Cellebrite Government Cloud SAML SSO Security Architecture

Cellebrite

Reviewed May 2026

Cellebrite Government Cloud
SAML 2.0 Single Sign-On Security Architecture

1. Purpose

This document describes how SAML 2.0 based Single Sign-On (SSO) connections are established between customer identity systems and the Cellebrite Government Cloud (CGC). The write-up aligns with cryptographic protections and data in transit descriptions documented in the CGC FedRAMP System Security Plan (SSP) Appendix A and supports FedRAMP High requirements.

2. Scope

This document applies to all SAML 2.0 authentication transactions originating from customer managed Identity Providers (IdPs) and terminating at CGC as the Service Provider (SP). This includes browser based SSO flows, IdP initiated and SP initiated authentication, and deployments leveraging PIV or CAC credentials at the customer IdP. Internal authentication mechanisms within the CGC boundary are out of scope.

3. System Overview

CGC operates as a SAML 2.0 Service Provider hosted within AWS GovCloud. All SSO authentication transactions crossing the CGC authorization boundary are encrypted in transit using Transport Layer Security (TLS) version 1.2. Incoming SAML traffic terminates at CGC managed ingress points that use FIPS validated cryptographic modules provided by AWS, consistent with SSP Appendix A.

4. SAML 2.0 Integration Model

CGC supports standard SAML 2.0 federation using XML based assertions exchanged between a customer Identity Provider and CGC as the Service Provider. Trust is established through exchange of SAML metadata, including entity identifiers, assertion consumer service endpoints, and signing certificates.

SAML bindings supported for authentication include HTTP Redirect and HTTP POST, in accordance with SAML 2.0 specifications.

5. Authentication Entry Points

5.1. Browser Based SSO

Browser based SSO is initiated when a user attempts to access CGC and is redirected to the customer IdP for authentication. Browser sessions use HTTPS with TLS 1.2. Incoming HTTPS traffic is decrypted on AWS managed ingress components, including AWS Application Load Balancers, which use FIPS validated cryptographic modules and re encrypt traffic before forwarding it to CGC authentication services.

5.2. PIV and CAC Enabled Authentication

CGC supports SAML 2.0 federation with customer IdPs that enforce Personal Identity Verification (PIV) or Common Access Card (CAC) authentication. PIV or CAC validation is performed entirely by the customer IdP. Following successful smart card authentication, the IdP issues a signed SAML assertion containing authenticated user identity attributes, which is transmitted securely to CGC over TLS 1.2. CGC does not directly process smart cards and relies on the IdP assertion for authentication assurance.

6. Assertion Validation and Integrity

All SAML assertions received by CGC are subject to strict validation prior to establishing a user session. Validation includes verification of the digital signature, issuer, audience, timestamps, and assertion lifetime. Signed assertions ensure integrity and non repudiation. Assertions failing validation are rejected and access is denied.

7. Cryptographic Protections

All SAML authentication traffic crossing the CGC authorization boundary is protected using TLS 1.2. Cryptographic operations are implemented using FIPS 140 validated cryptographic modules provided by AWS managed services and underlying operating system platforms. Legacy protocols and weak cryptographic algorithms are disabled, consistent with SSP Appendix A.

8. Logging and Monitoring

SSO authentication events, including assertion validation success or failure, are logged by CGC components. Logs are protected against unauthorized modification and forwarded to centralized monitoring systems for analysis and audit support in accordance with FedRAMP High requirements.

9. Compliance Agreement

This SAML 2.0 SSO architecture aligns with the following FedRAMP High and NIST SP 800-53 controls as documented in SSP Appendix A:

SC 8 and SC 13 for confidentiality and cryptographic protection of authentication traffic.
IA 2 and IA 7 for federated identity and authentication assurance through trusted IdPs.
SI 7 for integrity verification of signed SAML assertions.

10. Summary

CGC uses standards based SAML 2.0 federation to securely integrate with customer identity systems. Authentication traffic is encrypted in transit, assertions are cryptographically validated, and support for PIV and CAC credentials is provided through trusted customer Identity Providers. This design ensures strong authentication while remaining consistent with FedRAMP High and SSP Appendix A requirements.

8065 Leesburg Pike, Suite T3-302, Vienna, VA 22182 USA / Tel. +1 201 848 8552 www.cellebrite.com