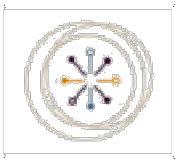

Glossary

Term	Acronyms	Definition
Access Management	AM	Broad umbrella of technical solutions that provide authentication and authorization of users and devices.
Adaptive Authentication		A risk-based approach enabling strong, multifactor authentication using various parameters as device forensics, behavioral analysis, IP Address, etc., that takes place in the background and is used to help prevent fraud.
Advanced Authentication Methods		Authentication methods using biometrics, SMS, voice recognition, etc.
Agent-based PeP		Protects resources by connecting to local APIs and container-level policies on Web servers and Web application servers. With local access to the server, agent-based PePs can broker authentication request and control HTTP sessions for all activity on the server. It can provide granular authorization of resource usage.
Attestation		An affirmation of authenticity in the realm of Governance or Compliance, typically created by the entity that wants to prove they meet the requirements for Governance or Compliance.
Attribute-Based Access Control		Granting access based on attributes.
Authentication		The method by which an entity is validated to be who they say they are.
Authentication Gateway	AG	A centralized, unified solution to all authentication of a particular group of often disparate systems. Typically integrated with Single Sign On.
Authentication Modality		The various types of Authentication, including, but not limited to: Fingerprints, Retina Scans, Voice Recognition, etc.
Authorization		The process of granting access to a particular set of resources after an entity has passed Authentication.

Term	Acronyms	Definition
Automated Entitlement Recertification		Periodically invite managers and application owners to review lists of users and security entitlements within their scope of authority, flagging inappropriate entries for further review and removal.
Automated Role-Based or Attribute Provisioning to Default Resources		Each user is given “birth-right” resources when on-boarded or registered based on their role and/or a number of attributes. This process should be automated.
Biometric Authentication		Any Authentication Modality using unique biometric possesions including, but not limited to: Fingerprints, Retina Scans, Voice Recognition, etc.
Certificate Authority	CA	A trusted, and an entity that issues digital certificates. A digital certificate certifies the ownership of a public key by the named subject of the certificate.
Common User Identifier Across Applications		Each user has a common identifier across all resources, and this identifier ties all of this user’s accounts regardless of the person’s role. For instance, a user can be an employee, a physician, and a student all at the same time. Each role has a set of entitlements to many resources. A user’s account in each resource can be associated with the actual end-user is via the common identifier.
Compliance, Reporting, Auditing		Reports generated from SIEM and Access Governance software can provide information about compliance to access rights. The process of reviewing logs is a way to audit information collected by the software.
Control Objectives for Information and Related Technology	COBIT	Control Objectives for Information and Related Technology (COBIT) is a framework created by ISACA for information technology (IT) management and IT governance. It is a supporting toolset that allows managers to bridge the gap between control requirements, technical issues and business risks.
Credential		A unique identifying attribute that is used to authenticate an entity.

Term	Acronyms	Definition
Data Feed		This is the initial process of loading identity information for each user into the identity management system. It is a laborious process and requires the following tasks: 1. Identification and integration of an authoritative source. 2. Data clean up, if needed to ensure that the information that's going to be loaded into the identity management system is clean and accurate. 3. Ensuring that the authoritative source has the required attributes to complete a person's identity. 4. If a person's complete identity cannot be gathered from one authoritative source then collecting the required attributes from other user registries needs to be done. While the definition of complete identity depends on each organization, it should include essential attributes relative to the industry. 5. The initial feed process can be from a CSV file, or from a database.
Enrollment		The process by which an entity's attributes are stored in a system to later be used for Authentication and Authorization.
Enterprise Authentication Service		An authentication method that is used throughout all most or all the organizations. (e.g. Secure LDAP authentication, two-factor authentication, etc.)
Enterprise Identities		Identities that are associated only with the entities within an organization.
Enterprise Reduced Sign-On		Reduced Sign-On is implemented to achieve seamless access to numerous resources without having to re-authenticate. Implementing reduced sign-on requires password synchronization to ensure consistent and seamless user experience.
Entitlement		A profile granting access to various resources.
Entitlement Catalog		Access rights over a resource. An entitlement contains the following information: • Entitlement name • Entitlement owner • Business description • Technical description • Plain language description

Term	Acronyms	Definition
Federal Information Processing Standards	FIPS	Federal Information Processing Standards (FIPS) are publicly announced standardizations developed by the United States federal government for use in computer systems by all non-military government agencies and by government contractors, when properly invoked and tailored on a contract.
Federation		The sharing of identities for the purposes of Authentication and/or Authorization between two or more disparate systems.
Federation with Partners		A model that enables companies with several different technologies, standards and use-cases to share their applications by allowing individuals to use the same login credentials or other personal identification information across security domains.
Identity and Access Management	IAM	A collection of technologies intended to simplify the provisioning and depovisioning entity access to different types of systems.
Identity as a Service	IDaaS	Cloud-based identity provisiong services.
Identity Events and Triggers		An event entails HR actions such as on-boarding of a new employee, which then triggers certain actions to start the provisioning process. An event also can trigger actions when a person registers at a portal. The triggered action may be the creation of the person's account.
Identity Integration and Correlation with SIEM		Ability to monitor identity information with the use of SIEM (Security Information and Event Management) software. SIEM software provides information about – what, why, when, and how the resources were accessed.
Identity Proofing		Identity proofing is about verifying people's identities before they are issued accounts and credentials. It is based on "life history" or transaction information aggregated from public and proprietary data sources. These services are also used as an additional interactive user authentication method, especially for risky transactions, such as accessing sensitive confidential information or transferring funds to external accounts.

Term	Acronyms	Definition
Identity Synchronization		Identity synchronization is a process to ensure that a person's attributes contained in all the resources managed by the IDM system are synchronized with the most current information. For instance, detecting changes to personal data, such as department codes, on one system and automatically make matching changes on other systems for the same user.
Identity Update		Identity updates happen daily in the form of new identities (e.g. new employees) or modification to existing identities (e.g. Name change). Updating identities in the IDM system is an automated process. Updates come from the authoritative source.
Identity Vault – Source of Record		The authoritative source where person information comes from and integrated with the Identity Management System. An identity vault contains person records consisting of attributes.
Identity, Credentialing and Access Management	ICAM	A Federal Standard; Identity, Credential, and Access Management Architecture ICAM represents the intersection of digital identities (and associated attributes), credentials, and access control into one comprehensive approach.
Information Technology Infrastructure Library	ITIL	A set of practices for IT service management (ITSM) that focuses on aligning IT services with the needs of business. In its current form (known as ITIL 2011 edition), ITIL is published as a series of five core volumes, each of which covers a different ITSM lifecycle stage. Although ITIL underpins ISO/IEC 20000 (previously BS15000), the International Service Management Standard for IT service management, the two frameworks do have some differences
Initiative for Open Authentication	OATH	An industry-wide collaboration to develop an open reference architecture using open standards to promote the adoption of strong authentication.
Integration with Source of Record		This is the process of connecting the identity management system to the source of record – directly or indirectly using component interfaces, or connecting to an externalized database for a more secure connection and preserving the integrity of the source of record.

Term	Acronyms	Definition
Interactive Voice Response	IVR	is a technology that allows a computer to interact with humans through the use of voice and DTMF tones input via keypad.
Internet Protocol Security	IPSec	Protocol suite for securing Internet Protocol (IP) communications by authenticating and encrypting each IP packet of a communication session.
Internet Protocol Services	IPS	Network services providing internet access.
Jump Server		A jump server is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them. User access is tightly controlled and monitored.
Knowledge Based Authentication	KBA	Commonly referred to as KBA, is a method of authentication which seeks to prove the identity of someone accessing a service, such as a website. As the name suggests, KBA requires the knowledge of personal information of the individual to grant access to the protected material. There are two types of KBA: "static KBA", which is based on a pre-agreed set of "shared secrets"; and "dynamic KBA", which is based on questions generated from a wider base of personal information.
Managed Resources		From the IDM system's perspective, these are systems (e.g. Active Directory, Badge, iOS, Android Devices, LDAP, AS400, Third Party Software, etc.) that are integrated to IDM via connectors and adapters. Each adapter is unique as it contains attributes enabling the IDM system to perform user management functions. To manage resources means that IDM automatically creates, updates, deletes user accounts on these resources.
Marketplace Identities		Identities that are associated only with the customer of an organization.
Medium Assurance Hardware tokens	MAH	A "Medium Token Assurance" certificate is a hardware based certificate, and is stored on a FIPS 140-2 Level 2 or higher cryptographic device (either a Smart Card or a USB device). This is a portable certificate and can be used on any computer where the utilities drivers have been installed. A Medium Token Assurance certificate is a higher assurance level certificate than a software based certificate

Microsoft Active Directory	AD	Repository storing user identity, group membership, resource information and first factor username and passwords.
Multi-Factor Authentication	MFA	A method of computer access control which a user can pass by successfully presenting authentication factors from at least two of the three categories: 1) knowledge factors ("things only the user knows"), such as passwords 2) possession factors ("things only the user has"), such as ATM cards 3) inherence factors ("things only the user is"), such as biometrics Requiring more than one independent factor increases the difficulty of providing false credentials.
National Institute of Standards and Technology	NIST	A non-regulatory agency of the United States Department of Commerce, one of the institute's official missions is to establish and promote U.S. standards around Information Security.
One-time password	OTP	Password that is valid for only one login session or transaction, on a computer system or other digital device. OTPs avoid a number of shortcomings that are associated with traditional (static) password based authentication; a number of implementations also incorporate two factor authentication by ensuring that the one-time password requires access to something a person has (such as a small keyring fob device with the OTP calculator built into it, or a smartcard or specific cellphone) as well as something a person knows.
Online certificate status protocol	OCSP	An Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 6960 and is on the Internet standards track.

Term	Acronyms	Definition
Open standard to Authentication	OAuth	OAuth is an open standard to authorization. OAuth provides client applications 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, or end-user. The client then uses the access token to access the protected resources hosted by the resource server. OAuth is commonly used as a way for web surfers to log into third party web sites using their Google, Facebook or Twitter accounts, without worrying about their access credentials being compromised.
Open Web Application Security Project	OWASP	Online association for Web Application Security.
Password Self-Service		Password self-service is a service that allows the end-user to reset his/her own password without the assistance of the help desk. It usually entails setting up security challenge questions for the verification process to ensure that the person resetting his/her password is authentic.
Password Vault		A secure repository for storing and accessing credentials, including passwords.

Term	Acronyms	Definition
Passwordless U2F, UAF, UX		Passwordless authentication is a method supported by the Universal Authentication Framework (UAF) protocol. In this experience, the user registers their device to the online service by selecting a local authentication mechanism such as swiping a finger, looking at the camera, speaking into the mic, entering a PIN, etc. The UAF protocol allows the service to select which mechanisms are presented to the user. Once registered, the user simply repeats the local authentication action whenever they need to authenticate to the service. The user no longer needs to enter their password when authenticating from that device. UAF also allows experiences that combine multiple authentication mechanisms such as fingerprint + PIN. Universal Second Factor (U2F) protocol allows online services to augment the security of their existing password infrastructure by adding a strong second factor to user login.
Physical Security Integration		Within the context of FV, the thought process here is to integrate the provisioning of the badge system with the identity management system
Privilege		Authorization to access a more secured resource.
Privileged User Management		It is both restricting and protecting high privileged accounts while also restricting and protecting local accounts with administrative privileges. It is about gaining visibility into everything that privileged users are doing on the systems across the environment.
Process Engineering		Within the context of identity, governance, and access, process engineering is an evaluation of the current processes that includes provisioning, de-provisioning, assigning access rights to privileged users, etc.
Provisioning		The process of creating a profile for an entity, that grants access to a set of pre-determined resources.
Provisioning and De-provisioning Workflows		Workflows are automated provisioning or de-provisioning set of processes that may include approval requests. Once the approval is fulfilled, the workflow continues to execute to completion.

Term	Acronyms	Definition
Provisioning of Addition Applications		Provisioning applications means integrating the application with IDM so that account creations, account updates, and account deletions can be automated. Once the application is integrated with IDM, the application is called a “managed resource.”
Proxy-based PeP		Proxy-based PeP, a reverse proxy server front-ends any number of Web servers and application servers.
Public Key Infrastructure	PKI	A set of hardware, software, people, policies, and procedures needed to create, manage, distribute, use, store, and revoke digital certificates.
Recertification		Recertification is a way to ensure that the end-user’s entitlements are current and based on the end-user’s role. For instance, if the end-user no longer needs access to a particular resource because of a role change, then the entitlement needs to be modified. Recertification can be a workflow that automatically executes when a person’s role changes. Recertification or attestation help the organization gain better transparency and enforce better access control.
Reconciliation		Reconciliation is a process of synchronizing a person’s accounts between what is known to IDM and the managed resources. Reconciliations ensure that the information in the IDM user registry is accurate.
Registration Authority System	RAS	An authority in a network that verifies user requests for a digital certificate and tells the certificate authority (CA) to issue it.
Remote Authentication Dial In User Service	Radius	A networking protocol that provides centralized Authentication, Authorization, and Accounting (AAA) management for users who connect and use a network service. RADIUS was developed by Livingston Enterprises, Inc. in 1991 as an access server authentication and accounting protocol and later brought into the Internet Engineering Task Force (IETF) standards.
Reporting		One of the many types of information that reports can provide is information about the end-user’s access rights for services that IDM has provisioned to this end-user. Reporting can also provided information about how many user accounts were created on a given day. IDM manages.
Role		Users are grouped by job functions so a single role can define access for all users who perform a function.

Term	Acronyms	Definition
Role Engineering		The process of discovering, and designing roles from the list of entitlements.
Role Lifecycle Management		Roles and role assignment are dynamic. As a result, the entitlements associated with a role must be reviewed and updated and the users assigned the role, implicitly or explicitly, must be reviewed and changed. The business processes used to effect these reviews and changes are collectively referred to as role lifecycle management.
Role-Based Access Control	RBAC	Granting access based on roles.
Secure Shell	SSH	Cryptographic network protocol for secure data communication, remote command-line login, remote command execution, and other secure network services between two networked computers. It connects, via a secure channel over an insecure network, a server and a client running SSH server and SSH client programs, respectively. The protocol specification distinguishes between two major versions that are referred to as SSH-1 and SSH-2.
Secure Socket Layer	SSL	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communication security over the Internet. They use X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom they are communicating, and to exchange a symmetric key. This session key is then used to encrypt data flowing between the parties. This allows for data/message confidentiality, and message authentication codes for message integrity and as a by-product, message authentication.
Security Assertion Markup Language (AM)	SAML	An XML-based, open-standard data format for exchanging authentication and authorization data between parties, in particular, between an identity provider and a service provider.
Services		From an end-user's perspective services represent resources that IDM manages and provisions to users. A properly configured end-user will have many services provisioned (e.g. Active Directory, LDAP, Exchange, Linux, HR Self Service, etc.).
Session Management		Method to manage the semi-permanent interchange of information between two connected systems.

Term	Acronyms	Definition
Short Message Service	SMS	Text messaging service component of phone, Web, or mobile communication systems. It uses standardized communications protocols to allow fixed line or mobile phone devices to exchange short text messages.
Simple Object Access Protocol (Access Management)	SOAP	A protocol specification for exchanging structured information in the implementation of web services in computer networks. It uses XML Information Set for its message format, and relies on other application layer protocols, most notably Hypertext Transfer Protocol (HTTP) or Simple Mail Transfer Protocol (SMTP), for message negotiation and transmission.
Single Sign-On	SSO	Property of access control of multiple related, but independent software systems. With this property a user logs in once and gains access to all systems without being prompted to log in again at each of them. This is typically accomplished using the Lightweight Directory Access Protocol (LDAP) and stored LDAP databases on servers. A simple version of single sign-on can be achieved using cookies but only if the sites are on the same domain.
Social Identities		Allowing the people with social identities (Google, Facebook, Twitter) to use FV resources using their own social identity.
Temporary Workforce Provisioning		Process to provision temporary. The thought process here is to ensure that temporary workforce have unique attributes and birth right resources as compared to permanent workforce.
The Open Group Architecture Framework	TOGAF	A framework for enterprise architecture which provides an approach for designing, planning, implementing, and governing an enterprise information technology architecture. TOGAF is a high level approach to design. It is typically modeled at four levels: Business, Application, Data, and Technology. It relies heavily on modularization, standardization, and already existing, proven technologies and products.
Token		Credentials are protected using a security token, thus typically offering multi-factor authentication by combining "something the user has" (smart card or USB stick) , "something the user knows" (PIN or password) and/or "something the user is" (biometrics - such as a fingerprint, hand, retina, or face scanner).

Term	Acronyms	Definition
Transport Layer Service	TLS	Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), are cryptographic protocols designed to provide communication security over the Internet. They use X.509 certificates and hence asymmetric cryptography to authenticate the counterparty with whom they are communicating, and to exchange a symmetric key. This session key is then used to encrypt data flowing between the parties. This allows for data/message confidentiality, and message authentication codes for message integrity and as a by-product, message authentication.
Trust Services		A collection of APIs that provides compliant devices with additional cryptographic security features. It permits the communication of applications with a smartcard, and it covers the following features, not natively supported by certain platforms: - Secure storage and exchange of data with third parties (such as the data exchanged during payment transactions). - User identification and authentication during the exchange of data with third parties.
Two-Factor Authentication	TFA	Provides unambiguous identification of users by means of the combination of two different components. These components may be something that the user knows, something that the user possesses or something that is inseparable from the user. A good example from everyday life is the withdrawing of money from a cash machine. Only the correct combination of a bank card (something that the user possesses) and a PIN (personal identification number, i.e. something that the user knows) allows the transaction to be carried out. Two-factor authentication is type of multi-factor authentication.
User Access Review		An intentional review of user access to various resources, typically done periodically, for the purpose of assuring Compliance and maintaining security.

Term	Acronyms	Definition
Web services description Language (AM)	WSDL	An XML-based interface definition language that is used for describing the functionality offered by a web service. The acronym is also used for any specific WSDL description of a web service (also referred to as a WSDL file), which provides a machine-readable description of how the service can be called, what parameters it expects, and what data structures it returns. It thus serves a purpose that corresponds roughly to that of a method signature in a programming language.
Workflows		When a process is refined, repeatable, and effective it can be developed into a workflow. The execution of a workflow requires triggers to initiate the process. Triggers can include on-boarding events, termination events, organizational changes, role assignments, or group assignments. The creation of a workflow results to automated provisioning or de-provisioning.