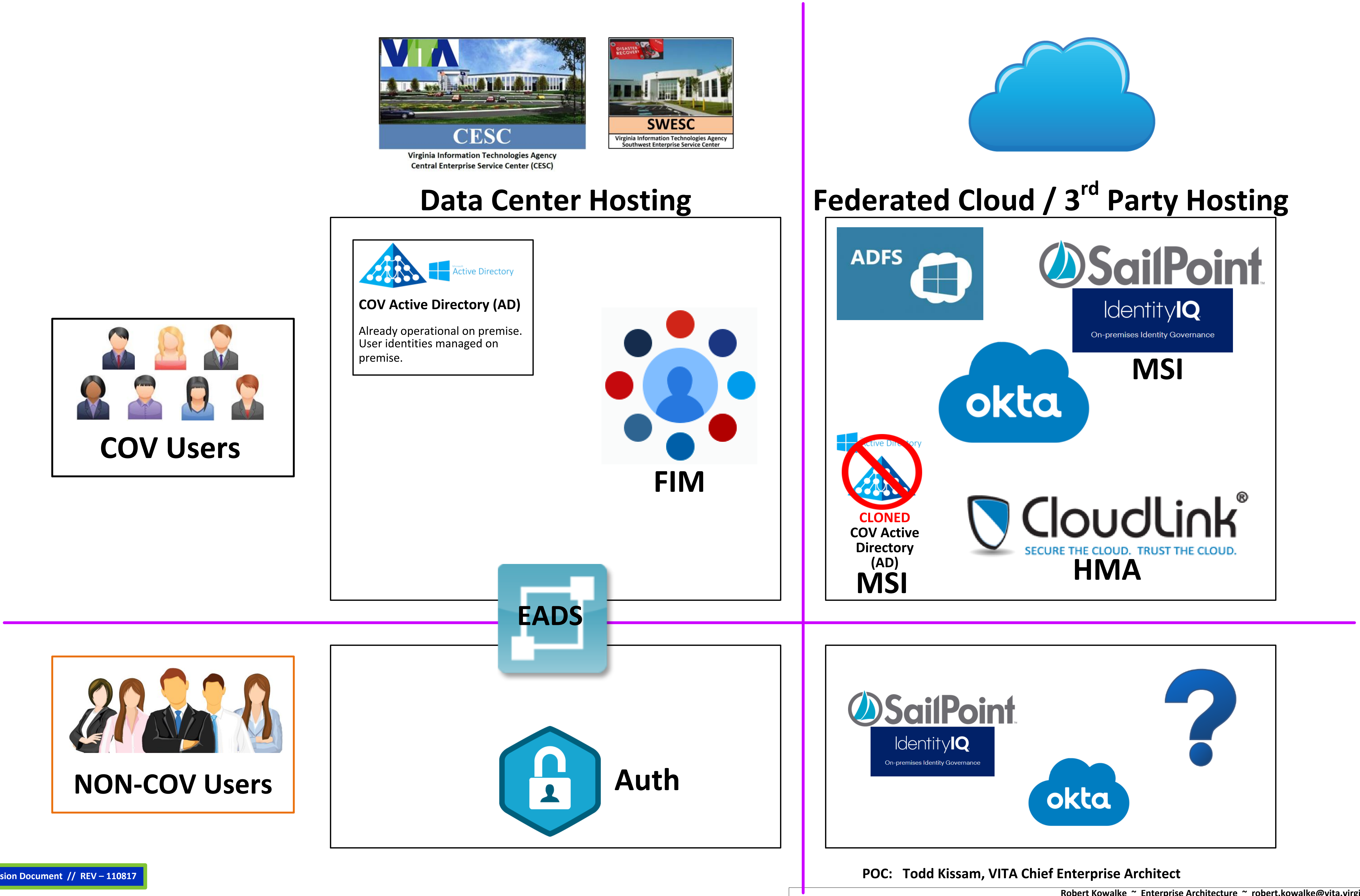
Virginia Information Technologies Agency

VITA

Enterprise Architecture
MSI SMS Authentication



Virginia Information Technologies Agency
Central Enterprise Service Center (CESC)

Virginia Information Technologies Agency
Southwest Enterprise Service Center

Data Center Hosting

Federated Cloud / 3rd Party Hosting

COV Active Directory (AD)

Already operational on premise. User identities managed on premise.

VITA Draft Discussion Document // REV – 110817

POC: Todd Kissam, VITA Chief Enterprise Architect

PURPOSE: To depict the authentication possibilities in support of a way-ahead decision for directory services; especially for non-COV users.

Robert Kowalke ~ Enterprise Architecture ~ robert.kowalke@vita.virginia.gov
Relationship Management & Governance (RM&G) @ Virginia Information Technologies Agency (VITA)
Commonwealth Enterprise Solutions Center (CESC)
Architectural Artifacts/Graphs/Views/Matrices/etc. reference page: http://pubs.opengroup.org/architecture/togaf9-doc/arch/chap35.html

Active Directory (AD): A directory service that Microsoft developed for Windows domain networks. Starting with Windows Server 2008, AD became an umbrella title for a broad range of directory-based identity-related services. AD authenticates and authorizes all users and computers in a Windows domain type network – assigning and enforcing security policies for all computers and installing or updating software. For example, when a user logs into a computer that is part of a Windows domain, AD checks the submitted password and determines whether the user is a system administrator or normal user. Also, it allows management and storage of information, provides authentication and authorization mechanisms, and establishes a framework to deploy other related services: Certificate Services, Federated Services, Lightweight Directory Services, and Rights Management Services. Active Directory uses Lightweight Directory Access Protocol (LDAP) versions 2 and 3, Microsoft's version of Kerberos, and DNS. https://en.wikipedia.org/wiki/Active_Directory.

Federated Identity Management (FIM): The means of linking a person's electronic identity and attributes, which are stored across multiple distinct identity management systems. Related to federated identity is single sign-on (SSO), in which a user's single authentication ticket, or token, is trusted across multiple IT systems or even organizations. SSO is a subset of federated identity management, as it relates only to authentication and is understood on the level of technical interoperability, which would not be possible without some sort of federation. https://en.wikipedia.org/wiki/Federated_identity
Federated identity management requires a complex set of technologies and business processes, but the goal behind it is simple; to automatically share identity information across administrative boundaries. https://www.csoonline.com/article/2121227/federated-identity/the-truth-about-federated-identity-management.html
Today, we see federated identity everywhere, most noticeably in what we call "single sign on." With single sign on, you can log into your GMail and then open up YouTube in a different tab, for instance, and you'll stay logged in. It all hinges on a central domain verifying the status of each user as they move across sub-domains: 1) You log in once; 2) Authentication is done through a central domain; 3) A token or cookie is generated to authenticate you across other domains. https://auth0.com/blog/why-identity-federation-matters/

Auth: The Authentication active directory will support apps that need AD authentication for external users. It contains accounts for both internal and external users. The domain will enable userPrincipalName authentication for applications supporting userPrincipalName authentication. The Organizational Unit (OU) structure for the Authentication domain is based on multiple security levels applied to users. Based on application security requirements, users will be placed in the highest security level required for applications. Current naming convention for the Authentication Active Directory Domain is: auth.cov.virginia.gov. This domain name service offers several layers such as: Enterprise Production, Domain Controllers, Application Servers, Administrative Accounts, and Service Accounts. Security policy is applied at the OU and domain level. The Authentication Active directory will implement a security policy based on the standard Windows 2008 Security Guide and standard SEC 501 policies, with the exception of account policies for external users. A separate policy is applied based on Global Group Membership. https://shop.vita.virginia.gov/ProductDetail.aspx?id=6442473736

FYI: OAuth is an open standard for access delegation, commonly used as a way for Internet users to grant websites or applications access to their information on other websites but without giving them the passwords. This mechanism is used by companies such as Google, Facebook, Microsoft and Twitter to permit the users to share information about their accounts with third party applications or websites. Generally, OAuth provides to clients a "secure delegated access" to server resources on behalf of a resource owner. It specifies a process for resource owners to authorize third-party access to their server resources without sharing their credentials. Designed specifically to work with Hypertext Transfer Protocol (HTTP), OAuth essentially allows access tokens to be issued to third-party clients by an authorization server, with the approval of the resource owner. The third party then uses the access token to access the protected resources hosted by the resource server. https://en.wikipedia.org/

Okta: Supports enterprise-wide comprehensive identity management across any app, user, or device. A future-proof cloud service designed for maximum ROI & ease of use. Okta Identity Management is in the Identity-Management-as-a-Service (IDaaS) arena and one of the top IDaaS performers. Okta Single Sign-on is *part* of a complete identity and access management solution. https://www.pcmag.com/article2/0,2817,2491438,00.asp Okta Single Sign-on is a light weight solution that securely connects your employees, contractors, and customers across any of their devices to all of their cloud and on-premise applications.

Cloudlink (HMA): CloudLink SecureVM provides organizations with the security controls necessary to run virtualized machines in the cloud with confidence. SecureVM enables encryption of the entire virtualized server or desktop running in the cloud, independent of the cloud service provider. Protection of the entire virtualized machine (server or desktop), enables organizations to define security policies to allow a particular virtual machine to start - including the ability to verify the integrity of the virtual machine. Ensures only trusted and verified VMs have the ability to run and access sensitive data residing in the cloud. Works in combination with native OS encryption such as Microsoft BitLocker volume encryption solution technology widely implemented for physical machines. Extends BitLocker functionality as BitLocker native authentication mechanisms are not supported in cloud environments. SecureVM's proven encryption key policy management functionality allows BitLocker to be used for automated encryption of boot volumes in the cloud while enabling enterprise administrators to control security policy and encryption keys. SecureVM also supports Linux native encryption, providing organizations with a single encryption management solution for multiple clouds and VM operating systems. Part of EMC Corporation. http://www.cloudlinktech.com/

SailPoint IdentityIQ (MSI): Sailpoint is an identity and access management (IAM) provider. It brings together single-sign on, password management, and user access provisioning on-premises and in SaaS. Other companies in the IAM space include Ping Identity and Okta. Delivered as a cloud service with no hardware or software to deploy, SailPoint's IdentityNow provides fully-integrated identity and access management (IAM) solution for compliance, provisioning and access management. IdentityNow meets the most stringent IAM-as-a-service (IDaaS) requirements and provides enterprise-grade services that meet security, scalability, performance, and availability demands. It uniquely provides the option of a staged on-ramp to the cloud for customers who need an on-premises solution today, but who also might want the future-proofing ability to transition over time to IAM-as-a-service (IDaaS). https://www.columninfosec.com/sailpoint/identity-and-access-management-sailpoint.html

AD FS: Active Directory Federation Services (AD FS). Microsoft prefers the acronym to have a space in between the letters AD and FS. Why? No clue – just call Bill look like this → AD FS. AD FS is a standards-based service that allows the secure sharing of identity information between trusted business partners (known as a federation) across an extranet. When a user needs to access a Web application from one of its federation partners, the user's own organization is responsible for authenticating the user and providing identity information in the form of "claims" to the partner that hosts the Web application. The hosting partner uses its trust policy to map the incoming claims to claims that are understood by its Web application, which uses the claims to make authorization decisions. AD FS is Microsoft's implementation of the WS-Federation Passive Requestor Profile protocol (passive indicates that the client requirements are just a cookie- and JavaScript-enabled Web browser). AD FS implements the standards based WS-Federation protocol and Security Assertion Markup Language (SAML). https://msdn.microsoft.com/en-us/library/bb897402.aspx

EADS: External Authentication Domain Service (EADS): Service that allows users internally and externally of the COV domain to have access to applications that require AD access, which is outside of the COV domain and areas of the COV networking infrastructure. https://shop.vita.virginia.gov/ProductDetail.aspx?id=6442473736

AD Clone (Rejected): It is what it is – a clone. **IAM** = Identity and Access Management. **IdP** = Identity Provider. **SAML** = Security Assertion Markup Language (Protocol for authentication and authorization). **LDAP** = Lightweight Directory Access Protocol (Open, vendor-neutral, and industry standard app protocol. A common use of LDAP is to provide a central place to store usernames and passwords. This allows many different applications and services to connect to the LDAP server to validate users. Sometimes called X.500-lite.). **Kerberos** = Network authentication protocol (Uses tickets to allow nodes communicating over a non-secure network to prove their identity to one another in a secure manner.). MFA = Multifactor Authentication.