

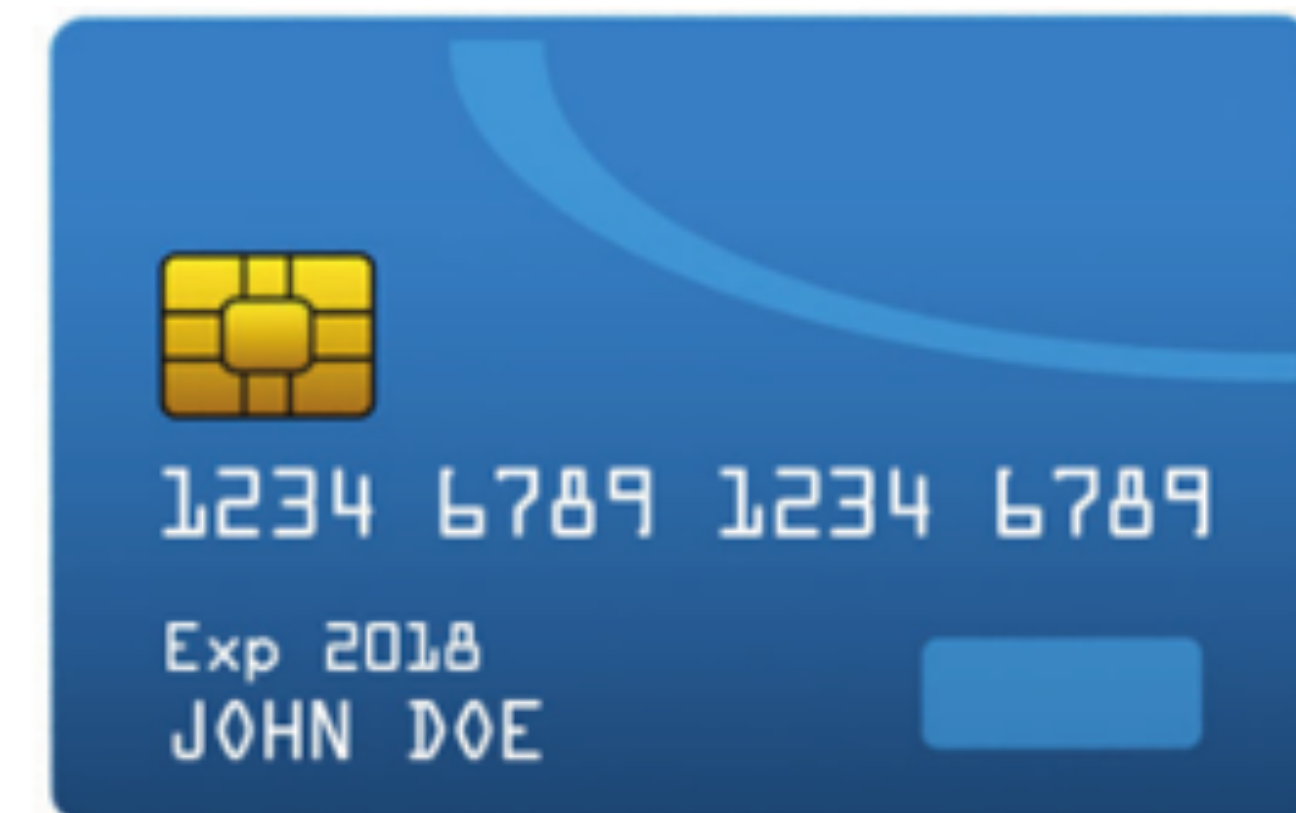
Applications

This Video Covers:

- Authentication
- HTTPS and TLS/SSL
- **Chip Technology Used in Credit Cards**

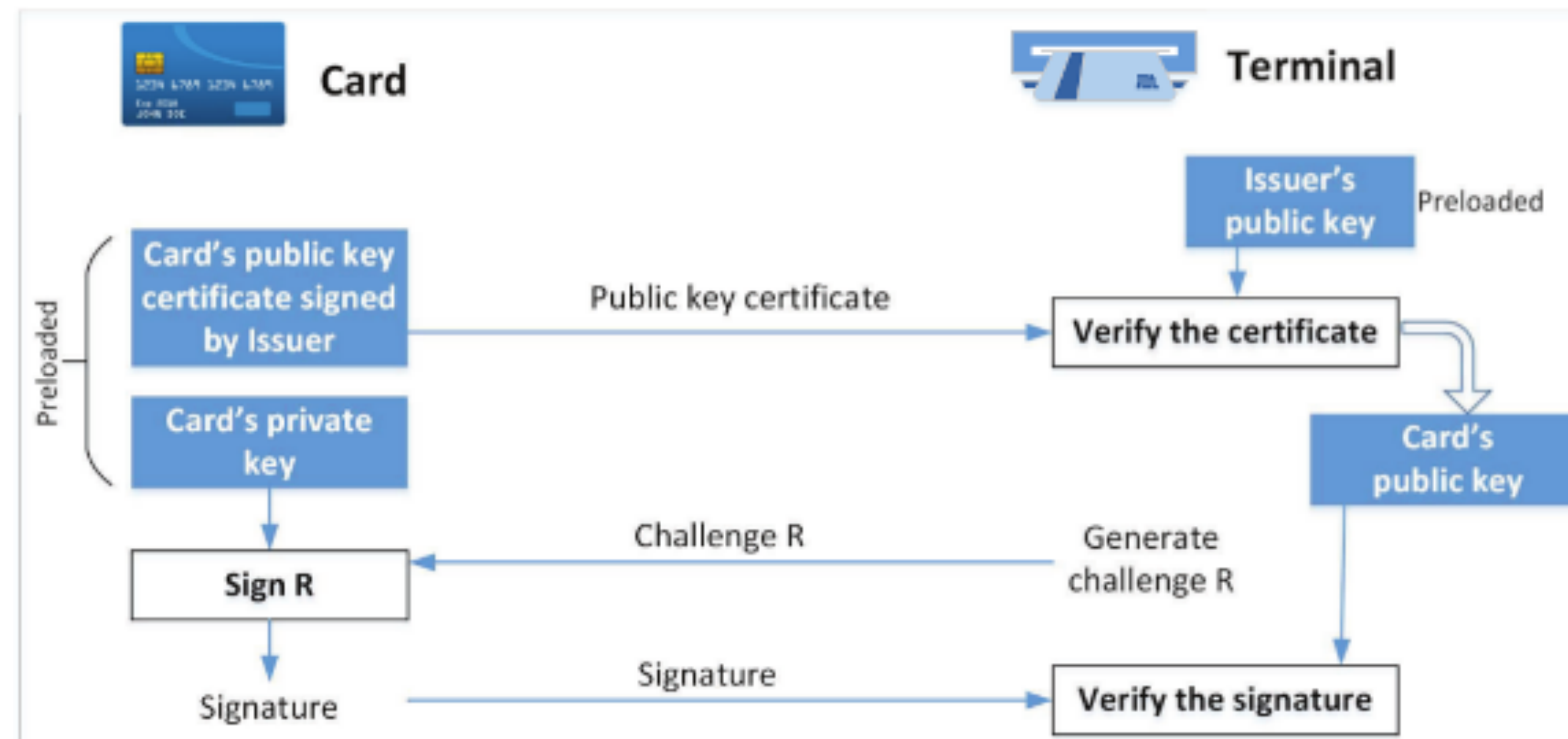
Applications: *Credit Card Chip*

- **Past:** cards store card information in magnetic stripe (easy to clone)
- **With Chip:**
 - Chips can conduct computations and store data (not disclosed to outside)
 - EMV standard (Europay, MasterCard, and Visa)
- We will cover how public key technologies are used for:
 - Card authentication
 - Transaction authentication



Applications: *Credit Card Chip — Card Authentication*

- Card contains a unique public and private key pair
 - Private key is protected and will never be disclosed to the outside
 - Public key is digitally signed by the issuer, so its authenticity can be verified by readers



Applications: *Credit Card Chip — Transaction Authentication*

- Issuer needs to know whether the transaction is authentic
- Transaction needs to be signed by the card using its private key
- Verified Signature:
 - To issuers: proves card owner has approved the transaction
 - To honest vendor: enables the vendor to save the transactions and submit them late

