SDG's Certificate Update Toolkit (CUT) Enhances Productivity and Simplifies SAML Signing Certificate Management

Provide IdP SAML Signing Certificate management self-service capabilities to application teams/owners

OVERVIEW

Effective management of signing certificates is essential for secure enterprise SAML-enabled applications. With certificate authorities now limiting the validity of CA-signed certificates to approximately 398 days, many enterprises face the annual task of updating certificates before expiration. This process requires coordinated efforts between the Identity Provider (IdP) and the Service Provider (SP) teams to ensure timely updates on both sides. The complexity of this task often results in operational overhead, including frequent meetings, extensive email exchanges, and significant collaboration to complete the updates efficiently.

To address this challenge, SDG developed the Certificate Update Toolkit (CUT) to simplify updating certificates at the IdP end and rich with additional features.

SIGNING CERTIFICATE MANAGEMENT CHALLENGES

Signing certificates are essential for secure SAML transactions, establishing a trusted channel between Identity Providers and Service Providers. Efficient management of SAML signing certificates is critical for maintaining security, operational efficiency, and compliance.

Improper and inadequate management processes create security and compliance risks. Common challenges include:

- **Frequent Expiration:** TLS/SSL certificate validity is now limited to 398 days (approximately 13 months), following decisions by several organizations to reject certificates with longer validity periods.

- **Missing Centralized Self-Service Signing Certificate Management Platform:** In major Identity Provider systems, SAML certificate management is primarily an administrative task requiring coordination between the Identity Provider and the Service Provider's technical team. Most Identity Provider solutions lack an out-of-the-box self-service platform for application owners or technical teams to manage certificates conveniently across multiple environments within the required time frame.

SDG's Certificate Update Toolkit (CUT) Enhances Productivity and Simplifies SAML Signing Certificate Management
Provide IdP SAML Signing Certificate management self-service capabilities to application teams/owners

1

- **Dependency:** Out-of-the-box SAML certificate management involves dependencies between the Identity Provider operations team, Service Provider application team, and, in some cases, the application COTS team, alongside organizational change management. Typically, the Identity Provider team coordinates with the Service Provider, which then aligns with the application COTS team to schedule the update. This process creates significant dependencies and operational overhead for all involved teams.

- **Reporting and Analytics:** Current Identity Provider solutions lack platforms for certificate management and offer limited or no features for reporting and analytics to track the status of these activities across all environments.

- **Operational Overhead:** Enterprises adhere to standard organizational change management processes, including ticket creation and change tracking for various activities. Managing these processes alongside certificate updates creates an operational burden for the Identity Provider team, leading to challenges such as reduced functional efficiency, missed SLAs, and sudden demands for increased team size.

- **Scalability:** As organizations expand, the number of environments grows, increasing the complexity of managing certificates across all environments. Admin-level certificate management often requires logging into multiple environments to update certificates for the same application.

SOLUTION: SDG'S CERTIFICATE UPDATE TOOLKIT (CUT)

SDG's CUT solution addresses organizational challenges by offering a comprehensive platform for efficiently and securely managing SAML signing certificates at the Identity Provider. It enables application owners and technical teams to perform certificate updates in a self-service manner, eliminating the need for intervention by the Identity Provider operations team while ensuring proper oversight and control.

Key Features Include:

- **Self-Service Application Owner/Team Interface:** SDG's CUT provides a user-friendly interface that does not require in-depth technical knowledge to use and is completely designed using a Java framework. It gives application owners access to multiple features as listed below:

  - Capability to select the environment in which the certificate needs to change.

  - Selecting the required connection from the list of authorized applications using coarse-grained, group-based authorization.

  - Single click certificate update at Identity Provider's end provides flexibility for the application team to sync the activity at the Service Provider's end.

  - Single click rollback in case of task failure restoring application functionality instantly.

  - Capability to download the metadata as well as new certificate as required.

SDG
SDG's Certificate Update Toolkit (CUT) Enhances Productivity and Simplifies SAML Signing Certificate Management
Provide IdP SAML Signing Certificate management self-service capabilities to application teams/owners
2

- **Identity Provider's Operation Admin Interface:** Although Identity Provider operations can use the out-of-the-box admin interface, the thin interface offers additional capabilities, including:
  - Capability to update backend information point in a single click;
  - To update owner details in case of outdated information since last year;
  - Generate reporting for the connections completed and those are left, and;
  - Updating the cases which are in queue and yet to be closed in the ITSM system.

- **Scalability:** SDG's CUT platform is designed in such a manner that it can be scaled to have:
  - Integration with multiple environments (up to 4 and can be customized), and;
  - Integration with REST-enabled ITSM systems.

- **Customizable:** The CUT is a prototype with extensive customization features that can be tailored to meet an organization's unique needs and enable support for various use cases, such as:
  - Delegated administration of limited functionalities to application teams;
  - Integration of applicable environments, and;
  - Customizable to adapt to multiple market-leading Identity Provider systems provided they meet the integration pre-requisites.

- **Real-Time Auditing and Reporting:** Robust auditing capabilities help organizations track changes and maintain compliance with security policies and regulations. Available options include the ability to export reports for certificate management tasks.

- **Additional Benefits:**
  - Reduced IT overhead
  - Reduced dependency
  - Reduced communication overhead
  - Quicker time to activity completion

CONCLUSION

IAM teams must efficiently manage SAML signing certificates signed by a CA to support integrated applications. SDG's Certificate Update Toolkit simplifies certificate management across Identity Provider environments by offering a self-service, automated solution. With an intuitive dashboard, CUT enhances productivity, strengthens security, ensures compliance, and reduces the administrative burden on Identity Provider teams. Investing in CUT is a strategic decision that supports organizational growth and long-term success.

SDG

75 North Water Street
Norwalk, CT 06854
203.866.8886
sdgc.com