

4.2.3 Authentication Methods

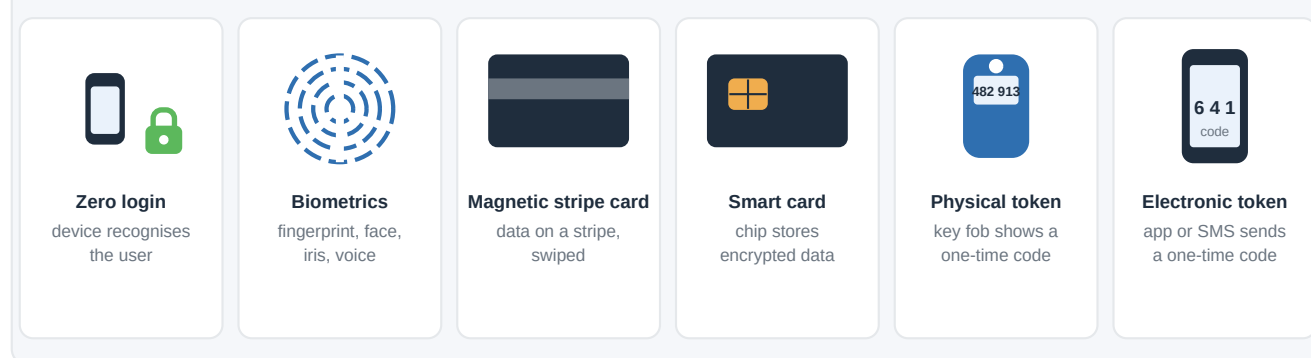
Syllabus 2026 - 2028

WHAT YOU NEED TO KNOW

- Other authentication methods: zero login, biometric methods, magnetic stripes, smart cards, physical tokens and electronic tokens

Authentication is how a system checks that a user is who they claim to be. A password is something you **know**. Other methods use something you **have** (a card or token) or something you **are** (a body feature). Using two methods together is more secure (two-factor authentication).

Figure 9: Authentication methods



Method	How it works and uses	Advantages	Disadvantages
Zero login	The user does not enter a password. The system recognises the user automatically, for example from a trusted device, location, a nearby phone or the way they use it. Used for phones, smart homes and apps.	Very convenient; no password to forget or steal; quick	Anyone with the device may get access; less control; relies on tracking user data; can wrongly recognise a user
Biometrics	Uses a unique body feature: fingerprint, face, iris, retina or voice. Used for phones, laptops, door entry and passports.	Cannot be forgotten or lent easily; hard to copy; quick	Equipment is costly; can fail (dirty fingers, poor light, noise); privacy concerns; cannot be changed if stolen
Magnetic stripe card	Data is stored on a magnetic stripe that is swiped through a reader. Used for hotel key cards, ID and access cards.	Cheap; quick; easy to issue	Easy to copy (skimming); stripe wears out and can be erased by magnets; can be lost or stolen; may need a PIN
Smart card	A card with an embedded chip that stores encrypted data and is read by a card reader. Used for bank cards, ID and building access.	More secure than a stripe; chip is hard to copy; can store a lot of data	Can be lost or stolen; needs a reader; costs more; chip can be damaged
Physical token	A small hardware device, such as a key fob or USB key, that shows or sends a one-time code that changes every few seconds. Used in online banking and company logins.	Code is used once, so a stolen code is useless; strong second check	Can be lost or stolen; costs money; battery can run out; user must carry it

Method	How it works and uses	Advantages	Disadvantages
Electronic token	A one-time code created by an app on the user's phone, or sent by text message or email. Used for logins and payments.	Nothing extra to carry; cheap; easy to set up	Needs a phone, battery and signal; a stolen phone is a risk; text messages can be intercepted

Choosing a method

- Use **biometrics** or a **smart card** where a person must be physically present, such as a door or a device
- Use a **token** as a second check for sensitive accounts such as banking
- Use **zero login** where convenience matters and the risk is low, such as a personal phone app
- Combine two methods for the best security, for example a card plus a PIN

EXAM TIP

Always **name** the method when you give an advantage or disadvantage. 'A fingerprint cannot be forgotten' is a good point about biometrics. 'It is more secure' on its own gains no mark.

Key terms

Term	Meaning
Authentication	Checking that a user is who they claim to be.
Zero login	Automatic recognition of a user without typing credentials.
Biometric	Authentication using a unique body feature.
Magnetic stripe	A strip on a card that stores data magnetically.
Smart card	A card with a chip that stores encrypted data.
Physical token	A hardware device that generates a one-time code.
Electronic token	A one-time code from an app, text or email.
Two-factor authentication	Using two different checks to log in.
Skimming	Illegally copying data from a magnetic stripe card.

Practice questions

Answer each question in full sentences. Command words used: State (give a short answer), Describe (say what it is like), Explain (give reasons), Analyse (break it down and examine it), Suggest (apply your knowledge to a situation), Compare and contrast (similarities and differences), Evaluate (weigh up and reach a judgement).

No.	Question	Marks
1	State two examples of biometric authentication methods.	[2]
2	Describe how a physical token can be used to log in to an online banking account.	[3]
3	Compare and contrast a magnetic stripe card with a smart card.	[4]
4	Suggest a suitable authentication method for a school server room and give two reasons.	[3]
5	Evaluate the use of biometric methods instead of passwords.	[6]

Total: 18 marks