Hosted Web Service Security

OVERVIEW

The MA RMV has adopted the following security measures for ATLAS-hosted web services:

- Authentication: X.509 client certificate
- Communication security: Transport Layer Security (TLS) 1.2 (or higher)
- Access control: Client IP address whitelisting

Authentication is handled over a TLS 1.2 connection which, as part of the TLS handshake, requests a X.509 client certificate - this is known as Transport Security with Certificate Authentication. The TLS 1.2 connection is terminated at the web service endpoint and the certificate is passed to the application to perform the authentication.

Authentication is specific to each ATLAS environment. This means that a separate X.509 client certificate is required to authenticate to web services hosted by the ATLAS Production and QA (Staging) environments. A single X.509 client certificate can be used to access multiple web services hosted by the same ATLAS environment. Communication security (TLS 1.2) applies to both ATLAS Production and QA (Staging) environments. Access control (IP address whitelisting) is specific to each ATLAS environment. It is required that IP address whitelist requests identify which ATLAS environment a specific IP address (or IP address range) will be used for. Specific IP addresses (or IP address ranges) can be whitelisted for access to both ATLAS Production and QA (Staging) environments.

Each ATLAS business partner is assigned an ATLAS web service credential. Business partner web service credentials are used to track activity, manage security, and store X.509 client certificate information.

X.509 Client Certificates

Authentication to ATLAS-hosted web services requires an X.509 client certificate issued by a trusted Certificate Authority (CA) and issued to an ATLAS business partner. The public key of the client certificate key pair is loaded into the ATLAS application and associated to a business partner web service credential. The business partner web service credential is identified using the X.509 certificate in the web service call that originates from the business partner. Business partner web service credentials are only allowed to access those ATLAS-hosted web services they have been authorized for.

File format requirements

Public key of the X.509 client certificate key pair provided in DER, CER, PEM, or CRT format

Minimum requirements for Certificate Attributes

- Signature algorithm
    - sha256RSA
- Signature hash algorithm
    - sha256
- Issuer
    - Trusted certificate authority (CA)
        - Examples: Digicert, Verisign
- Valid period (to/from)
    - 2 years or less
- Subject
    - CN: Common Name
        - Description of the purpose of the client certificate
        - Example 1: ATLAS QA Web Service - Organization ABC
        - Example 2: ATLAS Production Web Service - Organization ABC
    - O: Organization
        - Organization the certificate is issued to
    - C: CountryName
        - Country of the Organization
    - Public key

        - RSA (2048 Bits)
    - Key Usage
        - Digital Signature
    - Enhanced Key Usage (Intended purpose)
        - Client Authentication (1.3.6.1.5.5.7.3.2)
            - "Proves your identity to a remote computer"
    - Thumbprint algorithm
        - sha1

TRANSPORT LAYER SECURITY (TLS) 1.2 (OR HIGHER)

All communications over the internet between a business partner and the ATLAS application are required to use the Transport Layer Security (TLS) protocol version 1.2 (or higher).

Client IP Address Whitelisting

Client access to internet-facing ATLAS servers is limited to only those IP addresses that have been approved for connectivity and added to the whitelist.

Client IP addresses eligible for whitelisting are restricted to the following:

- Servers that submit system-to-system (automated) requests
- Business partner-managed network gateways used for manual access to the web service - i.e. proxy, VPN, etc.

IP Address Whitelist Request Process

Note: The following procedures are subject to change without notice

- Business partner submits a request that includes a list of IP addresses, including single IP addresses and/or range(s) of IP address(es) (CIDR notation), to be whitelisted
  - The request should clearly state which ATLAS environment each IP address will be used for - Production or QA (Staging)
  - The request should clearly state which ATLAS-hosted web service(s) will be used
- The IP address whitelist request is forwarded to the MassDOT IT Security team for review.
  - See "IP Address Whitelist Review Guide" below
- The IP address whitelist request is forwarded to the IT Network team to complete the whitelisting
- Notification is sent to the requesting business partner stating the IP address whitelist request process is complete. Business partner is prompted to confirm connectivity from each IP address source.

IP ADDRESS WHITELIST REVIEW GUIDE

Requested IP addresses are researched to determine the following:

- Autonomous System Number (ASN) and address block owner
- Delegation details (if any)
- Geolocation details
- Domain Name Server (DNS) resolution (forward & reverse)

Requested IP addresses are checked against the following list of items during review (note: this is not an exhaustive list of review items):

Review Item	Approval Status
Static IP address registered to a business partner-managed network gateway – i.e. proxy, VPN, etc.	Approved
IP address registered to a business partner server that submits system-to-system (automated) requests	Approved
IP address registered to a private hotspot device	Automatic rejection
IP address registered to an unrelated business – i.e. hotel, coffeehouse, etc.	Automatic rejection
IP address registered to a US-based internet service provider DHCP pool	Pending rejection. Justification of usage needed.
IP address registered to a foreign internet service provider	Automatic rejection
IP address not located in North America	Pending approval. Additional information needed.
IP address range that contains more than 8 IP addresses - CIDR notation /29	Pending approval. Additional information needed.
IP address listed on a security-related IP address blacklist	Automatic rejection

Disclaimer: Whitelisted IP addresses are subject to periodic review for usage and to ensure they remain in compliance with MassDOT/ATLAS guidelines.