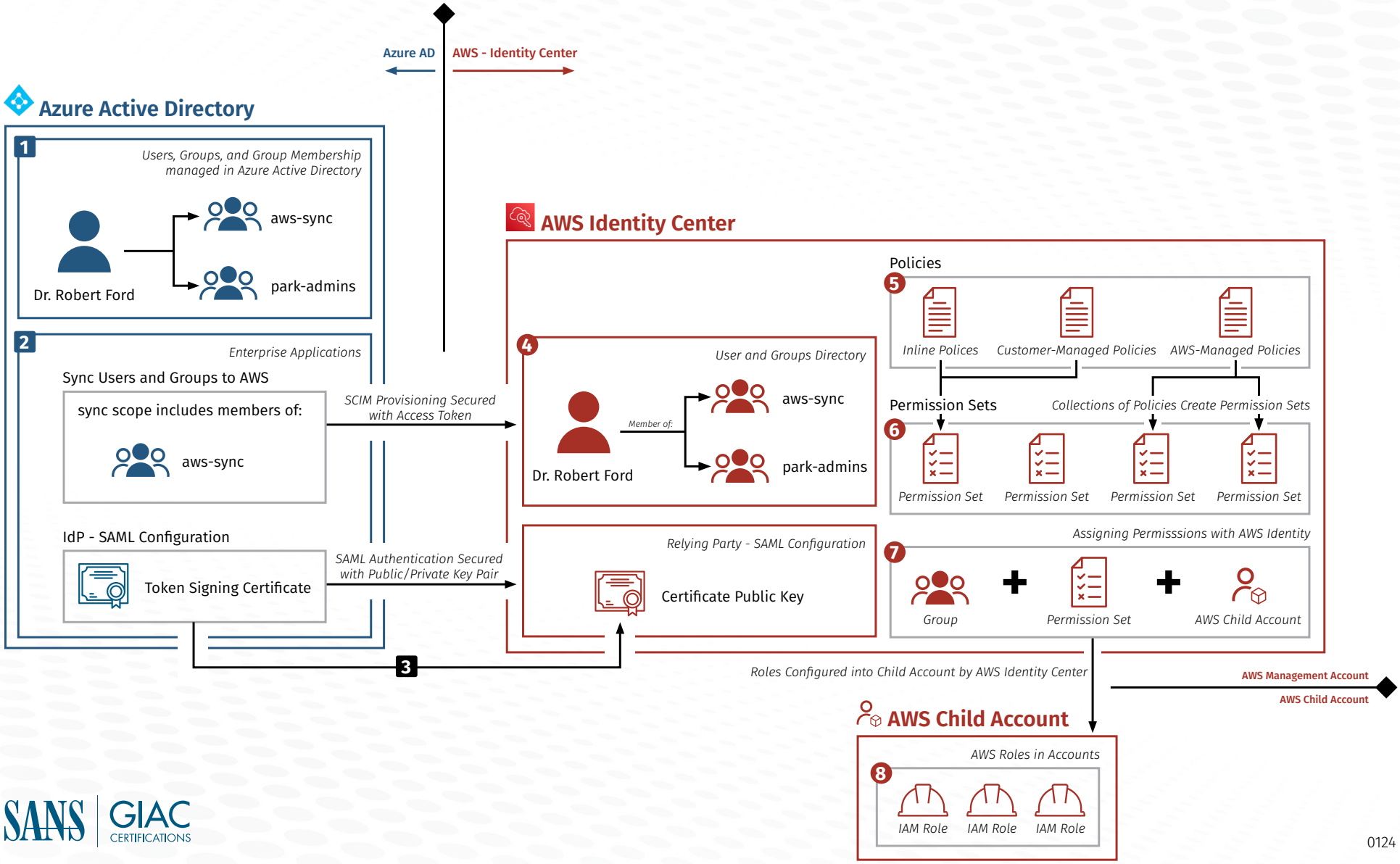
# Azure to AWS Identity Architecture

CLOUD SECURITY

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




SANS | GIAC CERTIFICATIONS

# Azure to AWS 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 AWS and configure SAML Federation
3. SAML tokens signed and secured with private key stored in Azure AD, Public key exported to AWS Identity Center and used to validate SAML tokens
4. In-scope users and groups are replicated to AWS Identity Center
5. Collections of permissions are maintained in AWS Identity Center as either inline, customer managed, or AWS managed policies'
6. Policies are bundled together in AWS Identity Center to form permission sets
7. Assigning permissions in AWS Identity Center requires binding of groups, permission sets, and the AWS account the permissions will effect
8. Assignments deployed as IAM Roles into Child Accounts