Certificate Discovery for Direct Project Implementation Guide

Version 4.1, 20 August 2015

Revision History

Date	Document Version	Document Revision Description	Revision Owner
2011-10-19	1.1	Revisions from F2F meeting	Ken Pool
2011-10-24	2.0	Revisions from Bob Dieterle	Bob Dieterle
2011-11-09	3.0	Revisions from Ken Pool	Ken Pool
2011-12-14	4.0	First revision following comments	Ken Pool
2015-08-20	4.1	Revision addressing corrections and clarifications identified by the Direct Certificate Discovery Tool (DCDT) team.	

Original Authors

Workgroup Lead	Ken Pool, OZ Systems
Workgroup Lead	Sri Koka, Techsant Technologies
Participating Author	Peter Bachman, Cequs Inc.
Participating Author	Bob Dieterle, EnableCare
Participating Author	Ernest Grove, SHAPE HITECH, LLC
Participating Author	Lester Keepper, SHAPE HITECH, LLC

1. Introduction

The Provider Directories Initiative focuses on identifying the requirements, core data set, and standards to support two specific use cases: Discovery of Digital Certificates for the Direct Project; and Discovery of Electronic Service Information (including electronic address and any required security information) in order to support the electronic exchange of health information.

The health care industry has utilized provider directories for years. The content of individual directories has varied substantially based upon intended use and audience. The Provider Directories Initiative created within the S&I Framework is not intended to replace existing directories - its primary goal is to support the electronic exchange of health information in a secure fashion.

This Implementation Guide addresses the use case for discovery of digital certificates for the Direct Project using a hybrid approach based on DNS and LDAP. The Direct Project DNS Configuration Guide addresses the discovery of digital certificates stored in DNS CERT records. The hybrid approach to discovery of digital certificates extends the work described in that document to enable the universal discovery of certificates via LDAP services.

Briefly, this guide’s approach for Direct Project certificate is:

DNS is used as the entry point leveraging its global discoverability.

LDAP is used when the DNS record does not support the CERT record or when LDAP is preferred by the publisher.

See Section 3.1 for a detailed description.

This guide provides specific technical guidance on:

Publishing and discovering LDAP services using the DNS SRV record.

Querying an LDAP service for digital certificate discovery using anonymous binding for a specific Direct Project address.

The digital certificate(s) obtained from the query facilitate the secure exchange of health information.

1.1 Purpose

This Implementation Guide enables providers and others to electronically obtain the digital certificate of a desired destination to support secure transfer of health information.

Adopting and implementing this guide’s approach to certificate discovery provides the following benefits:

The ability for providers and other authorized entities to retrieve digital certificate(s) to facilitate secure exchange of health information

A standardized query mechanism for Certificate Directories that can be adopted by EHR and HIE vendors, State HIEs, HISPs and other mediators of exchange

The standardization and simplification of the implementation of interfaces to query Certificate Directories

1.2 Scope

The scope of this guide addresses a single scenario - in it, the digital certificate requester has a Direct Address associated with the digital certificate(s) being requested and queries a Certificate Directory to retrieve the digital certificate(s):

Scenario 1: The digital certificate requester or the digital certificate requester system has a known Direct Address associated with the digital certificate being requested. The digital certificate requester’s system does not have the digital certificate(s) associated with the Direct Address. The digital certificate requester system sends a query to the Certificate Directory without user intervention. The Certificate Directory returns zero or more digital certificate(s) associated with the Direct Address. The digital certificate requester performs Certificate Validation on the digital certificate returned by the Certificate Directory. The digital certificate requester selects the correct digital certificate(s) for the intended use when multiple certificates are returned.

1.3 Audience

This Implementation Guide is intended to assist providers, payers, and any other health care organization that wants to participate in secure health information exchange. Specifically it informs:

Vendors/Developers, who need to understand, design, and develop Direct project compliant messaging.

HISPS/Providers who are configuring DNS and LDAP services to support Direct certificate discovery.

Registration Authorities/Certificate Authorities who certify health care organizations and/or individuals and issue Direct digital certificates.

1.4 Assumptions

The Certificate Discovery for Direct Project Implementation Guide assumes the following:

The certificate recipient will validate the certificate but this is not covered in this guide.

Access to digital certificates for the Direct Project is assumed to be world readable.

The Provider, Patient, and health care organizations and individuals who implement the Use Case will use the guide to enable interoperable exchange of protected health information (PHI) using Direct Project messaging.

The Implementation Guide continues the methodology for defining needs, selecting and developing standards, and implementing those standards in a testable, sustainable way via the “Standards and Interoperability Framework – Use Case Development and Functional Requirements for Interoperability."

The reader is familiar with the Direct Project.

The Direct address is the canonical address.

2 Development of Guidance

The Certificate Discovery for Direct Project Implementation Guide provides specific guidance for the development, implementation, and ongoing discovery of S/MIME digital certificates for known Direct defined addresses. To develop this guidance, the S&I Framework PD sprint team investigated currently available options for an open and universally accessible approach to discovering S/MIME digital certificates using only the Direct address. The investigation focused on two specific, highly deployed technologies – DNS and LDAP. The hybrid approach to discovery of digital certificates is based on the findings of this investigation.

This hybrid approach ensures:

That the digital certificate can be obtained if located in a DNS CERT record

That the digital certificate can be obtained if located in an LDAP implementation

That existing DNS implementations that do not support CERT can facilitate locating the digital certificate

That data contained in LDAP implementations by health care organizations that store S/MIME certificates can contribute to this use case.

A complete summary of the team’s findings can be found in Appendix D: Development of Guidance.

3 Implementation Guide

As defined by Direct project, a “Security Trust Agent (STA)” refers to the actor who has a Direct address to which they wish to send information and for which they need to obtain the associated digital certificate. In general, we expect the STA to actually be an application or a service used by the sender. The “Publisher” refers to the actor who has digital certificates for specific Direct addresses and wishes to make those digital certificates available for use. We also will refer to the organization Direct address DNS record as the full domain specification consistent with the Direct Project Rules of the Road communities.

We assume that both the consumer application and the publisher are familiar with the basics of DNS and LDAP. We also assume they both adhere to industry best practices in their use of these technologies. Lastly, we assume the reader is familiar with the Direct Project Rules of the Road and especially the Direct Project – Applicability Statement for Secure Health Transport.

Briefly, this guide’s approach for Direct Project certificate discovery is:

- DNS is used as the entry point leveraging its global discoverability.
- LDAP is used when the DNS record does not support the CERT record or is preferred by the publisher.

See Section 3.1 for a detailed description.

DNS allows for multiple Resource Records (RR) that support the storage of a number of different content types.

This guide uses RR capability in two ways. First, a digital certificate can be stored in a CERT RR if the CERT RR has been entered into a DNS zone record. Second, the domain name and port information for an LDAP service can be stored in a SRV RR as defined by RFC-2782, “A DNS RR for specifying the location of services (DNS SRV)”. The SRV RR standard also allows for multiple LDAP service instances to be advertised with a standard protocol for establishing the relative priority among them.

For this guide, the STA is expected to establish their criteria for what they consider a valid digital certificate for their use. For guidance on validating certificates for use in Direct, see the policies as detailed in Direct Project – Applicability Statement for Secure Health Transport Section 4.0 and Direct Communities of interest for specific stakeholders.

While security surrounding the proper use of digital certificates is beyond the scope of this initiative the STA may wish to consider whether the DNS resolver implements DNSSEC to protect against security flaws.

3.1 DNS/LDAP Hybrid Digital Certificate Discovery Model

The following flow is intended to describe the logic. During the process below, the consumer will need to query DNS once or several times depending on the implementation using the known Direct address (full email address such as billy.bob@direct.stelsewhere.org) and the domain address (e.g. direct.stelsewhere.org).

The hybrid process flow is as follows:

Using the known Direct address and domain the consumer queries DNS;

Using the DNS response data the consumer determines if there is a CERT resource record for the individual;

If a valid digital certificate for the individual is returned then that certificate should be used;

Using the DNS response data the consumer determines if there is a CERT resource record for the Direct domain;

If a valid digital certificate for the organization Direct domain is returned then that certificate should be used;

Else the consumer must examine the DNS response for a SRV resource record for the LDAP service;

If a valid LDAP resource is identified then the consumer must submit the Direct address to that service with anonymous binding;

If a valid digital certificate is returned then that certificate should be used;

Else if no usable LDAP SRV resource record is returned or no valid digital certificate is returned then the consumer must use some other approach to obtain the certificate of interest.

3.2 Guidance for directory publishers

The decision as to where digital certificates are published is at the discretion of the publisher.

3.2.1 DNS Publishing

For the DNS publisher the primary guidance has already been established and is detailed in the document Direct Project: Applicability Statement for Secure Health Transport.

Consistent with the Direct Project guidance, the certificate must be validated to a known trust anchor upon use, and therefore is not dependent on an initial validated response protocol to a query for a certificate. This allows the certificate to be published anywhere.

3.2.2 LDAP Publishing

3.2.2.1 LDAP considerations

X.500/LDAP protocol allows for three types of native access or "binding".

Anonymous

Password

Strong Authentication with Digital Certificate

For this use case, the LDAP implementation must allow anonymous binding.

In LDAP the inetOrgPerson schema allows for all the information needed to support this use case. Specifically, the Direct address must be the “mail” attribute and the digital certificate must be the userCertificate attribute.

The directory must make the “mail” and the “userCertificate” attributes of inetOrgPerson available for this use case.

A Digital Certificate for use for the Direct Project must be published in a 'person' entry using the well-established inetOrgPerson schema. When a Direct Project endpoint (e-mail address) is not an individual but a department or whole organization, this guidance recommends that this be represented as a 'person' entry as defined above.

In this use case, returning information other than the “mail” and “userCertificate” attributes may reveal confidential information; this has the implication that one’s internal LDAP directory will not be used to serve the Internet as typically configured. A typical solution is that the relevant information from an internal LDAP directory can be exported (via a secure air gap) to a border/proxy LDAP server for this use case.

3.2.2.2 DNS SRV resource record for LDAP server discovery

Once the LDAP service is available and configured, the corresponding DNS entry must have an associated DNS SRV resource record to allow a consumer to locate the service.

DNS SRV resource records are defined by RFC-2782. In the SRV resource record for an LDAP service:

- The service field must be "_ldap",
- The proto field must be "_tcp",
- The name field must be a Direct Project health domain name (see Section 3.3 and its subsections below for more on health domain names),
- The port field must be set to the TCP port on which the LDAP service is available (the conventional port for LDAP is 389), and
- The target field must be the domain name of the LDAP service.

The values of the remaining SRV resource record fields are as discussed in RFC-2782.

If the publisher has multiple LDAP implementations it wishes to advertise, each must have its own associated SRV record.

The publisher may find a utility known as Domain Information Groper (dig) useful to examine their SRV records.

3.3 Guidance for directory consumers

If the consumer already has a valid certificate or knows how to obtain a valid certificate from a directory then that certificate may be used.

This use case is intended for the circumstance where the consumer needs to obtain the certificate.

For this guidance the “health domain name” is as defined by Direct Project: Applicability Statement for Secure Health Transport. A Direct Project endpoint address is defined as being composed of two parts: the "health domain name" (aka health-domain-name) and the "Health Endpoint Name" (aka health-endpoint-name) combined in the format <health-endpoint-name@health-domain-name>, which is the commonly understood e-mail address.

The following flow is intended to describe the logic. During the process below, the consumer will need to query DNS once or several times depending on the implementation using the known Direct address (full email address such as billy.bob@direct.stelsewhere.org) and the domain address (e.g. direct.stelsewhere.org).

The hybrid process flow is as follows:

Using the known Direct address and domain the consumer queries DNS;

See Direct Project: Applicability Statement for Secure Health Transport

Using the DNS response data the consumer determines if there is a CERT resource record for the individual;

If a valid digital certificate for the individual is returned then that certificate should be used;

Using the DNS response data the consumer determines if there is a CERT resource record for the Direct domain;

If a valid digital certificate for the organization Direct domain is returned then that certificate should be used;

Else the consumer must examine the DNS response for a SRV resource record for the LDAP service;

See Section 3.3.1 below

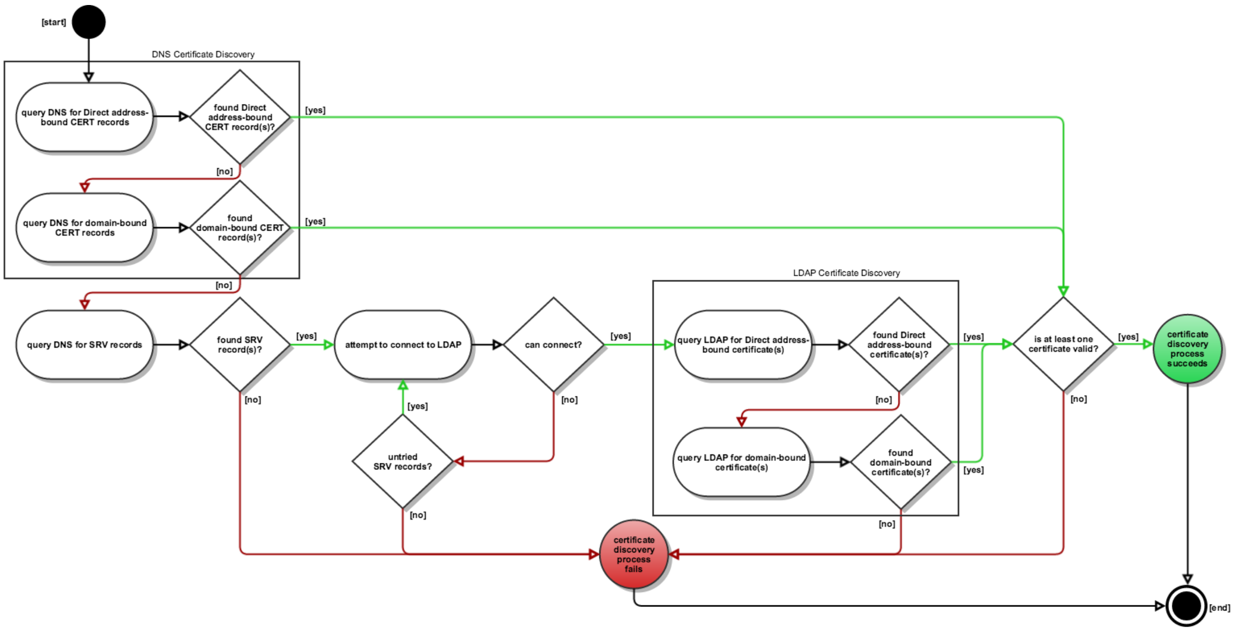
If a valid LDAP resource is identified then the consumer must submit the Direct address to that service with anonymous binding;

See Section 3.3.2 below

If a valid digital certificate is returned then that certificate should be used;

Else if no usable LDAP SRV resource record is returned or no valid digital certificate is returned then the consumer must use some other approach to obtain the certificate of interest.

This flow process is diagramed below:


[start]
DNS Certificate Discovery
query DNS for Direct address-bound CERT records
found Direct address-bound CERT record(s)?
[yes]
[no]
query DNS for domain-bound CERT records
found domain-bound CERT record(s)?
[yes]
[no]
query DNS for SRV records
found SRV record(s)?
[yes]
[no]
attempt to connect to LDAP
can connect?
[yes]
[no]
untried SRV records?
[yes]
[no]
LDAP Certificate Discovery
query LDAP for Direct address-bound certificate(s)
found Direct address-bound certificate(s)?
[yes]
[no]
query LDAP for domain-bound certificate(s)
found domain-bound certificate(s)?
[yes]
[no]
is at least one certificate valid?
[yes]
[no]
certificate discovery process succeeds
certificate discovery process fails
[end]

3.3.1 DNS Query for CERT record

Normally DNS queries are executed as UDP which has a limitation on the size of the response. In the event that the response is over the limit then one must repeat the query using TCP.

The certificate responses for this usage could be over the implemented UDP size limit.

Thus, the Direct Project: Applicability Statement for Secure Health Transport Section 5.4 encourages starting with TCP:

The DNS protocol can run on either UDP or TCP. Both methods use Port 53. STAs should be aware that certificate records are likely to overflow UDP buffer limits and will need to upgrade to TCP or use TCP by default.

3.3.2 DNS Query for LDAP SRV record

This section describes the discovery of LDAP service endpoints given a Direct address.

In order to discover the LDAP directory that has knowledge about the endpoint address, we first must find the LDAP directories that are available to support queries on the 'health-domain-name'.

The consumer must query for an LDAP SRV resource record based on the health domain from the Direct address consistent with Direct Project: Applicability Statement for Secure Health Transport. The query must be executed as specified in RFC-2782, for example "_ldap._tcp.health-domain-name.com".

In any LDAP SRV resource record returned, the response will include the priority value, the weight value, the port, and the domain name; as noted above, the conventional port for LDAP services is 389. The "Usage rules" section of RFC-2782 details how the consumer should use this information to contact the associated LDAP services.

3.3.3 LDAP query

We now use LDAP queries to discover the available Digital Certificates for the endpoint address. This must be done using RFC-4510 - Lightweight Directory Access Protocol (v3) Technical Specification Road Map, and the schema for individuals -- RFC-2798 - Definition of the inetOrgPerson LDAP Object Class. Specifically the e-mail address must be searched for in the "mail" attribute, and the Digital Certificate must be returned in the "userCertificate" attribute.

The LDAP query steps are:

Bind to the Directory using LDAP v3 anonymous authentication

Anonymous authentication must be used to access the LDAP Directory. Anonymous authentication is described in the RFC-4511 in Section 4.2 Bind Operation.

Discover the Base DNs

Branches in LDAP must be defined by a “Base DN”. The list of Base DNs that are provided by a LDAP directory are found by doing a LDAP Query with a NULL (i.e. “”) Base DN, and ObjectClass=”DN”.

Query across the Base DN for entries where "mail" contains the endpoint address

The LDAP query must search for a valid certificate using each of the "Base DN" found for the "mail" attribute equal to the Direct address.

Scope must be set to "subtree" to allow for multiple branches to the tree defined by the returned Base DN.

The attributes must include "userCertificate" to assure that this attribute is returned if it is available. Note that, strictly speaking, RFC-4523 Section 4.1 dictates that the userCertificate be requested using the binary encoding option defined by RFC-4522 (i.e., "userCertificate;binary"). However, due to the defined syntax of the userCertificate attribute, if the binary encoding option is not specified, RFC-4522 Section 5 states that the userCertificate will be returned as binary nonetheless.

For each entry returned, examine the Digital Certificate in the 'userCertificate' attribute for acceptability

Acceptability should be determined as per the Direct Project formal specification Section 4.0 Trust Verification. This is not further constrained by this guide.

3. Appendix A: Acronym List

Refer below for a list of acronyms found in the Certificate Discovery for Direct Project Implementation Guide:

ID	Acronym	Description
1	DIT	Directory Information Tree
2	DN	Distinguished Name
3	DNS	Domain Name System
4	EHR	Electronic Health Record
5	FPKI	Federal Public Key Infrastructure
6	HIE	Health Information Exchange

7	HISP	Health Information Service Provider
8	HITSC	Health Information Technology Standards Committee
9	ICANN	Internet Corporation for Assigned Names and Numbers
10	IP	Internet Protocol
11	LDAP	Lightweight Directory Access Protocol
12	NwHIN	Nationwide Health Information Network
13	OCSP	Online Certificate Status Protocol
14	PD	Provider Directories
15	PHI	Protected Health Information
16	RR	Resource Records
17	S&I	Standards and Interoperability
18	S/MIME	Secure/Multipurpose Internet Mail Extensions
19	STA	Security Trust Agent
20	TCP	Transmission Control Protocol
21	UDP	User Datagram Protocol

4. Appendix B: References

Refer below for a list of documents referenced in the Certificate Discovery for Direct Project Implementation Guide:

ID	Reference Document	Description
1	The Direct Project DNS Configuration Guide	Guide to Direct DNS configuration specifications required for successful operation
2	Direct Communities of interest for specific stakeholders	A list of Direct communities at various stages of development
3	Direct Project – Applicability Statement for Secure Health Transport	This document describes how to use SMTP, S/MIME, and X.509 certificates to securely transport

health information over the Internet

4 Direct Project Rules of the Road Direct Project rules and best practices to establish trust communities

5 RFC-2782 A DNS RR for specifying the location of services (DNS SRV)

6 RFC-2798 Definition of the inetOrgPerson LDAP Object Class

7 RFC-4510 Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map

8 RFC-4511 Lightweight Directory Access Protocol (LDAP): The Protocol

9 RFC 4522 Lightweight Directory Access Protocol (LDAP): The Binary Encoding Option

10 RFC 4523 Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates

11 S&I Framework – Use Case Development and Functional Requirements for Interoperability

12 Overview of Use Case and Functional Requirements development process followed by the S&I Framework

5. Appendix C: Suggested Reading

The following documents provide additional context about the purpose and recommendations in this implementation guide.

To begin with, the reader should have a clear understanding of the Provider Directory Query for Digital Certificate Use Case for Direct Project and functional requirements in order to understand this implementation guide. The information regarding this use case can be found in the location:
http://wiki.siframework.org/Query+for+Digital+Certificate+Use+Case+for+Direct+Project

The DIRECT project recommendations have been used in this use case in order to query and obtain digital certificate to enable secured health information exchange across organization. It is highly recommended to understand how DIRECT project is instrumental in improving the transport of health information, making it faster, more secure, and less expensive. The following link gives overview of the DIRECT project:

http://wiki.directproject.org/The+Direct+Project+Overview

The Direct Project security specifications provide a set of functional requirements that need to be implemented by the various Direct Project technologies and protocols in order to satisfy the message handling policy recommendations of the HIT Policy Committee. This will facilitate Direct Project users or organizations to trust each other in the real world, and can mutually agree on standards, protocols and policies for handling PHI and securely sending messages to each other containing PHI. The Direct project security specifications and service descriptions are documented here:

http://wiki.directproject.org/Direct+Project+Security+Overview

Below are a few other recommended links related to Direct Project which will give insight in terms of workflow, compliance criteria, and RFC's used in the Direct project.

References:

User Stories: The user stories can be used to understand the clinical workflow relevance of the DIRECT specifications.

http://wiki.directproject.org/User+Stories

DIRECT Project Compliance: This provides an overview of the compliance criteria and some examples that help in creating compliant reference implementations and test cases that test compliance.

http://wiki.directproject.org/Direct+Project+Compliance

SMTP Secure Health Transport: Relevant RFC's are embedded in the link for further information

http://wiki.directproject.org/Applicability+Statement+for+Secure+Health+Transport

XDR Simple Health Transport:

http://wiki.directproject.org/XDR+and+XDM+for+Direct+Messaging

The DNS Direct project recommendation review

http://wiki.siframework.org/DNS+Direct+Project+Recommendation+Review

The LDAP Direct project recommendation review

http://wiki.siframework.org/LDAP+Direct+Project+Recommendation+Review

6. Appendix D: Development of Guidance

6.1 Approach

To generate this Implementation Guide, the S&I Framework harmonization team gathered details regarding the provider directory implementation landscape. To expedite the S&I Framework harmonization effort, environmental scans were discussed on sub-workgroup calls. Support team members and members of the harmonization team also conducted a series of phone calls outside of PD workgroup and sub-workgroup calls.

Information obtained is presented as part of the evaluation of standards, maturity of solutions and in the evaluation of specific solution strengths and weaknesses. Relevant sources of information include:

Discussions with the Direct DNS Pilot participants to gather information on their experiences with DNS to date

Outreach to the Health Information Technology Standards Committee (HITSC) and the HITSC Privacy and Security Workgroup to reuse environmental scanning data collected during their provider directory review

Outreach to federal agencies, vendors and provider organizations on the use of LDAP in the delivery of certificates and for purposes similarly scoped to those needed by Direct

6.2 Standards Criteria

A set of standards criteria was developed to evaluate each standard against the requirements defined in the use case. The criteria are broadly based and do not reflect a numeric score. Their intent is to provide factual information about each standard based on a set of understandable data points.

The criteria are listed in the table below:

Criteria Name Description of Criteria Example of Criteria

Suitability Does the standard meet the Query for Digital Certificate use case for Direct Project business and technical requirements? Do DNS and/or LDAP CLEARLY meet the business and technical requirements within the use case?

Compatibility Is there an appropriate migration path from this standard to another standard (does this standard restrict technical choices in the future)?

Can this standard be integrated with other standards to build the desired solution? Do DNS and/or LDAP integrate with each other in a way that would allow one or more standards to be used together in the same organization? Do DNS and/or LDAP support clear migration from one standard to another?

Regulatory Impact Are there jurisdictional and regulatory impacts in using this standard? Would the selection of DNS and/or LDAP have any known policy or regulatory impacts at the national, state and local level?

Data Element Usage Does the standard support all the data elements proposed in the use case (full, comprehensive support)? Do DNS and/or LDAP have underlying data schemas that support the data elements listed in the use case?

Maturity How widely is the standard in use in the United States within the context of the use case requirements? How widely used are DNS and/or LDAP to query digital certificates in healthcare?

Technology Architecture

and Vendor Neutrality Is there an undesired bias toward a given technology architecture or toward the platform of a particular vendor? Do DNS and/ or LDAP favor a specific vendor or a specific

architecture that is proprietary and/or difficult to migrate to?

Availability Is the standard easily available and able to be used/implemented without

barriers? Are DNS and/ or LDAP available freely for use by implementers and vendors and is there some level of support available from the

IT community for these standards?

Expected Total Costs of

Implementation What are the expected total costs of implementation across the industry, disruption of current processes due to conversion, coordination and

communication costs borne by implementers or the lost revenue of current solutions in place that will no longer be useful? If a decision is made to implement DNS and/ or LDAP what is a rough estimate of the total costs of implementation within

health care, are there any anticipated disruptions that might occur during implementation, and are there specific costs for conversion if moving from one standard to another?

Economic Impacts What are the expected business and economic impacts from the selection

of this standard? If a decision is made to implement DNS and/ or LDAP what are the expected business model changes that will need to be supported and what are associated economic issues to consider

for health care stakeholders?

Pilot Recommendations Are there existing pilots using the standard that are aligned to the

use case requirements? How many DNS and/or LDAP pilots are currently in use in the United States that specifically include the requirements of Query for Digital Certificate Use Case?

Conformance Criteria Does the standard have standard conformance language to enable testing? Is there specific conformance testing language written into

DNS and/or LDAP that would allow an organization to test their conformance?

Viability Does the selection of a standard lead to a specific implementation model that is not viable? Would the use of DNS and/or LDAP be commercially or

technically viable in real-world implementation settings?

6.3 Evaluation of DNS

6.3.1 Strengths and Weakness

Strengths Weaknesses

Global availability with centralized root servers controlled by ICANN with a governance structure for domain names.

DNS has been implemented to provide Digital Certificate discovery for Direct Project, albeit pilots at a limited scale. Use of CERT records other than Direct Project have limited implementation history.

DNS servers generally support the SRV record. A significant number of DNS servers currently do not support the CERT record and therefore cannot participate as repositories for Digital Certificates for Direct Addresses.

Attack opportunity limited to client-side, making worldwide compromise unlikely. OCSP revocation is based on HTTP which is further based on DNS; if DNS is compromised revocation may be as well.

6.3.2 Opportunity Costs of failure to use DNS

The failure to implement DNS will affect the global availability of delivering certificates via the DNS protocol.

Failure to leverage ICANN responsibility of the management of top-level domain name space which includes the operation of name server.

Existing DNS only Direct Project Digital Certificate initiatives cannot be leveraged.

6.3.3 DNS Mitigation of Weakness

The primary identified weakness related to DNS for this use case is that many existing DNS servers do not support the CERT record.

6.4 Evaluation of X.500/LDAP

6.4.1 General Strengths and Weaknesses of X.500/LDAP

X.500/LDAP has demonstrated capacity to deliver x509v3 Certificates

X.500/LDAP has sophisticated management tools to facilitate the handling of a large number of Digital Certificates

Off the shelf email applications inherently support LDAP for retrieval of certificates

DNS implementations widely support the SRV record to identify Internet accessible services such as LDAP access to Directories

An X.500/LDAP service is not generally discoverable without a reference to a known root Directory Information Tree or an SRV record

6.4.2 Opportunity Costs of failure to use LDAP

If we fail to incorporate LDAP into the methodologies of this use case, then:

Many widely available commercial-off-the-shelf and open source email programs that already support LDAP for certificate discovery; and

Data contained in LDAP implementations by health care organizations that store S/MIME certificates would be inaccessible and thus would not contribute to adoption of this guidance.

6.4.3   X.500 LDAP Mitigation of Weaknesses

The primary identified weakness related to LDAP for this use case has been stated as a lack of global discovery. Primarily the NwHIN is a set of policies and standards that address national, rather than global standards.

Certificate repository standards are clearly described on the ICAM and FPKI websites for Federal agencies, and participating cross certified Certificate Authorities. This effort is currently done under the organization=U.S. Government entry in the X.500/LDAP certificate repository. One mitigation could be to develop additional resources that are consistent with that Directory Information Tree (DIT), leveraging directories and repositories, which can be located under the current c=US root object as is currently the case for o=US Government.

At the same time, there are multiple directories that may choose to operate independently, on a statewide, or on a regional basis, without adopting the same schema as a national root for NwHIN, and must still be reachable. This is a natural usage for the SRV DNS record to associate the Subject-Alt entry defined by the Direct Project.

6.5 Rationale of Hybrid Approach

Based upon our evaluations of DNS and LDAP it is clear that neither of them currently provides a complete solution for this use case. Each of them offers specific strengths as well as limiting weaknesses. It became apparent that their strengths and weaknesses were essentially complementary.

The workgroup endeavored to establish a method that synergistically leveraged their strengths. In this use case the assumption is that a “consumer” knows a direct address and needs to obtain the digital certificate to enable secure communication. This use case also recognizes that a digital certificate may be associated with a specific address or may be associated with a direct domain. Thus the first problem facing the consumer is to find a resource that can provide the certificate, in other words, global discoverability is the first challenge.

Since global discoverability is a strength for DNS and a weakness for LDAP, we elected to use DNS first. Although many DNS implementations do not support the CERT record, if the direct address in question is in a DNS implementation that does support the CERT record and the certificate is present, then it can be obtained from DNS.

LDAP is designed for accessing Digital Certificates when the LDAP server location is known. We elected to locate LDAP services using the SRV record support in DNS.

This hybrid approach ensures:

That the digital certificate can be obtained if located in a DNS CERT record

That the digital certificate can be obtained if located in an LDAP implementation

That existing DNS implementations that do not support CERT can facilitate locating the digital certificate

That data contained in LDAP implementations by health care organizations that store S/MIME certificates can contribute to this use case.