financial institutions to move towards image-based processing of electronic checks. Effective October 28, 2004, U.S. banks are no longer required to physically exchange the original checks. This legislation, combined with the anticipated savings and benefits, is expected to promote broad adoption of image interchange among financial institutions.

However, the industry must clear several hurdles on the track towards adoption. Among these, the most significant are quality and security of the image. The success of any plan to implement Check 21 relies heavily on standards-compliant solutions which consider image quality, usability, and image security. Any security solution for check image interchange among banks must meet the following requirements:

- **guarantee the same legal status as an original paper check**
- **reduce the risk of fraud**
- **resist tampering**
- **facilitate the rapid processing of settlement transactions**
- **maintain security throughout long term storage**
- **pursue standards-based implementations for industry-wide adoption**

Converting paper checks to images, and the potential for a further conversion to a substitute check by printing the scanned image to paper, removes most paper-based security features. These conversions not only expose banks to increased rates of processing error, they may also increase the opportunity for and incidence of fraud by internal and external perpetrators. Under Check 21 legislation, banks are liable for any losses resulting from errors involving check truncation or substitution, regardless of the source of the error.

Institutions using applications to process substitute checks must guard against errors that involve payment of both an original check and one or more of its electronic or paper substitutes. Likewise, an application that enables check truncation must also prevent fraudulent changes to a check image. These requirements demand that every check image or substitute include security features that prevent alteration as well as indisputable proof of identity for the source of each item. Banks must take care to choose an unaltered version of the check before rendering payment, and also to pay it only once.

For the sake of processing speed and secure storage, a secure check image application must be highly efficient to allow for rapid processing yet be strong enough to maintain the security of images throughout long term storage. In the United States, banks are required by law to maintain financial documents for seven years. Check images stored electronically need to remain secure, from the time they are created, to a time seven years later when they will be deleted. Technological advances might present significant challenges to a cryptographic system while that time elapses. The security of the image will depend upon the longevity of the cryptographic key chosen as part of the solution to secure it.

Finally, the value of a move to image interchange among financial institutions can only be realized through a common standards-based approach across the entire industry. In the United States and Canada, the American National Standards Institute (ANSI) is the de facto authority in this regard and financial institutions must insist that any proposed solutions are ANSI compliant to ensure industry-wide adoption. In North America, ANSI is also a mandatory first step on the road to recognition by the International Organization for Standardization (ISO). Worldwide, all nations face a common need to standardize the process of image interchange through their own governing bodies en route to ISO certification.

THE SOLUTION

Today, several ANSI publications identify appropriate solutions for moving towards check image interchange as described by Check 21. Among these publications, X9.90 (Specifications for an Image Replacement Document) and X9.37 (Specifications for an Electronic Exchange of Check & Image Data), are approved draft standards for trial use. Draft standards typically become final after one year.

The ANSI drafts recommend Elliptic Curve Digital Signature Algorithms (ECDSA) to provide the security and efficiency required by applications that convert, process, and store check images for the financial industry. A third proposed ANSI standard, X9.81 (Media-Based Image Exchange Format) also recommends ECDSA.

ECC offers high security using much smaller key sizes than any other known public key cryptographic scheme available today. This mix of strength and efficiency makes ECC ideal for applications targeting the high security, high volume needs of the financial industry. Through its exceptionally small key sizes, ECC also provides extremely fast digital signing operations, another key requirement for processing check images.

ANSI publication	Recommended Cryptographic Algorithm
X9.90	ECDSA only
X9.37	ECDSA or RSA
X9.81	ECDSA or RSA

Certicom is the authority for strong, efficient cryptography. Through Certicom's Security Builder® PKI™ developer toolkit, application developers can quickly add optimized implementations of ECDSA, RSA and other standards-based digital signatures and key management to applications such as those used by banks to process check images.

With a footprint as small as 100 KB, Security Builder PKI can be integrated on a range of devices and platforms from handhelds, to desktops and servers. As a standards-based solution, Security Builder PKI adheres to a wide range of industry standards including ANSI.

THE IMPLEMENTATION

The Security Builder PKI toolkit by Certicom allows developers to integrate the integrity, non-repudiation and trust necessary to satisfy the legal requirements for exchanging digital images (i.e., check verification). But the process of efficiently securing high volumes of check image captures presents a major challenge: machines scan thousands of images, and each must be signed to ensure that the information on the check cannot be altered or denied afterwards regardless of the number of servers over which it is transmitted. Likewise, once a check image is created and digitally signed at one institution, speed is equally important for quickly verifying that digital signature, along with thousands of others, at a receiving institution.

Current industry requirements demand a security solution able to digitally sign up to 10,000 images per minute. ECDSA is the only technology capable of meeting this requirement and major check transport vendors have already selected ECDSA for this reason. The optimized ECDSA implementation available through Security Builder PKI satisfies the financial industry's need for speed in terms of secure transactions per minute without requiring any additional hardware to accelerate the process.

Added to an original check image, an ECDSA signature guarantees the integrity of the image against alteration and allows for authentication. Integrity is accomplished in two steps: first, by creating a hash value for the image or "hashing" it, and second, by digitally signing the resulting sequence of bits. Combined with digital certificates that are provisioned by a trusted third party or the banking institution itself, an ECDSA signature also enables non-repudiation: indisputable proof that the institution claiming to have created the check substitute from the original check actually did.

- **optimized ECDSA (ANSI X9.62) for speed and performance**
- **enables support for ANSI X9.37: Specifications for an Electronic Exchange of Check & Image Data**
- **robust PKI security for applications**
- **designed on a FIPS 140-2 validated cryptographic module for high security**
- **also supports RSA (PKCS#1) digital signatures**

For electronic check presentment to work seamlessly, banks must first agree to exchange electronic checks and exchange root certificates in order to trust one another's ECDSA signatures. Figure 1.0 shows how applications secured by Security Builder PKI contribute to the secure creation, interchange and storage of a check image between two banks.

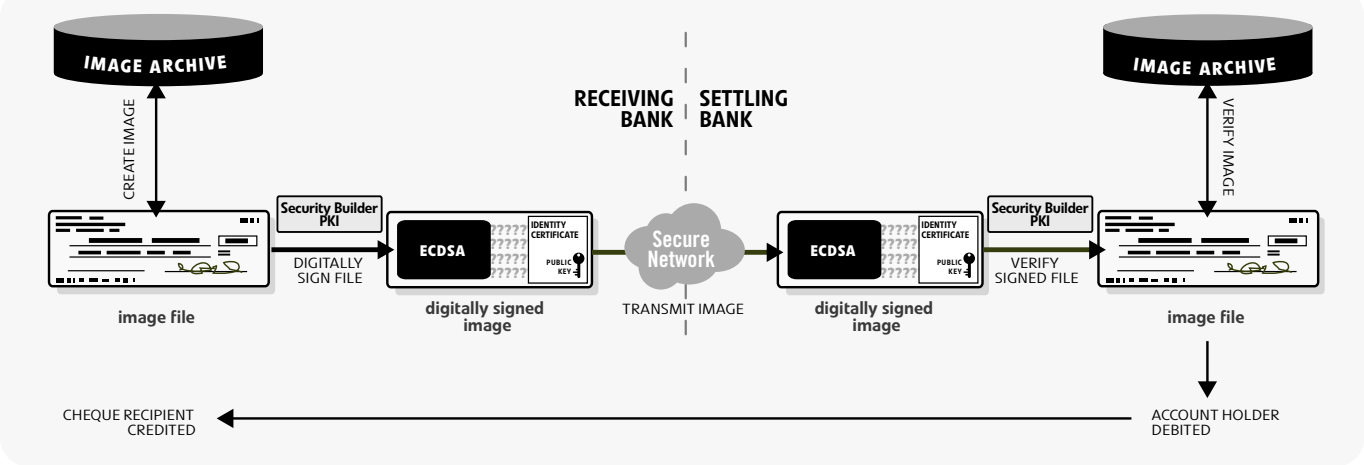

Figure 1.0. Upon receiving an original paper check, the receiving bank scans it to create a check image using an application secured by Security Builder PKI. Upon creation, the application adds an ECDSA signature to the check image. The receiving bank sends the cheque image to the settling bank via a secure network, and keeps another copy in its image archive for seven years.

The settling bank receives the digitally signed check image and uses another application secured by Security Builder PKI to verify the ECDSA signature. Once verified, the settling bank debits the appropriate customer and credits the appropriate recipient. the settling bank also stores the cheque image in its own image archive for seven years.

RESULTS

Using Security Builder PKI, application vendors targeting the financial industry are able to integrate the ECDSA security that ANSI recommends for use in electronic image interchange among banks.

Encouraged by the potential for 2 billion dollars in cost savings and Check 21 legislation, financial institutions throughout the United States are adopting check images and check image substitutions for daily use. The same process, either complete or underway in other industrialized nations, contributes to improved efficiency for clearing international checks as well. The motivation for the financial industry to adopt check truncation is strong:

- **optimized ECDSA (ANSI X9.62) for speed and performance**
- **enables support for ANSI X9.37: Specifications for an Electronic Exchange of Check & Image Data**
- **robust PKI security for applications**
- **designed on a FIPS 140-2 Validated cryptographic module for high security**
- **also supports RSA (PKCS#1) digital signatures**

As the United States – the world's largest economy - accelerates its move towards electronic image interchange, the transition is sure to have a global impact and trigger increased demand for associated solutions such as secure applications for capturing, processing and storing digital images.

Application vendors that integrate ANSI X9F-based security into their solutions can access this lucrative and growing financial services market while gaining a competitive advantage over vendors that do not provide strong, efficient and standards-based ECDSA signatures.

Beyond the financial industry, application vendors that integrate ECDSA-based image interchange security are ideally positioned to access additional markets such as medical imaging and insurance providers that require similar safeguards for their digital images.

Note: Some pieces of background material for this application note were sourced from two different whitepapers published by Unisys: "The Implications of Check 21 on Item Processing" and "Check 21 Review and Operational Issues".

about certicom

Certicom Corp. (TSX:CIC) is the authority for strong, efficient cryptography that software vendors and device manufacturers use to embed security into 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 XM Radio. 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.

North America 1.800.561.6100
EMEA +44 20 7484 5025
International +1.905.507.4220
E-mail info@certicom.com
www.certicom.com

certicom™