EPCS and Pharmacy Applications

Jerry Cox, CISSP
Jerry.Cox@IdenTrust.com

American Society for Automation in Pharmacy
2017 Annual Conference | January 8-20 | Amelia Island, FL

Disclosures

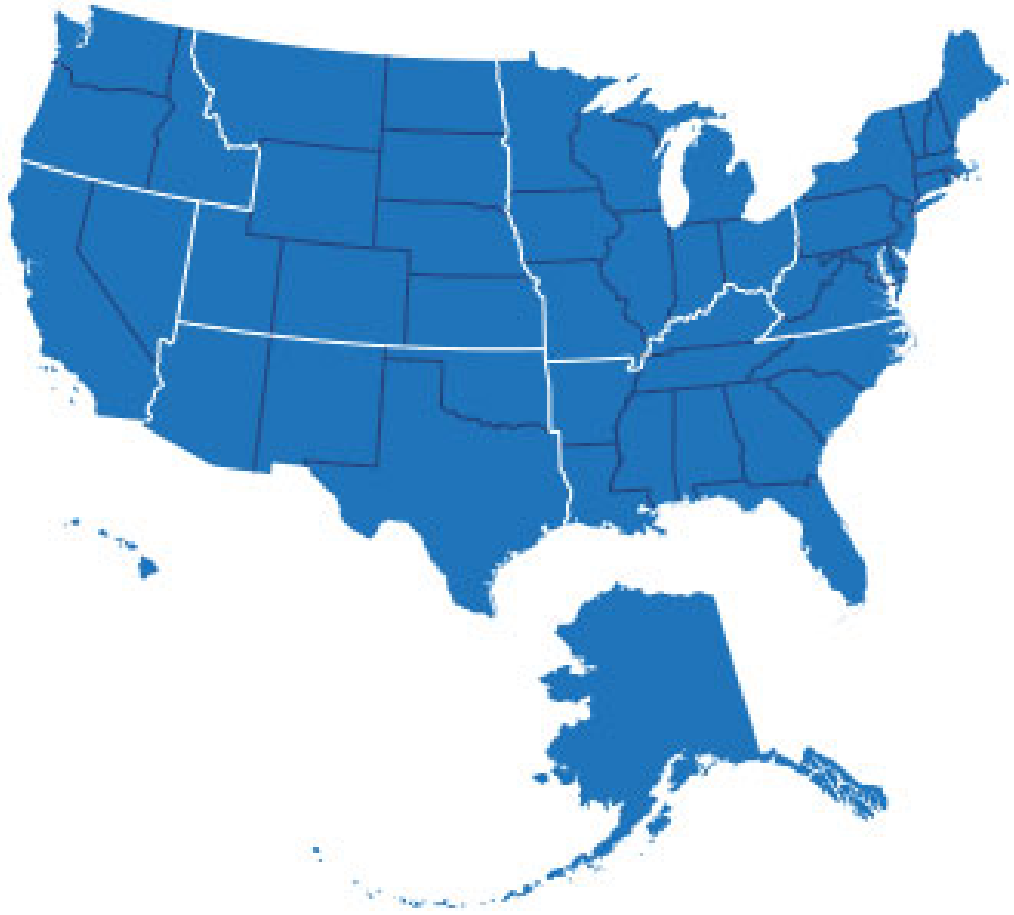
Jerry Cox is an employee of IdenTrust, Part of HID Global. The conflict of interest was resolved by peer review of the slide content. He declares no other conflicts of interest or financial interest in any product or service mentioned in this program, including grants, employment, gifts, stock holdings, and honoraria.

ASAP's and NCPA's education staff declares no conflicts of interest or financial interest in any product or service mentioned in this program, including grants, employment, gifts, stock holdings, and honoraria.

Learning Objectives

1. Describe base DEA requirements for pharmacy handling of EPCS messages.
2. State methods used for transmission of EPCS messages.
3. Describe requirements on pharmacies, based on the types of messages received.
4. Explain the linkage from DEA requirements to other NIST requirements related to digital signatures.
5. Explain what it means to validate digitally signed messages.

States in Which EPCS is Legal



States in Which EPCS is **Mandatory**

March 2016

Education law 6802 and Sections 80.67 and Title 10 NYCRR Part 80

January 2018

32 MRSA §1062-B(1)(B)

Learning Objective #1

Base DEA Requirements for Pharmacy Handling of EPCS Messages

The Focus of This Presentation is Federal Law 21CFR§1311.205, Pharmacy Application Requirements

- Set and enforce logical access controls by user or role
- ***Digitally sign or validate digital signatures on incoming EPCS messages***
- Read and retain the full DEA number of practitioner
- Archive messages

See this presentation appendix and DEA Rules*

* https://www.deadiversion.usdoj.gov/21cfr/cfr/1311/subpart_c100.htm#200

Why Do I Care?

- You don't want your customers here

- Pharmacy application providers are held accountable by DEA
  - 21CFR§1311.302

DEA fines local CVS pharmacies $22 million for filling ... - WES...
www.wesh.com/article/**dea-fines**...**pharmacies**...**prescriptions**.../4442246
May 15, 2015 - **DEA fines** local CVS **pharmacies** $22 million for filling illegitimate prescriptions. ... Federal agents and CVS **pharmacy** officials are speaking out about a $22 million **fine** the chain received for its poor **prescription** drug practices in Florida. ... The **fine** is connected to a **DEA** ...

Long-Term Care Pharmacy to Pay $31.5 Million to Settle Lawsu...
https://www.justice.gov/.../long-term-care-**pharmacy**-pay-315-million-set...
May 14, 2015 - Long-Term Care **Pharmacy** to Pay $31.5 Million to Settle Lawsuit Alleging ... The False Claims Act imposes treble damages and **penalties** for the knowing ... "**DEA** registrants are responsible to handle controlled substances in ...

Clovis Pharmacy Owner Agrees to Pay $200,000 in Civil Penal...
https://www.justice.gov/.../clovis-**pharmacy**-owner-agrees-pay-200000-ci...
Mar 21, 2016 - Clovis **Pharmacy** Owner Agrees to Pay $200,000 in Civil **Penalties** to Resolve ... Khoa Tan Huynh, owner of the Script Life **Pharmacy** in Clovis has agreed ... Act (CSA) authorizes the **Drug Enforcement Administration** (**DEA**) to ...

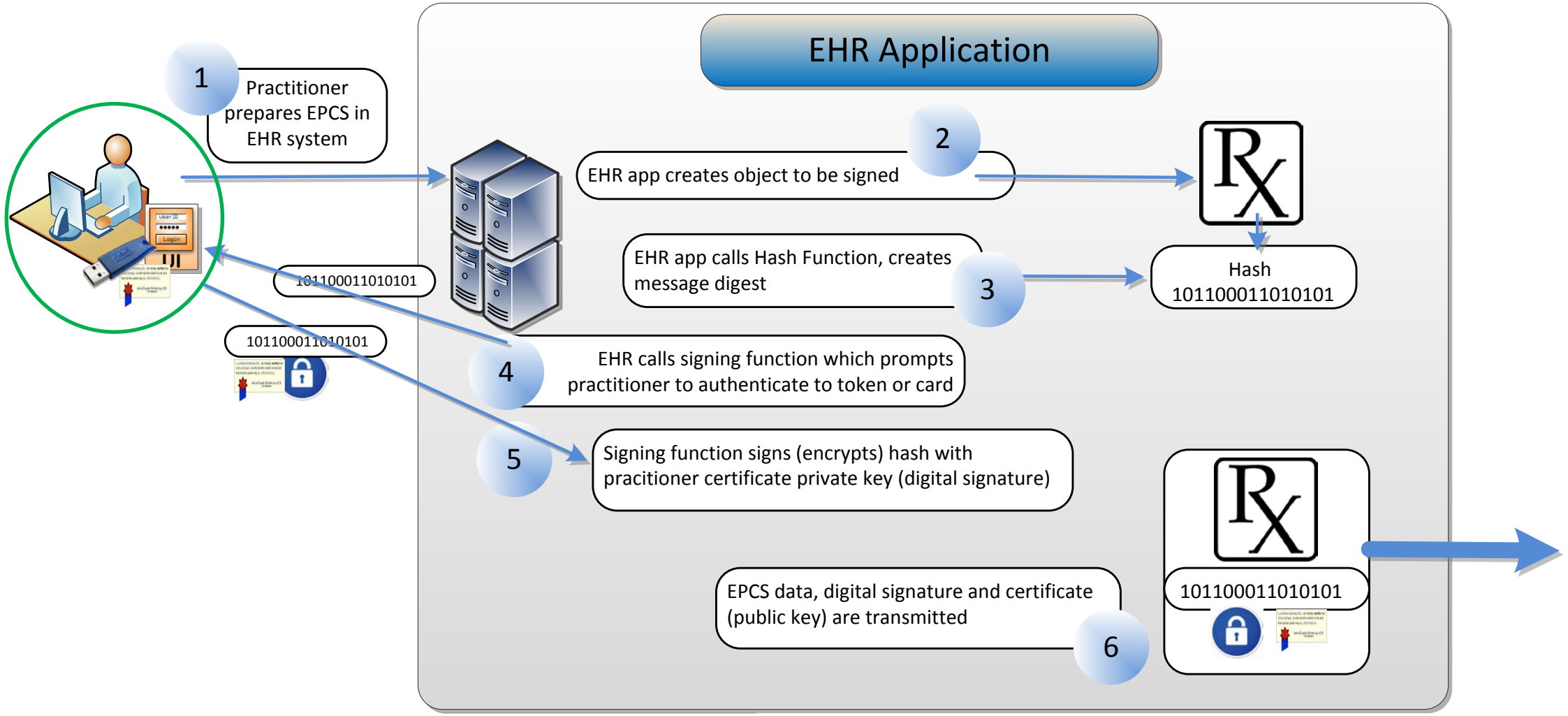
CVS to Pay $3.5 Million to Resolve Allegations that Pharmacist...
https://www.justice.gov/.../cvs-pay-35-million-resolve-allegations-**pharm**...
Jun 30, 2016 - "When **pharmacies** ignore red flags that a **prescription** is fraudulent, they ... In the first investigation, the **DEA** identified forged prescriptions filled ...

Fresno Pharmacy Agrees To Pay $1 Million In Civil Penalties T...
https://www.justice.gov/.../fresno-**pharmacy**-agrees-pay-1-million-civil-**p**...
Mar 9, 2015 - Fresno **Pharmacy** Agrees To Pay $1 Million In Civil **Penalties** To Resolve ... Cedar **Pharmacy** has agreed to pay $1 million to settle claims that it failed to ... by the U.S. Attorney's Office and the **Drug Enforcement Administration**.

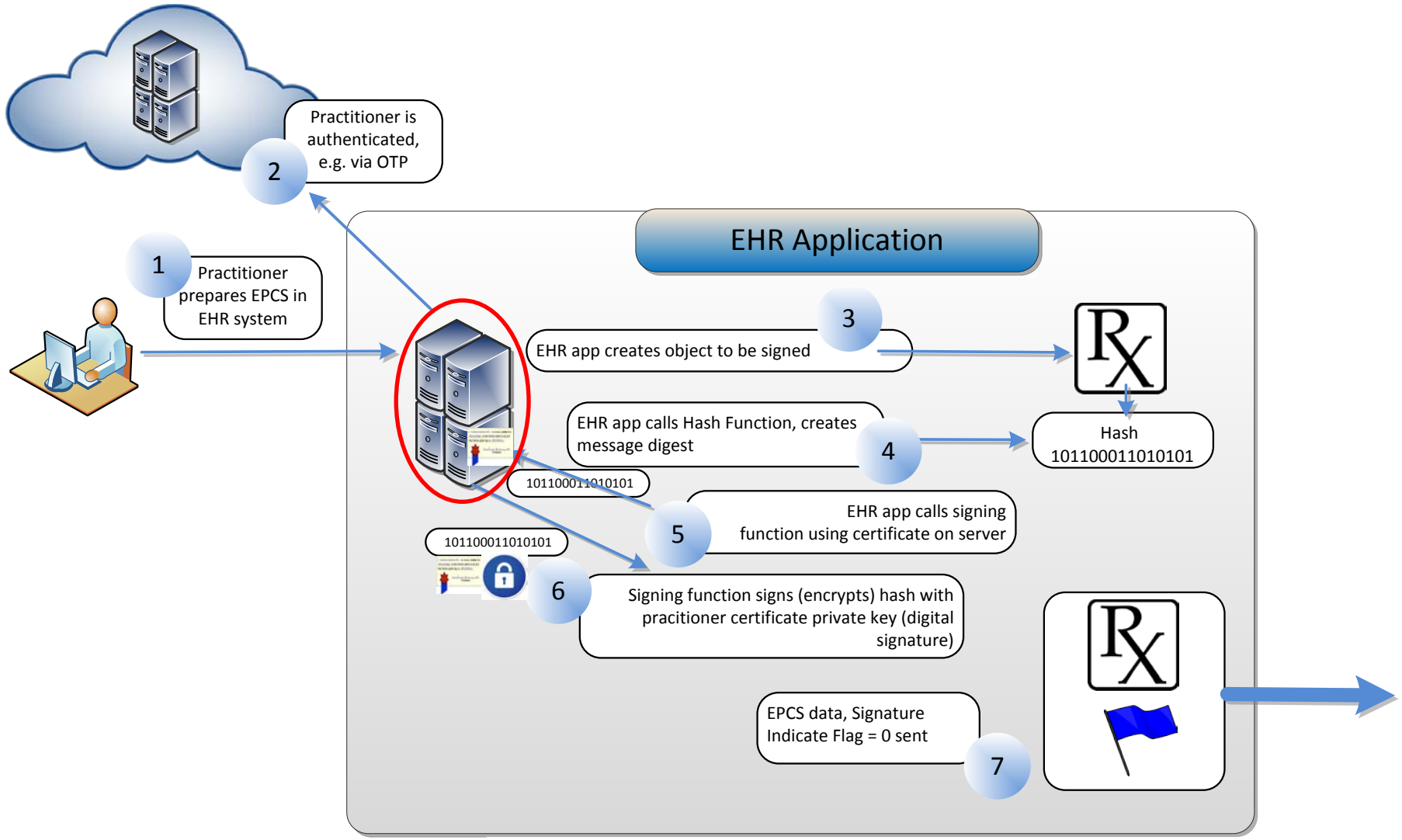
Learning Objective #2

EPCS Transmission Methods

Transmission With Practitioner's Digital Signature (EHR)



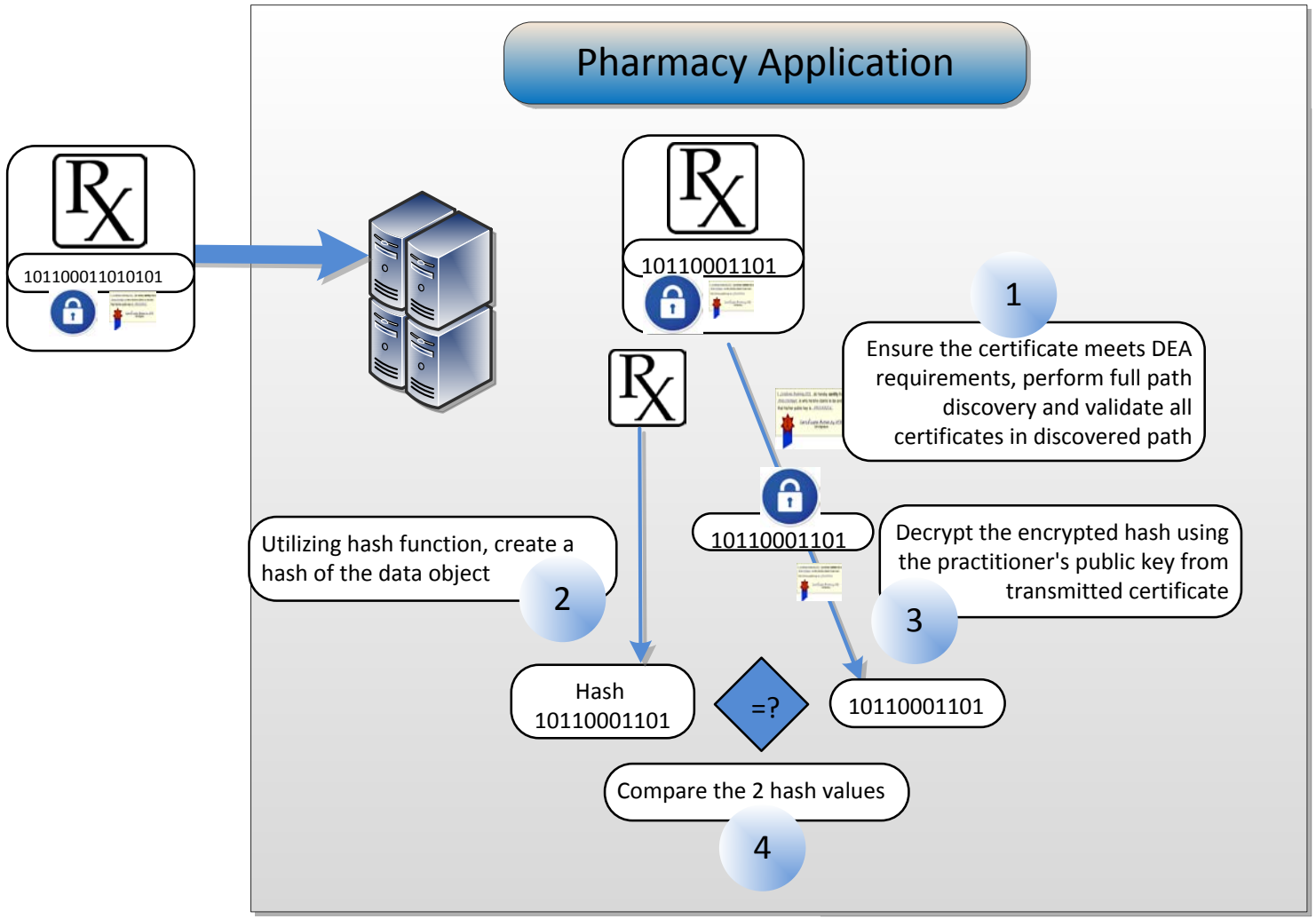
Transmission Without Practitioner's Digital Signature (EHR)



Learning Objective #3

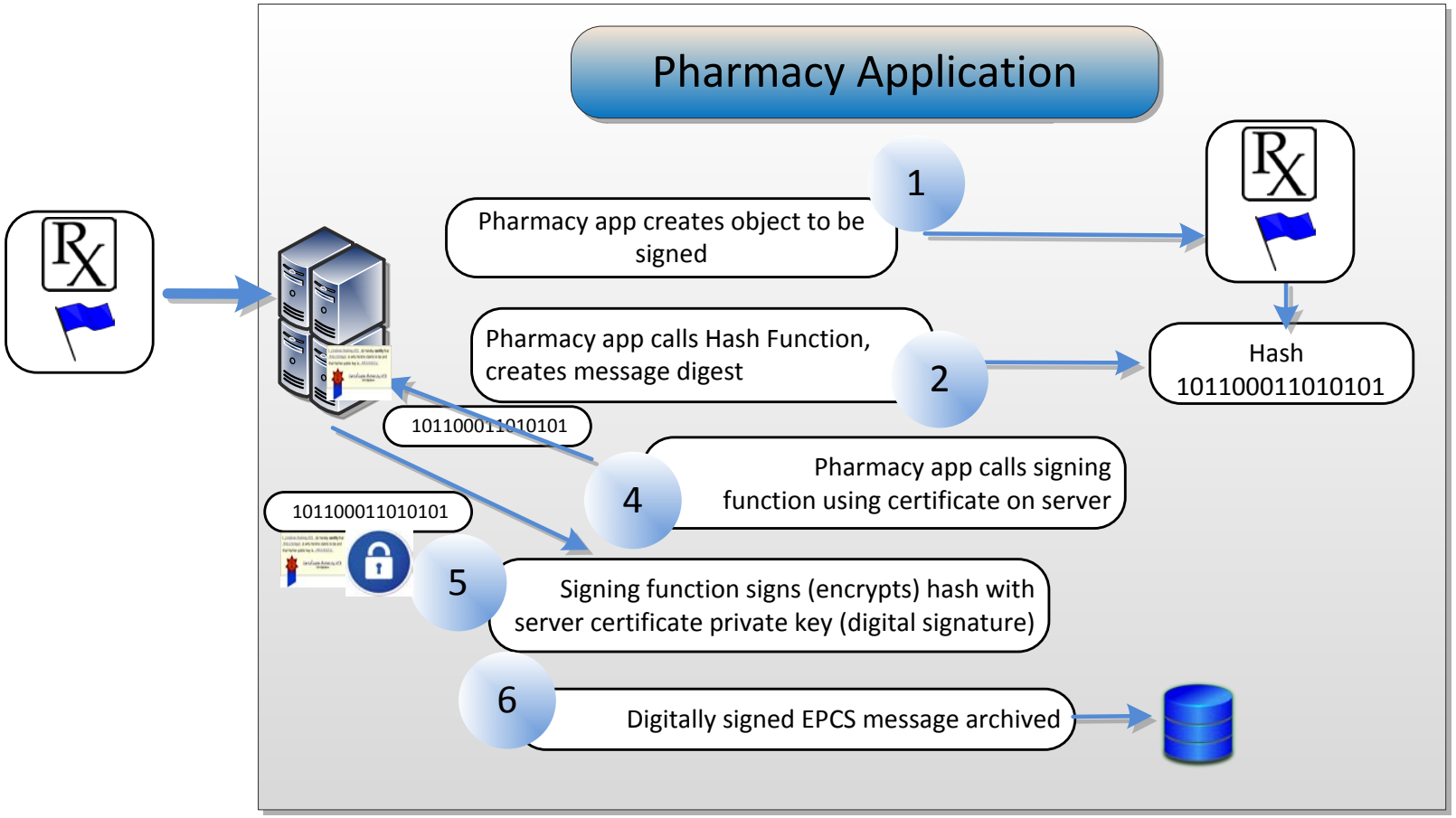
EPCS Message Handling

Receipt of Message With Practitioner Digital Signature



- EPCS messages signed with practitioner certificate are most secure
  - Non-repudiable to practitioner
  - End-to-end security
- Step #1 perceived as being difficult
  - Services exist to help

Receipt of Message Without Practitioner Digital Signature



- Nothing for Pharmacy to validate!
  - No end-to-end security
- Perceived as being easier for pharmacies
  - Must be careful to digitally sign in a compliant manner

Learning Objective #4

NIST Standard Applicability

EPCS Message Handling and NIST Standards

With Practitioner Digital Signature

- FIPS PUB 186: *Digital Signature Standard*
- Ensure certificate is valid
  - Check CRL or via OCSP
- Ensure practitioner certificate meets minimum assurance level required
  - Understand certificate OIDs
- Build certificate chain to trusted Root CA
  - Must be Federal Common CA
- Validate all CA Certificates in chain

Without Practitioner Digital Certificate

- FIPS PUB 186: *Digital Signature Standard*, NIST SP 800-57: *Recommendation for Key Management*, FIPS PUB 140: *Security Requirements for Cryptographic Modules*
- Ensure certificate keys are created with FIPS approved algorithms, meeting minimum key length requirements
- Protect certificate private key in a FIPS validated cryptomodule
- Ensure algorithms used for digital signing are FIPS approved

Learning Objective #5

Validating Digitally Signed Messages

Certificate Validation Basic Steps

Validation of digitally signed EPCS messages requires four elements:

1) Certificate Trust Anchor Discovery
    1) Determine the type of digital certificate being presented to the pharmacy application
    2) Determine whether the certificate, if validated, meets minimum DEA requirements for EPCS
2) Certificate Path Discovery
    1) Identify all intermediate certificates in path to Trust Anchor
    2) Determine exactly what process (i.e. OCSP, CRL) and path to be followed in order to validate the certificate and all intermediate certificates
3) Certificate Validation Execution
    1) Execute the validation process for the certificate presented
    2) Execute the validation process for all intermediate certificates
4) EPCS Digital Signature Validation

Validation Complexity Under the Covers

Step 1

Determine who issued the certificate – was it a DEA qualified CA?

1. Examine the certificate
2. Parse the certificate, examining for the CA issuer field
3. From the certificate, identify from where certificate authority can be directly obtained
4. Download the file at that location that contains all certificates issued to the CA
5. Extract the items needed to chain to the Federal Bridge or the entire chain for the CA Trust Anchor
6. Examine file to see if CA has been cross-certified
7. Check with the Federal Bridge to see whether still cross-certified
8. Check with Trust Anchor to determine whether still cross-certified
9. **PLUS another 15 – 35 steps depending on the Trust Anchor**

Step 2

1. Parse the certificate
2. Check the Policy OID(s)
3. Translate the Policy OID(s), utilizing trust anchor mapping to Federal Bridge certificate assurance OID(s)
4. Ensure that minimum level is Basic or above
5. **PLUS another 25 steps**

Step 3

Validate integrity of signature and message

Step 4

Check validity of certificate and signature date

Step 5

Validate the certificate attributes

Summary

- Pharmacy application providers accepting EPCS messages are obligated by law to correctly process them
- EPCS messages can arrive with or without the practitioner's digital signature
  - Message handling requirements are different
- Messages digitally signed by practitioners are more secure from end-to-end
  - More challenging to correctly process; requires validation

- Challenge:
  - Support both EPCS message types, correctly
  - Trend towards more secure EPCS messaging

Thank you!

The American Society for Automation in Pharmacy
2017 Annual Conference | Jan 8-20 | Amelia Island, FL

Appendix

The Focus of This Presentation is Federal Law 21CFR§1311.205, Pharmacy Application Requirements

Additional requirements:

- 21CFR§1311.200 Pharmacy responsibilities*
- 21CFR§1311.210 Archiving the initial record
- 21CFR§1311.215 Internal audit trail
- 21CFR§1311.300 Application provider requirements—Third-party audits or certifications
- 21CFR§1311.302 Additional application provider requirements
- 21CFR§1311.305 Recordkeeping

* https://www.deadiversion.usdoj.gov/21cfr/cfr/1311/subpart_c100.htm#200

21CFR§1311.205, Pharmacy Application Requirements (1 of 3)

- Set and enforce logical access controls by user or role for:
  - Annotation, alteration or deletion of prescription information
  - Setting and changing the logical access controls
- Digitally sign or validate digital signatures on incoming EPCS messages
- Read and retain the full DEA number including the specific internal code number assigned to individual practitioners
  - Incorporates 21CFR§1301.22(c)
- Read and store, and be capable of displaying, all information required by 21CFR§1306

21CFR§1311.205, Pharmacy Application Requirements (2 of 3)

- Provide for the following information to be added or linked to each EPCS record for each dispensing:
  - Number of units or volume of drug dispensed
  - Date dispensed
  - Name or initials of the person who dispensed the prescription
- Be capable of retrieving controlled substance prescriptions by practitioner name, patient name, drug name and date dispensed
- Allow downloading of prescription data into a database or spreadsheet that is readable and sortable
- Maintain an audit trail for specific events, capturing specific information, detail at 21CFR§1311.205(13)(14), 21CFR§1311.215

21CFR§1311.205, Pharmacy Application Requirements (3 of 3)

- Conduct internal audits and generate reports on any of the events specified in 21CFR§1311.215 in a format that is readable by the pharmacist (generally automated)
- Protect the stored audit records from unauthorized deletion and prevent modifications to the audit records
- Back up the EPCS records daily
- Archive EPCS records electronically for at least two years, detail at 21CFR§1311.210 and 21CFR§1311.305
- Third party audit / certification of application in accordance with 21CFR§1311.300