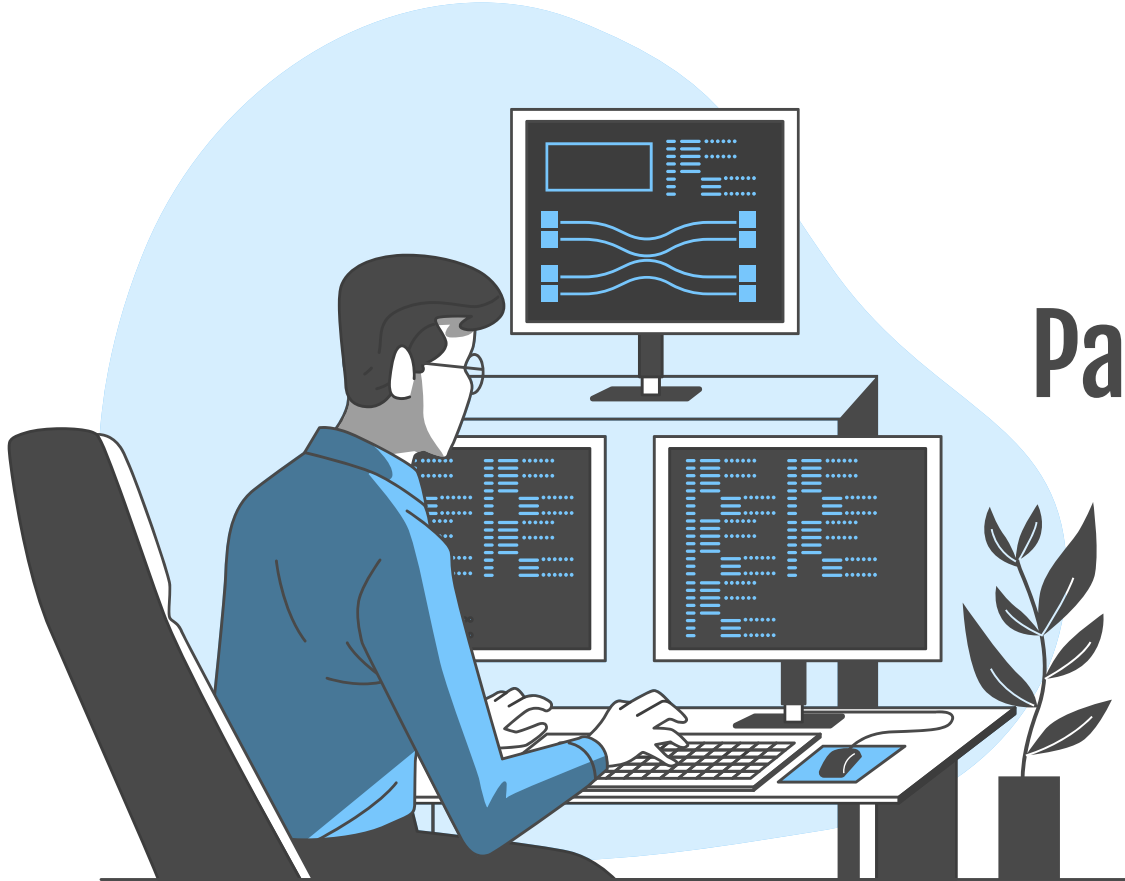




Passwords & MFA

Keeping Bad Actors Out

Julian Smith - Hoover City Schools

01

Definitions

02

Password

Are following best practices? A

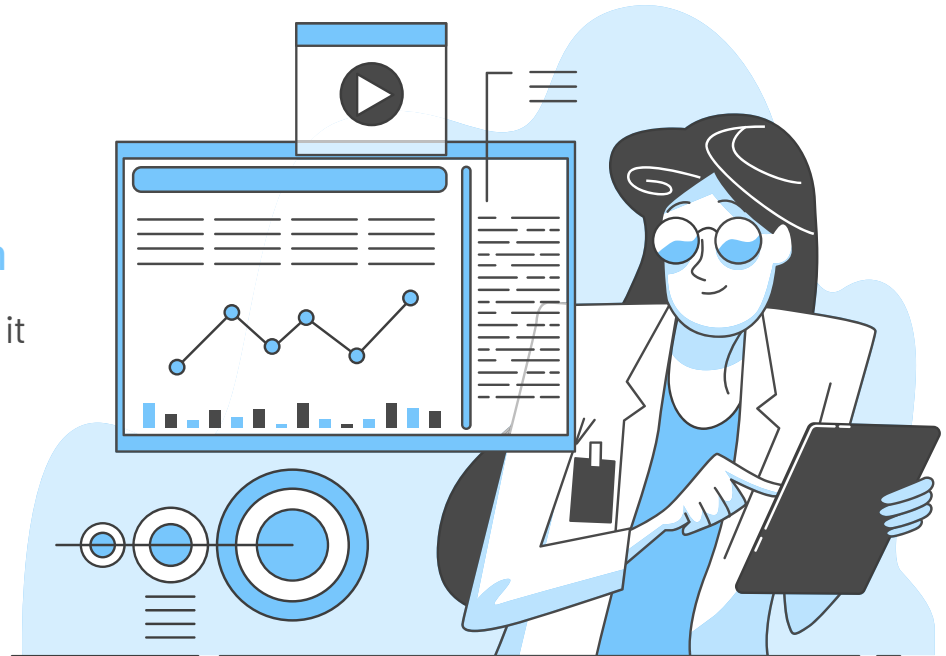
03

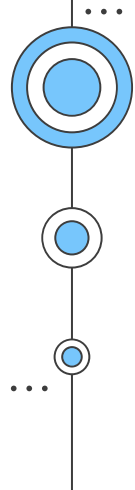
Multi-Factor Authentication

What it is and why you should use it

04

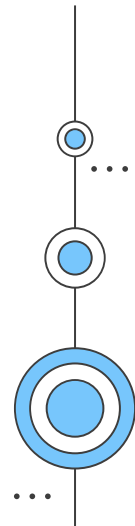
Why Implement MFA?





01

Definitions



01 – Definitions

NIST

National Institute of
Standards and Technology

CSP

Credential Service Provider

Subscriber

A party who has received a
credential or authenticator from a
CSP

01 – Definitions

Claimant

A subject whose identity is to be verified using one or more authentication protocols.

Authenticator Assurance Level (AAL)

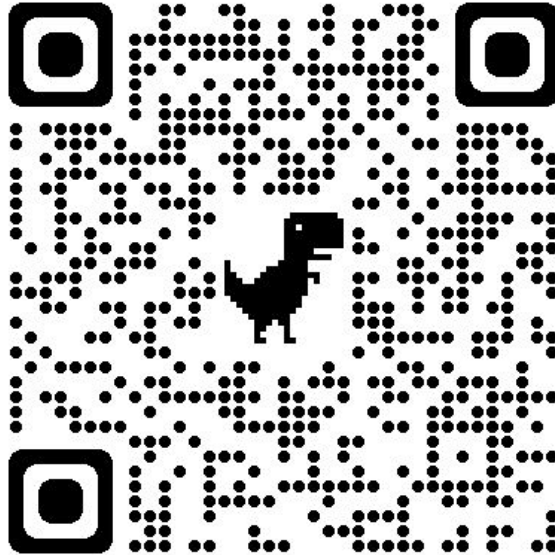
A category describing the strength of the authentication process.

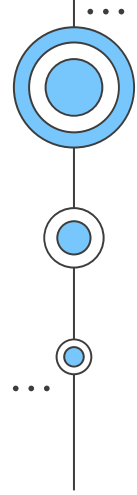
Verifier

An entity that verifies the claimant's identity by verifying the claimant's possession and control of one or two authenticators using an authentication protocol.

NIST 800-63B

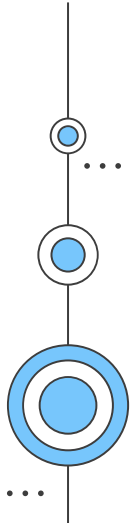
Digital Identity Guides



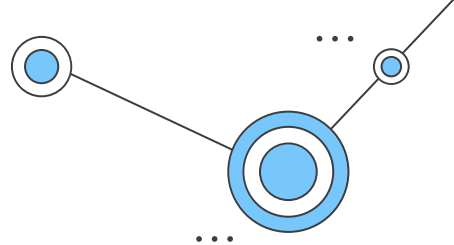


02

Passwords



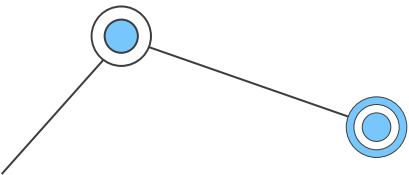
02 – Passwords



Definition from NIST

- A Memorized Secret authenticator – commonly referred to as a **password** or, if numeric, a **PIN** – is a secret value intended to be chosen and memorized by the user. Memorized secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. A memorized secret is **something you know**.

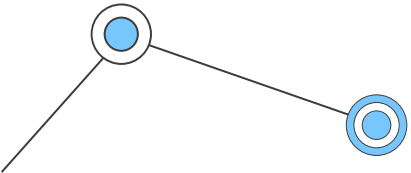
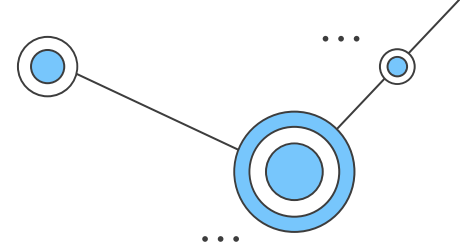
Welcome1



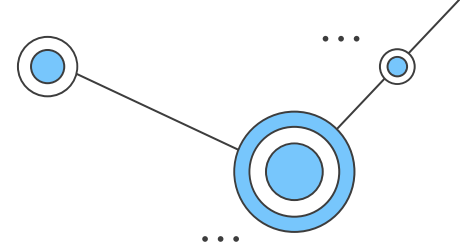
02 – Passwords

Common “best practices” for secure passwords:

- Must be complex
 - 8 character minimum
 - Include letters, numbers, symbols
 - Upper and lower case letters
- Must be changed periodically



02 – Passwords

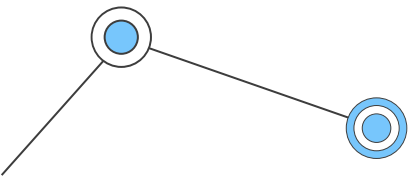


Updated NIST guidance:

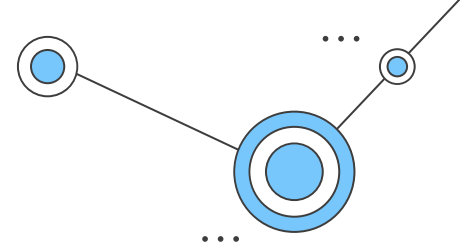
- Password Length > Complexity
- <https://howsecureismypassword.net/>

HOW PASSWORD
LENGTH WINS
THE INTERNET

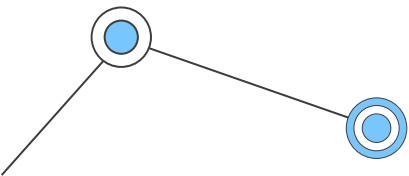
Passwords 102



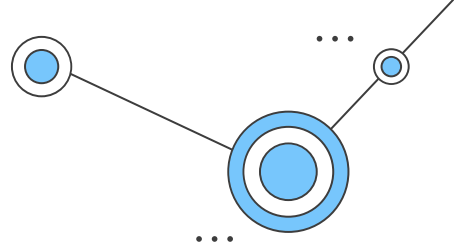
02 – Passwords



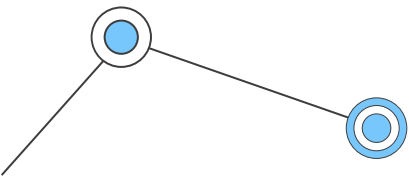
- NIST guidelines require a strict 8 character minimum limit on passwords
- However, additional research shows that requiring new passwords to include a certain amount of complexity can actually make them less secure. And that's why NIST has also removed all password-complexity requirements from their guidelines.



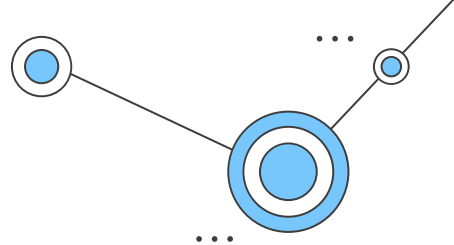
02 – Passwords



- Complexity rules often encouraged password reuse amongst varying systems
- Users would often adhere to complexity rules by capitalizing first letter of password and adding 1 or ! to the end. This allowed for password cracking tools to account for these patterns and reduce the amount of time needed to crack a password



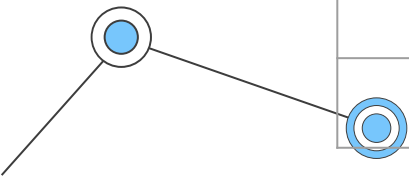
02 – Passwords

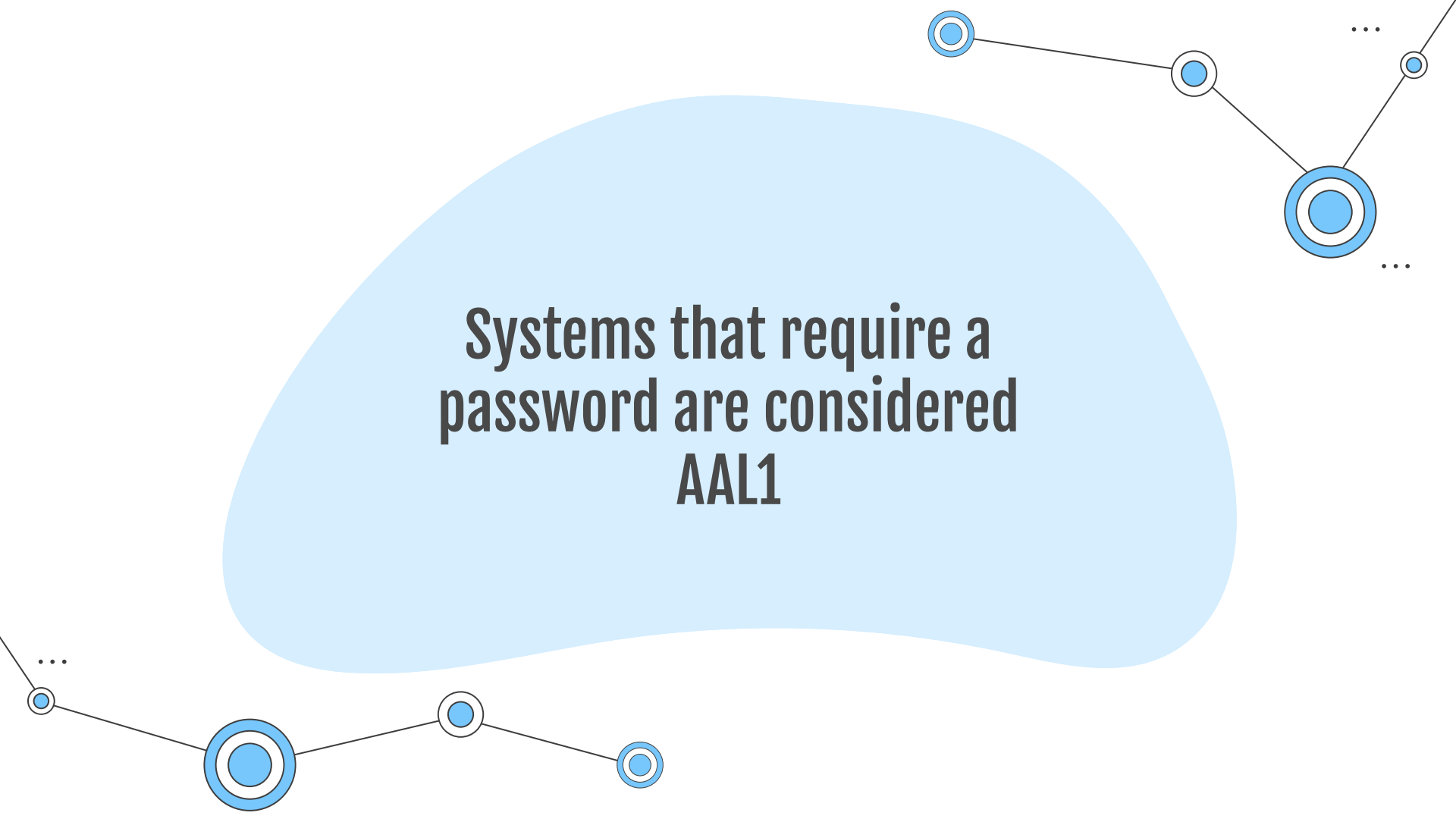


Encourage passphrases in lieu of passwords. A passphrase should easily exceed the 8 character limit and be easier for end users to remember, thus increasing complexity while reducing the need to store the password in plain text digitally or in analog fashion

Example:

ThisIsJulian'sPassword	42 Sextillion Years
I work for hoover cs	8 Quintillion Years
ALET > The Office	23 Trillion Years



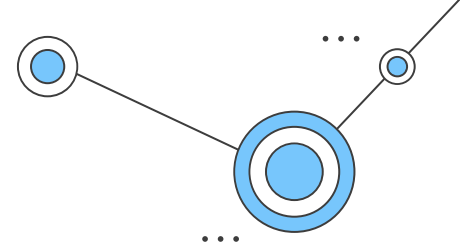


**Systems that require a
password are considered
AAL1**

03

Multi-Factor Authentication

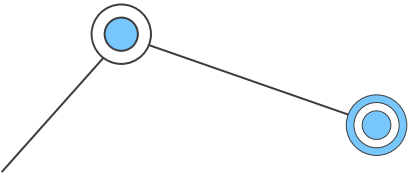
03 – Multi-Factor Authentication



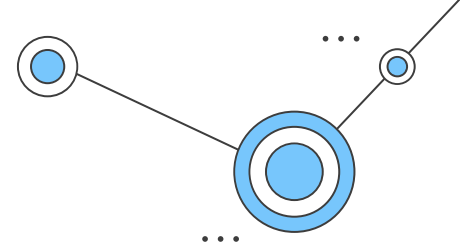
Definition according to NIST:

- A look-up secret authenticator is a physical or electronic record that stores a set of secrets shared between the claimant and the CSP. The claimant uses the authenticator to look up the appropriate secret(s) needed to respond to a prompt from the verifier.

For example, the verifier may ask a claimant to provide a specific subset of the numeric or character strings printed on a card in table format. A common application of look-up secrets is the use of "recovery keys" stored by the subscriber for use in the event another authenticator is lost or malfunctions. A look-up secret is ***something you have***.

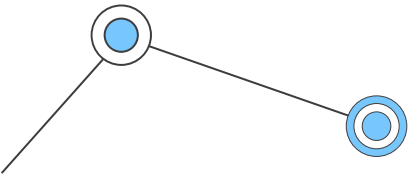


03 – Multi-Factor Authentication

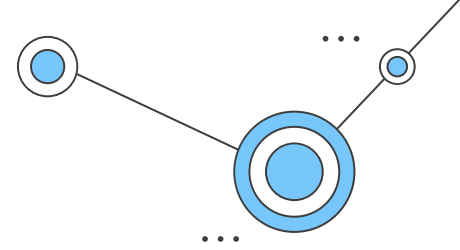


Guidelines from NIST:

- CSPs must use an approved random bit generator to generate a list of secrets and must deliver the authenticator to the subscriber securely.
- CSPs can distribute SECRETS in person, by postal mail, or online distribution
- If using online distribution, SECRETS must be delivered over a secure channel with the post enrollment binding requirements
- If the authenticator uses look-up secrets sequentially from a list, the subscriber can dispose of used secrets after a successful authentication

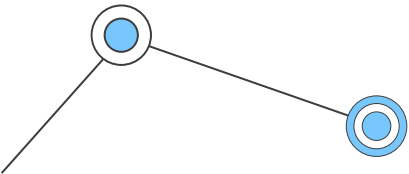


03 – Multi-Factor Authentication

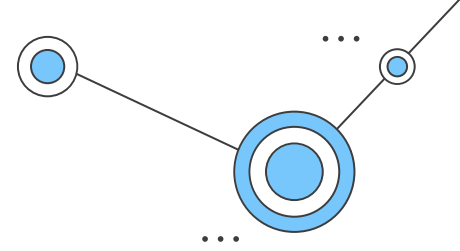


Guidelines from NIST:

- Verifiers must prompt the subscriber for the next secret from their authenticator or for a specific secret
- The given secret will be successful only once
- Out-of-band authenticator is a physical device that is uniquely addressable and can communicate securely with the verifier over a distinct communications channel, referred to as the secondary channel.



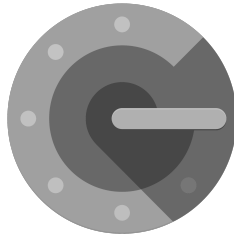
03 – Multi-Factor Authentication



Authenticator Applications



Cisco DUO



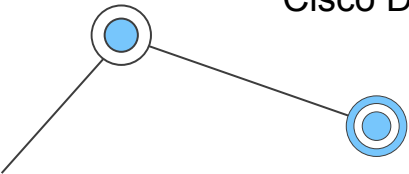
Google
Authenticator



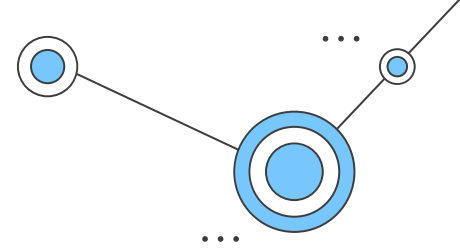
Microsoft
Authenticator



Twilio Authy



03 – Multi-Factor Authentication



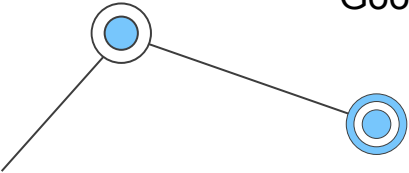
Out-of-band authenticator

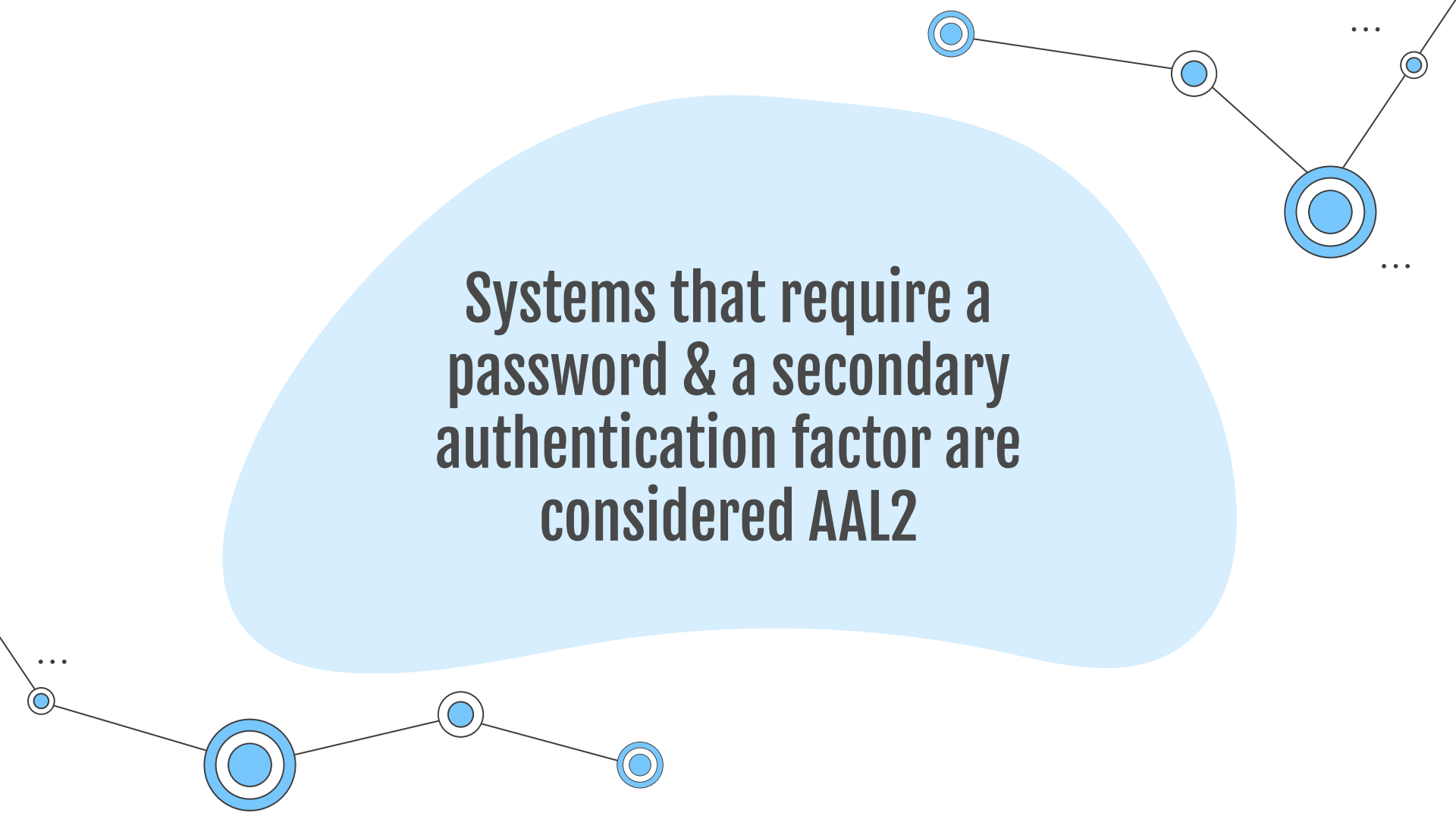


Google Titan Security Key



RSA SecureID





**Systems that require a
password & a secondary
authentication factor are
considered AAL2**

04

Why Implement MFA?

04 – Why implement MFA?

- A compromised password does not immediately provide access to systems when a second authenticator is required
- Use of federated accounts has created single point of failure
- Cyber insurance requirement

Thanks!

Do you have any questions?

NIST SP 800-63B

CREDITS: This presentation template was created by [Slidesgo](#), including icons by [Flaticon](#), infographics & images by [Freepik](#) and illustrations by [Stories](#)

Please keep this slide for attribution

