



DataMotion Direct Certification Practices Statement (Abbreviated Version)

CONFIDENTIAL
Access Limited to Authorized Personnel

June 18, 2019
Part # 060013-04-A

Copyright © 2019, DataMotion, Inc. ("DataMotion"). ALL RIGHTS RESERVED.

Your right to print, copy, reproduce, publish or distribute this document or parts of this document is limited by copyright law.

DataMotion® is a registered trademark of DataMotion, Inc. All other brand and product names are trademarks or registered trademarks of their respective companies.

The information contained in this document is subject to change without notice. THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. IN NO EVENT SHALL DATAMOTION BE LIABLE FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND ARISING FROM ANY ERROR IN THIS DOCUMENT, INCLUDING WITHOUT LIMITATION ANY LOSS OR INTERRUPTION OF BUSINESS, PROFITS, USE, OR DATA.

DataMotion Direct Certification Practices Statemen (Abbreviated Version) v4-A

Publication Date: June 18, 2019

Printed in the United States of America.

DataMotion, Inc. Confidential and Proprietary Information.

Published By:

DataMotion, Inc.
200 Park Ave.
Florham Park, NJ 07932
USA

1 800-672-7233 or +1 973-455-1245

<http://www.datamotion.com/>

Table of Contents

1	Introduction	13
1.1	Overview	14
1.1.1	Certificate Policy (CP)	15
1.1.2	Relationship between the DirectTrust CP and this CPS	15
1.1.3	Relationship between the DirectTrust CP and the DataMotion Direct CP	15
1.1.4	Relationship between DirectTrust CP and DirectTrust-EHNAC Accredited Entities	16
1.2	Document Name and Identification	16
1.3	PKI Participants	17
1.3.1	DataMotion Direct Management	17
1.3.2	Certification Authorities (CAs)	17
1.3.3	Registration Authorities (RAs)	18
1.3.3.1	Trusted Agents (TAs)	18
1.3.4	Subscribers	18
1.3.4.1	Health Information Service Providers (HISPs)	18
1.3.4.2	Sponsors and Sponsoring Organizations	18
1.3.5	Relying Parties	19
1.3.6	Other Participants	19
1.3.6.1	Affiliates	19
1.4	Certificate Usage	19
1.4.1	Appropriate Certificate Uses	19
1.4.2	Prohibited Certificate Uses	19
1.5	Policy Administration	20
1.5.1	Organization Administering the Document	20
1.5.2	Contact Person	20
1.5.3	Person Determining Certification Practices Statement Suitability	20
1.6	Definitions and Acronyms	20
1.6.1	Acronyms	20
1.6.2	Definitions	22
2	Publication and Repository Responsibilities	26
2.1	Repositories	26
2.1.1	Repository Obligations	26

2.2	Publication of Certification Information.....	26
2.2.1	Publication of Certificates and Certificate Status	26
2.2.2	Publication of CA Information.....	27
2.2.3	Interoperability	27
2.3	Frequency of Publication	27
2.4	Access Controls on Repositories	27
3	Identification and Authentication.....	28
3.1	Naming.....	28
3.1.1	Types of Names.....	28
3.1.2	Need for Names to be Meaningful.....	29
3.1.3	Anonymity or Pseudonymity of Subscribers	29
3.1.4	Rules for Interpreting Various Name Forms	29
3.1.5	Uniqueness of Names.....	29
3.1.6	Recognition, Authentication, and Role of Trademarks.....	29
3.2	Initial Identity Validation	30
3.2.1	Method to Prove Possession of Private Key.....	30
3.2.2	Authentication of Organization Identity	30
3.2.3	Authentication of Individual Identity	31
3.2.3.1	Authentication of Human Subscribers	31
3.2.3.2	Authentication of Human Subscribers for Role-based Certificates.....	34
3.2.3.3	Authentication of Human Subscribers for Group Certificates.....	34
3.2.3.4	Authentication of Devices.....	35
3.2.3.5	Verification of NPI Number.....	36
3.2.4	Non-verified Subscriber Information	36
3.2.5	Validation of Authority	36
3.2.6	Criteria for Interoperation	37
3.3	Identification and Authentication for Re-key Requests.....	37
3.3.1	Identification and Authentication for Routine Re-key	37
3.3.2	Identification and Authentication for Re-key after Revocation.....	37
3.4	Identification and Authentication for Revocation Request	37
4	Certificate Life-Cycle	38
4.1	Certificate Application	38
4.1.1	Submission of Certificate Application	38

4.1.2	Enrollment Process and Responsibilities.....	38
4.2	Certificate Application Processing	38
4.2.1	Performing Identification and Authentication Functions	38
4.2.2	Approval or Rejection of Certificate Applications	38
4.2.3	Time to Process Certification Applications	39
4.3	Certificate Issuance	39
4.3.1	CA Actions During Certificate Issuance.....	39
4.3.2	Notification to Subscriber of Certificate Issuance	39
4.4	Certificate Acceptance.....	39
4.4.1	Conduct Constituting Certificate Acceptance	39
4.4.2	Publication of the Certificate by the CA	39
4.4.3	Notification of Certificate Issuance by the CA to Other Entities	39
4.5	Key Pair and Certificate Usage.....	40
4.5.1	Subscriber Private Key and Certificate Usage.....	40
4.5.2	Relying Party Public Key and Certificate Usage	40
4.6	Certificate Renewal	40
4.6.1	Circumstance for Certificate Renewal	40
4.6.2	Who May Request Renewal.....	41
4.6.3	Processing Certificate Renewal Requests.....	41
4.6.4	Notification of New Certificate Issuance to Subscriber	41
4.6.5	Conduct Constituting Acceptance of a Renewal Certificate	41
4.6.6	Publication of the Renewal Certificate by the CA	41
4.6.7	Notification of Certificate Issuance by the CA to Other Entities	41
4.7	Certificate Re-Key	41
4.7.1	Circumstance for Certificate Re-Key	41
4.7.2	Who May Request Certification of a New Public Key	42
4.7.3	Processing Certificate Re-Keying Requests.....	42
4.7.4	Notification of New Certificate Issuance to Subscriber	42
4.7.5	Conduct Constituting Acceptance of a Re-Keyed Certificate	42
4.7.6	Publication of the Re-keyed Certificate by the CA	42
4.7.7	Notification of Certificate Issuance by the CA to Other Entities	42
4.8	Certificate Modification	42
4.8.1	Circumstance for Certificate Modification	42

4.8.2	Who May Request Certificate Modification.....	42
4.8.3	Processing Certificate Modification Requests	43
4.8.4	Notification of New Certificate Issuance to Subscriber	43
4.8.5	Conduct Constituting Acceptance of Modified Certificate	43
4.8.6	Publication of the Modified Certificate by the CA.....	43
4.8.7	Notification of Certificate Issuance by the CA to Other Entities	43
4.9	Certificate Revocation and Suspension	43
4.9.1	Circumstances for Revocation	43
4.9.2	Who Can Request Revocation	44
4.9.3	Procedure for Revocation Request	44
4.9.4	Revocation Request Grace Period.....	44
4.9.5	Time Within Which CA Must Process the Revocation Request	44
4.9.6	Revocation Checking Requirements for Relying Parties	44
4.9.7	CRL Issuance Frequency.....	44
4.9.8	Maximum Latency of CRLs	44
4.9.9	On-Line Revocation/Status Checking Availability	44
4.9.10	On-Line Revocation Checking Requirements.....	45
4.9.11	Other Forms of Revocation Advertisements Available.....	45
4.9.12	Special Requirements Related to Key Compromise.....	45
4.9.13	Circumstances for Suspension.....	45
4.9.14	Who Can Request Suspension	45
4.9.15	Procedure for Suspension Request.....	45
4.9.16	Limits on Suspension Period.....	45
4.10	Certificate Status Services.....	45
4.10.1	Operational Characteristics	45
4.10.2	Service Availability	45
4.10.3	Optional Features	46
4.11	End of Subscription	46
4.12	Key Escrow and Recovery.....	46
4.12.1	Key Escrow and Recovery Policy and Practices	46
4.12.2	Session Key Encapsulation and Recovery Policy and Practices	46
5	Facility Management and Operations Controls.....	47
5.1	Physical Controls.....	47

5.1.1	Site Location and Construction	47
5.1.2	Physical Access	47
5.1.3	Power and Air Conditioning.....	47
5.1.4	Water Exposures	47
5.1.5	Fire Prevention and Protection.....	47
5.1.6	Media Storage.....	48
5.1.7	Waste Disposal	48
5.1.8	Off-Site Backup.....	48
5.2	Procedural Controls.....	48
5.2.1	Trusted Roles	48
5.2.1.1	Administrator.....	49
5.2.1.2	Officer	49
5.2.1.3	Auditor	49
5.2.1.4	Operator.....	49
5.2.2	Number of Persons Required Per Task.....	49
5.2.3	Identification and Authentication for Each Role	50
5.2.4	Separation of Roles	50
5.3	Personnel Controls	50
5.3.1	Background, Qualifications, Experience, and Security Clearance Requirements	50
5.3.2	Background Check Procedures.....	50
5.3.3	Training Requirements.....	50
5.3.4	Retraining Frequency and Requirements.....	50
5.3.5	Job Rotation Frequency and Sequence	50
5.3.6	Sanctions for Unauthorized Actions	50
5.3.7	Independent Contractor Requirements	51
5.3.8	Documentation Supplied to Personnel	51
5.4	Audit Logging Procedures	51
5.4.1	Types of Events Recorded.....	51
5.4.2	Frequency of Processing Log.....	53
5.4.3	Retention Period for Audit Logs	53
5.4.4	Protection of Audit Logs	53
5.4.5	Audit Log Backup Procedures.....	53
5.4.6	Audit Collection System (internal vs. external)	54

5.4.7	Notification to Event-Causing Subject	54
5.4.8	Vulnerability Assessments	54
5.5	Records Archival	54
5.5.1	Types of Records Archived	54
5.5.2	Retention Period for Archive	55
5.5.3	Protection of Archive	55
5.5.4	Archive Backup Procedures	55
5.5.5	Requirements for Time-Stamping of Records	55
5.5.6	Archive Collection System (Internal vs. External)	55
5.5.7	Procedures to Obtain & Verify Archive Information	56
5.6	Key Changeover.....	56
5.7	Compromise and Disaster Recovery	56
5.7.1	Incident and Compromise Handling Procedures	56
5.7.2	Computing Resources, Software, and/or Data Are Corrupted	56
5.7.3	Entity Private Key Compromise Procedures.....	56
5.7.4	Business Continuity Capabilities after a Disaster	56
5.8	CA and RA Termination.....	57
6	Technical Security Controls	58
6.1	Key Pair Generation and Installation.....	58
6.1.1	Key Pair Generation.....	58
6.1.1.1	CA Key Pair Generation.....	58
6.1.1.2	Subscriber Key Pair Generation.....	58
6.1.2	Private Key Delivery to Subscriber	58
6.1.3	Public Key Delivery to Certificate Issuer.....	58
6.1.4	CA Public Key Delivery to Relying Parties.....	58
6.1.5	Key Sizes.....	59
6.1.6	Public Key Parameters Generation and Quality Checking.....	59
6.1.7	Key Usage Purposes	59
6.2	Private Key Protection and Cryptographic Module Engineering Controls	60
6.2.1	Cryptographic Module Standards and Controls	60
6.2.2	Private Key (n out of m) Multi-person Control.....	60
6.2.3	Private Key Escrow.....	60
6.2.4	Private Key Backup.....	60

6.2.5	Private Key Archival.....	60
6.2.6	Private Key Transfer into or from a Cryptographic Module	60
6.2.7	Private Key Storage on Cryptographic Module.....	61
6.2.8	Method of Activating Private Keys.....	61
6.2.9	Methods of Deactivating Private Keys.....	61
6.2.10	Method of Destroying Private Keys	61
6.2.11	Cryptographic Module Rating.....	61
6.3	Other Aspects of Key Management	61
6.3.1	Public Key Archival	61
6.3.2	Certificate Operational Periods/Key Usage Periods	61
6.4	Activation Data	61
6.4.1	Activation Data Generation and Installation.....	61
6.4.2	Activation Data Protection.....	62
6.4.3	Other Aspects of Activation Data	62
6.5	Computer Security Controls.....	62
6.5.1	Specific Computer Security Technical Requirements.....	62
6.5.2	Computer Security Rating	62
6.6	Life-Cycle Security Controls	62
6.6.1	System Development Controls.....	62
6.6.2	Security Management Controls	63
6.6.3	Life Cycle Security Ratings	63
6.7	Network Security Controls	63
6.8	Time Stamping	63
7	Certificate, CRL, and OCSP Profiles Format	64
7.1	Certificate Profile	64
7.1.1	Version Numbers	64
7.1.2	Certificate Extensions	65
7.1.3	Algorithm Object Identifiers	65
7.1.4	Name Forms	65
7.1.5	Name Constraints	66
7.1.6	Certificate Policy Object Identifier	66
7.1.7	Usage of Policy Constraints Extension.....	66
7.1.8	Policy Qualifiers Syntax and Semantics	66

7.1.9	Processing Semantics for the Critical Certificate Policy Extension	66
7.2	CRL Profile	66
7.2.1	Version Numbers	66
7.2.2	CRL and CRL Entry Extensions	66
7.3	OCSP Profile	67
7.3.1	Version Number(s)	67
7.3.2	OCSP Extensions	67
8	Compliance Audits and Other Assessments	68
8.1	Frequency and Circumstances of Assessment	68
8.2	Identity/Qualifications of Assessor	68
8.3	Auditor's Relationship to Assessed Entity	68
8.4	Topics Covered by Assessment	69
8.5	Actions Taken as a Result of Deficiency	69
8.6	Communication of Results	69
9	Other Business and Legal Matters.....	70
9.1	Fees	70
9.1.1	Certificate Issuance/Renewal Fees	70
9.1.2	Certificate Access Fees	70
9.1.3	Revocation or Status Information Access Fee.....	70
9.1.4	Fees for other Services	70
9.1.5	Refund Policy	70
9.2	Financial Responsibility	71
9.2.1	Insurance Coverage.....	71
9.2.2	Other Assets	71
9.2.3	Insurance/Warranty Coverage for End-Entities	71
9.3	Confidentiality of Business Information	71
9.3.1	Scope of Confidential Information	71
9.3.2	Information Not Within the Scope of Confidential Information.....	72
9.3.3	Responsibility to Protect Confidential Information	72
9.4	Privacy of Personal Information	72
9.4.1	Privacy Plan.....	72
9.4.2	Information Treated as Private	73
9.4.3	Information Not Deemed Private	73

9.4.4	Responsibility to Protect Private Information	73
9.4.5	Notice and Consent to Use Private Information.....	73
9.4.6	Disclosure Pursuant to Judicial/Administrative Process	73
9.4.7	Other Information Disclosure Circumstances	73
9.5	Intellectual Property Rights	73
9.6	Representations and Warranties	73
9.6.1	CA Representations and Warranties	73
9.6.2	RA Representations and Warranties	74
9.6.3	Subscriber Representations	74
9.6.4	Relying Parties Representations and Warranties	74
9.6.5	Representations and Warranties of Affiliated Organizations.....	74
9.6.6	Representations and Warranties of Other Participants.....	75
9.7	Disclaimers of Warranties	75
9.8	Limitations of Liabilities	75
9.9	Indemnities	75
9.9.1	Indemnification by Subscribers	75
9.9.2	Indemnification by Relying Parties	76
9.10	Term and Termination	76
9.10.1	Term for CPS.....	76
9.10.2	Termination.....	76
9.10.3	Effect of Termination and Survival.....	76
9.11	Individual Notices and Communications with Participants.....	76
9.12	Amendments	77
9.12.1	Procedure for Amendment	77
9.12.2	Notification Mechanism and Period	77
9.12.3	Circumstances Under Which OID Must be Changed.....	77
9.13	Dispute Resolution Provisions	77
9.14	Governing Law	77
9.15	Compliance with Applicable Law	77
9.16	Miscellaneous Provisions	78
9.16.1	Entire Agreement.....	78
9.16.2	Assignment	78
9.16.3	Severability	78

9.16.4 Enforcement (Attorney Fees/Waiver of Rights)	78
9.16.5 Force Majeure.....	78
9.17 Other Provisions.....	78

List of Tables

Table 1. List of References	14
Table 2. DirectTrust.org Certificate Policy Object Identifiers.....	16
Table 3. Acronyms	20
Table 4. Glossary of Terms	22
Table 5. x.501 Distinguished Name Attributes in DataMotion Direct CA Certificates	28
Table 6. x.501 Distinguished Name Attributes in DataMotion Direct Subscriber Certificates	29
Table 7. DirectTrust.org Authentication of Organization Healthcare Categories	30
Table 8. DirectTrust.org Authentication of Subscriber Identity by Level of Assurance	32
Table 9. DirectTrust.org Authentication of Patient Subscriber Identity	34
Table 10. Trusted Roles	48
Table 11. Auditable Events	51
Table 12. DataMotion Direct X.509 Certificate Basic Profile Fields.....	64
Table 13. CRL Reason Code	67

Revision History

For a list of revisions to the document, see the [Revision History on page 79](#).

1 Introduction

This document is the DataMotion Direct Certification Practices Statement (Abbreviated Version) (CPS), which is also referred to as “this DataMotion Direct CPS,” “this CPS,” or “this document.” This document also serves as the DataMotion Direct Registration Practice Statement (RPS).

This document states the policies and associated practices that DataMotion, Inc. (DataMotion) employs in operating the DataMotion Direct Public Key Infrastructure (DataMotion Direct PKI) as the Certification Authority (CA) and Registration Authority (RA) for X.509 digital certificates used in the exchange of electronic messages grounded in the [Direct Project's Applicability Statement for Direct Secure Health Transport](#).

The Direct Project is an initiative sponsored by the [Office of the National Coordinator \(ONC\) for Health Information Technology](#) to allow participants to send authenticated, encrypted health information directly to known, trusted recipients over the Internet. The Direct Project is based on S/MIME message signatures and message encryption for the purposes of achieving privacy, authentication, message integrity, and non-repudiation.

The DataMotion Direct CPS is based on and is governed by the [Direct Trust Community X.509 Certificate Policy](#) (DirectTrust CP), and it is compliant with the DirectTrust CP version as specified in Section 1.1.2.

DirectTrust is a non-profit, competitively neutral, self-regulatory entity operated by and for participants in the Direct community. The DirectTrust Board of Directors, with the assistance of the DirectTrust Policy Committee, is responsible for the DirectTrust CP, the approval of related practice statements, and overseeing the conformance of CA practices with its CP.

The DataMotion Direct CPS also generally conforms to the policy framework described in [RFC 3647](#), Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, issued by the Internet Engineering Task Force (IETF). None of the sections stipulated by RFC 3647 have been omitted; however, to preserve the framework of RFC 3647, some sections of this CPS will include the statement “No stipulation” where the CP and CPS imposes no requirements or makes no disclosure, or “Not applicable” if the particular topic addressed by that section does not apply. DataMotion reserves the right to vary from this framework in its sole discretion.

This CPS is intended to be fully consistent with US Federal Government requirements for identity proofing as described in NIST Special Publication 800-63. More specifically, identity proofing levels of assurance defined in this CPS are intended to align with NIST SP 800-63 identity proofing levels of assurance. However, this CPS also specifies requirements that further constrain the conditions under which a DirectTrust Community conformant digital certificate may be issued, utilized and managed.

Operational requirements for issuing Certification Authorities and Registration Authorities operating under this CP are intended to be, at a minimum, consistent with operational requirements defined in the U.S. Federal Bridge Certification Authority CP for an entity operating at a Basic assurance level.

References

The following list identifies documents and related information referenced in this CPS.

Table 1. List of References

Document ID	Document Name
FIPS 140-2	Federal Information Processing Standard (FIPS) Publication 140-2, Security Requirements for Cryptographic Modules, 3 December 2002.
FIPS 186-2	Federal Information Processing Standard (FIPS) Publication 186-2, Digital Signature Standard (DSS), January 2000.
RFC 1034	Internet Engineering Task Force (IETF) Request for Comments 1034, "Domain Names – Concepts and Facilities," November 1987
RFC 2560	Internet Engineering Task Force (IETF) Request for Comments 2560, "X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP", issued by the IETF, June 1999.
RFC 3647	Internet Engineering Task Force (IETF) Request for Comments 3647, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework," November 2003
RFC 5280	Internet Engineering Task Force (IETF) Request for Comments 5280, "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", May 2008
NIST SP 800-63-2	National Institute of Standards and Technology (NIST) Special Publication 800-63-2, Electronic Authentication Guideline, August 2013
X.500	ITU-T X.500 Recommendation (also ISO/IEC Standard 9594-1:2008), "The Directory: Public-key and attribute certificate frameworks", November 2008
X.509	ITU-T X.509 Recommendation (also ISO/IEC Standard 9594-8:2014), "The Directory: Public-key and attribute certificate frameworks", October 2012

1.1 Overview

This CPS describes the practices under which the DataMotion Direct Public Key Infrastructure (PKI) operates. Specifically, this document defines the creation and life-cycle management of X.509 version 3 public key certificates for use in applications supporting Direct Project message exchange.

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1.1.1 Certificate Policy (CP)

According to the ITU-T X.509 standard, a “certificate policy” (CP) is defined as “a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.”

Digital Certificates that conform to this CPS must contain a minimum of three registered certificate policy object identifiers (OIDs), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. An OID specifying the version of the Direct Trust CP, an OID corresponding to an identity proofing Level of Assurance (LoA), and an OID corresponding to a healthcare category shall be available to Relying Parties. The DataMotion Direct CA asserts the appropriate OIDs in the *certificatePolicies* extension of Subscriber certificates.

1.1.2 Relationship between the DirectTrust CP and this CPS

DataMotion has determined that substantial equivalence exists between the provisions of this CPS and the DirectTrust Community X.509 Certificate Policy, Version 1.4. Accordingly, DataMotion Direct certificates issued by the DataMotion Direct CA will assert the OID(s) defined in the DirectTrust Community X.509 Certificate Policy, Version 1.4. These include the OIDs for the following:

- DirectTrust Certificate Policy v1.4 OID: 1.3.6.1.4.1.41179.0.1.4
- One of the following Identity Proofing Level of Assurance (Levels 1 through 3) OIDs:
 - 1.3.6.1.4.1.41179.1.1
 - 1.3.6.1.4.1.41179.1.2
 - 1.3.6.1.4.1.41179.1.3
- One of the following Healthcare Entity Categories (Cat) OIDs:
 - 1.3.6.1.4.1.41179.2.1
 - 1.3.6.1.4.1.41179.2.2
 - 1.3.6.1.4.1.41179.2.3
 - 1.3.6.1.4.1.41179.2.4
 - 1.3.6.1.4.1.41179.2.5
- If the certificate is issued to a device, the Device OID is also asserted:
 - 1.3.6.1.4.1.41179.3

If DataMotion determines that its policies and practices continue to conform substantively to any future version of the DirectTrust CP, DataMotion may choose to assert the updated DirectTrust CP OIDs in its certificates instead.

1.1.3 Relationship between the DirectTrust CP and the DataMotion Direct CP

If in the future DataMotion creates its own CP governing this CPS, it will assert a mapping between its CP and the DirectTrust CP in the *policyMappings* extension of its CA and/or Subscriber certificates.

1.1.4 Relationship between DirectTrust CP and DirectTrust-EHNAC Accredited Entities

Conformance to an active DirectTrust CP version is a requirement for accreditation under the DirectTrust-EHNAC accreditation program, and entities accredited under this program have been audited regarding implementation of practices in compliance with an active DirectTrust CP version in conjunction with proper use of the DirectTrust policy OIDs. DirectTrust publishes bundles of trust anchors for the purpose of assisting Relying Parties in verifying the accredited status of HSPs, CAs, and RAs, available at bundles.directtrust.org.

1.2 Document Name and Identification

This document is the DataMotion Direct Certification Practices Statemen (Abbreviated Version) (CPS) version 4-A.

This CPS defines multiple levels of assurance each assigned a unique object identifier (OID). The set of policy OIDs are registered under an arc of DirectTrust.org assigned organizational identifier as registered in the ISO/ITU OID Registry. The applicable OIDs pertaining to this CPS and the trust community are defined as follows:

[iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprise(1)]

Table 2. DirectTrust.org Certificate Policy Object Identifiers

id-DTorg arc		1.3.6.1.4.1.41179
id-DTorg-policies	id-DTorg.(0)	1.3.6.1.4.1.41179.0
DT.org CP 1.4	id-DTorg-policies.(1.4)	1.3.6.1.4.1.41179.0.1.4
Id-DTorg-LoAs	id-DTorg.(1)	1.3.6.1.4.1.41179.1
DT.org LoA 1	id-DTorg-LoAs.(1)	1.3.6.1.4.1.41179.1.1
DT.org LoA 2	id-DTorg-LoAs.(2)	1.3.6.1.4.1.41179.1.2
DT.org LoA 3	id-DTorg-LoAs.(3)	1.3.6.1.4.1.41179.1.3
DT.org LoA 4	id-DTorg-LoAs.(4)	1.3.6.1.4.1.41179.1.4
Id-DTorg-Cat	id-DTorg.(2)	1.3.6.1.4.1.41179.2
DT.org CE	id-DTorg-Cat.(1)	1.3.6.1.4.1.41179.2.1
DT.org BA	id-DTorg-Cat.(2)	1.3.6.1.4.1.41179.2.2
DT.org HE	id-DTorg-Cat.(3)	1.3.6.1.4.1.41179.2.3
DT.org Patient	id-DTorg-Cat.(4)	1.3.6.1.4.1.41179.2.4
DT.org Non Declared	id-DTorg-Cat.(5)	1.3.6.1.4.1.41179.2.5
DT.org Device	id-DTorg.(3)	1.3.6.1.4.1.41179.3

DataMotion Direct CA asserts only the OIDs above when issuing under the DirectTrust arc. Policy OIDs asserting additional compliance with other CPs, i.e., under a different policy arc MAY also be asserted.

NOTE: The Direct Project specification does not explicitly require utilization of policy OIDs as a mechanism of asserting trust. Rather, a set of trust anchor certificates are maintained by a relying party and each presented certificate must chain to a certificate within this set of trust anchor certificates. The DataMotion Direct CA only issues Direct certificates, and indicates which policy OIDs it issues certificates for, in order to be effectively utilized by Subscribers that depend exclusively upon binary trust of CA certificates.

1.3 PKI Participants

The community governed by this CPS is DataMotion Direct PKI. The DataMotion Direct PKI accommodates individuals and organizations with a need to securely exchange health information over the Internet.

PKI Participants are those entities involved in the registration, issuance, use of, or reliance upon DirectTrust Certificates. Participants include DataMotion, Customers, Subscribers, Relying Parties, Certification Authorities, and Registration Authorities. This DataMotion Direct CPS applies to all Participants in the DataMotion PKI. The following are descriptions of the roles relevant to the administration and operation of the DataMotion Direct PKI.

1.3.1 DataMotion Direct Management

The DataMotion Compliance Committee (DMCC) is the management team of DataMotion Direct that has established this PKI, oversees its operation, and is responsible for governing its use. This CPS was established under the authority of and with the approval of the DMCC. The DMCC is comprised of DataMotion security and business management individuals. The DMCC represents the interests of DataMotion and is responsible for:

- Approving the CPS and any successive changes,
- Ensuring continued conformance of this CPS with the DirectTrust CP, and
- Overseeing the conformance of DataMotion Direct practices with this CPS.

1.3.2 Certification Authorities (CAs)

The DataMotion Direct CA issues public key X.509 certificates for Direct exchange or Direct Project organizational or individual Subscribers, and, through such issuance, attests to the binding between an identity and cryptographic Key Pair to a Subscriber. The DataMotion Direct CA is also referred to as the Issuing CA or the Certificate Issuer in this document. As described in other sections of this document, the DataMotion Direct CA also publishes, maintains, and revokes certificates; publishes and updates Certificate Revocation Lists; and may also provide an OCSP service.

The DataMotion Direct CA is accredited through the DirectTrust and Electronic Healthcare Network Accreditation Commission (EHNAC) Direct Trusted Agent Accreditation Program (DTAAP) for issuing DirectTrust-compliant certificates, and this CPS is reviewed as part of that accreditation process to ensure conformance to the policies of the DirectTrust CP. This CA conforms to the policies of the DirectTrust.org CP v1.4.

1.3.3 Registration Authorities (RAs)

Registration Authorities (RA) are organizations responsible for collecting and proofing a Subscriber's identity and any other information provided by the Subscriber for inclusion in a certificate. DataMotion may act as its own RA or may delegate or subcontract the collection of identity proofing to a Trusted Agent that has executed an agreement establishing the agent in the role for performing identity proofing. This CPS also serves as the Registration Authority Practice Statement (RPS).

RAs collect and verify identity information from Direct Subscriber Applicants using procedures that implement the identity validation policies set forth in this document. If DataMotion delegates RA activities, it monitors their compliance with this CPS or the DirectTrust CP and if applicable, any Registration Practices Statement (RPS) under which the RA operates.

1.3.3.1 Trusted Agents (TAs)

Trusted Agents are individuals who act on behalf of the CA or RA to collect and/or verify information regarding Subscribers, and where applicable to provide support regarding those activities to the Subscribers. While not an employee of the CA or RA, Trusted Agents are individuals who have a direct contractual relationship with the CA or RA, either as: a) an Individual; or b) an employee of an Organization that has a direct contractual relationship with the CA or RA that involves performance of collection and/or confirmation of information regarding Subscribers.

1.3.4 Subscribers

A DataMotion Direct *Subscriber* is an individual, organization or Device to whom or to which a certificate is issued. Subscribers are named in the certificate subject and hold either directly or through its designated HISP (or other authorized third party), a Private Key that corresponds to the Public Key listed in the certificate. A Subscriber is an entity who uses Direct services and PKI to support Direct message exchange. Prior to proofing of *Applicant*.

1.3.4.1 Health Information Service Providers (HISPs)

DataMotion is accredited by DirectTrust and the Electronic Healthcare Network Accreditation Commission (EHNAC) as a Health Information Service Provider (HISP) that processes Direct-compliant messages to and from Direct addresses, each of which is bound to a Direct-compliant certificate. Acting in the capacity of an agent for the Subscriber, the DataMotion Direct HISP holds and manages PKI private keys associated with a Direct digital certificate on behalf of the Subscriber.

1.3.4.2 Sponsors and Sponsoring Organizations

A Sponsor fills the role of a Subscriber for groups, organizations, disabled personnel, or non-human system components named as public key certificate Subjects. The Sponsor works with the CA and RA to register the above elements in accordance with CPS Sections 3.2.2 and 3.2.3, and is responsible for meeting the obligations of Subscribers as defined throughout this document.

An organization may sponsor an individual or device to be a Subscriber to a certificate. An authenticated and authorized organizational representative shall confirm the affiliation between the individual or device and the

organization. When an organization has sponsored an individual or device as a Subscriber of a certificate, the individual or device is considered as acting on behalf of and as an agent of the sponsoring organization when using the certificate and/or the corresponding keys.

1.3.5 Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the Subscriber's name to a public key. A Relying Party may use a Subscriber's certificate to verify the integrity of a digitally signed message, to identify the creator of a message, or to establish confidential communications with the Subscriber. The Relying Party is responsible for deciding whether or how to check the validity of the certificate by checking the appropriate certificate status information (CRL or OCSP).

1.3.6 Other Participants

1.3.6.1 Affiliates

An Affiliate is an individual or organization legally distinct from the Subscriber who is permitted by the Subscriber to use Direct Addresses bound to the Subscriber's certificate, provided that the Affiliate is performing its work, duties or activities on behalf of the Subscriber when using that Direct Address.

An individual granted proxy account access by a patient, such as a parent of a minor, spouse or health care proxy for an elderly person, is considered an Affiliate.

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

The primary use for a DataMotion Direct CA certificate is in the exchange of electronic messages grounded in the [specification](#) of the Direct Project. Other usages include but are not limited to securing healthcare applications and providing consumer/patient access to data.

Certificates issued by this CA shall only be used for the purposes designated in the *keyUsage* extension of the certificate key usage and extended key usage fields found in the certificate. However, each Relying Party should evaluate the application environment and associated risks before deciding on whether to accept a certificate issued by this CA for a particular transaction. In accepting a certificate issued by this CA, the Relying Party accepts all risks associated with its use.

An Affiliate that is a health care provider or health care organization may only use the certificate of a Subscriber if that Affiliate provides care on behalf of the Subscriber and the Subscriber is a HIPAA Covered Entity. A Covered Entity shall only be an Affiliate of another Covered Entity and shall not be an Affiliate of a Business Associate. For example, an HIE (Business Associate) shall not allow use of its own certificate by a health care provider or health care organization (Covered Entity).

1.4.2 Prohibited Certificate Uses

Certificates do not guarantee that the Subject is trustworthy, honest, reputable in its business dealings, compliant with any laws, or safe to do business with. A certificate only establishes that the information in the

certificate was verified as reasonably correct to a known level of assurance when the certificate was issued. Certificates issued under this policy may not be used where prohibited by law.

1.5 Policy Administration

1.5.1 Organization Administering the Document

The DataMotion Compliance Committee (DMCC) is responsible for this CPS.

1.5.2 Contact Person

Questions regarding this document should be directed to:

CISO
DataMotion Compliance Committee
DataMotion, Inc.
200 Park Ave.
Florham Park, NJ 07932
USA

Phone: 1 800-672-7233 or +1 973-455-1245
Fax: +1 973-455-0750

1.5.3 Person Determining Certification Practices Statement Suitability

The DMCC is responsible for determining suitability of all documents under this CPS and for approving the content of this CPS and any future changes, updates, or modifications to it. Such approval shall be declared in Section 1.1.2.

1.6 Definitions and Acronyms

1.6.1 Acronyms

Table 3. Acronyms

Acronym	Meaning
BA	Business Associate
CA	Certificate Authority
CE	Covered Entity
CFR	Code of Federal Regulations
CN	Common Name
CP	Certificate Policy

CPS	Certification Practices Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As
DMCC	DataMotion Compliance Committee
DN	Distinguished Name
DS	Discovery Service
DSA	Digital Signature Algorithm cryptography
DTAAP	Direct Trusted Agent Accreditation Program
EDSA	Elliptic Curve Digital Signature Algorithm cryptography
EHNAC	Electronic Healthcare Network Accreditation Commission
EIN	Employer Identification Number
FBCA	Federal Bridge Certificate Authority
FIPS	Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HE	Healthcare Entity
HIPAA	Health Insurance Portability and Accountability Act of 1996
HISP	Health Information Service Provider
HITECH	Health Information Technology for Economic and Clinical Health Act (part of the American Recovery and Reinvestment Act of 2009)
HSM	Hardware Security Module
HTTP	Hypertext Transfer Protocol
ID	Identifier
IETF	Internet Engineering Task Force
ISSO	Information System Security Officer
ITU	International Telecommunication Union
ITU-T	ITU Telecommunication Standardization Sector
LoA	Level of Assurance
NIST	National Institute of Standards and Technology
NPI	National Provider Identifier
OCSP	Online Certificate Status Protocol
OID	Object Identifier

ONC	Office of the National Coordinator for Health Information Technology (part of the U.S. Department of Health and Human Services)
PKI	Public Key Infrastructure
RA	Registration Authority
RFC	Request For Comments
RP	Relying Party
RPA	Relying Party Agreement
RPS	Registration Practice Statement
RSA	Rivest Shamir Adleman cryptosystem
SHA	Secure Hashing Algorithm
S/MIME	Secure Multipurpose Internet Mail Extensions
SSL	Secure Sockets Layer
TA	Trusted Agent
TLS	Transport Layer Security
URI	Uniform Resource Identifier
URL	Uniform Resource Locator

1.6.2 Definitions

Table 4. Glossary of Terms

Term	Definition
Address-Bound Certificate	A digital certificate that contains full Direct address in the form of an RFC 822 email address in the certificate <i>subjectAlternativeName</i> extension. It may also be referred to as an Individual Certificate or Individual Address Certificate.
Affiliate	An individual or organization legally distinct from the Subscriber who is permitted by the Subscriber to use Direct addresses bound to the Subscriber's certificate, provided that the Affiliate is performing its work, duties or activities on behalf of the Subscriber when using that Direct address. See CPS Section 1.3.6.1 Affiliates.
Applicant	A person or other legal entity that submits an application and identifying information to the CA or RA for the purpose of obtaining or renewing a certificate.
Business Associate or BA	An organization that helps Covered Entities carry out health care activities and functions under a written Business Associate contract or other arrangement with the Business Associate that establishes specifically what the Business Associate has been engaged to do and requires the Business Associate to comply with the requirements to protect the privacy and security of protected health information. Business Associates in this CPS are as defined under HIPAA at 45 CFR 160.103.
Certificate	An X.509 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.
Certification Authority or CA	An entity that issues public key X.509 certificates and, through such issuance, attests to the binding between an identity and cryptographic key pair to a Subscriber. See CPS Section 1.3.2 Certification Authorities (CAs). Sometimes referred to as a Certificate Authority.
Certificate Policy or CP	A Certificate Policy (CP) is a specialized documentation of administrative policy describing electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, distribution, accounting, revoking, compromise recovery and administration of digital certificates.
Certification Practices Statement or CPS	A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing revocation status to Relying Parties.
Certificate Revocation List or CRL	A list maintained by a Certification Authority of the certificates that are suspended or revoked prior to their stated expiration date.
Code of Federal Regulations or CFR	Regulations imposed by U.S. Federal law.
Covered Entity or CE	An individual, organization, or agency that protects the privacy and security of health information and provides individuals with certain rights with respect to their health information. Covered Entities are defined under HIPAA at 45 CFR 160.103.
Device	A non-human Subscriber of a certificate. Examples of Devices include but are not limited to routers, firewalls, servers, imaging systems, consumer diagnostics, cameras, and other devices capable of securely handling private keys and properly implementing PKI technologies, either directly or through a HISP when used for Direct messaging.
Device Certificate	A certificate issued to a device.
Direct Address	Direct Addresses consist of a Health Endpoint Name, the “@” symbol, and a Health Domain Name, which is a fully qualified domain name (FQDN). For example: janedoe@direct.datamotion.com . Direct Addresses must be linked to an associated certificate that confirms the identity either of the domain name or of the full address. The intent of a Direct Address is to provide a method of routing from an origination point to the addressed recipient, not to provide a single, definitive ID for the intended recipient. The same real-world person may have multiple Direct Addresses.
Direct Project	An initiative from the Office of the National Coordinator (ONC) for Health Information Technology that created a set of standards and services that, with a policy framework, enables simple, routed, scalable, and secure message transport over the Internet between known participants.
Domain-Bound Certificate	A certificate that contains a Health Domain Name in the form of a <i>dNSName</i> in the <i>subjectCommonName</i> and <i>subjectAlternativeName</i> extensions of the certificate. Also known as an Organizational Certificate.
Group Certificate	Certificate with a private key that is shared by multiple Subscribers. An Organizational Certificate is a type of Group Certificate that is shared among authenticated employees and agents of the organization. An Individual Address Certificate is a type of Group Certificate when the private key is held by the HISP on behalf of the Subscriber.
Health Domain Name	A fully qualified domain name dedicated solely to the purposes of health information exchange. The domain name string must conform to the requirements of RFC 1034 (Domain Names – Concepts and Facilities). For example: direct.datamotion.com .
Health Endpoint	A string conforming to the local-part requirements of RFC 5322 and that expresses real-

Name	world origination points and endpoints of health information exchange, as vouched for by the organization managing the Health Domain Name. For example: janedoe (referring to an individual), familypractice (referring to an organizational inbox), and diseaseregistry (referring to a processing queue).
Health Information Service Provider or HISP	An organization that provides the management of security and transport as it relates to information exchange using Direct Project standards on behalf of the sending or receiving organization or individual. The HISP assigns and maintains the Direct email addresses for EHRs, HIEs, individual providers, as well as others, and relays their medical data securely using Direct protocols.
Healthcare Entity	An entity involved in healthcare that has agreed to protect private and confidential patient information consistent with the requirements of HIPAA although it is not a Covered Entity or Business Associate as defined under HIPAA at 45 CFR 160.103.
HIPAA	The Health Insurance Portability and Accountability Act of 1996, as amended.
HIPAA Representative	A person named by a patient granting authority to have access to the patient's Protected Health Information. The designation of HIPAA representative does not in itself grant the representative authority to make health care decisions for the patient.
Internet Engineering Task Force or IETF	A standards development organization responsible for the creation and maintenance of many Internet-related technical standards.
Individual Certificate	Certificate tied to an individual full Direct address. See Address Certificate.
Information System Security Officer or ISSO	A person at the HISP who is responsible for managing the registration process, certificate requests, and private keys for Direct. This includes ensuring adequate protection of cryptographic keys held on behalf of customers, and also for tracking and recording who has access to the keys at any given point.
Key Pair	A Private Key and associated Public Key.
Level of Assurance or LoA or LOA	The identity proofing level implemented for issuance of a certificate. LoAs as used in this CPS are intended to correspond to identity proofing LoAs as defined in NIST SP 800-63.
Non-Declared Entity	An entity that has not asserted it will protect personal health information with privacy and security protections that are equivalent to those required by HIPAA and is not a Patient/Consumer.
Non-Declared Entity Certificate	A certificate issued to a Non-Declared Entity.
OCSP	An Internet protocol used for obtaining certificate's revocation status.
OCSP Responder	An Online Certificate Status Protocol service that processes certificate status queries.
Organizational Certificate	Certificate that asserts an organization affiliation and is tied to a Health Domain Name. It is a type of Group Certificate. See Domain-Bound Certificate.
Patient	An individual using his or her Direct Address for information exchange for personal reasons and not as a health care professional, Business Associate or individual associated with a HIPAA covered entity.
Patient Certificate	An address certificate issued to a patient containing a full Direct address in the form of an RFC 822 email address in the certificate <i>subjectAlternativeName</i> extension.
Private Key	The confidential key kept secret by its holder and which is part of an asymmetric key pair. It is used to create digital signatures or to decrypt data encrypted with the holder's corresponding Public Key.

Professional	An individual who acts on behalf of an organization which is a covered entity or business associate under HIPAA, or is a healthcare related organization which treats protected health information with privacy and security protections that are equivalent to those required by HIPAA.
Public Key	The non-confidential key that is publicly disclosed by the holder in the form of a digital certificate and which is part of an asymmetric key pair. It is used for validation of a digital signature or to encrypt data that may then be decrypted using the corresponding private key.
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.
Registration Authority	An organization that is responsible for proofing a Subscriber's identity and verifying any other information provided by Subscriber for inclusion in a certificate.
Relying Party	A person or entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them.
Sponsor	An individual who fills the role of a Subscriber for non-human system components named as public key certificate subjects. The Sponsor works with the CA and RA for registration of the components and is responsible for meeting the obligations of Subscribers as defined throughout this document.
S/MIME	A standard for public key encryption and digital signing of email messages.
Subscriber	An entity that either (1) authorized application for the certificate, or (2) is the subject named or identified in a certificate issued to that entity. A Subscriber may request certificate modification, renewal, suspension and revocation and holds, directly or through its designated HISP (or other Subscriber-authorized third party), a private key that corresponds to the public key listed in the certificate.
Subscriber Applicant	An individual that requests Direct enabled communication on behalf of their organization.
Trust Bundle	A collection of CA certificates used as trust anchors by a relying party.
Trusted Agent	An organization authorized to act as a representative of a Subscriber in confirming the Subscriber Applicant identification during the registration process.
Trusted Role	A role held by individuals performing functions fundamental to the integrity of the PKI.
User	An individual authorized by a Subscriber to access or make use of a private key corresponding to a certificate for the purpose of originating or accepting delivery of Direct messages.
X.509	The ITU-T standard for certificates and their corresponding authentication framework.

NOTE: The Remainder of the Document is Available on Request.

2 The Remainder of the Document is Available on Request

CONFIDENTIAL

Access Limited to Authorized Personnel

Confidential and Proprietary Information [#060013-04-A] 

The Remainder of the Document is Available on Request

Page 26 of 26