Table of Contents

1.0 GENERAL 2
1.1 SUMMARY 2
1.2 REFERENCES 2
1.3 SUBMITTALS 3
1.3.1 General 3
1.3.2 Service Request Criteria 3
1.4 EXPECTATIONS 3
1.4.1 CDT 3
1.4.2 Customer 4
1.5 SCHEDULING 4
1.5.1 Maintenance 4
1.5.2 Change Management Schedule 5
1.6 DEFINITIONS 5
2.0 PRODUCTS 6
2.1 MANUFACTURER 6
2.1.1 Unit Pricing 6
2.2 PLATFORM 6
2.3 PRODUCT FORMATS 6
3.0 EXECUTION 8
3.1 SECURITY 8
3.2 QUALITY CONTROL 8
3.2.1 CDT Responsibilities 8
3.2.2 Customer Responsibilities 9
3.3 SUPPORT AVAILABILITY 9
3.4 INSTALLATION 9
3.4.1 CDT Responsibilities within Application Hosting where CDT manages the Web Server 9
3.4.2 Customer Responsibilities include but are not limited to 9
3.4.3 Customer Responsibilities for certificates outside of CDT managed Web Servers 10
3.4.4 Certificate Signing Request (CSR) File Creation 10

1.0 GENERAL

1.1 *SUMMARY*

The California Department of Technology (CDT) provides Secure Certificates (also known as SSL, TLS or X.509 certificates) on leased equipment in the Application Hosting environment within the data center and external CDT customers. These certificates are a nonproprietary protocol for securing data communications across computer networks and will provide data encryption while in transit for TCP/IP connections.

Included in the offering, where CDT manages Customer web servers, are certificate procurement, installation, and administration. Staff performs these tasks according to internal procedures and standard configurations. CDT will provide certificate procurement services for all other Customer systems; including Application Hosted web servers unmanaged by CDT.

As an alternative, CDT also offers delegated administrator access to customers who prefer to generate and manage their own certificates. Customers utilizing this option are provided to access CDT's certificate console and are granted permission to issue certificates under approved third level domains or specific URLs within root domains.

CDT provides version(s) of certificates in accordance with current certificate industry standards. Certificates are offered on both dedicated and virtual server platform configurations. CDT is authorized to offer certificates only for the following domains:

.ca.gov
.california.gov
.cahwnet.gov
.state.ca.us

1.2 *REFERENCES*

Items referenced here are support information provided in this document:

	IDENTIFIER	DATE	TITLE
	01.05.884	2012	Secure Certificate Submittal
	01.05.885		Delegated Administrator Secure Certificate Submittal
	2.6.852		Domain Name Request Guideline
			Domain Name Request Submittal
	n/a	2013	Environment Submittal
	n/a	2013	Environment Submittal Instructions
	4000	2011	CDT Software Version Support Policy
	4000	2011	CDT Software Version Support Procedure
	Web Site	NA	CDT Contact Information

1.3 *SUBMITTALS*

1.3.1 General

CDT is available to advise and assist customers in formulating IT designs that will leverage available service offerings. Contact your Account Manager to engage architectural/engineering and design consulting services. Additional charges may be incurred.

The CDT requires the following method be used for work requests:

Item	Request Method
Quotes & Billable Service (new or changes to existing services)	CDT Customer Service Request
Modifications to Existing Systems	CDT Service Desk or CDT Service Request
Technical Problems	CDT Service Desk or Service Incident
Security Related Issues/Incidents	CDT Service Desk
SSL Submittal Questions	Certificate_Services@state.ca.gov

Include the Customer's name, contact information and associated project name on forms, documents, and requests submitted to CDT.

1.3.2 Service Request Criteria

A completed Secure Certificate Submittal is required for new certificates and renewals requests prior to the start of work. Please submit one submittal per URL, except in the case of SAN certificates. To aid in the preparation of providing this technology, all information must be included in the CDT Service Request. Multiple submittal documents may be attached to a single Service Request.

Customers using the delegated administration option should submit the Delegated Administrator Secure Certificate Submittal to initiate service setup but do not need to submit service requests for individual certificates.

This Submittal is to be revised at appropriate intervals providing for expeditious and practicable execution of the work. Revised submittal(s) must indicate changes, if any.

1.4 *EXPECTATIONS*

1.4.1 CDT

CDT manages contract and licensing for certificate management software and may serve as liaison between the customer and certificate vendor for technical issues.

CDT will notify Customers of upcoming renewals in accordance with the contact information provided on the Secure Certificate Submittal. Technology products must be within vendor supported versions to sustain availability and integrity.

CDT will obtain certificate backups for web servers managed by CDT.
CDT follows change management practices. Change requests are recorded in Remedy, as a Change Request (CRQ). Contact your CDT Account Lead for current change procedures.

1.4.2 Customer

Customers are expected to notify Certificate_Services@state.ca.gov of changes to certificate contact(s).

Certificates purchased for systems outside of Application Hosting where CDT is managing the web server, must be installed and verified by the Customer.

Customers are to determine and submit technology details required to meet their certificate needs.

1.5 *SCHEDULING*

CDT's goal is to provide timely, comprehensive and economical technology service manner. Customers promote this goal by promptly providing information requested, and by keeping the CDT Account Manager / Project Manager informed of technology project status.

Completed and approved service requests for new certificates will typically be available 3 to 5 business days after the normal service request processing time. Renewals are not processed by CDT until a week prior to the current certificate expiration date. If they are needed earlier please note the requested delivery date on the service request. Certificates will expire at 1700 on the final day of the active certificate.

Delays in the service request process, server readiness to obtain the certificate, or the lack of or validity of the CSR file will impact the timeliness of the certificate delivery.

A 25 calendar day window immediately following the delivery of a certificate from CDT is provided for certificate testing, revocation or changes.

1.5.1 Maintenance

Not Used

1.5.2 Change Management Schedule

Change proposal / requests follow the established CDT Change Management process. Work performed during scheduled maintenance periods is subject to the CDT Change Management Schedule. Changes require 2-week prior notification. Shorter periods may not always be expedited; additional charges may be incurred for expedited change requests.

1.6 *DEFINITIONS*

Term, phrase, abbreviation	**Definition**
SSL	Secure Sockets Layer
TLS	Transport Layer Security
SAN	Subject Alternative Name
CSR	Certificate Signing Request
DNS	Domain Name Service
HTTPS	Hypertext Transfer Protocol over SSL
TCP/IP	Transmission Control Protocol/Internet Protocol
URL	Uniform Resource Locator (also known as Common Name)

2.0 PRODUCTS

2.1 *MANUFACTURER*

Comodo Group, Inc.

2.1.1 Unit Pricing

Certificates are available in one or two year units. Expedited certificate requests are subject to expedite fee(s).

Certificate Pricing	1 Year	2 Year
Certificate Fee (per certificate)	$250.00	$500.00
Administration Fee	$130.00	
CDT Installation Fee	$130.00	

One certificate *administration* fee is applied per certificate.

Certificate *installation* fees are applied per server, per certificate. This is in addition to the certificate administration fee. Installation fees only apply when CDT performs the certificate installation(s).

If certificate revocation occurs within the 25 calendar day testing window, the cost of the certificate license will be reimbursed however the administration and installation fee(s) will not. Contact your CDT Account Manager for information regarding the Credit Reimbursement process.

Customers who choose the delegated administration option do not pay the fees above. This option is provided at no charge.

2.2 *PLATFORM*

Certificates are compatible on servers running the following:

Microsoft Internet Information Server (IIS)

Apache HTTP Server

For additional platform options contact Certificate_Services@state.ca.gov.

2.3 *PRODUCT FORMATS*

Certificates are available from CDT in the following formats:

PKCS#7 (.p7b file)

X.509 (.cer and .crt files)

Within Application Hosting where CDT manages the web servers, CDT will also convert the certificate into PFX (.pfx file) format for use on load balancers and proxy devices.

Additional technical specifications:

CDT provides 3rd party certificates signed by a trusted Certificate Authority and does not issue self-signed certificates.

Certificates support both client and server authentication.

Certificates include one free SAN with “www”. For instance, if you request a certificate for mysite.ca.gov, the certificate will also accept an alternative name of www.mysite.ca.gov.

Up to 100 domain names may be applied to a single SAN certificate.

3.0 EXECUTION

3.1 *SECURITY*

Secure certificates should be used if information in transit between different computer networks needs to be protected. Common certificate applications include:

1. Encrypting personally identifiable information (PII) while in transit.
2. Complying with required regulatory privacy or security requirements.

CDT complies with industry standard security guidelines; therefore the following security guidelines apply:

1. Wildcard certificates require an approved security exception from CDT. Contact your Account Manager or refer to the Information Security Exception Request Procedure for more information.
2. The minimum key length is 2048.bits.
3. The minimum signature algorithm is SHA2. SHA1 and MD5 hashing algorithms are no longer accepted.

Configuration changes made outside the scope delineated above and needing intervention, correction, or troubleshooting by CDT staff may result in delays and/or incur additional charges.

3.2 *QUALITY CONTROL*

1. New domain names must be approved by CDT and must comply with federal General Services Administration (GSA) guidelines. For more information, contact your Account Manager or refer to the Domain Name Request Guideline.
2. A new web site typically needs a new DNS entry request for the new domain name.
3. When using HTTPS (port 443) confirm the network port opening is permitted to allow this traffic across applicable network devices (e.g., proxies, routers).

Prohibited

1. Top-level domain name endings in: .com .net .biz .org
2. Use of top-level domain name containing "/" symbol. Examples: "xyz.ca.gov/secure" or "xyz.ca.gov/finance"

3.2.1 CDT Responsibilities

1. Contract management
2. Engage Certificate Authority as necessary for vendor problem resolution involving the service.
3. Review and recommend optional certificate application that may better meet requirements in accordance with the project and/or 1.3 - SUBMITTALS
4. Review submittal for completeness and approve prior to beginning work
5. Notify Customer of submittal flaws, if any

6. Send Customer 30,60,90 day automated certificate expiration notifications

Additionally within Application Hosting where CDT manages the web server:

7. Certificate installation and verification.
8. Troubleshoot certificate related issues and engage vendor support, if required.
9. Assist customer in specifying design, if applicable, in accordance with information provided in 1.3 - SUBMITTALS

3.2.2 Customer Responsibilities

1. Initiate renewal of certificate prior to its expiration. Refer to 1.5 – SCHEDULING
2. Provide complete and timely submittal; refer to 1.3 - SUBMITTALS information
3. Notify CDT of changes that impact the certificates use
4. Document certificates within the application architecture and keep it current

3.3 *SUPPORT AVAILABILITY*

Core business hours for technical support are Monday through Friday 0800-1700. State holidays and mandated schedule alterations are observed and may impact staff availability. Customers may be provided vendor support contact information and can leverage their 24x7 phone support directly, if needed.

3.4 *INSTALLATION*

3.4.1 CDT Responsibilities within Application Hosting where CDT manages the Web Server

1. Installation of certificates will be in accordance with the 1.3 - SUBMITTALS and current industry certificate standards
2. Coordinate with other, internal CDT teams regarding proxy/load balancer certificate installation
3. Verify certificate functionality
4. Communicate certificate installation

3.4.2 Customer Responsibilities include but are not limited to

1. Notify CDT of changes that impact the certificates use
2. Document certificates within the application architecture and keep it current
3. Test third party application functionality with the certificate
4. Additional charges for CDT intervention, troubleshooting and correction of unauthorized changes that impact CDT's responsibilities of the certificate.
5. Test system upon certificate modifications.
6. The Customer is responsible for conversion into formats not listed in Section 2.3 - *PRODUCTS FORMATS*.

3.4.3 Customer Responsibilities for certificates outside of CDT managed Web Servers

This includes unmanaged web servers within Application Hosting.

1. Installation, Certificate Signing Request (CSR) generation, and certificate configuration
2. Certificate backups, including private key retention.

3.4.4 Certificate Signing Request (CSR) File Creation

The following applies ONLY in the event that a Customer is performing the certificate installation. The customer must create the initial Certificate Signing Request (CSR) file from the server or device and attach the file to the CDT Service Request.

Certificate criteria must be valid and entered correctly. Failure to accurately complete and submit the Certificate Signing Request (CSR) may result in processing delays.

Tips:

- ✓ Only one CSR is required per common name or URL.
- ✓ Do not include the private key but ensure that it is retained on your server.
- ✓ Confirm values entered in the CSR contain no spaces at the beginning or end.

1. Create the CSR file from your server or device. For platform specific assistance with creating the CSR, our vendor provides instructions to Generating a Certificate Signing Request (CSR).
2. Select/enter **2048-bit** key length (minimum level).
3. Select signature algorithm strength of at least SHA2. SHA1 and MD5 hashing algorithms are no longer accepted.
4. Common Name/ Top-level Domain Name (this is the fully qualified domain name registered in DNS for an authorized state domain. Example: dts.ca.gov). For SAN certificates please enter only the primary URL. Alternate names will be entered by CDT upon certificate generation.
5. Organization : **State of California**
6. Organizational Unit: (no special characters)
7. Locality: **Sacramento**
8. State/Province (no abbreviation): **California**
9. Country (2-letter code, no punctuation): **US**
10. Attach created CSR text file to the Service Request (SR) only if the certificate is Customer managed.