PIV Token Issuance

Ketan Mehta
Mehta_Ketan@bah.com
October 6, 2004

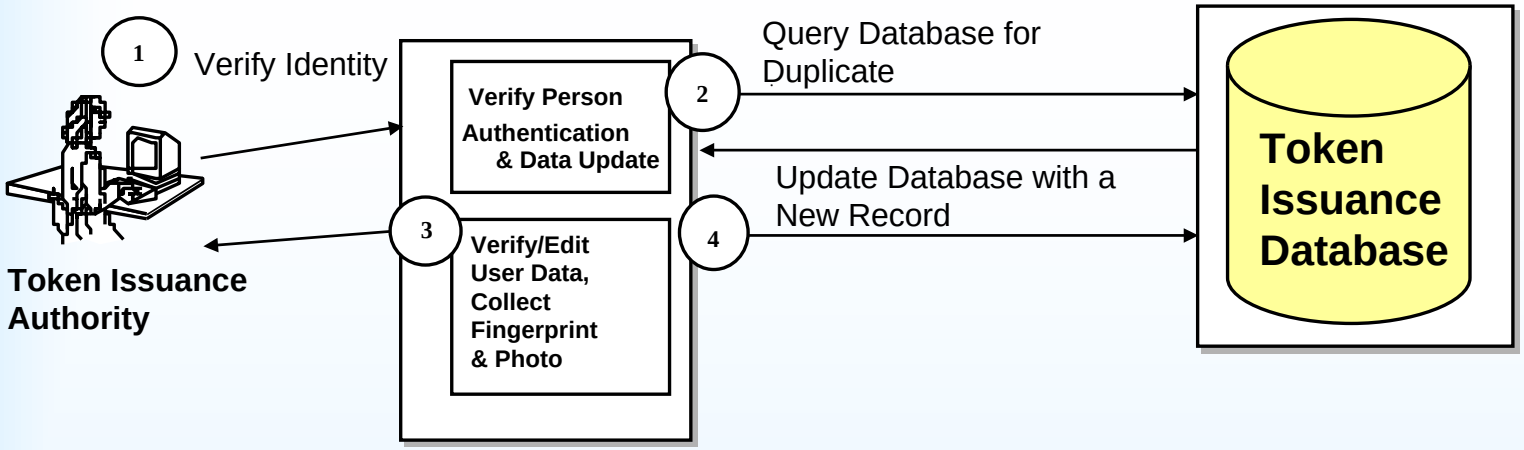
Agenda

- Definition and Purpose
- Issuance Process
- Token Issuance Authority Requirements
- Token Personalization Requirements
- Standards Compliance

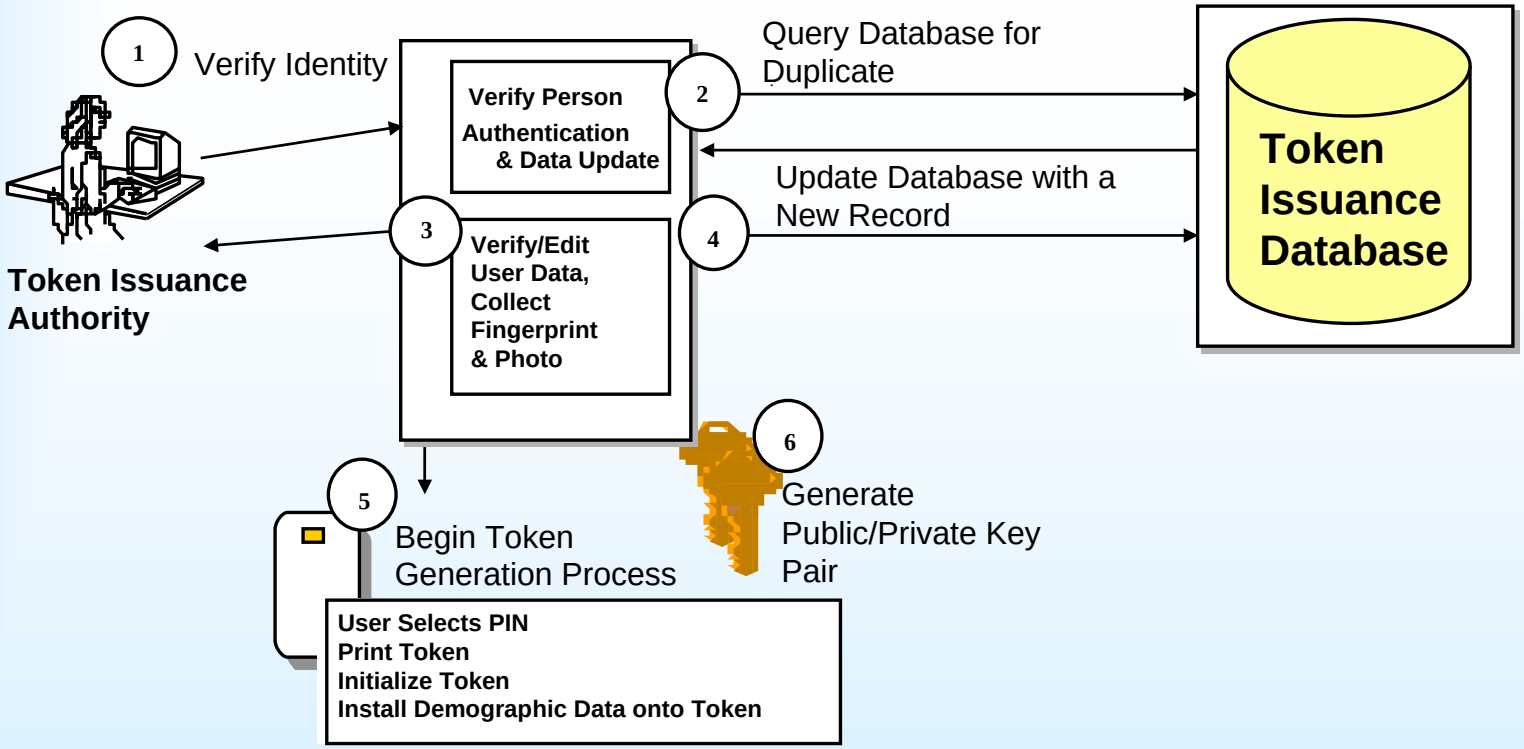
Definition and Purpose

- Definition
  - The process of issuing identity credentials on a token
- Purpose
  - Provide an identity token to the applicant
  - Create and maintain a directory server that reports on the status of the token

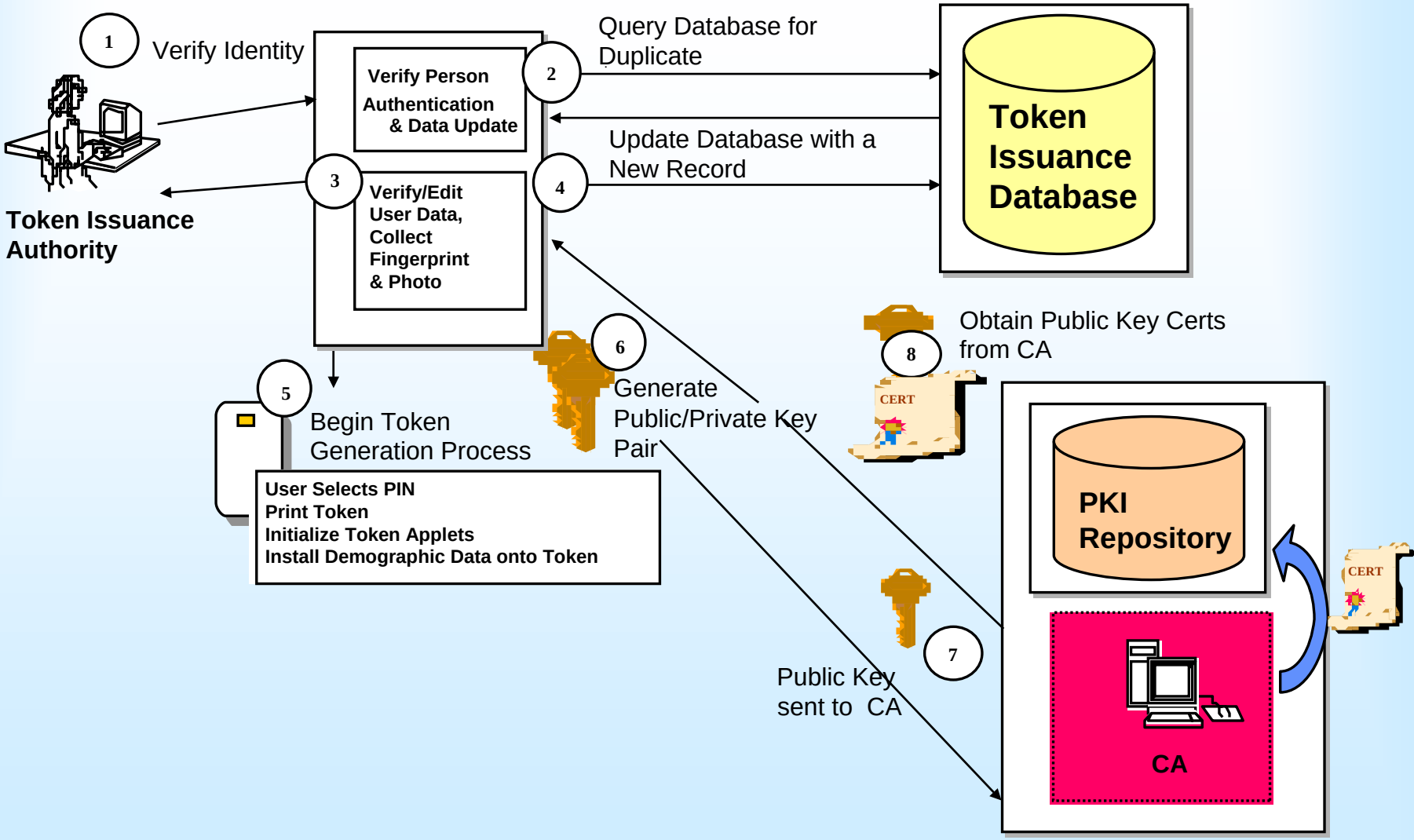
PIV Token Issuance Process



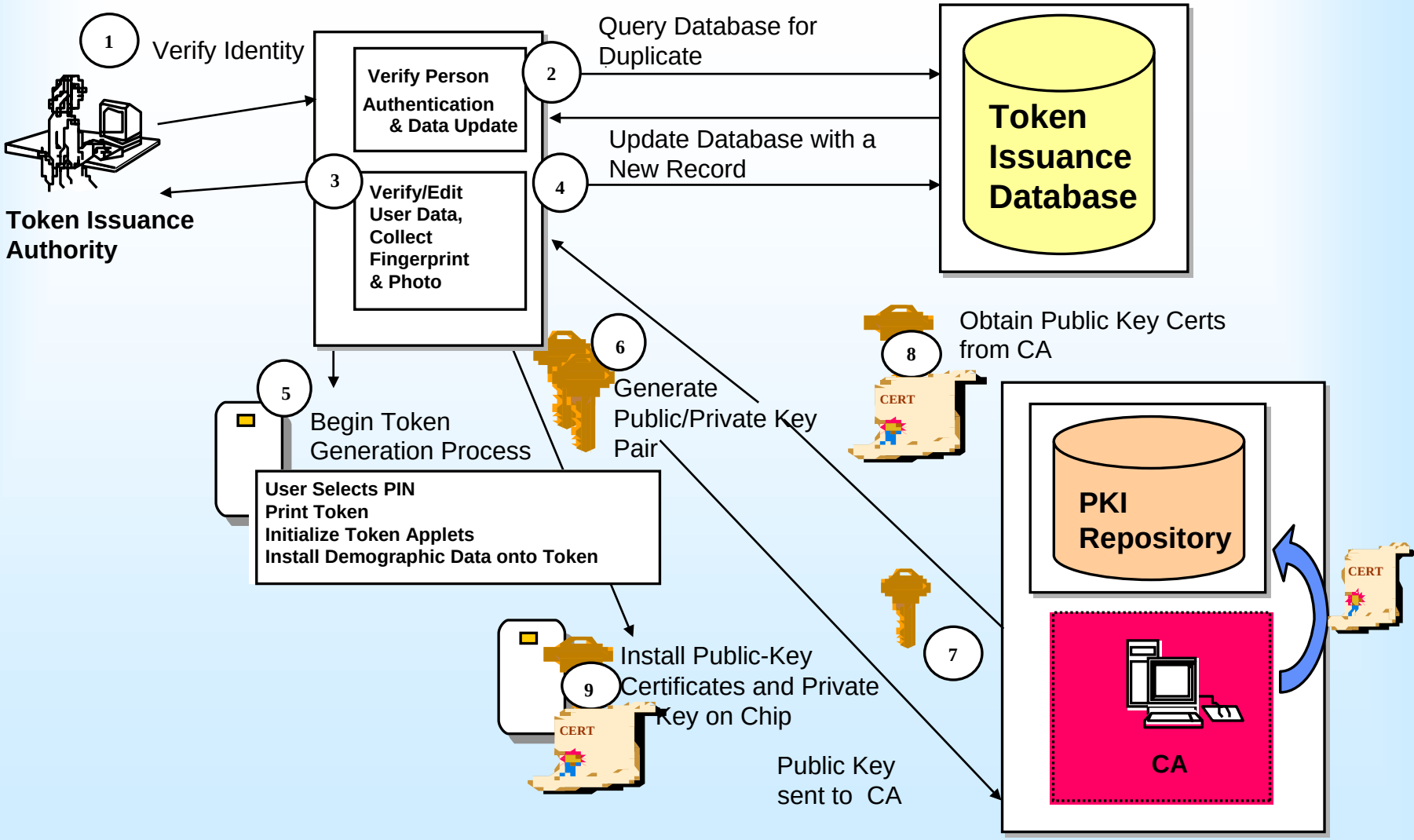
PIV Token Issuance Process



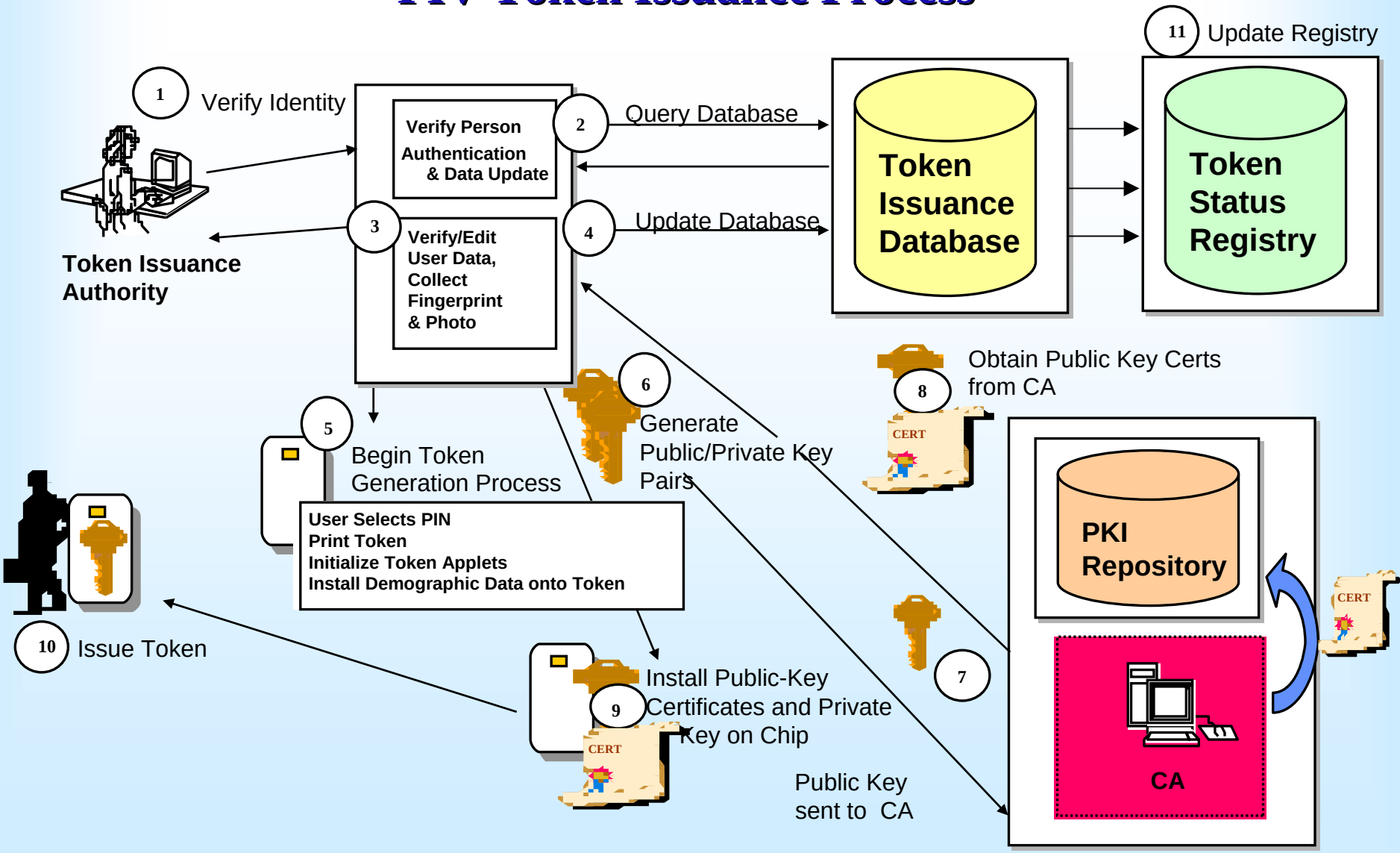
PIV Token Issuance Process



PIV Token Issuance Process



PIV Token Issuance Process



Token Issuance Authority Requirements

- Issuance authority shall assure that PIV tokens cannot be cloned, counterfeited, modified without authorization, probed to obtain cryptographic keys, and used to gain access by anyone other than the authorized applicant.
- All applicants that are issued a PIV token must appear in person to obtain credentials.
- The PIV token personalization shall include printing of photograph, name and information on the token as well as loading the relevant Token applications, biometrics, Personal Identification Number (PIN), PKI certificates, and symmetric keys.
- Biometric characteristics captured during the PIV token personalization include two index fingerprints and a digital photograph.
- Issuance authority will maintain a LDAP directory server that reports on the status of the token and may provide additional authentication services.
- Issuance authority may acquire Certificate Authority services who shall maintain and operate Certificate Revocation List and On-line Certificate Status Protocol.

Token Issuance Authority Requirements

- Access to LDAP and OCSP servers will be authenticated and access to the status information is at the agency discretion; agencies may choose to make the certificate or token status information publicly available to unauthenticated parties.
- All certificates issued to support PIV token authentication shall be issued under the id-CommonHW policy as defined in the X.509 Certificate Policy for the Common Policy Framework.
- This standard mandates the inclusion of a 1024-bit RSA Identity Authentication key within a PIV token. The associated certificate and all other certificates in the verification chain including the Root trust anchor must be included on the PIV token.
- Digital signatures (optional feature) generated by infrastructure components must be generated using 2048-bit RSA private keys.

Token Personalization Requirements

- Following authentication data is required on the token:
  - A Token holder unique identification string (CHUID)
  - Personal Identification Number (PIN)
  - Biometric templates
  - Symmetric keys
  - Asymmetric key pairs and associated certificates
- Biometric match-on-card is NOT required
- The token shall support contact (ISO 7816) and contactless (ISO 14443) interfaces. The standard does not require dual interface readers; an agency can choose contact readers for logical access application and contactless readers for physical access.
- The assurance levels being considered require both symmetric and asymmetric key challenge-response protocols. In addition to these operations, the agency may require Token holder to submit PIN.
- The CHUID and biometric templates shall be stored in the root file system of the Token. The CHUID must be openly readable.

Standards Compliance

- The format of the CHUID shall be as defined in PACS
- The format of biometric templates shall be as defined in CBEFF
- The public key certificates stored on the PIV token shall conform to RFC 3280
- The internal format of cryptographic keys stored on the Token is not specified in this standard
- The physical access control systems where the reader is not connected to general purpose desktop computing system, the reader-to-host system interface is not specified in this standard.
- The CHUID data element that contains the Token holder's FASC-N identifier is used for various symmetric key based challenge-response schemes that are specified within the PACS model.

Questions

Comments

Discussion