

Definition: A one-time password is valid for only one user authentication.

Implementations: No information available Examples: No examples available

Examples: No examples available

How it works: When a user initiates authentication, they are asked for a one-time password or smart card. The one-time password or smart card to the internet in additional verification, they are asked for a one-time password or smart card. The one-time password or smart card to the internet in additional verification, can adjust for clock skew between the token and the verification system as needed.

Considerations: Compromise of delivery channel, SIM Swapping, Secure token visual compromise of long-term backup codes: These are often provided in the case that the user forgets where they put them. This digital file or printed document could be recovered from the system printer spool unless the spooler cache is cleared.

Definition: Modifying system configuration to increase password strength.

How it works: Password strength guidelines include increasing password length, permitting passwords that contain ASCII or Unicode characters, and requiring systems to screen new passwords against lists of commonly used or compromised passwords.

Considerations: Extremely complex password requirements may lead users to saving passwords in text files or picking obvious passwords that meet the policy.

Implementations: No information available

Device: Rockwell Automation MicroLogix 1400 Controllers Series B EPSS Score: 0.013040000