6.2.3 Authentication Facts

This lesson covers the following topics:

- Authentication
- Identity
- Authentication methods

Authentication

To access resources on a network, you must prove who you are and that you have the required permissions. This process consists of the following elements:

- *Identification* is the initial process of confirming your identity when you request credentials. It occurs when you enter a userid to log on. Identity proofing occurs during the identification phase as you prove that you are who you say you are in order to obtain credentials. If you have been identified previously but cannot provide the assigned authentication credentials (such as a lost password), identity proofing is called upon again.
- *Authentication* is the verification of the issued identification credentials. It is usually the second step in the identification process and establishes your identity, ensuring that you are who you say you are.

To verify an identity, you need some unique piece of information or data that could come only from you. Multi-Factor Authentication (MFA) requires more than one method of identification and uses factors and attributes. The following is a description of each type of factor:

Factor	Description
Something you know	Something you know authentication requires you to provide a password or some other data that you know. This is the weakest type of authentication, but also the most commonly used. Examples of something you know authentication controls are: ▪ Passwords, codes, or IDs. ▪ PINs. ▪ Passphrases (long, sentence-length passwords). ▪ Cognitive information, such as questions that only you can answer, such as mother's maiden name, the model of your first car, or the city where you were born. ▪ Composition passwords are created by the system and are usually two or more unrelated words divided by symbols on the keyboard. Usernames are not a form of something you know authentication. Usernames are often easy to discover or guess. Only the passwords or other information associated with the usernames can be used to validate identity. To be safe, the same password should not be used for more than one application or website.
Something you have	Something you have, also called token-based authentication, bases authentication on something physical you have in your possession. Examples of something you have authentication controls include: ▪ Swipe cards (similar to credit cards) with authentication information stored on the magnetic strip. ▪ Photo IDs are very useful when combined with other forms of authentication, but are high-risk if they are the only form of required authentication. Photo IDs are easily

	manipulated or reproduced, require personnel for verification, and cannot be verified against a system.
	▪ Key fobs are small, programmable hardware often used to provide access to buildings and open doors. Key fobs are often attached to a keychain.
	▪ Security tokens generate a unique password when activated manually. These passwords are used one time and usually expire in minutes. Types of token-based authentication include:
	  ▪ A static password that is saved on the token device. Swiping the token supplies the password for authentication.
	  ▪ Synchronous dynamic password systems that generate new passwords at specific intervals on the hardware token. You must read the generated password and enter it along with the PIN to gain access.
	  ▪ An asynchronous dynamic password system that generates new passwords based on an event, such as pressing a key.
	  ▪ A challenge response system that generates a random challenge string. The challenge text is entered into the token, along with the PIN. The token then uses both to generate a response used for authentication.
	▪ Smart cards contain a memory chip with encrypted authentication information. Smart cards can:
	  ▪ Require contact such as swiping, or they can be contactless.
	  ▪ Contain microprocessor chips with the ability to add, delete, and manipulate data.
	  ▪ Store digital signatures, cryptography keys, and identification codes.
	  ▪ Use a private key for authentication to log a user into a network. The private key is used to digitally sign messages.
	  ▪ Be based on challenge response. You are given a code (the challenge) which you enter into the smart card. The smart card then displays a new code (the response) that you can present to log in.
	▪ Smart cards typically use certificates for identification and authentication. With certificates, the digital document is associated with a user in one of the following ways:
	  ▪ With a one-to-one mapping, each certificate maps to an individual user account (each user has a unique certificate).
	  ▪ With many-to-one mapping, a certificate maps to many user accounts (a group of users share the same certificate).

Something you are	Something you are authentication uses a biometric system. A biometric system attempts to identify you based on metrics or a mathematical representation of a biological attribute, such as eye or fingerprint. This is the most expensive and least accepted but is generally considered to be the most secure form of authentication.

Attributes are different from factors because they do not, on their own, verify your identity. However, they do help to improve security and work well when Multi-Factor Authentication is needed. The following table describes each type of attribute:

Attribute	Description
Something you can do	This requires you to perform a particular action to verify your identity. Here are a few examples of an action that can be used: ▪ Supply a handwritten sample that's analyzed against a baseline sample for authentication. ▪ Type sample text. Your typing behaviors are analyzed against a baseline before authentication.

Something you exhibit	Something that you exhibit could include a personality trait or a habit. For example: ▪ The time of day you usually log on. ▪ The method you usually use to access information. ▪ The types of tasks you usually perform. When administrators notice unusual or risky behavior, they may choose to restrict access. This could mean requiring a password change, requiring another method of authentication, or even blocking your access.
Somewhere you are	Somewhere you are (also known as geolocation) uses physical location to verify your identity. Examples of implementations include: ▪ A desktop system configured to allow authentication requests only if you have passed through the building's entrance using your ID card. If your are not in the building, your account is locked. ▪ A system configured with an RFID proximity reader and required RFID badges. If you are within the RFID range of the workstation, authentication requests are allowed. If you move out of range, the workstation is immediately locked and re-authentication is not allowed until you move back within range. ▪ GPS location data is used to determine a device's location. If you and the device are in a specified location, authentication requests are allowed. If not, the device is locked or additional authentication factors are requested. ▪ Wi-Fi triangulation is used to determine a device's location. If you and the device are in a specified location, authentication requests are allowed. If not, the device is locked, or additional authentication factors are requested.
Someone you know	Having someone who can vouch for you can go a long way in establishing relationships and building trust. The same is true with authentication. Certificates and attestation are examples of this attribute.

Identity

Identity is as simple as telling someone your name. In the computer world, a username is a form of identification. Because anyone could pretend to be you, identification alone is not very secure. To substantiate your identity, you need to provide some type of verification that you are who you say you are. The following chart provides a few of the basics of identity authentication.

Term	Description
Identity Provider (IdP)	An identity provider is an online service that manages identity information for other organizations. The IdP creates records from an organization’s existing data and policies. These records are used to authenticate user requests.
Attributes	Attributes can be your role, position, or current project. This information can be used to determine policy and permission.
Certificates	Certificates are issued by a certificate authority and verify identity by providing the following: ▪ Public keys ▪ Details on the owner of the certificate ▪ Details on the issuer of the certificate

Tokens	A token is a device or a file used to authenticate. A hardware token, such as a key fob, serves as something you have. A software token, also known as a soft token, is stored in devices such as laptops, desktops, or mobile phones. These tokens are specific to the device, and cannot be altered or duplicated.
SSH Keys	A secure shell (SSH) key is an access credential. It operates like usernames and passwords but is mostly used to implement single sign-on and other automated processes.

Authentication Methods

The following table describes authentication methods.

Method	Description
Directory Services	Directory services implement single sign-on for resources on the network. Examples are: ▪ Active Directory on a Microsoft network ▪ LDAP Directory Services ▪ Azure Active Directory is an identity and access management solution for the cloud Single sign-on can be implemented between directory services of different systems. For example, single sign-on can be implemented if the directory services are compatible, such as Microsoft and Linux systems. In this case, logging into a Linux system would authenticate you to access resources on the Microsoft network that you have permissions to access. Directory services users sign on using a domain user account and password to gain access to resources available on the domain.
Federation	A federation is a group of domains that have established trust and therefore shared authorizations. A federation can be within one organization with multiple domains or it can include several trusted organizations to share resources. The good thing about this method of authentication is that everything happens onsite and provides detailed levels of access control.
Attestation	Attestation is a protocol that is used to prove that software can be trusted. It tells the remote user that the application or OS software is legitimate and has been certified. Attestation can work both ways. Say you were going to log into your bank account. You want to be sure that the site you are logging into is trustworthy and the bank wants to be sure that the correct individual is logging into the account.