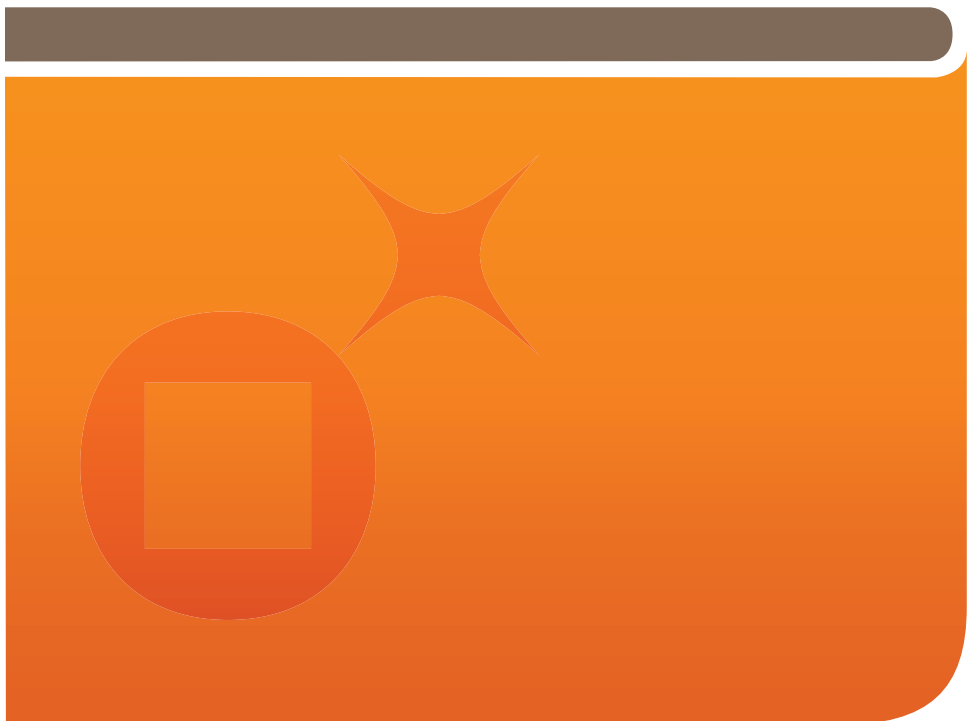




Gemalto Explains

Healthcare Employee Authentication

Complying with DEA authentication regulations for e-prescriptions of controlled substances



How it works

Healthcare employee authentication

To safeguard against unauthorized people having access to medical records, strong security measures need to be in place.

1

Why not give healthcare workers a password?

- If passwords are the only protection used, then anyone obtaining the password can gain access to the system and have access to whatever is “protected” by that password...



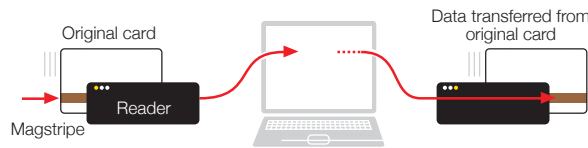
- Passwords are vulnerable to:



2

Why not give healthcare workers a magstripe card?

- Swiping a card through an (illegal) magstripe reader (skimming) makes it possible to produce a clone of the card, with all its relevant data intact.



- When data breaches occur (account numbers stolen from card databases), unauthorized authentication is possible because the physical card is not needed.



1

Smart card authentication

To ensure that an authentication system knows exactly who is looking at private data such as medical records, smart cards offer secure solutions.

Smart cards cannot be hacked.

- The healthcare worker must physically have the smart card with him or her for network or information access.
- This is called **strong authentication**, something you have and something you know, and it eliminates the threat of stolen passwords.
- A smart card is invulnerable to keyboard logging because security key calculations are done by the computer inside it; only encrypted information passes through the computer.
- Even if a hacker captures the authentication exchange, nothing can be done with it, because every authentication is unique and created on the fly.
- Complies with the U.S. Drug Enforcement Agency's proposed rules for e-prescribing controlled substances.



2

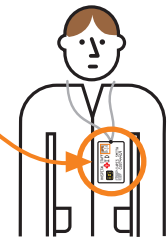
Skimming and data breaches are eliminated with smart cards.

- The smart card chip is used for authentication instead of the magnetic stripe.
- Each smart card has a unique identifier and a digital seal that cannot be copied or cloned and put onto another card, authentication terminals will know that it's a fake, and will refuse authorization.



Since the smart card is needed as an ID badge for other parts of the health worker's job, it must be carried by the individual at all times.

This means that no one else can log into a system as that person. The card cannot be left in a computer, allowing others to have access. Each user must log in separately.



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



The whole piece is embedded into a plastic card or hard token.

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

