Federal Health Architecture

Federal Common Trust Bundle Requirements

Federal Health Architecture
Directed Health Exchange
Security Sub-Work Group

Version 1.0

July 2015

ATTN: Eric Larson
Directed Exchange Work Group
Federal Health Architecture
Federal.health@hhs.gov

Document Change Control

Version	Release Date	Summary of Changes	Addendum Number	Name
11.12.14	TBD	New Report	N/A	Mike Davis
1.14.15	TBD	Added in person or antecedent, section 1.2.C	N/A	Eric Larson
7.15.15	TBD	Adjusted document Title to more accurately reflect Document intent	N/A	Eric Larson

1. Identity Axis Elements

The FHA Directed Exchange Security Sub-Work Group conducted an extensive survey of the federal exchange requirements outlined by The National Institute of Standards and Technology (NIST), Federal Information Security Management Act (FISMA) and Federal Identity, Credential and Access Management (FICAM) that all potentially impact federal agency participation in Direct Messaging. The tables below summarize those policies as they apply to federal agencies and their health information

1.1. IDENTITY OF ENTITY ASSERTING TRUST FRAMEWORK ATTRIBUTES

Policy	Example	Reference
A. Identity (name asserting Trust Framework attributes)	DirectTrust.org	
B. Class of Identity covered under Trust Framework (individual or real person), pseudo identity, endpoint address, organization, service, <others>?		
C. Type of identity (hospital, internationalized domain name (IDN), provider organization, provider, Health Information Exchange (HIE), Connector, etc.)	Health Information Service Provide (HISP)	
a. Issuing Certificate Authority – if there is a chain, perhaps the full chain back **to the** root organization needs to be specified	…Enter chain	
b. Certificate Policy		
c. Federal Bridge Certificate Authority_External Certificate Authority (FBCA_ECA)=FBCA Medium Hardware or ECA Medium, Medium Token, Medium Hardware **OR** FBCA_Med=FBCA Medium Assurance for identity proofing and credential management **OR** FBCA approved DirectTrust equivalent.	FBCA Med	http://www.idmanagement.gov/sites/default/files/documents/FBCA%20Certificate%20Policy%20v2.27.pdf

Policy	Example	Reference
d. DOC (Dual_Object Identifier (OID)_Certs)= Both FBCA Cross-certified Security Trust Agent (STA)/HISP Certificates+ DirectTrust OIDs	Yes	
e. DualCert=Two certificates one of signing and a second for encryption. Single-use certificates (a single certificated used for both encryption and signing) is not allowed	Yes	X509 Certificate Policy for the Federal Bridge Certification Authority (FBCA) section 6.1.7 FPKIA May 14, 2013 Meeting Minutes CPWG Report section c. http://www.idmanagement.gov/sites/default/files/documents/FPKIPA%2014%20May%202013%20Meeting%20Minutes.pdf Considering the existing Direct RIs are already in production, use by numerous implementations and mandated by MU2 requirements and there was a clear planned path forward to eliminate dual use by the end of 2015, the CPWG determined that the current implementation could be considered a legacy application Given that Direct explicitly requires the non-repudiation bit to be turned off, it was determined that Direct was not in violation of their policy NIST will "tolerate" Dual-Use certificates for legacy systems as long as there is a path forward; FBCA permits Dual-Use certificates. ONC is requesting that DIRECT be considered a "legacy system" until the end of 2015. ONC has indicated they already have a plan in place to eliminate the requirement for Dual-Use certificates for federal participants that will end by then.
D. Accreditation (need to know what these values may be)	DirectTrust Member in good standing	Accredited Organizations: https://www.ehnac.org/accredited-organizations/
E. Accrediting Entity	Electronic Healthcare Network Accreditation Commission (EHNAC)	https://www.ehnac.org/

Policy	Example	Reference
F. Accreditation Date	26 Sep 2013	https://www.ehnac.org/accredited-organizations/
G. Policy requires a Business Associate Agreement (BAA) or equivalent language between the HISP supported entities	Yes	FHA Directed Exchange Security WG FAQ item 3.4 FHA Directed Exchange Guideline 5 DirectTrust HISP Policy, Version 1.0 Section 5.3.7.1 If Sender is CD on acting on behalf of a CE (e.g is a BA and has a BAA with a CE), then a BAA with HISP must be established, and if not established, under the Omnibus rule, the HISP will be considered a BA anyway. Under the HIPAA Privacy Rule, promulgated by the United States (U.S.) Department of Health and Human Services, a covered entity must enter into a business associate agreement(BAA) with any individual who needs access to protected health information (PHI) in order to perform some activity for the covered entity before releasing PHI to that individual or entity. A BAA is required even if no contract vehicle exists between the covered entity and the business associate. If Sender is CE or acting on behalf of a CE (e.g. is a BA and has a BAA with a CE), then a BAA with HISP must be established, and if not established, under the Omnibus rule, the HISP will be considered a BA anyway.

1.2. USER ATTRIBUTES

Policy	Example	Reference
A. Category of User covered under Trust Framework (Patient, Provider, Local, Remote, Contractor, Employee, Affiliate, pseudo identity, endpoint address, organization, service, <others>?)	Provider	The term 'health care provider' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations. Section 160.103— Provider of services (as defined in section 1861(u) of the [Social Security] Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.3 3 Social Security Act, Section 1861 definitions for (u) and (s) are available online at http://www.ssa.gov/OP_Home/ssact/title18/1861.htm.
B. Identity Policy	NIST SP 800-63 v2	NIST SP 800-63 v2
C. User Identity Proofing level	NIST Level of Assurance (LOA)3 with in person or antecedent verification or higher	NIST SP 800-63 v2
D. Contact person information (this is info on a live person who "represents" this identity if the identity is not a real person):		
a. Name		
b. Address		
c. Contact Number		

1.3. GENERAL OPERATIONAL ELEMENTS

Policy	Example	Reference
A. HcDom=Healthcare Domain exclusive use STA/HISP for all exchanges EXCEPT patient directed **OR** PatDom=Patient Domain exclusive use STA/HISP (for all "Patient Directed" exchanges)	HcDom	The term 'health care provider' has the meaning given such term in section 160.103 of title 45, Code of Federal Regulations. Section 160.103— Provider of services (as defined in section 1861(u) of the [Social Security] Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.3 3 Social Security Act, Section 1861 definitions for (u) and (s) are available online at http://www.ssa.gov/OP_Home/ssact/title18/1861.htm.
B. DomCert=Domain-bound Certificate AND Header encryption (Y/N) **OR** AddCert=Address-bound Certificate	DomCert	NIST SP 800-63 v2
C. FISMA_Equiv (FISMA Equivalent)=HIPAA + TF	Yes	
D. Federal Information Processing Standards (FIPS) 140-2=FIPS 140-2 for encryption	Yes	
E. FIPS 186-2: FIPS 186-2 for digital signatures	Yes	

2. References

American Bar Association Trust Framework

North American Security Products Organization

Office of the National Coordinator: Health Information Technology Policy Committee (ONCHITPC)

Health Information Exchange (HIE) Governance Forum

National Association for Trusted Exchange (NATE)

DirectTrust

Blue Button Plus (BB+)

National Institute of Standards and Technology (NIST)

Office of Management and Budget (OMB)

Federal Identity, Credential, and Access Management (FICAM)