MaxMD Registration Practices Statement

MaxMD Direct HISP
January 30, 2013
Version 1.00

TABLE OF CONTENTS

1. INTRODUCTION

1.1. OVERVIEW

This document is the MaxMD Direct HISP Registration Practices Statement (RPS). The RPS outlines the procedures that MaxMD Direct HISP and its customers follow to comply with the MaxMD CP and CPS and the DirectTrust Ecosystem Community X.509 CP (Draft for Trial Use). If any inconsistency exists between this RPS and the MaxMD CPS, the MaxMD CPS takes precedence.

1.2. DOCUMENT NAME AND IDENTIFICATION

This document is the MaxMD Direct HISP Registration Practices Statement and was approved on 30 January 2013 by MaxMD and MaxMD Direct HISP.

1.3. PKI PARTICIPANTS

1.3.1. Certification Authorities

MaxMD is a certification authority (CA) that issues high quality and highly trusted digital certificates in accordance with its CPS. As a CA, MaxMD performs functions associated with Public Key operations, including receiving certificate requests, issuing, revoking and renewing a digital certificate, and maintaining, issuing, and publishing CRLs and OCSP responses.

1.3.2. Registration Authorities

MaxMD Direct HISP is a Registration Authority (RA) that can request certificates and perform identification and authentication for end-user certificates. MaxMD Direct HISP is contractually obligated to abide by MaxMD's CPS and any industry standards that are applicable to MaxMD Direct HISP's role in certificate issuance, management, and revocation.

1.3.3. Subscribers

Subscribers are the customers of MaxMD Direct HISP who use MaxMD's certificates to conduct secure transactions and communications. Subscribers are not always the party identified in a certificate, such as in a group certificate or when certificates are issued to an organization's employees. The *Subject* of a certificate is the party named in the certificate. A *Subscriber*, as used herein, refers to both the Subject of the certificate and the entity that contracted with the HISP who employs MaxMD for the certificate's issuance. Prior to verification of identity and issuance of a certificate, a Subscriber is an *Applicant*.

1.3.4. Relying Parties

Relying Parties are entities that act in reliance on a certificate and/or digital signature provided by MaxMD Direct HISP. Relying parties must check the appropriate CRL or OCSP response prior to relying on information featured in a certificate.

1.3.5. Other Participants

Certain MaxMD Direct HISP customers are designated as "Trusted Agents". Trusted Agents are authorized by MaxMD Direct HISP and MaxMD to gather documentation in relation to the issuance of a digital certificate.

1.4. CERTIFICATE USAGE

A *digital certificate* (or *certificate*) is formatted data that cryptographically binds an identified subscriber with a Public Key. A digital certificate allows an entity taking part in an electronic transaction to prove its identity to other participants in such transaction. Digital certificates are used in commercial environments as a digital equivalent of an identification card.

1.4.1. Appropriate Certificate Uses

Customers may use issued certificates for the purposes set forth in MaxMD's CPS.

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 when the certificate issued.

Certificates may not be used (i) for any application requiring fail-safe performance such as (a) the operation of nuclear power facilities, (b) air traffic control systems, (c) aircraft navigation systems, (d) weapons control systems, or (e) any other system whose failure could lead to injury, death or environmental damage; or (ii) where prohibited by law.

1.5. PRACTICE STATEMENT ADMINISTRATION

1.5.1. Organization Administering the Document

This RPS is maintained by MaxMD Direct HISP , which can be contacted at:

MaxMD Direct HISP
Address 2200 Fletcher Ave
Fort Lee NJ 07024
Tel: 201-963-0005

MaxMD may be contacted at:

MaxMD Policy Authority
2200 Fletcher Ave
Fort Lee New Jersey 07024 USA
Tel: 1-201-963-0005
Fax: 1- 201-482-5925

1.5.2. Contact Person

MaxMD Direct HISP c/o Bruce B Schreiber
2200 Fletcher Ave
Fort Lee New Jersey 07024
Tel: 201-963-0005

1.5.3. Person Determining RPS Suitability

MaxMD Direct HISP's management team and the MaxMD Certificate Policy Authority (DCPA) are responsible for determining the suitability and applicability of this RPS.

1.5.4. RPS Approval Procedures

MaxMD Direct HISP and the MAXMD RA approve this RPS and any amendments. Amendments are made by either updating the entire RPS or by publishing an addendum.

1.6. DEFINITIONS AND ACRONYMS

"Affiliated Organization" means an organization that has an organizational affiliation with a Subscriber and that approves or otherwise allows such affiliation to be represented in a certificate.

“Applicant” means an entity applying for a certificate.

“Application Software Vendor” means a software developer whose software displays or uses MaxMD certificates and distributes MaxMD’s root certificates.

“Direct Address” means a name used to identify a Direct endpoint (a Sender or Receiver) when information is exchanged. The Direct Address has two parts, a Health End Point Name and a Health Domain Name, for example, drbob@samplehispname.org.

“Health Domain Name” means the delivery location for messages to an individual MaxMD Direct HISP, the HISP portion of a Direct Project Address

“Health End Point” means the delivery location for messages to an individual Direct user, the user portion of a Direct Project Address.

“HISP” or Health Information Service Provider means the entity that is responsible for delivering health information as messages between senders and receivers over the Internet.

“Key Pair” means a Private Key and associated Public Key.

“MaxMD CA” means MaxMD acting as Certificate Authority.

“MaxMD RA” means MaxMD acting as Registration Authority or an Agent of MaxMD acting as Registration Authority.

“OCSP Responder” means an online software application operated under the authority of MaxMD and connected to its repository for processing certificate status requests.

“Private Key” means the key of a key pair that is kept secret by the holder of the key pair, and that is used to create digital signatures and/or to decrypt electronic records or files that were encrypted with the corresponding Public Key.

“Public Key” means the key of a key pair that may be publicly disclosed by the holder of the corresponding Private Key and that is used by a Relying Party to verify digital signatures created with the holder's corresponding Private Key and/or to encrypt messages so that they can be decrypted only with the holder's corresponding Private Key.

“Relying Party” means an entity that relies upon either the information contained within a certificate or a time-stamp token.

“Relying Party Agreement” means an agreement which must be read and accepted by the Relying Party prior to validating, relying on or using a Certificate or accessing or using MaxMD’s Repository. The Relying Party Agreement is available for reference through a MaxMD online repository.

“Subscriber” means either entity identified as the subject in the certificate or the entity that is receiving MaxMD’s time-stamping services.

“Subscriber Agreement” means an agreement that governs the issuance and use of a certificate that the Applicant must read and accept before receiving a certificate.

Acronyms:

CA	Certificate Authority or Certification Authority
CP	Certificate Policy DirectTrust.org V1-1.2
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSR	Certificate Signing Request
DBA	Doing Business As (also known as "Trading As")
FIPS	(US Government) Federal Information Processing Standard
FQDN	Fully Qualified Domain Name
HISP	Health Information Service Provider
HTTP	Hypertext Transfer Protocol
IGTF	International Grid Trust Federation
ISSO	Information Systems Security Officer
OCSP	Online Certificate Status Protocol
OID	Object Identifier
PKI	Public Key Infrastructure
PKIX	IETF Working Group on Public Key Infrastructure
PKCS	Public Key Cryptography Standard
RA	Registration Authority
SHA	Secure Hashing Algorithm
SSL	Secure Sockets Layer
TLD	Top-Level Domain
TLS	Transport Layer Security
URL	Uniform Resource Locator
X.509	The ITU-T standard for Certificates and their corresponding authentication framework

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

Conforming RAs shall operate repositories in support of operations required by the CP and related CPS.

Repositories holding certificate status data should be operated 24 hours a day, 7 days a week with a minimum of 99% availability overall per year .

Conforming RAs shall protect repository information not intended for public dissemination or modification.

3. IDENTIFICATION AND AUTHENTICATION

3.1. NAMING

3.1.1. Types of Names

All certificates shall use non-null DN name forms for the issuer and subject names. As specified in the Direct Project Applicability Statement for Secure Health Transport, certificates tied to full Direct addresses (“Address certificates”) shall contain the Direct address in the subjectAltName extended attribute as an rfc822Name. Certificates tied to a Direct domain (“Organizational certificates”) shall contain the domain name in two places:

1. The subjectAltName extension formatted as a dNSName, and
2. The CN of the Subject DN.

3.1.2. Need for Names to be Meaningful

Names used in certificates shall uniquely identify the organization or person to which they are assigned and shall be easily understood by humans

3.1.3. Anonymity or Pseudonymity of Subscribers

CAs shall not issue anonymous certificates. Pseudonymous certificates may be issued as long as name space uniqueness requirements are met.

3.1.4. Rules for Interpreting Various Name Forms

No Stipulation.

3.1.5. Uniqueness of Names

Each certificate contains a unique subject name and/or serial number.

3.1.6. Recognition, Authentication, and Role of Trademarks

Subscribers and HISPs are contractually required to refrain from requesting certificates with content that infringes on the intellectual property rights of another entity. MaxMD does not verify an Applicant's right to use a trademark and does not resolve trademark disputes.

3.2. INITIAL IDENTITY VALIDATION

3.2.1. Method to Prove Possession of Private Key

A HISP must submit a CSR on behalf of a Group certificate Applicant to establish that it holds the Private Key corresponding to the Public Key in the certificate request. A PKCS#10 format or Signed Public Key and Challenge (SPKAC) is recommended.

3.2.2. Authentication of Organization Identity

Organizational certificate applicants are required to include their name. address, domain name, and evidence of the organization's existence in the certificate application. The requesting organization must be a HIPAA covered entity, a HIPAA business associate, or a healthcare-related organization that treats protected health information with privacy and security protections that are equivalent to those required by HIPAA. Each organizational certificate must represent a legally distinct entity. MaxMD Direct HISP may rely on a representation from the organization to verify the organization's status as an entity qualifying for a Direct Certificate.

MaxMD Direct HISP shall verify the included applicant's name and address using a reliable third party database, a government databases, or through MaxMD Direct HISP means of communication with the entity or jurisdiction responsible for the organization's creation or recognition. If MaxMD Direct HISP cannot use these sources to verify the name and address, then MaxMD Direct HISP may verify the name and address using official company documentation that is submitted by the applicant, such as a business license, filed or certified articles of incorporation/organization, tax certificate, corporate charter, official letter, sales license, or other relevant documents.

For SSL Certificates, MaxMD Direct HISP must use MaxMD's domain validation systems to verify the applicant's right to use the domain name that will be listed in the certificate. If an entity other than the domain owner is requesting the certificate, then MaxMD Direct HISP shall obtain a document authorizing the Applicant's request for a certificate. This document must be signed by the Registrant (e.g. a domain owner's authorized representative) or the Administrative Contact on the Domain Name Registrar record.

If the certificate asserts an organizational affiliation between an individual and an organization, then the MaxMD Direct HISP will obtain documentation from the organization that recognizes the affiliation and obligates the organization to provide updates if the affiliation changes.

3.2.3. Authentication of Individual Identity

Direct Certificates require verification of several individuals: 1) A representative of an organization named in a Direct Organizational Certificate, 2) an ISSO of the HISP for each group certificate, 3) a sponsor for each device certificate, and 4) Any individual named in a Direct Address Certificate.

The required validation depends on the level of assurance:

Certificate	Validation
LOA1 Certificates (email certificates) (Equivalent to NIST 800-63/Kantara Level 1 and FBCA CP Rudimentary)	MaxMD Direct HISP uses MaxMD's email validation system to verify the Applicant's control of the email address or website listed in the certificate.
LOA2 Certificates (Equivalent to NIST 800-63 Level 3/Kantara Levels 2 and 3, IGTF Classic/MICS, and FBCA CP Basic)	The applicant must supply his legal name, address, and date of birth. This information is verified using either an in-person or remote vetting process. In-Person Vetting: 1. The applicant provides a valid government-issued photo ID. MaxMD Direct HISP inspects the photo ID and compares the picture to the applicant. 2. MaxMD Direct HISP records the ID number, address, date of birth. 3. MaxMD issues the certificate in a manner that confirms the applicant's ability to receive phone calls or emails using a mechanism associated with the applicant. Remote Vetting: 1. The applicant provides a valid government issued photo ID identifier and a utility or financial account identifier. The applicant must also provide sufficient information to identify and verify the ID or account. 2. MaxMD Direct HISP inspects the ID and account numbers and verifies either the ID or account number through a record check. The check must confirm the name date of birth, address, and other personal information and be sufficient to identify a unique individual. 3. MaxMD issues the certificate in a manner that confirms the applicant's ability to receive phone calls or emails using a mechanism associated with the applicant.

LOA 3 Client Certificates (Equivalent to NIST 800-63/Kantara Level 3 and FBCA CP Medium and Medium Hardware)	The applicant must supply his legal name, address, and date of birth. This information is verified using either an in-person or remote vetting process. In-Person Vetting: 1. The applicant provides a valid government-issued photo ID. MaxMD Direct HISP inspects the photo ID and compares the picture to the applicant. 2. MaxMD Direct HISP records the ID number, address, date of birth and verifies the information through a record check that confirms the information. 3. MaxMD issues the certificate in a manner that confirms the applicant’s ability to receive phone calls or emails using a mechanism associated with the applicant. Remote Vetting: 1. The applicant provides a valid government issued photo ID identifier and a utility or financial account identifier. The applicant must also provide sufficient information to identify and verify the ID or account. 2. MaxMD Direct HISP inspects the ID and account numbers and verifies either the ID or account number through a record check. The check must confirm the name date of birth, address, and other personal information and be sufficient to identify a unique individual. 3. MaxMD issues the certificate in a manner that confirms the applicant’s ability to receive phone calls or emails using a mechanism associated with the applicant.
LOA4 Client Certificates (Equivalent to NIST 800-63/Kantara Level 4 and FBCA CP Medium Hardware)	The applicant must supply his legal name, address, and date of birth. The applicant must also provide a valid government issued photo ID and a second independent government ID or financial account. MaxMD Direct HISP inspects the ID, compares the picture to the applicant, and verifies the ID using record checks. The record checks must confirm the applicant’s name, date of birth, address, and other information. A biometric is recorded. MaxMD issues the credentials in a way that confirms the Applicant’s address.

Acceptable forms of government photo ID include a driver's license, state-issued photo ID card, passport, national identity card, permanent resident card, trusted traveler card, tribal ID, or military ID.

Acceptable forms of non-government ID include a:

1. voided check from a current checking account,
2. recent utility bill showing Applicant’s name, address, and utility account number, or
3. Social security card.

MaxMD Direct HISP may allow other forms of comparable identification. For LOA3 and LOA4, the identity must be verified within 30 days of the certificate's issuance.

For each certificate, the MaxMD RA shall provide MaxMD CA with a Declaration of Identity that includes the following:

1. the identity of the person performing the verification,
2. a signed declaration by the verifying person stating that they verified the identity of the Subscriber as required using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law,
3. a unique identifying number from the verifier's identification,
4. a unique identifying number from the Applicant's identification,
5. the date and time of the verification, and
6. a declaration of identity by the Applicant that is signed in handwriting in the presence of the person performing the verification using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury) or comparable procedure under local law.

MaxMD Direct HISP may rely on in-person or remote identity vetting performed by a trusted agent provided that the trusted agent is authorized to confirm identities on behalf of MaxMD Direct HISP and the trusted agent forwards the information collected directly to MaxMD Direct HISP in a secure manner. A trusted agent is authorized to confirm identities if the agent is a) appointed by the state or federal government to do so; or b) is an agent under direct contract with MaxMD Direct HISP, or c) is a qualified professional with a publicly verifiable credential e.g. Doctor, Lawyer, Accountant; or d) is any existing subscriber with a credential issued at or above the requested LoA their credential is utilized to make the trusted agent attestation. Identification performed by a trusted agent does not relieve MaxMD Direct HISP of its responsibility to verify presented information.

If an Applicant cannot participate in face-to-face registration, a trusted person who already has a certificate of the same type as applied for by the Applicant may represent the Applicant during the validation process. The trusted person must present their certificate and the Applicant's information to the person performing the face-to-face registration.

For Certificates used by patients or on behalf of patient, MaxMD Direct HISP will also collect a representation from the applicant that the digital certificate will only be used for personal healthcare Direct exchange message purposes. MaxMD Direct HISP must verify that the patient's representation.

3.2.3.1. Authentication for Role-based Client Certificates

Role-based certificates identify a specific role that the Subscriber holds, provided that the role identifies a specific individual within an organization (e.g., *Chief Information Officer* is a unique individual whereas *Program Analyst* is not). These role-based certificates are used when non-repudiation is desired. MaxMD Direct HISP may only provide role-based certificates to Subscribers who first obtain an individual Subscriber certificate that is at the same or higher assurance level as the requested role-based certificate. MaxMD Direct HISP may provide certificates with the same role to multiple Subscribers. However, MaxMD Direct HISP requires that each certificate have a unique key pair. Individuals may not share their issued role-based certificates and are required to protect the role-based certificate in the same manner as individual certificates.

MaxMD Direct HISP shall verify the identity of the individual requesting a role-based certificate (i.e. the sponsor) in accordance with Section 3.2.3. MaxMD Direct HISP shall also record the information identified in Section 3.2.3 for a sponsor associated with the role before issuing a role-based certificate. The sponsor must hold an individual certificate in his/her own name issued from MaxMD at the same or higher assurance level as the role-based certificate. If the certificate is a pseudonymous certificate that identifies subjects by their organizational roles, then MaxMD Direct HISP shall verify that the individual either holds that role or has the authority to sign on behalf of the role.

3.2.3.2. Authentication for Group Client Certificates

If there are several entities acting in one capacity and non-repudiation is not necessary, then MaxMD Direct HISP may provide a Group Certificate. A Group Certificate corresponds to a Private Key that is shared by multiple Subscribers. The MaxMD Direct HISP shall record the information identified in Section 3.2.3 for a sponsor from the MaxMD Direct HISP Information Systems Security Office or equivalent before issuing a group certificate.

In addition, MaxMD Direct HISP shall:

1. Require that an Information Systems Security Office, or equivalent, be responsible for ensuring control of the private key, including maintaining a list of Subscribers who have access to the private key, and account for the time period during which each Subscriber had control of the key,
2. Not include a subject Name DN in the certificate that could imply that the subject is a single individual,
3. Require that the sponsor provide and continuously update a list of individuals who hold the shared private key, and
4. Ensure that the procedures for issuing group certificates comply with all other stipulations of the CPS (e.g., key generation, private key protection, and Subscriber obligations).

3.2.3.3. Authentication of Devices with Human Sponsors

MaxMD Direct HISP may issue certificates for use on computing or network devices, provided that the entity owning the device is listed as the subject. In all cases, the device must have a human sponsor who provides:

1. Equipment identification (e.g., serial number) or service name (e.g., DNS name),
2. Equipment public keys,
3. Equipment authorizations and attributes (if any are to be included in the certificate), and
4. Contact information.

If the certificate’s sponsor changes, the new sponsor is required to review the status of each device to ensure it is still authorized to receive certificates. MaxMD Direct HISP must contact each sponsor annually using verified information to ensure that the device is still under the sponsor’s control or responsibility. MaxMD Direct HISP shall contractually obligate all sponsors to notify MaxMD Direct HISP if the equipment is no longer in use or no longer requires a certificate. MaxMD Direct HISP shall verify each registration in accordance with the requested certificate type.

3.2.4. Non-verified Subscriber Information

LOA1 Certificates common name information is not verified. All other certificate information is verified.

3.2.5. Validation of Authority

MaxMD Direct HISP shall verify the authority of the individual requesting a certificate on behalf of an organization as follows:

Certificate	Verification
SSL Server and Federated Device Certificates	MaxMD Direct HISP shall independently verify that the individual is affiliated with the requesting Organization to verify the authority of the certificate requester.
Object Signing Certificates	MaxMD Direct HISP shall confirm the contact information and authority of the certificate requester with an authoritative source within the organization (e.g. corporate, legal, IT, HR, or other appropriate organizational sources) using a reliable means of communication; and MaxMD Direct HISP shall then use that information to contact the certificate requester to verify the authenticity of the request.
LOA1 Client Certificates	MaxMD Direct HISP shall use MaxMD's email validation system.
LOA2 Client Certificates	MaxMD Direct HISP shall verify that the requester is authorized by the organization to obtain a certificate. The organization must be contractually obligated to request revocation of the certificate if the authorization ends. Email addresses in certificates are validated using MaxMD's email validation system.

3.3. IDENTIFICATION AND AUTHENTICATION FOR RE-KEY REQUESTS

3.3.1. Identification and Authentication for Routine Re-key

Subscribers may request automatic re-key of a certificate prior to a certificate's expiration. Re-keyed certificates have the same certificate contents except for a new Public Key and, optionally, an extended validity period.

Subscribers re-establish their identity as follows:

Certificate	Routine Re-Key Authentication	Re-Verification Required
SSL Server Certificates	Username and password	At least every six years
Code Signing Certificates	Username and password	At least every six years
LOA1 Client Certificates	Username and password	At least every nine years
LOA2 Client Certificates	Shared secret (PIN/password) meeting NIST 800-63 Level 2 entropy requirements (Table A.2)	At least every nine years
LOA3 and LOA4 Client Certificates	Current signature key	At least every nine years

Subscribers may not re-key a certificate without additional authentication if doing so would allow the Subscriber to use the certificate beyond the limits described above.

3.3.2. Identification and Authentication for Re-key After Revocation

MaxMD will not rekey a certificate if it was revoked for any reason other than a renewal or update action. MaxMD Direct HISP must re-verify these Subscribers using the initial registration process.

3.4. IDENTIFICATION AND AUTHENTICATION FOR REVOCATION REQUEST

MaxMD Direct HISP must authenticate all revocation requests. MaxMD Direct HISP may authenticate revocation requests using the Certificate's Public Key, even if the associated Private Key is compromised.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1. CERTIFICATE APPLICATION

4.1.1. Who Can Submit a Certificate Application

MaxMD Direct HISP may accept a certificate application from either the Applicant or an individual authorized to request certificates on behalf of the Applicant. For certificates that include a domain name, the Domain Name Registrar record maintained by the domain registrar presumptively indicates who has authority over the domain. If a certificate request is submitted by an agent of the domain owner, the agent must also submit a document that authorizes Subscriber's use of the domain.

MaxMD Direct HISP may not provide certificates to an entity that is on a government denied list maintained by the United States or that is located in a country with which the laws of the United States prohibit doing business.

4.1.2. Enrollment Process and Responsibilities

MaxMD Direct HISP shall require each Applicant to approve a certificate request with relative application information prior to requesting issuance of the certificate. MaxMD Direct HISP must implement a system that protects all communication from an Applicant from modification.

4.2. CERTIFICATE APPLICATION PROCESSING

4.2.1. Performing Identification and Authentication Functions

After initiating a certificate application, MaxMD Direct HISP shall verify the applicant in accordance with Section 3.2. After verification is complete, MaxMD Direct HISP must evaluate the corpus of information and decides whether or not to issue the certificate.

MaxMD Direct HISP shall ensure that all communication between MaxMD RA and MaxMD CA regarding certificate issuance or changes in the status of a certificate are made using secure and auditable methods. MaxMD Direct HISP shall protect all sensitive information obtained from the Applicant and securely exchange this information with MaxMD in a confidential and tamper-evident manner that is protected from unauthorized access. MaxMD Direct HISP must track the exchange using an auditable chain of custody.

4.2.2. Approval or Rejection of Certificate Applications

MaxMD Direct HISP shall reject any certificate application that MaxMD Direct HISP cannot verify. MaxMD Direct HISP shall also not initiate a certificate application if MaxMD Direct HISP reasonably believes that issuing the certificate could damage or diminish MaxMD's reputation or business.

If some or all of the documentation used to support the application is in a language other than English, an MaxMD Direct HISP employee skilled in such language and having the appropriate training, experience, and judgment in confirming organizational identification and authorization performs the final cross-correlation and due diligence. MaxMD Direct HISP may also rely on a translation of the relevant portions of the documentation by a qualified translator.

If the certificate application is not rejected and is successfully validated, MaxMD Direct HISP will approve the certificate application, upload all of the information used to verify the applicant to a server controlled by MaxMD, and issue the certificate. Rejected Applicants may re-apply. MaxMD Direct HISP shall contractually obligate Subscribers to check the data listed in the certificate for accuracy prior to using the certificate.

4.2.3. Time to Process Certificate Applications

MaxMD Direct HISP shall confirm certificate application information and requests issuance of the digital certificate within a reasonable time frame, usually within two days after receiving all necessary details and documents from the Applicant.   For LOA3 and LOA4 Certificates, MaxMD Direct HISP must ensure that the Applicant's identity was verified within 30 days of the initial issuance.

4.3. CERTIFICATE ISSUANCE

4.3.1. Actions during Certificate Issuance

MaxMD Direct HISP shall verify the source of a certificate request and the identity of the Applicant in a secure manner prior to issuing a certificate.

4.3.2. Notification to Subscriber of Issuance of Certificate

MaxMD Direct HISP may deliver certificates in any secure manner within a reasonable time after issuance.

4.4. CERTIFICATE ACCEPTANCE

4.4.1. Conduct Constituting Certificate Acceptance

Certificates are considered accepted on the earlier of (i) the Subscriber's use of the certificate or (ii) 30 days after the certificate's issuance.

4.4.2. Publication of the Certificate

End-entity certificates are published by delivering them to the HISP with notification to the Subscriber.

4.4.3. Notification of Certificate Issuance to Other Entities

No stipulation.

4.5. KEY PAIR AND CERTIFICATE USAGE

4.5.1. Subscriber Private Key and Certificate Usage

Each party with access to the Private Key must be contractually obligated to protect the Private Key from unauthorized use or disclosure, discontinue using a Private Key after expiration or revocation of the associated certificate, and use Private Keys only as specified in the key usage extension.

4.5.2. Relying Party Public Key and Certificate Usage

No stipulation.

4.6. CERTIFICATE RENEWAL

4.6.1. Circumstance for Certificate Renewal

MaxMD Direct HISP may authorize the renewal of a certificate if:

1. the associated public key has not reached the end of its validity period,
2. the Subscriber name and attributes are unchanged,
3. the associated private key remains un compromised, and
4. Re-verification of the Subscriber’s identity is not required under Section 3.3.1.

MaxMD Direct HISP shall make reasonable efforts to notify Subscribers via email of the imminent expiration of a digital certificate and may begin providing notice of pending expiration 60 days prior to the expiration date.

4.6.2. Who May Request Renewal

Only an authorized representative of a Subscriber may request renewal of the Subscriber’s certificates.

4.6.3. Processing Certificate Renewal Requests

Renewal application requirements and procedures are the same as those used during the certificate’s original issuance. MaxMD Direct HISP may not renew a certificate if it cannot verify any rechecked information. MaxMD Direct HISP may reuse identity vetting if location and Domain Name Registrar information have not changed. If the Subscriber's contact information and Private Key have not changed, the HISP may use the Subscriber’s same CSR as was used for the previous certificate.

4.6.4. Notification of New Certificate Issuance to Subscriber

MaxMD Direct HISP shall notify Subscribers of renewed certificates in a secure fashion.

4.6.5. Conduct Constituting Acceptance of a Renewal Certificate

Renewed certificates are considered accepted on the earlier of (i) the Subscriber’s use of the certificate or (ii) 30 days after the certificate’s renewal.

4.6.6. Publication of the Renewal Certificate

Renewed certificates are published by delivering the certificate to the HISP on behalf of the Subscriber.

4.6.7. Notification of Certificate Issuance to Other Entities

No stipulation.

4.7. CERTIFICATE RE-KEY

4.7.1. Circumstance for Certificate Rekey

Re-keying a certificate consists of creating a new certificate with a new public key and serial number while keeping the subject information the same. The new certificate may have a different validity period, key identifiers, CLR and OCSP distributions, and a different signing key. After re-keying a certificate, MaxMD Direct HISP may revoke the old certificate but may not further re-key, renew, or modify the old certificate.

4.7.2. Who May Request Certificate Rekey

The certificate subject may request certificate rekey.

4.7.3. Processing Certificate Rekey Requests

If the Subscriber's other contact information and Private Key have not changed, the request may use the previously provided CSR for that Subscriber. Otherwise, the HISP must submit a new CSR for the Subscriber. MaxMD Direct HISP may re-use existing verification information unless re-verification is required under section 3.3.1 or MaxMD Direct HISP believes that the information has become inaccurate.

4.7.4. Notification of Certificate Rekey to Subscriber

MaxMD Direct HISP shall notify the Subscriber within a reasonable time after the certificate issues.

4.7.5. Conduct Constituting Acceptance of a Rekeyed Certificate

Issued certificates are considered accepted on the earlier of (i) the Subscriber’s use of the certificate or (ii) 30 days after the certificate is rekeyed.

4.7.6. Publication of the Issued Certificate

Rekeyed certificates are published by delivering them to the HISP on behalf of the Subscribers.

4.7.7. Notification of Certificate Issuance to Other Entities

No stipulation.

4.8. CERTIFICATE MODIFICATION

Modifying a certificate means creating a new certificate for the same subject with authenticated information that differs slightly from the old certificate (e.g., changes to email address or non-essential parts of names or attributes). The new certificate may have the same or a different subject public key.

After modifying a certificate, MaxMD Direct HISP may revoke the old certificate but cannot further re-key, renew, or modify the old certificate.

4.8.1. Who May Request Certificate Modification

MaxMD Direct HISP or a Subscriber may request modification of a certificate.

4.8.2. Processing Certificate Modification Requests

Prior to requesting certificate modification, MaxMD Direct HISP shall verify any information that will change. MaxMD Direct HISP shall not request a modified certificate that has a validity period that exceeds the applicable time limits found in section 3.3.1 or 6.3.2.

4.8.3. Notification of Certificate Modification to Subscriber

MaxMD Direct HISP shall notify the Subscriber within a reasonable time after the modified certificate issues.

4.8.4. Conduct Constituting Acceptance of a Modified Certificate

Issued certificates are considered accepted on the earlier of (i) the Subscriber’s use of the certificate or (ii) 30 days after the certificate is rekeyed.

4.8.5. Publication of the Modified Certificate

Modified certificates are published by delivering them to the HISP on behalf of Subscribers.

4.8.6. Notification of Certificate Modification to Other Entities

No stipulation.

4.9. CERTIFICATE REVOCATION AND SUSPENSION

4.9.1. Circumstances for Revocation

Revocation of a certificate permanently ends the operational period of the certificate prior to the certificate reaching the end of its stated validity period. Prior to revoking a certificate, MaxMD Direct HISP shall verify the identity and authority of the entity requesting revocation. MaxMD Direct HISP must revoke a certificate if any of the following occur:

1. The Subscriber requested revocation of its certificate;
2. The Subscriber did not authorize the original certificate request and did not retroactively grant authorization;
3. Either the Private Key associated with the certificate or the Private Key used to sign the certificate was compromised;
4. The Subscriber or their contracted HISP breached a material obligation under the CP, the CPS, or the relevant Subscriber Agreement;
5. The Subscriber’s or MaxMD Direct HISP ’s obligations under the CP or CPS are delayed or prevented by circumstances beyond the party’s reasonable control, including computer or communication failure, and, as a result, another entity’s information is materially threatened or compromised;
6. The certificate was not issued in accordance with the CP, CPS, or applicable industry standards;
7. MaxMD Direct HISP received a lawful and binding order from a government or regulatory body to revoke the certificate;
8. MaxMD Direct HISP ’s right to manage certificates under applicable industry standards was terminated (unless arrangements have been made to continue revocation services and maintain the CRL/OCSP Repository);
9. A court or arbitrator revoked the Subscriber’s right to use a name or mark listed in the certificate, or the Subscriber failed to maintain a valid registration for such name or mark;
10. Any information appearing in the Certificate was or became inaccurate or misleading;
11. The Subscriber was added as a denied party or prohibited person to a blacklist or is operating from a destination prohibited under the laws of the United States;
12. For code-signing certificates, the certificate was used to sign, publish, or distribute malware, code that is downloaded without user consent, or other harmful content.

MaxMD Direct HISP must also revoke a certificate if the binding between the subject and the subject's public key in the certificate is no longer valid or if an associated Private Key is compromised.

4.9.2. Who Can Request Revocation

The Subscriber or another appropriately authorized party may request revocation of a certificate. MaxMD Direct HISP may require that the revocation request be made by either the organizational contact, billing contact or domain registrant.

MaxMD Direct HISP or MaxMD shall revoke a certificate if it receives sufficient evidence of compromise of loss of the private key. Entities other than the certificate subject may request revocation of a certificate for problems related to fraud, misuse, or compromise by filing a "Certificate Problem Report". All certificate revocation requests must include the identity of the entity requesting revocation and the reason for revocation.

4.9.3. Procedure for Revocation Request

Entities submitting certificate revocation requests must list their identity and explain the reason for requesting revocation. After receiving a revocation request:

1. MaxMD Direct HISP shall log the identity of the entity making the request or problem report and the reason for requesting revocation and submit a copy of the request to MaxMD.
2. If applicable, MaxMD Direct HISP shall confirm the revocation request with a known administrator via out-of-band communication (e.g., telephone, fax, etc.). MaxMD Direct HISP must always revoke the certificate if the request is confirmed as originating from the Subscriber.
3. If the request originated from a third party, then MaxMD Direct HISP shall investigate the report within 24 hours after receipt and decide whether revocation is appropriate based on the following criteria:
   a. the nature of the alleged problem,
   b. the number of complaints/reports received about a particular certificate or website,
   c. the entity making the complaint (for example, complaints from a law enforcement official that a web site is engaged in illegal activities have more weight than a complaint from a consumer alleging they never received the goods they ordered), and
   d. relevant legislation.
4. If revocation is appropriate, MaxMD Direct HISP shall revoke the Certificate.

MaxMD Direct HISP shall maintain a continuous 24/7 ability to internally respond to any high priority complaints and problems. If appropriate, MaxMD Direct HISP may forward complaints to law enforcement.

4.9.4. Revocation Request Grace Period

No stipulation.

4.9.5. Time within which RA Processes the Revocation Request

MaxMD Direct HISP shall process all certificate revocation requests within 8 hours after their receipt.

4.9.6. Revocation Checking Requirement for Relying Parties

No stipulation.

4.9.7. CRL Issuance Frequency

CRLS for MaxMD Direct HISP -provided certificates are issued at least every 24 hours.

4.9.8. Maximum Latency for CRLs

No stipulation.

4.9.9. On-line Revocation/Status Checking Availability

No stipulation.

4.9.10. On-line Revocation Checking Requirements

No stipulation.

4.9.11. Other Forms of Revocation Advertisements Available

No stipulation.

4.9.12. Special Requirements Related to Key Compromise

No stipulation.

4.9.13. Circumstances for Suspension

Not applicable.

4.9.14. Who Can Request Suspension

Not applicable.

4.9.15. Procedure for Suspension Request

Not applicable.

4.9.16. Limits on Suspension Period

Not applicable.

4.10. CERTIFICATE STATUS SERVICES

4.10.1. Operational Characteristics

Certificate status information is available via CRL and OCSP responder.

4.10.2. Service Availability

Certificate status services are available 24x7 without interruption.

4.10.3. Optional Features

OCSP Responders may not be available for all certificate types.

4.11. END OF SUBSCRIPTION

A Subscriber’s subscription service ends if its certificate expires or is revoked or if the applicable Subscriber Agreement expires without renewal.

4.12. KEY ESCROW AND RECOVERY

MaxMD Direct HISP does not escrow Subscriber key management keys.

4.12.1. Session Key Encapsulation and Recovery Policy and Practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1. PHYSICAL CONTROLS

5.1.1. Site Location and Construction

MaxMD Direct HISP shall implement a security policy that is designed to detect, deter, and prevent unauthorized access to MaxMD Direct HISP's operations.

5.1.2. Physical Access

MaxMD Direct HISP shall protect its equipment from unauthorized access and implements physical controls to reduce the risk of equipment tampering.

5.1.3. Power and Air Conditioning

No stipulation.

5.1.4. Water Exposures

No stipulation.

5.1.5. Fire Prevention and Protection

No stipulation.

5.1.6. Media Storage

MaxMD Direct HISP shall protect its media from accidental damage and unauthorized physical access.

5.1.7. Waste Disposal

MaxMD Direct HISP shall shred and destroy all outdated or unnecessary copies of printed sensitive information before disposal. MaxMD Direct HISP shall zeroize all electronic media used in the RA operations using programs that meet the U.S. Department of Defense requirements.

5.2. PROCEDURAL CONTROLS

5.2.1. Trusted Roles

Personnel acting in trusted roles include MaxMD Direct HISP's system administration personnel and personnel involved with identity vetting and the issuance and revocation of certificates. MaxMD Direct HISP shall distribute the functions and duties performed by persons in trusted roles so that one person alone cannot circumvent security measures or subvert the security and trustworthiness of the PKI operations. MaxMD Direct HISP shall ensure that all personnel in trusted roles are free from conflicts of interest that might prejudice the impartiality of MaxMD Direct HISP's operations. MaxMD Direct HISP shall maintain a list of personnel appointed to trusted roles and review this list annually.

5.2.2. Number of Persons Required per Task

No stipulation.

5.2.3. Identification and Authentication for each Role

MaxMD Direct HISP shall require all personnel to authenticate themselves to MaxMD Direct HISP's systems before they are allowed access to the system.

5.2.4. Roles Requiring Separation of Duties

Roles requiring a separation of duties include:

1. The verification of information in certificate applications,

2. The approval of certificate applications, and
3. The approval of revocation requests.

5.3. PERSONNEL CONTROLS

5.3.1. Qualifications, Experience, and Clearance Requirements

MaxMD Direct HISP’s practices shall provide reasonable assurance of the trustworthiness and competence of its employees and of the satisfactory performance of their duties. For Level 3 and Level 4 certificates, an individual performing a trusted role MaxMD Direct HISP must be citizens of the United States.

5.3.2. Background Check Procedures

MaxMD Direct HISP shall verify the identity of each person appointed to a trusted role and perform a background check prior to allowing the person to act in a trusted role. MaxMD Direct HISP shall require each individual to appear in-person before a human resources employee whose responsibility it is to verify identity. The human resources employee shall verify the individual’s identity using the required forms of government-issued photo identification (e.g., passports and/or driver’s licenses reviewed pursuant to U.S. Citizenship and Immigration Services Form I-9, Employment Eligibility Verification, or comparable procedure for the jurisdiction in which the individual’s identity is being verified). Background checks must include employment history, education, character references, social security number, previous residences, driving records and criminal background. Background investigations are performed by a competent independent party that has the authority to perform background investigations. MaxMD Direct HISP shall perform checks of previous residences are over the past three years. All other checks are for the previous five years. MaxMD Direct HISP shall verify the highest education degree obtained regardless of the date awarded. MaxMD Direct HISP shall refresh Background checks at least every ten years.

5.3.3. Training Requirements

MaxMD Direct HISP shall provide skills training to all personnel involved in PKI operations. The training relates to the person’s job functions and covers:

1. basic Public Key Infrastructure (PKI) knowledge,
2. software versions used by MaxMD Direct HISP ,
3. authentication and verification policies and procedures,
4. disaster recovery and business continuity procedures,
5. common threats to the validation process, including phishing and other social engineering tactics, and
6. Applicable industry and government guidelines.

MaxMD Direct HISP shall maintain records of who received training and what level of training was completed. MaxMD Direct HISP shall provide these records to MaxMD upon request. Validation personnel must have the minimum skills necessary to satisfactorily perform validation duties before being granted validation privileges.

5.3.4. Retraining Frequency and Requirements

Personnel must maintain skill levels that are consistent with industry-relevant training and performance programs in order to continue acting in trusted roles. MaxMD Direct HISP shall make all individuals acting in trusted roles aware of any changes to MaxMD Direct HISP’s operations. If MaxMD Direct HISP ’s operations change, MaxMD Direct HISP must provide documented training to all personnel acting in trusted roles.

5.3.5. Job Rotation Frequency and Sequence

No stipulation.

5.3.6. Sanctions for Unauthorized Actions

MaxMD Direct HISP shall make any employee or agent that fails to comply with this RPS or the MaxMD CPS subject to administrative or disciplinary actions, including termination of employment or agency and criminal sanctions. If a person in a trusted role is cited by MaxMD or MaxMD Direct HISP for unauthorized or inappropriate actions, MaxMD Direct HISP must immediately remove that person from the trusted role pending review.

5.3.7. Independent Contractor Requirements

MaxMD Direct HISP shall make its independent contractors who are assigned to perform trusted roles subject to the duties and requirements specified for such roles in this Section 5.3 and subject to the sanctions stated in Section 5.3.6.

5.3.8. Documentation Supplied to Personnel

MaxMD Direct HISP shall provide personnel in trusted roles the documentation necessary to perform their duties, including a copy of this RPS.

5.4. AUDIT LOGGING PROCEDURES

5.4.1. Types of Events Recorded

MaxMD Direct HISP's systems shall require identification and authentication at system logon using a unique user name and password. MaxMD Direct HISP shall enable all essential event auditing capabilities of its operations in order to record the events listed below. If an application cannot automatically record an event, MaxMD Direct HISP shall use a manual procedure to satisfy these requirements. For each event, MaxMD Direct HISP shall record the relevant (i) date and time, (ii) type of event, (iii) success or failure, and (iv) user or system that caused the event or initiated the action. MaxMD Direct HISP shall make these event records available to MaxMD and MaxMD's auditors as proof of MaxMD Direct HISP's practices.

Auditable Event
SECURITY AUDIT
Any changes to the audit parameters, e.g., audit frequency, type of event audited
Any attempt to delete or modify the audit logs
AUTHENTICATION TO SYSTEMS
Successful and unsuccessful attempts to assume a role
The value of maximum number of authentication attempts is changed
Maximum number of authentication attempts occur during user login
An administrator unlocks an account that has been locked as a result of unsuccessful authentication attempts
An administrator changes the type of authenticator, e.g., from a password to a biometric
LOCAL DATA ENTRY
All security-relevant data that is entered in the system
REMOTE DATA ENTRY
All security-relevant messages that are received by remote access to the RA systems
DATA EXPORT AND OUTPUT
All successful and unsuccessful requests for confidential and security-relevant information
SECRET KEY STORAGE

Auditable Event
The manual entry of secret keys used for authentication
CERTIFICATE REGISTRATION
All certificate requests, including issuance, re-key, renewal, and revocation
Verification activities
CERTIFICATE REVOCATION
All certificate revocation requests
CERTIFICATE STATUS CHANGE APPROVAL AND REJECTION
ACCOUNT ADMINISTRATION
Roles and users are added or deleted
The access control privileges of a user account or a role are modified
CERTIFICATE PROFILE MANAGEMENT
All changes to the certificate profile
MISCELLANEOUS
Appointment of an individual to a Trusted Role
Designation of personnel for multiparty control
Installation of an Operating System
Installation of a PKI Application
System Startup
Logon attempts to PKI Application
Receipt of hardware / software
Attempts to set passwords
Attempts to modify passwords
File manipulation (e.g., creation, renaming, moving)
All certificate compromise notification requests
CONFIGURATION CHANGES
Hardware
Software
Operating System
Patches
Security Profiles
PHYSICAL ACCESS / SITE SECURITY
Known or suspected violations of physical security
Firewall and router activities
ANOMALIES
System crashes and hardware failures
Software error conditions
Software check integrity failures
Receipt of improper messages and misrouted messages
Network attacks (suspected or confirmed)
Equipment failure
Electrical power outages
Uninterruptible Power Supply (UPS) failure
Obvious and significant network service or access failures
Violations of the CPS or RPS
Resetting Operating System clock

5.4.2. Frequency of Processing Log

MaxMD Direct HISP shall periodically review the logs generated by MaxMD Direct HISP ’s systems, make system and file integrity checks, and conduct a vulnerability assessment. During these checks, MaxMD Direct HISP shall (1) check whether anyone has tampered with the log, (2) scan for anomalies or specific conditions, including any evidence of malicious activity, and (3) prepare a written summary of the review. MaxMD Direct HISP shall investigate any anomalies or irregularities found in the logs. MaxMD Direct HISP shall make these logs available to MaxMD upon request.

5.4.3. Retention Period for Audit Log

MaxMD Direct HISP shall retain audit logs on-site until after they are reviewed.

5.4.4. Protection of Audit Log

MaxMD Direct HISP personnel are required to keep all generated audit log information on their equipment until after it is copied by an MaxMD Direct HISP system administrator. MaxMD Direct HISP shall configure its systems to ensure that (i) only authorized people have read access to logs, (ii) only authorized people may archive audit logs, and (iii) audit logs are not modified. Audit logs are protected from destruction prior to the end of the audit log retention period.

5.4.5. Audit Log Backup Procedures

MaxMD Direct HISP shall make backup copies of its audit logs on a monthly basis.

5.4.6. Audit Collection System (internal vs. external)

Automatic audit processes must begin on system startup and end at system shutdown. MaxMD Direct HISP shall promptly notify MaxMD if the integrity of the system or confidentiality of the information protected by a system is at risk.

5.4.7. Notification to Event-causing Subject

No stipulation.

5.4.8. Vulnerability Assessments

MaxMD Direct HISP shall perform routine risk assessments that identify and assess reasonably foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of its RA systems. MaxMD Direct HISP shall routinely assess the sufficiency of its risk control policies, procedures, information systems, technology, and other arrangements.

5.5. RECORDS ARCHIVAL

MaxMD Direct HISP shall comply with all record retention policies that apply by law. MaxMD Direct HISP shall include sufficient detail in all archived records to show that a certificate was issued in accordance with the CPS.

5.5.1. Types of Records Archived

MaxMD Direct HISP shall retain the following information in its archives:

1. RPS versions,
2. Contractual obligations and other agreements regarding certificates,
3. System and equipment configurations, modifications, and updates,
4. Certificate and revocation requests,
5. Identity authentication data,
6. Any documentation related to the receipt or acceptance of a certificate or token,
7. Subscriber Agreements,
8. A record of certificate re-keys,
9. Any data or applications necessary to verify an archive’s contents,
10. Any changes to MaxMD Direct HISP ’s audit parameters,
11. Any attempt to delete or modify audit logs,
12. Access to Private Keys for key recovery purposes,
13. Export of Private Keys,
14. Approval or rejection of a certificate status change request,

15. Appointment of an individual to a trusted role,
16. Certificate compromise notifications,
17. Remedial action taken as a result of violations of physical security, and
18. Violations of the RPS or the CPS.

5.5.2. Retention Period for Archive

MaxMD Direct HISP shall retain archived data for at seven years & 6 months.

5.5.3. Protection of Archive

MaxMD Direct HISP shall store archive records in a manner that prevents unauthorized modification, substitution, or destruction. MaxMD Direct HISP shall maintain any software application required to process the archive data until the data is either destroyed or transferred to a newer medium.

If MaxMD Direct HISP needs to transfer any media to a different archive site or equipment, MaxMD Direct HISP shall maintain both archived locations and/or pieces of equipment until the transfer are complete. All transfers to new archives must occur in a secure manner.

5.5.4. Archive Backup Procedures

MaxMD Direct HISP shall create an archive disk of the data listed in section 5.5.1 annually and stores it in a secure location for the duration of the 7.5-year retention period.

5.5.5. Requirements for Time-stamping of Records

MaxMD Direct HISP shall automatically time-stamp archived records with system time (non-cryptographic method) as they are created. MaxMD Direct HISP shall synchronize its system time at least every eight hours using a real time value distributed by a recognized UTC(k) laboratory or National Measurement Institute.

MaxMD Direct HISP shall stamp and record information collected during the identity verification process, including IP addresses associated with applicant submissions and screen shots provided by verification information sources where applicable.

5.5.6. Archive Collection System (internal or external)

No stipulation.

5.5.7. Procedures to Obtain and Verify Archive Information

No stipulation.

5.6. KEY CHANGEOVER

Not applicable.

5.7. COMPROMISE AND DISASTER RECOVERY

5.7.1. Incident and Compromise Handling Procedures

MaxMD Direct HISP shall promptly notify MaxMD if a disaster causes MaxMD Direct HISP’s operations to become inoperative.

5.7.2. Computing Resources, Software, and/or Data Are Corrupted

MaxMD Direct HISP shall reestablish operations as quickly as possible after a disaster or data corruption.

5.7.3. Entity Private Key Compromise Procedures

Not applicable.

5.7.4. Business Continuity Capabilities after a Disaster

MaxMD Direct HISP shall implement data backup and recovery procedures. MaxMD Direct HISP shall develop a Business Continuity Management Program (BCMP) that provides for the resestablishment of capabilities as quickly as possible. This plan is reviewed, and updated annually.

5.8. RA TERMINATION

Before terminating its RA activities, MaxMD Direct HISP shall:

1. Provide notice and information about the termination by sending notice by email to its customers and by posting such information on MaxMD Direct HISP ’s web site; and
2. Transfer all certificate responsibilities to MaxMD.

6. TECHNICAL SECURITY CONTROLS

6.1. KEY PAIR GENERATION AND INSTALLATION

6.1.1. Key Pair Generation

Subscriber public keys must be generated in a secure manner that is appropriate for the certificate type.

6.1.2. Private Key Delivery to Subscriber

If MaxMD Direct HISP generates a key for a Subscriber, then it must protect the Private Key with a FIPS 140 Level-2 HSM or equivalent process and must securely notify the Subscriber of such. MaxMD Direct HISP may protect keys electronically or on a hardware cryptographic module / SSCD. In all cases:

1. MaxMD Direct HISP may only retain a copy of the Subscriber’s Private Key when authorized by the Subscriber,
2. MaxMD Direct HISP must protect the private key from activation, compromise, or modification during its entire life cycle,
3. The Subscriber must acknowledge generation of the private key(s), and
4. MaxMD Direct HISP must control the Private Key in a way that ensures that the correct tokens and activation data are provided to the correct Subscribers, including:
    a. For hardware modules, maintaining accountability for the location and state of the module until the Subscriber accepts possession of it and
    b. For electronic activation of private keys, encrypting key material using a cryptographic algorithm and key size at least as strong as the private key or an equivalent process. MaxMD Direct HISP will deliver activation data using a separate secure channel.

MaxMD Direct HISP shall maintain a record of the Subscriber’s acknowledgement of receipt of the activation data or the device containing the Subscriber’s Key Pair where applicable. MaxMD Direct HISP provides a copy of this record to MaxMD.

6.1.3. Public Key Delivery to Certificate Issuer

MaxMD Direct HISP generates key pairs on behalf of Subscribers and submits the Public Key to MaxMD in a CSR as part of the certificate request process. The signature on the request is authenticated prior to issuing the certificate.

6.1.4. CA Public Key Delivery to Relying Parties

No stipulation.

6.1.5. Key Sizes

Subscriber keys must be at least 2048 bits for RSA, DSA, or Diffie-Hellman and 224 bits for elliptic curve algorithms, except for certificates issued to smart cards or other hardware devices that are incapable of accepting 2048-bit RSA certificates, then the key length must be at least 1024 bits for RSA and that the certificate expire on or before December 31, 2013. Any certificates expiring after 12/31/2030 must be at least 3072-bit for RSA and 256-bit for ECDSA.

Signatures on all certificates are generated using at least SHA-1. Federated Device Certificates and Levels 3 and 4 (US and CBP) Certificates require the use of the SHA-256 algorithm.

Subscribers may fulfill their requirements using TLS or another protocol that provides similar security, provided the protocol requires at least:

1. AES (128 bits) or equivalent for the symmetric key and at least 2048 bit RSA or equivalent for the asymmetric keys after 12/31/2010, and
2. AES (128 bits) or equivalent for the symmetric key and at least 3072 bit RSA or equivalent for the asymmetric keys after 12/31/2030.

6.1.6. Public Key Parameters Generation and Quality Checking

No stipulation.

6.1.7. Key Usage Purposes (as per X.509 v3 key usage field)

Direct Trust Subscriber public keys that are bound into certificates shall be certified for use in signing and encryption of S/MIME packages as required by the Direct Project specifications. Specifically, Subscriber certificates shall assert the following key usage bits:

- digitalSignature
- keyEncipherment

Subscriber certificates that are dual-use certificates MUST not assert the non-repudiation bit. Subscriber certificates shall also assert an extended key usage bit of emailProtection and a BasicConstraint of CA:FALSE.

A conforming Direct Trust CA root certificate shall assert the following key usage bits:

- cRLSign
- keyCertSign

The CA root certificate shall also assert a Basic Constraint of CA:TRUE.

6.2. PRIVATE KEY PROTECTION AND CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

6.2.1. Cryptographic Module Standards and Controls

Cryptographic module requirements are as follows:

Subscribers must use a FIPS 140 Level 1 hardware or software module.
MaxMD Direct HISP must use a FIPS 140 Level 2 hardware module.

6.2.2. Private Key (n out of m) Multi-person Control

No stipulation.

6.2.3. Private Key Escrow

Subscribers may not escrow their private signature keys or dual use keys.

6.2.4. Private Key Backup

MaxMD Direct HISP will provide backup services for subscriber signature keys. Backup keys are stored with security controls that are consistent with the protection provided by the Subscriber's cryptographic module. Backed up keys can never be stored in a plain text form outside of the cryptographic module.

6.2.5. Private Key Archival

MaxMD Direct HISP may not archive Private Keys for which it is not a party to under a Group profile.

6.2.6. Private Key Transfer into or from a Cryptographic Module

All keys must be generated by and in a cryptographic module.

6.2.7. Private Key Storage on Cryptographic Module

HISP must protect storage of Subscriber private keys using a FIPS 140 Level 2 or equivalent process.

6.2.8. Method of Activating Private Keys

Subscribers are responsible for activating their Private Keys. Subscribers should use a strong password or equivalent authentication method to prevent unauthorized access or use of the Subscriber's Private Key. At a minimum, Subscribers are required to authenticate themselves to the cryptographic module before activating their private keys.

6.2.9. Method of Deactivating Private Keys

No stipulation.

6.2.10. Method of Destroying Private Keys

HISPs shall destroy Subscriber Private Keys when the corresponding certificate is revoked or expired or if the Private Key is no longer needed.

6.2.11. Cryptographic Module Rating

See Section 6.2.1.

6.3. OTHER ASPECTS OF KEY PAIR MANAGEMENT

6.3.1. Public Key Archival

MaxMD archives copies of Public Keys in accordance with Section 5.5.

6.3.2. Certificate Operational Periods and Key Pair Usage Periods

Direct Certificates have maximum validity period of one year. Private keys may be used for six years.

6.4. ACTIVATION DATA

The MaxMD activation process requires secure private key administrator access to the activation server at Rackspace. The activation process requires an additional memorized activation password to sign the subscriber certificate.

.

6.5. COMPUTER SECURITY CONTROLS

6.5.1. Specific Computer Security Technical Requirements

MaxMD Direct HISP shall secure its systems and authenticate and protect communications between its systems and trusted roles. MaxMD Direct HISP's servers and support-and-vetting workstations must run on trustworthy systems that are configured and hardened using industry best practices. MaxMD Direct HISP shall scan all systems for malicious code and protected against spyware and viruses.

MaxMD Direct HISP's systems, including any remote workstations, must be configured to:

1. authenticate the identity of users before permitting access to the system or applications,
2. manage the privileges of users and limit users to their assigned roles,
3. generate and archive audit records for all transactions,
4. enforce domain integrity boundaries for security critical processes, and
5. support recovery from key or system failure.

6.5.2. Computer Security Rating

No stipulation.

6.6. LIFE CYCLE TECHNICAL CONTROLS

6.6.1. System Development Controls

MaxMD Direct HISP shall control and monitor the acquisition and development of its RA systems. MaxMD Direct HISP shall only install software on RA systems that is necessary to MaxMD Direct HISP 's operation.

MaxMD Direct HISP shall select vendors based on their reputation in the market, ability to deliver quality product, and likelihood of remaining viable in the future. MaxMD Direct HISP shall have all hardware and software shipped under standard conditions to ensure delivery of the component only to a trusted MaxMD Direct HISP employee who installs the equipment without opportunity for tampering.

Software developed in-house or by consultants using standard software development methodologies were developed using a formal, documented, development methodology in a controlled environment. Quality assurance is maintained throughout the process through testing and documentation or by purchasing from trusted vendors as discussed above.

MaxMD Direct HISP shall scan all hardware and software essential to MaxMD Direct HISP's operations for malicious code on first use and periodically thereafter.

6.6.2. Security Management Controls

MaxMD Direct HISP has mechanisms in place to control and monitor the security-related configurations of its RA systems, including change control data entries that are processed, logged and tracked for any security-related changes. When loading software onto a RA system, MaxMD Direct HISP verifies that the software is the correct version and is supplied by the vendor free of any modifications.

6.6.3. Life Cycle Security Controls

No stipulation.

6.7. NETWORK SECURITY CONTROLS

MaxMD Direct HISP shall document and control the configuration of its systems, including any upgrades or modifications made. MaxMD Direct HISP shall protect its systems with firewall(s) and shall only use internal IP addresses. MaxMD Direct HISP shall configure its firewalls and boundary control devices to allow access only by the addresses, ports, protocols and commands required for the trustworthy provision of its RA services.

MaxMD Direct HISP shall block all ports and protocols and open only necessary ports to enable RA functions. All RA equipment is configured with a minimum number of services and all unused network ports and services are disabled. MaxMD Direct HISP shall allow MaxMD to review MaxMD Direct HISP ’s network configuration upon request.

6.8. TIME-STAMPING

The system time on computers operating the RA process must be updated using the Network Time Protocol (NTP) to synchronize system clocks at least once every eight hours (Windows default). All times are traceable to the real time value distributed by a UTC (k) laboratory or National Measurement Institute and are updated when a leap second occurs as notified by the appropriate body.

7. CERTIFICATE, CRL, AND OCSP PROFILES

No stipulation.

7.1. CERTIFICATE PROFILE

7.1.1. Version Number(s)

All certificates are X.509 version 3 certificates.

7.1.2. Certificate Extensions

See MaxMD’s Certificate Profiles document.

7.1.3. Algorithm Object Identifiers

End Entity Certificates signed by a conforming Direct Trust CA shall use the SHA-256 signature algorithm and identify it using the following OID: sha256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

Certificates issued by a conforming Direct Trust CA shall use the following OID for identifying the subject public key algorithm: rsaEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1}

7.1.4. Name Forms

Each certificate includes a unique serial number that is never reused.

7.1.5. Name Constraints

No stipulation.

7.1.6. Certificate Policy Object Identifier

The OIDs used by MaxMD Direct HISP are set forth in MaxMD's Certificate Profiles document.

7.1.7. Usage of Policy Constraints Extension

Not applicable.

7.1.8. Policy Qualifiers Syntax and Semantics

Certificates may include a brief statement about the limitations of liability and other terms associated with the use of a certificate in the Policy Qualifier field of the Certificates Policy extension.

7.1.9. Processing Semantics for the Critical Certificate Policies Extension

No stipulation.

7.2. CRL PROFILE

7.2.1. Version number(s)

CRLs are version 2 and conform to RFC 3290/5280. CRLs contain the following fields:

Field	Value
Issuer Signature Algorithm	sha-1WithRSAEncryption [1 2 840 113549 1 1 5] OR sha-256WithRSAEncryption [1 2 840 113549 1 1 11] OR ecdsa-with-sha284 [1 2 840 10045 4 3]
Issuer Distinguished Name	MaxMD
this Update	CRL issue date in UTC format
next Update	Date when the next CRL will issue in UTC format. The field is set to this Update plus 24 hours
Revoked Certificates List	List of revoked certificates, including the serial number and revocation date
Issuer's Signature	[Signature]

7.2.2. CRL and CRL Entry Extensions

CRLs have the following extensions:

Extension	Value
CRL Number	Never repeated monotonically increasing integer
Authority Key Identifier	Same as the Authority Key Identifier listed in the certificate
Invalidity Date	Optional date in UTC format
Reason Code	Optionally included reason for the revocation

7.3. OCSP PROFILE

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1. FREQUENCY OR CIRCUMSTANCES OF ASSESSMENT

MaxMD electronically audits MaxMD Direct HISP's issuance systems and procedures. MaxMD may audit MaxMD Direct HISP's compliance with the CPS at any time.

8.2. IDENTITY/QUALIFICATIONS OF ASSESSOR

MaxMD personnel are responsible for auditing MaxMD Direct HISP’s compliance with this RPS.

8.3. ASSESSOR'S RELATIONSHIP TO ASSESSED ENTITY

MaxMD Direct HISP is a RA of MaxMD CA.

8.4. TOPICS COVERED BY ASSESSMENT

The audit covers MaxMD Direct HISP ’s systems and validation process.

8.5. ACTIONS TAKEN AS A RESULT OF DEFICIENCY

If an audit reports any material noncompliance with applicable law, this RPS, the CPS, the CP, or any other contractual obligations related to MaxMD Direct HISP ’s services (to the extent such information is audited), then (1) MaxMD will document the discrepancy, (2) MaxMD will promptly notify MaxMD Direct HISP , and (3) MaxMD Direct HISP will develop a plan to cure the noncompliance.

8.6. COMMUNICATION OF RESULTS

No stipulation.

8.7. SELF-AUDITS

MaxMD Direct HISP shall perform regular internal audits to ensure compliance with this RPS.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1. FEES

No stipulation.

9.2. FINANCIAL RESPONSIBILITY

No stipulation.

9.3. CONFIDENTIALITY OF BUSINESS INFORMATION

9.3.1. Scope of Confidential Information

MaxMD Direct HISP shall protect the following as confidential information using a reasonable degree of care:

1. Private Keys;
2. Activation data used to access to MaxMD Direct HISP ’s systems;
3. Business continuity, incident response, contingency, and disaster recovery plans;
4. Other security practices used to protect the confidentiality, integrity, or availability of information;
5. Information held by MaxMD Direct HISP as private information in accordance with Section 9.4;
6. Audit logs and archive records; and
7. Transaction records, financial audit records, and external or internal audit trail records and any audit reports.

9.3.2. Information Not Within the Scope of Confidential Information

Information not listed as confidential is considered public information. Published certificate and revocation data is considered public information.

9.3.3. Responsibility to Protect Confidential Information

MaxMD Direct HISP shall contractually obligate its employees, agents, and contractors to protect confidential information. MaxMD Direct HISP shall ensure that employees receive training on how to handle confidential information.

9.4. PRIVACY OF PERSONAL INFORMATION

9.4.1. Privacy Plan

MaxMD Direct HISP follows the privacy policy posted on its website when handling personal information. Personal information is only disclosed when required by law or when requested by the subject of the personal information. MaxMD Direct HISP will disclose information related to the issuance or use of a certificate to MaxMD upon request.

9.4.2. Information Treated as Private

MaxMD Direct HISP shall treat all personal information about an individual that is not publicly available in the contents of a certificate or CRL as private information. MaxMD Direct HISP shall protect private information using appropriate safeguards and a reasonable degree of care.

9.4.3. Information Not Deemed Private

Private information does not include certificates, CRLs, or their contents.

9.4.4. Responsibility to Protect Private Information

MaxMD Direct HISP employees and contractors shall handle personal information in strict confidence and shall meet the requirements of US and European law concerning the protection of personal data. All sensitive information is securely stored and protected against accidental disclosure.

9.4.5. Notice and Consent to Use Private Information

Personal information provided during the application or identity verification process is considered private information provided that the information is not included in a Certificate. MaxMD Direct HISP shall only use private information after obtaining the subject's express written consent or as required by applicable law or regulation. All Subscribers must consent to the global transfer and publication of any personal data contained in a certificate.

9.4.6. Disclosure Pursuant to Judicial or Administrative Process

MaxMD Direct HISP may disclose private information, without notice, when required to do so by law or regulation.

9.4.7. Other Information Disclosure Circumstances

No stipulation.

9.5. INTELLECTUAL PROPERTY RIGHTS

Certificate and revocation information are the exclusive property of MaxMD. MaxMD does not allow derivative works of its certificates or products without prior written permission. Private and Public Keys remain the joint property of the HISP and the Subscribers who rightfully control them. All secret shares (distributed elements) of the MaxMD Private Keys are the property of MaxMD.

9.6. REPRESENTATIONS AND WARRANTIES

9.6.1. CA Representations and Warranties

MaxMD's offers the warranties described in its CPS. Further, MaxMD as CA shall notify the RA if the CA becomes aware of any changes of information that may affect the status of the certificate.

9.6.2. RA Representations and Warranties

RA represents that:

1. MaxMD Direct HISP 's certificate issuance and management services conform to the MaxMD CP and CPS,
2. Information provided by RA does not contain any false or misleading information,
3. Translations performed by RA are an accurate translation of the original information, and
4. All certificates requested by RA meet the requirements of the MaxMD CPS.
5. RA shall notify CA of any changes that may affect the status of the certificate issued on the basis of the RA's identity verification activity

9.6.3. Subscriber Representations and Warranties

MaxMD Direct HISP shall make Subscribers solely responsible for any misrepresentations they make to third parties and for all transactions that use Subscriber's Private Key, regardless of whether such use was authorized. Subscribers are required to represent to MaxMD, Application Software Vendors, and Relying Parties that, for each certificate, the Subscriber will:

1. Require the HISP to securely generate its Private Keys and protect its Private Keys from compromise,
2. Provide accurate and complete information when communicating with MaxMD Direct HISP ,
3. Confirm the accuracy of the certificate data prior to using the certificate,
4. Promptly cease using a certificate and notify MaxMD Direct HISP if (i) any information that was submitted to MaxMD Direct HISP or is included in a certificate changes or becomes misleading or (ii) there is any actual or suspected misuse or compromise of the Private Key associated with the certificate,
5. Ensure that individuals using certificates on behalf of an organization have received security training appropriate to the certificate,
6. Use the certificate only for authorized and legal purposes, consistent with the certificate purpose, the CPS, any applicable CP, and the relevant Subscriber Agreement, including only installing SSL certificates on servers accessible at the domain listed in the certificate and not using code signing certificates to sign malicious code or any code that is downloaded without a user's consent,
7. Abide by the Subscriber Agreement and the CPS when requesting or using a Certificate, and
8. Promptly cease using the certificate and related Private Key after the certificate's expiration.

9.6.4. Relying Party Representations and Warranties

A relying party shall use a Direct Trust certificate for the purpose for which it was intended and check each certificate for validity

9.6.5. Representations and Warranties of Other Participants

No stipulation.

9.7. DISCLAIMERS OF WARRANTIES

MaxMD Direct HISP shall incorporate the disclaimers set forth in MaxMD's CPS into each Subscriber agreement. MaxMD does not guarantee the availability of any products or services and may modify or discontinue any product or service offering at any time.

9.8. LIMITATIONS OF LIABILITY

The limitations of liability related to MaxMD's certificates are set forth in MaxMD's CPS. MaxMD Direct HISP shall incorporate these limitations on liability into its agreements with Subscribers.

9.9. INDEMNITIES

9.9.1. Indemnification by MaxMD Direct HISP

MaxMD Direct HISP's indemnification obligations are set forth in a contract between MaxMD RA and Max*M*D CA.

9.9.2. Indemnification by Subscribers

To the extent permitted by law, MaxMD Direct HISP shall contractually require Subscribers to indemnify MaxMD and any cross-signed entities, and their respective partners, MaxMD Direct HISP officers, employees, agents, and contractors against any loss, damage, or expense, including reasonable attorney's fees, related to (i) any misrepresentation or omission of material fact by Subscriber, regardless of whether the misrepresentation or omission was intentional or unintentional; (ii) Subscriber's breach of the Subscriber Agreement, the CPS, or applicable law; (iii) the compromise or unauthorized use of a certificate or Private Key caused by the Subscriber's negligence; or (iv) Subscriber's misuse of the certificate or Private Key.

9.9.3. Indemnification by Relying Parties

No stipulation.

9.10. TERM AND TERMINATION

9.10.1. Term

This RPS and any amendments to the RPS are effective when approved by MaxMD and MaxMD Direct HISP and remain in effect until replaced with a newer version.

9.10.2. Termination

This RPS and any amendments remain in effect until replaced by a newer version.

9.10.3. Effect of Termination and Survival

MaxMD Direct HISP shall communicate the conditions and effect of this RPS's termination in a manner mutually agreed to by MaxMD and MaxMD Direct HISP . The communication will specify which provisions survive termination. At a minimum, all responsibilities related to protecting confidential information will survive termination.

9.11. INDIVIDUAL NOTICES AND COMMUNICATIONS WITH PARTICIPANTS

MaxMD accepts notices related to the CP/CPS/RPS by means of digitally signed messages or in paper form addressed to the locations specified in Section 2.2 of the CPS. Upon receipt of a valid, digitally signed acknowledgment of receipt from MaxMD, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five (5) days, or else written notice must then be sent in paper form through a courier service that confirms delivery or via certified or registered mail, postage prepaid, return receipt requested, addressed to the street address specified in Section 2.2.

9.12. AMENDMENTS

9.12.1. Procedure for Amendment

This RPS is reviewed annually. Amendments are made by mutual agreement between MaxMD RA and MaxMD CA.

9.12.2. Notification Mechanism and Period

Notice of amendments is not provided to any third party.

9.12.3. Circumstances under which OID Must Be Changed

Not applicable.

9.13. DISPUTE RESOLUTION PROVISIONS

No stipulation.

9.14. GOVERNING LAW

The laws of the state of New Jersey govern the interpretation, construction, and enforcement of this RPS and all proceedings related to MaxMD's products and services, including tort claims, without regard to any conflicts of law principles. The state of New Jersey has non-exclusive venue and jurisdiction over any proceedings related to the RPS or any MaxMD product or service.

9.15. COMPLIANCE WITH APPLICABLE LAW

No stipulation.

9.16. MISCELLANEOUS PROVISIONS

9.16.1 Entire agreement

This CP/CPS/RPS shall be interpreted consistently within the boundaries of business customs, commercial reasonableness under the circumstances, and intended usage of the product or service described herein. In interpreting this CP/CPS/RPS the parties shall also take into account the international scope and application of the services and products of MaxMD as well as the principle of good faith as it is applied in commercial transactions.

The headings, subheadings, and other captions in this CP/CPS/RPS are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CP/CPS/RPS. Appendices and definitions to this CP/CPS/RPS are for all purposes an integral and binding part of the CP/CPS/RPS. If/when this CP/CPS/RPS conflicts with other rules, guidelines, or contracts, this CP/CPS/RPS shall prevail and bind the Subscriber and other parties. If there is any conflict between the sections of this CP/CPS/RPS and any other document that relate to MaxMD, then the sections benefiting MaxMD and preserving MaxMD's best interests, at MaxMD's sole determination, shall prevail and bind the applicable parties.

9.16.2 Assignment

Parties to this CP/CPS/RPS may not assign any of their rights or obligations under this CP/CPS/RPS or applicable agreements without the written consent of MaxMD.

9.16.3 Severability

If any provision of this CP/CPS/RPS or the application thereof, is for any reason and to any extent found to be invalid or unenforceable, the remainder of this CP/CPS/RPS (and the application of the invalid or unenforceable provision to other persons or circumstances) shall

remain in full force and effect and shall be interpreted in such manner as to implement the original intention of the parties to the fullest extent possible.
Each and every provision of this CP/CPS/RPS that provides for a limitation of liability, disclaimer of or limitation upon any warranties or other obligations, or exclusion of damages is intended to be severable and independent of any other provision and is to be enforced as such.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

MaxMD reserves the right to seek indemnification and attorneys' fees from any party related to that party's conduct described in Section 9.9. Except where an express time frame is set forth in this CP/CPS/RPS, no delay or omission by any party to exercise any right, remedy or power it has under this CP/CPS/RPS shall impair or be construed as a waiver of such right, remedy or power. A waiver by any party of any breach or covenant in this CP/CPS/RPS shall not be construed to be a waiver of any other or succeeding breach or covenant. Bilateral agreements between MaxMD and the parties to this CP/CPS/RPS may contain additional provisions governing enforcement.

9.16.5 Force Majeure

MaxMD INCURS NO LIABILITY IF IT IS PREVENTED, FORBIDDEN OR DELAYED FROM PERFORMING, OR OMITS TO PERFORM, ANY ACT OR REQUIREMENT BY REASON OF: ANY PROVISION OF ANY APPLICABLE LAW, REGULATION OR ORDER; CIVIL, GOVERNMENTAL OR MILITARY AUTHORITY; THE FAILURE OF ANY ELECTRICAL, COMMUNICATION OR OTHER SYSTEM OPERATED BY ANY OTHER PARTY OVER WHICH IT HAS NO CONTROL; FIRE, FLOOD, OR OTHER EMERGENCY CONDITION; STRIKE; ACTS OF TERRORISM OR WAR; ACT OF GOD; OR OTHER SIMILAR CAUSES BEYOND ITS REASONABLE CONTROL AND WITHOUT ITS FAULT OR NEGLIGENCE.

9.17 OTHER PROVISIONS

This CP/CPS/RPS shall be binding upon the successors, executors, heirs, representatives, administrators, and assigns, whether express, implied, or apparent, of the parties that this CP/CPS/RPS applies to. The rights and obligations detailed in this CP/CPS/RPS are assignable by the parties, by operation of law (including as a result of merger or a transfer of a controlling interest in voting securities) or otherwise, provided such assignment is undertaken consistent with this CP/CPS/RPS articles on termination or cessation of operations, and provided that such assignment does not effect a novation of any other debts or obligations the assigning party owes to other parties at the time of such assignment.