8.2.3 Authentication Facts

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

- *Identification* is the initial process of confirming the identity of a user requesting credentials and occurs when a user types in a user ID to log on. *Identity proofing* occurs during the identification phase as the user proves that they are who they say they are in order to obtain credentials. If a person has been identified previously but cannot provide their assigned authentication credentials (such as a lost password), then 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 the user's identity, ensuring that users are who they say they are.

The five ways a user can prove identity to an authentication server are explained in the following table:

Type	Description

Type 1: 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 the user can answer, including:
	  - Your mother's maiden name
	  - The model or color of your first car
	  - The city where you were born
	- Composition passwords, which are created by the system and are usually two or more unrelated words divided by symbols on the keyboard.
	- One-time passwords, which are only valid for a single use. There are two main types of one-time passwords:
	  - HMAC-based one-time passwords (HOTP) use a mathematical algorithm to generate a new password based on the previous password that was generated. This algorithm relies on two basic tools: a shared secret and a counter. An HMAC-SHA1 hash of the counter that is generated using the shared secret. Whenever a new OTP is generated, the counter is incremented, which causes each new password generated to be different from all previous passwords.
	  - Time-based one-time passwords (TOTP) are based on time synchronization between the client providing the password and the authentication server. The TOTP algorithm works in a manner similar to HOTP, relying on a shared secret and a counter. However, in the case of TOTP, the counter constantly increments based on the passing of time. An HMAC-SHA1 hash of the counter is generated using the shared secret. Because the counter is constantly incremented, each new password generated is different from all previous passwords.
	
	User names are not a form of something you know authentication. User names are often easy to discover or guess. Only the passwords or other information associated with the user names can be used to validate identity. To be safe, the same password should not be used for more than one application or website.

Type 2: Something You Have	*Something you have* (also called token-based authentication) is authentication based on something physical a user has in their 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, which 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, which are small, programmable hardware often used to provide access to buildings and open doors. Key fobs are often attached to a keychain.
	- Security tokens, which generate a unique password when activated manually. These passwords are used one time and usually expire in minutes.
	- 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.
	  - Can store digital signatures, cryptography keys, and identification codes.
	  - Use a private key for authentication to log a user into a network. The private key will be used to digitally sign messages.
	  - Be based on challenge response. A user is given a code (the challenge) which he or she enters into the smart card. The smart card then displays a new code (the response) that the user can present to log in.
	
	Types of token-based authentication include:
	- A static password, which is saved on the token device. Swiping the token supplies the password for authentication.
	- A synchronous dynamic password, which generates new passwords at specific intervals on the hardware token. Users must read the generated password and enter it along with the PIN to gain access.
	- An asynchronous dynamic password generates new passwords based on an event, such as pressing a key.

	▪ A challenge-response password 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 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). Digital certificates require the implementation of a PKI, which have high administrative overhead.

Type 3: Something You Are	*Something you are* authentication uses a biometric system. A biometric system attempts to identify a person based on *metrics* or a mathematical representation of the subject's biological attribute. This is the most expensive and least accepted, but is generally considered to be the most secure form of authentication.
	
	Common attributes used for biometric systems are:
	
	▪ Fingerprints (end-point and bifurcation pattern)
	▪ Hand topology (side view) or geometry (top-down view)
	▪ Palm scans (pattern, including fingerprints)
	▪ Retina scans (blood vein pattern)
	▪ Iris scans (color)
	▪ Facial scans (pattern)
	▪ Voice recognition
	▪ Handwriting dynamics
	▪ Keyboard or keystroke dynamics (behavioral biometric systems)
	  ▪ Dwell time (key press time)
	  ▪ Flight time (how fingers move from key to key)
	
	When implementing a biometric system, the attribute that is used for authentication must meet the following criteria:
	
	▪ *Universality* means that all individuals possess the attribute.
	▪ *Uniqueness* means that the attribute is different for each individual.
	▪ *Permanence* means that the attribute always exists and will not change over time.
	▪ *Collectability* ensures that the attribute can be measured easily.
	▪ *Performance* means that the attribute can be accurately and quickly collected.
	▪ *Circumvention* allows for acceptable substitutes for the attribute in case the original attribute is missing or can't be read.
	▪ *Acceptability* identifies the degree to which the technology is accepted by users and management.
	
	Biometric systems include multiple scans of the biological attribute. Scans are then translated into a numeric constellation map of critical points. That mathematical representation is bound to a digital certificate that links to the subject's user account in the user database. Most biometric systems require implementation of a PKI system.

Type 4: Somewhere You Are	*Somewhere you are* (also known as geolocation) is a supplementary authentication factor that uses physical location to verify a user's identity. Examples of implementations include: ▪ A desktop system that is configured to allow authentication requests only if the user has passed through the building's entrance using their ID card. If the user is not in the building, the user's account is locked. ▪ A desktop system that is configured with an RFID proximity reader and a user that carries a corresponding RFID badge. If the user is within RFID range of the workstation, authentication requests are allowed. If the user moves out of range, the workstation is immediately locked and re-authentication is not allowed until the user moves back within range. ▪ GPS location data that is used to determine a device's location. If the user and the device are in a specified location, authentication requests are allowed. If not, the device is locked. ▪ Wi-Fi triangulation that is used to determine a device's location. If the user and the device are in a specified location, authentication requests are allowed. If not, the device is locked.
Type 5: Something You Do	*Something you do* is a supplementary authentication factor that requires an action to verify a user's identity. Example implementations include: ▪ Requiring the user to supply a handwriting sample that is analyzed against a baseline sample before allowing authentication. ▪ Requiring the user to type sample text. The user's typing behaviors are analyzed against a baseline sample before allowing authentication.

You should be aware of the following terms used to measure the effectiveness of authentication solutions:

Measure	Description
False Negative	A false negative (or Type I error) occurs when a person who should be allowed access is denied access. The false rejection rate (FRR) is a measure of the probability that a false negative will occur.

False Positive	A false positive (or Type II error) occurs when a person who should be denied access is allowed access. The False Acceptance Rate (FAR) is a measure of the probability that a false positive will occur. False positives are more serious than false negatives and represent a security breach because unauthorized persons are allowed access.
Crossover Error Rate	The *crossover error rate*, also called the equal error rate, is the point at which the number of false positives matches the number of false negatives in a biometric system. Select the system with the lowest crossover error rate within your budget.
Processing Rate	The *processing rate*, or system throughput, identifies the number of subjects or authentication attempts that can be validated. An acceptable rate is 10 subjects per minute or more.

To increase security, you can use a combination of authentication methods as described in the following table:

Authentication Method	Description	Example
Two-Factor Three-Factor Multi-Factor	Requires two (or more) different authentication types to be deployed.	To enter a secured building, you must insert your key card (Type 2) and undergo a retina scan (Type 3).
Strong	To log in to an online banking system, you enter your user name and password and must answer a random personal question (such as your birthplace or mother's maiden name).	
One-Factor	Uses credentials of only one type, but may require multiple methods within the same type.	To log in, you supply a user name and a password (the user name is not used for authentication, so the only credential supplied for authentication is the password). To log in, you supply a user name, PIN, and a passphrase (all credentials are of the same type).
Mutual	Requires that both parties authenticate with each other before beginning communications.	To log in, your computer sends its digital certificate to prove its identity to a network server. The server then proves its identity to your computer before the computer and server exchange messages.

If you are considering implementing biometrics, keep in mind the following:

- Some biometric factors are unique, even between identical twins.
- When a biometric is used by itself, it is no more secure than a strong password. A single successful attack can subvert a biometric in much the same way that a single successful attack can subvert a password.
- Biometric attacks need not be physical harm-based (such as cutting off a finger), but can include a wide variety of realistic reproductions that fool the biometric reader device.
- The most important consideration for a biometric device is accuracy.
- When a biometric device has its sensitivity set too high, it will result in numerous false negative rejections when authorized users are not recognized.
- To use a biometric, new users must go through a physical enrollment process that is more complex and time-consuming than the enrollment process for a password-only system.
- Biometric enrollment requires the new users to prove their identity to a user administrator. The new user must then provide the first example of their biometric to a reader device under the supervision of the user administrator. This first example is digitized and stored as a reference template. All future uses of the biometric will compare the contemporary biometric sample offered to the historical recorded template.
