certicom™
securing innovation

Certicom Security Architecture for Check 21

The Check Clearing Act for the 21st Century (Check 21) streamlines the check clearing process, reducing overall operation and administrative costs. Although faster than a physical exchange of checks, Check 21 poses a security risk if check images are altered at any point in the check exchange process. Digital signatures can prevent this, ensuring:

- **Detection of modifications to digital images at any point in the exchange process**
- **Certainty behind the source of the image (image and device)**

Solution

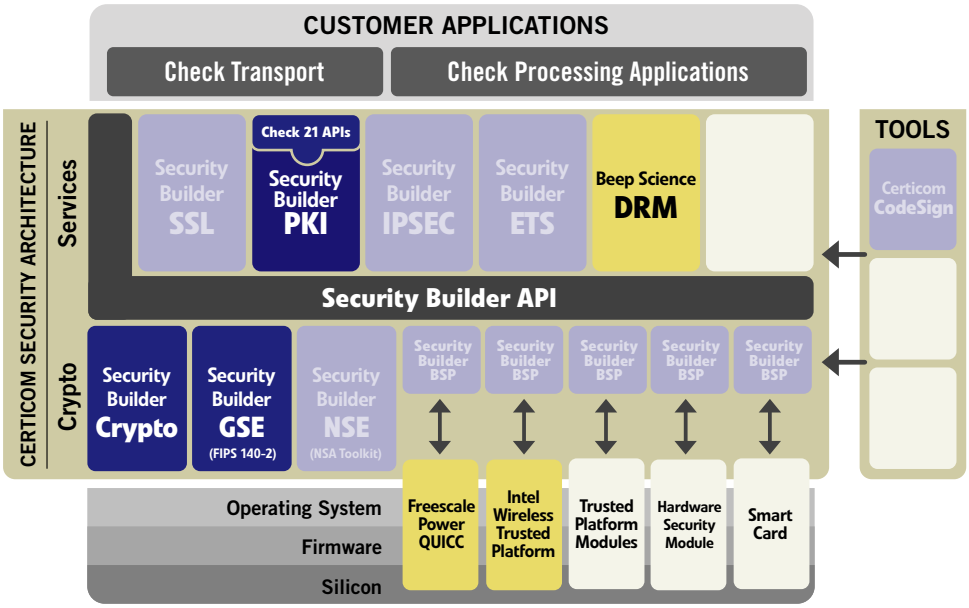
The Certicom Security Architecture for Check 21 is a comprehensive solution specifically designed to allow check application and transport vendors to quickly and cost-effectively add digital signature functionality supported within the ANSI X9.37 security standards. These digital signatures add strong security to the digital image exchange process. Should a signed image be compromised en route (by changing of the amount or changing name of payor/payee), the signature will not be verifiable, and the check will not be cleared.

You can also leverage these digital signatures to make your own applications more secure and address your customers' growing security requirements.

The Certicom Security Architecture for Check 21 uses Elliptic Curve Digital Signature Algorithm (ECDSA), one of the strongest and fastest implementations available for digital signatures.

Other advantages include:

- Competitive differentiation with added security value to meet your customer's growing security requirements
- Check image security that meets current standards and will evolve with changing standards
- Strong security that doesn't bog down application performance
- Small signatures that protect the images throughout the seven year archive requirement



Certicom Security Architecture for Check 21

CSA FOR CHECK 21 FEATURES

Concise and Intuitive API

- reduces need for cryptographic and PKI expertise
- speeds time-to-market

Standards-based

- meets ANSI DSTU-X9.37 FIPS and IETF-PKIX security standards
- X.509 v3 digital certificate management
- meets and will evolve with changing standards

Comprehensive Security

- signing and verifying check images
- digital certificate management
- certificate chain validation to a trusted Check 21 root
- Certificate Revocation List [CRL] parsing and verification

FIPS 140-2 Validation

Allows sale to government institutions such as Federal Reserve Bank and Department of Commerce.

Fast and Efficient

ECC allows signing and verification of thousands of images per minute – faster and more efficient than other recommended signature algorithms.

Key Solution Modules

Certicom Security Architecture for Check 21 secures financial applications through a modular set of security protocol services, software cryptographic providers, and middleware that are pulled together by a single, intuitive application programming interface (API) between the applications and the cryptographic providers.

Security Builder® PKI™
digital certificate management module
- required to store, import or export digital certificates.

Check 21 APIs
The following APIs have been developed by Certicom specifically to meet Check 21 requirements, and are included as part of the overall solution:

- Verify digital signature
- Certificate chain validation to trusted Check 21 root
- Parse and verify CRL

Security Builder® API™
- enables the seamless access to cryptographic support from a variety of Certicom-supported cryptographic providers to an application

One of:

Security Builder® GSE™
FIPS 140-2 Validated cryptographic module
- quickly incorporate FIPS 140-2 Validated ECDSA, RSA and DSA signatures
- meet stringent government security requirements

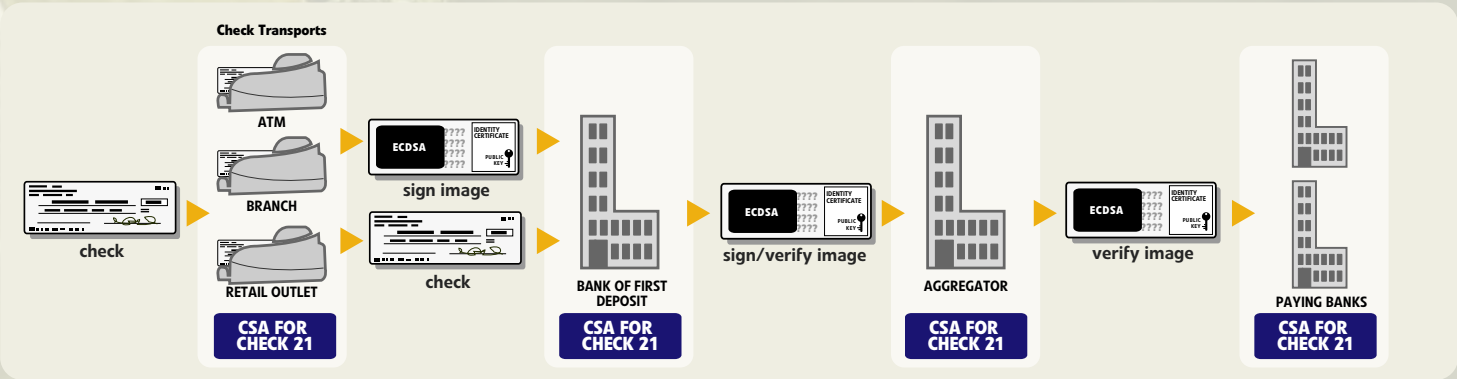
Or:

Security Builder® Crypto™
cross-platform cryptographic module
- complete suite of cryptographic algorithms to easily integrate encryption, digital signatures, and other security mechanisms into applications, including AES, ECDSA, ECDH, RSA and SHA-1.

Certicom Security Architecture for Check 21 Applied: How it all Works Together

Integrating Certicom Security Architecture for Check 21 into your application or check transport device ensures that the digital signature will travel with the image and provide security against tampering at any point in the process where the image is signed and/or verified.

Physical checks are collected at an ATM, a branch, or a retail outlet. The check image can be captured by a check transport at these locations or at the Bank of First Deposit [BOFD]. 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]. Certicom Security Architecture for Check 21 can also be used by the Payment Aggregator, who verifies the images upon receipt, sorts them according to the paying bank and sends the check images on to the paying banks for payment. The Paying Banks then in turn use the Certicom Security Architecture for Check 21 to verify the check images prior to payment.



How Certicom Security Architecture for Check 21 protects digital images.

about certicom

Certicom Corp. (TSX:CIC) is the authority for strong, efficient cryptography required by software vendors, and device manufacturers to embed security into their products. Adopted by the US Government's National Security Agency, Certicom technologies for Elliptic Curve Cryptography provide the most security per bit of any known public key scheme, making it ideal for constrained environments.

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™