

## SSL DIGITAL CERTIFICATE PROVISIONING

### Service Description

SSL (Secure Sockets Layer) Digital Certificate Provisioning service provides Secure Sockets Layer (SSL) Certificate service across multiple enterprise service offerings. SSL certificates are used to provide communication security to various web sites and communications protocols over the internet (ex. Web Servers, Network Devices, Application Servers, Internet Information Server (IIS), Apache, F5 devices and Exchange servers). SSL Digital Certificate Provisioning supports the delegation of administration and reporting processes for each designated customer agency while leveraging a common portal.

### Customer Benefits

- **Cost-Savings** – The customer will save money by having all certificates issued from a central source
- **Efficiency** – This service is centralized, allowing for a single service to issue certificates for many different Agencies and/or Divisions.
- **Support** – Service support is provided by staff skilled and experienced in planning and provisioning as well as maintaining and troubleshooting the services.

### OIT Provides

- Delegation Design
- Enterprise License
- Authentication
- SSL certificate provisioning
- Administration through SSL certificate lifecycle
- Incident resolution services via the Customer Service Center
- Billing
- Reporting

### Maintenance Schedule

Scheduled maintenance of SSL Digital Certificate Provisioning occurs on Wednesday evenings from 6:00 p.m. to midnight when needed. Outages are minimized or canceled whenever possible. OIT schedules extended outages twice per year. The scheduled extended outage dates are established at the beginning of the year and typically run from 6:00 a.m. to midnight. If a shorter outage window is required, the outage will be scheduled from 6:00 p.m. to midnight.

### Incident Response & Resolution

As a primary service, SSL Digital Certificate Provisioning support staff is available 24 x 7 for both incident reporting and resolution. SSL Digital Certificate Provisioning staff will respond to the customer within 30 minutes of a reported incident. Customer involvement is essential to resolving issues; therefore, the customer will need to provide a Technical Contact resource. With collaboration from the customer and vendor resources, staff will commit to resolve the incident within 4 hours.

## Service Objectives

Category	Evaluation Criteria	Target
Availability	SSL Digital Certificate Provisioning service uptime	99%
Incident Responsiveness	SSL Digital Certificate Provisioning support staff responds to the customer (i.e. acknowledges and confirms receipt of incident ticket) within 30 minutes.	100%
Incident Resolution	SSL Digital Certificate Provisioning support staff resolves incident within 4 hours	75%

## Customer Requirements

- Generate Certificate Signing Request (CSR)
- Install issued certificate
- Maintain agency and service contact lists via the IT Enterprise Services portal at: <http://itenterprise.ohio.gov>.
- Obtain Domain Certificate if required (UNS)
- Place service order via the OIT Enterprise Service Catalog
- Provide Authorized Certificate Requestor (State Employee)
- Provide DAS OIT with a valid billing number
- Provide Technical Support for Certificate Owners
- Review and Verify Certificates data accuracy

## Additional Information

For more information on this service or the Service Level Agreement, contact the Customer Service Center at [CSC@ohio.gov](mailto:CSC@ohio.gov).

Visit us on the web at: <http://das.ohio.gov/Divisions/InformationTechnology.aspx>.