Identity Management

What is Identity Management?

Identity Management (IdM) is the framework for policies and technologies that ensure the management of digital identities. It is a key component of an organization's security architecture. The goal is to keep internal systems and data secure by managing individual network entities (users and devices) access to internal technical resources. This includes the management of organizational policies and technologies that encompass a company-wide process to properly identify, authenticate, and authorize people, groups of people, or software applications through attributes including user access rights and restrictions based on their identities.

What is an Identity?

A digital identity is a set of validated digital attributes and credentials. It is at the center of identity management. Identities contain information and attributes that define a role, specifically provide or deny access to a given resource, and informs others in the organization who or what that identity belongs to, how to contact them if a person, and where they fit in the overall enterprise structure. Digital identities are not just for people within your organization. Software such as applications or programs and hardware like IoT devices can also have an identity.

Digital identities are based on public key infrastructure (PKI) certificates and stored on smart cards, virtual smart cards on mobile phones or laptops. These digital identities can be used by users (employees, customers, etc.) to log in to Windows with two-factor authentication (2FA), access cloud resources and servers, send encrypted emails and digitally sign documents.

What is an Identity Management System?

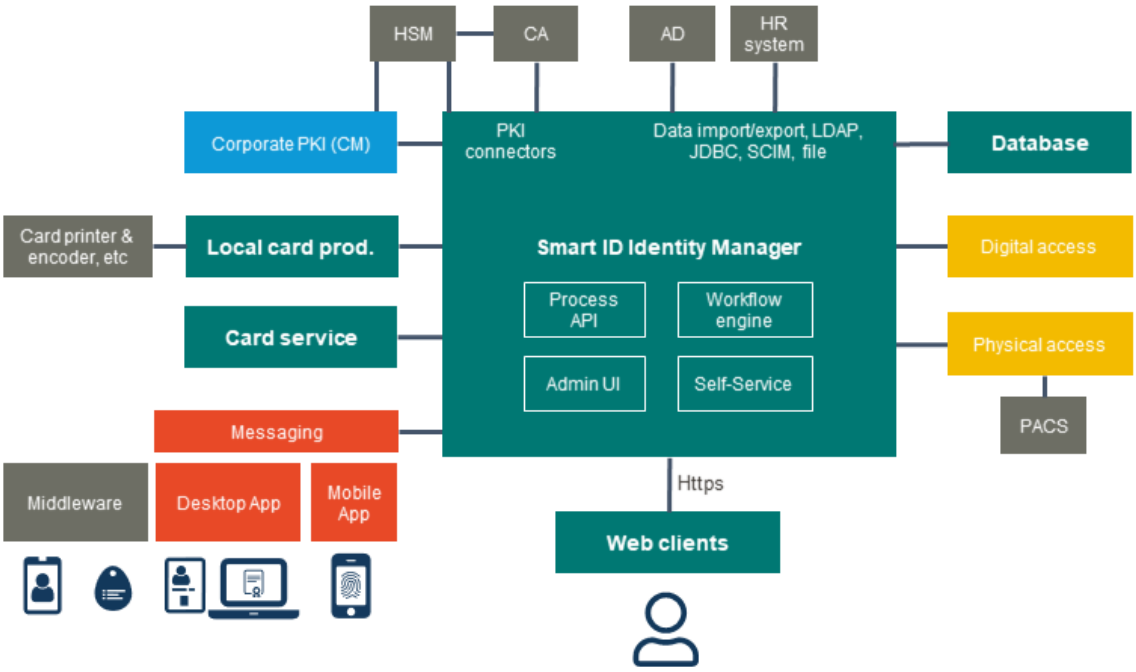
Identities are managed by an Identity Management System. These rather complex tools are designed to streamline and secure the identity management process by integrating various components to make identity management efficient, seamless and secure. IdM systems can be deployed on-premises, provided as a service, or deployed in a hybrid model.

IdM systems provide a central platform for managing identities and integrate with a number of important tools such as device management tools.

Legacy systems are often built up of many vendors' separate solutions, such as one or several smart cards, middleware, mini drivers, a card management system and various certificate authorities (CAs).

Modern systems should integrate seamlessly with different systems, allow for the lifecycle of all digital identities to be managed in one system, offer easy approval steps to ensure authorized identity issuance, offer best practices, self-service features and automated processes.

(Figure1: Nexus Smart ID Identity Manager architecture. Smart ID Identity Manager enables organizations to manage the lifecycle of identities for physical and digital access with self-service and automation.)



Nexus' identity management solution

Benefits of identity management

The IdM system is a perfect way to achieve a balance between high security and a good user experience. This is based on the ability to simplify or automate administration processes which help to improve business productivity while reducing costs, downtime and time-consuming tasks.

Organizations can benefit from functions such as Self-Service as it allows users to use their existing credentials to request additional credentials for a mobile device or virtual

smartcard. The Self-service function keeps administrative tasks to a minimum, even if the number of credentials and devices are increased.

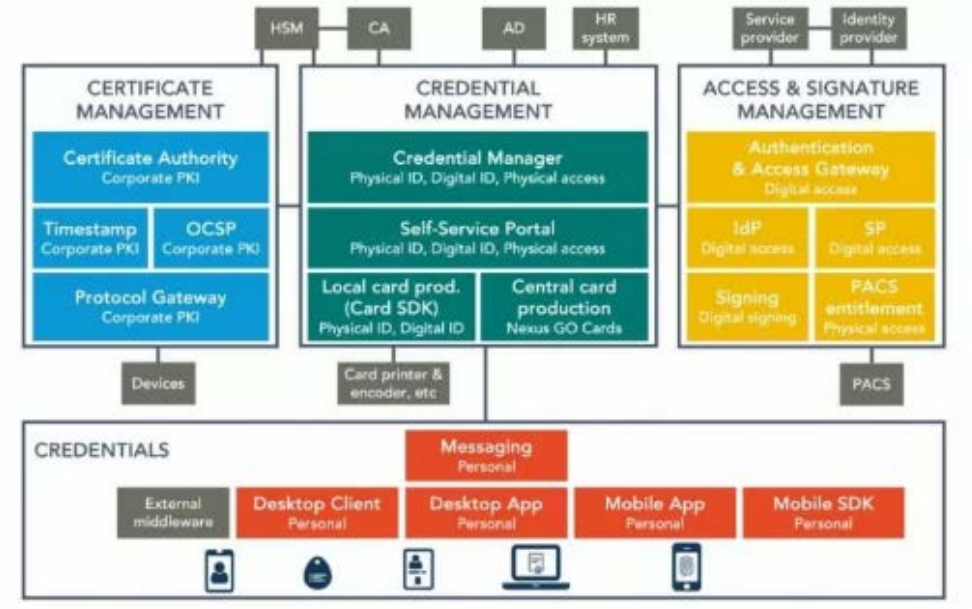
Lastly, modern business environments are no longer locked in the four walls of an office. Between working remotely and using multiple devices to access resources the requirements for security put on IT departments is steadily increasing. IdM is crucial in ensuring all company networks, system applications and internal resources are not only protected but accessible for necessary company users. Without a system, this would be an extremely complex and time-consuming process.

Identity Management (IdM) vs Identity and Access Management (IAM)

IdM and IAM are often used interchangeably, however, identity management is more focused on user identity, and the roles, permissions, and groups that user belongs to. IdM also focuses on protecting identities through a variety of technologies such as passwords, biometrics, multi-factor authentication, and other digital identities. This is usually achieved by the adoption of identity management software applications and platforms. Alternatively, Access Management is the authentication of an identity that is asking for access to a particular resource, and access decisions are simply the yes or no decision to grant that access.

In short, Identity Management focused on the authentication portion while access management covers authorization. Each is an important layer within enterprise security processes.

(Figure2: Nexus Smart ID is an identity and security platform that consists of standardized and easy-to-use modules.)



Summary

Identity Management aligns with the organization's transitioning from firewalls to zero trust security models and with the security requirements of IoT. This is due to its strong control of resource access, especially in highly distributed and dynamic environments. IdM is a critical component within IT security and a solid identity management strategy establishes the first line of protection for your organization's networks and resources.

Watch a video at

https://youtu.be/Tcvsefz5DmA?feature=shared