

Notice of Proposed Changes to CP 1.1
(Typographical and formatting changes have been omitted)

CP Section	Current CP Content	Proposed New CP content
1.1(a)	The Enterprise Security Guide, which describes detailed requirements for Managed PKI Customers and Gateway Customers concerning personnel, physical, telecommunications, logical, and cryptographic key management security	The Enterprise Security Guide, which provides recommendations for Managed PKI Customers and Gateway Customers concerning personnel, physical, telecommunications, logical, and cryptographic key management Security
1.1(a) table 1	N/A	Added: VeriSign Information Systems Security Policy Confidential N/A
1.1(b)	A brief summary of PKI meant to facilitate review of this CP is available at: https://www.verisign.com/repository/training . More general educational and training information is accessible from VeriSign at http://www.verisign.com .	Educational and training information is accessible from VeriSign at http://www.verisign.com .
1.1.1. Table 2	Deleted reference to MPKI for Class 1 certs	Deleted reference to MPKI for Class 1 certs
1.1.1 Table 2 <i>Confirmation of Certificate Applicants' Identity</i>	N/A	deleted"...with the Managed PKI Customer or ..."
1.1.1 Table 2	Same as Class 1 Managed PKI plus checking internal documentation or databases to confirm identity of the Certificate Applicant (e.g., human resources documentation).	Same as Class 1 retail plus checking internal documentation or databases to confirm identity of the Certificate Applicant (e.g., human resources documentation) and that the Certificate Applicant is affiliated with the Managed PKI Customer.
1.1.1 Table 2 > Class 3, Organizations, Retail, Applications implemented or contemplated by Users (CPS § 1.3.4.1)	Server authentication, confidentiality encryption, and (when communicating with other servers) client authentication (Secure Server ID, Global Server ID, OFX, and Wireless Transport Layer Security Certificates); authentication, message integrity, and confidentiality encryption with Electronic Data Interchange (EDI Certificates); and authentication and integrity of software and other content.	Server authentication, (some examples being web, ftp, or directory authentication), secure SSL/TLS sessions, confidentiality encryption, and (when communicating with other servers) client authentication (Secure Server ID, Global Server ID, OFX, and authentication and integrity of software and other content (Code and Content Signing Digital IDs).
1.1.1 Page 9	N/A	Deleted ", and Wireless Transport Layer Security Certificates"

1.1.1 Page 9	...authentication and integrity of software and other content.	...authentication and integrity of software and other content (Code and Content Signing Digital IDs).
1.1.1 Page 9	N/A	Deleted: authentication, message integrity, and confidentiality encryption with Electronic Data Interchange (EDI Certificates)
1.1.2.1.1	The security requirements for Managed PKI are set forth in the Enterprise Security Guide	The security recommendations for Managed PKI are set forth in the Enterprise Security Guide
1.1.2.1.5	Like Managed PKI Customers, a Gateway Customer must meet the standards within the Enterprise Security Guide.	The security recommendations for gateway Customers are set forth in the Enterprise Security Guide.
1.1.2.3.2	<p>1.1.2.3.2 VeriSign Managed PKI Key Manager Services</p> <p>Managed PKI Key Manager permits Managed PKI Customers to generate key pairs on behalf of Subscribers whose Certificate Applications they approve. It also permits Managed PKI Customers to transmit to Subscribers the private keys of such Subscribers in a secure fashion, store a retained backup copy of the Subscribers' private keys in a secure fashion, and recover private keys when needed. Managed PKI Key Manager facilitates both a single key pair system and a dual key pair system. Single key pair systems generate keys that an end-user Subscriber uses for both digital signature and confidentiality functions. The Subscriber obtains one Certificate for both functions. Dual key pair systems, by contrast, generate a key pair that the end-user Subscriber uses for confidentiality. The Subscriber, however, generates his or her own key pair for digital signature functions. In a dual key pair system, the Subscriber receives two Certificates, one for each public key. The Managed PKI Key Manager software operates in conjunction with a VeriSign Key Recovery Service. Managed PKI Key Manager is described in detail in CP § 1.1.2.3.2.</p> <p>Managed PKI Key Manager software stores the backup copy of private keys at the Managed PKI Customer's site in an encrypted form. Each Subscriber's private key is individually encrypted with its unique key encryption key. A key recovery block ("KRB") is generated from this encryption key using key recovery technology, then the encryption key is deleted. Both the Subscriber's encrypted private key and the KRB are stored in the Key Manager database on the Managed PKI Customer's systems.</p> <p>The Managed PKI Key Manager software operates in conjunction with a VeriSign Key Recovery Service. Recovery of a private key requires Managed PKI Key Manager, under the Managed PKI Customer's administrator's direction, to retrieve the KRB from the database and send it online to the Key Recovery Service operated out VeriSign's</p>	<p>1.1.2.3.2 VeriSign Managed PKI Key Management Service</p> <p>Key Management Service is an optional software system installed on an enterprise premises forming part of the VeriSign Managed PKI product family. Key Management Service operates in conjunction with a VeriSign Managed PKI Service. This combination allows an enterprise manager to control the backup and recovery of user private keys and digital certificates.</p> <p>Private keys are stored on the enterprise's premises in encrypted form. Each Subscriber's private key is individually encrypted with its own triple-DES symmetric key generated in FIPS 140-1 level 2 registered hardware. A Key Escrow Record (KER) is generated, then the triple-DES key is combined with a random session key mask also generated in hardware and destroyed. Only the resulting masked session key (MSK) is securely sent and stored at VeriSign. The KER (containing the end user's private key) and the random session key mask are stored in the Key Manager database on the enterprise premises.</p> <p>Recovery of a private key and digital certificate requires the Managed PKI administrator to securely log on to the Managed PKI Control Center, select the appropriate key pair to recover and click a "recover" hyperlink. Only after an approved administrator clicks the "recover" link is the MSK for that key pair returned from the Managed PKI database operated out of VeriSign's secure data center. The Key Manager combines the MSK with the random session key mask and regenerates the triple-DES key which was used to originally encrypt the private key, allowing recovery of the end user's private key. As a final step, an encrypted PKCS#12 file is returned to the administrator and ultimately distributed to the end user.</p>

	secure data center. Only VeriSign holds the private key that can unlock the KRB and recover the embedded encryption key. The recovery request to VeriSign will include enterprise emergency recovery codes needed to authorize the unlocking of the KRB. If a valid KRB is delivered, and the correct emergency recovery codes are supplied, the Key Recovery Service returns the encryption key to the Managed PKI Key Manager software, allowing it to recover the corresponding user private key.	
1.1.2.3.3	The VeriSign Roaming Service encrypts Roaming Subscribers' private keys with symmetric keys that are split and stored on one or two servers in two physical locations to protect against attacks on a single credential server. Specifically, components of these symmetric keys are split between a server residing at the site of the Managed PKI Customer ("Enterprise Roaming Server") (or a trusted fourth party in lieu of the Managed PKI Customer) and another server at VeriSign ("VeriSign Roaming Server"). The private key itself is stored in encrypted form on the Enterprise Roaming Server. The Roaming Subscriber authenticates himself or herself to these server(s) using a password, and assuming the password is successfully provided to the servers, the encrypted private key and the components of the symmetric key needed to decrypt the Subscriber's private key are downloaded to the client terminal. At the client terminal, the symmetric key is reconstituted, the Subscriber's private key is decrypted, and the private key is then available for use during a single session. Following the session, the private key on the client terminal is deleted such that it is unrecoverable.	The VeriSign Roaming Service encrypts Roaming Subscribers' private keys with symmetric keys that are split and stored on one server or two servers in two physical locations to protect against attacks on a single credential server. The private key itself is stored in encrypted form on the Enterprise Roaming Server. The Roaming Subscriber authenticates himself or herself to the server(s) using a password, and assuming the password is successfully provided, the encrypted private key and the components of the symmetric key needed to decrypt the Subscriber's private key are downloaded to the client terminal. At the client terminal, the symmetric key is reconstituted, the Subscriber's private key is decrypted, and the private key is then available for use during a single session. Following the session, the private key on the client terminal is deleted such that it is unrecoverable.
1.3.2	N/A	Moved the following sentence to the top of the paragraph: "RAs assist a CA by performing front-end functions of confirming identity, approving or denying Certificate Applications, requesting revocation of Certificates, and approving or denying renewal requests"
1.3.3	N/A	1. Changed "Class 1- 2 Certificates and Class 3 individual Certificates may either be Retail Certificates or Managed PKI Certificates" to "Class 1 Certificates are Retail Certificates. Class- 2 Certificates and Class 3 individual Certificates may either be Retail Certificates or Managed PKI Certificates." 2. Deleted: • "WTLS servers, Electronic Data Interchange ("EDI") servers"
1.3.4.2	In addition, Class 3 organizational Certificates issued to devices are limited in function to web servers (in the case of Secure Server IDs and Global Server IDs), EDI applications (in the case of EDI Certificates), OFX (in the case of OFX Certificates)	In addition, Class 3 organizational Certificates issued to devices are limited in function to web servers and to secure SSL/TLS sessions (in the case of Secure Server IDs and Global Server IDs), OFX (in the case of OFX Certificates)

1.3.4.1.3.2 - Table 3	N/A	<p>Deleted:</p> <p>1. "WTLS Certificates WTLS server authentication and confidentiality encryption Wireless Application Protocol EDI Certificates Authentication, message integrity, and confidentiality encryption ANSI X12, EDIFACT, and other standards-based message formats"</p> <p>2. "Wireless Transport Layer Security Certificates are defined as a part of the Wireless Application Protocol. They are used to authenticate a WTLS server to a WTLS client, i.e., a wireless handset. In addition, they facilitate encrypted communications between the WTLS server and the WTLS client.</p> <p>Electronic Data Interchange Certificates facilitate secure EDI. EDI is a method of exchanging business documents using computer-to-computer communications between different organizations, thereby bridging external and internal business formats and procedures. Documents sent via EDI include requisitions, purchase orders, billing documents, accounts payable, and fund transfers. Ultimately, EDI allows companies to create a seamless link to their suppliers, distributors, customers, banks, and transportation carriers.</p> <p>EDI Certificates allow the use of digital signatures for messages sent over any open network using ANSI X12, EDIFACT, and other standards-based message formats. Digital signatures on EDI messages provide assurances of authentication and message integrity. In addition, such Certificates enable the encryption of EDI messages."</p>
2.7.4.4	<p>Audit of VeriSign or an Affiliate (Class 1 -3) VeriSign and each Affiliate shall be audited pursuant to the Affiliate Audit Program Guide, which incorporates guidelines provided in the American Institute of Certificate Public Accounts' Statement on Auditing Standards (SAS) Number 70, Reports on the Processing of Transactions by Service Organizations. Their Compliance Audits shall be a SAS 70 Type II Review: A Report of Policies and Procedures in Operation and Test of Operational Effectiveness.</p>	<p>Audit of VeriSign or an Affiliate (Class 1 -3) VeriSign and each Affiliate shall be audited pursuant to the Affiliate Audit Program Guide, which incorporates guidelines provided in the American Institute of Certificate Public Accounts' Statement on Auditing Standards (SAS) Number 70, Reports on the Processing of Transactions by Service Organizations. Their Compliance Audits shall be a SAS 70 Type II Review: A Report of Policies and Procedures in Operation and Test of Operational Effectiveness, or an equivalent audit standard approved by VeriSign.</p>
2.9.4	<p>Finally, without limiting the generality of the foregoing, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares.</p>	<p>Finally, without limiting the generality of the foregoing, Secret Shares of a CA's private key are the property of the CA, and the CA retains all Intellectual Property Right in and to such Secret Shares even though they cannot obtain physical possession of the those shares or the CA from VeriSign.</p>

3.1.8.1.1	<ul style="list-style-type: none"> • A confirmation by telephone, confirmatory postal mail, or comparable procedure to the Certificate Applicant to confirm certain information about the organization, confirm that the organization has authorized the Certificate Application, and confirm that the person submitting the Certificate Application on behalf of the Certificate Applicant is authorized to do so, and 	<ul style="list-style-type: none"> • A confirmation of the employment of the Organizational contact with the Organization by telephone, confirmatory postal mail, or comparable procedure and further confirming with the Organizational contact by telephone, postal mail, or a comparable procedure certain information about the organization and that the organization has authorized the Certificate Application. and
3.1.8.1.1	<ul style="list-style-type: none"> • In the case of Global Server IDs, the additional checks necessary to satisfy United States export regulations and licenses issued by the United States Department of Commerce Bureau of Export Administration (“BXA”). 	<ul style="list-style-type: none"> • In the case of Global Server IDs, the additional checks necessary to satisfy United States export regulations and licenses issued by the United States Department of Commerce Bureau of Industry and Science (“BIS”) (formerly known as the Bureau of Export Administration (“BXA”).
3.1.9.3	N/A	<p>Added: VeriSign and Affiliate may approve Administrator Certificates to be associated with a non-human recipient such as a device, or a server. Authentication of a Class 3 Administrator Certificate Applications for a non-human recipient shall include:</p> <ul style="list-style-type: none"> • Authentication of the existence and identity of the service named as the Administrator in the Certificate Application • Authentication that the service has been securely implemented in a manner consistent with it performing an Administrative function • Confirmation of the employment and authorization of the person enrolling for the Administrator certificate for the service named as Administrator in the Certificate Application.
3.2.1	<p>One acceptable procedures is through the use of a Challenge Phrase. Subscribers choose and submit with their enrollment information a Challenge Phrase. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber’s Challenge Phrase with the Subscriber’s reenrollment information, and the enrollment information (other than contact information) has not changed, a renewal Certificate is automatically issued.</p>	<p>One acceptable procedures is through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key. Subscribers choose and submit with their enrollment information a Challenge Phrase. Upon renewal of a Certificate, if a Subscriber correctly submits the Subscriber’s Challenge Phrase with the Subscriber’s reenrollment information, and the enrollment information (including contact information) has not changed, a renewal Certificate is automatically issued. After rekeying or renewal in this fashion, and on at least alternative instances of subsequent rekeying or renewal thereafter, the CA or RA shall reconfirm the identity of the Subscriber in accordance with the requirements specified in its CPS for the authentication of an original Certificate Application.</p>
3.3	<p>...Renewal of an individual Certificate following revocation again must ensure that the person seeking renewal is, in fact, the Subscriber. One acceptable procedure is the use of a Challenge Phrase, as described in CP § 3.2.1. Other than this procedure or another VeriSign-approved procedure, the requirements for the validation of an original Certificate Application in CP §§ 3.1.8.1, 3.1.9 shall be used</p>	<p>..Renewal of an individual Certificate following revocation again must ensure that the person seeking renewal is, in fact, the Subscriber. One acceptable procedure is the use of a Challenge Phrase (or the equivalent thereof), as described in CP § 3.2.1. Other than this procedure or another VeriSign-approved procedure, the requirements for the validation of an original Certificate Application in CP §§ 3.1.8.1, 3.1.9 shall be used for</p>

	for renewing a Certificate following revocation.	renewing a Certificate following revocation.
3.4	<ul style="list-style-type: none"> Having the Subscriber submit the Subscriber's Challenge Phrase and revoking the Certificate automatically if it matches the Challenge Phrase on record, 	<ul style="list-style-type: none"> Having the Subscriber submit the Subscriber's Challenge Phrase (or the equivalent thereof) and revoking the Certificate automatically if it matches the Challenge Phrase (or the equivalent, thereof) on record,
4.1.1.	Certificate Applications are submitted either to a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer for processing, either approval or denial.	Certificate Applications are submitted either to a Processing Center, Service Center, Managed PKI Customer, or Gateway Customer for processing and ultimate approval or denial.
4.4.1.1	N/A	Added: "• the continued use of that certificate is harmful to the VTN."
4.4.1.2	N/A	Added: "• the continued use of that certificate is harmful to the VTN."
4.4.9	If a Certificate listed in a CRL expires, it shall be removed from later-issued CRLs starting thirty (30) days after the Certificate's expiration.	If a Certificate listed in a CRL expires, it may be removed from later-issued CRLs starting thirty (30) days after the Certificate's expiration.
4.5.2	Audit log reviews include a verification that the log has not been tampered with, a brief inspection of all log entries, and a more thorough investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also be documented.	Audit log reviews include a verification that the log has not been tampered with, an inspection of all log entries, and an investigation of any alerts or irregularities in the logs. Actions taken based on audit log reviews are also be documented.
4.8	Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: application logs, Certificate Application data, audit data (per CP § 4.5), and database records for all Certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with CP § 6.2.4. Processing Centers shall maintain backups of the foregoing CA information for their own CAs, as well as the CAs of Service Centers, Managed PKI Customers, and ASB Customers within their Subdomains.	Backups of the following CA information shall be kept in off-site storage and made available in the event of a Compromise or disaster: application logs, Certificate Application data, audit data (per CP § 4.5), and database records for all Certificates issued. Back-ups of CA private keys shall be generated and maintained in accordance with CP § 6.2.4. Processing Centers shall maintain backups of the foregoing CA information for their own CAs, as well as the CAs of Service Centers, Managed PKI Customers, and ASB Customers within their Subdomains.
5.1.1	Managed PKI and Gateway physical environments shall comply with the recommend Enterprise Security Guide.	VeriSign recommends that Managed PKI and Gateway Customer physical environments comply with the recommendations provided in Enterprise Security Guide.
5.3.2	The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person are discussed in the Security and Audit Requirements Guide, but in general fall within the following categories: <ul style="list-style-type: none"> Misrepresentations made by the candidate or Trusted Person, Highly unfavorable or unreliable personal references, Certain criminal convictions, and Indications of a lack of financial responsibility. 	The factors revealed in a background check that may be considered grounds for rejecting candidates for Trusted Positions or for taking action against an existing Trusted Person are discussed in the Security and Audit Requirements Guide, generally include (but are not limited to) the following: <ul style="list-style-type: none"> Misrepresentations made by the candidate or Trusted Person, Highly unfavorable or unreliable professional references, Certain criminal convictions, and Indications of a lack of financial responsibility.
6.1.9	N/A	Replaced RFC 2459, January 1999 with RFC 3280 April 2002.

6.2.2	6.2.2 Private Key (n out of m) Multi-Person Control	6.2.2 Private Key (m out of n) Multi-Person Control
6.2.2	A threshold number of Secret Shares (n) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (m) is required to activate a CA private key stored on the module	A threshold number of Secret Shares (m) out of the total number of Secret Shares created and distributed for a particular hardware cryptographic module (n) is required to activate a CA private key stored on the module
6.2.2	N/A	Deleted Table 9 and replace with the following: The threshold number of shares needed to sign a CA certificate is 3. It should be noted that the number of shares distributed for disaster recovery tokens may be less than the number distributed for operational tokens, while the threshold number of required shares remains the same. Secret Shares are protected in accordance with CPS § 6.4.2.
6.2.3	Managed PKI Customers using the Managed PKI Key Manager service are permitted to escrow end-user Subscribers' single private key (in single key pair systems) or to escrow the decryption private key (in dual key pair systems). Escrowed private keys shall be stored in encrypted form using the Managed PKI Key Manager software. Except for Managed PKI Customers using the Managed PKI Key Manager service, the private keys of CAs or end-user Subscribers shall not be escrowed.	Managed PKI Customers using the Managed PKI Key Management service are permitted to escrow end-user Subscribers' private key as described in CP §1.1.2.3.2. Escrowed private keys shall be stored in encrypted form using the Managed PKI Key Manager software. Except for Managed PKI Customers using the Managed PKI Key Manager service, the private keys of CAs or end-user Subscribers shall not be escrowed.
6.2.7.4	An online CA's private key shall be activated by a threshold number of Shareholders, as defined in CP § 6.2.2, supplying their activation data.	An online CA's private key shall be activated by a threshold number of Shareholders, as defined in CP § 6.2.2, supplying their activation data (stored on secure media).
6.3.2 Table 10	N/A	Added CA to end-user administrator devices with a validity period of up to 5 years for each class of certificate
6.5	CA and RA functions shall take place on Trustworthy Systems in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates), or the Enterprise Security Guide (in the case of Managed PKI Customers and Gateway Customers).	CA and RA functions shall take place on Trustworthy Systems in accordance with the Security and Audit Requirements Guide (in the case of VeriSign and Affiliates). VeriSign recommends that Managed PKI Customers and Gateway Customers follow the guidelines provided in Enterprise Security Guide.
7.1	N/A	Replaced RFC 2459 January 1999 with RFC 3280 April 2002
7.1	WTLS Certificates shall conform to the most current version of the Wireless Application Protocol.	WTLS Certificates conform to the most current version of the Wireless Application Protocol.

7.1.1	<p>Except for WTLS Certificates, all VTN Certificates shall be X.509 Version 3 Certificates although certain Root Certificates are permitted to be X.509 Version 1 Certificates to support legacy systems. Processing Centers shall issue X.509 Version 1 or Version 3 CA Certificates. Also, Processing Centers and Gateway Customers shall issue X.509 Version 3 end-user Subscriber Certificates. Processing Centers shall issue WTLS Certificates that conform to the most current version of the Wireless Application Protocol.</p>	<p>Except for WTLS Certificates, that conformed to the most current version of the Wireless Application Protocol, all VTN Certificates shall be X.509 Version 3 Certificates although certain Root Certificates are permitted to be X.509 Version 1 Certificates to support legacy systems. Processing Centers shall issue X.509 Version 1 or Version 3 CA Certificates. Also, Processing Centers and Gateway Customers shall issue X.509 Version 3 end-user Subscriber Certificates.</p>
7.1.2.1	<p>Processing Centers and Gateway Customers shall populate the KeyUsage extension of X.509 Version 3 CA, Automated Administration, and end-user Subscriber Certificates by setting and clearing the bit(s) and the criticality field in accordance with CP § 6.1.9. The criticality field of this extension shall be set to FALSE.</p>	<p>Processing Centers and Gateway Customers shall populate the KeyUsage extension of X.509 Version 3 CA, Automated Administration, and end-user Subscriber Certificates by setting and clearing the bit(s) and the criticality field in accordance with CP § 6.1.9. The criticality field of this extension is generally set to FALSE.</p>
7.1.2.5	<p>Processing Centers and Gateway Customers, shall populate X.509 Version 3 VTN Certificates with an ExtendedKeyUsage extension configured so as to set and clear bits and the criticality field in accordance with Table 12 below.</p>	<p>Processing Centers and Gateway Customers, shall populate X.509 Version 3 VTN End-Entity Certificates with an ExtendedKeyUsage extension configured to include the key purpose object identifiers (OID) shown in Table 12 below. By default, ExtendedKeyUsage is set as a non-critical extension. VTN CA Certificates generally do not include the ExtendedKeyUsage extension. [NOTE Table 12 has also been updated]</p>
7.1.2.7	<p>Processing Centers and Gateway Customers shall populate X.509 Version 3 VTN Certificates with an authorityKeyIdentifier extension, and the method for generating the keyIdentifier based on the public key of the CA issuing the Certificate shall be calculated in accordance with one of the methods described in RFC 2459. The criticality field of this extension shall be set to FALSE.</p>	<p>Processing Centers and Gateway Customers generally populate X.509 Version 3 VTN Certificates with an authorityKeyIdentifier extension, and the method for generating the keyIdentifier based on the public key of the CA issuing the Certificate shall be calculated in accordance with one of the methods described in RFC 3280. The criticality field of this extension shall be set to FALSE.</p>

7.1.3	<p>Processing Centers and Gateway Customers shall sign VTN Certificates using one of following algorithms.</p> <p>sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}</p> <p>md5WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}</p> <p>md2WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 2}</p> <p>id-dsa-with-sha1 ID ::= { iso(1) member-body(2) us(840) x9-57 (10040) x9cm(4) 3}</p> <p>Certificate signatures produced using these algorithms shall comply with RFC 2459. Use of sha-1WithRSAEncryption shall be given strong preference over md5WithRSAEncryption. Use of md5WithRSAEncryption shall be given very strong preference over md2WithRSAEncryption</p>	<p>Processing Centers and Gateway Customers shall sign VTN Certificates using one of following algorithms.</p> <p>sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}</p> <p>md5WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 4}</p> <p>md2WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 2}</p> <p>Certificate signatures produced using these algorithms shall comply with RFC 3279. Use of sha-1WithRSAEncryption shall be given strong preference over md5WithRSAEncryption. Use of md5WithRSAEncryption shall be given very strong preference over md2WithRSAEncryption (which was used to sign certain legacy CA and End-User Subscriber Certificates)</p>
7.2	7.2 CRL Profile	7.2 CRL and OCSP Profile
7.2	Processing Centers and Gateway Customers shall issue CRLs that conform to RFC2459.	Processing Centers and Gateway Customers shall issue CRLs that conform to RFC 3280 and OCSP responders that conform with RFC2560 (with the exception of including nonce as one of the requestExtensions in requests).
7.2	N/A	Replaced RFC 2459 with RFC 3280
8.2.2	This CP is published in electronic form within the VeriSign Repository at https://www.verisign.com/CP . The CP is available in the VeriSign Repository in Word format, Adobe Acrobat pdf, and HTML. VeriSign also makes the CP available in Adobe Acrobat pdf or Word format upon request sent to practices@verisign.com . The CP is available in paper form from the PMA upon requests sent to: VeriSign, Inc., 487 E. Middlefield Road, Mountain View, CA 94043 USA, Attn: Practices and External Affairs – CP	This CP is published in electronic form within the VeriSign Repository at https://www.verisign.com/CP . The CP is available in paper form from the PMA upon requests sent to: VeriSign, Inc., 487 E. Middlefield Road, Mountain View, CA 94043 USA, Attn: Practices and External Affairs – CP.
Definitions	N/A	Added BIS
	The United States Bureau of Export Administration of the United States Department of Commerce	The United States Bureau of Export Administration of the United States Department of Commerce (which has been replaced by the BIS)
	Enterprise security guide: A document setting forth security requirements and practices for Managed PKI Customers and Gateway Customers	Enterprise Security Guide: A document setting forth security recommendations for Managed PKI Customers and Gateway Customers
		added EOL footnote for EDI

