The PIV card’s 3-factor security:

- Something you know: **a password**.
- Something you have: **the card itself**.
- Something you are: **your fingerprint**.

**Uses:**

- Gain physical access to federal buildings.
- Verifiable ID at security checkpoints.
- Online login, security and document encryption

The PIV card is compliant with FIPS 201 standards.

**How the employee’s ID is authenticated:**

1. Security guard places PIV card into a reader. Data on the card verifies it was issued by the government and has not been altered.
2. Employee places finger on pad.
3. Reader verifies fingerprint against template stored on the card.

Smart card contact technology is used for online security and login.

There is also a **fingerprint** template in the smart card.

Contactless technology is used for building access.

This is representative; depiction of the actual appearance of the card is prohibited.

Source: Gemalto
How it works
Smart card technology

What is smart card technology?
Smart card technology uses a computer and software with 100s of built-in security features.

The contacts on the surface of the device are connected...
The whole piece is embedded into a plastic card or hard token.

...to wires running from a computer chip under the surface.

Smart card technology is used to create personal, portable security devices:

- Passports
- Cards and credentials
- Unconnected tokens
- USB tokens
- SIM/UICC applets