Authentication Guidance: A Summary

This infographic summarizes some key points from the PCI SSC Authentication Guidance document published in August 2025. Refer to the full Authentication Guidance document for details.

Authentication factors

The table to the right provides examples of authentication factors, their relative strengths, and indicates the type for each authentication factor.

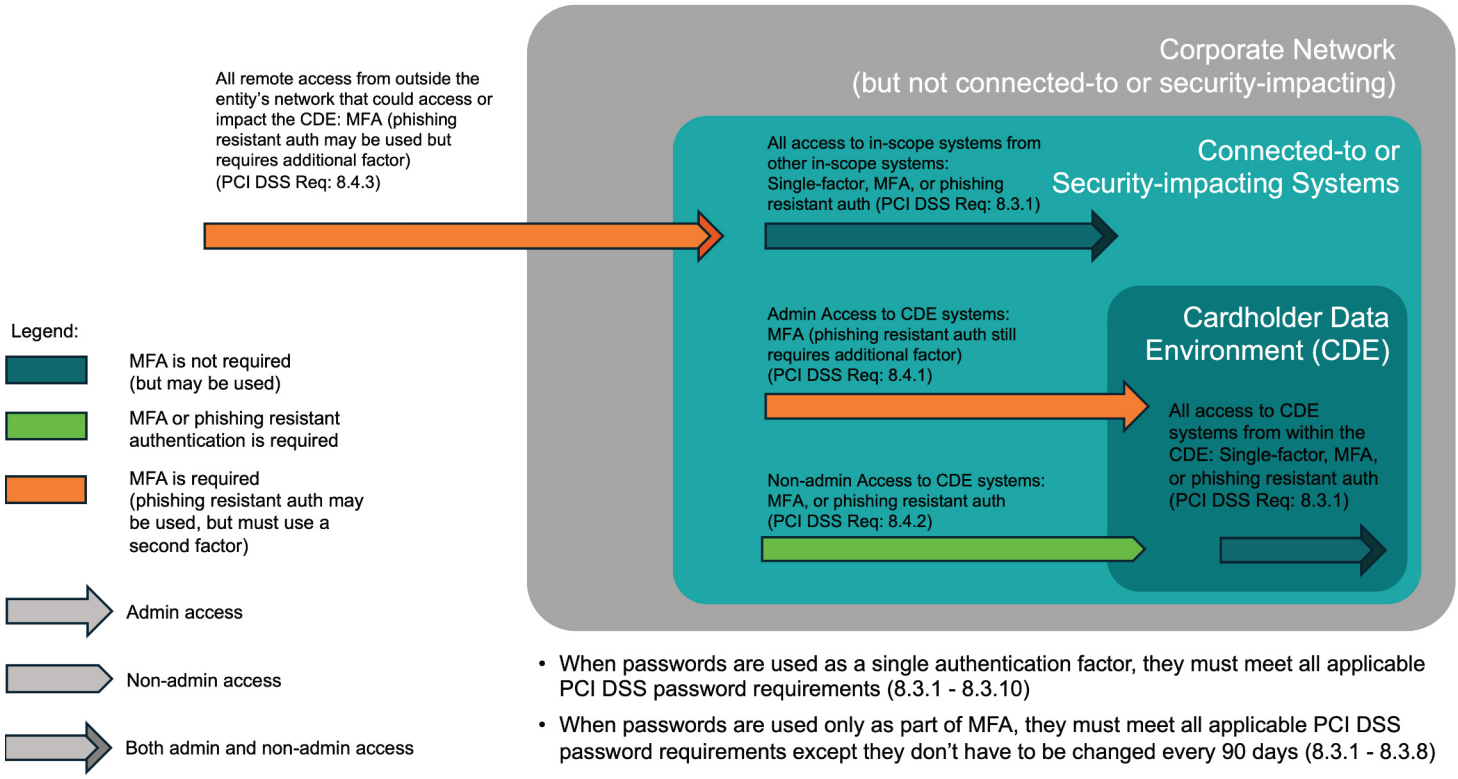
Each item is a single factor. Implementing MFA requires use of two or more factor types from this table, such as coupling a phishing-resistant factor (a possession factor type) with a biometric (an inheritance factor type).

The order of factors within each rank does not imply additional ranking beyond best practice, good practice, and acceptable practice.

Rank	Factor	Factor Type
Best practice	Phishing-resistant authentication	Possession
	Cryptographic challenge / response	Possession
Good practice	Long, randomly generated password	Knowledge
	Locally generated OTP	Possession
	Biometric	Inheritance
Acceptable practice	Remotely generated OTP	Possession
	Out-of-band session token	Possession
	User generated password	Knowledge
	User gesture	Knowledge

PCI DSS v4.x Authentication Requirements

The below illustration shows the PCI DSS MFA requirements and where they apply for PCI DSS environments.



- When passwords are used as a single authentication factor, they must meet all applicable PCI DSS password requirements (8.3.1 - 8.3.10)
- When passwords are used only as part of MFA, they must meet all applicable PCI DSS password requirements except they don't have to be changed every 90 days (8.3.1 - 8.3.8)

Authentication Best Practices

Below are shortened examples of authentication best practices. While these practices are not required, entities are encouraged to consider them when implementing authentication systems.

1. Educate users on how to generate secure passwords.

2. Implement controls to mitigate deepfake attacks.

3. Provide time-limits for OTP use. Let users paste data into password and OTP fields.

4. Store authentication secrets securely.

5. Implement online and offline brute-force protections for credentials.

6. Secure systems that provide access to authentication factors.

7. Consider using more secure authentication factors instead of messaging-based factors.

8. Apply security controls to all locations where credentials exist.

9. Implement phishing-resistant authentication wherever possible.

10. Implement device-bound factors for access to sensitive operations.

11. Limit the business use of synced passkeys.

12. Implement multi-factor authentication wherever possible.

13. Secure the (re)enrollment process to prevent account takeover attacks.

14. Bind session credentials to specific devices or users.

15. Validate all MFA factors first before indicating success/ failure.

16. Include authentication methods when considering acceptable cryptography and crypto agility.

Phishing-Resistant Authentication

Phishing-resistant authentication helps prevent attacks that rely on the transfer of secret data (for example, passwords or one-time-passwords (OTPs)) between the user and the system to which the user is authenticating. Phishing-resistant authentication ensures that secret data is not shared without first validating the authentication system making the request. The figure below shows how it works: