Gemalto Explains

DEA Compliance
Complying with DEA authentication regulations for e-prescriptions of controlled substances
How it works

DEA Compliance

Smart cards and e-prescription authentication
Strong security measures must be put in place to safeguard electronic prescription for controlled substances as proposed by the U.S. Drug Enforcement Administration (DEA).

1. Physicians must go to a DEA-registered hospital, a state licensing board or law enforcement agency in person and prove their identity.

Patients receive a two-factor authentication device such as a smart card ID or hard token.

Federal government doctors can use their Personal Identity Verification (PIV) card.

What’s stored on your ID card:
- Identification information.
- A government issued secure document authorizing controlled substance prescriptions.
- A digital identity for securely signing unalterable, non-reputable e-prescriptions.
- A personal, unique PIN code, like an ATM card.

2. When e-prescribing a controlled substance, insert the ID card into a device connected to the PC and enter the PIN code to confirm identity and digitally sign the e-prescription.

3. Ideally, the pharmacist filling the prescription also has a smart card and a PIN device for security and auditing purposes.

E-prescription card benefits:
- No need to fill out prescriptions or call.
- Both parties retain a digitally signed copy of the prescription providing an unalterable, non-reputable audit trail.
- Controlled substances remain controlled with nationwide e-prescription flexibility.

= Efficient e-prescription security.
How it works

DEA Compliance

Why not let physicians use passwords for controlled substance e-prescriptions?

- If passwords are the only protection used, anyone obtaining that password could issue e-prescriptions in that physician’s name...
- Passwords are vulnerable to:
  - Shoulder surfing.
  - Reading sticky note reminders.
  - Keyboard logging, password sharing, phishing and spyware.
  - Leaving the door open for abuse of controlled substances.

Smart cards stop abuse and cannot be hacked.

- The physician must physically have the smart card with him or her and enter the PIN to authorize an e-prescription.
- 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.

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.