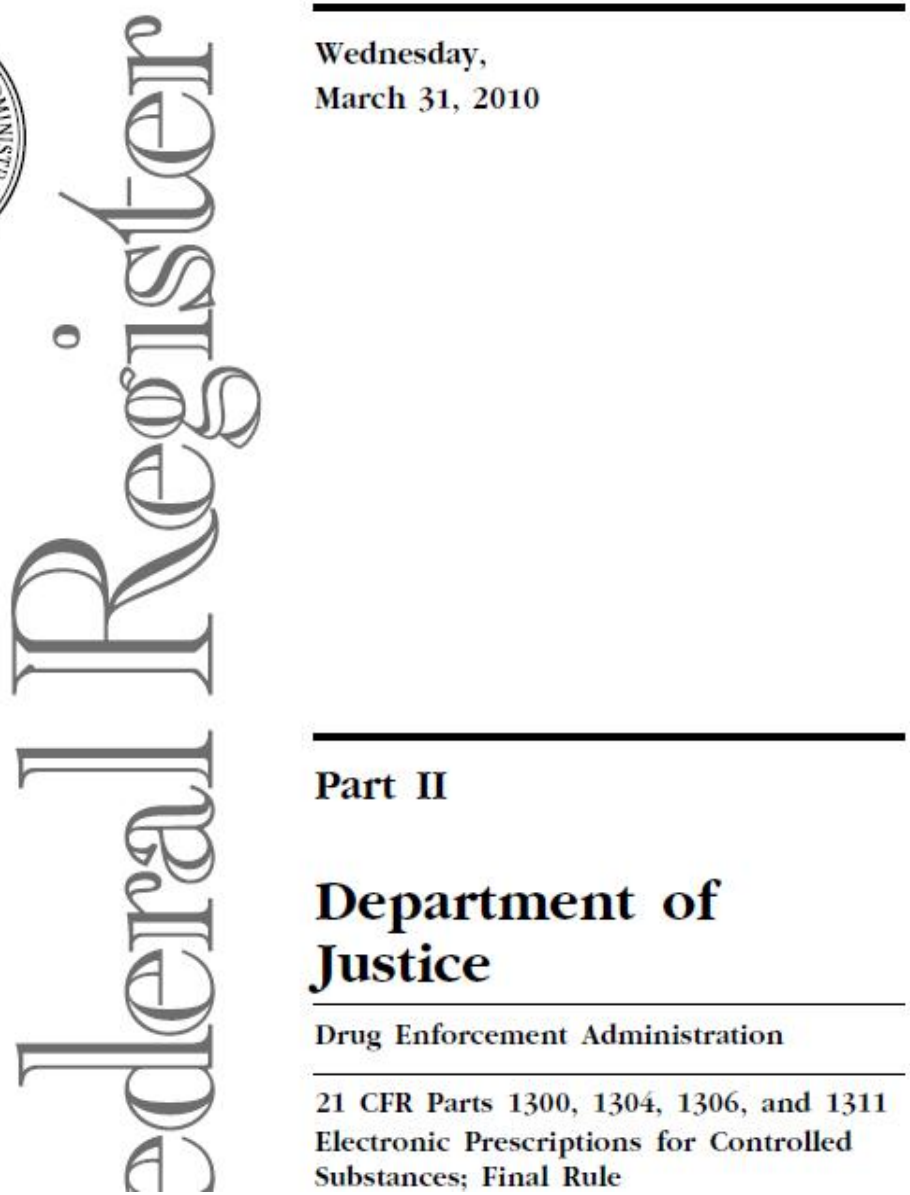
SAML for EPCS

(Electronic Prescription of Controlled Substances)

Discussion Slides for review in the OASIS Security Services (SAML) TC

August, 2014

DEA Regulation



Compliance with New York's "iStop" law- requires all prescriptions to be ePrescribed in NY by March 27, 2015

Source: http://www.gpo.gov/fdsys/pkg/FR-2010-03-31/pdf/2010-6687.pdf

Excerpt from the EPCS Rule

Based on DEA's concerns, certain requirements must exist for any system to be used for the electronic prescribing of controlled substances:

• *Only DEA registrants may be granted the authority to sign controlled substance electronic prescriptions.* The approach must, to the greatest extent possible, protect against the theft of registrants' identities.

• *The method used to authenticate a practitioner to the electronic prescribing system must ensure to the greatest extent possible that the practitioner cannot repudiate the prescription.* Authentication methods that can be compromised without the practitioner being aware of the compromise are not acceptable.

• *The prescription records must be reliable enough to be used in legal actions* (enforcing laws relating to controlled substances) without diminishing the ability to establish the relevant facts and without requiring the calling of excessive numbers of witnesses to verify records.

• The security systems used by any electronic prescription application must, to the greatest extent possible, *prevent the possibility of insider creation or alteration of controlled substance prescriptions.*

Engineering View of the EPCS Rules

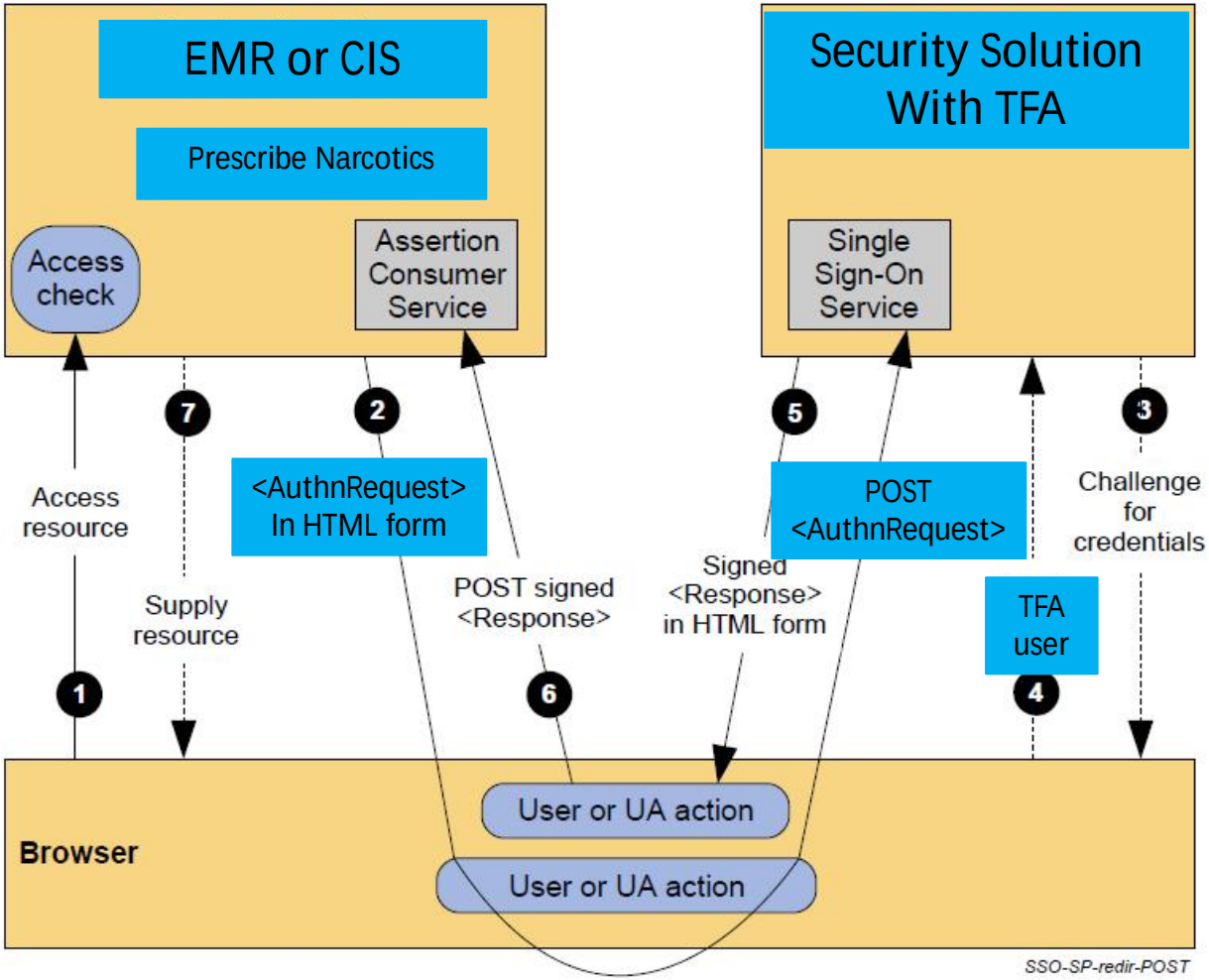
- TFA (Two Factor Authentication) for 2 workflows
  - Provisioning process and assigning EPCS capability to designated individuals
  - Prescribing of controlled substances
- TFA with strong authentication
  - One-time password
  - Biometric (i.e. fingerprint)
  - Smartcard with PIN
- NIST FIPS 140-2 Security Level 1 (http://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)
- Auditing:
  - Setting/changes to access controls,
  - ePrescription signed/created/transmitted
  - ePrescription transmission failures
- Digital signing of the prescriptions
- Secure transmission

Vendors

- Electronic Medical Records (EMR) & Clinical Information Systems (CIS)
  - Provide functionality for use by clinicians to maintain and manage a patient medical record
  - Provide ordering functionality for medications
- Single Sign-On (SSO) and Security Systems
  - Support for various authentication factors
  - Used in many industries, including Healthcare

Solution for EPCS

Leverage SAML Web SSO Profile/HTTP Post Binding



SAML SP Initiated (Source: SAML Technical Overview)

EPCS Request/Response Specifics

- SAML SP requests a TFA for a controlled substance prescription
  - Needs to be certified to perform this function
  - EMR/CIS does not know what the devices are that are used within a particular environment; it requests an “EPCS” DEA compliant workflow
- SAML IdP performs a TFA and responds with a success if a DEA EPCS compliant authentication can be performed
  - Needs to be certified to perform this function
  - Performs the TFA from devices conforming to the DEA requirements
  - Responds with the authentication modalities used
- Various existing SAML constructs are used to express the subject and other metadata on the request and response; these are not discussed here since they use the standards as-is

Additional Context Info (1)

The AuthnRequest uses the following *RequestedAuthnContext / AuthnContextDeclRef* information to request an EPCS workflow:

- urn:oasis:names:draft:SAML:2.0:ac:workflows:EPCS

This value indicates to the SAML Identity Provider that a two factor authentication is required that conforms to the DEA requirements.

ForceAuthn is set to true, which should force an authentication request (and NOT leverage existing context).

Additional Context Info (2)

The SAML Response shall contain the actual used modalities of authentication in *AuthnStatement/AuthnContext/AuthnContextClassRef* elements.

The SAML Response shall contain an *AuthnStatement/AuthnContext/AuthnContextDeclRef* element

containing the *RequestedAuthnContext/AuthnContextDeclRef* from the authentication request.

The following authentication mechanisms are identified for EPCS:

PIN (if complexity is high enough)

- urn.oasis:names:draft:SAML:2.0:ac:classes:PIN

Fingerprint

- urn.oasis:names:draft:SAML:2.0:ac:classes:Biometric:Fingerprint

ID Token

- urn.oasis:names:draft:SAML:2.0:ac:classes:OneTimePassword

Smart Card

- urn.oasis:names:tc:SAML:2.0:ac:classes:X509

Other Considerations (1)

- How to model multifactor authentication in SAML?
  - suggestion: to use a separate authentication statement in the assertion for each auth. factor, e.g. one for “fingerprint” and one for “smart card” which results in 2-factor authentication biometrics fingerprint+SC
- Definition of AuthnContextClasses for biometric modalities
  - fingerprint,palm, iris, face, etc.
- if biometrics are used for authentication it is important to distinguish verification (1:1) and identification (1:n)
  - definition of AuthnContextClass for Verification and one for Identification and adding it to the assertion like the authentication factors?
- How to express the need of a certain authentication need in the SAML request?
  - either by requesting a specific workflow -> like EPCS
  - or by requesting authentication of certain strength which would need concept to categorize the different authentication methods into a certain strength factor in the SAML standard e.g. categorization by Know, Have, Have One Time, Be – [biometrics]
  - biometrics need to be distinguished by their strength again and verify, identify was applied

Other Considerations (2)

- More specific definition of the subject
  - In the EPCS use case, the Subject is a clinician identified by a username
  - Many customers use Active Directory (UPN or sAMAccount) or an application specific username
- More specific definition of username mapping
  - Use of the SPProvidedID construct
- How to exchange certificates
  - Manual setup or automated setup?
  - Self-signed or CA?

Questions & Next Steps

Contact: Alex DeJong (alex.dejong@siemens.com)