PKI in Today's Government

Mary Dixon
Director, Access Card Office

29 November 2001

Background

- Pilots / Studies since 1993
- Long list of benefits
- No “real savings” to pay for program
- Data-centric smart card
  - Synchronization issues

Background (cont.)

- Killer application - PKI
  - Needed hardware-based token
  - Securing our networks
  - Non-repudiation for e-business
    - Legally accepted
    - Paperless contracting

Added Benefit: PKI facilitates moving from a data-centric to web-centric model

The Decision

Common Access Card

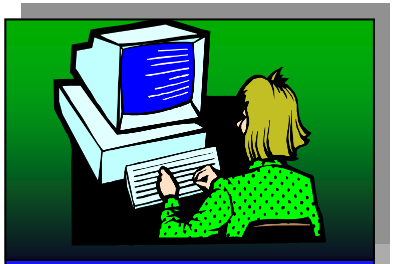
November 10, 1999

MEMO FROM:
Dr. John Hamre
(Deputy Secretary of Defense)

Create a Common Access Card

- I.D. card for:
  - Active military
  - Selected Reserves
  - DoD civilians
  - “Inside the wall” contractors
- Physical and logical access
  - Authentication keys
- Military ID card infrastructure

Issuance Process
(Business Process Re-engineering)

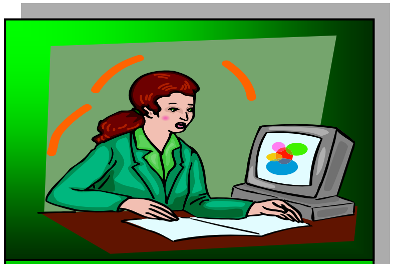


RAPIDS

ID Cards
Avg. 10 Minutes

LRA

PKI Registration
Avg. 15-20 Minutes



Kiosk or Client PC

Download Certificates
Avg. 15-20 Minutes

Integrated

CAC-Enabled RAPIDS

SMARTCARD

One Stop CAC Issuance
10-15 Minutes and
Going Down!

Why A Smart Card?

- Facilitate E-commerce (non-repudiation)
- Use PKI and the Internet to
  - Reduce paperwork
  - Decrease transaction / business process time
  - Access legacy databases (with strong authentication and security)
- Improve / re-engineer business processes
- Improve security of physical access
- Improve security of unclassified networks

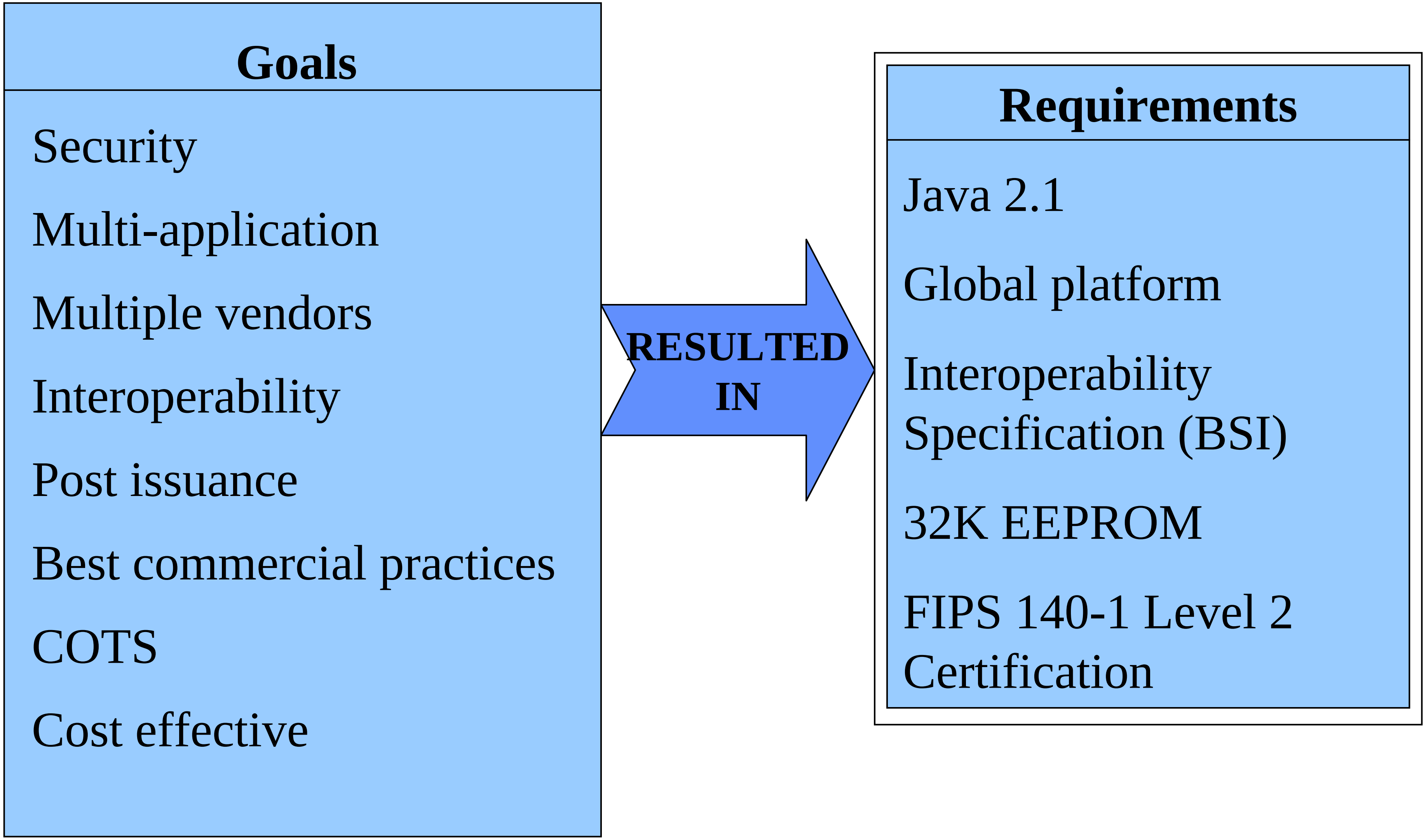
Development Strategy

- Incremental - do what can be done today; defer other issues

- Backward Compatible - do not obsolete tomorrow what we did today

- Keep up with emerging standards
- Migration with technology
- Adherence to best commercial practices

Card Architecture Goals



Goals

- Security
- Multi-application
- Multiple vendors
- Interoperability
- Post issuance
- Best commercial practices
- COTS
- Cost effective

RESULTED IN

Requirements

- Java 2.1
- Global platform
- Interoperability Specification (BSI)
- 32K EEPROM
- FIPS 140-1 Level 2 Certification

Strengthens Authentication of Identity

- Checks Credentials vs. DEERS (Not Source Database)
  - Biometric
  - Data from Component Personnel Systems
- Identity management - key ingredient in PKI

Strengthens Security of Issuance Process

- Card to be issued & checked vs. Card Management System
  - DoD Card
  - Provided to that RAPIDS site
- VOs need:
  - CAC present
  - Registered w/ access at site logging in
  - Biometric verified vs. DEERS
- No Access granted by VOs (split function)
- Rules-based system

System Audits

- **Security**
  - – Servers govern access list for RAPIDS log on and privilege level for each user
- **Fraud Prevention**
  - – Servers audit data for potential fraud analysis (date of birth changes, lost or stolen ID cards, and invalid issuance)
- **Card Production**
  - – Servers audit number and type of card produced ; sorted by site, service, personnel status, card type, and user
  - – Server card production data is rolled up to the main frame level for summaries at site, Service, and system wide levels

Initial Uses of Card

Core PKI Functions

Authentication

Encryption

Signing

PK-Enabled Applications

Defense Travel System

Wide Area Workflow

Electronic Document Access

What Else Have We Accomplished?

- PKI Requirements
  - Certificate Practice Statement
  - Certificate Acceptance Form
- CAC Policy Memo / Working on Directive
- OT&E / Interoperability Testing
- Middleware Specifications
- Two Developers Conferences / Developers Guide
- Card Management System

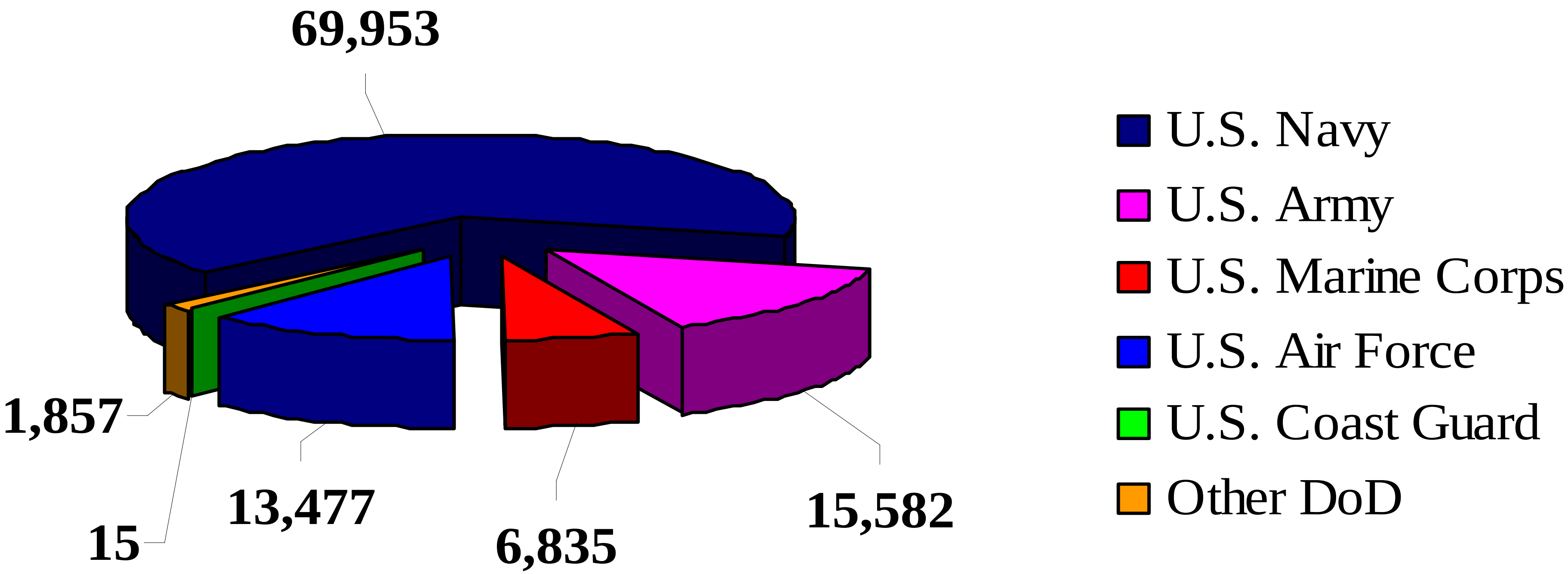
Where Are We Today?

246 Workstations in 113 Locations

107,719 Cards Issued as of 19 Nov
(issuing about 1,400 cards per day)

Where Are We Today? (cont.)

CACs Issued by Service

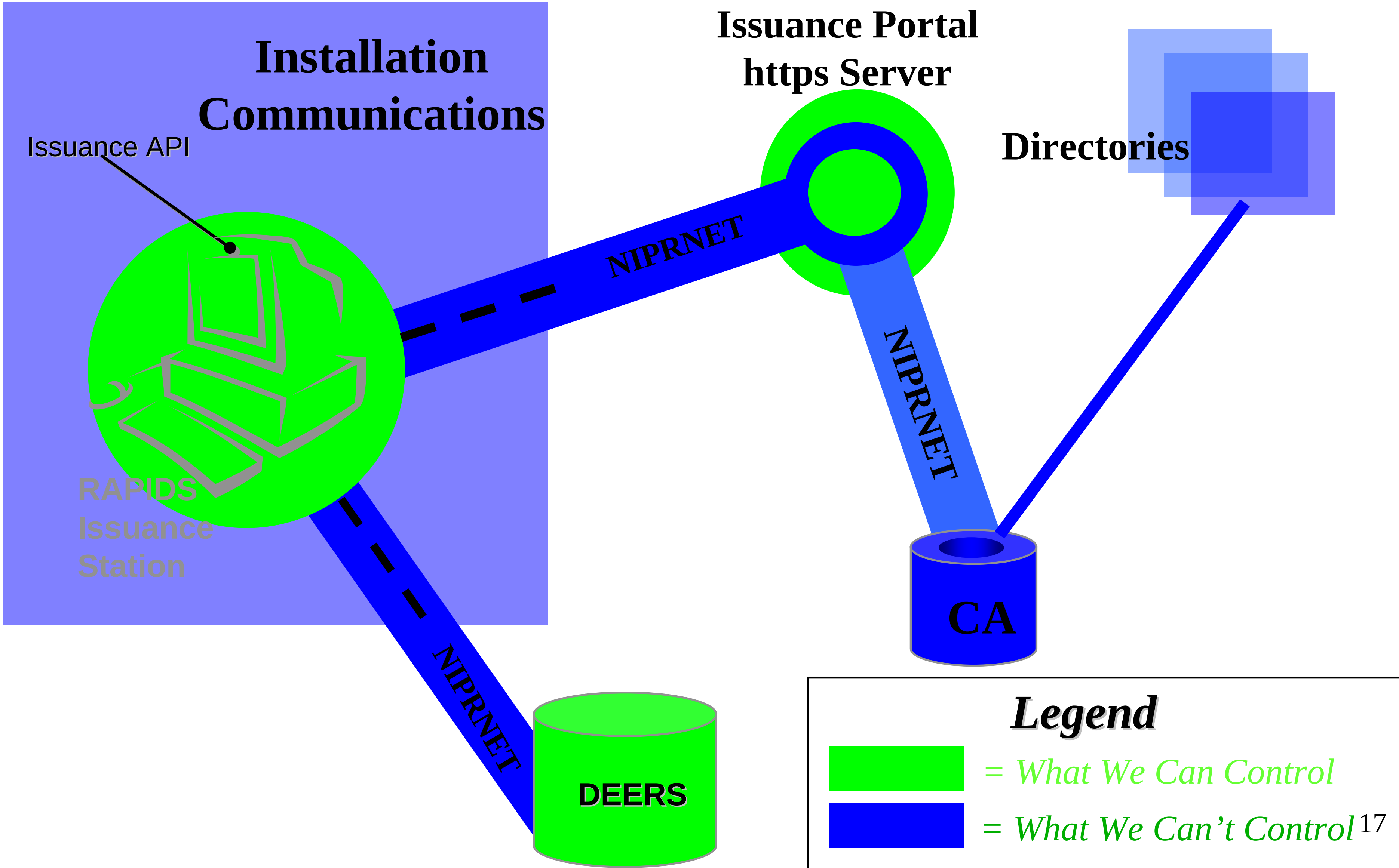


Average Issuance Time < 15 minutes

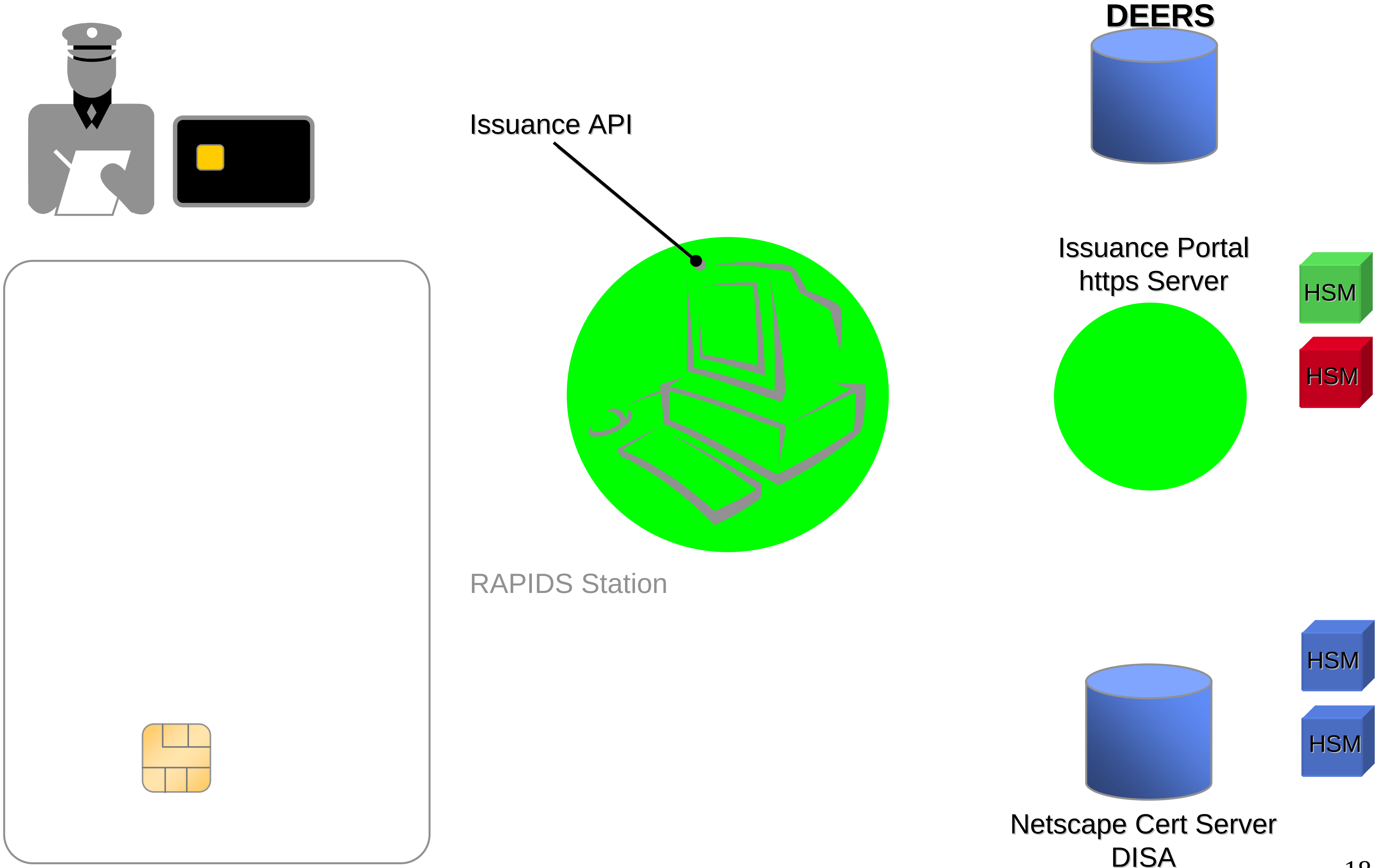
Where Are We Today? (cont.)

- Began 15-month fielding of production system 5 Nov 2001
- Military Services deploying readers / middleware and mass issuing of cards
- FIPS 140-1 Level 2 certified card
- First uses of chip on card
  - core PKI functions
  - warfighter support
  - e-business applications

Issuance Infrastructure



Distributed Issuing



DEERS

Issuance API

Issuance Portal
https Server

HSM

HSM

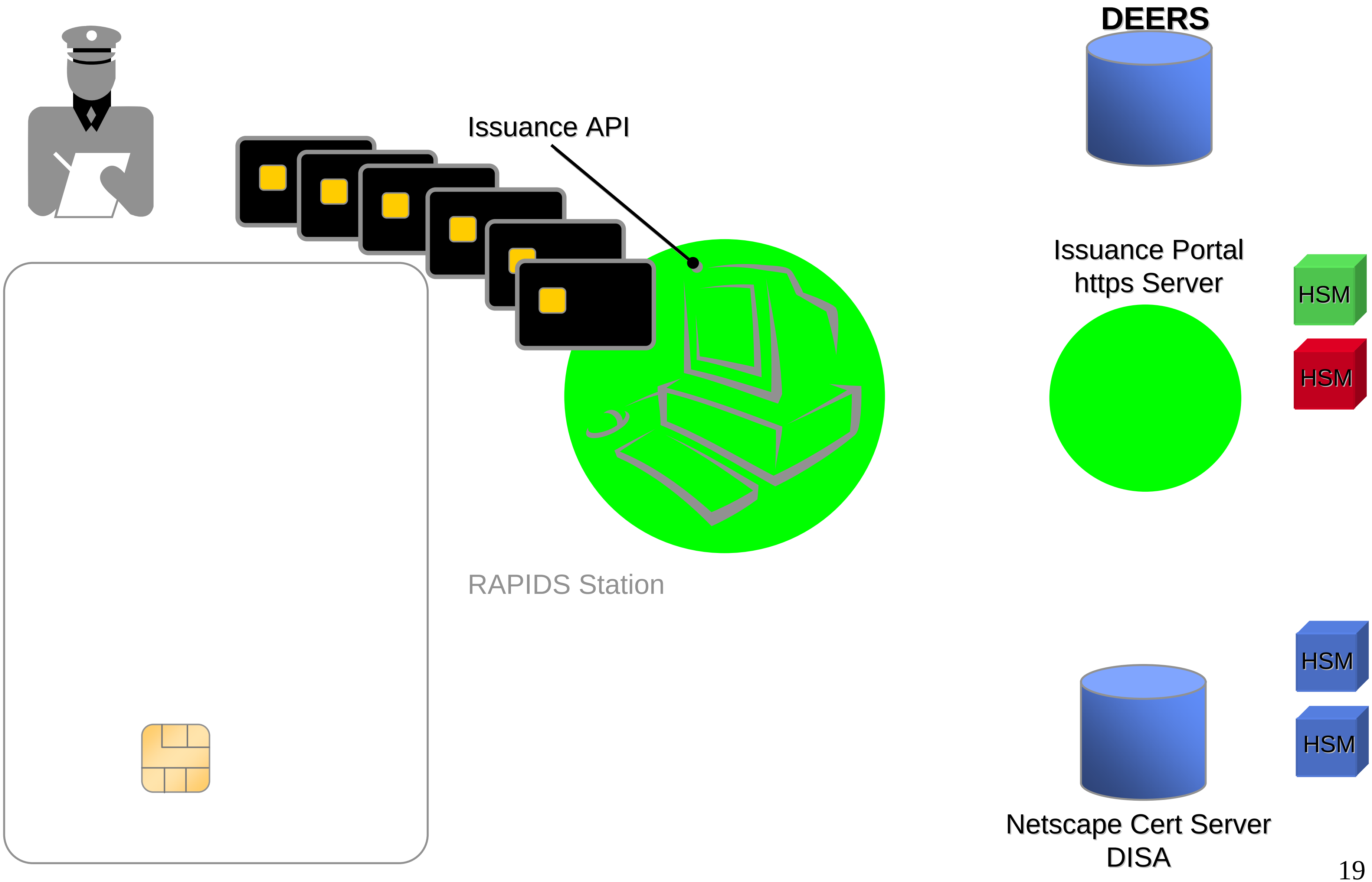
RAPIDS Station

HSM

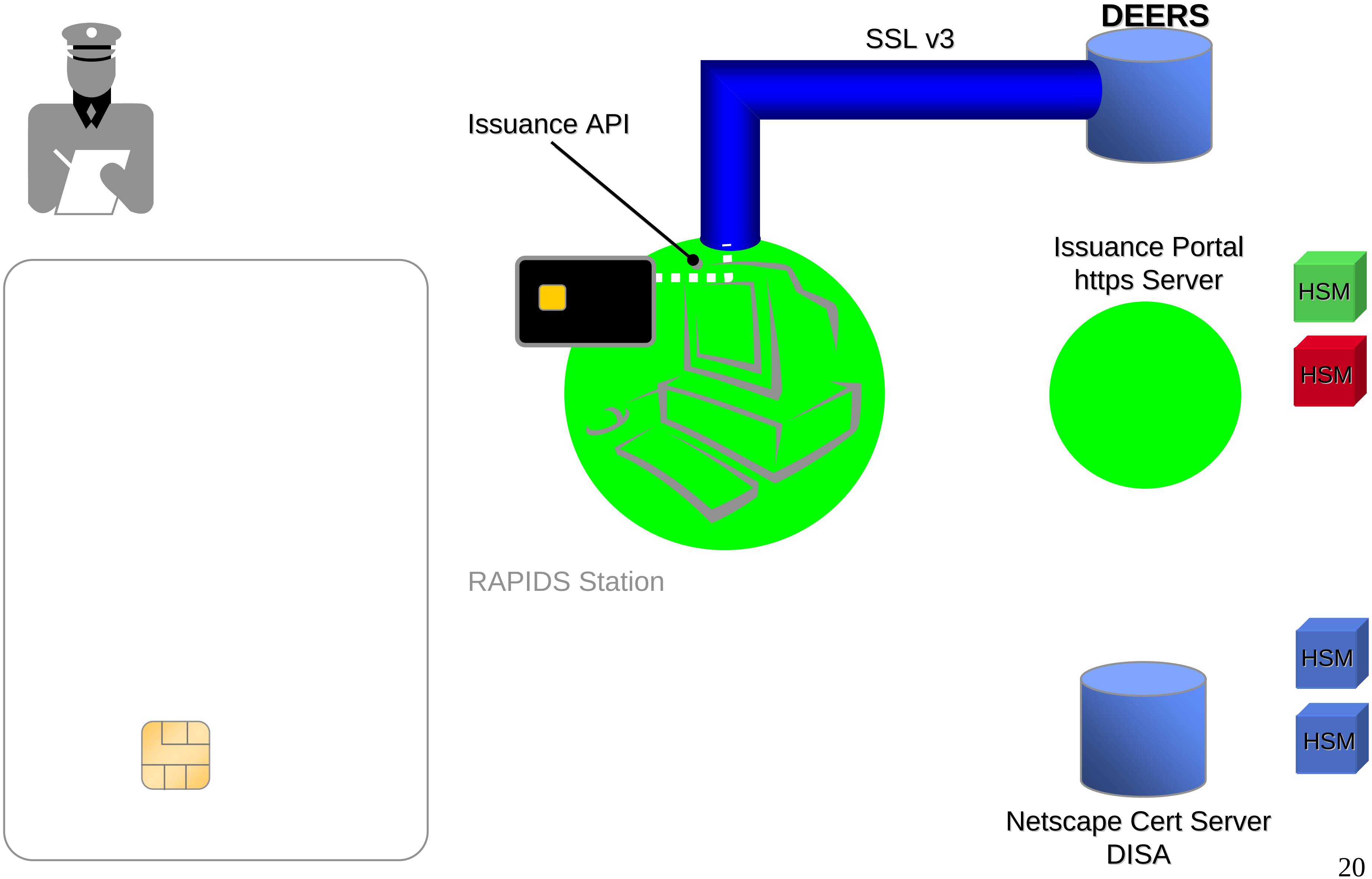
HSM

Netscape Cert Server
DISA

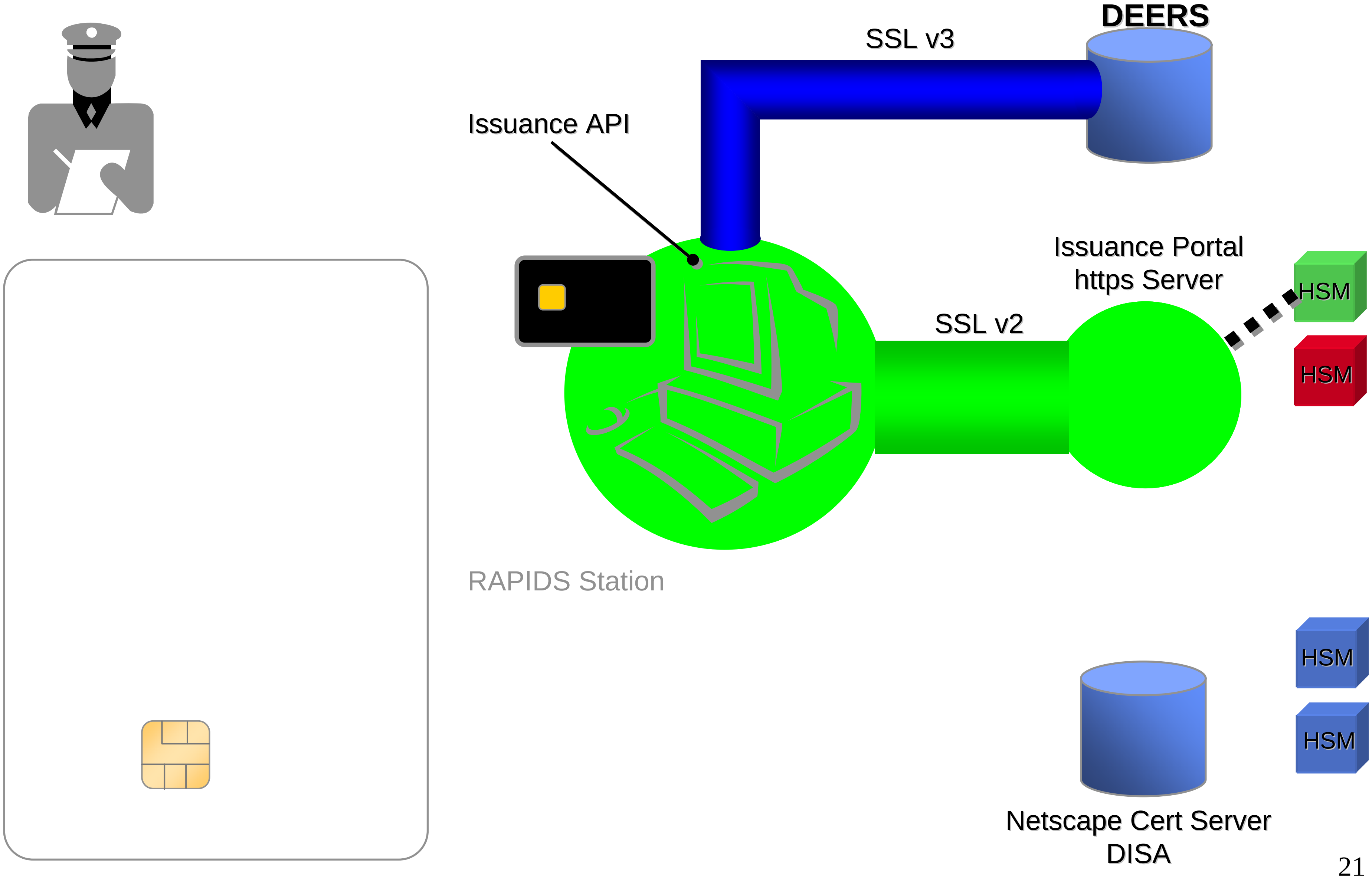
Verification Officer Authentication to DEERS



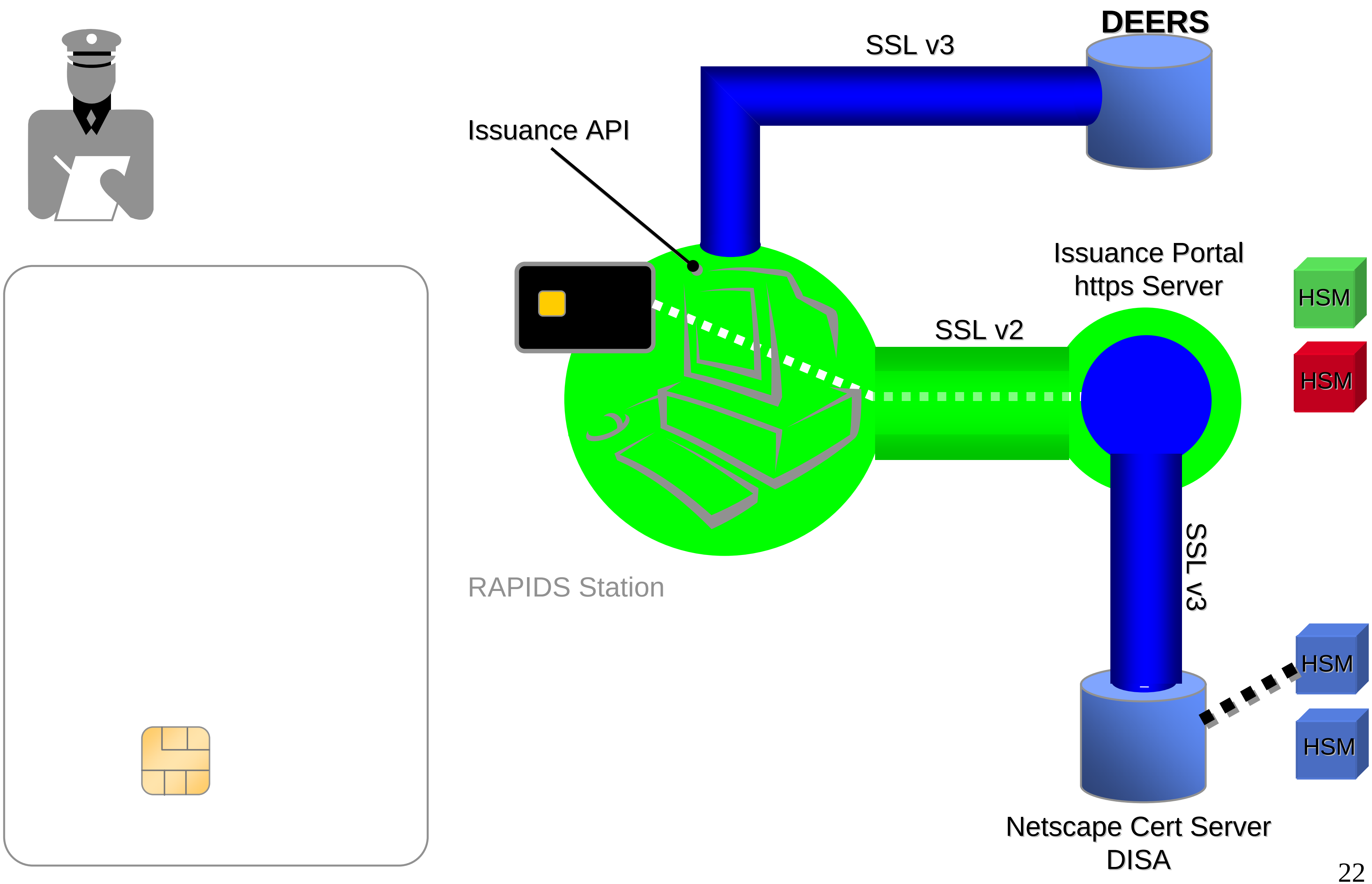
SSL v3 Session to DEERS



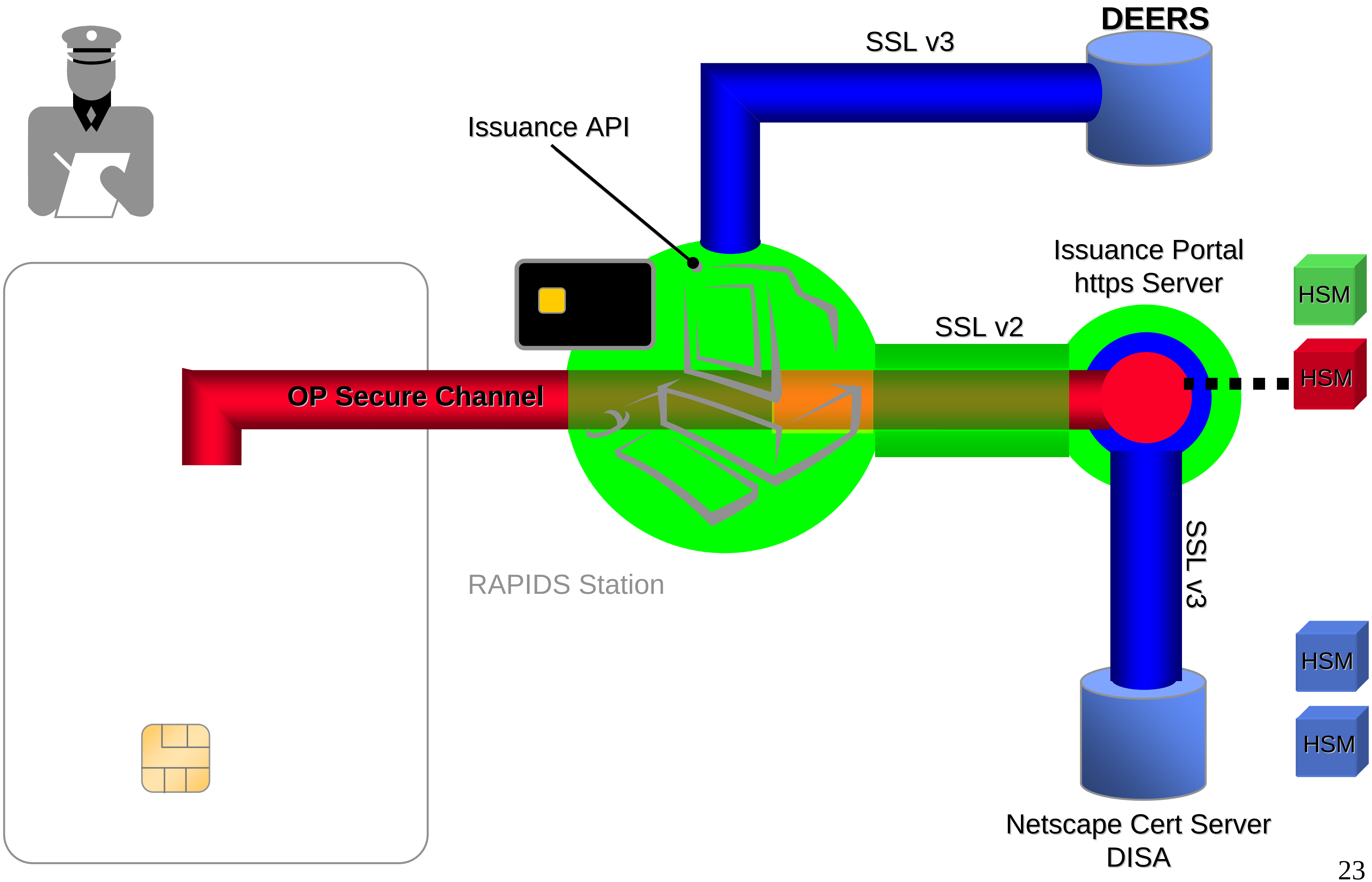
SSL v2 Session with Issuance Portal



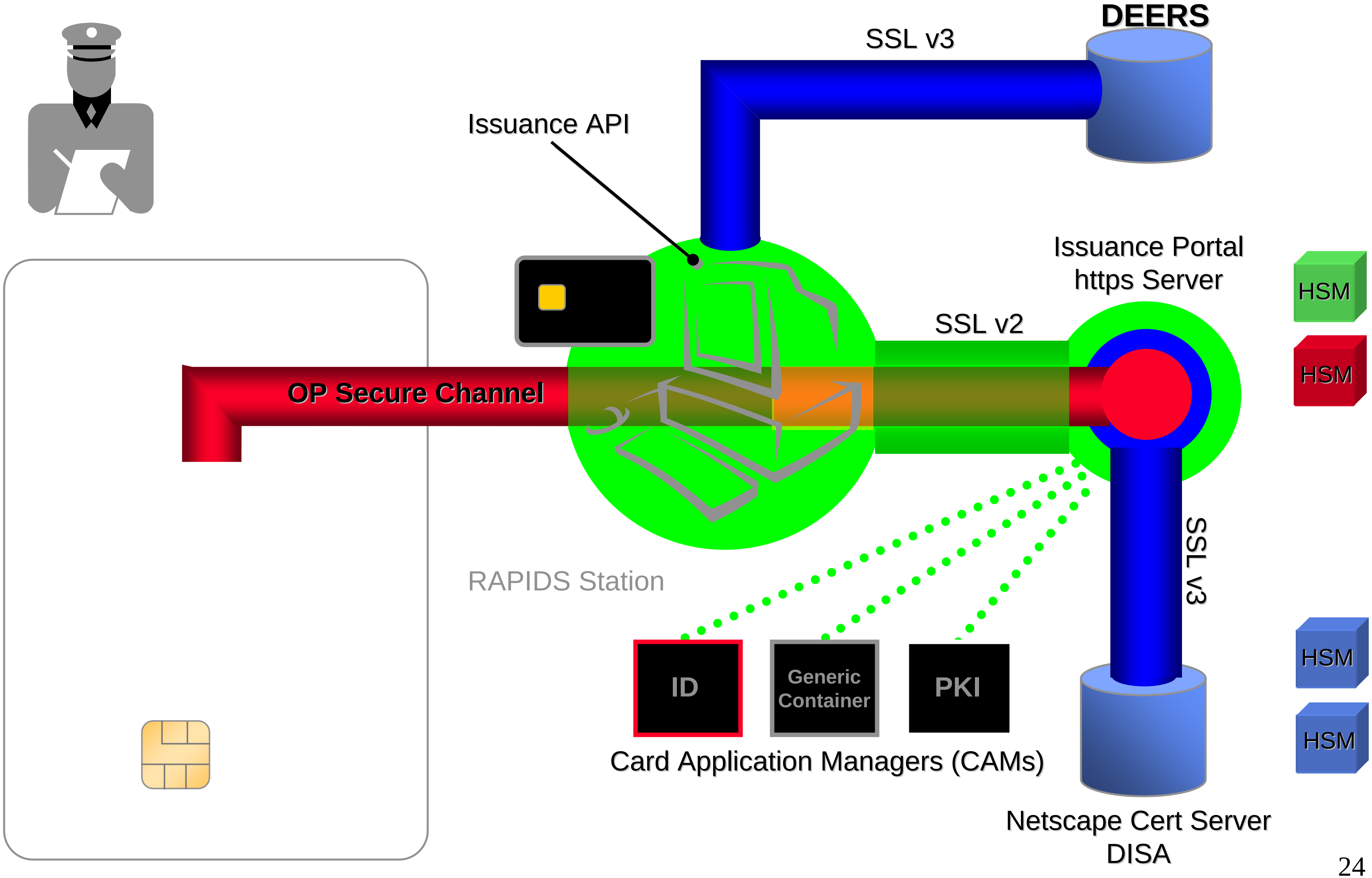
VO Authenticates to CA



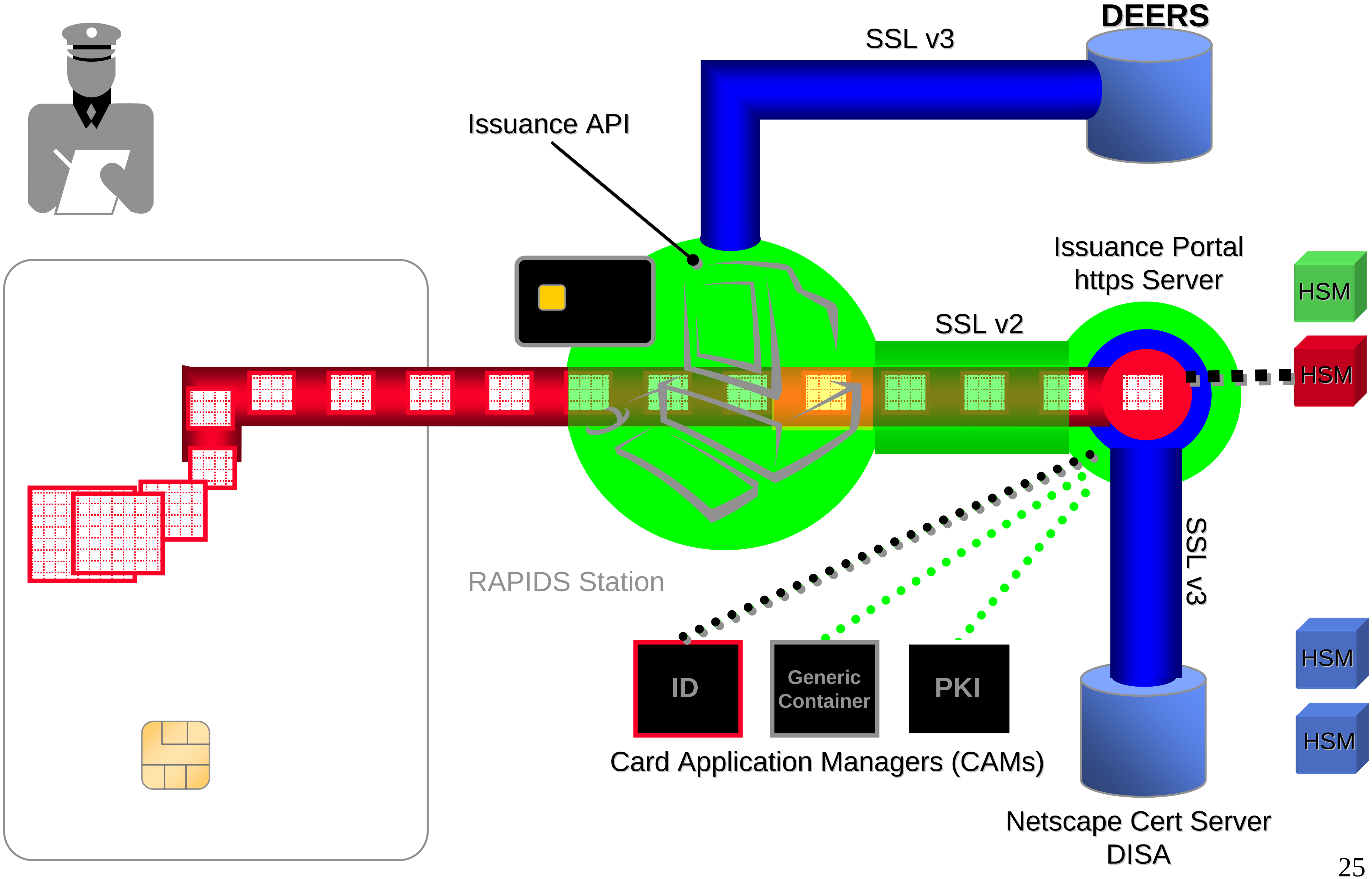
OP Secure Channel to New Card



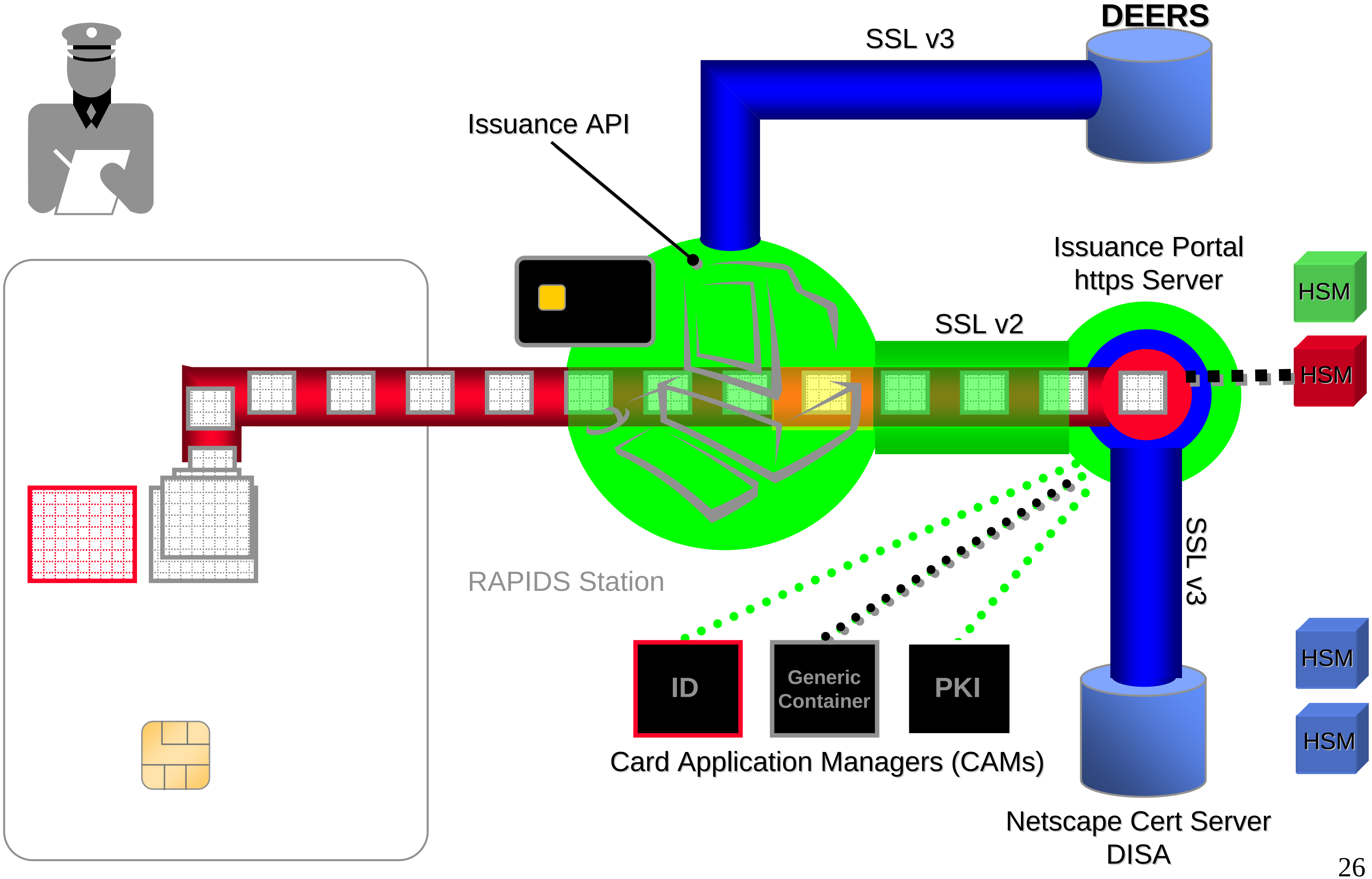
Card Application Managers (CAMs)



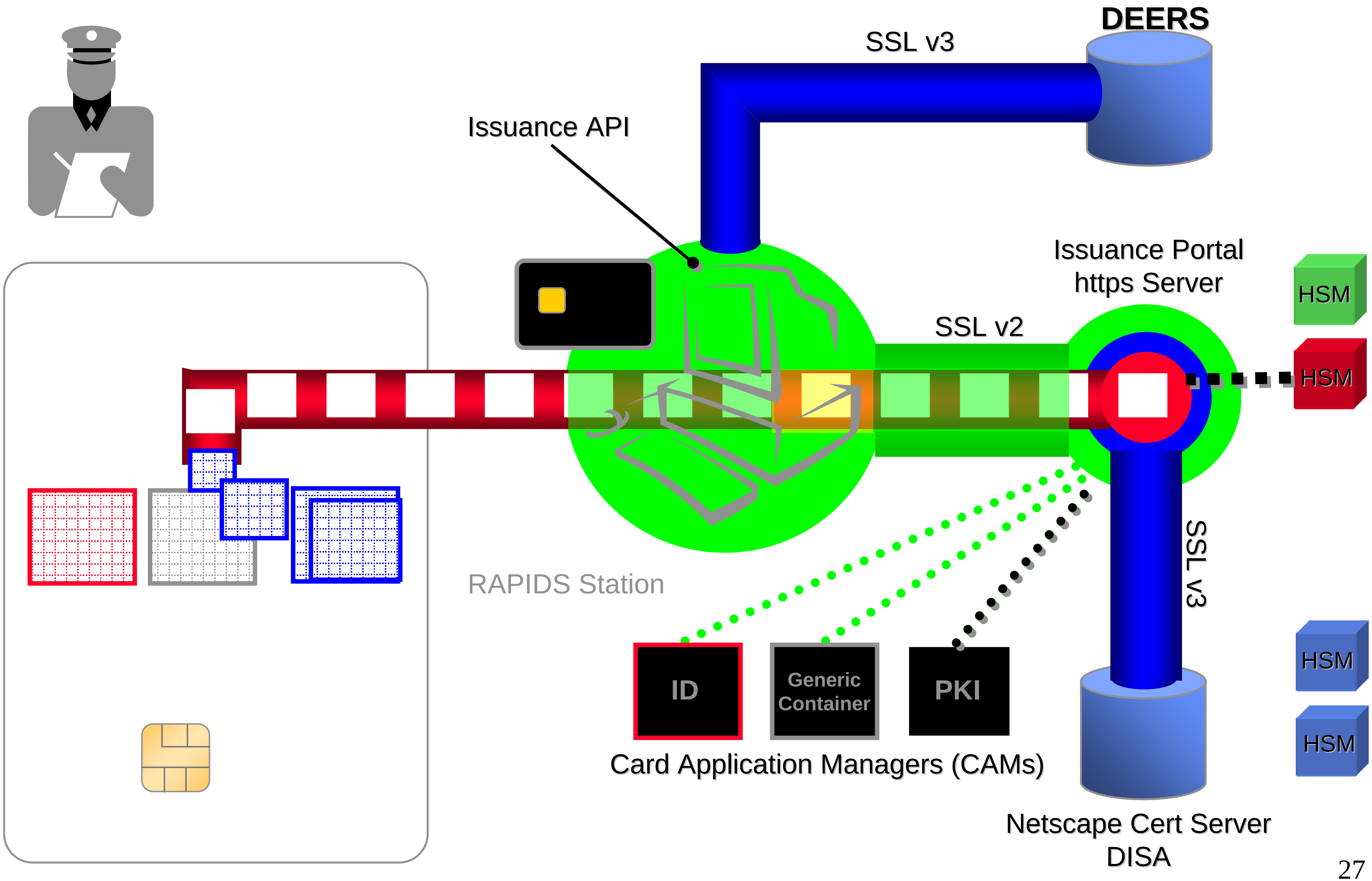
Create Card Applets - ID



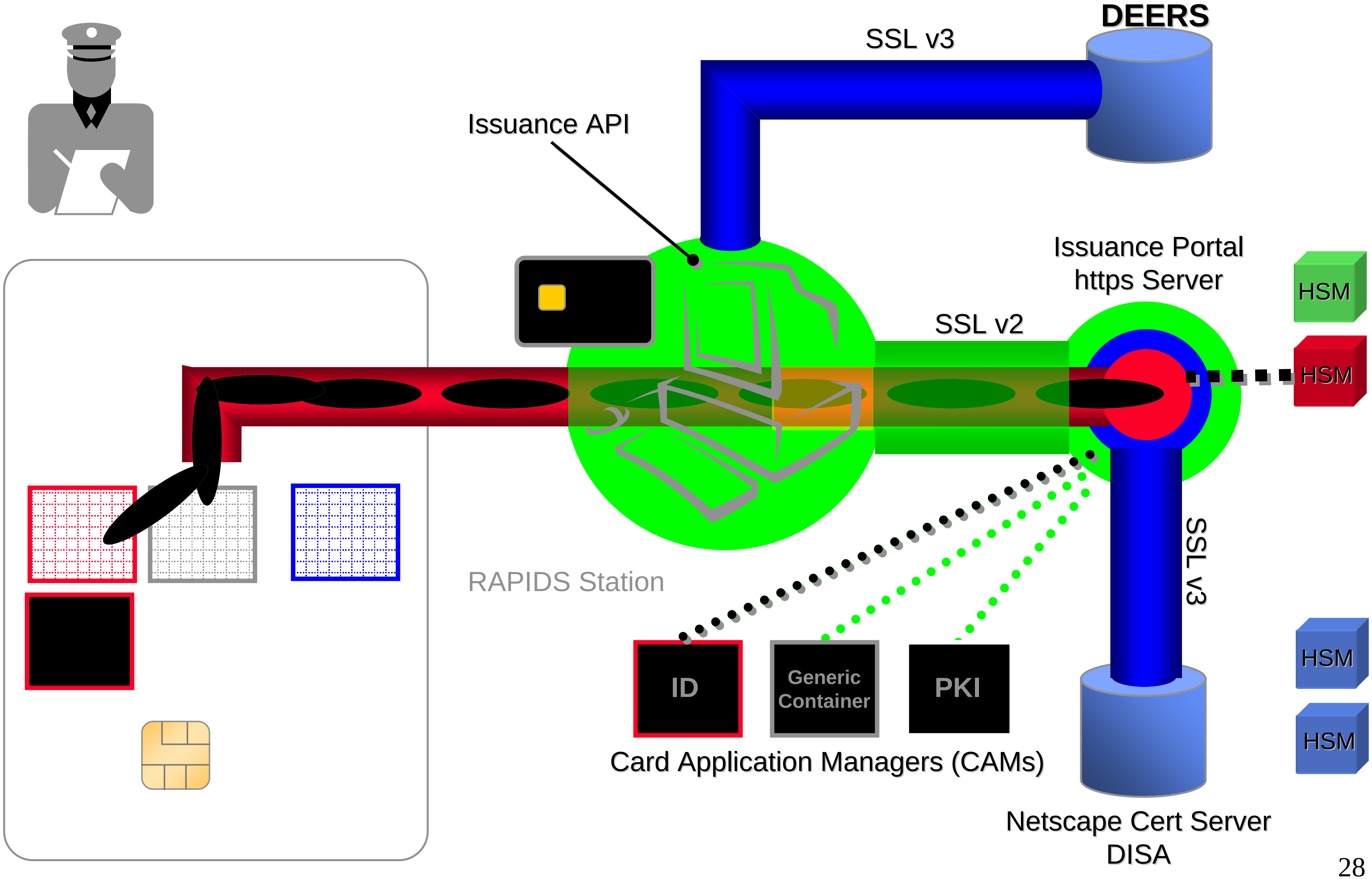
Create Card Applets – Generic Containers



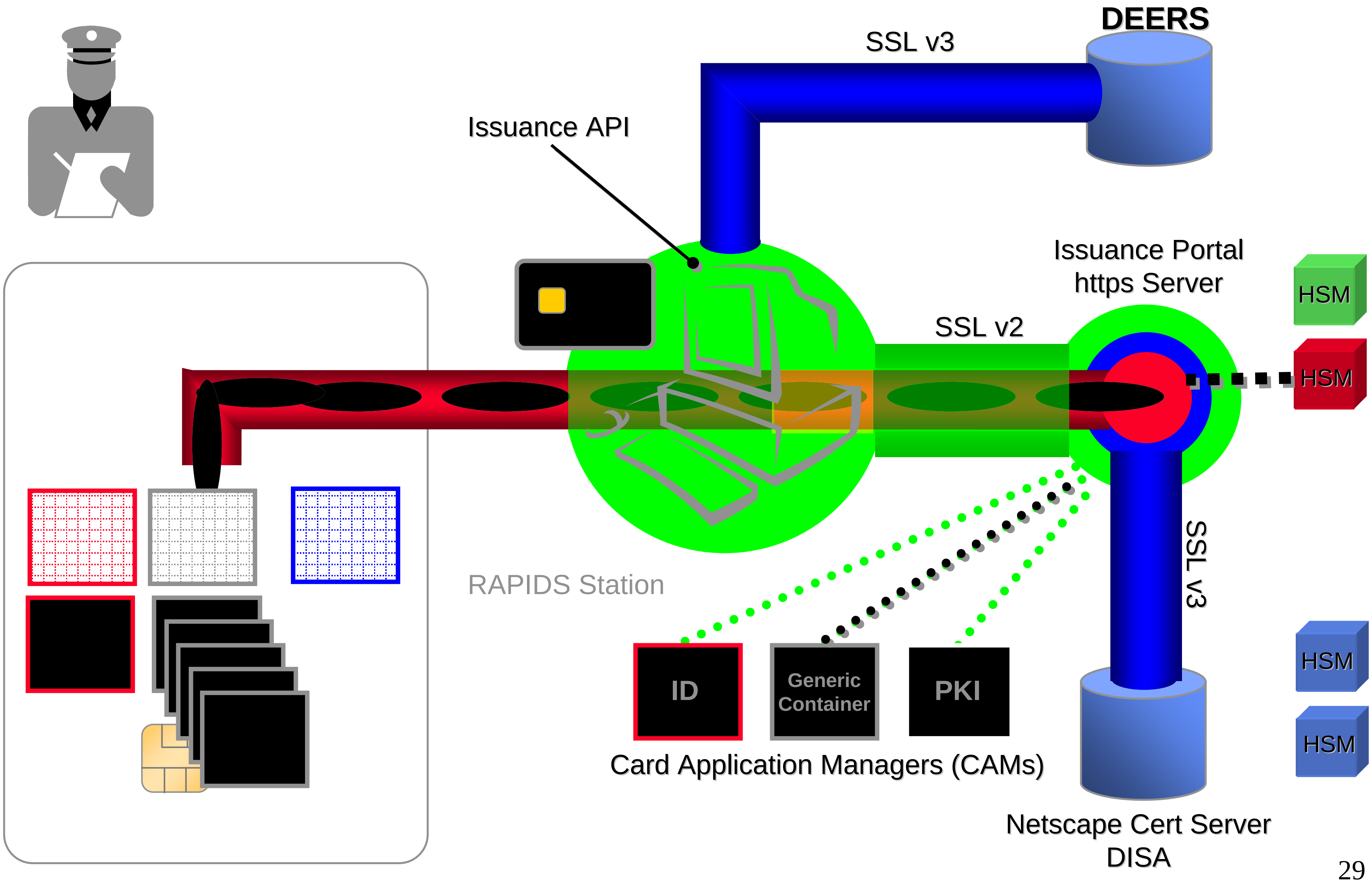
Create Card Applets - PKI



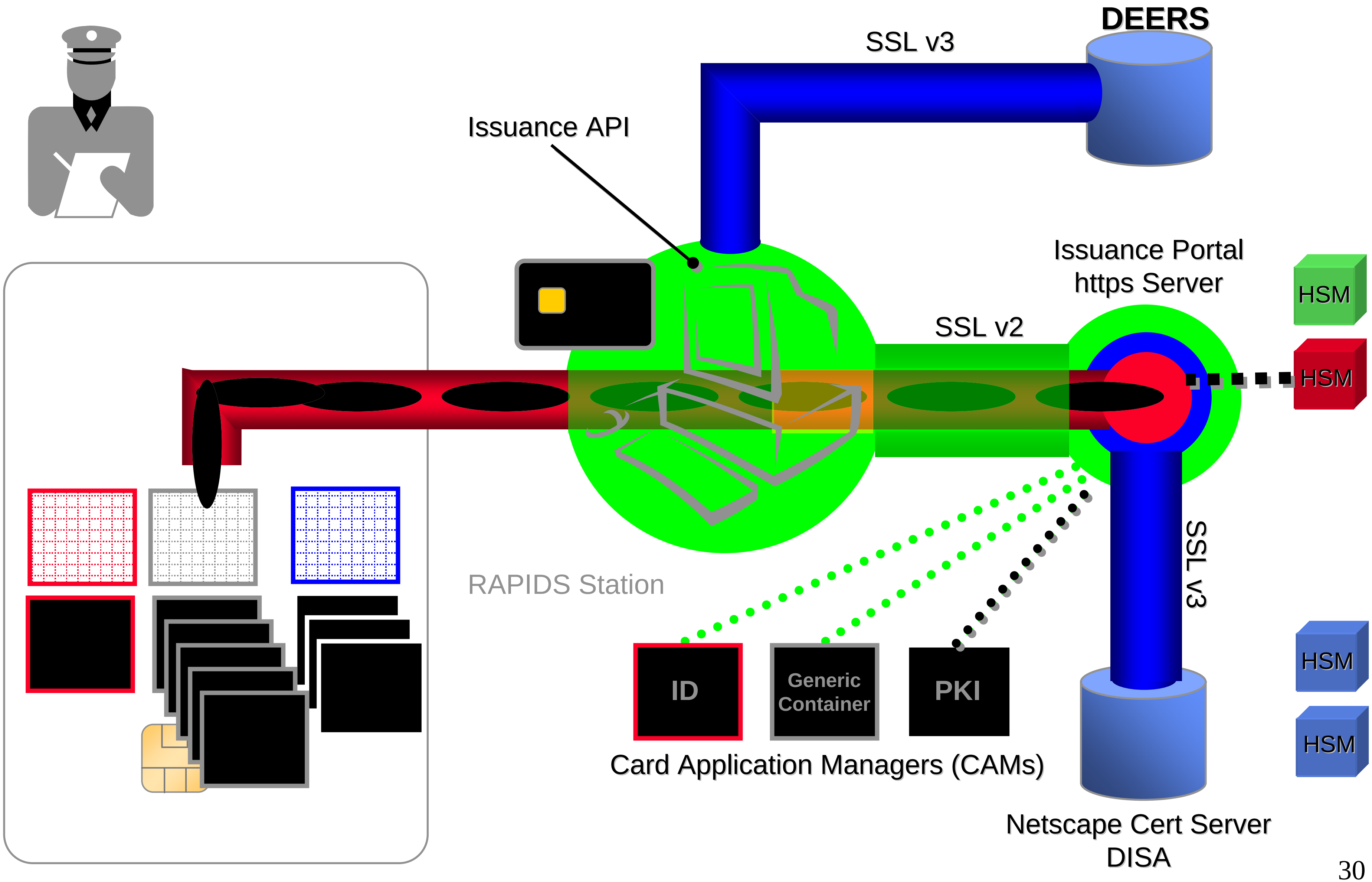
Instantiate ID Applet



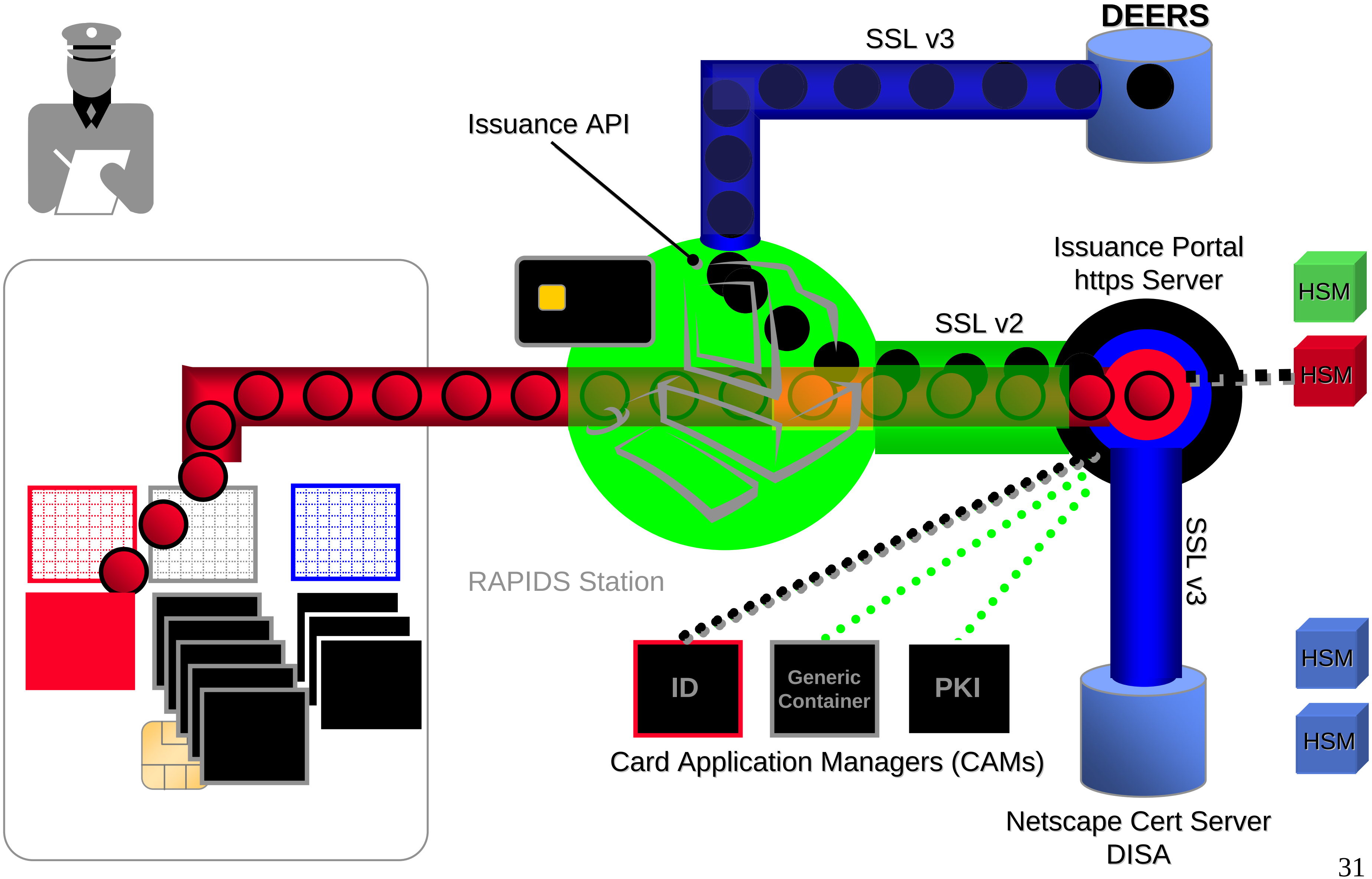
Instantiate Generic Container Applet



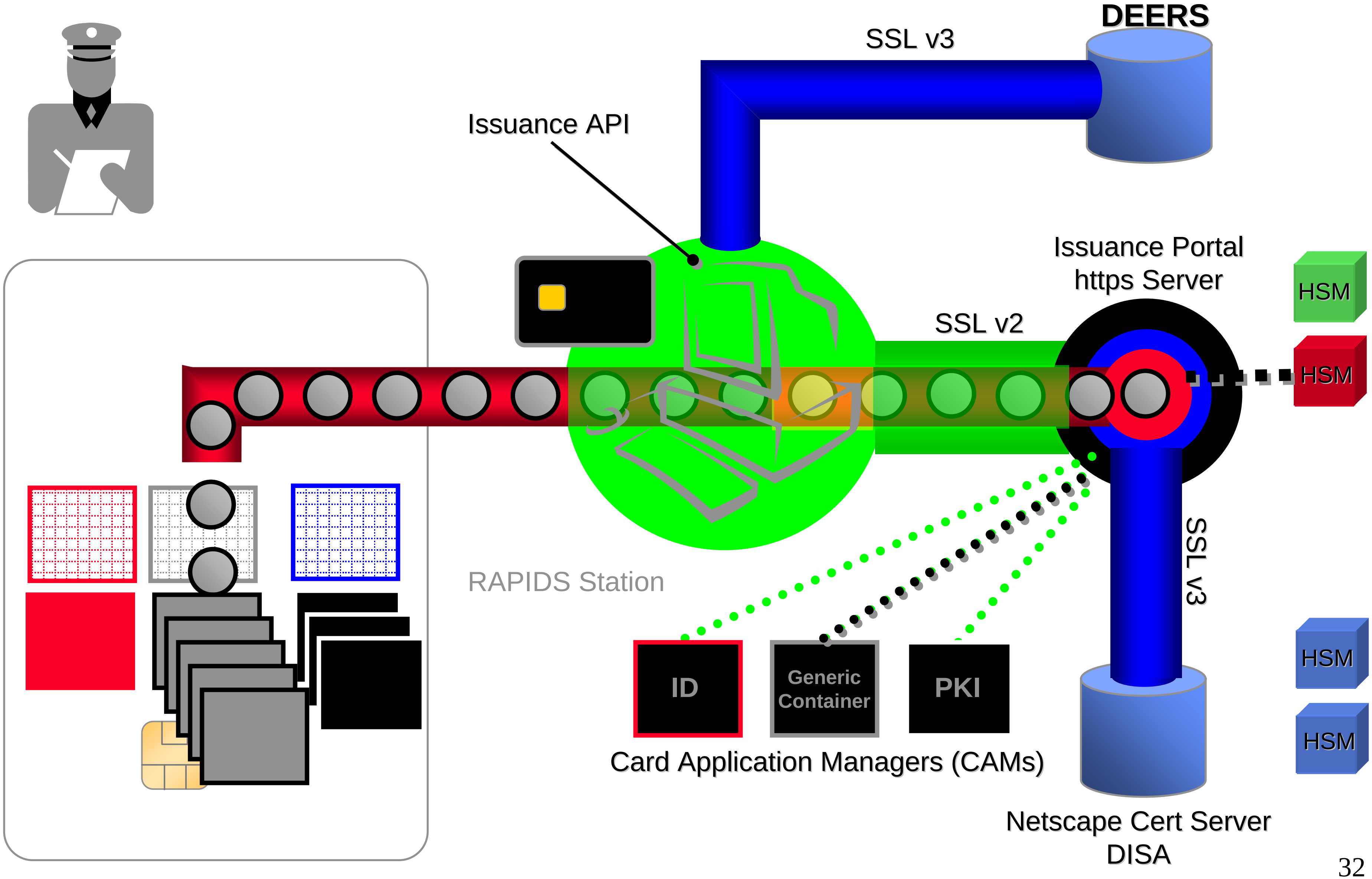
Instantiate PKI Applet



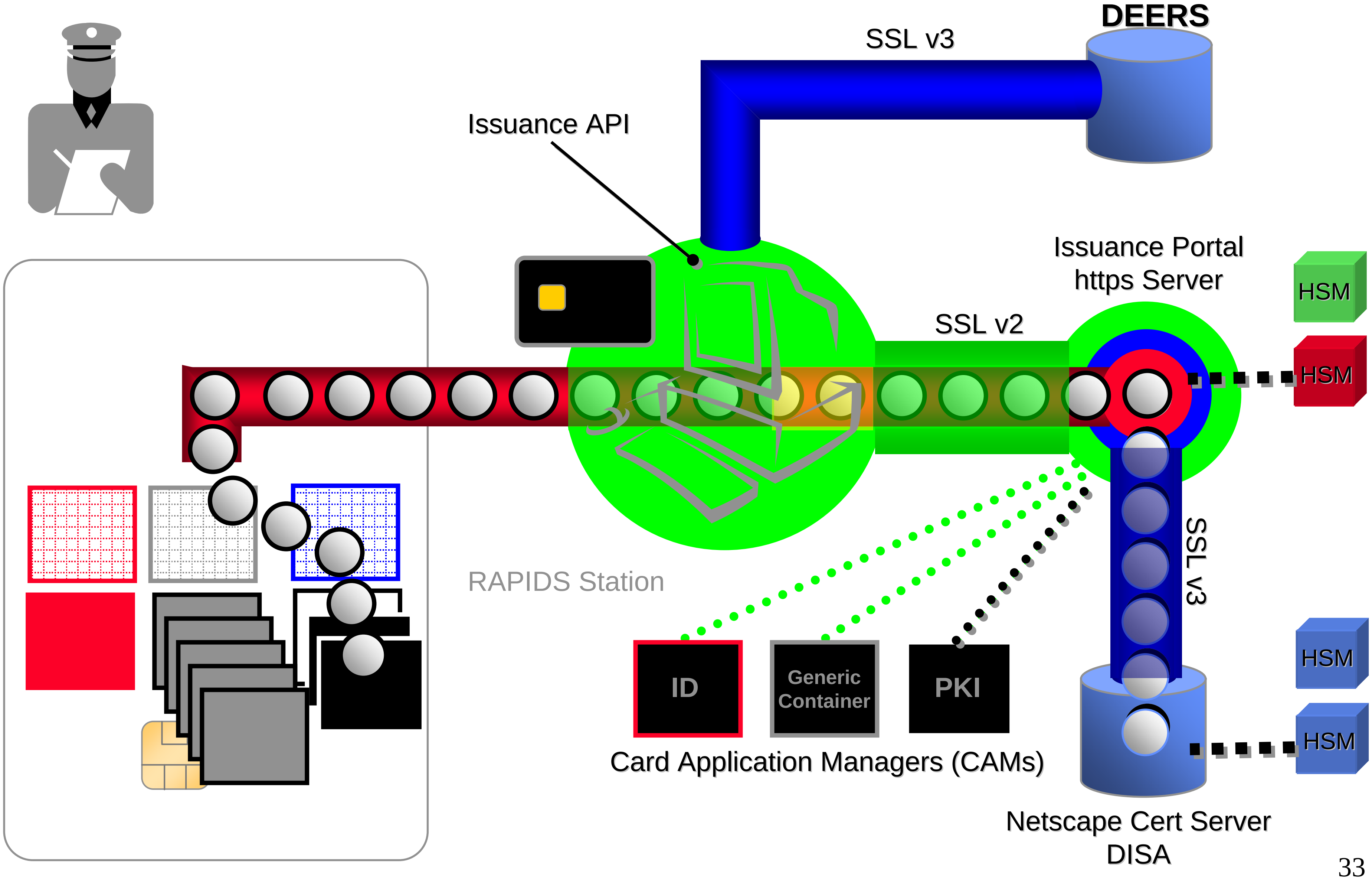
Profile, Parameters, PIN Data



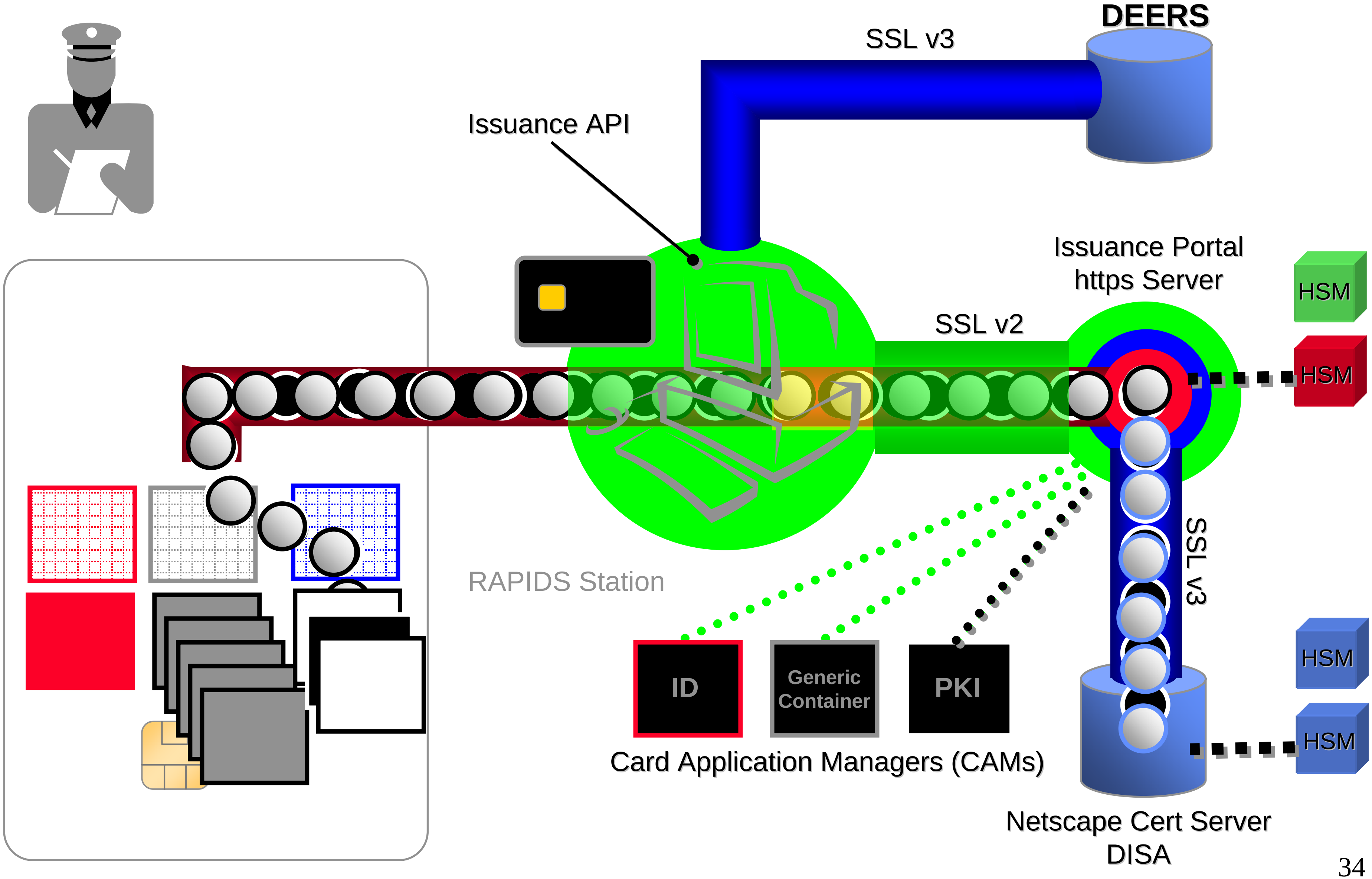
Generic Container Data



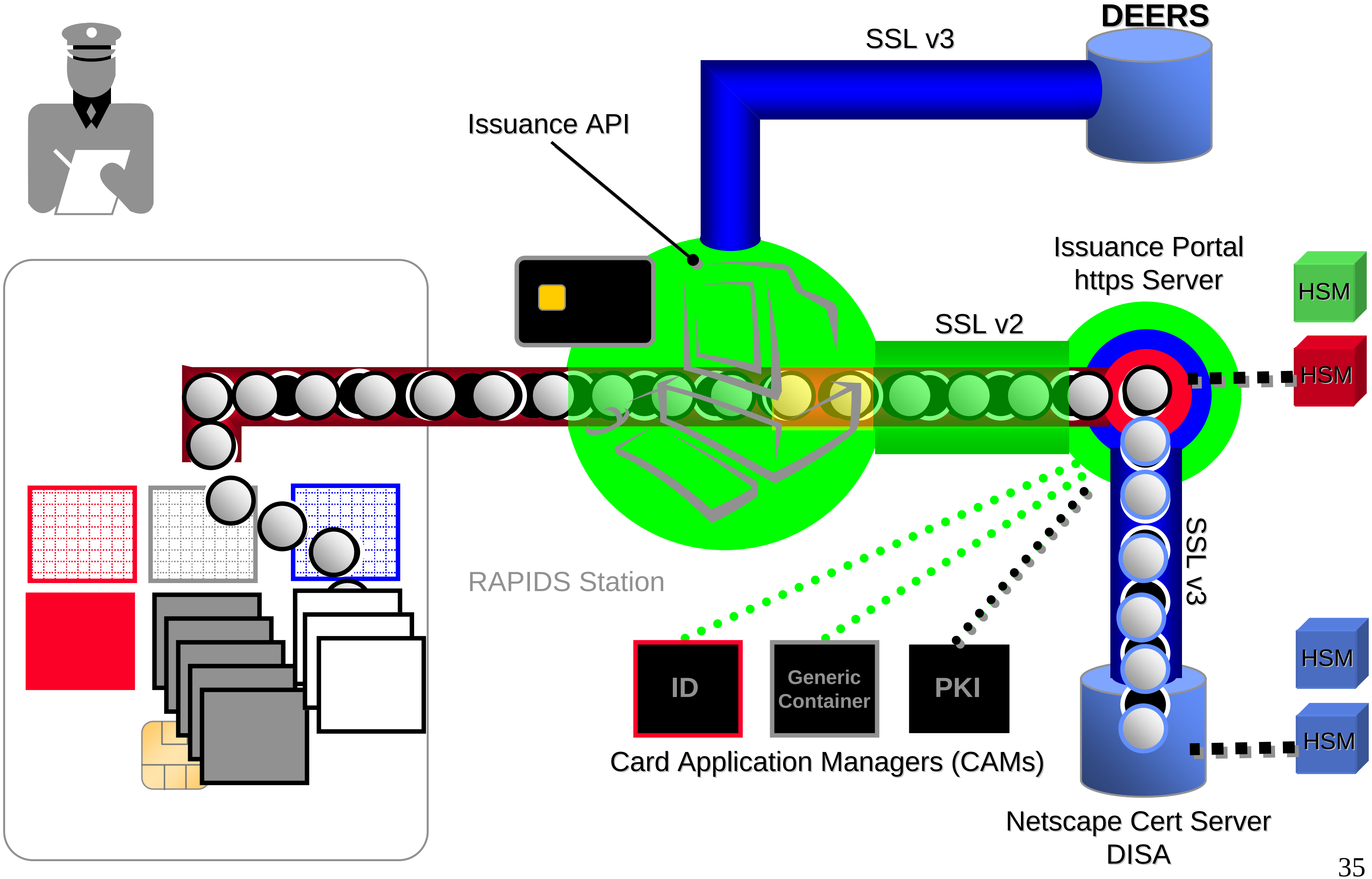
Encryption Key



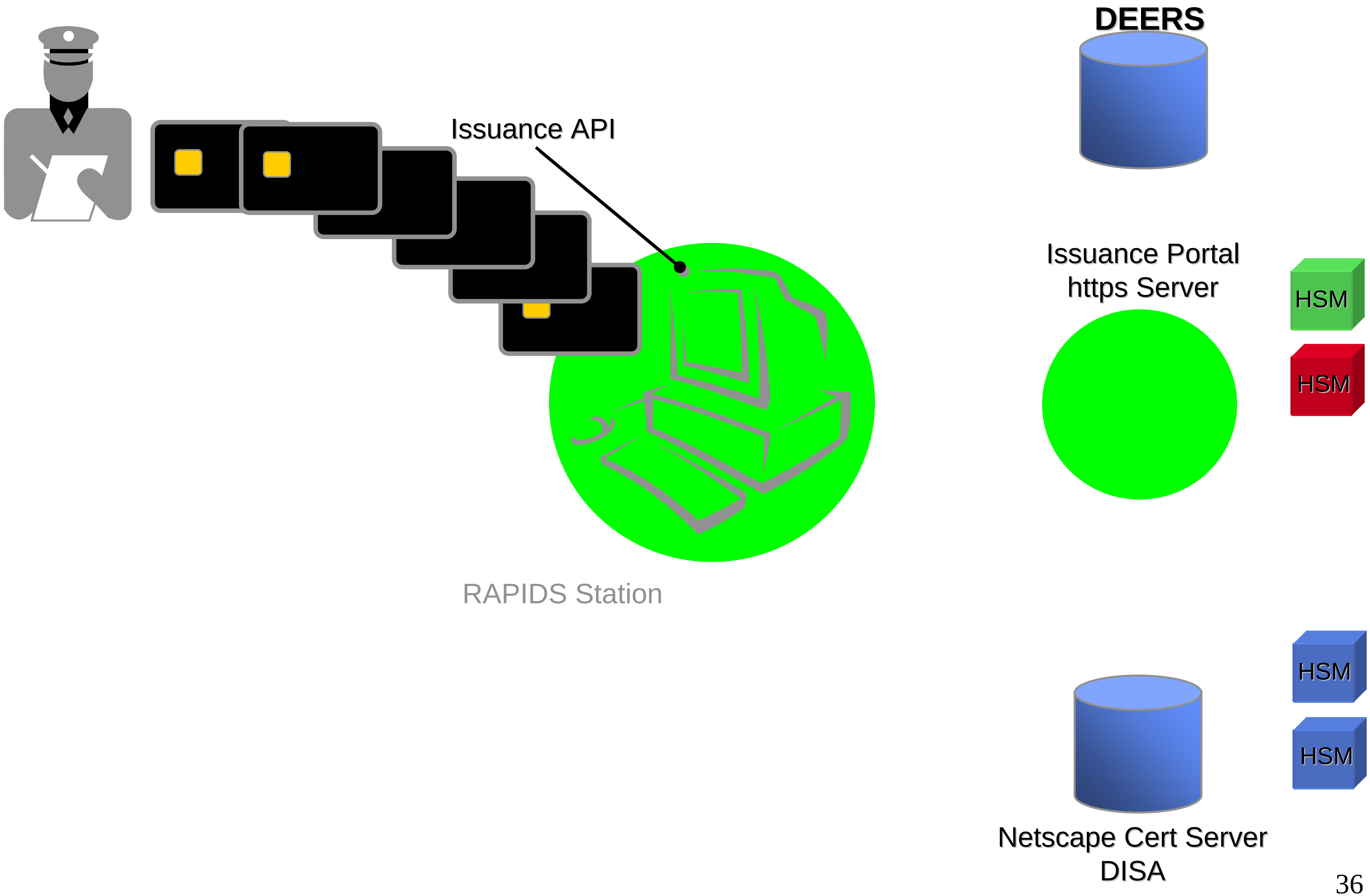
First Signature Key



Second Signature Key



Print Card



DEERS

Issuance API

Issuance Portal
https Server

HSM

HSM

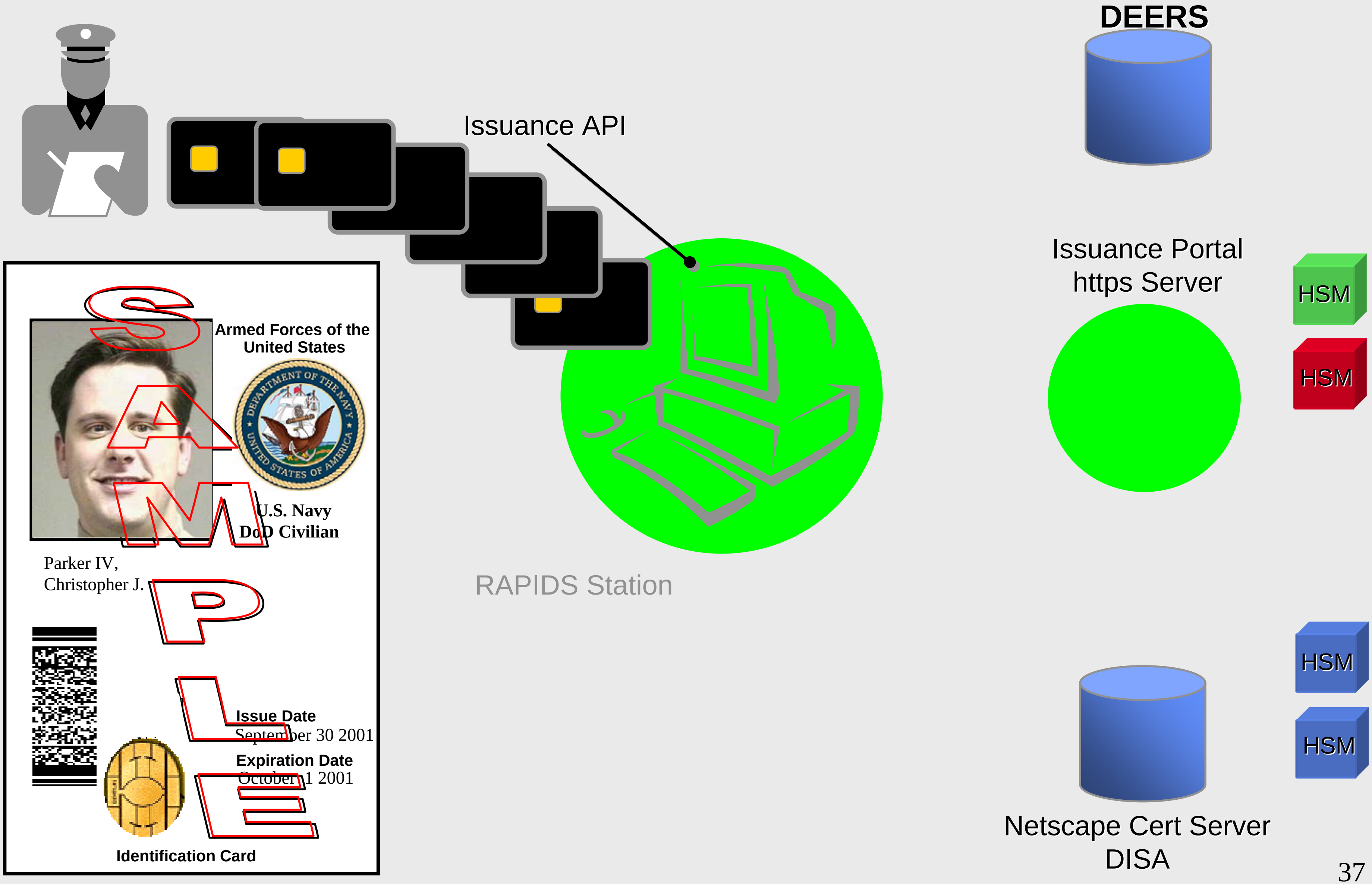
RAPIDS Station

HSM

HSM

Netscape Cert Server
DISA

Print Card



Armed Forces of the United States

U.S. Navy
DoD Civilian

Parker IV,
Christopher J.

Issue Date
September 30 2001

Expiration Date
October 1 2001

Identification Card

Interoperability

- Most interoperable solution in industry
- Standards subject to interpretation
- Industry participation

In Development

- Biometrics
- Physical Access
- Warfighter support
- Card maintenance
- Centralized issuance process

Questions?

Mary Dixon

(703) 696-7396

dixonmm@osd.pentagon.mil

www.dmdc.osd.mil/smartcard/