Advanced Encryption Standard (AES)

Secure Hash Standard (SHS)

Digital Signatures (DSA, RSA and ECDSA)

Triple-DES Encryption Algorithm (TDEA)

CYBERDI

FIPS 140-2A

WHAT IS FIPS-140-2A VALIDATED ENCRYPTION?

A Government publication of encryption standards from the Federal Information Processing Standards in accordance with the Federal Information Security Management Act (FISMA) and approved by the Secretary of Commerce

WHAT IS A FIPS-140-2A VALIDATED MODULE?

FIPS 140-2a does not provide encryption or keys. Vendors can validate modules, part of the software encrypting data encrypting CUI or security to protecting CUI to the standard

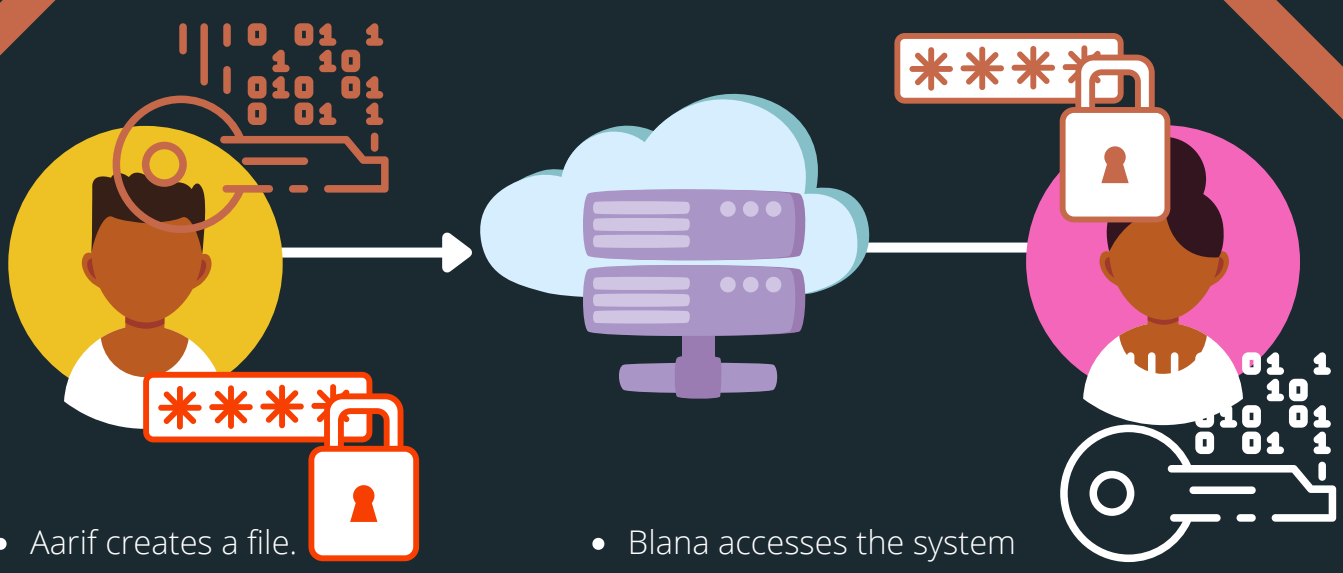
WHEN MUST FIPS-140-2A VALIDATED MODULES GET USED

FISMA dictates that U.S. government agencies must use FIPS 140-2 validated cryptography modules to protect data such as CUI classified at the moderate level

WHAT IS THE DIFFERENCE BETWEEN COMPLIANCE AND VALIDATION?

Compliant-Just the modules, often from a third party validated
Validation: Entire tool tested and validated at an accredited laboratory.

FIPS 140-2 requires hardware or software cryptographic modules use approved algorithms



- Aarif creates a file.
- The System creates public/private key pair.
- Aarif gave Blanca, and anyone with her role access.
- Aarif's public key gets stored on the server. The private key on his device.
- The public key encrypts the file Aarif uploads with a symmetric key.

- Blana accesses the system
- Her role has authorized use of Aarif's file.
- Blanca downloads the file encrypted with a symmetric key.
- The private key on Blanca's device matches her public key in the symmetric key of the file
- The file opens

The system providers or privliged users never have access to keys in End-to-End Encryption

- **FIPS-validated cryptography required whenever encryption needed to protect CUI in accordance with NIST SP 800-171**
- **Digital CUI in Transit need encryption (files sending)**
- **Digital CUI at rest (files saved) needs encryption**
- **Portbale media devices (transit and rest) need encryption**
- **Online clouds and email need encryption (transit and rest)**
- **Devices such as routers inside physical security can use other encryption**
- **Many systems have a FIPS and not FIPS mode. Know the defaults**

Message Authentication (Triple-DES, AES and HMAC)