



FPKI in Healthcare

Scott Rea,
VP GOV/EDU Relations & Sr. PKI Architect,
DigiCert, Inc.

What is Direct?

- Direct exchange is part of a long term national strategy to transition from paper-based to electronic health care records that can be shared more easily to reduce costs and improve the quality of patient care.
- The Office of the National Coordinator (ONC) within the department of Health and Human Services (HHS) is the lead author and publisher of the Direct standard
- Direct was also designed to support the goal of health information exchange between providers using electronic health records (EHRs) engaged in Meaningful Use, the Medicare and Medicaid programs that help providers to pay for and meaningfully use EHRs.
- The Center for Medicare and Medicaid Services (CMS) governs the Incentive Programs for the use of EHRs
- Direct is also intended as a general means of secure exchange (both directions) between providers and patients.

Direct Technology

- The Direct protocol enables SMIME messages with disposition notification within dedicated healthcare domains
- Sender and receiver must both have SMIME certificates of which there are 2 types:
 - Direct Address cert is traditional SMIME
 - RFC822name in subjectAltName
 - Direct Organization cert is like SMIME wildcard
 - DNSname (FQDN of mail domain) in SAN

Direct Technology

Direct Address

- Direct Addresses are used to route information
 - Look like email addresses
 - Used only for health information exchange

b.wells@direct.aclinic.org



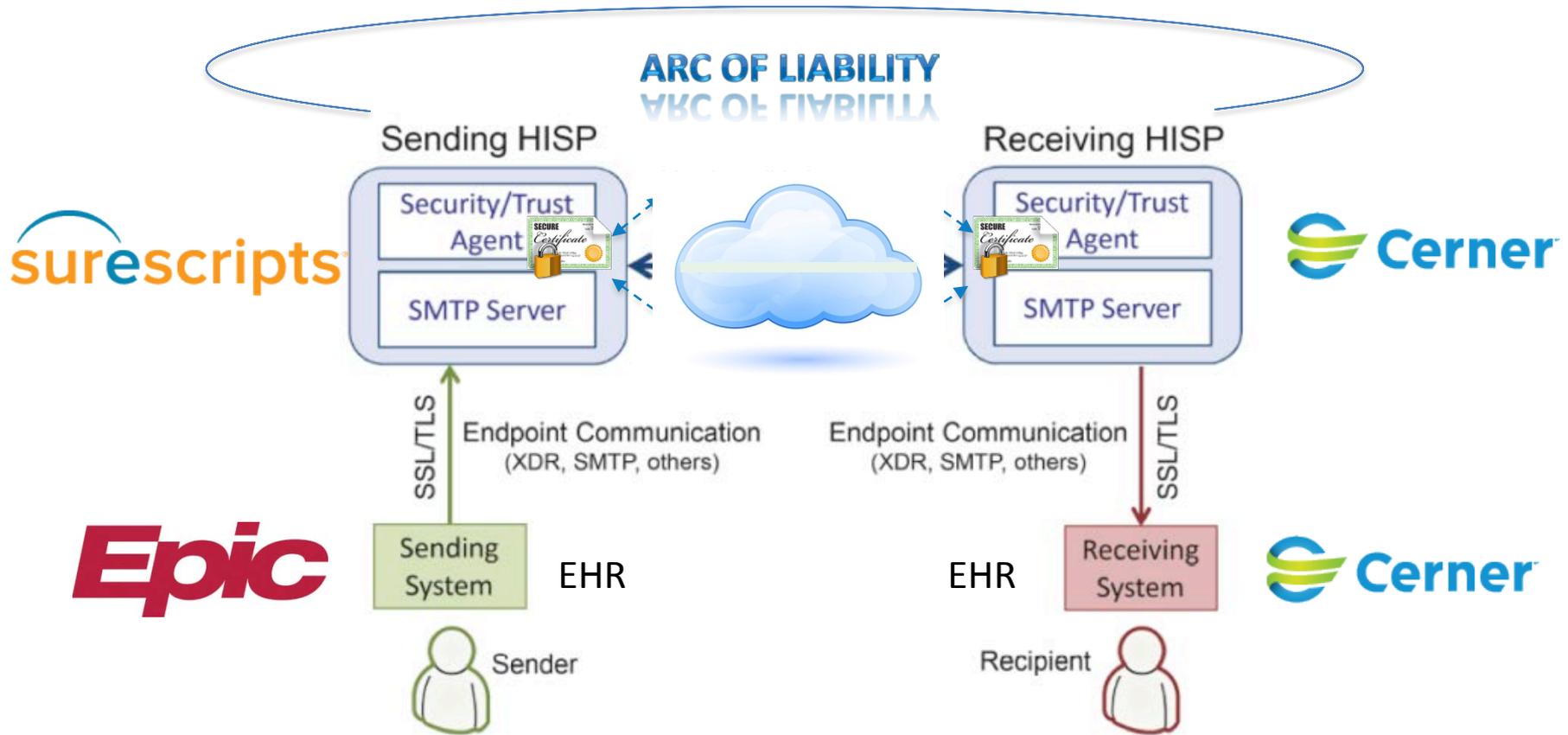
The diagram shows the structure of the Direct Address `b.wells@direct.aclinic.org`. It is underlined in blue. Below the address, there are three brackets: a top-left bracket under `b.wells` labeled "Endpoint", a top-right bracket under `direct.aclinic.org` labeled "Domain", and a bottom bracket under the entire address labeled "Direct Address".

- An individual may have multiple Direct addresses

Health Information Service Provider

- Direct introduces the concept of a Health Information Service Provider (HISP)
- The purpose of the HISP is to primarily operate the STA functions on behalf Direct Users
- The role of a HISP is to alleviate the difficulties of implementing the nuts and bolts of PKI e.g. managing private keys and publishing address-to-certificate bindings; and those controls required by Direct in addition to standard SMIME e.g. Message Disposition Notices (MDN)
- Direct can however, be used without a HISP, if an individual wishes manage their own keys and provide the appropriate MDN responses

Direct Implementation



DrBob@direct.familypractice.com
(has been identity vetted, has X.509
Digital certificate bound to address.)

DrSusan@direct.cardiology.com
(has been identity vetted, has X.509
Digital certificate bound to address.)

DirectTrust

- To facilitate Directed Exchange among healthcare community in a trusted manner, a trade association called DirectTrust was formed
- DirectTrust established a PKI based trust framework to facilitate Directed Exchange among its members. Policies utilized were based upon a template of the FBCA CP
- DirectTrust is a non-profit national industry alliance of 140+ organizations that is supporting Direct exchange adoption and use through policy setting, accreditation, trust anchor distribution, and outreach activities.

Direct for Federal Agencies

- There are several federal agencies that are considering the implementation of Direct
 - IHS, VA, USPS, CMS, DoD...
- The Federal Health Architecture (FHA) has a Work Group dedicated to Directed Exchange
 - The FHA has produced a set of recommendations for agencies implementing Direct:
 - The use of FBCA cross-certified CAs for issuing Direct certificates over next 2 years
 - FBCA Medium for Providers and Business Associates
 - Use of a Federal Trust Bundle to define requirements for security and privacy in relations to federal HISP operations

(http://www.healthit.gov/sites/default/files/fha-directed-exchange-guidelines_82214.pdf)

Direct Use Cases for FBCA

- Two use cases for FBCA when federal agencies implement Direct

Relying party

- Under the Relying Party Use Case, federal agencies rely upon FBCA policies implemented by Healthcare community participants to ensure minimum levels of trust are met in the credentialing and use of certificates for Directed Exchange

Identity Provider

- Under the IDP Use Case, FBCA cross-certified IDPs utilize federal PKI policies to translate identities bound in agency PIV credentials into an FBCA cross-certified Direct certificate via an appropriate derived process

Direct Use Cases for FBCA

- Relying Party Use Case
 - The FBCA is allowing federal agencies to access the expanding national DirectTrust network for Directed Exchange through the cross-certification of DirectTrust members' Direct certificates
 - Approximately 75% of accredited issuing CAs within the DirectTrust community are already FBCA cross-certified
 - NOTE: there are approximately 55-60 issuing CAs in the DirectTrust network
 - Directed Exchange uses trust bundles for establishing trust, FHA has specified requirements (draft) for a federal trust bundle that requires FBCA cross-certified issuing CAs

Direct Use Cases for FBCA

- Identity Provider
 - HISPs and their issuing CAs within the DirectTrust network can rely upon PIV or PIV-I or FBCA Medium Hardware certificates to provision Direct credentials via a derived credential process
 - DigiCert utilizes a digitally signed PDF declaration of Identity process to provision Direct certificates to federal agency customers
 - Federal HISPs utilize PIV credentials to authenticate federal subscribers to Direct services facilitated by the HISP

Summary

- Healthcare Providers have incentives under MU2 to communicate electronically with their patients, other providers, and government agencies
- Direct Protocol is one mechanism to enable scalable secure PHI to be transmitted over the internet directly to dedicated healthcare end points
- The FHA has made recommendations for agencies to utilize FBCA policies for Directed Exchange to ensure minimum trust and security controls are commensurate with the risk of PHI disclosure
- DirectTrust.org has established a Trust Framework for facilitating Directed Exchange for the healthcare community built upon an FBCA compatible CP
- Approximately 75% of accredited issuing CAs within DirectTrust are already FBCA cross-certified (there are 55-60 issuing CAs in DirectTrust network)
- Federal agencies can leverage existing PIV credentials to obtain Direct certificates via a derived credential process, and subsequently to access Direct services protected by those certificates

Questions

- Q & A...

Contact Details

Links:

<http://www.digicert.com/direct-project>

<http://www.healthit.gov/policy-researchers-implementers/fha-workgroups>

Scott Rea: (801) 701-9636, Scott@DigiCert.com