The Office of the National Coordinator for Health Information Technology

Certificate Interoperability S&I Framework Initiative

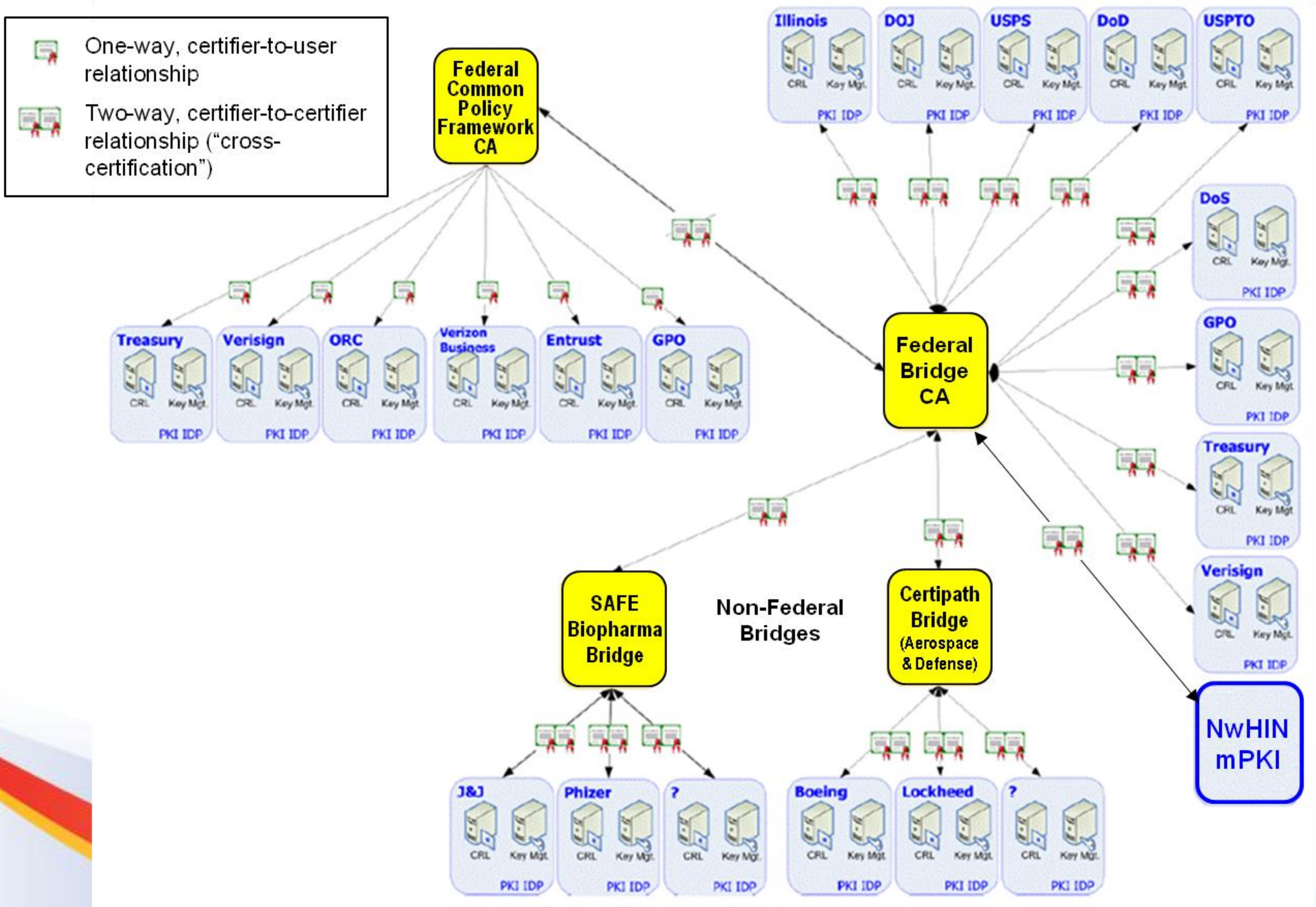
Final Report

August 17, 2011

Task for the S&I Framework

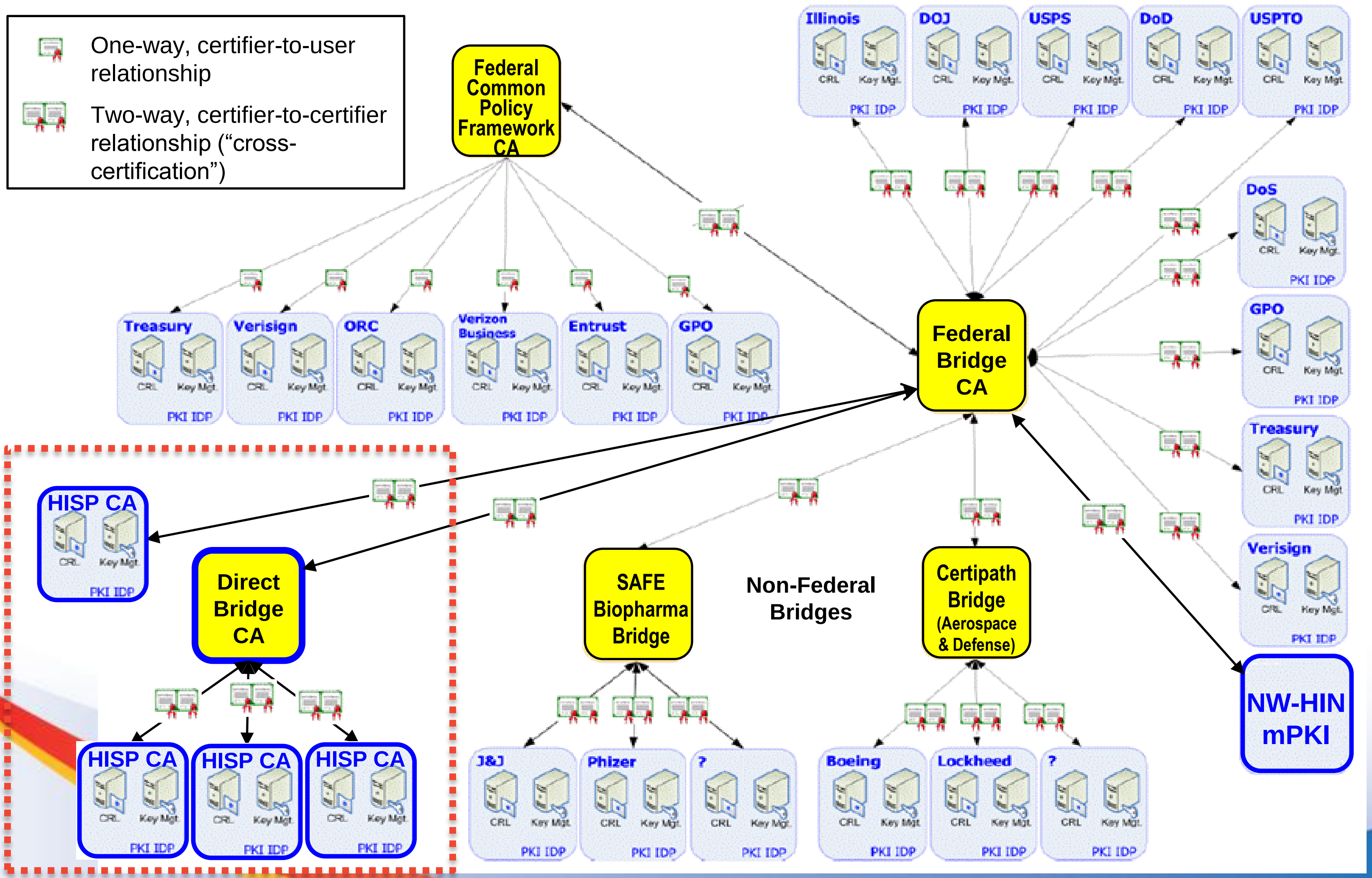
- Recommendation from the HIT Standards Committee to ONC:
  - "To enable Direct users to exchange health information with federal health agencies, the HIT Standards Committee recommends that the ONC investigate architectural and operational alternatives for cross-certifying Health ISPs (HISPs) with the Federal Bridge Certificate Authority, including an examination of potential benefits and implications on cost, market dynamics, and complexity"

Federal PKI Architecture*



*Adapted from *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, Nov 10, 2009

Notional Architecture with Direct Cross-Certification (as presented to HITSC)

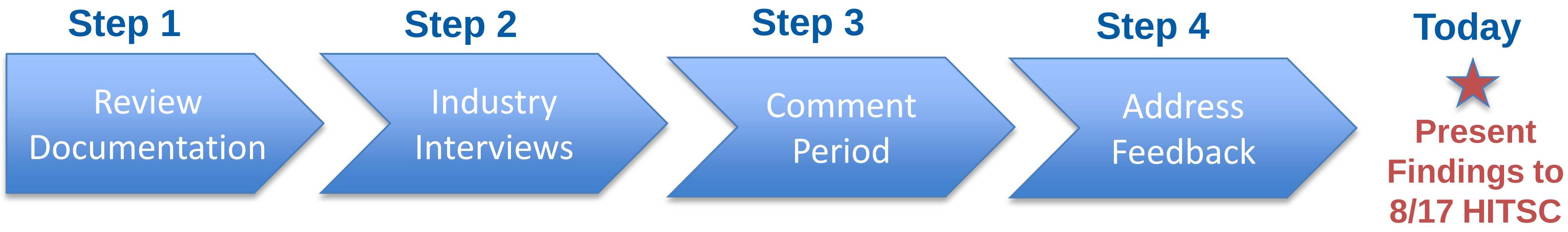


*Adapted from *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, Nov 10, 2009

Scope

- In Scope
  - Organization level certificates
    - Exchange a secret key that is used for encryption
    - Digital signature for the organization
- Out of Scope
  - Individual level certificates for digital signatures

Certificate Interoperability Analysis Process



Step 1

Review Documentation

Step 2

Industry Interviews

Step 3

Comment Period

Step 4

Address Feedback

Today

★

Present Findings to 8/17 HITSC

Certification requirements for…

- Federal Bridge (cross-certification)
- WebTrust
- ETSI

(Bridges, Certificate Authorities, HIEs, Vendors, Agencies)

- SAFE BioPharma
- REBCA
- NIST
- Verizon Business
- Entrust
- GE Healthcare IT
- HealthBridge
- Lockheed Martin
- Thawte
- Nationwide Health Information Network

- Draft Report posted to S&I Wiki for public comments
- Thirteen public comments from several individuals & organizations
- S&I Framework Teams' review of analysis & summary of public comments

- Update to summarize public comments
- Additional research on difference between FBCAs and commercial CAs requirements,
- Additional research on alternatives for cross-certifying HISPs with FBCA with analysis of benefits, cost, market dynamics, and complexity for each option

FBCA Organizational Certificates

- Current FBCA policy does not issue organization-level certificates, as required by Direct – nor does it address the policies and procedures to verify organizational identities
- ONC staff has met with GSA staff to discuss this gap in policy
- GSA indicates that development of policy for organization identity verification will take 6 – 9 months
- ONC staff will coordinate with GSA on the development of these policies
- The Direct Project Rules of the Road Work Group is developing guidance to Direct Project to ensure that any certificates used in the interim will align with anticipated FBCA policy and comply with commercial best practice

Options for ONC's role

In light of the gap in the availability of organizational certificates, we investigated what support ONC could provide

- **Current state:** Direct participants identify and assess cross-certified CA's to make a purchasing decision
- **ONC provides governance and facilitate market competition to meet needs:** ONC issues guidance that goes beyond the FBCA requirements for certificates and identifies vendors that comply with certificate guidance and are cross-certified with FBCA
- **ONC charters a Bridge:** ONC directly (or contractually) establishes a Bridge that is chartered by the Federal Bridge
- **ONC negotiates an agreement with CAs to obtain discounted certificates:** ONC issues an RFP to select one or more vendors that are cross-certified and meet any additional requirements

Option Comparison Summary

Option for ONC	Pros	Cons
Current State	• Rapid to deploy • Low complexity and low overhead for ONC	• No healthcare root • Higher burden on purchaser to research and acquire CA options • Uncertain impact on certificate costs
Provide Governance and facilitate Market Competition	• Possible limited number of healthcare roots • Purchaser can rely on ONC vetting of vendors • Can require compliance with healthcare policies that go beyond FBCA	• Time and resources to vet CA's
Charter a Bridge	• Healthcare root can be established • Can require compliance with healthcare policies that go beyond FBCA • Purchaser can rely on ONC vetting of vendors	• Time and resources to set up and maintain a bridge • Uncertain impact on certificate costs
Negotiate Discounts with CA's	• Possible limited number of healthcare roots • Can require compliance with healthcare policies that go beyond FBCA • Purchaser can rely on ONC vetting of vendors • Reduced certificate costs for purchasers	• ONC responsibility for procurements and contract management • Likely to reduce the number of vendor choices

Implication of Findings

The findings of this initiative suggest that ONC can pursue the following actions:

- Work with GSA to ensure that policies regarding authentication of organizational identity and issuing organizational certificates are developed on an expedited timetable
- Ensure that in the interim Nationwide Health Information Network (including Direct Project) participants acquire and use certificates that align to the maximum extent possible with the Federal PKI policies
- Once Federal policies for authentication of organizational identity are in place, ONC should ensure that Nationwide Health Information Network (including Direct Project) participants have a process for an orderly migration to certificates that are issued by Certificate Authorities cross-certified with the Federal Bridge
- Pursue a longer term strategy to establish a Health bridge that is cross-certified with the Federal bridge

APPENDICES

APPENDIX A

HITPC PRIVACY & SECURITY TIGER TEAM RECOMMENDATIONS

HITPC Privacy and Security Tiger Team Recommendations

1. Certificates required for exchange under the NwHIN brand should be issued consistent with the following principles:
   - A high level of assurance with respect to organization/entity identity needs to be obtained.
   - The certificate should be acceptable to federal agencies, given the frequent need for providers to exchange health information with the federal health architecture.
   - Multiple competitive sources for digital certificates should be available, in order to ensure that small or less resourced provider entities are able to obtain and use digital certificates.
2. All certificates used in NwHIN exchanges must meet Federal Bridge standards and must be issued by a Certificate Authority (or one of its authorized resellers) that is a member of the Federal PKI framework.

HITPC Privacy and Security Tiger Team Recommendation

Recommendation adjusted in response

The HIT Policy Committee will revisit (or ask the HIT Standards Committee to revisit) this recommendation if the S&I Framework process to further investigate the costs and implementation burdens of requiring cross-certification to the Federal Bridge reveals new facts that call into question the conclusion that it is financially and operationally feasible for small or less resourced provider entities to obtain certificates pursuant to this recommendation.

APPENDIX B
OPTIONS FOR ONC'S ROLE

Current State

- **Description** – Direct participants identify cross-certified CA's, assess their services and pricing, and make a purchasing decision
- **Potential Benefits**
  - Rapid deployment
  - Low overhead for ONC
- **Cost Implications**
  - May have higher costs for certificate purchasers than other options
- **Market Dynamics**
  - May increase competition with the influx of new certificate purchasers
- **Complexity**
  - Simple for ONC
  - More complex for purchasers because they will need to research the options for obtaining certificates and deal directly with the CAs

Provide Governance and Allow Market Competition to Meet Needs

- **Description** – ONC issues guidance that goes beyond the FBCA requirements for certificates and identifies vendors that comply with these requirements and are cross-certified with the Federal Bridge.
- **Potential Benefits**
  - Consistent and reliable standards for certificate users
  - Incorporation of additional assurances relevant to healthcare
- **Cost Implications**
  - ONC would bear costs to develop guidance and vet CA. Could become self-sustaining over time.
  - Uncertain impact on purchaser costs
- **Market Dynamics**
  - May increase competition with the influx of new certificate purchasers
- **Complexity**
  - ONC will need to develop guidance
  - For purchasers it would simplify the selection of a CA because they would be vetted by ONC

Charter a Bridge

- **Description** – ONC directly or through a contracted mechanism establishes a Bridge that is chartered by the Federal Bridge
- **Potential Benefits**
  - Could provide a certificate root that can be recognized as a healthcare certificate root
  - Would allow for healthcare specific certificate policies to be mandated through the process of cross-certifying CAs to the bridge (These would be policies that go beyond those established by FBCA)
- **Cost Implications**
  - Would increase costs for ONC to set up and sustain a bridge. Could become self-sustaining over time
  - Uncertain for purchasers: Would depend on the number of CA's that decided to cross-certify to the bridge
- **Market Dynamics**
  - Could narrow the choice of CA's depending on the number of CA's that would choose to be cross-certified to the bridge
- **Complexity**
  - Time, cost, and effort to establish and maintain a bridge increases the complexity of this option for ONC
  - Could simplify for the purchaser by providing a choice of CA's that are vetted for health care data exchange requirements

Negotiate Agreement with One or More Cross-Certified CAs for Discounted Certificates

- **Description** – ONC would issue an RFP to select one or more vendors that are cross-certified and meet any additional healthcare related requirements
- **Potential Benefits**
  - Could be used to establish a defined set of certificate roots that can be trusted by health care organizations
  - May reduce pricing to a bulk purchase level
- **Cost Implications**
  - ONC would incur the cost to develop a procurement and manage the resulting contracts
  - Purchaser costs could be reduced based on a bulk purchase arrangement
- **Market Dynamics**
  - Likely to reduce the number of vendor choices but introduce pricing competition through the bidding process
- **Complexity**
  - ONC would take on the procurement and contracting responsibility
  - Purchasers will be able to rely on ONC vetting when making their purchasing decisions

APPENDIX C

FINDINGS

Findings:
Cost

- Federal agencies will require a cross-certified digital certificate
- The cost for certificates for servers are estimated to be:

Volume Tier / Validity Period	0-100	101-500	501-1000	1001+
1 Yr	$400	$300	$250	$225
2 Yr	$600	$500	$450	$400
3 Yr	$800	$700	$600	$550

- Commercial best practice high assurance server certificates (EV/SSL) start at a high of **$995** with discounts for multi-year and bulk purchases

Findings:
Certificate Process and Contents

- **Process to obtain a server certificate**
  - Submit application to CA
  - Designate a human (employee) who is responsible for the certificate
  - CA or RA will identity proof the responsible human
  - CA will verify the identity of the organization

- **Certificate Information**
  - Signature of CA that issued certificate
  - Algorithm used by the CA to sign the certificate
  - Version
  - Serial number
  - Name of the CA that issued certificate
  - Period of time for which the certificate is valid
  - Name of the subject to whom the certificate is issued
  - The subject’s public key
  - Optional extensions – such as the purposes for which the certificate may be used

Findings:
Operational Alternatives

- **Become a Bridge**

- **Become a Certificate Authority (CA)**
  - FBCA creates significant compliance expectations for CAs
  - Organizations interested in becoming a CA must understand the requirements and effort necessary to be a CA cross-certified to the Federal Bridge

- **Become a Reseller or assist in acquisition of certificates**
  - Resellers can purchase certificates from Certificate Authorities on behalf of provider organizations and issue certificates to the end user/server
  - Resellers will need to cover any associated costs for providing support services including those related to maintenance and renewal of certificates

Findings: *(continued)* Operational Alternatives

- **Become a Registration Authority (RA) – across organizations**
  - RAs assist in completion of information required to obtain a certificate
  - RAs provide Identity proofing and certificate issuance across organizations, e.g., within a geographic area
    - An approved organization for identity proofing, e.g., notary, CPA
    - The certificate itself is issued by CA
- **Act as a Trusted Agent – within a single organization**
  - Identity proofing and certificate issuance within a single organization
  - A CA or RA can allow an organization, such as a hospital or large group practice to have one person (a trusted agent) identity proofed by the CA and delegate to that person the responsibility for identity proofing other employees in the organization and attesting to the CA that each person issued a certificate has had their identity proofed following the CA's policies
- **Provide directory management of access to public keys**
  - A certificate directory can be queried for digital certificates
  - A provider directory could support queries for digital certificates
  - Users approved to access the provider directory could submit queries to the provider directory and the provider directory would return the digital certificate

APPENDIX D

REVIEW OF FEDERAL AND COMMERCIAL REQUIREMENTS

Review of Federal and Commercial Requirements

- Federal certificate policy provides the framework for the Federal program to review and certify certificate authorities to issue certificates that will be accepted by Federal agencies
  - This policy currently covers individual certificates

Review of Federal and Commercial Requirements

Broad Distinctions

- Federal requirements are more heavily focused in the areas of system management and have a higher degree of specificity in these requirements
- Standard industry practices address the verification of the information provided by the entity applying for the certificate
  - This is the gap that would need to be filled by new GSA policies
- A high quality CA would be likely to comply with both sets of requirements, because they align with standard industry practices in each area
- A CA with strong practices on verification and IT management and security should meet the Federal requirements
- For a CA with strong practices the additional effort to meet the certification requirements for both programs would be to **document** compliance with a second set of requirements and **go through a second review process**.

Overlap of Federal and Commercial Requirements

- Terms of use
- In person proofing
- Certificate status checking
- Certificate revocation
- Employee screening and training
- Separation of duties
- Independent audits
- Root CA pair generation controls
- Cryptographic algorithms and key size

Focus of Federal and Commercial Requirements

Extended Validation Focus Areas

- Warranties
- Insurance/liability
- Qualifications to obtain certificates
- Certificate application content
- Applicant verification process and methods
- Verification information sources
- Delegation to RAs
- Document retention
- Risk assessment/ security policy

FPKI Focus Areas

- Certificate creation
- Transmission of keys
- Verification of key binding
- Physical and logical security
  - CA
  - Certificate Status Service
  - RA
- Records archives
- Internal audits
- CA key protection
- CA key compromise

APPENDIX E
SUMMARY OF PUBLIC COMMENTS

Appendix 1: Public Comments

- Comments were constructive and without objections to current considerations and discussions
- Comments focused on following themes:
  - Options for HISPs related to certificate issuance and management and implications on benefits, cost, market competition, and complexity of implementation
  - Roles for ONC to support acquisition and use of cross-certified certificates to enable data exchanges with Federal Agencies
  - Difference in costs and time requirements for Cross-Certified CA vs. WebTrust/ETSI-certified CA
  - Burden to obtain and manage certificates at organizational vs. individual provider level

Summary of Public Comments

- Thirteen comments were received from several individuals and organizations shown below:
  - Paul Egerman
  - John Moehrke
  - B. Cabral
  - Vince Lewis
  - Brett Peterson
  - Durwin Day
  - T. H. Boyd
  - Peter Bachman
  - Covisint
  - McKesson Corporation
  - SAFE BioPharma
  - Health IT Now
- Based on the scope of this assessment, all comments were analyzed and summarized as shown in the following pages

Summary of Public Comments

Topic	Disposition of Comment
Role of HIEs and HISPs	HISPs and HIEs can play varying roles in obtaining and managing digital certificates including becoming resellers, Registration Agents (RAs), or cross-certified Certificate Authorities (CAs) under a Business Agreement. However, the level of authority granted to these intermediaries and the effect on price & management of the certificates and benefits will need to be analyzed. The costs and time requirements associated with each role vary and will also need to assessed.
Cost and Time Requirements (General)	Assumptions are needed for each role option for HIEs and HISPs to determine costs and pricing structures . One difficulty of obtaining precise information especially costs relies on the fact that most vendor costs to become a certificate authority are proprietary.
Costs for Cross-Certified CA vs. WebTrust/ETSI-certified CA	The incremental cost between a cross-certified CA and a WebTrust/ETSI-certified CA does not appear to be significantly higher.
Market Competition	There are varying views on whether there is sufficient competition to ensure providers have access to best pricing and service of certificates and how competition can increase. This observation may need to be addressed further including whether: 1) multiple Federal Bridge cross-certified CAs that exist eliminate the need for providers to establish their own cross-certifying bridges or CAs; 2) lowering FBCA costs and simplifying certification process without reducing quality and security can foster competition.

Summary of Public Comments

Topic	Disposition of Comment
Suggestions to ONC	Varying views exist about the role that ONC can play including: • Assisting providers with the cost of acquiring certificates and internal policy management • Instituting a CA and providing services at a low cost or free • Instituting a tiered model for implementation. • Establishing a national certificate authority to ensure nation-wide scale and interoperability and management of digital certificates. A "Health Bridge" cross-certified with the FBCA may be a strong enabling factor if established through an innovative cross-certification application process and if provisional approval is granted.
Tiger Team Recommendations	The recommendation for use of PKI certificates issued by a cross-certified FBCA promote trust broadly. While the recommendations only address organizational level certificates, the Tiger Team should leverage the credentialing schema of the FICAM Program when addressing individual level certificates.
Burden to Obtain and Manage Certificates – Organizational Level	There is agreement that obtaining a federal bridge cross-certified certificate at the organization level is appropriate and does not pose much burden because costs are reasonable.
Policy and Procedures to support implementation and use of certificates	The issues related to policy and procedures to assure trust and manage PKI should be addressed rather than the technology. Simplifying the implementation of certificates without impacting adoption negatively as well as how certificates will be used need to be addressed further.

Summary of Public Comments

Topic	Disposition of Comment
Individual Level Certificate Use	Though out of scope, there are multiple issues yet to be addressed for individual level use of certificates including providing multiple token forms for use, providing multiple methods of identity proofing, and using a master certificate by multiple providers. Resources such as the US Federal Identity, Credentialing and Access Management FICAM Program can be leveraged to address these issues.
Burden to Obtain and Manage Certificates – Individual Level	Though out of scope, the burden to individual providers to obtain and manage certificates would be significant for multiple reasons. Some reasons include that providers will need to learn how to obtain the certificates, undergo ID-proofing, implement enrollment policies, manage CRLs and renewals, etc. As a result, individuals are encouraged to partner with a technology partner or outsource the acquisition and management of digital certificates.
Reducing Burden on Providers to Obtain and Manage Digital Certificates	Approaches that balance need for a high level of assurance with costs and implementation burden are preferred. Some options include issuing certificates at organizational level with strong end user authentication requirements, providing access to a trusted partner or online-ID proofing. Some issues are yet to be resolved including: ensuring trusted partners that manage certificates have sufficient authentication controls to avoid misuse, providing regulations that guide automation of certification process, avoiding lower standards and raising usefulness of certificates, and coordinating needs for identity across multiple health projects e.g. Direct, Exchange, etc.

APPENDIX F

GLOSSARY OF TERMS

(ADAPTED FROM THE MARCH 9TH HITSC PRIVACY & SECURITY WORKGROUP PRESENTATION)

Glossary of Terms

(Ref: NIST SP 800-32 - Introduction to Public Key Technology and the Federal PKI Infrastructure)

Term	Definition/Source
Authentication	Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009]
Digital Certificate	A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG].
Certificate Authority	An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs.
Certificate Authority Revocation List (CARL)	A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates that have been revoked.
Certificate Policy	A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications

Glossary of Terms

(Ref: NIST SP 800-32 - Introduction to Public Key Technology and the Federal PKI Infrastructure)

Term	Definition/Source
Certification Practice Statement (CPS)	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).
Certificate Revocation List (CRL)	A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date.
Certificate Status Authority	A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate.
Digital Signature	The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer's digital certificate; and (2) whether the message has been altered since the transformation was made.
Duration	A field within a certificate that is composed of two subfields; “date of issue” and “date of next issue”.
Encryption Certificate	A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes.

Glossary of Terms

(Ref: NIST SP 800-32 - Introduction to Public Key Technology and the Federal PKI Infrastructure)

Term	Definition/Source
Key Escrow	A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"]
Key Exchange	The process of exchanging public keys in order to establish secure communications.
Non-Repudiation	Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009
Object Identifier (OID)	A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the four policies and cryptographic algorithms supported.
Private Key	(1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret.
Public Key	(1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate.
Public Key Infrastructure	A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Glossary of Terms

(Ref: NIST SP 800-32 - Introduction to Public Key Technology and the Federal PKI Infrastructure)

Term	Definition/Source
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA).
Signature Certificate	A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions.
Subscriber	A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device
Trust Anchor	A CA that serves as the “root” for certificate path validation; a trust anchor can be the top CA in a hierarchical PKI, the CA that issued the verifier's own certificate(s), or any other CA in a network PKI.
Trusted Certificate	A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor".

APPENDIX G

HITSC PRIVACY & SECURITY WORKGROUP RECOMMENDATIONS

RECOMMENDATION #1: REQUIREMENTS AND EVALUATION CRITERIA FOR DIGITAL CERTIFICATE STANDARD

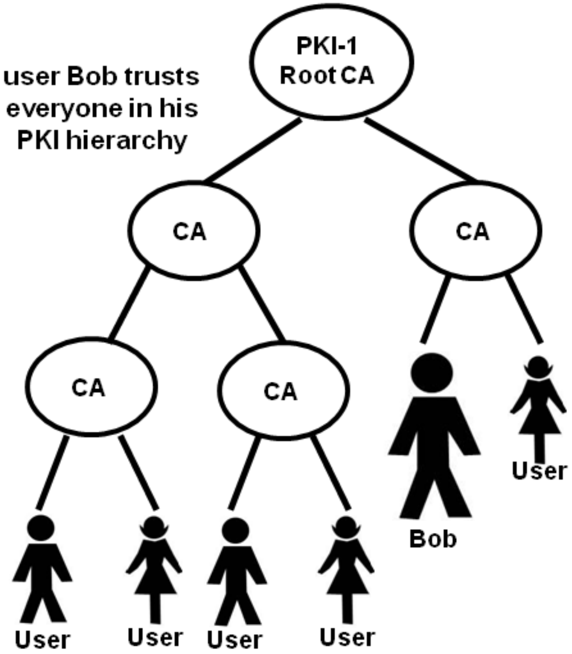
Digital Certificate Basics

- A “digital certificate” is an electronic document that certifies that the subject (person or entity) has been issued a pair of encryption keys that are related in such a way that if one key is used to encrypt something (e.g., file, message, data stream), it can be decrypted only by someone holding the other key
  - One key is published for anyone to see (“public key”)
  - The other key is kept secret by the entity/person to whom the digital certificate has been issued (“private key”)
  - Digital certificates are issued by a “certificate authority” (CA) – and digitally signed by the issuing CA
    - CA certificates may be self-issued and self-signed certificates
- CAs periodically publish a “certificate revocation list (CRL)” that identifies those certificates that no longer are valid and that have not expired

Digital Certificate Basics

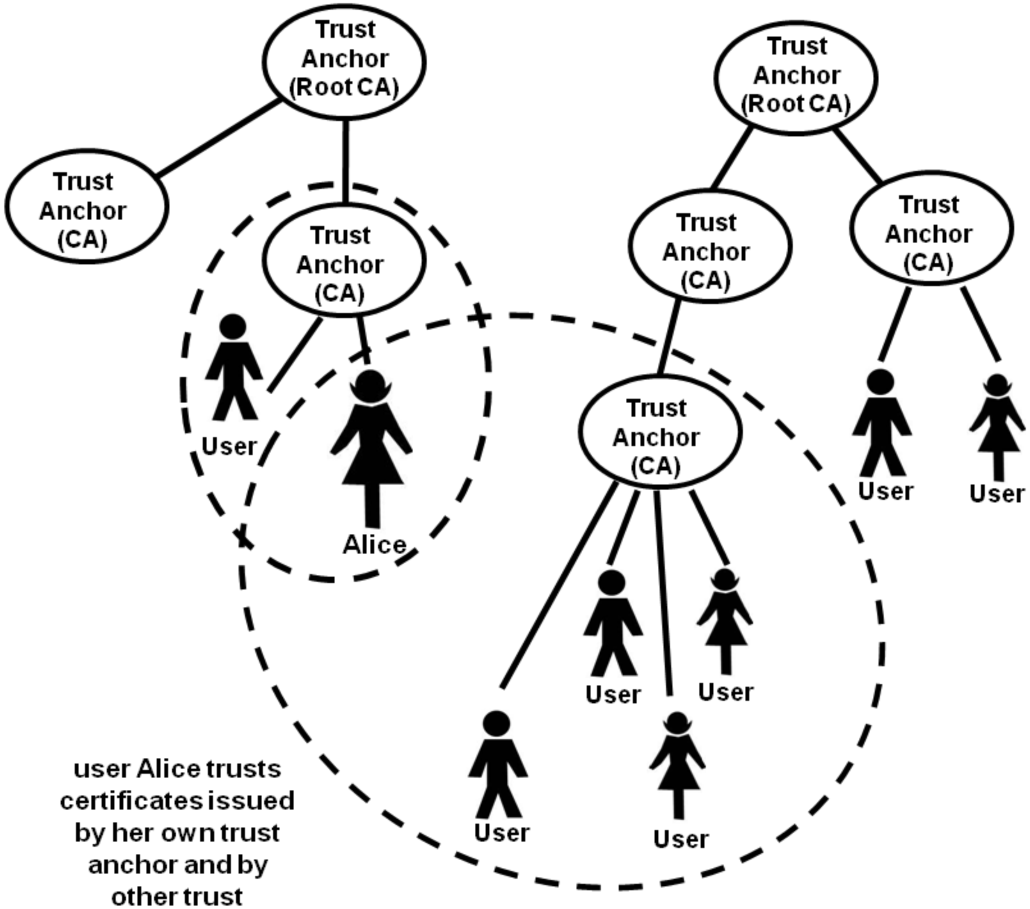
- Digital certificates are used for a number of purposes, including:
  - To authenticate the identity of an entity or person using a challenge-response mechanism
  - To digitally sign a message or other transmitted content ("digital signature")
  - To share a secret key to be used to exchange private or sensitive information
- The trustworthiness of a digital certificate is dependent upon how much the user trusts the issuer of the certificate – which may be the top CA in a hierarchical PKI, the CA that issued the user's own certificate, or any other trusted CA
  - The practices used by a CA in issuing and managing certificates are described in its Certification Practice Statement (CPS)
  - CPSs may be certified by organizations such as the European Telecommunications Standards Institute (ETSI) and WebTrust, or as meeting minimal standards established by specific communities, such as SAFE Bio-Pharma and Federal Bridge

Digital Certificate Trust Models



user Bob trusts everyone in his PKI hierarchy

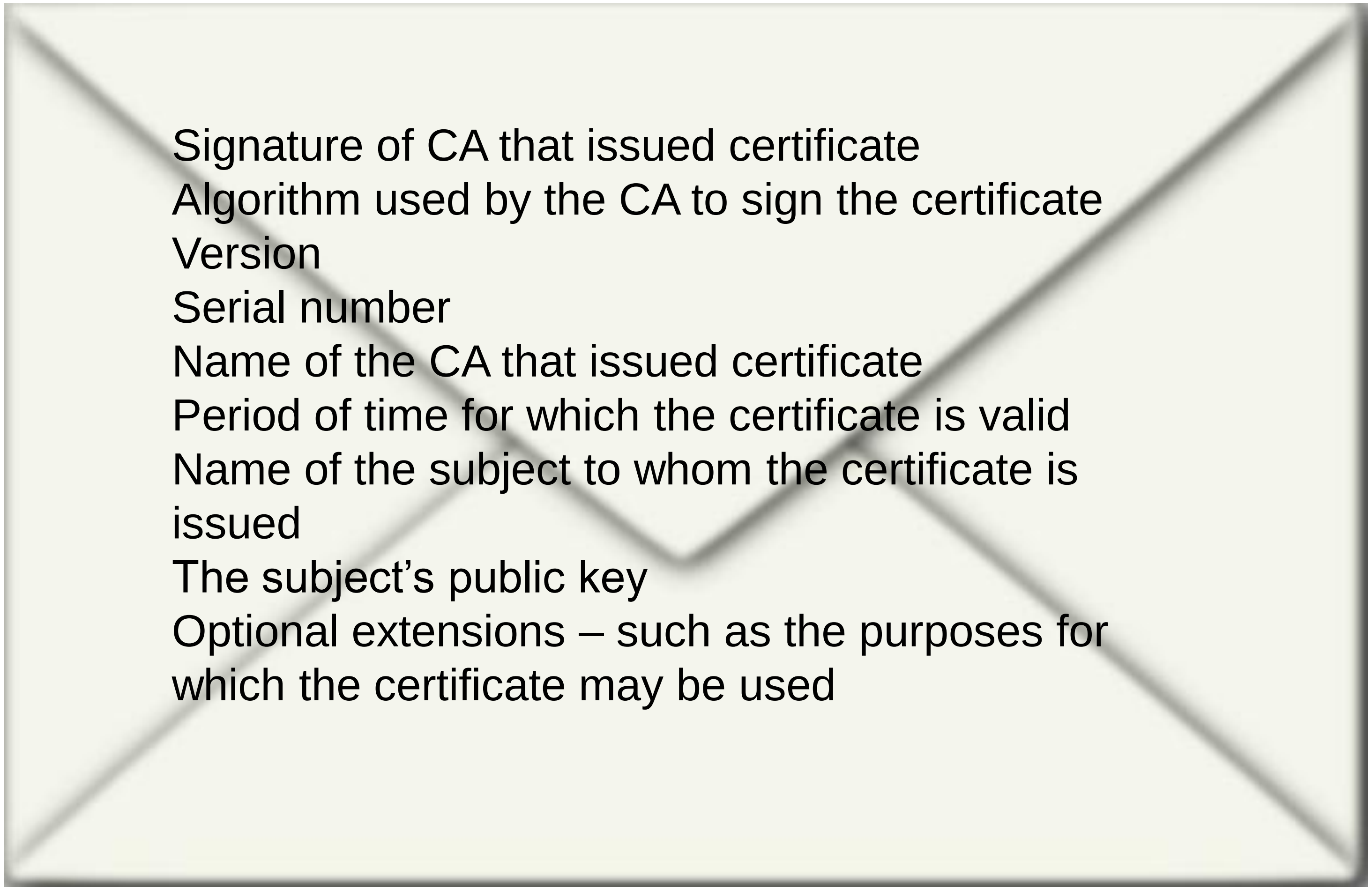
Hierarchical PKI



user Alice trusts certificates issued by her own trust anchor and by other trust anchors she deems trustworthy

“Multi-Root” Model
(e.g., the Direct Project)

Digital Certificate Content



Signature of CA that issued certificate
Algorithm used by the CA to sign the certificate
Version
Serial number
Name of the CA that issued certificate
Period of time for which the certificate is valid
Name of the subject to whom the certificate is issued
The subject’s public key
Optional extensions – such as the purposes for which the certificate may be used

Recommended Requirements

- Digital certificates must conform to the X.509 V3 certificate profile defined in RFC 5280 (May 2008)
- Digital certificates to support Direct exchanges:
  - MUST include the set of Basic Certificate Fields defined in Section 4.1 of RFC 5280
  - MUST include the Standard Extensions needed to support the simple mail transfer protocol (SMTP) with Secure/Multipurpose Internet Mail Extensions (S/MIME)
  - MAY include additional Standard Extensions as defined in Section 4.2 of RFC 5280
- Digital certificates to support NW-HIN exchanges:
  - MUST include the set of Basic Certificate Fields defined in Section 4.1 of RFC 5280
  - MUST include the Standard Extensions needed to support mutually authenticated transport layer security (TLS) connections
  - MAY include additional Standard Extensions as defined in Section 4.2 of RFC 5280
- Certificate revocation lists (CRLs) MUST conform to the X.509 V2 CRL profile defined in Section 5 of RFC 5280 (which supports both Online Certificate Status Protocol (OCSP) and full CRL retrieval)
- Nothing in these requirements precludes the specification of a single standard for a certificate usable for both Direct and NW-HIN exchanges

Recommended Evaluation Criteria

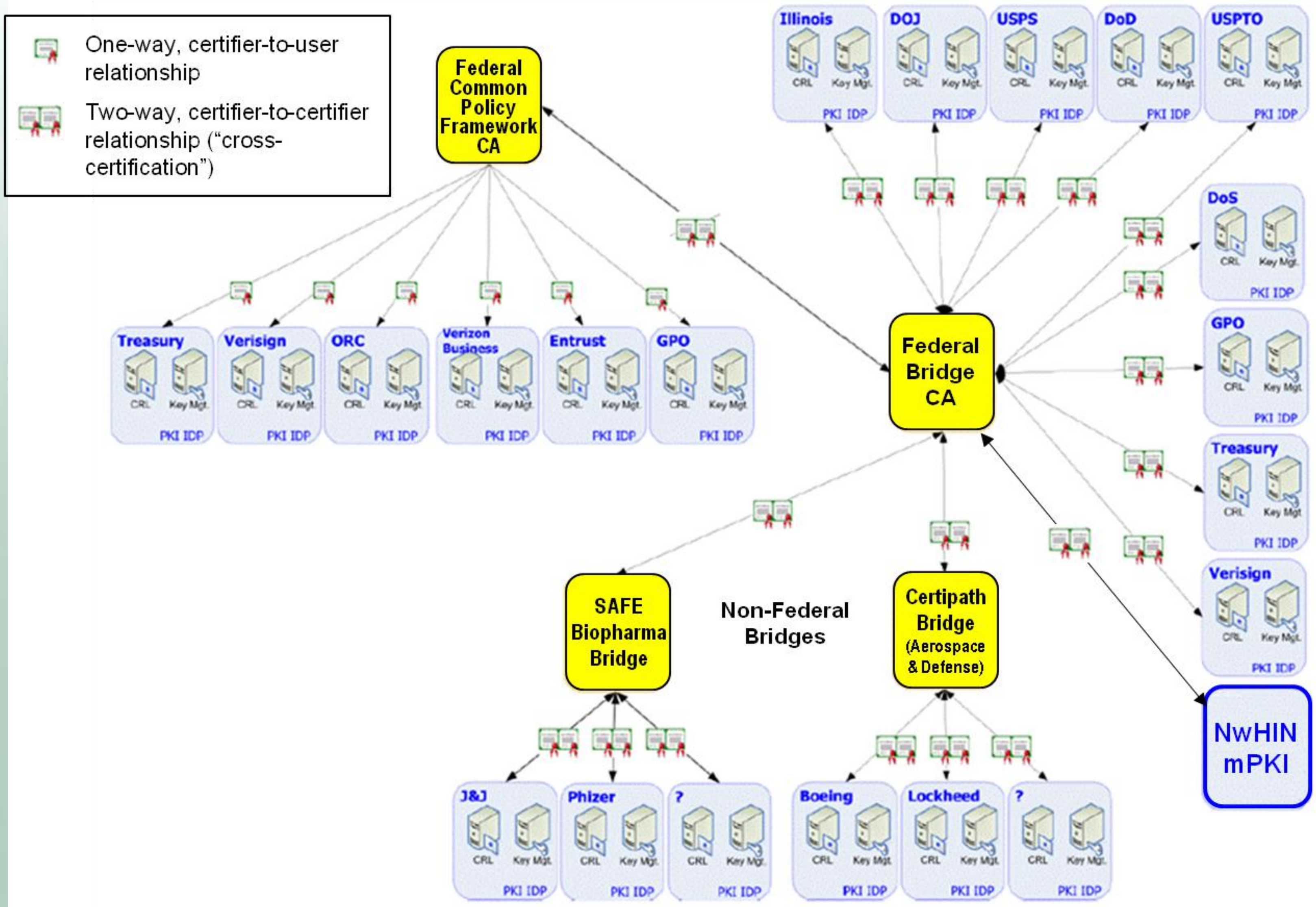
- Does the standard conform to the X.509 V3 profile defined in RFC 5280?
- Does the standard specify the Basic Certificate Fields and Extensions as REQUIRED for Direct exchanges?
- Does the standard specify the Basic Certificate Fields and Extensions as REQUIRED for NW-HIN exchanges?
- If the standard includes one or more additional Extensions, are these as specified in the Standard Certificate Extensions defined in RFC 5280?
- If the standard includes Extensions applicable only to Direct or NW-HIN exchanges, are the intended usage of these Extensions clear and unambiguous?
- Does the standard include X.509 V2 certificate revocation lists (CRLs) as defined in RFC 5280?
- Is the standard specified clearly and completely enough for a developer to implement?

RECOMMENDATION #2:
NEED FOR INVESTIGATION OF ALTERNATIVES FOR CROSS-CERTIFYING DIGITAL CERTIFICATE ISSUERS WITH FEDERAL BRIDGE CA

Bridging with Federal Certificate Authority

- All digital certificates used by federal agencies must link back to the Federal Common Policy Framework Certificate Authority (CA) and must include the assurance level under which the certificate was issued
  - Four levels (rudimentary, basic, medium, high) correspond to NIST levels 1-4
  - Includes several "flavors" of medium assurance for software, hardware and Personal Identity Verification (PIV)-card-based certificates
- Certificates used to support exchanges between federal agencies and state agencies must be issued by a CA that is cross-certified with the Federal Bridge CA
- To enable health exchanges between the NW-HIN Exchange and federal health agencies, the NW-HIN managed Public Key Infrastructure (mPKI) is cross-certified with the Federal Bridge CA

Federal PKI Architecture*

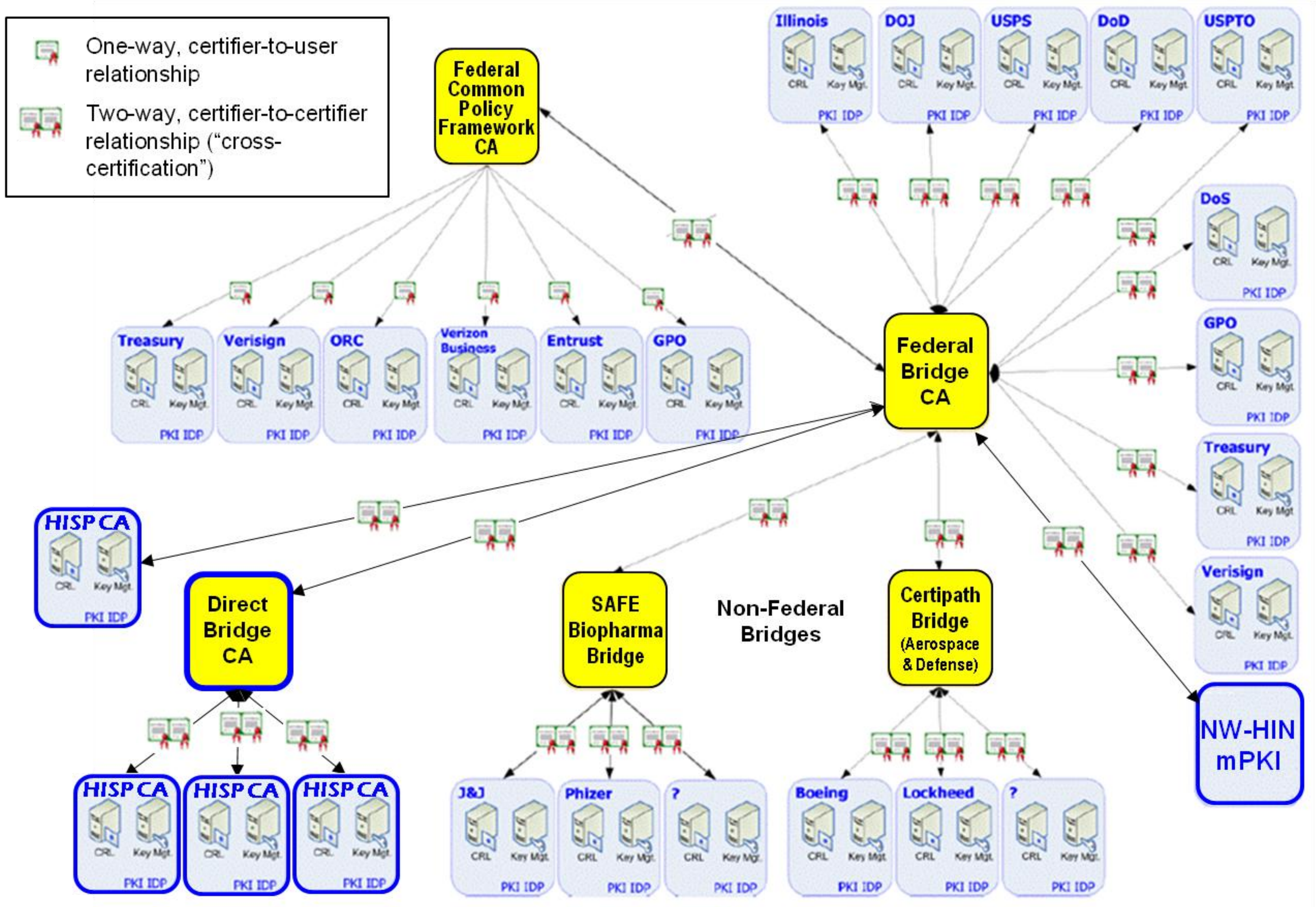


*Adapted from *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, Nov 10, 2009

Direct Exchanges with Federal Entities

- The Direct Project allows a “multi-root” model in which certificates are generated by CAs without a common root – such as Healthcare Interoperability Service Providers (HISPs)
- Both NW-HIN and Direct users will need to exchange health information with federal health agencies – most prominently the VA and CMS
- **How feasible would it be to require that certificates used in Direct exchanges be obtained from CAs linked to a bridge or CA cross-certified with the Federal Bridge CA?**

Notional Architecture with Direct Cross-Certification



*Adapted from *Federal Identity, Credential, and Access Management (FICAM) Roadmap and Implementation Guidance*, Nov 10, 2009

Recommendation to ONC

- To enable Direct users to exchange health information with federal health agencies, the HITSC Privacy and Security Workgroup recommends that the ONC investigate architectural and operational alternatives for cross-certifying Direct CAs with the Federal Bridge CA, including implications on cost, market dynamics, and complexity