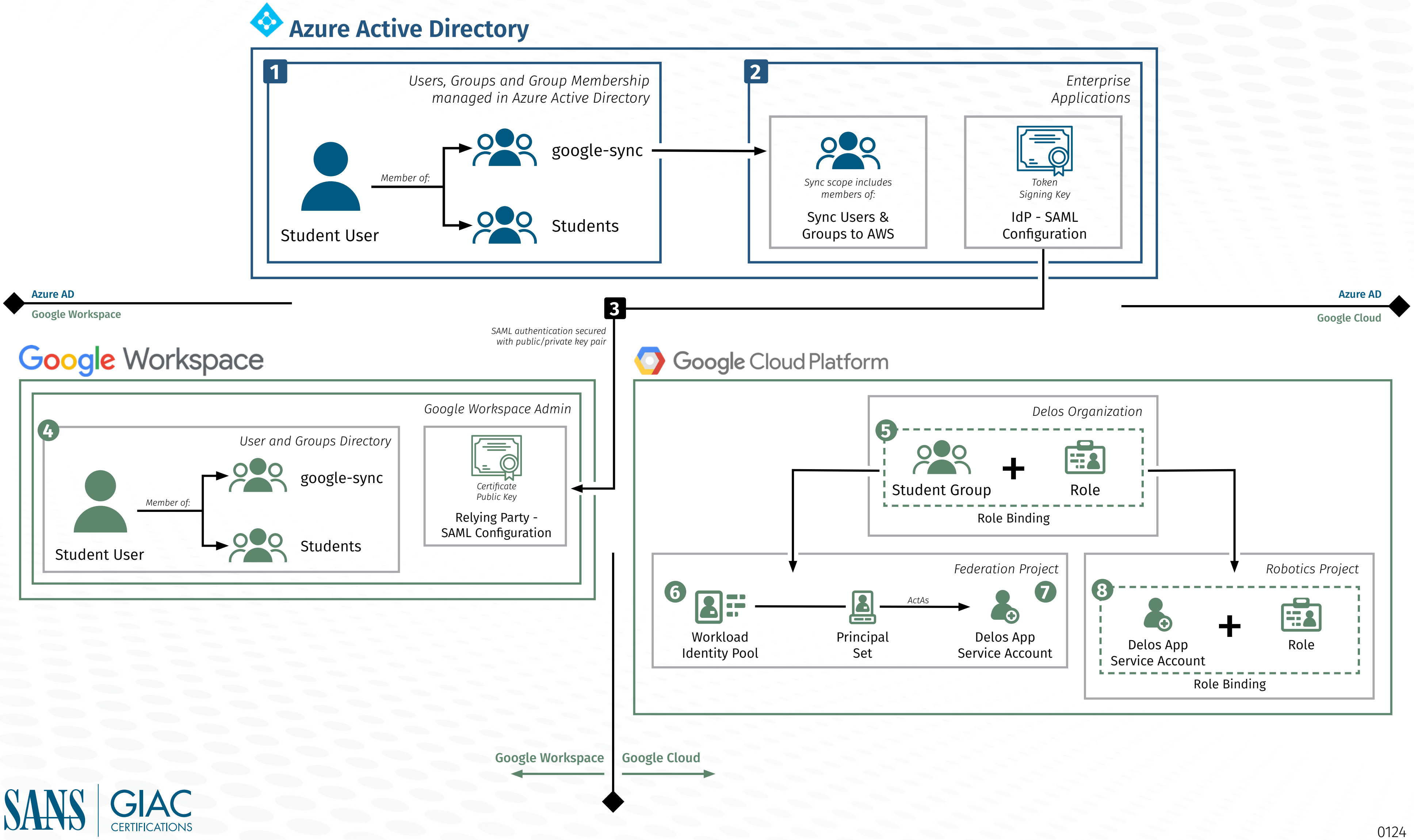
Azure to GCP Identity Architecture

CLOUD SECURITY

Created by Kat Traxler and Eric Johnson, co-authors of
SEC549: Enterprise Cloud Security Architecture | *sans.org/sec549*



Azure Active Directory

1 *Users, Groups and Group Membership managed in Azure Active Directory*

Student User

Member of:

google-sync

Students

2 *Enterprise Applications*

Sync scope includes members of:

Sync Users & Groups to AWS

Token Signing Key

IdP - SAML Configuration

Azure AD

Google Workspace

3

SAML authentication secured with public/private key pair

Azure AD

Google Cloud

Google Workspace

Google Workspace Admin

4 *User and Groups Directory*

Student User

Member of:

google-sync

Students

Certificate Public Key

Relying Party - SAML Configuration

Google Cloud Platform

Delos Organization

5

Student Group + Role

Role Binding

Federation Project

6

Workload Identity Pool

Principal Set

ActAs

7

Delos App Service Account

Robotics Project

8

Delos App Service Account + Role

Role Binding

Google Workspace

Google Cloud

SANS | GIAC CERTIFICATIONS

0124

Azure to GCP Identity Architecture

DIAGRAM KEY

1 User and groups managed within Identity Provider (Azure AD)

2 Azure Enterprise Applications used to sync in-scope users and groups to GCP and configure SAML Federation

3 SAML tokens signed and secured with private key stored in Azure AD, Public key exported to the Google Workspace Admin Console and used to validate SAML tokens

4 In-scope users and groups are replicated to a directory in Google Workspace

5 Google Cloud Roles are assigned to the Student User at the Organization Level and the permissions cascade down the hierarchy to all Projects and Resources

6 All Workload Identity Pools are created in a dedicated Project in order to confine blast radius and reduce identity sprawl.

7 Service Accounts are created within Projects. Where federation is configured, Workload Identity Principal Sets are allowed to ‘Act As’ Service Accounts.

8 Cross-Project Permissions are assigned to Service Accounts though Role Bindings. The confluence of a Principal, a Role and Resource such as a Project constitutes a Role Binding