

Notice of Proposed Amendments to CPS 2.1
(Typographical and formatting changes have been omitted)

CPS Section	Current CPS Content	Proposed New CPS content
1.1(a)	N/A	Added: VeriSign may publish Certificate policies supplemental to this CPS in order comply with the specific policy requirements of Government, or other industry standards requirements. These supplemental certificate policies shall be made available to subscribers for the certificates issued under the supplemental policies and their relying parties.
	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
1.1.1. Table 2	N/A	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 Class 2 MPKI > Confirmation of Certificate Applicants' Identity	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:	Check of third-party database or other documentation showing proof of right to use the organizational name. Validation check by telephone (or comparable procedure) to confirm information in, and authorization of, the Certificate Application. In the case of web server Certificates, confirmation that the Certificate Applicant has the right to use the domain name to be placed in the Certificate.	Automated, and/or manual check of third-party database or other documentation showing proof of right to use the organizational name. Validation check by telephone (or comparable procedure) to confirm information in, and authorization of, the Certificate Application. In the case of web server Certificates, confirmation that the Certificate Applicant has the right to use the domain name to be placed in the Certificate.
1.1.1. Table 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	Server authentication, (some examples being web, ftp, or directory authentication), secure SSL/TLS sessions, confidentiality encryption, and (when communicating with other servers) client authentication
	N/A	Deleted ", and Wireless Transport Layer Security Certificates"
	N/A	Added footnote that Secure Server ID is offered as Secure Site Services and Global server IDs are offered as Commerce Site Services
	...and authentication and integrity of software and other content.	and authentication and integrity of software and other content (VeriSign Code and Content Signing Digital IDs).

	authentication, message integrity, and confidentiality encryption with Electronic Data Interchange (EDI Certificates)	Deleted: authentication, message integrity, and confidentiality encryption with Electronic Data Interchange (EDI Certificates)
1.1.2.1.1	Customers of VeriSign obtaining VeriSign Managed PKI ("Managed PKI Customers") fall into three categories.	Customers of VeriSign Managed PKI ("Managed PKI Customers") fall into three categories.
	Within VeriSign's Subdomain, the security requirements for Managed PKI are set forth in the Enterprise Security Guide.	Within VeriSign's Subdomain, the security recommendations for Managed PKI are set forth in the Enterprise Security Guide.
	For a discussion of the differences between Secure Server IDs and Global Server IDs, see CPS § 1.3.4.1.3.2	Deleted: (For a discussion of the differences between Secure Server IDs and Global Server IDs, see CPS § 1.3.4.1.3.2.)
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>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</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>

	<p>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 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.</p>	
1.1.2.3.3	<p>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.</p>	<p>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.</p>
1.3	<p>Most of the VeriSign Subdomain Participants are located in the United States of America. VeriSign authenticates Class 3 Administrator Certificate Applications for Managed PKI Customer and trusted third party employees as follows.</p>	<p>Deleted : Most of the VeriSign Subdomain Participants are located in the United States of America. VeriSign authenticates Class 3 Administrator Certificate Applications for Managed PKI Customer and trusted third party employees as follows.</p>
1.3.3 Table 4 - Class 1	<p>Individuals who are, in relation to the Managed PKI Customer or Gateway Customer, an Affiliated Individual.</p>	<p>Individuals who are affiliated with Gateway Customer.</p>
1.3.3 Table 4 - Class 3 > Organizations > retail	<ul style="list-style-type: none"> • WTLS Servers • Electronic Data Interchange servers 	<p>Deleted:</p> <ul style="list-style-type: none"> • WTLS Servers • Electronic Data Interchange servers
1.3.4.2	<p>EDI applications (in the case of EDI Certificates) and added a footnote that it has been EOL'd</p>	<p>Deleted: EDI applications (in the case of EDI Certificates) and added a footnote that it has been EOL'd</p>
	<p>In addition, Class 3 organizational Certificates issued to devices are limited in function to web servers or web traffic management devices (in the case of Secure Server IDs and Global Server IDs)</p>	<p>In addition, Class 3 organizational Certificates issued to devices are limited in function to web servers or web traffic management devices (in the case of Secure Server IDs and Global Server IDs) and to secure SSL/TLS sessions</p>

2.7	<p>An annual SAS 70 Type II audit is performed for VeriSign's data center operations and key management operations supporting VeriSign's public and Managed PKI CA services. In addition, an annual WebTrust for Certification Authorities examination is performed for the VTN Root CAs, Class 3 Organizational CAs, Class 2 Organizational and Individual CAs, and Class 1 Individual CAs specified in CPS § 1.3.1. Customer-specific CAs are not specifically audited as part of the audit of VeriSign's operations unless required by the Customer. VeriSign shall be entitled to require that Managed PKI Customers and Gateway Customers undergo a compliance audit under this CPS § 2.7 and audit programs for these types of Customers.</p> <p>In addition to compliance audits, VeriSign shall be entitled to perform other reviews and investigations to ensure the trustworthiness of VeriSign's Subdomain of the VTN, which include, but are not limited to:</p> <ul style="list-style-type: none"> • VeriSign shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on itself or a Customer in the event VeriSign has reason to believe that the audited entity has failed to meet VTN Standards, has experienced an incident or Compromise, or has acted or failed to act, such that the audited entity's failure, the incident or Compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the VTN. • VeriSign shall be entitled to perform "Supplemental Risk Management Reviews" on itself or a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business. <p>VeriSign shall be entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with VeriSign and the personnel performing the audit, review, or investigation.</p>	<p>An annual WebTrust for Certification Authorities examination is performed for VeriSign's data center operations and key management operations supporting VeriSign's public and Managed PKI CA services including the VTN Root CAs, Class 3 Organizational CAs, Class 2 Organizational and Individual CAs, and Class 1 Individual CAs specified in CPS § 1.3.1. Customer-specific CAs are not specifically audited as part of the audit of VeriSign's operations unless required by the Customer. VeriSign shall be entitled to require that Managed PKI Customers and Gateway Customers undergo a compliance audit under this CPS § 2.7 and audit programs for these types of Customers.</p> <p>In addition to compliance audits, VeriSign shall be entitled to perform other reviews and investigations to ensure the trustworthiness of VeriSign's Subdomain of the VTN, which include, but are not limited to:</p> <ul style="list-style-type: none"> • VeriSign shall be entitled, within its sole and exclusive discretion, to perform at any time an "Exigent Audit/Investigation" on a Customer in the event VeriSign has reason to believe that the audited entity has failed to meet VTN Standards, has experienced an incident or Compromise, or has acted or failed to act, such that the audited entity's failure, the incident or Compromise, or the act or failure to act poses an actual or potential threat to the security or integrity of the VTN. • VeriSign shall be entitled to perform "Supplemental Risk Management Reviews" a Customer following incomplete or exceptional findings in a Compliance Audit or as part of the overall risk management process in the ordinary course of business. <p>VeriSign shall be entitled to delegate the performance of these audits, reviews, and investigations to a third party audit firm. Entities that are subject to an audit, review, or investigation shall provide reasonable cooperation with VeriSign and the personnel performing the audit, review, or investigation.</p>
2.7.4	<p>The scope of VeriSign's annual SAS 70 Type II audit includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls,. In addition, the scope of VeriSign's annual WebTrust for Certification Authorities examination includes certificate life cycle management and CA business practices disclosure.</p>	<p>The scope of VeriSign's annual WebTrust for Certification Authorities (or equivalent) audit includes CA environmental controls, key management operations and Infrastructure/Administrative CA controls, certificate life cycle management and CA business practices disclosure.</p>
2.7.6	<p>Results of the compliance audit of VeriSign's operations may be released at the discretion of VeriSign management.</p>	<p>A copy of VeriSign's WebTrust for CA audit report can be found at http://www.verisign.com/repository.</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, a CA's private key is the property of the CA, and the CA retains all Intellectual Property Right in and to such its private key.</p>
3.1.1 Table 9 > Organization (O) =	<p>Not used for code/object signing Certificates</p>	<p>Deleted: Not used for code/object signing Certificates</p>

3.1.1 Table 9 > E-Mail Address (E) =	E-mail address for Class 1 individual Certificates.	E-mail address for Class 1 individual Certificates and MPKI Subscriber Certificates
3.1.8.1.1	<ul style="list-style-type: none"> Confirming with an appropriate Organizational contact by telephone, postal mail, or a comparable procedure certain information about the organization, that the organization has authorized the Certificate Application, and that the person submitting the Certificate Application on behalf of the Organization is authorized to do so. 	<ul style="list-style-type: none"> Confirming the employment of the Organizational contact with the Organization 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.
3.1.8.1.1	N/A	Added to Table 10: "Hardware Protected SSL : VeriSign verifies that the key pair was generated on FIPS 140 certified hardware"
	N/A	Added to table 10: "Managed PKI for Intranet SSL Certificates: VeriSign verifies that the host name or IP address assigned to a Device is not accessible from the Internet (publicly facing), and is owned by the Certificate Subscriber."
	VeriSign performs performing 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").	VeriSign performs 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")).
	VeriSign verifies that the Organization is classified under one of the following SIC codes	VeriSign verifies that the Organization is a bank or financial institution, or classified under one of the following SIC codes
3.1.9.3.1	The authentication of Class 3 individual Certificate Applications is based on the personal (physical) presence of the Certificate Applicant before an authorized VeriSign representative, Managed PKI Customer, notary public, or other official with comparable authority within the Certificate Applicant's jurisdiction. The agent, notary or other official checks the identity of the Certificate Applicant against a well-recognized form of government-issued identification, such as a passport or driver's license and one other identification credential.	The authentication of Class 3 individual Certificate Applications is based on the personal (physical) presence of the Certificate Applicant before an authorized VeriSign representative, Managed PKI Customer, notary public, or other official with comparable authority within the Certificate Applicant's jurisdiction. The authorized representative, MPKI customer, notary or other official checks the identity of the Certificate Applicant against a well-recognized form of government-issued identification, such as a passport or driver's license and one other identification credential.
3.1.9.3.2	VeriSign authenticates Class 3 Administrator Certificate Applications for Managed PKI Customer and trusted fourth party employees as follows	VeriSign authenticates Class 3 Administrator Certificate Applications for Managed PKI Customer and trusted third party employees as follows
3.1.9.3.2	N/A	Added: "VeriSign may also approve Certificate Applications for its own Administrator Certificates to be associated with a non-human recipient such as a device, or a service. VeriSign authenticates Class 3 Administrator Certificate Applications for a non-human recipient as follows: <ul style="list-style-type: none"> VeriSign authenticates the existence and identity of the service named as the Administrator in the Certificate Application VeriSign authenticates that the service has been securely implemented in a manner consistent with it performing an Administrative function VeriSign confirms the employment and authorization of the person enrolling for the Administrator certificate for the service named as Administrator in the Certificate Application."

3.2	<p>Class 1, Class 2, Class 3 Code and Object Signing, and Class 3 Administrator Certificates</p> <p>For these types of Certificates, Subscriber key pairs are browser generated as part of the online enrollment process. The Subscriber does not have the option to submit an existing key pair for "renewal." Accordingly, for these types of Certificates, rekey is supported and Certificate renewal is not.</p>	<p>Class 1, Class 2, Class 3 Code and Object Signing, and Class 3 Administrator Certificates</p> <p>For these types of Certificates, Subscriber key pairs are generally browser generated as part of the online enrollment process and the Subscriber does not have the option to submit an existing key pair for "renewal." Accordingly, for these types of Certificates, rekey is supported and Certificate renewal is not.</p> <p>In so far as a Subscriber is able to submit an existing key pair for "renewal" VeriSign may renew the certificate renew that Certificate. However, VeriSign recommends that customers generate a new key pair as that is most secure.</p>
3.2.1	<p>For all VeriSign Certificates (except for Class 3 Organizational ASB certificates), VeriSign or the Managed PKI Customer authenticates Subscribers seeking Certificate replacement through the use of a Challenge Phrase.</p> <p>Upon rekey or renewal of a Certificate within the specified timeframe, 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 new Certificate is automatically issued.</p> <p>N/A</p>	<p>For all VeriSign Certificates (except for Class 3 Organizational ASB certificates), VeriSign or the Managed PKI Customer authenticates Subscribers seeking Certificate replacement through the use of a Challenge Phrase (or the equivalent thereof), or proof of possession of the private key.</p> <p>Upon rekey or renewal of a Certificate within the specified timeframe, if a Subscriber correctly submits the Subscriber's Challenge Phrase (or the equivalent thereof) with the Subscriber's reenrollment information, or proves possession of the private key and the enrollment information (including contact information) has not changed, a new Certificate is automatically issued.</p> <p>Added footnote: Where the subscriber is unable to use a challenge phrase the subscriber's reenrollment information will be reauthenticated by VeriSign or the Managed PKI customer</p>
3.3	<p>For replacement of an organizational or individual Certificate following revocation of the Certificate, VeriSign verifies that the person seeking certificate replacement is, in fact, the Subscriber (for individuals) or an authorized organizational representative (for organizations) through the use of a Challenge Phrase, as described in CPS § 3.2.1. Other than this procedure, the requirements for the validation of an original Certificate Application in CPS §§ 3.1.8.1, 3.1.9 are used for replacing a Certificate following revocation. Such Certificates contain the same Subject distinguished name as the Subject distinguished name of the Certificate being replaced.</p>	<p>For replacement of an organizational or individual Certificate following revocation of the Certificate, VeriSign verifies that the person seeking certificate replacement is, in fact, the Subscriber (for individuals) or an authorized organizational representative (for organizations) through the use of a Challenge Phrase (or the equivalent thereof), as described in CPS § 3.2.1. Other than this procedure, the requirements for the validation of an original Certificate Application in CPS §§ 3.1.8.1, 3.1.9 are used for replacing a Certificate following revocation. Such Certificates contain the same Subject distinguished name as the Subject distinguished name of the Certificate being replaced.</p>
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,
4.4.1.1	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	Expired Certificates are removed from the CRL starting thirty (30) days after the Certificate's expiration.	Expired Certificates may be removed from the CRL 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.
4.8.2	VeriSign maintains offsite backups of important CA information for VeriSign CAs as well as the CAs of Service Centers, Managed PKI Customers, and ASB Customers within VeriSign's Subdomain. Such information includes, but is not limited to: application logs, Certificate Application data, audit data (per CPS § 4.5), and database records for all Certificates issued.	VeriSign maintains offsite backups of important CA information for VeriSign CAs as well as the CAs of Service Centers, Managed PKI Customers, and ASB Customers within VeriSign's Subdomain. Such information includes, but is not limited to: Certificate Application data, audit data (per CPS § 4.5), and database records for all Certificates issued.
4.8.3	Compromise Incident Response Team (CIRT).	VeriSign Security Incident Response Team (VSIRT).
5.1.1	VeriSign's CA and RA operations are conducted within VeriSign's primary facilities in Mountain View, California, which meet the requirements of Security and Audit Requirements. All VeriSign CA and RA operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration... ...VeriSign also maintains disaster recovery facilities in Herndon, Virginia for its CA operations. VeriSign's disaster recovery facilities are protected by multiple tiers of physical security comparable to those of VeriSign's primary facility....	VeriSign's CA and RA operations are conducted within facilities which meet the requirements of VeriSign's Security and Audit Requirements Guide. All VeriSign CA and RA operations are conducted within a physically protected environment designed to deter, prevent, and detect covert or overt penetration... ...VeriSign also maintains disaster recovery facilities for its CA operations. VeriSign's disaster recovery facilities are protected by multiple tiers of physical security comparable to those of VeriSign's primary facility...
	VeriSign's primary facilities have seven physical security tiers as described in CPS § 5.1.2 with : •RA validation operations, performed within Tier 3 •CA functions, and performed within Tier 4 •Sensitive servers, including the VeriSign Roaming Server, located in Tier 4 •Online CA cryptographic modules stored in Tier 5 •Offline CA cryptographic modules stored in Tier 7.	Deleted: VeriSign's primary facilities have seven physical security tiers as described in CPS § 5.1.2 with : •RA validation operations, performed within Tier 3 •CA functions, and performed within Tier 4 •Sensitive servers, including the VeriSign Roaming Server, located in Tier 4 •Online CA cryptographic modules stored in Tier 5 •Offline CA cryptographic modules stored in Tier 7.
	Managed PKI Customers and Gateway Customers must ensure that their secure facilities meet the requirements in the Enterprise Security Guide.	Managed PKI Customers and Gateway Customers must ensure that their facilities are secure. VeriSign recommends that Managed PKI Customers and Gateway Customers follow the recommendations provided in Enterprise Security Guide.

5.1.2	VeriSign CA systems are protected by four tiers of physical security, with access to the lower tier required before gaining access to the higher tier. In addition, the physical security system includes three additional tiers for key management security. The characteristics and requirements of each tier are described in Table 15 below.	VeriSign CA systems are protected by a minimum of four tiers of physical security, with access to the lower tier required before gaining access to the higher tier. Progressively restrictive physical access privileges control access to each tier. Sensitive CA operational activity, any activity related to the lifecycle of the certification process such as authentication, verification, and issuance, occur within very restrictive physical tiers. Access to each tier requires the use of a proximity card employee badge. Physical access is automatically logged and video recorded. Additional tiers enforce individual access control through the use of two factor authentication including biometrics. Unescorted personnel, including untrusted employees or visitors, are not allowed into such secured areas. The physical security system includes additional tiers for key management security which serves to protect both online and offline storage of CSUs and keying material. Areas used to create and store cryptographic material enforce dual control, each through the use of two factor authentication including biometrics. Online CSUs are protected through the use of locked cabinets. Offline CSUs are protected through the use of locked safes, cabinets and containers. Access to CSUs and keying material is restricted in accordance with VeriSign's segregation of duties requirements. The opening and closing of cabinets or containers in these tiers is logged for audit purposes. DELETED TABLE 15
5.2.2	Other operations such as the validation and issuance of Class 3 Certificates require the participation of at least 2 Trusted Persons.	Other manual operations such as the manual validation and issuance of Class 3 Certificates require the participation of at least 2 Trusted Persons, or a combination of at least one trusted person and an automated validation and issuance process..
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 generally include the following: • 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 generally include (but are not limited to) the following: • 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.
5.3.3	VeriSign provides its personnel with training upon hire and the requisite on-the-job training needed for personnel to perform their job responsibilities competently and satisfactorily. VeriSign periodically reviews and enhances its training programs as necessary.	VeriSign provides its personnel with training upon hire as well as the requisite on-the-job training needed for them to perform their job responsibilities competently and satisfactorily. VeriSign maintains records of such training. VeriSign periodically reviews and enhances its training programs as necessary.
5.3.7	Independent contractors and consultants who have not completed the background check procedures specified in CPS § 5.3.2 are permitted access to VeriSign's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons.	Independent contractors and consultants who have not completed or passed the background check procedures specified in CPS § 5.3.2 are permitted access to VeriSign's secure facilities only to the extent they are escorted and directly supervised by Trusted Persons at all times.
5.3.8	VeriSign personnel involved in the operation of VeriSign's PKI services are required to read this CPS, the VTN CP, and the VeriSign Security Policy. VeriSign provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.	VeriSign provides its employees the requisite training and other documentation needed to perform their job responsibilities competently and satisfactorily.

6.1.2	N/A	Added: Where end-user Subscriber key pairs are pre-generated by Managed PKI Customers on hardware tokens or smart cards, such devices are distributed to the end-user Subscriber using a commercial delivery service and tamper evident packaging. The required activation data required to activate the device is communicated to the RA or end-user Subscriber using an out of band process. The distribution of such devices is logged by the Managed PKI Customer.
6.1.4	Microsoft and Netscape	Deleted "Microsoft and Netscape"
6.1.9	RFC 2459, January 1999	Replaced RFC 2459, January 1999 with RFC 3280 April 2002.
	. In addition, VeriSign does not currently use the Key Usage extension for WTLS Certificates.	. In addition, VeriSign did not use the Key Usage extension for WTLS Certificates.
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
	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
	Table 17	Deleted Table 17 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	VeriSign does not escrow CA, RA or end-user Subscriber private keys with any third party for purposes of access by law enforcement. Managed PKI Customers using Managed PKI Key Manager can escrow copies of the private keys of Subscribers whose Certificate Applications they approve. VeriSign does not store copies of Subscriber private keys but plays an important role in the Subscriber key recovery process as described below: •For each end user key pair backed up, the Managed PKI Key Manager randomly generates a symmetric key used to encrypt the backed up private key at the Customer site. This encrypted private key is then stored in the local database at the Customer site. The symmetric key is also encrypted, using a public key belonging to the VeriSign key recovery service, and stored in the local database at the Customer site. • When an end user's backed up private key must be recovered, the Managed PKI administrator identifies the appropriate key using the key history stored by the Key Manager at the Customer site, and sends the corresponding encrypted symmetric key to the VeriSign Recovery Service. The VeriSign Key Recovery Service decrypts and returns the symmetric key, which is then used locally to decrypt the end user's private key from the database. This key and the corresponding certificate can then be redistributed to the end user.	VeriSign does not escrow CA, RA or end-user Subscriber private keys with any third party for purposes of access by law enforcement. CA private signature keys shall not be escrowed by a third party. Managed PKI Customers using Managed PKI Key Management Service can escrow copies of the private keys of Subscribers whose Certificate Applications they approve. VeriSign does not store copies of Subscriber private keys but plays an important role in the Subscriber key recovery process as described in CPS § 1.1.2.3.2.
6.2.7.4	VeriSign CA private keys are activated by a threshold number of Shareholders supplying their activation data (tokens or passphrases)	VeriSign CA private keys are activated by a threshold number of Shareholders supplying their activation data (stored on secure media)

6.3.2 Table 18	N/A	Added CA to end-user administrator devices with a validity period of up to 5 years for each class of certificate
6.3.2	Table 19	Deleted Table 19
6.3.2	VeriSign also operates several legacy self-signed issuing root CAs which are part of the VeriSign Trust Network. End-user Subscriber Certificates issued by these CAs meet the requirements for CA to end-user Subscriber Certificates specified in Table 18 above. The requirements for these CAs are described in Table 19 below.	VeriSign also operates the RSA Secure Server CA as a legacy self-signed issuing root CA which is part of the VeriSign Trust Network. End-user Subscriber Certificates issued by this CA meet the requirements for CA to end-user Subscriber Certificates specified in Table 18 above.
6.5	Managed PKI Customers and Gateway Customers must use Trustworthy Systems that meet the requirements of the Enterprise Security Guide.	Managed PKI Customers and Gateway Customers must use Trustworthy Systems. VeriSign recommends that Managed PKI Customers and Gateway Customers follow the guidelines provided in Enterprise Security Guide.
6.5.1	Direct access to VeriSign databases supporting the VeriSign repository is limited to Trusted Persons in VeriSign's operations group having a valid business reason for such access.	Direct access to VeriSign databases supporting VeriSign's CA Operations is limited to Trusted Persons in VeriSign's Production Operations group having a valid business reason for such access.
7.1	RFC 2459	Replaced RFC 2459 with RFC 3280
	Except for WTLS Certificates, VeriSign Certificates conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999 ("RFC 3280").	Except for WTLS Certificates, VeriSign Certificates conform to (a) ITU-T Recommendation X.509 (1997): Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, June 1997 and (b) RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 3280"). Not all certificate services allow the use of UTF8String encoding of DirectoryString.
		Added footnote, "WAP and WTLS certificates are no longer available from VeriSign"
	RFC 2459: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, January 1999 ("RFC 2459").	RFC 3280: Internet X.509 Public Key Infrastructure Certificate and CRL Profile, April 2002 ("RFC 3280").
	Valid From Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 2459.	Valid From Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 3280.
	Valid To Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 2459. The validity period will be set in accordance with the constraints specified in CPS § 6.3.2.	Valid To Universal Coordinate Time base. Synchronized to Master Clock of U.S. Naval Observatory. Encoded in accordance with RFC 3280. The validity period will be set in accordance with the constraints specified in CPS § 6.3.2.
	Subject Public Key Encoded in accordance with RFC 2459 using algorithms specified in CPS § 7.1.3 and key lengths specified in CPS § 6.1.5.	Subject Public Key Encoded in accordance with RFC 3280 using algorithms specified in CPS § 7.1.3 and key lengths specified in CPS § 6.1.5.
	Signature Generated and encoded in accordance with RFC 2459	Signature Generated and encoded in accordance with RFC 3280
7.1.1	• WTLS User and WTLS Server Certificates which are issued in WAP format.	• Any WTLS User and WTLS Server Certificates still in existence which are issued in WAP format.
7.1.2.1	Where X.509 Version 3 Certificates are used, VeriSign populates the KeyUsage extension of in accordance with CPS § 6.1.9. The criticality field of this extension is set to FALSE.	Where X.509 Version 3 Certificates are used, VeriSign populates the KeyUsage extension of in accordance with CPS § 6.1.9. The criticality field of this extension is generally set to FALSE.
7.1.2.4	The criticality of the Basic Constraints extension is generally set to FALSE, except for the VeriSign Class 3 Managed PKI Authentication Services Bureau CA. The criticality of this extension may be set to TRUE for other Certificates in the future.	The criticality of the Basic Constraints extension is generally set to FALSE for End-Entity Certificates and TRUE for CA Certificates. The criticality of this extension may be set to TRUE for additional Certificates in the future.

7.1.2.5	Table 22	Updated settings in table 22
7.1.2.6	VeriSign X.509 Version 3 Secure Server and Class 1 Individual end-user Subscriber Certificates use the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE. The use of CRL Distribution Points will be supported for other VeriSign CA Certificates in the future.	Most VeriSign X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates include the cRLDistributionPoints extension containing the URL of the location where a Relying Party can obtain a CRL to check the CA Certificate's status. The criticality field of this extension is set to FALSE. The use of CRL Distribution Points will be supported for other VeriSign CA Certificates and end user Subscriber Certificates in the future
7.1.2.7	VeriSign populates the Authority Key Identifier extension of X.509 Version 3 end user Subscriber Certificates issued by the VeriSign Commercial Software Publishers CA. The Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the CA issuing the Certificate. The criticality field of this extension is set to FALSE. The use of Authority Key Identifier extension may be supported for other VeriSign CAs in the future.	VeriSign generally populates the Authority Key Identifier extension of X.509 Version 3 end user Subscriber Certificates and Intermediate CA Certificates. When the certificate issuer contains the Subject Key Identifier extension, the Authority Key Identifier is composed of the 160-bit SHA-1 hash of the public key of the CA issuing the Certificate. Otherwise, the Authority Key Identifier extension includes the issuing CA's subject distinguished name and serial number. The criticality field of this extension is set to FALSE. The use of Authority Key Identifier extension may be supported for other VeriSign CAs and end user Subscriber Certificates in the future.
7.1.3	VeriSign X.509 Certificates are signed with sha1RSA (OID: 1.2.840.113549.1.1.5) or md5RSA (OID: 1.2.840.113549.1.1.4) in accordance with RFC 2459. VeriSign signed certain legacy CA and end user Subscriber Certificates with md2RSA (OID: 1.2.840.113549.1.1.2). VeriSign WTLS Certificates are signed with sha1RSA (OID: 1.2.840.113549.1.1.5) or ecdsa-with-SHA1 (OID: 1.2.840.10045.1).	VeriSign X.509 Certificates are signed with sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) or md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) in accordance with RFC 3279 VeriSign signed certain legacy CA and end user Subscriber Certificates with md2WithRSAEncryption (OID: 1.2.840.113549.1.1.2). VeriSign WTLS Certificates still in existence are signed with sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) or ecdsa-with-SHA1 (OID: 1.2.840.10045.1).
7.2	7.2 CRL Profile	7.2 CRL and OCSP Profile
	N/A	VeriSign's OCSP responders conform with RFC2560 with the exception of including nonce as one of the requestExtensions in requests.
		Replaced RFC 2459 with RFC 3280
	Signature Algorithm used to sign the CRL. VeriSign CRLs are signed using md5RSA (OID: 1.2.840.113549.1.1.4) or md2RSA (OID: 1.2.840.113549.1.1.2) in accordance with RFC 2459.	Algorithm used to sign the CRL. VeriSign CRLs are signed using sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) or md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) in accordance with RFC 3279 .
7.2.1 Version Number(s)	VeriSign currently issues X.509 Version 1 CRLs.	VeriSign issues both X.501 Version1 and Version 2 CRLs. VeriSign's OCSP responders implement Version 1 of the OCSP specification as defined by RFC2560, with the exception of including nonce as one of the requestExtensions in requests.
8.2.2	VeriSign also makes the CPS available in Adobe Acrobat pdf or Word format upon request sent to CPS-requests@verisign.com.	Deleted: VeriSign also makes the CPS available in Adobe Acrobat pdf or Word format upon request sent to CPS-requests@verisign.com.
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
	N/A	added EOL footnote for EDI