

Certicom Certificate Practice Statement

Addendum for Check21

Certicom Corp.

Check21 CPS Addendum Version 1.0

10 Dec. 2008

www.Certicom.com

Beginning December 10th, 2008, Certicom Corp. ("Certicom") will offer Check21 Certificates which are issued to Unisys digital imaging check transport and archiving systems with image security features. The purpose of this Addendum to the Certicom Certificate Practice Statement ("ACPS") is to amend version 1.0 of the Certicom Certificate Practice Statement ("CPS") to include the Check21 Certificate product offering. All provisions of the CPS not specifically amended or added herein remain in full force and effect and where applicable shall apply to the new product offerings. Amended portions in this ACPS are included within brackets. Nothing in the CPS shall be deemed omitted, deleted or amended unless expressly stated in this ACPS or identified in brackets below. Information not located in brackets is to be included in addition to all information in the CPS. Headings from the CPS are included to identify the location of the Amended information, and are not intended to be duplicative.

1. INTRODUCTION

...

1.4 Certificate Usage

...

1.4.1 Appropriate Certificate Use

...

Check21 Certificates allow subscribers using the Check21 protocol to digitally sign digital check-related image data.

...

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

...

2.2 Publication of Certificate Information

An updated Check21 Certificate CRL is published on the Certicom website every 24 hours; however, under special circumstances the CRL may be published more or less frequently.

...

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of Names

...

Certificate Distinguished Names may consist of a combination of the following Components:

Attribute	Abbr.	Value
Common Name	CN	[The Common Name is the name of the Subscriber or domain name for which the certificate has been issued. For Check21 the Common Name is the Unique ID assigned to the Image Security Certificate.]
Organization	O	The organization or blank
Organizational Unit	OU	Certificates may be multiple OU attributes. The attributes may include:

Organization information or Issuer

		Information
		Copyright information
		References to the terms and conditions of use
		Description of the Certificate
		Certificate warranty information
		Verification or validation information
		Issuance and/or hosting information
		Special certificate notes
Country	C	The two letter ISO country code or not used
Locality	L	Subscriber's locality or not used
State or Province	S	State or Providence or not used
Street	STREET	Street address or not used
Postal code	PostalCode	Postal code or not used
Email address	E	Email address for Email certificates

...

3.3 Identification and Authentication for Re-key Requests

3.3.1 Identification and Authentication for Routines Re-Key

Check21 certificates are not re-keyed.

...

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

...

4.2 Certificate Application Processing

4.2.1 Performing Identification and Authentication Functions

...

4.2.1.6 Check21 Certificates

Validation of Check21 certificates involves validating the organization named in the certificate. This process involves Certicom automatically or manually reviewing the application information provided by the applicant (as per section 4.1 of this CPS) in order to check that:

1. The applicant is authorized to make certificate requests.
 - Validation may be supplemented through the use of the administrator contact associated with the domain name Certicom record for communication with Certicom validation staff or for automated email challenges.

...

4.6 Certificate Renewal

Check21 Certificates are not renewed.

...

4.7 Certificate Re-key

Check21 Certificates are not re-keyed.

4.8 Certificate Modification

Check21 Certificates are not modified.

....

4.9 Certificate Revocation and Suspension

...

4.9.7 CRL Issuance Frequency

An updated Check21 Certificate CRL is published on the Certicom website every 24 hours. Under special circumstances the Check21 Certificate CRL may be published more frequently.

...

4.10 Certificate Status Services

4.10.1 Operational Characteristics

Each Check21 Certificate CRL contains entries for all revoked un-expired Check21 certificates issued and is valid for 24 hours.

...

6 TECHNICAL SECURITY CONTROLS

...

6.1 Key pair generation and installation

...

6.1.5 Key sizes

[Key pairs are of sufficient length to prevent unauthorized determination or reverse engineering of the private key. Certicom keys are either RSA 2048 bit or ECC 163, 256 or 384 bit keys. See Appendix A for the size of each issued key.]

APPENDIX B
CERTIFICATE TYPES

Certicom Certificate offerings may include the following types of certificates:

...

8. Check21 Certificates

Check21 certificates are issued to subscribers who own Unisys or compatible check imaging and archiving machines to provide assurance regarding the ability to digitally sign check image data. With a Check21 certificate, a digital signature can be appended to the check image data in accordance to the Check21 protocol specification.

APPENDIX C
PKI HEIRARCHY

...

8. Check21 Certificate

Certicom RSA Public Primary CA (*serial number = 44 20 79 44 3F B8 89 FD AD 3B FB BA A5 49 9B 51, expiry = 31 December 2029 23:59:59*)

↳ Certicom Check21 CA (*serial number = 54 D0 20 AA A0 F0 62 88 AE 2A 8A 42 CF 2E 92 C3, expiry = 31 December 2026 23:59:59*)

↳ End Entity Check21 Certificate (*serial number = x, expiry = 1 month or up to 5 years from issuance*)

APPENDIX D
CERTIFICATE POLICIES

...

Certicom RSA Check21 CA

Field	Content
Version	v3
Serial Number	54D020AAA0F06288AE2A8A42CF2E92C3
Signature Algorithm	sha1WithRSAEncryption
Issuer	CN=Certicom RSA Public Primary CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US
Validity:	
Not Before	2008-12-04 00:00:00
Not After	2026-12-31 23:59:59
Subject	CN=Certicom RSA Check21 CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US
Public Key:	
Algorithm Identifier	rsaEncryption
Size	2048-bit
Modulus	00C61999F38F5A4E1651B0A79170414F1F655444EB38E5303C40D8BBE238D1C302848EB686107F4FFA596BE1050A640DFDF426D3AF347E09BC3CB33FA2449459BF3C778A7A2E054B32529979329F2017B578827B0122549320311A548E08D2A0B9256B8641CCE210C86B35FA3A9B1AF5EAC71AC4651ABEC1FCE524F0C83BB58C927AC29C606E1C6FC234C14E00F570E32805347789C98C0E4685C9CA593D2C7D0D1033EAE1B6586F5E364CC77CF473B12550D5AE1CBC4551CB0C7559954E7AB6DB38AE2C30532D4EB53A84CA2F9DAA0BF163E035F656451EC34F40ADE3D3589E2353DA30DFBC5F98AD7227E59112FF8AE56900105686429A873733732E996E6311
Public Exponent	65537 (0x10001)
Extensions:	
Authority Key Identifier (non-critical)	Key ID: 7424CE35E5022CF9FFB6DD8E3FA71FEA5C8DDF0D
Subject Key Identifier (non-critical)	731B7585BB0ECD065C1C3864EA6A32D725D23EEB

Key Usage (critical)	Certificate Signing, CRL Signing
Basic Constraints (critical)	Subject Type=CA Path Length Constraint=0
Certificate Policies (non-critical)	OID: anyPolicy CPS URL: http://www.certicom.com/repository/cps
CRL Distribution Points (non-critical)	URI: http://crl.certicom.com/CerticomRSAPublicPrimaryCA.crl
Authority Info Access (non-critical)	CA Issuer: http://crt.usertrust.com/CerticomRSAUTNObjectCA.crt OCSP: http://ocsp.certicom.com
Other Information:	
SHA-1 Thumbprint	DD297A6DA75113A8E3E1F500E007D78BBF78194A
"Official" Filename	CerticomRSACheck21CA.crt
HSM Private Key ID	2005

Check21 Certificates

Field	Content
Version	v3
Serial Number	<a 16-byte integer>
Signature Algorithm	Sha1WithRSAEncryption
Issuer	CN=Certicom RSA Check21 CA OU=Certicom Certification Authority OU=Terms and Conditions of use: http://www.certicom.com/repository O=Certicom Corp. C=US
Validity Period	1 year
Subject	(Required) CN=<Organization Name> (Optional) OU=<Organizational Unit Name 1> (Optional) OU=<Organizational Unit Name 2> (Optional) OU=<Organizational Unit Name 3> (Required) O=<Organization Name> (Optional) Street=<Street Address 1> (Optional) Street=<Street Address 2> (Optional) Street=<Street Address 3> (Optional) L=<Locality Name>

	(Optional) ST=<State or Province Name> (Optional) PostalCode=<Postal Code> (Required) C=<Country Name>
Public Key:	
Algorithm Identifier	id-ecPublicKey
ECPParameters (namedCurve)	sect163k1
ECPPoint	<Supplied by customer>
Extensions:	
Authority Key Identifier (non-critical)	Key ID: 731B7585BB0ECD065C1C3864EA6A32D725D23EEB
Subject Key Identifier (non-critical)	<SHA-1 hash of customer-supplied ECC Public Key>
Key Usage (critical)	Digital Signature, Non Repudiation
Basic Constraints (critical)	Subject Type=End-entity
Certificate Policies (non-critical)	OID: 1.3.132.11.0 CPS URL: http://www.certicom.com/repository/cps
CRL Distribution Points (non-critical)	URI: http://crl.certicom.com/CerticomRSACheck21CA.crl
Authority Info Access (non-critical)	CA Issuer: http://crt.certicom.com/CerticomRSACheck21CA.crt