Federal Health Architecture

Certificate Issuance and Assurance in Direct Messaging

March 25, 2015

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

Executive Summary

This paper discusses and compares issuance and assurance of Direct Domain and Address-bound certificates in the context of an appropriate certificate policy. It discusses the policies and methods for certificate issuance, identity assurance, and authentication services for Directed messaging exchange in operational use. It compares the controls observed when issuing Direct certificates and methods for ensuring the correct identity of sender and receiver for Direct messaging with the subsequent use of Direct certificates.

CONTENTS

Introduction

Federal agencies are required to meet a number of laws, regulations and policies in any exchange of protected health information (PHI). Many of these key policies also apply specifically to federal participation in and implementation of Direct. The focus of this paper is on federal policy relevant to certificate issuance and assurance methods for Direct.

This paper focuses only on relevant federal operating and policy requirements as applied to Directed Exchange. It covers certain federal agency considerations when implementing Direct and when evaluating the benefits applied to the use and management of either of the two types of certificates used in Direct. The relevant operating and policy environment include:

- Direct addresses may be managed individually by agency, or by a service from a Health Information Service Provider (HISP),
- A single Direct address may represent an individual, a practice, an organizational inbox, or a service queue,
- Direct certificates are used to bind security keys to Direct addresses,
- Federal agencies require Federal Bridge Certificate Authority (FBCA) cross-certified issuers of Direct certificates,
- Direct certificates include two types either: 1) Address bound (for single address) or 2) Organization bound (a wildcard for all addresses in a specific healthcare domain),
- HISP Information System Security Officer(s) (ISSO) must be minimally identity proofed at FBCA Medium prior to issuance of HISP- managed Direct certificates,
- HISP-managed Direct certificates require the primary end user, if either an organizational representative (Org Rep) or Healthcare Provider, to be identity-proofed minimally at FBCA medium or National Institute of Standards and Technology (NIST) Level of Assurance (LoA) 3 in person prior to issuance,
- HISP-managed Direct certificates require the primary end user, if a patient or consumer, to be minimally identity-proofed at FBCA Basic or NIST LOA 2 prior to issuance,
- Legal relationship between a covered entity and a patient is established through appropriate rights, limitations and disclaimers established as conditions of service
- The Public Key Infrastructure (PKI) credentials at the HISP must be protected by IAW NIST FIPS Pub 140-2,
- Organization representatives must ensure that 1) every user of a Direct address protected by that certificate is identity- proofed to the LoA included in the cert, and 2) agrees to the terms of usage of that certificate prior to being given access,
- Additional Federal policy requirements for Direct are contained in the FHA Directed Exchange Federal Trust Bundle.

Core Standards

Within the federal government, there are two agencies principally responsible for specifying authentication and identity assurance standards — the Department of Commerce, NIST and the FBCA.

NIST

NIST Special Publication 800-63-2, Electronic Authentication Guideline provides technical guidelines for federal agencies implementing electronic authentication and covers remote authentication of users (such as employees, contractors, or private individuals) interacting with government information technology (IT) systems over open networks.

NIST Special Publication 800-63-2 defines technical requirements for each of four levels of assurance in the areas of identity proofing, registration, tokens, management processes, authentication protocols and related assertions. In addition to being a requirement for federal agencies, NIST SP 800-63-2 has become a de facto global standard for identity-proofing and subsequent authentication.

DirectTrust has adopted the NIST identity assurance model as the basis for defining LoA in the DirectTrust Certificate Policy (CP). In addition, the Direct Trust CP provides healthcare specific considerations for establishing identity and binding it to a Direct Address in an X.509 certificate.

FBCA

The FBCA is an organization that facilitates acceptance of certifications for transactions with or between federal agencies and their business partners. Since its initial conceptualization and operation, the FBCA has evolved into the Federal Public Key Infrastructure (FPKI) Trust Infrastructure that encompasses Certification Authorities (CAs) from multiple vendors supporting different FPKI policies and functions. The FPKI Policy Authority (PA) governs the interoperation of federal and external PKIs through the policies and practices defined in the FBCA Certificate Policy (CP).

Federal agencies will only accept Direct Certificates cross-certified with the Federal Bridge Certificate Authority

Identity Assurance and Authentication

Assurance and identity-proofing of both healthcare providers and patients is an essential element of Direct. Who is responsible for the identity proofing event and how that is related to certificates determines how much assurance a relying party may have that the message received actually came from the "To Address" on a Direct message. The DirectTrust Accreditation Program (DTAP) is discussed as an exemplar for implementing the identity assurance framework Direct.

IDENTITY-PROOFING FOR HEALTHCARE PROVIDERS

In May 2013, ONC published HISP to HISP messaging guidelines to the Direct Applicability Statement (ONC Direct Guidelines to Assured Security and Interoperability) that recommended non-patient Direct addresses only be issued to individuals and organizations that have been identity proofed to LoA 3 or higher. The guidelines also recommended that the equivalent of NIST LoA 3, and that FBCA cross-certified certificates (or their equivalence), should be utilized. Individual identity proofing requirements are detailed at various LoAs within the FBCA CP[1], and there not an exact one-to-one mapping between the FBCA LoAs and the NIST LoAs. The NIST standard however, does provide guidance on what FBCA LoAs map to an overall NIST LoA equivalence, and both FBCA Basic and FBCA Medium are considered equivalent to or exceed NIST LoA 3.

Identity-proof Providers and Organizational Representatives at LoA 3, Identity-proof patients at LOA2 or better.

The NIST LoA 3 standard requires cross-certification by the credential issuer with the FBCA when relying upon those credentials for equivalence. The FBCA Basic LoA may be obtained by in-person or remote vetting processes whereas FBCA Medium is in-person only, including an antecedent in-person option. When the remote identity proofing processes are utilized, there are additional controls required by the issuing CA in validating the claimed address of the PKI Subscriber. FBCA Medium meets the highest assurance in identity as identified by the FHA risk assessment[2] for federal agencies relying upon credentials issued for Direct messaging purposes, and is the minimum assurance that requires actual FBCA cross-certification of the issuing CA as recommended by the Federal Health Architecture's Directed Exchange Workgroup.

[1] http://www.idmanagement.gov/sites/default/files/documents/FBCA Certificate Policy v2.27.pdf

[2] http://www.healthit.gov/sites/default/files/final_-_fha_directed_exchange_risk_assessment_pertaining_to_federal_agencies_508.pdf

The ONC Direct Guidelines specifically excluded Patient identity verification processes from its set of recommendations. These Direct Guidelines require that:

- ONLY individuals with a legal affiliation to the named organization in an organizational certificate (e.g. employees, professionals, contractors, etc.) are eligible to use that certificate.
- An organizational representative is only authorized on behalf of his/her own organization – by definition – and therefore separate organizations cannot share a single organizational certificate. This has the effect of requiring different legal entities who wish to use Direct organizational certificates, to have a unique Fully Qualified Domain Name (FQDN) as a health domain assigned for their specific organization. A HISP that manages Direct services for more than one organization, must be able to provision each organization they service with a unique health domain, and by necessity will then have different organizational certificates for each of those organizations.

The May 2013, *ONC Direct Guidelines to Assured Security and Interoperability* recommended that non-patient Direct addresses only be issued to individuals and organizations that have been identity proofed to at least the equivalent of NIST LoA 3. This places specific requirements around the Identity proofing processes of the Registration Authority (RA) responsible for ensuring the identity being bound to Direct address(es) represented by cryptographic keys in a given Direct certificate. These processes will be detailed in a Certification Practices Statement (CPS) or Registration Practices Statement (RPS) that corresponds to the appropriate CP being utilized to govern the certificate issuance process (e.g. DirectTrust CP), and by which the RA is audited against.

IDENTITY-PROOFING FOR PATIENTS/CONSUMERS.

The Health IT Policy Committee (HITPC) has published recommendations[3] regarding patient access to PHI almost simultaneously to the ONC Direct Guidelines in 2013. These guidelines can be taken as guidance for what LoA is appropriate for proofing patients prior to the issuance of Direct certificates for that community.

The DirectTrust community has published a recommendation[4] that Direct certificates for patients also be proofed to LoA3, the same as for providers, however, DirectTrust also recognizes multiple LoAs within its policy framework which facilitates a use case based approach for securing Direct messaging with patients.

[3] http://www.healthit.gov/sites/default/files/hitpc_transmittal_050313_pstt_recommendations.pdf

[4] http://www.directtrust.org/policies-public Consumer/Patient Identity Proofing Prior to Issuance of a Direct Credential v1.1 PDF

FHA has conducted a risk assessment for the implementation of Direct messaging and also advocates a use case-based approach for securing Direct messaging with patients. FHA considers LoA 2 to be sufficient for some patient-based use cases but agencies should individually consider controls necessary to mitigate patient identity misrepresentation when using Direct messaging under a specific use case scenario.

FHA has indicated that use of patient-based Direct Organization Certificates may be appropriate when there is an association with a common service provider with whom the patient has entered into an agreement[5] to manage Direct messaging on their behalf (e.g. a patient portal for a particular provider office.) Regardless of what LoA is accepted for patient subscribers to a Direct organizational certificate, the FHA recommends that the ISSO at the HISP (where HISP services are used) and the organizational rep for the service in question be identity proofed to LoA 3 to ensure maximum trust in key responsibilities. It is anticipated that this requirement will be embodied in controls required for acceptance into Federal Direct Trust Bundles.

In such a scenario, all patient/consumer subscribers MUST authorize the organizational representative of the associated organization to act on their behalf in the fulfillment of the obligations related to the organizational certificate and the healthcare domain it protects. All patient/consumer subscribers MUST also grant the organizational representative and ISSO at the HISP a release to access and manage any PHI contained in messages to Direct accounts protected by the organizational certificate in a manner appropriate and sufficient for the fulfillment of their service obligations. The RA must confirm that such representations are made in an appropriate legally binding agreement as part of the certificate provisioning process.

ADDITIONAL ORGANIZATIONAL CONSIDERATIONS

In addition to individual identities there are also organizational vetting requirements whenever an organizational affiliation exists. In this case, the following items must also be verified to the applicable NIST/FBCA/DT requirements:

- The identity of the requesting representative (e.g. from the Information Systems Security Office or equivalent) of the organization
- The representative’s authorization to act on behalf of the organization,
- The organization’s name and address, and
- Verified documentation of the existence of the organization.
- The organization must also qualify to be issued Direct credentials by:

[5] The Direct Trust CP requires Subscriber Agreements for all Subscribers. For patients, this would typically be handled via click-through an “Acceptable Use Policy” the user must agree to before accessing the portal or services technology.

- must be a HIPAA covered entity, a business associate of a HIPAA covered entity, or an organization that is involved in health care related activities
- agrees to hold themselves to the same security requirements as provided in the HIPAA Security Rule

DirectTrust, along with the Electronic Healthcare Network Accreditation Commission (EHNAC) have defined and operate an accreditation program for certifying the implementation of Direct infrastructures in accordance with both the ONC Guidelines and the DT CP, and in compliance with HIPAA privacy and security requirements. The DT Agent Accreditation Program (DTAAP) certifies three types of entities:

- **Health Information Service Provider** – the HISP operates the infrastructure necessary to send and receive Direct messages in accordance with the Direct protocol and trusted through compliance with security and privacy regulations. The HISP relies upon Direct certificates to perform many of its functions.
- **Certificate Authority (CA)** – the CA issues Direct certificates after confirming identities are bound to specific cryptographic keys. The CA publishes periodic validation information about the certificate and provides ways to manage the certificate during its valid life cycle.
- **Registration Authority** – the RA performs identity proofing on entities and confirms their eligibility to hold or continue to hold a Direct certificate.

DIRECTTRUST AGENT ACCREDITATION PROGRAM (DTAAP)

As indicated above, DirectTrust (DT) is a commercial non-profit trade association that was granted funding by ONC to set up a national Direct-based trust infrastructure. (DT) has published a CP that defines LoAs for Direct certificates based on NIST SP800-63 in terms of Identity proofing, however there are additional community qualifications that must also be met before a Direct certificate can be issued. The DT CP requires provisioning Direct to only one of the following classes of entities: a) a HIPAA covered entity; b) a business associate of a HIPAA covered entity; or c) a person or organization who is involved in health care related activities and voluntarily agrees to be bound by HIPAA privacy and security rules: or d) a patient or healthcare consumer.

Each Direct certificate requires that any subscriber (e.g. user) of that certificate be proofed in accordance with the corresponding CP, to the LoA included in the certificate. Within the DirectTrust community for example, the DirectTrust Agent Accreditation Program (DTAAP) certifies that this ID Proofing requirement is being met prior to the issuance of a DirectTrust certificate – any policy being relied upon for certificate issuance for protecting Direct messaging should specifically address this requirement. An RA is responsible to ensure that proofing requirements are met prior to issuance of a Direct certificate, and should receive assurances from appropriate representatives that any user subsequently provided access to a Direct account protected by that certificate, will first be identity proofed to the equivalent or a higher LoA as specified in the certificate.

The DTAAP provides a way to ensure that each of the three classes of entities within the trust framework are accredited to be performing their respective roles in accordance with the Direct protocol, the ONC and FHA Guidelines, DirectTrust policies and HIPAA privacy and security regulations. In particular, DTAAP ensures that identities are proofed at the requisite LoA by an RA prior to the certificate being issued by the CA and used by a HISP to provide Direct messaging on behalf of the HISP's subscribers.

Each Direct certificate issued by a DTAAP accredited CA requires that any subscriber (e.g. user) of that certificate be proofed in accordance with the corresponding CP to the LoA included in the certificate. DTAAP certifies that this ID Proofing requirement is being met prior to the issuance of a DirectTrust certificate. The ONC Guidelines require that any policy being relied upon for certificate issuance for protecting Direct messaging should specifically address this requirement. An RA has the responsibility to ensure that proofing requirements are met prior to issuance of a Direct certificate. The RA should also receive assurances from appropriate representatives that any user subsequently provided access to a Direct account protected by that certificate will first be identity proofed to the equivalent or a higher LoA as specified in the certificate.

Comparing Direct Domain and Address-bound certificates

A Direct domain bound certificate will always have an organizational affiliation and the May 2013 ONC Direct Implementation Guidelines require that different organizations be represented by different domains (and therefore by different certificates.) A Direct address-bound certificate may have an organizational affiliation (i.e. if it represents a common inbox for multiple individuals within an organization, or a service queue for the organization.) In either of these cases, an Organization Representative must be identified and accept responsibility for the use of the certificate on behalf of all organizational users. If a Direct address certificate represents an account held by a single user, then verification of organizational affiliations may not be required.

Regardless of whether an address- or domain-bound certificate is used for Direct, every individual with access to use an account protected by that Direct certificate is considered a subscriber to the certificate. Each subscriber of a Direct certificate must be identity proofed to the LoA included in the certificate before being granted access to use it.

For a HISP-managed Direct address certificate issued to a single individual, there will be at least two proofing events required by the RA prior to issuance of the certificate: 1) for the Information Systems Security Officer (ISSO) or equivalent at the HISP who has responsibility to protect and manage access to the corresponding private key; and 2) for the individual to whom the certificate is issued and who uses the corresponding Direct address contained in the certificate for Direct messaging.

When a HISP-managed Direct Organization Certificate is issued there will also be at least two entities proofed by the RA prior to issuance i.e. the ISSO at the HISP, and an organizational representative who accepts responsibility for the use of the credential on behalf of the organization or affiliation. A key responsibility of the organizational representative is to ensure that any user of the certificate subsequently granted access to it must qualify to do so by having an appropriate organizational relationship and must also be proofed to the LoA specified in the certificate prior to being granted access to a Direct account secured by that certificate. It should be noted that in the case of Direct Organization Certificates, the ID proofing of certificate subscribers granted access to use the certificate after its issuance may not necessarily be completed by an audited entity (i.e. the RA.) Instead, this responsibility may be conducted by the organizational representative or a designated representative. As discussed in the previous section, if the Organizational cert is used in a patient context where the LoA it is issued at lower than level 3 (e.g. a use case that supports LoA2 for patients/consumers) then FHA still requires the HISP ISSO and corresponding Org Rep users to be identity proofed at LoA3 regardless. This facilitates strong accountability for the key responsible parties managing the use and access to the private key associated with the certificate.

Comparison Summary. The following table provides comparative information for Direct address and domain-bound certificates for criteria that may be applicable to a specific use case: Y=Yes, N=No, C=Conditionally Yes (with condition described in the footnote)

Figure 1 Comparison of Direct Certificate Types

#	CRITERIA	ADDRESS-BOUND	DOMAIN-BOUND
1	Direct address bound to certificate?	Y	N
2	Identity proofing verifies individual has right to the Direct address?	Y	C[6]
3	Provides resistance to "Header Vulnerability" attack?	Y	C[7]
4	Direct mail can be sent to a recipient's Direct address?	Y	Y
5	Limits cost impact for patient use of Direct	C[8]	C[8]
6	Simple management model	C[9]	C[9]

[6] The owner of the domain is responsible for ensuring that the individual has the right to the Direct address. Degree of trust in this process is based on the policies of the specific trust framework.

[7] Requires that parties implement and follow the recommendations of the Direct Implementation Guide. Receiving parties should only use the Direct address inside the encrypted envelope for routing to the specific end-point.

[8] Where cost of certificate issuance is significant, the use of Domain bound certificates can reduce this burden. However, it should be noted that the primary cost of certificate issuance is typically the identity validation of the individual to a specific LOA. There may also be an impact on cost with large turnover or where multiple certificates may be needed for the same individual (e.g. when issuing certificates for each patient-provider relationships)

[9] Address bound certificates may require the management of a large number of certificates by the STA. Domain bound certificates reduce this STA burden, but requires the management of end-point validation by each Domain.

A Note on Non-Repudiation

A PKI certificate has the ability to include an indicator that its subscriber/user should not be able to repudiate transactions secured with the certificate. When more than one subscriber has access to use a certificate the relying party does not necessarily have any way of verifying which subscriber used the certificate for a given transaction. This situation occurs in Direct primarily when the certificate is a domain bound certificate or an address bound certificate issued to an organization address (e.g. department). Under FPKI policies, the concept of a Group certificate is recognized where more than one subscriber has access to use a digital certificate and its corresponding private key. When a certificate is a Group certificate, it is not appropriate to include the indicator that non-repudiation can be conveyed by just the use of the certificate alone[10].

For this reason the ONC Guidelines recommend that the non-repudiation bit NOT be set in Direct certificates. This does not mean that Direct is not capable of providing non-repudiation on the messages, rather that the certificate alone is not sufficient to convey this. The ability to provide non-repudiation via Direct is still achievable, but it means that the binding and trust in user authentication by the HISP and the security of their Direct implementation must also be taken into account. Non-repudiation of Direct messages is therefore possible but is also reliant on HISP policy, and one purpose of DTAAP accreditation is to ensure that HISPs have implemented the required policies and processes to achieve this.

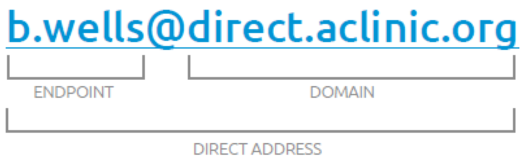
- Providers that are using Direct certificates MUST be proofed to at least LoA 3, In person or antecedent.
- Agencies may accept Non-provider users of Direct certificates e.g. patients and consumers, who have been at least proofed to LoA2, under some use cases

[10] When Direct uses the X.509 group certificate for organizations (Domain bound) or shared addresses (Address bound, but issued to non-individuals), the certificate is available to many users, albeit with a primary subscriber who accepts responsibility for its use on behalf of the group of users. In addition, even for address bound certificates issued to an individual, *any Healthcare Organization (HCO) that employs a HISP for services will have, as one of the subscribers of their certificates, the HISP ISSO who has responsibility to control logical and physical access to key material. It may be possible however under more proscriptive trust frameworks built upon PKI e.g. FPKI Group Certificates, DirectTrust, DEA EPCS etc, where certification of processes that control access to private keys is also evaluated and audited, to re-establish non-repudiation through the surrounding processes, even though this is indirect of certificate use alone. Under such frameworks, some dispute resolution process is invoked whenever a group member wishes to repudiate a transaction, and the system has controls that track external to the certificate, the access and use of key material for any given transaction. Absent any trust framework that certifies such systems however, an obvious way to obtain non-repudiation of a Direct message is to apply a digital signature directly to the message itself using a credential in continuous exclusive control of the sender.*

Appendix A, Introduction to Direct Certificates

DIRECT ADDRESSES

The Direct Applicability Statement for Secure Health Transport[11] defines the terms and processes for implementing Direct in a standardized way. The Applicability Statement defines Direct Addresses, which typically resemble standard email addresses, but differ in that they are dedicated exclusively for health information exchange where the privacy of personal health information (PHI) must be protected. The addresses consist of two parts – a healthcare endpoint (on the left side of the @ sign) and healthcare domain (on the right side of the @ sign) and a e.g.:



Applicability Statement: *Healthcare Endpoint Names express real-world origination points and endpoints of health information exchange, as vouched for by the organization managing the Health Domain Name. Example: johndoe (referring to in individual), sunnyfamilypractice, memoriallab (referring to organizational inboxes), diseaseregistry (referring to a processing queue).*

DIRECT CERTIFICATES

The Applicability Statement then defines two types of X.509 digital certificates for use within Direct:

- Direct Address Certificate
- Direct Organizational Certificate

The Direct X.509 certificate identifies participants in the exchange using standard email addresses associated with the cryptographic keys assigned to the certificate. An appropriate Certificate Policy (CP) e.g. DirectTrust CP, defines (among other requirements) the set of controls that must be observed when issuing Direct certificates – including: whose identities must be validated; the valid lifetimes of the certificate and associated keys; and the acceptable usages for which the certificate is authorized.

Direct Address Certificate

A **Direct Address Certificate** behaves like a standard Secure/Multipurpose Internet Mail Extensions (SMIME) certificate for securing Direct information exchanges. It contains a full

[11] http://wiki.directproject.org/file/view/Applicability%20Statement%20for%20Secure%20Health%20Transport%20v1.1.pdf/353270730/Applicability%20Statement%20for%20Secure%20Health%20Transport%20v1.1.pdf

Direct address in the Subject Alternative Name (SAN) extension field in the certificate e.g. Endpoint+@+Health Domain, to denote that the associated cryptographic keys are bound to that specific Direct address only (e.g. scott.rea@direct.digicert.com).[12]

Direct Organizational Certificate

A **Direct Organizational Certificate** is a single SMIME certificate for securing Direct information exchanges. It contains a Health Domain as a Fully Qualified Domain Name (FQDN) in the SAN extension field in the certificate, to denote that the associated cryptographic keys are authoritative for any Direct address that is provisioned within that FQDN, e.g. direct.DigiCert.com would be authoritative for Dr.Bob@direct.DigiCert.com; or scott.rea@direct.DigiCert.com; or clinicA.inbox@direct.DigiCert.com; (i.e. any Direct Address that has a Health Domain of direct.DigiCert.com). This Organization Certificate can be used to secure any healthcare endpoint whose Direct address is of the format endpoint@direct.DigiCert.com).

Issuing Direct Certificates

When issuing either type of certificate, the Applicability Statement indicates methods for ensuring the correct identity of the sender and receiver in the transaction will be dependent on:

- the policies governing, and the methods used for certificate issuance;
- identity assurance; and
- authentication to services for Directed messaging in operational use

The certificate issuance and identity assurance aspects are covered within the applicable CP governing the issuance and management of the Direct certificates being used.

[12] The Direct protocol allows a HISP (see below) to manage Direct services on behalf of a user, but does not require it, e.g. an end point might directly manage their own certificates.