8.2 Authentication

As you study this section, answer the following questions:

- What is the difference between authentication and identification?
- Which authentication type is the most common?
- What are some characteristics of the "something you are" authentication type?
- What are some characteristics of the "something you have" authentication type?
- What are some characteristics of the "something you know" authentication type?
- Which form of authentication is generally considered the strongest?
- What is the difference between synchronous and asynchronous token devices?
- Which type of biometric processing error is more serious, a false positive or a false negative? Why?
- What is the difference between strong authentication, two-factor authentication, and multi-factor authentication?
- What are the main advantages of SSO authentication? Disadvantages?
- What are examples of authentication services beside SSO?

In this section, you will learn to:

- Use a biometric scanner
- Use single sign-on

Key terms for this section include the following:

Term	Definition
Identification	The initial process of confirming the identity of a user requesting credentials, which occurs when a user types in a user ID at logon.
Authentication	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.
Multifactor Authentication	A method of confirming identity by using two or more pieces of evidence (or factors) to an authentication mechanism.
False Negative	An error that occurs when a person who should be allowed access is denied access.
False Positive	An error that occurs when a person who should be denied access is allowed access.
Crossover Error Rate	The point at which the number of false positives matches the number of false negatives in a biometric system.
Processing Rate	The number of subjects or authentication attempts that can be validated.
Single Sign-On (SSO) Authentication	A distributed access method that allows a subject to log in (sign on) to a network once and access all authorized resources on the network.
Kerberos	A network protocol that uses secret-key cryptography to authenticate client-server applications.
Secure European System for Applications in a Multi-Vendor Environment (SESAME)	An SSO technology that uses asymmetric cryptography.
Directory Services	A customizable information store that functions as a single point from which users can locate resources and services distributed throughout the network and can be used to implement SSO.

This section helps you prepare for the following certification exam objectives:

Exam	Objective
TestOut Security Pro	1.2 Harden Authentication ▪ Implement centralized authentication

CompTIA Security+	4.1 Compare and contrast identity and access management concepts
	▪ Multifactor authentication
	  ▪ Something you are
	  ▪ Something you have
	  ▪ Something you know
	  ▪ Somewhere you are
	  ▪ Something you do
	▪ Single sign-on
	4.3 Given a scenario, implement identity and access management controls
	▪ Biometric factors
	  ▪ Fingerprint scanner
	  ▪ Retinal scanner
	  ▪ Iris scanner
	  ▪ Voice recognition
	  ▪ Facial recognition
	  ▪ False acceptance rate
	  ▪ False rejection rate
	  ▪ Crossover error rate