Internal Certificate Authority

Last updated 12-07-22

The Internal Certificate Authority (ICA) service provides digital certificates for use inside the State Government Network (SGN) to address the need to protect data in transit. The ICA provides a Certificate Revocation List (CRL) and Online Certificate Status Protocol service (OCSP) that allows agency systems to validate that a certificate has not been revoked. The WaTech ICA, CRL, and OCSP services all maintain 99.9% uptime. Manual certificate requests are returned within two business days.

Certificates issued to state agencies are used for encryption, authentication and identification of servers and clients, or both via Secure Socket Layer and Transport Layer Security. Some agencies use the ICA to provide protection of sensitive data and high-value resources.

The ICA was created as part of the decision package for the Integration Competency Center. The Secure Gateway Services group provides the ICA service.

Intended customers

This service is only available to WaTech customers on the SGN. As the service stewards and user groups explore greater automation, integration with identity services, and the creation of a request portal, we expect to meet the growing demand from agencies for internal certificates.

Customer engagement

- The Secure Gateways Team holds a biweekly Secure Gateway Services Fireside Chat. Topics include resource utilization, future goals, and objectives, planned maintenance and updates, and feature enhancement requests.
- Semi-annual customer Town Hall with all Computing Services teams providing updates and gathering customer feedback.
- Monthly Technology Management Council (TMC) and Business Management Council (BMC) meetings for agency CIOs and IT leaders to inform and sponsor enterprise strategy, policy and investments.
- Regularly scheduled meetings between customers and Business Relationship Managers (BRM) to connect, advise, address concerns and provide solutions.
- Weekly group calls for state CIOs and CISOs to provide updates on important and immediate issues and actions.
- Regular outreach to solicit feedback, provide updates and inform agencies on emerging projects, initiatives, and services.
- Requests for new consultations and modifications to existing applications.

Helpful information

Service category
Security

Service availability
24/7/365

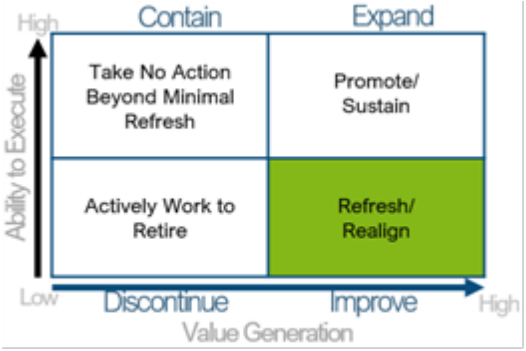
Planned maintenance
Performed as required during non-peak hours.

Related services
- Virtual Private Network (VPN)
- Active Directory Services

How to request service
Submit a request for service through our Customer Portal.

Service owner
Audrey Leckner

Action plan



Current activity

Proof-of-concept work is currently well underway to replace the legacy hardware security modules. Security Design Review is near completion with focus turning toward governance of PKI.

One- to two-year goals

Refresh hardware to deprecate the current legacy hardware security modules and replace them. With this change, users will have a greater ability to automate their certificate requests and reduce manual actions currently required by this service. A new Terms of Service document will be created to outline acceptable use cases outside of VPN and other bundled services.

Three- to five-year goals

- As agency customers move their services to the cloud, we anticipate the need for this service may decline in favor of public certificate providers or otherwise evolve. Currently, there is still a great need for certificate authentication on the SGN, which remains the focus of this service.
- External certificates for cloud services are available through a variety of legitimate external certificate authorities and are not served internally via WaTech. WaTech PKI SMEs will provide consultation and guidance as needed to aid agencies in transitioning as needed.
- WaTech will continue to provide ongoing support for Internal Certificate needs as well as providing internal consultation as the SASE Blueprint is developed.

Service review and fully loaded service budget projection

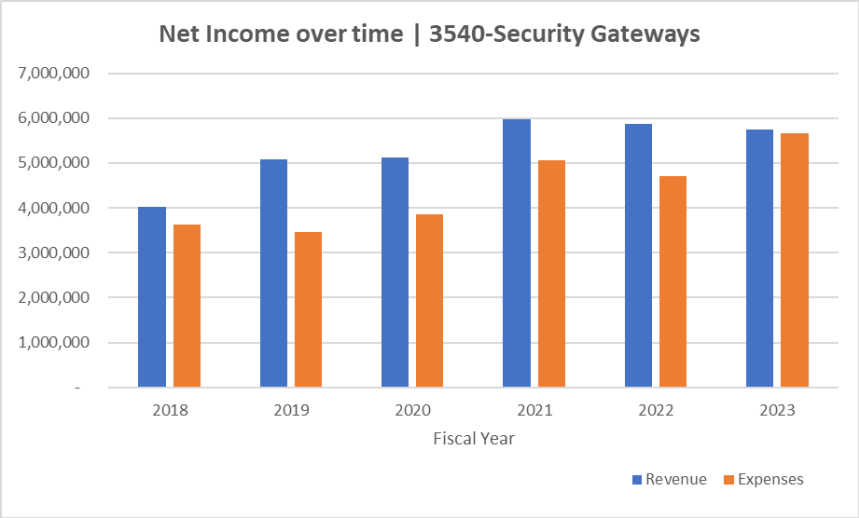
Revenue source

The Secure Certificates service is bundled and funded using revenue from the Security Gateway central service model.

The Security Gateway Allocation funds a central point of authentication for all public-facing services provided by Washington state agencies, which enforces security standards to ensure resident's private information is protected when accessing government services. It provides a consistent method of authentication and should result in efficiencies/savings at the agency level with these services provided at the enterprise level.

Allocation funding is based on the agency's number of budgeted FTEs and the number of applications each agency has using the gateway. OFM maintains the source data for budgeted FTEs and WaTech tracks the number of applications. Additionally, agencies with 50+ FTEs pay a yearly base fee of $1,500.

Net Income over time


Net Income over time | 3540-Security Gateways
7,000,000
6,000,000
5,000,000
4,000,000
3,000,000
2,000,000
1,000,000
-
2018
2019
2020
2021
2022
2023
Fiscal Year
Revenue
Expenses