Federal Health Architecture
Patient Identity in Directed Exchange: How Much Assurance?

July 2014

Federal Health Architecture Program Management Office | Office of the National Coordinator for Health IT | Department of Health and Human Services

Capital View Office Building
425 3rd Street SW, Washington, DC 20004

Website: healthit.gov/fha

General Email: federal.health@hhs.gov

Abstract

ONC's May 2013, *Direct: Implementation Guidelines to Assure Security and Interoperability* document calls for Level of Assurance 3 (LOA3) for HISP to HISP Direct user identity but did not go as far as to define the minimum LOA for Patient exchange. This paper attempts to fill that gap by focusing on patients having access to their records and therefore recommends LOA2 as the minimum federal agency level of assurance (as defined by OMB) supporting patient identity proofing. The recommendation is supported by a review of federal technical, operational standards, policy guidelines and examples applied to a Directed Exchange recipient's trust that a particular Direct message came from a specific patient as a real person.

Issue

A recipient may have little assurance that a Direct message actually came from a claimed patient:

- If the identity proofing process for patients does not provide identity at the appropriate level of trustworthy assurance, or
- If patient certificate provisioning does not strongly bind a Direct address to an assured patient identity, or
- If the authentication level used to access Direct services provides little assurance of that identity

Introduction

The goal of this paper is to determine of the appropriate level of identity assurance required for a recipient to trust that a received Direct message actually came from a specific patient.

Patients participate in Direct much like other Direct users. Under the provisions of Meaningful Use 2, patients should be able to "view, download, and transmit" (VDT) their healthcare information to a Direct endpoint of their choice.

The principal purpose of the Direct Project is to enable secure transport of protected health information (PHI) for participants. To do this, patients will generally need to have a Direct address (the "From" address on a Direct e-mail). In order to obtain a Direct address and gain access to Federal systems, they will need to be identity-proofed and then obtain and use

authentication credentials. Assurance occurs when each step of the process, identity proofing, credential use, secure Direct transport and delivery occur as it should. [See: Applicability Statement for Secure Health Transport v.1.1]

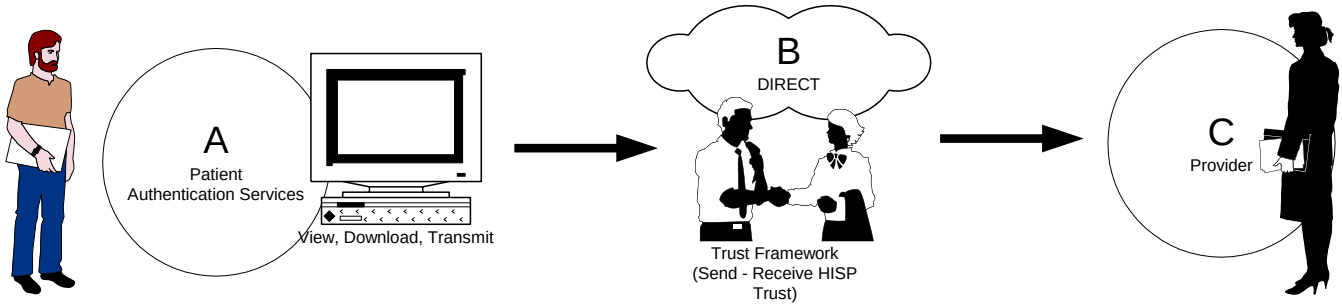

Figure 1 illustrates the process of communication between a patient and a recipient of direct communications. There are four policy points that uniquely determine everything that a recipient needs to know in order to obtain assurance that a communication actually came from a patient as a real person:

PRE-CURSOR EVENT: IDENTITY PROOFING AND CREDENTIAL ISSUANCE

At this point, the patient becomes known as an individual identity for the first time. Through a managed process, either in-person or remotely, they are identity-proofed and provided credentials in accordance with agency policy and NIST SP 800-63-2. This is the initial phase of establishing LOA and will typically serve as a pre-cursor event prior to any particular Direct exchange. This step establishes the degree of confidence that the recipient may have in the vetting process used to establish the identity of the individual to whom the credential was issued. Refer to Attachment A: Definitions (Assurance).

A. LOGON

During logon, the patient, with the intent of choosing to send a specific message to a particular recipient, uses their provided credentials to authenticate to authority "A," acting as the sender. This step establishes the degree of confidence that the recipient may have that the individual who uses the authentication credential is the individual to whom the credential was issued.

B. TRANSMISSION

At this point, the patient's message is introduced into the Direct secure transmission services "B". This paper assumes Direct operates correctly; however, the recipient needs to know the sender's policy regarding the governance and selection of credentials used to secure the transmission. In addition, the sender and receiver may need to establish a memorandum of

agreement, or understand that they participate in a policy trust framework mutually agreeable to both. This trust may be established through negotiation of trust framework policies, trust bundles and trust circles.

C. VERIFICATION

Finally, the recipient verifies satisfaction of phases 1 through 3. The recipient verifies that patient identity proofing and credential provisioning, run time authentication and transmission meet the recipients trust assurance policies. Such assurances may be satisfied through technical, operational or purely policy mechanisms, but the recipient must be assured that each step 1-3 above has been satisfactorily completed. Successful verification provides trust that the transmission received actually came from the patient holding the Direct address, that they can be associated with the Direct address or domain bound certificate used to secure the communication and that they can trust that the transmission actually came from the actual patient. Verification provides the recipient confidence that the patient was actually in possession of the information transmitted and intended to send it.

Scope

This paper is the work product of the Federal Health Architecture (FHA) Directed Exchange Working Group convened under the authority of the Office of the National Coordinator for Health IT. Participation of this Working Group consisted solely of representatives of federal agencies and therefore, the scope of discussions and recommendations are therefore limited to those agencies.

In-scope are considerations including HIPAA, HITECH, and in particular applicable Federal regulations and standards as applied to patient identity proofing, digital certificates, and authentication assurance.

In-scope are Federal agencies receiving Meaningful Use Stage 2 "View, Download and Transmit" (VDT) Direct exchanges from patients. This case includes "sent on behalf-of" models. See the discussion of representative operational trust models in the "Operational Trust Models and Options" section that follows.

The special case of patient-patient controlled endpoint is considered out-of-scope. Patients sending information to themselves is in essence self-verifying.

Out-of-scope are all cases already addressed in ONC's May 2013, *Direct: Implementation Guidelines to Assure Security and Interoperability* where the recipient wishes to verify the trust in the LOA of a non-patient Direct sender. The organizational representatives and individual

providers must be identity proofed at LOA3 per NIST SP 800-63-2 Electronic Authentication Guideline. Provider to patient exchanges are included in this use case.

Patient-directed exchange (including provider supported VDT) to non-Federal agency recipients is out of scope by definition. Regardless, non-Federal agencies may find the analysis generally relevant to making their own determinations.

Background

The Direct Project describes how to use SMTP, S/MIME, and X.509 certificates to securely transport health information over the Internet. Participants are identified using standard email addresses associated with X.509 certificates. The data is packaged using standard MIME content types. Authentication and privacy are obtained by using Cryptographic Message Syntax (S/MIME), and confirmation delivery is accomplished using encrypted and signed Message Disposition Notifications. Certificate discovery of endpoints is accomplished through the use of the DNS or LDAP. Advice is given for specific processing to ensure security and trust validation on behalf of the ultimate message originator or receiver.

Direct may be implemented using a variety of deployment models, which provide significant flexibility to implementers. The Direct Applicability Statement specifies constraints on the S/MIME standard needed to implement the ubiquitous services expected for a nationwide basis.

ORGANIZATIONAL REPRESENTATIVES AND INDIVIDUAL PROVIDERS

ONC has established the guideline that organizational representatives and individual providers must be identity-proofed at NIST SP 800-63-2 Electronic Authentication Guideline Level of Assurance 3 (LOA3). Patients were not included in this definition, leaving uncertainty as to their status. That is, this guidance does not extend to patients who are expressly excluded. Accordingly, this paper examines the issues and potential methods of providing *patient identity* assurance in Direct.

GENERAL CONSIDERATIONS

1. Patient identity assurance involves consideration of:
   - The level of assurance of identity appropriate for patient access to their own information,
   - The breach risk for the entity sending or providing access to patient information,
   - The potential risk to patient safety if a recipient uses or responds to information received from a patient-controlled source, and

- The potential risk to patient safety, fraud, patient identity theft and breach if an entity uses or responds to information received from *an apparently* patient-controlled source.

2. Patient LOA provides a means for a recipient to know and trust self-reported information provided by a patient. This facilitates automated exchange between patient and provider and eliminates paper and manual verification. On the other hand, LOA by itself cannot guarantee the integrity or provenance of information forwarded by a patient owned by others, such as an EHR extract that may be modified, by deletion or addition of content *prior* to transmission.

Content assurance is out of scope of the Direct project, which is wholly concerned with *transmission* security. In this case, per ASTM E1762, the appropriate security service is data origin authentication (source authentication), which safeguards against content tampering and is defined to be corroboration that the source of data received is as claimed. Data origin authentication binds the entity and verification to a piece of information, typically by means of a digital signature applied to and retained with message content.

Many of the Federal issues concerning VDT through Direct trust also involve data origin authentication in addition to patient LOA. In these cases, both may be appropriate to providing a complete view of the trust that a Federal agency may obtain in a Directed exchange and associated limitations, if any, which may be necessary in use.

3. As the Direct Applicability Statement focuses on the technical aspects of transport security, it does not provide mechanisms for the recipient of a Direct mail to obtain confidence in the identity and certificate assurance vetting or e-authentication technology used by the sender at logon. Instead, the matter of trust in the sender is assumed to be known or deferred to policy considerations. Per the Direct Applicability Statement:

> "Methods for evaluating trust anchors must ensure common floor definitions of certificate issuance policy, including associated mechanisms for identity assurance and operational control and authentication to the issued certificates after issuance. "

Policy definitions are necessarily indirect and variable, being based upon the Credential Service Provider, Certificate Policies (CP) and governance of identity Trust Frameworks of a policy domain (e.g. Federal domain), which are always just beyond the scope of the Direct Applicability Statement.

Of note, patients are not Federal agencies and may initiate or authorize communications of their own information by providing a recipient Direct address, which could be their own personal

account, that of a spouse, another patient representative, or any other Direct endpoint of their choosing. Such endpoints may be out-of bounds of what Federal policy might otherwise require, do not involve establish of memoranda of agreement, or assertion of a common trust framework. Regardless, such endpoints may take advantage of ONC and Federal policy.

ASSUMPTIONS

The following assumptions are made regarding the purpose and use of patient LOA:

- The LOA required for Federal agency trust in patient-provider communications within Direct is wholly governed by applicable Federal law, regulation, and standards, agency policy and applicable patient preferences,
- In order for patients to receive or send health information via a Federal agency-provided Direct address, they will need to be identity proofed,
- Trust in the clinical content of patient-provider Direct communications as "patient provided information" can be effectively established through trust in the identity assurance of the patient, and
- Trust in the reliability and integrity of clinical information forwarded by patient use of Direct from one provider to another, cannot be established through patient identity assurance alone. Thus there cannot be trust, for clinical purposes, that information received from patients was not modified prior to introduction into the Direct system. This assumption is a consequence of the fact that the Direct Applicability Statement makes no policy regarding the trust in the message content other than simple transmission security.

Determining Federal Agency Levels of Assurance

FEDERAL GUIDELINES FOR E-AUTHENTICATION

It is through authentication services that patients access capabilities to originate and send Direct mail. However, per NIST, it is the individual agency or application acting as the relying party (in this case the Direct mail recipient relying on an authentication process that occurred elsewhere) that makes the decision to grant access or process a transaction based on the specific application requirements.1 It is then up to the recipient to reject, accept "at risk" or validate the information, each time received, by some out of band method (such as reviewing the material face-to-face with the patient.)

This is consistent with the Direct Applicability Statement:

[1] NIST SP 800-63 pg 17

"The methods for ensuring the correct identity of sender and receiver are only as strong as the methods for certificate issuance, identity assurance, and authentication in operational use."

OMB MEMORANDUM M-04-04.

Fundamental to this paper is establishing a clear understanding of what is meant by the concept of "Assurance" and "Level of Assurance". This paper adopts OMB M-04-04 definitions for these terms as follows:

Assurance. 1) The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.

Level of Assurance. OMB guidance also describes four identity authentication assurance levels for e-government transactions[2]. Each assurance level describes the agency's degree of certainty that the user has presented an identifier (a credential[3] in this context) that refers to his or her identity. The four assurance levels are:

- Level 1: Little or no confidence in the asserted identity's validity.
- Level 2: Some confidence in the asserted identity's validity.
- Level 3: High confidence in the asserted identity's validity.
- Level 4: Very high confidence in the asserted identity's validity.

STEPS IN DETERMINING OMB ASSURANCE LEVELS

OMB specifies that Agencies should determine assurance levels using the following steps:

1. Conduct a risk assessment of the e-government system.
2. Map identified risks to the applicable assurance level.
3. Select technology based on e-authentication technical guidance.
4. Validate that the implemented system has achieved the required assurance level.
5. Periodically reassess the system to determine technology refresh requirements.

[2] For the purposes of OMB M-04-04, a transaction is defined as: a discrete event between user and systems that supports a business or programmatic purpose.

[3] A credential is defined as: an object that is verified when presented to the verifier in an authentication transaction.

OMB ASSURANCE LEVELS APPLIED TO DIRECTED EXCHANGE

This paper adopts the methodology of OMB Memorandum M-04-04 in order to assess the level of assurance required in order for a recipient to trust that a Direct message actually came from a specific patient. To that end, OMB guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance.

Per OMB, agencies should determine assurance levels using steps, described in Section 2.3. Based upon application of the steps in Table 1, risk mitigating technology solutions for e-authentication credentials are chosen for use in logging onto systems providing Direct related services. Table 1 describes these steps and reference artifacts established by the FHA Directed Exchange Working Group.

Table 1 OMB e-Authentication Assurance Levels Applied to Directed Exchange

Step	Activity	Reference Artifact
1.	Conduct a risk assessment of the e-government system.	• Federal Agency Directed Exchange Risk Assessment Pertaining to Policy Concerns, Version 1 dated July 2013 • Direct Project Threat Model_Simple SMTP • Threat Model - SMTP with Full Service HISPs • Threat Model - Direct to and from XDR • Individual Federal Agency/Department Risk Assessments[4]
2.	Map identified risks to the applicable assurance level.	• ONC Direct Implementation Guidelines to Assure Security and Interoperability • Individual Federal Agency/Department assurance level determinations
3.	Select technology based on e-authentication technical guidance based upon NIST SP 800-63-2 guidelines.	• Individual Federal Agency/Department technology selections
4.	Validate that the implemented system has achieved the required assurance level.	Out of scope of this analysis
5.	Periodically reassess the system to determine technology refresh requirements.	Out of scope of this analysis

[4] GSA has an e-RA tool for conduction LOA assessments. Located at http://www.idmanagement.gov/resource/electronic-risk-and-requirements-assessment-e-ra-tool

Step 1. The FHA Directed Exchange Subworkgroup has completed a risk assessment of policy concerns applicable to Federal agencies. Supplementing this risk assessment are the technical risk assessments of the Direct Project. In addition, each member Federal agency has conducted individual risk assessments of patient e-authentication. See Appendix E for a discussion of risk considerations associated with trusted patient identity in Direct.

Step 2. ONC has established NIST SP 800-63-2 level of assurance 3 for organizational representatives and individuals (not including patients). The level of assurance for exchanges involving patients should not need to exceed the ONC guidelines established for non-patients. In this regard, ONC has established LOA3 as the "high-bar" for patient exchange of healthcare information using Direct.

Step 3. Federal healthcare agencies already provide various types access to patients based upon risk considerations. The minimum level of e-authentication assurance for such services is LOA1 which provides access to publically available information and steps for obtaining further access. In all cases, the minimum e-authentication LOA for access to an individual's healthcare information is established as LOA 2. This is typically based upon an evaluation that considers and accepts some risk of exposure of a single patinet's information as a tradeoff against imposing burdensome and expensive mechanisms to all.

Conclusion: Federal LOA Policy Determination

Based upon the foregoing, this paper establishes patient e-Authentication LOA2 (as defined by OMB M-04-04/NIST SP 800-63-2) as the "low bar" for Federal agency trust in patient exchange of healthcare information using Direct.

Operational Trust Models and Options

Federal agencies rely upon Trust Frameworks to define technical (infrastructure hardware and software), operational (certificate issuance policies operational governance), and policy/contract agreements for information exchange between partners. Such frameworks inevitably involve legal considerations in order to deal with liability and risk. There are multiple sources of such policy applicable to federal organizations, including:

- Federal Bridge Certificate Authority (FBCA) and Public Key Infrastructure (PKI) Policy Authority (FPKIPA), Note: Required by federal agencies
- National Strategy for Trusted Identity in Cyberspace (NSTIC),
- Federal Identity, Credential and Access Management (FICAM),

- American Bar Association Identity Trust Framework (Draft),
- Kantara Trust Framework,
- National Association for Trusted Exchange,
- DirectTrust, and
- Blue Button+.

In general, Federal agencies are expected to comply with the principles of many trust frameworks. In this sense, Direct is an instance of a specific framework that must fit under other more general frameworks that apply, for example, NSTIC or the FBCA. For Federal agencies, The Federal PKI program is a core component of the Federal Trust Framework as a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs. This program is managed by the Federal PKI Management Authority.

In the case of Direct, certificate issuance policies provide the means for a recipient to put in place operational controls to ensure that:

a) The sending STA/HISP has obtained necessary verification that the owner of the Direct address in the certificates, which the STA/HISP holds, has been identity proofed to an appropriate NIST SP 800-63-1 LOA in accordance with a common Trust Framework policy,
b) Sender and Receiver Trust Bundles have been selected based on Sender or Receiver assurance requirements,
c) The organization maintaining the Health Domain Name has associated the Health Domain Name and/or Direct Address with one or more X.509 certificates,
d) Organizations that maintain Organizational Certificates assert that they have validated the identity of all Direct Addresses recipients at the Health Domain Name tied to the certificate(s),
e) Trust in patient identity has been established by identity proofing and associating their identity with the subject alternative name of the STA/HISP certificate.

A number of options exist to establish the policy and trust framework needed to support the above operational controls. These include:

OPTION 1: BINDING A DIRECT ADDRESS TO AN IDENTITY-PROOFED PATIENT (ADDRESS-BOUND CERTIFICATES)

The patient's Direct address provides the mechanism for recipients to know a message came from a patient and for senders to look up certificates for encrypting Direct mail sent "To" a patient. Referring to Attachment C, "Patient Directed Exchange with Full-Service HISP ", the binding of a patient to a Direct mail address involves:

1) Identity proofing a patient at known level of assurance (item a) above),
2) Creating address-bound certificates associated with the patient based upon linking the asserted level of patient identity proofing to the Trust Framework of the issuing Certificate Authority (e.g., The CP asserts a policy that the individual (patient) whose full Direct address appears in the certificate was identity proofed at a known level as asserted by the RA (item c) above. The Direct mail "From" addressee must match the Direct mail address in the certificate used for Direct transport integrity.

In addition to 1) and 2), in order to fully meet OMB M-04-04 requirements there is the need to establish confidence that the individual who uses the credential is the individual to whom the credential was issued. In Direct the credential used by a STA/HISP to secure the transmission path is most likely not the credential (e.g. Password/ID) use by a patient for authentications purposes. Direct does not provide technical means to obtain knowledge regarding the authentication method used by users to access STA/HISP services. Accordingly, such assurances must be met by other means within a trust framework, e.g.:

3) The STA/HISP controlling address-bound certificates asserts compliance to identity proofing and authentication assurance policy, governance, and certification suitable to meeting the requirements of the Trust Framework to which it belongs and establishing authentication trust.
4) While compliance to the Trust Framework requirements should optimally be legally binding with penalties for default linked to HIPAA and other applicable state and federal laws, patients are not employees and their legal relation to the STA/HISP in a patient directed exchange may be unclear. Furthermore, since patients may direct communications at endpoints not in the STA/HISP trust bundle, the STA/HISP may wish to disavow any responsibility for patient directed exchanges.
5) Since LOA assurance obtained in this manner is inherently indirect, the relying party will need to determine whether this OPTION represents acceptable risk to the Federal organization for LOA purposes.

OPTION 2. BINDING A DIRECT ADDRESS TO AN IDENTITY-PROOFED PATIENT (DOMAIN-BOUND CERTIFICATES)

This case is similar to OPTION 1 except that the certificates used by the STA/HISP do not contain the Direct mail address of the sender. Instead the single identifier is the Direct mail "From" addressee. This increases the risk of false identity since now there is risk of modification of the "From" header without any validation check. Here assurance is established at the Domain level and again, the legal relation of the patient-participant in the Direct exchange may be unclear and the STA/HISP concerns described in 4) above apply.

OPTION 3: SEnT "ON BEHALF OF"

Figure 2 illustrates the flow of information in a Blue Button+ "Patient Initiated Transmit-VDT" intended to illustrate Meaningful Use (MU)2 requirements for a patient to view, download, and transmit (VDT) portions of their health record[5]. In this case, a data holder acts to transmit information "on behalf of" the patient. Using Data Holder credentials provides assurance of provenance of the medical record. First, the provider is 'vouching for' the information and its relationship to the patient. The receiver may also have greater assurance that the transmission is exactly what was in the provider EHR or what was sent from PHR entries for a specific patient. Second, the recipient is not dependent upon the level of assurance provided by the Direct Cert for the content but rather by the credential used by the data holder to sign the payload

This OPTION eliminates many of the complexities and risks of OPTION 1 and 2; however, the concern regarding patient directed communications to an endpoint not in the sender's trust bundle remains. For example, the DoD security protocols specify that end-to-end system integrity must be maintained at a high assurance, LOA 4. Meaning, the DoD cannot push a direct message to any receiving entity that does not share the same level of assurance.

Reliance on a Trust Framework should be legally binding upon the sender acting "On behalf of",

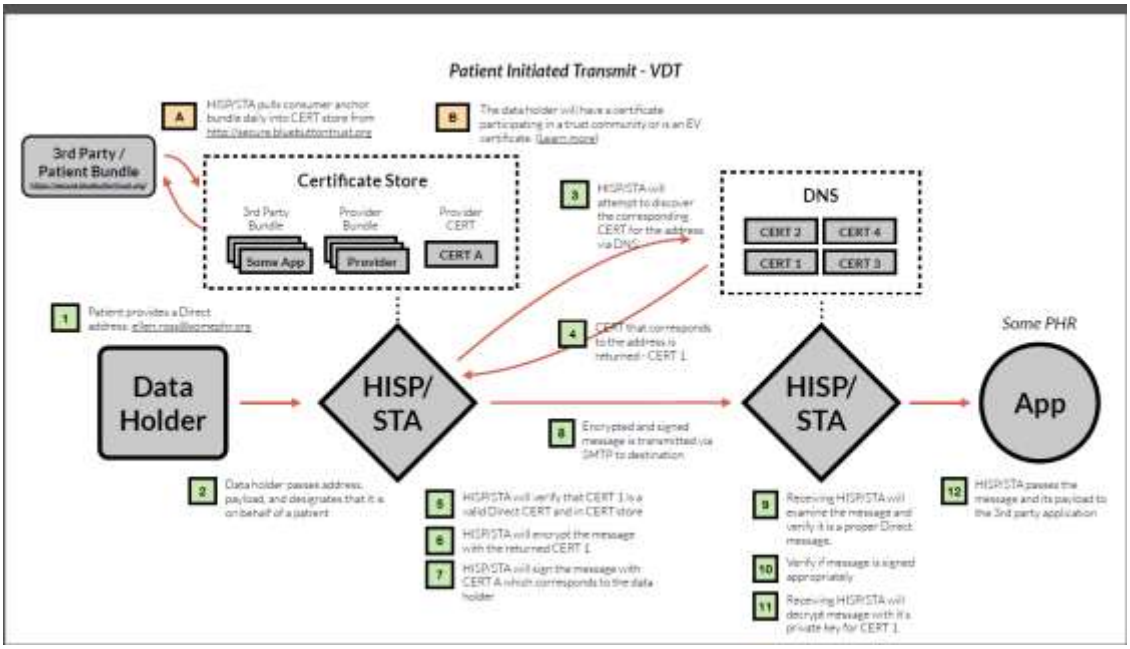

Figure 2 Blue Button+ VDT

[5] Blue Button+ Implementation Guide

OPTION 4: DATA: ORIGIN (SOURCE) AUTHENTICATION

Data origin authentication provides document assurance and binding to an individual for a variety of purposes.[6] Data origin authentication provided by means of a digital signature additionally provides assurance that a document has not been modified in an unauthorized way and non-repudiation. Data origin authentication is applied to the content of a Direct message. Data origin authentication involves credentials owed by the patient and in their possession at all times.[7]

As an example, one simple form of digital signature would be a domain managed patient digital signature service. The patient would access the digital signature service as part of a workflow associated with creating, using, preparing, sending and signing a document. The signature is applied by presenting credentials such as a password/ID. The patient signature can be further enhanced for trust and interoperability by wrapping the patient signed document with a domain/STA or HISP signature. Since the signature remains with the document and can be independently verified by the recipient, knowledge of the person signing the document is assured. Note that in this case, it is not important who actually sent the document since the recipient is guaranteed of the binding of the signer.

A variation of this would be for the sender STA/HISP to digitally sign the message content. In this case the signature would not reflect the patient but rather the sender "verification", "source" or other purpose. Such a signature may serve as the equivalent of the sent "on *b*ehalf of" approach presented in OPTION 3 above.

Again, this OPTION provides far greater simplicity than OPTION 1 or 2. The STA/HISP may choose to re-purpose their Direct credentials used for transport integrity to also provide the content signature for the purpose of "sent on behalf of <patient>".

Signature services of message content are outside of the scope of the Direct Applicability Statement and the Direct Project but provide the greatest degree of content assurance and the greatest interoperability since the document received by one entity can be passed on to another retaining the binding to the original sender.

As in the previous OPTIONS, the concern regarding patient directed communications to an endpoint not in the sender's trust bundle remains.

OPTION 5: ELEVATING IDENTITY ASSURANCE

In this example, the patient has sent their information (VDT) from one organization to a destination address that does not manage identity at the LOA2-3 level as would be required for

[6] See ASTM E1762 Standard Guide for Electronic Authentication of Health Care Information
[7] See for example "HL7 Digital Signatures on the CDA"

Federal recipients (e.g. a public PHR at LOA1) to receive information. In this case, if the patient were to attempt to provide this information to a different provider, then the LOA1 policy would mean that this source would not be in the Federal agency trust bundle and so delivery may not be validated or accepted.

This OPTION would address this issue by elevating the assurance of the patient's LOA1 status. This might occur for example, if the patient used their LOA1 PHR to send the desired information to their LOA2 Federal provider tethered PHR. At this point, the patient can turn around the information to their PHR provider via secure messaging or other mechanism. The provider would have confidence that the information came from the patient since the patient was using the provider approved authentication service to elevate trust in the information.

Summary

This paper has reviewed the Federal policy and standards supporting mechanisms for a Directed Exchange recipient to trust that a particular Direct message came from a particular patient as a real person.

In order for a recipient to trust that a Direct address is reliably bound to and only available for use by a specific patient (real person), the processes for establishing both level of identity assurance (LOA) and the Direct address of such persons must be trustworthy and complimentary and their use within Direct must also be assured correct within the parameters of acceptable operational risk. This involves consideration of:

- Technical Issues. The technical capabilities and limitations described in the Direct Applicability Statement and S/MIME.
- Operational Issues. LOA is established by: 1) The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued,
- Policy Issues
    - Trust Framework. Trust in the Direct address is established by methods for certificate issuance. For Federal agencies, the Federal PKI program is a core component of the Federal Trust Framework as a set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs. This program is managed by the Federal PKI Management Authority.
    - The evaluation of risk per OMB M-04-04, and selection of technical remedial mechanisms,
    - Legal considerations.

Conclusions

The intent of this paper was to consider how trust could be achieved that the sender of a Direct message could actually be associated to a real person within a verifiable level of assurance per OMB M-04-04. Methods to achieve this assurance appear to be generally indirect, reliant upon adherence to trust framework governance rather than direct technical features (e.g. such as might be available from possession of a SAML identity assertion.)

- The way trust is establish between partners might vary but in the end the trust framework you use should be legally binding upon the participants, ideally under HIPAA rules.
- From a recipient's perspective, replacing the original stated problem with providing assurance of the information content captured in "View, Download and Transmit" appears to be a more appropriate objective. In this case, BlueButton+ "sent on behalf of" may provide a simpler and more meaningful approach.
- Source authentication methods provide another standard security approach to assuring a permanent record of trust in the message content. In this case, the trust (identity of the signer) is permanently retained with the document, and is independent of the path used for communications or the trustworthiness of the sender identity.

Attachment A: Definitions

Term	Definition
Assurance	1) The degree of confidence in the vetting process used to establish the identity of the individual to whom the credential was issued, and 2) The degree of confidence that the individual who uses the credential is the individual to whom the credential was issued.
Credential	An object that is verified when presented to the verifier in an authentication transaction
Transaction	A discrete event between user and systems that supports a business or programmatic purpose.
Trust Communities	Trust Communities are formed by organizations electing to follow a common set of policies and processes related to health information exchange. Examples of these policies are identity proofing policies, certificate management policies, HIPAA compliance processes etc.
Trust Community Profile:	A Trust Community can create multiple sets of policies and processes and enforce these sets of policies on selected organizations that want to conform. For example, a Trust Community can create a set of policies and processes which organizations have to conform to for regular treatment related use cases, a different set of policies and processes that organizations have to conform to for Behavioral Health related use cases and so on. These sets of policies and processes are called as Trust Community Profiles. The word "Profile" indicates a set of policies and processes
Trust Bundles	Trust Bundle is a collection of Direct Trust Anchors within a Trust Community that conform to a Trust Community Profile. Trust Anchor's of member organizations who have elected to conform to a Trust Community Profile are included in the Trust Bundle for that particular Trust Community Profile. Some examples of Trust Bundles conforming to different Trust Community Profiles are: • A Trust Bundle could have Trust Anchors that conform to NIST Level of Assurance 3 • A Trust Bundle could have Trust Anchors that are FBCA Cross-certified at Medium Level of Assurance.
Trust Anchors	An X509 certificate that is used to validate the first certificate in a sequence of certificates. The trust anchor public key is used to verify the signature on a certificate issued by a trust anchor CA. The security of the validation process depends upon the authenticity and integrity of the trust anchor.
"Full Service" HISP	Please see attachment C: Patient Directed Exchange with Full-Service HISP, page 20

Attachment B: NIST SP 800-63-2

NIST provides guidelines for implementing the third step of the above OMB process. NIST defines technical requirements applicable to federal agencies for each of four levels of assurance in the areas of identity proofing, registration, tokens, management processes, authentication protocols and related assertions. This version of the NIST specification for electronic authentication also provides for remote identity proofing at Levels of Assurance 1 through 3 (LOA1-LOA3). Level 4 can only be done by in-person proofing. See Attachment A for further description of the NIST SP800-63 specifications.

Registration Authorities (RA), along with Certificate Authorities (CAs) and Security Trust Agents/Health Information Service Providers (STA/HISP) provide the backbone for Directed Exchange Trust Frameworks. RAs attest to the identity proofing of individuals and groups of individuals to CAs and to STA/HISPS for issuance of local authentication credentials and Direct mail addresses.

At both LOAs 2/3, the RA, as part of Identity proofing, verifies the Applicant's submitted documentation. There is, however, a slight distinction. For LOA 2, the RA must verify only one of the two submitted identifiers, for LOA3 the RA must verify both. LOA 2 and LOA 3 are generally considered to be the minimum levels of assurance appropriate for patient access to their own health records contained in a data holder's EHR.

EXTRACTS FROM NIST SP 800-63-2

Level 2 Identity Proofing

Table 3 - Identity Proofing Requirements by Assurance Level

	In-Person	Remote
Level 2[12]		
Basis for issuing credentials	Possession of a valid current primary government picture ID[13] that contains Applicant's picture, and either address of record or nationality of record (e.g., driver's license or Passport)	Possession of a valid current government ID[14] (e.g., a driver's license or Passport) number and a financial or utility account number (e.g. checking account, savings account, utility account, loan or credit card, or tax ID) confirmed via records of either the government ID or account number. Note that confirmation of the financial or utility account may require supplemental information from the applicant.
RA and CSP actions	***RA*** inspects photo-ID; compares picture to Applicant; and records the ID number, address and date of birth (DoB). (***RA*** optionally reviews personal information in records to support issuance process "a" below.) If the photo-ID appears valid and the photo matches Applicant then: a) If personal information in records includes a telephone number or e-mail address, the ***CSP*** issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or e-mail address associated with the Applicant in records. Any secret sent over an unprotected session shall be reset upon first use; or b) If ID confirms address of record, ***RA*** authorizes or ***CSP*** issues credentials. Notice is sent to address of record, or; c) If ID does not confirm address of record, ***CSP*** issues credentials in a manner that confirms the claimed address.	• ***RA*** inspects both ID number and account number supplied by Applicant (e.g., for correct number of digits). Verifies information provided by Applicant including ID number OR account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are on balance consistent with the application and sufficient to identify a unique individual. For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity. (This technique may also be applied to some financial accounts.) • Address/phone number confirmation and notification:[15] a) ***CSP*** issues credentials in a manner that confirms the ability of the applicant to receive mail at a physical address associated with the Applicant in records; or b) If personal information in records includes a telephone number or e-mail address, the ***CSP*** issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or e-mail address associated with the Applicant in records. Any secret sent over an unprotected session shall be reset upon first use; or c) ***CSP*** issues credentials. ***RA*** or ***CSP*** sends notice to an address of record confirmed in the records check.[16]

Level 3 Identity Proofing

Level 3[12]		
Basis for issuing credentials	Possession of verified current primary Government Picture ID that contains Applicant's picture and either address of record or nationality of record (e.g., driver's license or passport)	Possession of a valid Government ID (e.g., a driver's license or Passport) number and a financial or utility account number (e.g., checking account, savings account, utility account, loan or credit card) confirmed via records of both numbers. Note that confirmation of the financial or utility account may require supplemental information from the applicant.
RA and CSP actions	***RA*** inspects photo-ID and verifies via the issuing government agency or through credit bureaus or similar databases. Confirms that: name, DoB, address and other personal information in record are consistent with the application. Compares picture to Applicant and records ID number. If ID is valid and photo matches Applicant, then: a) If personal information in records includes a telephone number, the ***CSP*** issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications at a number associated with the Applicant in records, while recording the Applicant's voice or using alternative means that establish an equivalent level of non-repudiation; or b) If ID confirms address of record, ***RA*** authorizes or ***CSP*** issues credentials. Notice is sent to address of record, or; c) If ID does not confirm address of record, ***CSP*** issues credentials in a manner that confirms the claimed address.	• ***RA*** verifies information provided by Applicant including ID number AND account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, DoB, address and other personal information in records are consistent with the application and sufficient to identify a unique individual. At a minimum, the records check for both the ID number AND the account number should confirm the name and address of the Applicant. For utility account numbers, confirmation shall be performed by verifying knowledge of recent account activity. (This technique may also be applied to some financial accounts.) • Address confirmation: a) ***CSP*** issues credentials in a manner that confirms the ability of the applicant to receive mail at a physical address associated with the Applicant in records; or[15] b) If personal information in records includes both an electronic address and a physical address that are linked together with the Applicant's name, and are consistent with the information provided by the applicant, then the CSP may issue credentials in a manner that confirms ability of the Applicant to receive messages (SMS, voice or e-mail) sent to the electronic address. Any secret sent over an unprotected session shall be reset upon first use.

Attachment C: Patient Directed Exchange with Full-Service HISP

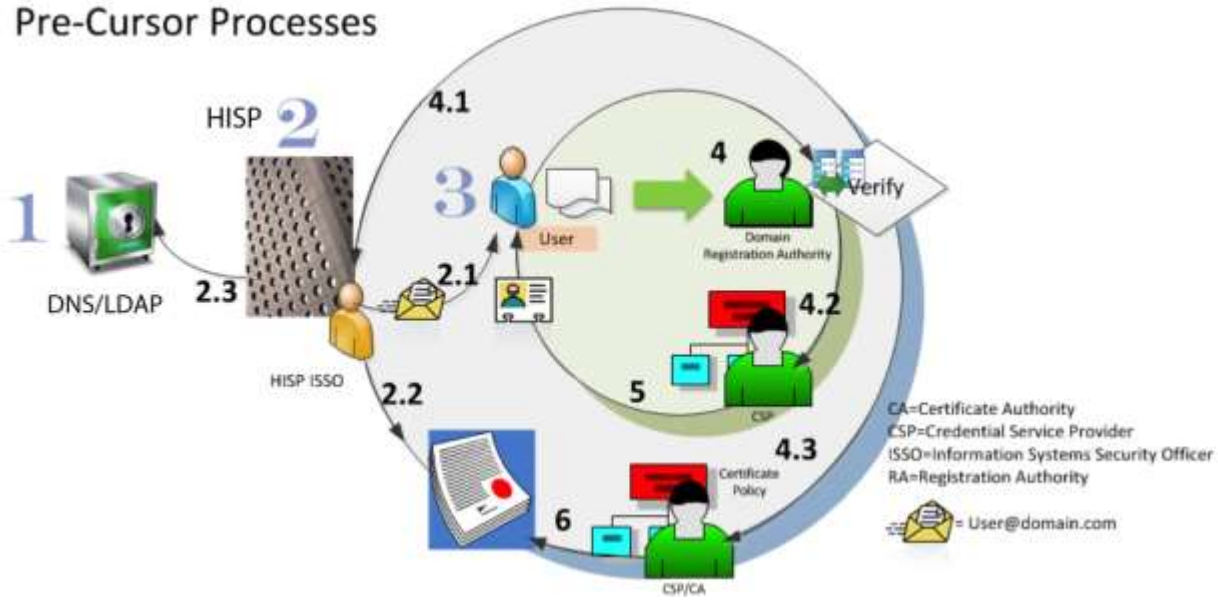

Figure 3 Initialization Processes with Full Service HISP

Figure 3 describes the initialization processes that apply to Direct including user identify proofing, provision of Direct address, registration with a HISP, certificate creation and issuance by a CSP and public key publication in a DNS/LDAP. This process is the basis for establishing core Direct credentials including:

- Basic authentication credentials for the purpose of User- HISP authentication,
- A Direct email address for the purpose of sending and receiving Direct mail,
- PKI credentials for securing the Direct transport from sender to receiver.

1. DNS/LDAP

The DNS/LDAP must be established so that senders can retrieve PKI credentials associated with a Direct address.

2. HISP

In this step, the HISP will have been certified to operate as such under the governance of a Trust Framework acceptable to each domain for which they are providing services. The HISP will periodically undergo re-certification and audit to ensure their practices conform to the governance policies of the Trust Framework(s) to which they belong. In performing its role the HISP will:

2.1 Create Direct Addresses. Following user identity proofing by the RA, the HISP registers a domain User to a domain Direct address. The HISP will:

- Associate the domain and these addresses with an Information Systems Security Officer (ISSO) who has also been appropriately identity proofed. It is expected that HISP ISSOs will be identity proofed at NIST SP 80-63 level of assurance 3 or 4.
- Generate a key pair (address or domain bound) to be associated with the Direct address. The private key is then installed in the HISP services protected key database.

2.2 The HISP provides a CSP issuing certificates in the Trust Circles of the domain with the Direct addresses of the domain users, the corresponding public key in a Certificate Signing Request (CSR) registered to the address, RA identity verification of the Domain Users, and the identity verification information for the HISP ISSO who will receive and manage CSP tokens.

The HISP ISSO will receive tokens (certificates) for all domain users and will be responsible for installing them into the HISP. The HISP will manage and protect these tokens associated with domain Trust Circles and Trust Bundles according to the policies of the Trust Framework for which they are a certified member.

2.3 The HISP will publish the public key portion of the domain certificates in a DNS so that they can be discovered and used by Direct participants.

3. DIRECT USER

The Direct User must collect acceptable information to be used for identity proofing.

The Direct User will, as part of identity proofing process, receive authentication credentials to be used for authentication to the HISP when they have information that they want the HISP to securely transport to a receiving Direct address.

The Direct User will also receive one or more Direct Addresses from the HISP that can be used in the "From" line of a Direct email.

4. REGISTRATION AUTHORITY (RA)

In this step, the Direct user appears before a domain Registration Authority (RA) and presents their identity proofing information (e.g. Government issued photo ID, utility, credit card or other information) in accordance with the identity proofing policy in effect.

The RA, depending upon the specific level of proofing required validates/verifies the information provided. There are a number of factors that could influence the level of identity proofing required:

- The level needed by policy to support the HISP CSP that issues tokens for user authentication to the HISP,
- The level needed by policy to support the CSP/CA that issues credentials for the HISP ISSO for S/MIME transmission supporting the Trust Circles of the supported organization, and
- For purposes such as may be required to support other policy needs of the User organization policy.

Upon successful identity proofing the RA will:

4.1 Make an attestation of Domain user identity to the HISP CSP at requested LOA for the issuance of HISP authentication credentials

4.2 Make attestation of Domain user identity to the HISP for the creation of User Direct addresses.

4.3 Make attestation of Domain user identity to a CSP/CA for the creation of PKI keys and certificates needed to secure the Direct transport.

5. HISP CSP

The HISP CSP issues credentials/tokens to the User for authentication to the HISP so that the User can reliably authenticate to request or receive Direct services. This is needed whenever the User is requesting HISP services.

6. CSP/CA

In this step, the CSP/CA receives all the verified identities and Direct addresses for which certificates are requested. The CSP/CA will:

- Accept CSR and Identity attestations for Domain User and associated HISP ISSO
- Validate that appropriate vetting, attestations and required documentation is in place to enable the issuance of a credential. Verify that the HISP accreditation status is appropriate.
- Issue electronic credentials (certificates) to the HISP ISSO based on the data provided (including CSR and associated metadata) using an approved profile of the Trust Framework. For Direct purposes, the CSP/CA is a CA that issues and revokes public key certificates according to a published and verifiable CP.
- Publish certificate status data to a public repository so that relying parties can verify the certificate upon use.

Appendix D: Risk Considerations

For Federal agencies, personal information, such as medical records, is evaluated under sensitivity criteria established by NIST. Security categorization, the first and arguably the most important step in the Risk Management Framework, employs FIPS 199 and NIST SP 800-60 to determine the criticality and sensitivity of the information system and the information being processed, stored, and transmitted by the system. Additional guidance is found in NIST SP 800-66-1, An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule.

This paper identifies the areas of concern associated with assurance that a Direct address is bound to a real person to be:

The RA process that performs initial identity proofing at a prescribed level of assurance.

In order to assign a Direct address to patient representing a real person:

- **The patient must be identity proofed by an RA according to a known standard (e.g. NISP SP 800-63)**
- A STA/HISP must assign a Direct mail address to the identity-proofed patient.
- A STA/HISP must make a DNS entry representing the Direct credentials associated with the patient's Direct address (address or domain-bound certificates).

ISSUING A DIRECT ADDRESS TO THE IDENTITY PROOFED INDIVIDUAL.

In order for a patient to send a Direct mail:

- **The patient must logon (i.e., authenticate) to some service using authentication credentials issued by a Credential Service Provider (CSP) following an identity proofing event attested to by an RA,**
- The patient must have been assigned a Direct address based upon an identity proofing event attested to by an RA,
- The patient must identify the "To" address
- The patient must identify the message content to be sent.
- Note: The patient may send Direct mail to endpoints not in the Data Holder's Trust Bundle.

ASSIGNING DNS ENTRIES TO LOOKUP CERTIFICATES BASED ON THE PATIENT DIRECT MAIL ADDRESS

In order to send the patient's Direct mail:

The message must be prepared for transmission as an S/MIME message, with a "To" address designated by the patient, a "From" address assigned to the patient, signed for transmission integrity with the private key associated with the patient/domain and encrypted with the public key of the recipient.

OPERATING A STA/HISP IN ACCORDANCE WITH A TRUST FRAMEWORK

In order to receive the patient's Direct mail:

- The Senders certificates must be part of a Trust Bundle that the recipient accepts.
- The receiver's STA/HISP must decrypt the message using the recipient's private key, and then verify the message using the sender's public key (additional verification of the integrity of the unencrypted message headers may also be required).
- The "From" address DNS lookup must retrieve a credential that can be used to validate the message transmission integrity.

IN ORDER FOR THE RECEIVER TO TRUST THAT THE DIRECT ADDRESS BELONGS TO A PARTICULAR PATIENT AS A REAL PERSON,

- All the pre-cursor processes above must be properly implemented,
- The patient's Direct address DNS lookup must retrieve a certificate that correctly validates the transmitted message's integrity.
- The sender STA/HISP must be in a Trust Bundle with the following characteristics:
    - Conforms to a policy that Direct addresses are only issued to patients following an identity proofing event performed by a RA at a known NIST SP 800-63 level of assurance acceptable by the receiver (As verified by the Senders status in a Trust Framework).
    - Conforms to a policy that patients may only send Direct mail following a linked authentication event using credentials issued for a trust level commensurate with an identity proofing event performed by a RA at a known NIST SP 800-63 level of assurance acceptable by the receiver (As verified by the Senders status in a Trust Framework).