

ArcGIS Online: Compliance and Security

Gregory Ponto
Pete Buwembo

Esri Software Security & Privacy Team
SoftwareSecurity@Esri.com



Agenda



- Compliance
 - FedRAMP Status
 - ISO 27001 Efforts
 - Some Milestones
- Shared Responsibility Model
 - Esri Responsibilities vs Customer Responsibilities
 - Process / Configuration
- Demos
 - ArcGIS Security and Privacy Adviser
 - Securing SAML
 - API Keys
- Summary
- Open Q&A Discussion

Compliance Roadmap



FedRAMP Moderate



Q2 2023

- FedRAMP Moderate authorization – Agency ATO May 2023
 - Security no longer needs to be primary factor for choosing ArcGIS Online (SaaS) or customer-managed GIS deployments
 - AGO Security posture now aligns with DISA SRG or DoD AA L2 (Non-Controlled Unclassified Information)
- Obtain 3rd party assessment report
 - Agencies use FedRAMP marketplace
 - Other customers – Ask account manager (NDA required)

Q1 2024

- Shift to NIST 800-53 (Rev 5) as part of the annual assessment
 - Major advancements include
 - Supply chain & privacy controls





Compliance Roadmap



Q4 2024

- ArcGIS Online EU Region & ArcGIS Platform aligned with ISO 27001
- Estimated certification completion – Q3 2025
- ISO 27001 to FedRAMP Control Mapping
 - See ArcGIS Trust Center – Updated July 2024 for moderate Rev 5 controls

Mapping of FedRAMP Moderate Rev 5 Baseline to ISO 27001 Security Controls

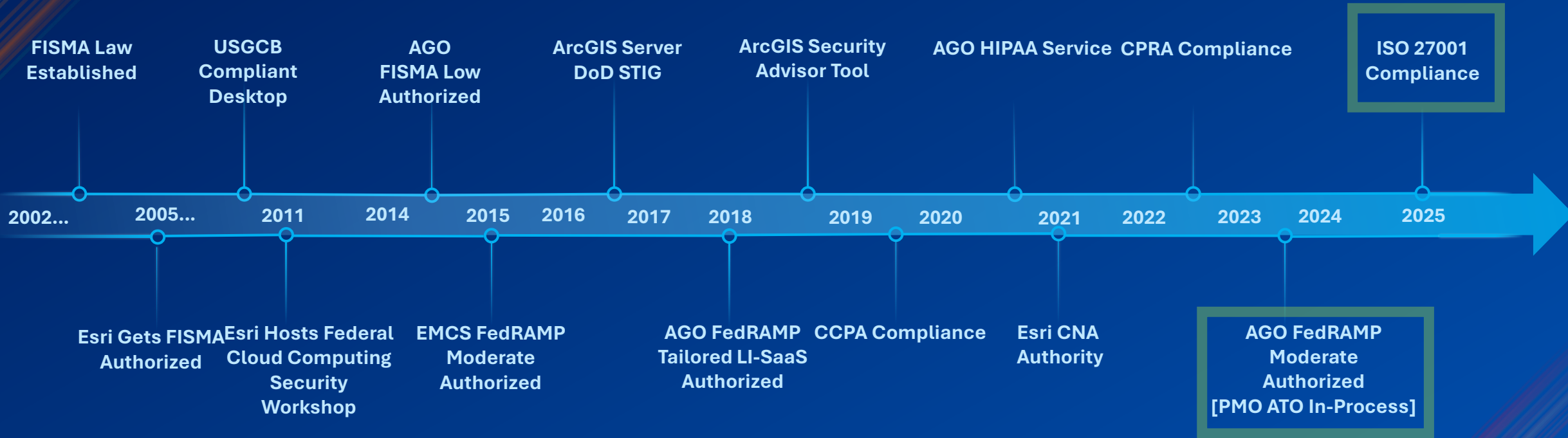
This document provides a list of all controls that require the Cloud Service Provider, Esri, to provide detailed descriptions of their implementation, that meets the intent of the security requirements. All required controls are tested by an approved assessor annually. ArcGIS Online does not undergo a separate ISO 27001 certification as the FedRAMP authorization meets requirements for equivalent or better security assurance, however ISO 27001 is planned for our EU Region. This mapping is aligned to the latest version of FedRAMP Moderate / NIST SP 800-53 Revision 5 controls to ISO/IEC 27001:2022 requirements.

Revision History

Date	Description	Version	Author
6/1/2024	Initial mapping of NIST 800-53 Rev5 FedRAMP security controls in-scope of Moderate authorizations (such as ArcGIS Online) to International Standards Organization (ISO) 27001:2022 security controls. Source documents are as follows:	1	Esri
5/30/2024	FedRAMP Security Controls Moderate Baseline		FedRAMP
10/12/2023	National Online Informative References Program CSRC (nist.gov)		NIST



Overall Compliance Milestones



Shared Responsibility Model



softwaresecurity@esri.com

Esri Responsibilities



Compliance and Assurance – CAIQ 4.0.2

Updated June 2023

“What we do” to make ArcGIS Online Secure

Basic questions include:

- **Where is my data hosted?** Within AWS and MS Azure datacenters on US Soil by default, new organizations can choose to have their data stored in regions outside the US, such as the EU or AP Regions.
- **Is my data encrypted at rest and in transit?** Yes, organizations use HTTPS w/TLS 1.2 for in-transit and AES-256 at rest.
- **Is my data backed up?** Customers are responsible for backing up their datasets.
- **Can I do security tests against ArcGIS Online?** Yes, however a Security Assessment Agreement (SAA) must be completed first.
- **Are my files scanned with Anti-virus?** Yes – Files containing malicious code are rejected from upload.
- **What privacy assurance is in place?** ArcGIS Online is both GDPR and CCPA aligned.

For any questions/concerns/feedback please contact Esri’s Software Security & Privacy Team at:
SoftwareSecurity@Esri.com

Esri Responsibilities

Guidance – FedRAMP CRM



- Align with Customer Responsibility Matrix

- Trust Center “customer exclusive docs”
- Both Tailored Low and Moderate available

Example of a customer Responsibility

AC-22.d – Customer is responsible for periodically reviewing publicly available customer-controlled content for nonpublic information (Process)

ArcGIS Trust Center

Overview Security Privacy Compliance Documents Launch Security Adviser

Search ArcGIS Trust Center

ArcGIS Online FedRAMP Authorized Services
A detailed list of ArcGIS Online capabilities and applications in scope for its FedRAMP authorization. Updated June 2023, pdf.

Esri Vulnerability Disclosure Program Scope
Esri's PSIRT is the point of contact for security researchers who want to responsibly and ethically disclose security issues to Esri. This document described our program scope. Updated December 2023, 5 page pdf.

ArcGIS Online FedRAMP Tailored Low CRM
Customers desiring alignment with FedRAMP Tailored Low can use this to determine their responsibilities. Updated February 2023, pdf.

ArcGIS Online FedRAMP Moderate CRM
Customers desiring alignment with FedRAMP Moderate can use this to determine their responsibilities. Updated February 2023, pdf.

ArcGIS Online FQDN (Domain) Requirements
Organizations that prefer to domain access via FQDN instead of wildcard may reference the domains listed here. Updated June 2021, 4 page pdf.

ArcGIS Enterprise Web Application Filter rules
Recommended endpoints that can be denied access from external users via your Web Application Firewall (WAF). Updated March 2024, 14 page pdf.

ArcGIS Vulnerability Scanning Guidance
Information to help minimize/identify configuration items as well as false positives, so that the only concerns you need to share with the Esri are items that are potential vulnerabilities. Updated March 2024.

ArcGIS Software 3rd party Component CVE Responses
ArcGIS Software 3rd party Component CVE Responses. Updated March 2024.

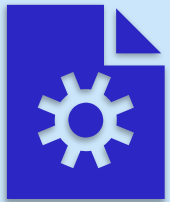
ArcGIS Online FedRAMP Moderate Customer Responsibility Matrix (CRM) Worksheet

Control ID	Specific Inheritance and Customer Agency/CSP Responsibilities
AC-3	Customers are responsible for managing access to their AGO Organization and for managing the AGO roles defined and any custom roles that are created by that Customer. Customer is also responsible for providing a SAML 2.0 Identity Provider for identity integration with the application, according to their policies and procedures to meet authentication requirements.
AC-8 (a)	Customers are responsible for adhering to all organizational policies and procedures in regard to displaying their system use notification banner. AGO allows customers to inject any banners or branding they might require at the application tier
AC-8 (c)	Customers are responsible for displaying system use information before granting further access to the publicly accessible resources in ArcGIS Online. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities and including a description of the authorized uses of the system. NOTE: If the customer has no publicly accessing resources in ArcGIS Online, then this control can be inherited from the CSP.
AC-14 (a)	Customer is responsible for identifying actions that can be performed on the customer-deployed resources without identification or authentication (e.g., such as viewing a publicly accessible services or apps or form).
AC-14 (b)	Customer is responsible for providing documentation for user actions not requiring identification or authentication in the customer organization. It is the responsibility of the customer to follow their own Rules of Behavior and policies around inviting and sharing to guests to application.
AC-21 (b)	The customer is responsible for employing a process to assist users with making information sharing decisions
AC-22 (a)	Customer is responsible for designating authorized personnel to post publicly accessible information in their AGO application.
AC-22 (b)	Customer is responsible for training the personnel defined in AC-21. a to prevent disclosure of nonpublic customer-controlled information.
AC-22 (c)	Customer is responsible for reviewing proposed content of customer-controlled information prior to posting publicly to ensure nonpublic information is not included.
AC-22 (d)	Customer is responsible for periodically reviewing publicly available customer-controlled content for nonpublic information.
AT-2 (a)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-2 (b)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-2 (c)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-2 (d)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-2(2)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-2(3)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-3 (a)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-3 (b)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-3 (c)	Customer is responsible providing training for their users, training may be developed using the AGO user guide and other online documentations.
AT-4 (a)	Customer is responsible for retaining the training records for their users.
AT-4 (b)	Customer is responsible for retaining the training records for their users.
CA-6 (a)	Sponsoring agency must identify a senior-level executive or manager as the authorizing official for the AGO.
CA-6 (b)	Agency must also determine whether the risk to the agency is acceptable. Following review of the security authorization package and discussing with agency officials and Independent Assessor/3PAO, the AO renders an authorization.
CA-6 (c)	Authorizing official for the system, are responsible for ensuring authorization before commencing operations
CA-6 (d)	Authorizing official is responsible for ensuring that for common controls for inheritance by organizational systems are authorized
CA-6 (e)	Authorizing official agency is responsible for updating the authorization in accordance with OMB A-130 requirements or when a significant change occurs
CP-9 (a)	Customer is responsible for conducting backups of user-level information in customer-deployed resources at a frequency consistent with customer-defined RTOs and RPOs.
CP-9 (d)	Customer is responsible for protecting the confidentiality, integrity, and availability of backup information they backed up.
CP-9(1)	Customer is responsible for backing up customer data and applications they developed. Customer is also responsible for testing those backups.
IA-2	Customer is responsible for providing a SAML 2.0 configuration to federate their ArcGIS Online organization with their agency identity provider for authentication.

Customer Security Responsibilities



PROCESSES



CONFIGURATION

Customer Responsibilities

Processes

- Establish a content **Publication Review Board**
 - Review content before publication
 - Then regularly review content after
 - **Disable the ability for users to share publicly**
- Classify your datasets and secure them appropriately
 - Leverage groups to bucket datasets
 - Public, Internal Use, Confidential, Restricted



PROCESSES

Customer Responsibilities

Processes

- Authentication enforcement
 - Enable multi-Factor Authentication (MFA)
 - Always disable Anonymous access in your org
 - SAML authentication
 - Leverage API keys for automation
- Use custom roles to granularly define permissions
 - Don't use the ADMIN role as a daily driver



PROCESSES

Customer Responsibilities

What else?



PROCESSES



CONFIGURATION



CONFIGURATION

Deeper Dives

SAML & Org Specific Login Guidance
AGO Security and Privacy Advisor

softwaresecurity@esri.com

Manage Security Posture

Item sharing status...

User security status...

Configuration drift...

ArcGIS Security and Privacy Adviser (STG)

Best Practice Validation and Discovery Tool



Risks & Mitigations

SAML Security



Entra ID



ArcGIS Online



Assertion



SAML Security Cheat Sheet

Introduction

The **Security Assertion Markup Language (SAML)** is an open standard for exchanging authorization and authentication information. The *Web Browser SAML/SSO Profile with Redirect/POST bindings* is one of the most common SSO implementation. This cheatsheet will focus primarily on that profile.

Validate Message Confidentiality and Integrity

TLS 1.2 is the most common solution to guarantee message confidentiality and integrity at the transport layer.

- Theft of User Authentication Information 7.1.1.2
- Theft of the Bearer Token 7.1.1.3
- Message Deletion 7.1.1.6
- Message Modification 7.1.1.7
- Man-in-the-middle 7.1.1.8

A digitally signed message with a certified key is the most common solution to guarantee message integrity and authentication. Refer to [SAML Security \(section 4.3\)](#) for additional information. This step will help counter the following attacks:

- Forged Assertion 6.4.3
- Message Modification 7.1.1.7

Risk: Message Modification

SAML Security



Entra ID



ArcGIS Online



Modified Assertion



Attacker

```
<samlp:Response ID="_3eda1900-a1be-4802-9604-52ae4a117132" Version="2.0" IssueInstant="2023-07-06T15:46:27.251Z" Destination="https://1
<Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">https://sts.windows.net/91f5663a-841b-4dec-b19d-c0fb6f66b4bc/</Issuer>
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
<Assertion ID="_38a4bdd1-b7f4-4f48-bab2-252bd2327e00" IssueInstant="2023-07-06T15:46:27.244Z" Version="2.0" xmlns="urn:oasis:names:
<Issuer>https://sts.windows.net/91f5663a-841b-4dec-b19d-c0fb6f66b4bc/</Issuer>
<Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
  <SignedInfo>
    <CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
    <SignatureMethod Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" />
    <Reference URI="#_38a4bdd1-b7f4-4f48-bab2-252bd2327e00">
      <Transforms>
        <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
        <Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      </Transforms>
      <DigestMethod Algorithm="http://www.w3.org/2001/04/xmlenc#sha256" />
      <DigestValue>LPZG44TPi39nM11165mre2jUTwzMSGUfHsQDJk1UdY=</DigestValue>
    </Reference>
  </SignedInfo>
  <SignatureValue>fp79C57aN0pgccL2ZiCk5S2Peb0G2IY1txs/69WNSRSVUF8n1Z5HijwOVfMtJib0IZBCQ12fj4kKii9hLL7+w9tJ58x8Ub0e8sq/knBgEEc
  <KeyInfo>
    <X509Data>
      <X509Certificate>MIIC8DCCAdigAwIBAgIQKsVGHf6/pVMXEn0EWXZTANBgkqhkiG9w0BAQsFADA0MTIwMAYDVQQDEylNaWNyb3NvZnQxLn
    </X509Data>
  </KeyInfo>
</Signature>
<Subject>
  <NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress">uc2023@SSPAzLaboutlook.onmicrosoft.com</NameID>
  <SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <SubjectConfirmationData InResponseTo="_yHcio0sHLYTziDgR" NotOnOrAfter="2023-07-06T16:46:26.938Z" Recipient="https://1f
  </SubjectConfirmation>
</Subject>
<Conditions NotBefore="2023-07-06T15:41:26.938Z" NotOnOrAfter="2023-07-06T16:46:26.938Z">
  <AudienceRestriction>
    <Audience>1687903745152.maps.arcgis.com</Audience>
  </AudienceRestriction>
</Conditions>
<AttributeStatement>
  <Attribute Name="http://schemas.microsoft.com/identity/claims/tenantid">
    <AttributeValue>91f5663a-841b-4dec-b19d-c0fb6f66b4bc</AttributeValue>
  </AttributeStatement>
</AttributeStatement>
</Assertion>
</samlp:Response>
```

Signed SAML Assertion

Risk: Forged Assertions

SAML Security



Entra ID



ArcGIS Online



Forged Assertion



Attacker

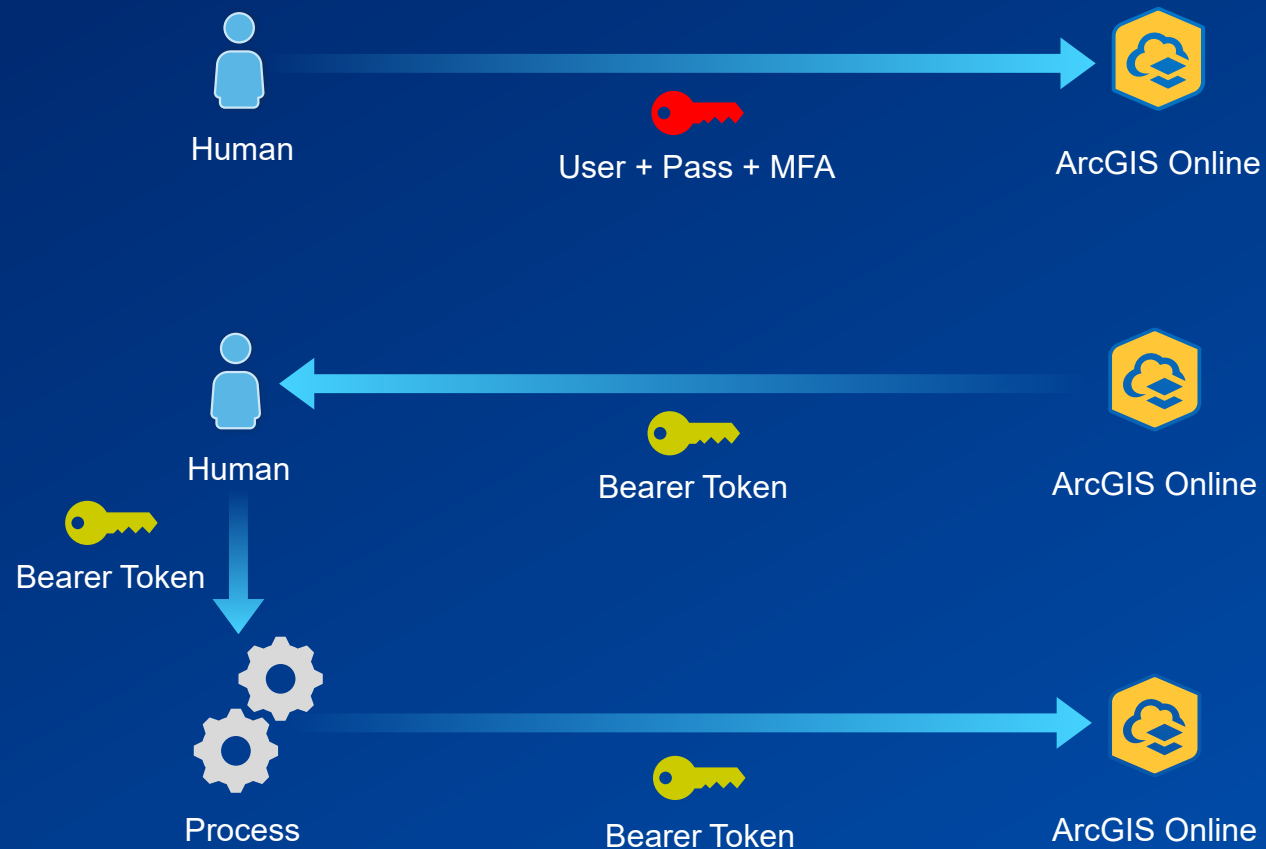
```
<samlp:Response ID="_e6812948-8856-471c-9ed2-3d8afc1dd797" Version="2.0" IssueInstant="2023-07-06T19:04:08.123Z"
  <Issuer xmlns="urn:oasis:names:tc:SAML:2.0:assertion">https://sts.windows.net/91f5663a-841b-4dec-b19d-c0fb6f
  <samlp:Status>
    <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
  </samlp:Status>
  <EncryptedAssertion xmlns="urn:oasis:names:tc:SAML:2.0:assertion">
    <xenc:EncryptedData Type="http://www.w3.org/2001/04/xmlenc#Element" xmlns:xenc="http://www.w3.org/2001/
    <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
    <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
      <e:EncryptedKey xmlns:e="http://www.w3.org/2001/04/xmlenc#">
        <e:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p">
          <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        </e:EncryptionMethod>
        <KeyInfo>
          <o:SecurityTokenReference xmlns:o="http://docs.oasis-open.org/wss/2004/01/oasis-200401-
            <X509Data>
              <X509IssuerSerial>
                <X509IssuerName>CN=DigiCert TLS RSA SHA256 2020 CA1, O=DigiCert Inc, C=US</
                <X509SerialNumber>17348719369614408394160810923335762973</X509SerialNumber>
              </X509IssuerSerial>
            </X509Data>
          </o:SecurityTokenReference>
        </KeyInfo>
        <e:CipherData>
          <e:CipherValue>NcQmZZxTzSwCmAYSmp+JcqyHr94+U0Qt6RsiRTqwiJ7Ndy4g1wEvkpg62RBjZueo+DZ01Fc13
          </e:CipherValue>
        </e:CipherData>
      </e:EncryptedKey>
    </KeyInfo>
    <xenc:CipherData>
      <xenc:CipherValue>VmmMcogck1B0r04sLB9321tvSMD0MCK0KrqSc+iPztfYB88HMe4+VRL6rHChLABtrQ5dhIdx0jTo1v
      </xenc:CipherValue>
    </xenc:CipherData>
  </xenc:EncryptedData>
</EncryptedAssertion>
</samlp:Response>
```

Encrypted Assertion



Challenge: Automation

How (not) to authenticate?



lifetime: <14 days

softwaresecurity@esri.com



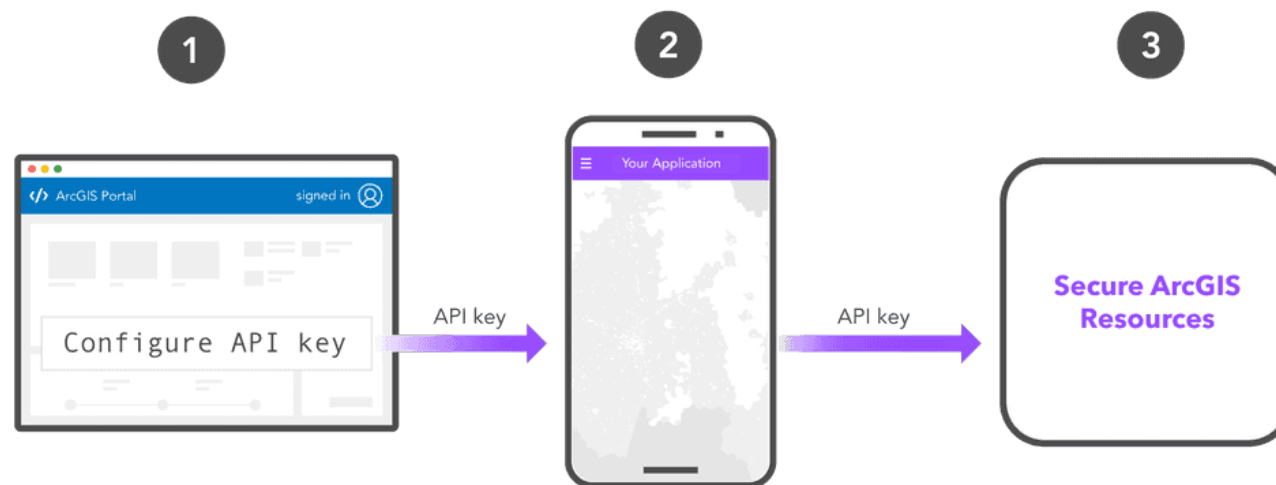
Solution: API Tokens

Released: June 2024

 Simplified Authentication

 Scoped Tokens

 Token Management



Summary

- Compliance
 - FedRAMP Moderate
 - ISO 27001 Efforts
- Shared Responsibility Model
 - Customer Responsibilities
- Demos
 - ArcGIS Security and Privacy Adviser
 - Automation: API Tokens
- Q&A





esri[®]

**THE
SCIENCE
OF
WHERE**[®]

Copyright © 2024 Esri. All rights reserved.

softwaresecurity@esri.com