
MedAllies Certificate Authority (CA)
Certificate Policy (CP)

Version
Date: August 1, 2019

Revision History

| Document Version | Document Date | Revision Details |
|---|---|---|
| 1.0 | Initial Draft | |
| 1.4 | | Updated to MedAllies CP v1.4 to align with DirectTrust™ Certificate Policy v1.4. |

MedAllies, Inc
300 Westage Business Center Drive
Suite 320
Fishkill, NY 12524
www.medallies.com
(845) 896-0191
www.medallies.com

## Table of Contents

# 1 Introduction

This MedAllies Certificate Authority CP (also referred to as "CP") follows the structure of the Internet Engineering Task Force (IETF) Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, Request For Comment (RFC) 3647.

The PKI to which this CP applies supports applications that includes secure exchange of electronic information by Covered Entities, Business Associates, Healthcare Entities, Consumer/Patients, Non-Declared Entities, Integrating the Healthcare Exchange (IHE) query-based transactions, Fast Healthcare Interoperability Resources (FHIR) and other specifications, including those grounded in the specifications of the Direct Project.

This CP is intended to be consistent with the United States Federal Bridge Certificate Authority (FBCA) Certificate Policy at the Basic assurance level and the Identity Vetting requirements of National Institute Standards and Technology (NIST) Special Publication 800-63. It is also compliant with the DirectTrust Community X.509 Certificate Policy V1.4 ("DirectTrust CP").

The terms and provisions of this CP shall be interpreted under and governed by applicable Federal law.

Pursuant to the IETF Public Key Infrastructure X.509 (PKIX) RFC 3647 CPS/CP framework, this CP is divided into nine parts that cover the security controls, and practices and procedures for Certificate and related services within the Direct PKI. To preserve the outline specified by RFC 3647, section headings that do not apply have the statement "Not applicable" or "No stipulation."

## 1.1 Overview

This CP describes the practices under which the MedAllies CA operates. Specifically, this document defines the creation and life-cycle management of X.509 version 3 Public key Certificates for use in applications supporting MedAllies' Direct secure message exchange.

### 1.1.1 Certificate Policy

Digital Certificates that conform to this CP contain at least 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 this CP, an OID corresponding to an identity proofing Level of Assurance (LoA), and an OID corresponding to a healthcare category. The MedAllies CA asserts the appropriate OIDs in the *certificatePolicies* extension of Certificates.

### 1.1.2 Relationship between the DirectTrust CP and this CP

The MedAllies CP is audited by the Direct Trusted Agent Accreditation Program (DTAAP) EHNAC Health Information Service Provider (HISP), Certification Authority (CA), and

Registration Authority (RA) Accreditation program.

### 1.1.3 Relationship between the DirectTrust CP and the MedAllies CP

The MedAllies CP is the DirectTrust CP v.1.4.

### 1.1.4 Relationship between DirectTrust CP and DirectTrust-EHNAC Accredited Entities

Compliance to an active CP version is a requirement for accreditation under the DirectTrust-EHNAC Accreditation as described in CP section 1.5.3, and entities accredited under this program have been audited regarding implementation of practices in compliance with an Active 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 Custodians (e.g. HISPs), CAs, and RAs, available at https://bundles.directtrust.org.

## 1.2 Document Name and Identification

This CP defines multiple LoAs each assigned an OID. The set of policy OIDs are registered under an arc of DirectTrust assigned organizational identifiers as registered in the ISO (International Organization for Standardization) and ITU (International Telecommunication Union) OID Registry. The applicable OIDs pertaining to this CP and the trust community are defined as follows:

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

| | | |
|---|---|---|
| **id- DirectTrust arc** | | **1.3.6.1.4.1.41179** |
| **id-DirectTrust-policies** | **id-DirectTrust(0)** | **1.3.6.1.4.1.41179.0** |
| **DirectTrust-CP 1.4** | **id-DirectTrust-policies.(1.4)** | **1.3.6.1.4.1.41179.0.1.4** |
| **Id-DirectTrust-LoAs** | **id-DirectTrust.(1)** | **1.3.6.1.4.1.41179.1** |
| DirectTrust LoA 3 | id-DirectTrust.(3) | 1.3.6.1.4.1.41179.1.3 |
| **Id-DTorg-Cat** | **id-DirectTrust.(2)** | **1.3.6.1.4.1.41179.2** |
| DirectTrust CE | id-DirectTrust-Cat.(1) | 1.3.6.1.4.1.41179.2.1 |
| DirectTrust BA | id-DirectTrust-Cat.(2) | 1.3.6.1.4.1.41179.2.2 |
| DirectTrust Patient | id-DirectTrust-Cat.(4) | 1.3.6.1.4.1.41179.2.4 |

| | | |
|---|---|---|
| DirectTrust Device | id-DirectTrust-Cat.(3) | 1.3.6.1.4.1.41179.3 |

Certificates issued by this CA are at a known LOA and/or conform to the requirements for a given healthcare entity category (Cat) assert that by listing the appropriate OID or OIDs representing the corresponding LoA as defined above in the *certificatePolicies* X.509 v3 standard extension.

See sections 3.2.2 and 3.2.3.1 for details of each LoA and Cat.

## 1.3 PKI Participants

The following are roles relevant to the administration and operation of this PKI.

### 1.3.1 PKI Authorities

#### 1.3.1.1 PKI Policy Authority

The MedAllies Security Steering Committee (SSC) is comprised of MedAllies security and business management individuals. The SSC owns this CP and represents the interest of MedAllies. The SSC is responsible for:

- Approving the CP and any successive change,
- Approving the compliance audit report for this CA, and
- Ensuring continued conformance of this CP with the CP.

#### 1.3.1.2 DirectTrust

DirectTrust is a not-for-profit, competitively neutral, self-regulatory entity operated by and for participants in the Direct community. DirectTrust operates the DirectTrust Policy Authority (DTPA) that is responsible for the DirectTrust CP, and overseeing the conformance of CA practices with its CP. DirectTrust Accreditation also reviews related practice statements such as this CP.

#### 1.3.1.3 Certification Authorities

The MedAllies CA signs Certificate Signing Requests (CSRs) and issues public key X.509 Certificates to Direct exchange or Direct Project organizational or individual Subscribers. This CA conforms to the policies of the DirectTrust CP V1.4.

### 1.3.2 Registration Authorities

Registration Authorities operate Identity Management systems (IdMs) and collect and verify Subscriber information on the MedAllies CA's behalf. MedAllies may act as its own RA or may delegate or subcontract the collection and verification of identity proofing

artifacts to an agent that has executed a RA agreement or Trusted Agent (TA) agreement that binds their behavior to the RA agreement.

RAs collect and verify identity information from Direct Subscribers using procedures that implement the identity validation policies set forth in this document. If MedAllies delegates RA activities, it monitors their compliance with its CP and if applicable, any Certificate Policy (CP) under which the RA operates. The MedAllies CA only relies on RAs that are accredited as RAs by DirectTrust.

#### 1.3.2.1 Trusted Agents

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. Trusted Agents are individuals who, while not an employee of the CA or RA, 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 the performance of collection and/or confirmation of information regarding Subscribers.

The MedAllies RA provides the Trusted Agent with material and training to facilitate the activities being performed by the Trusted Agent on behalf of the CA and RA. All activities of the Trusted Agent are performed in accordance with this CP.

### 1.3.3 Subscribers

A MedAllies Direct Subscriber is an entity who uses Direct services and PKI to support Direct transactions and communications. Subscribers are not always the party identified in a Certificate, such as when Direct organizational Certificates are issued to a Health Domain address. A Subscriber, as used herein, refers to both the subject of the Certificate and the entity that contracted with MedAllies CA for the Certificate's issuance. A Subscriber may contract a third party to manage their subscriptions. Prior to verification of identity and issuance of a Certificate, a Subscriber is an Applicant.

#### 1.3.3.1 Custodian

A Custodian acts in the capacity of an agent for the Subscriber for the purpose of enabling health information exchange by holding and managing Private Keys associated with a Certificate on behalf of that Subscriber in a Custodial Subscriber Key Store.

#### 1.3.3.2 Health Information Service Providers

A HISP is an entity that processes Direct-compliant messages to and from Direct addresses, each of which is bound to a Direct-compliant X.509 digital Certificate. Acting in the capacity of an agent for the Subscriber, the HISP holds and manages PKI private keys associated with a Direct digital Certificate on behalf of the Subscriber.

#### 1.3.3.3 Sponsors

A Sponsor fills the role of a Subscriber for groups, organizations, disabled personnel, and 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 section 3.2.2 and 3.2.3, and is responsible for meeting the obligations of Subscriptions as defined throughout this document.

### 1.3.4 Relying Parties

A Relying Party uses a Subscriber's X.509 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 using the Certification Revocation List (CRL) or Online Certificate Status Protocol (OCSP).

### 1.3.5 Other Participants

#### 1.3.5.1 Affiliates

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

#### 1.3.5.2 Affiliated Organizations

Subscriber Certificates may be issued in conjunction with an organization that has a relationship with the Subscriber; this is termed organizational affiliation. The organizational affiliation will be indicated in the Certificate. Affiliated Organizations are responsible for verifying the affiliation at the time Certificate application and requesting revocation of the certificate if the affiliate is no longer valid.

## 1.4 Certificate Usage

### 1.4.1 Appropriate Certificate Uses

The primary use for a MedAllies CA Certificate is in the exchange of electronic information for healthcare purposes. This includes Secure/Multipurpose Internet Mail Extensions (S/MIME) message signature verification and S/MIME message encryption. Certificates issued by this CA will be used for the purposes designated in the 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.

### 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 LoA 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 MedAllies SSC is responsible for this CP. The SSC includes members representing security and business management individuals. The SSC may amend this CP or any part thereof, at any time, at its discretion.

### 1.5.2 Contact Person

Questions regarding this certificate policy should be directed to:

Bruce Schreiber
Chief Technology Officer
MedAllies, Inc.
300 Westage Business Center Drive
Suite 320
Fishkill, NY 12524
Telephone - 845.896.0191
bschreiber@medallies.com

### 1.5.3 Person Determining Certification Practices Statement Suitability for the Policy

This CP states how the MedAllies CA establishes the assurance required by its corresponding DirectTrust CP. The MedAllies CA is responsible for asserting that the CP conforms to the DirectTrust CP. The MedAllies CA designates the SSC as the organization authorized to make these assertions.

The MedAllies CA operates under an accreditation program governed by DirectTrust that certifies the compliance of Issuing CA CPs to corresponding CP. See section 8 for further details.

## 1.6 Definitions and Acronyms

### 1.6.1 Acronyms

| Abbreviation | Meaning |
|---|---|
| ATS | Automatic Transfer Switches |
| BA | Business Associate |

| | |
|---|---|
| BMS | Building Monitoring System |
| CA | Certification Authority |
| CAT | Category |
| CCTV | Closed Circuit Television |
| CE | Covered Entity |
| CFR | Code of Federal Regulations |
| CMS | Center for Medicare and Medicaid Services |
| RP | Registration Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSR | Certificate Signing Request |
| DN | Distinguished Name |
| DN | Domain Name |
| DSA | Digital Signature Algorithm |
| DTAAP | Direct Trust Agent Accreditation Program |
| DTPA | Direct Trust Policy Authority |
| DTPC | Direct Trust Policy Committee |
| DVR | Digital Video Recording |
| EHNAC | Electronic Healthcare Network Accreditation |
| FBCA | Federal Bridge Certificate Authority |
| FHIR | Fast Healthcare Interoperability Resources |
| FIPS | Federal Information Processing |
| FTP | File Transfer Protocol |
| GLBA | Gramm-Leach-Bliley Act |
| HE | Healthcare Entity |
| HIPAA | Health Insurance Portability and Accountability Act |
| HISP | Health Information Service Provider |
| HSM | Hardware Security Model |
| HVAC | Heating, Ventilation, and Air Conditioning |
| ID | Identification |
| IdM | Identity Management |
| IETF | Internet Engineering Task Force |
| IHE | Integrating Healthcare Enterprise |
| ISO | International Organization for Standardization |
| ISSO | Information Systems Security Officer |
| ITU | International Telecommunication Union |
| LDAP | Lightweight and Directory Access Protocol |
| LEED | Leadership in Energy and Environment Design |
| LoA | Level of Assurance |
| MAPPA | MedAllies Public Key Infrastructure (PKI) Policy Authority |
| NERC | North American Electric Reliability Corporate |
| NIST | National Institute Standards and Technology |
| NPI | National Provider Identifier |

| | |
|---|---|
| NTP | Network Time Protocol |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| ONC | Office of the National Coordinator for Health Information Technology |
| PCI-DSS | Payment Card Industry Data Security Standard |
| PDU | Power Distribution Units |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure X.509 |
| RA | Registration Authority |
| RFC | Request For Comments |
| RPS | Registration Authority Practice Statement |
| RSA | Rivest-Shamir-Adleman |
| S/MIME | Secure Multipurpose Internet Mail Extensions |
| SSC | MedAllies Security Steering Committee |
| SHA | Secure Hash Algorithm |
| SOC | System and Organization Controls |
| SOX | Sarbanes-Oxley Act |
| SSL | Secure Socket Layer |
| TA | Trusted Agent |
| URI | Uniform Resource Identifier |
| VESDA | Very Early Smoke Detection Apparatus |

### 1.6.2 Definitions

| Term | Definition |
|---|---|
| **Certificate** | A digital representation of information which at least (1) identifies the Certification Authority issuing it, (2) names or identifies its Subscriber, (3) contains the Subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the Certification Authority issuing it. |
| **Certification Authority** | An authority trusted by one or more users to create and assign Certificates. Also known as a Certificate Authority. |
| **Registration Policy** | A Registration Policy is a specialized form of administrative policy tuned to electronic transactions performed during Registration management. A Registration Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital Certificates. |
| **Registration Practice Statement** | A statement of the practices that a CA employs in issuing, suspending, revoking, renewing certificates, and providing access to them, in accordance with specific requirements typically provided in a Registration Policy. |
| **Certificate Revocation List** | A list maintained by a Certification Authority of the certificates which it has issued that are revoked prior to their stated expiration date. |

| | |
|---|---|
| **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. |
| **Internet Engineering Task Force** | A standards development organization responsible for the creation and maintenance of many Internet-related technical standards. |
| **Information Systems Security Officer (ISSO)** | An individual responsible for establishing and maintaining the enterprise vision, strategy and program as it relates to Information Systems Security, to ensure information assets are adequately protected. |
| **Private Key** | (1) The key of a signature key pair used to create a digital signature.<br>(2) The key of an encryption key pair that is used to decrypt confidential information.<br>In both cases, this key must be kept secret. |
| **Public Key** | (1) The key of a signature key pair used to validate a digital signature.<br>(2) The key of an encryption key pair that is used to encrypt confidential information.<br>In both cases, this key is made publicly available normally in the form of a digital certificate. |
| **Public Key Infrastructure** | A set of policies, processes, server platforms, software and workstations used for the purpose of administering Certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key Certificates. |
| **Registration Authority** | Entity responsible for identification and authentication of Certificate subjects. |
| **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. |
| **Subscriber** | A Subscriber is an entity that does not itself issue Certificates to another party and is either (1) the subject named or identified in a Certificate issued to that entity, or (2) holds, directly or through its designated HISP (or other authorized third party), a private key that corresponds to the public key listed in the Certificate. |

# 2 Publication and Repository Responsibilities

## 2.1 Repositories

The MedAllies Direct CAs and RAs operate repositories in support of operations required by this CP and the DirectTrust CP. The MedAllies CA ensures that its Root Certificate and the revocation data for issued Certificates are available through a repository.

The MedAllies document repository can be found at:
http://pki.medalliesdirect.net/docs/

The MedAllies Root Certificates and CRLs can be found at:
http://pki.medalliesdirect.net/certs/

### 2.1.1 Repository Obligations

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

## 2.2 Publication of Certification Information

### 2.2.1 Publication of Certificates and Certificate Status

The MedAllies Issuing CA maintains a CRL and exposes its location in the CRL Distribution Points X.509 v3 extension. MedAllies also maintains an equivalent OCSP Responder and exposes its location in the Authority Information Access X.509 extension. The OCSP Responder is maintained in accordance with the relevant requirements in sections 4.9 and 7.3.

The MedAllies Issuing CA Certificates only contain valid Uniform Resource Identifiers (URIs) that are accessible by relying parties. MedAllies publishes its CA certificate and any other intermediate or Trust Anchor Certificates necessary to validate its Issuing CA.

### 2.2.2 Publication of CA Information

The MedAllies CA publishes information necessary to support its operation and use. A copy of this Registration Policy may be obtain from the links in 2.1 or by inquiry to support@medallies.com. The MedAllies CA may choose to publish their CP in its entirety or make available a redacted version.

### 2.2.3 Interoperability

No stipulation.

## 2.3 Frequency of Publication

This Certification Practice Statement, and any ensuing changes, is made available within 14

days of approval through the SSC consensus process.

## 2.4 Access Controls on Repositories

The MedAllies CA and associated RAs protect repository information not intended for public dissemination or modification. The CA operator provides unrestricted read access to its public repositories for legitimate uses and implements logical and physical controls to prevent unauthorized write access to such repositories.

# 3 Identification and Authentication

## 3.1 Naming

### 3.1.1 Types of Names

All Organizational certificates use non-null Domain Name Server name forms for the issuer and subject names.

Addresses-Bound Certificates contain a full Direct Address in the form of an *rfc822Name* in the Subject Alternative Name (also referred to as *subjectAltName*) extension of the certificate.

Domain-Bound Certificates contain a Health Domain Name Server in the form of a *dNSName* in the subject common name and the Subject Alternative Name extensions of the certificate.

### 3.1.2 Need for Names to be Meaningful

Names used in Certificates uniquely identify the organization or person to which they are assigned and are easily understood by humans.

### 3.1.3 Anonymity or Pseudonymity of Subscribers

This CA does 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

This CA enforces name uniqueness of the Certificate Subject Distinguished Name within the CA's X.509 namespace.

### 3.1.6 Recognition, Authentication, and Role of Trademarks

Should it come to the attention of the Officer or the Administrator that a Certificate infringes on the Intellectual Property of another entity, the MedAllies CA reserves the right to revoke such certificates.

## 3.2 Initial Identity Validation

### 3.2.1 Method to Prove Possession of Private Key

In the case where the private key is generated by the CA, no proof of private key possession is required. In the case where the Subscriber named in the Certificate

generates its own private key, then the Subscriber digitally signs a CSR with the private key and sends it to the MedAllies CA. The CA verifies the signature, thus proving private key possession.

### 3.2.2 Authentication of Organization Identity

Requests for Certificates that assert an organizational name in the subject field or Subject Alternative Name extension of the certificate will include the organization name, mailing address, and documentation of the legal existence of the organization. The RA shall confirm the legal status of the organizational representative. For Address-Bound and Domain-Bound Certificates, the requested Health Domain Name or Health Endpoint Name will be included (see section 3.1.1 for details).

The requesting organization will represent in a signed statement such as a Certificate Application their healthcare category as defined by Health Insurance Portability and Accountability Act (HIPAA) at 45 Code of the Federal Register (CFR) 160.103. Any organization not providing attestation to one of the above categories is considered a Non-Declared Entity.

An organization acting as a Subscriber or named in a Certificate that asserts organization affiliation must be a legally distinct entity. If a domain name or email address (*RFC822 name*) is asserted in the Certificate then the RA will validate the Subscriber's right to use it.

For all Certificates asserting an organization name, the Issuer CA or the RA will verify the organization and the organization's category in accordance with the following minimum requirements. The organization's category OID will be asserted in all Certificates.

| | |
|---|---|
| DT.org CE | Applicant represents in a statement such as a signed Certificate Application that it is a Covered Entity (CE) as defined by HIPAA at 45 CFR 160.103. *The RA shall verify the application includes the signed statement, the organization information submitted, the identity of the representative in accordance with section 3.2.3.1. and the representative's authorization to act in the name of the organization.* |
| DT.org BA | Applicant represents in a statement such as a signed Certificate Application that it is a Business Associate (BA) as defined in HIPAA at 45 CFR 160.103. *The RA verifies the application includes the signed statement, the organization information submitted, the identity of the representative in accordance with section 3.2.3.1 and the representative's authorization to act in the name of the organization*. |
| DT.org HE | Applicant represents in a statement, such as a signed Certificate Application, that it is a Non-HIPAA Healthcare Entity (HE), defined as an entity that is not covered by HIPAA and handles Protected Health Information in accordance |

| | |
|---|---|
| | with HIPAA Privacy and Security Rules as required for Covered Entities. *The RA shall verify application includes the signed statement, the organization information submitted, the identity of the representative in accordance with section 3.2.3.1 and the representative's authorization to act in the name of the organization.* |
| DT.org Non-Declared | Entity 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. *The RA shall verify application, the organization information submitted, the identity of the representative's in accordance with section 3.2.3.1 and the representative's authorization to act in the name of the organization.*<br><br>If a certificate asserts an organizational affiliation, the RA will obtain documentation from the organization that authorizes the affiliation and an agreement which obligates the organization to: request modification or revocation of the Certificate if information in the Certificate subject is no longer accurate, and request revocation of unexpired Certificates if organizational affiliation ends. See sections 3.2.3.3, 4.9.1 and 9.6.1. |

## 3.2.3 Authentication of Individual Identity

### 3.2.3.1 Authentication of Human Subscribers

Identity proofing is required for an individual acting as a:

1. Subscriber,
2. Organizational representative,
3. Information System Security Officer (ISSO) or equivalent at the organization physically controlling the Private Key of a Certificate, or
4. Sponsor of a Device Certificate.

DirectTrust identity proofing LoAs are intended to provide equivalent assurances to identify proofing LoAs as defined by NIST SP 800-63-2. At a minimum, the Issuers CA or the RA will proof an individual's identity in accordance with one of the following LoAs:

| | |
|---|---|
| DT.org LoA 3 | Applicant supplies his or her full legal name, an address of record, and date of birth.<br><br>For **In-Person vetting**: the applicant also provides valid government issued photo identification (ID).<br><br>**RA** inspects the photo-ID and records the ID number; compares picture to Applicant; and verifies information provided through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, date of birth, address and other personal information in records are consistent with the application.<br><br>**CA** issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications at phone number associated with the Applicant in records – or – confirms the ability of the Applicant to receive mail at the claimed address– or – sends notice to the confirmed physical address associated with the Applicant in the records after issuance.<br><br>If the telephone method is used, CA also records Applicant's voice or uses alternative means that establish an equivalent level of non-repudiation.<br><br>For **Remote vetting**: the applicant provides valid government issued Photo ID identifier and a utility or financial account identifier, along with appropriate metadata sufficient to identify and verify the respective ID and account.<br><br>**RA** verifies both ID and account numbers provided through record checks either with the applicable agency or institution or through credit bureaus or similar databases, and confirms that: name, date of birth, address and other personal information in records are consistent with the application. (For utility or financial account numbers, confirmation may be performed by verifying knowledge of recent account activity, when applicable).<br><br>**CA** issues credentials in a manner that confirms the ability of the Applicant to receive telephone communications or text message at phone number or email address associated with the Applicant in records – or – confirms the ability of the Applicant to receive mail at a physical address associated with the Applicant in the records.<br><br>Any of the identity verification methods listed for a higher level are also acceptable. |

Any government issued ID provided by the Applicant that includes an expiration date must be unexpired.

In-Person vetting for LoA 3 may be performed by the RA, Trusted Agent of the RA, or an entity certified by a State or Federal Entity as being authorized to confirm identities. A trust relationship between the Trusted Agent and the Applicant which is based on an in-person antecedent event may suffice as meeting the In-Person identity vetting requirements for LoA 3.

For Patient Certificates, the Issuer CA or the RA shall proof the Patient identity in accordance with any of the above LoA requirements, collect the Subscriber representation, and shall assert in the Certificate the Patient OID and the appropriate LoA OID.

Practice note: A Trust Bundle may require a particular identity proofing LoA be completed.

HIPAA representatives or other types of patient representatives may be issued Patient Certificates. In such cases, the Direct address shall correspond to the representative (not the patient). The Issuer CA or the RA shall proof the identity of the individual in accordance with any of the about LoA requirements, collect the Subscriber representation, and shall assert in the Certification the Patient OID and the appropriate LoA OID.

| | |
|---|---|
| **DT.org Patient** | Applicant represents that any Digital Certificate issued pursuant to this CP will be used for their personal healthcare Direct message exchange purposes. The RA verifies that the patient or the patient's Authorized Representative has made this representation. |

Practice Note: Allowing representatives access to patient data is outside the scope of this CP.

### 3.2.3.2 Authentication of Human Subscribers for Role-based Certificates

No stipulation.

### 3.2.3.3 Authentication of Human Subscribers for Group Certificates

A MedAllies Direct Trust certificate that is held and managed on behalf of a Subscriber organization is a group Certificate. Identity verification of the Subscriber organization and its representative is covered in sections 3.2.2 and 3.2.3.1.

For MedAllies managed group Certificates, the MedAllies CA and/or its subcontracted RAs also record(s) the information identified in section 3.2.3.1 for the MedAllies Chief Security Officer before issuing the certificate. In addition to the authentication of the Subscriber (and their organization when required), the following procedures is performed:

- The MedAllies Chief Security Officer is responsible for ensuring control of the private key, including maintaining a list of any Subscribers who have access to use of the private key, and accounting for which Subscriber had control of the key at what time,

- The subjectName Domain Name does not imply that the subject is a single individual, e.g. by inclusion of a human name form without also clearly indicating the group nature of its issuance, and

- The list of those holding the shared private key is provided to, and retained by, the MedAllies CA and its Security Officer.

In the case of a Direct Organizational Certificate, a Direct Address "User" is any human person or device human sponsor that submits a message to the Direct network or receives a message from the Direct Network on behalf of the Subscriber Organization. If the identity proofing component is performed by the Subscriber Organization, then the conforming RA must retain documentation that the Subscriber Organization is bound through a legally binding contract with, or an attestation to, the RA to meet the identity verification requirements of this paragraph. In this case, prior to authorizing access to the Direct network by a User, the Subscriber Organization must collect the User's full legal name, an address of record, date of birth and an ID number (and the ID type). This information must be made available by the Subscriber Organization to the RA upon request. In addition, the Subscriber Organization must have processes in place that are sufficient to verify the User's identity at the LoA of the associated Direct Organizational certificate or a higher LoA.

Practice Note: The Subscriber Organization may be able to leverage its existing relationship as an employer or affiliate of a User to meet the identity verification requirements. For example, Federal Employment Eligibility Verification Form I-9 may be sufficient with supplemental verification of submitted information to meet LoA 3 requirements. Acceptable ID numbers may include a government ID number, a current employee number, or other ID number bound to the User and recognized by the Subscriber Organization.

### 3.2.3.4 Authentication of Devices

The MedAllies CA may issue a Certificate for use on a computing or network device. In such cases, the device has a human sponsor who provides:

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

Registration includes verification of the sponsor to an assurance level commensurate with the Certificate assurance level being requested for the device. Methods for performing this authentication and integrity checking include, but are not limited to:

- Verification of digitally signed messages sent from the sponsor (using Certificates of equivalent or greater assurance than that being requested).
- In-person or remote registration by the Sponsor, with the identity of the Sponsor confirmed in accordance with the requirements of section 3.2.3.1.

If the Certificate's Sponsor changes, the new Sponsor reviews the status of each device to ensure it is still authorized to receive certificates. This CP describes procedures to ensure that certificate accountability is maintained.

#### 3.2.3.5 Verification of NPI Number

If the National Provider Identification (NPI) number is included in a Certificate, it must be verified against the NPI Registry provided by the Centers for Medicare and Medicaid (CMS). The RA must utilize the Applicant-provided NPI number and confirm that the data elements returned are consistent with the information provided in the application.

### 3.2.4 Non-verified Subscriber Information

Non-verified Subscriber information is not included in a Certificate.

### 3.2.5 Validation of Authority

Reference section 3.2.2.

### 3.2.6 Criteria for Interoperation

To be deemed a conforming Direct Trust Issuing CA, the MedAllies CA issues Certificates according to the DirectTrust Registration Policy.

## 3.3 Identification and Authentication for Re-key Requests

### 3.3.1 Identification and Authentication for Routine Re-key

The MedAllies CA does not re-key existing certificates. The process to replace a key is to

revoke the existing certificate and key, create a new Certificate Signing Request (CSR) and upon verification of the certificate owner the new CSR will be verified and the certificate published.

### 3.3.2 Identification and Authentication for Re-key after Revocation

If a MedAllies Trust Certificate is revoked, the Subscriber goes through the initial as described in section 3.2 to obtain a new Certificate.

## 3.4 Identification and Authentication for Revocation Request

All revocation requests are authenticated. Requests to revoke a Certificate may be authenticated using that Certificate's public key, regardless of whether or not the associated private key has been compromised.

# 4 Certificate Life-Cycle

## 4.1 Application

This section specifies requirements for the initial application for a MedAllies Direct X.509 certificate.

### 4.1.1 Submission of Certificate Application

MedAllies or a Subscriber creates the official Certificate Signing Request based on input received from the Subscriber as validated by the MedAllies RA during the identity verification process.

### 4.1.2 Enrollment Process and Responsibilities

A Subscriber is responsible for providing accurate information about himself and his organization during identity verification. The MedAllies RA is responsible for ensuring that the identity of each Certificate Applicant is verified in accordance with this CP and its corresponding CP prior to the issuance of a Certificate. The MedAllies CA and RA authenticate and protect all communication made during the Certificate Application process.

## 4.2 Certificate Application Processing

The MedAllies CA and RA are responsible for verifying that the information in a Certificate Signing Request is accurate and reflect the information presented by the Subscriber.

### 4.2.1 Performing Identification and Authentication Functions

The identity verification of Subscribers is done by the MedAllies RA as specified in section 3.2 using procedures detailed in this CP.

### 4.2.2 Approval or Rejection of Certificate Applications

A Certificate application may be rejected by the MedAllies CA due to missing or inaccurate information. The SSC retains the right to reject MedAllies Direct Certificate Applications if, in its judgment, the requesting individual or organization does not have a legitimate reason to possess a MedAllies Direct Certificate.

### 4.2.3 Time to Process Certification Applications

Subscriber information placed in a MedAllies Direct Certificate is verified and a Certificate is issued within 30 days of completion of verification.

## 4.3 Issuance

### 4.3.1 CA Actions During Certificate Issuance

The MedAllies CA ensures that the public key is bound to the correct Subscriber and

generates the X.509 certificate. The MedAllies CA publishes the Certificate as specified in section 4.4.2. The MedAllies CA performs its actions during the Certificate issuance process in a secure data center using specialized cryptographic hardware devices.

### 4.3.2 Notification to Subscriber of Certificate Issuance

Upon issuance of the Certificate by the MedAllies CA, the administrator of the account is notified by the MedAllies CA operator. The administrator is responsible for notifying the subscribers.

## 4.4 Certificate Acceptance

### 4.4.1 Conduct Constituting Certificate Acceptance

All Subscribers either sign a Subscriber Agreement Form or agree to the MedAllies Terms and Conditions. Both stipulate the terms of Certificate acceptance and use. This process and the use of the credential is considered Certificate acceptance.

### 4.4.2 Publication of the Certificate by the CA

The MedAllies Direct CA delivers its Direct Certificates to the operating HISP which then publishes it to the public according to current Direct standards. Non Direct certificates are delivered to the client via email or FTP.

### 4.4.3 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

## 4.5 Key Pair and Certificate Usage

### 4.5.1 Subscriber Private Key and Certificate Usage

Subscribers or their authorized Custodian (e.g. HISP) representatives, who take possession of their Private Key shall protect it from access by unauthorized parties and shall use the Private Keys only as specified by the *certificatePolicies* and *keyUsage* extensions of the corresponding Certificate.

### 4.5.2 Relying Party Public Key and Certificate Usage

MedAllies Direct Certificates conform to the policies provided by the corresponding Registration Policy. Relying Parties should understand these policies. The MedAllies Direct CA publishes a Certificate Revocation List (CRL) and maintains an OCSP Responder. Relying Parties should process the CRL on a regular basis and reject Certificates found on it and/or respect the Certificate status reflected in an OCSP response.

## 4.6 Certificate Renewal

After Certificate renewal, the old Certificate may or may not be revoked, but is not further re-keyed, renewed, or modified.

### 4.6.1 Circumstance for Certificate Renewal

Certificate renewal may be renewed if the public key has not reached the end of its validity period, the associated Private Key has not been compromised, and the Subscriber name and attributes are unchanged. Re-verification of the Subscriber's identity is not required under section 3.3.1.

### 4.6.2 Who May Request Renewal

The MedAllies CA may request renewal of its own Certificate. For Subscriber Certificates, the Subscriber or their Authorized Representative, or the RA may request renewal.

### 4.6.3 Processing Certificate Renewal Requests

The MedAllies CA or RA shall approve or reject Subscriber Certificate renewal requests. Identity proofing of the Subscriber when required shall be the equivalent to the initial identity proofing process or executed via proof of possession of the Private Key through a digital signature.

### 4.6.5 Conduct Constituting Acceptance of a Renewal Certificate

Failure to object to the renewed Certificate or its contents, or actual use of the Certificate, constitutes the Subscriber's acceptance of the Certificate.

### 4.6.6 Publication of the Renewal Certificate by the CA

Renewed Direct certificates are published by delivering the certificate to the HISP on behalf of the Subscriber. All renewed Direct certificates are published according to current Direct standards. Non-Direct certificates are delivered to the Subscriber via email or FTP.

### 4.6.7 Notification of Certificate Issuance by the CA to Other Entities

No stipulation.

## 4.7 Certificate Re-Key

Re-keying a Certificate consists of creating new Certificates with a different public key (and serial number) while retaining the remaining contents of the old Certificate that describe the Subject. The new Certificate may be assigned a different validity period, key identifiers, specify a different CRL (cRLDistributionPoints) or OCSP Responder location, and/or be signed with a different key. Re-key of a Certificate does not require a change to the *subjectName* and does not violate the requirement for name uniqueness.

After Certificate re-key, the old Certificate may be revoked and will not be further re-keyed, renewed, or modified.

### 4.7.1 Circumstance for Certificate Re-Key

A Certificate is re-keyed before its end of its validity period and when no other information besides its keys and validity period are changing. A revoked Certificate is not re-keyed.

### 4.7.2 Who May Request Certification of a New Public Key

A MedAllies Direct RA or the Subscriber or their Authorized Representative may request the re- key of a Subscriber Certificate.

### 4.7.3 Processing Certificate Re-Keying Requests

The MedAllies CA approves or rejects Subscriber Certificate re-keying requests. Identity verification of the Subscriber is equivalent to the initial identity verification.

### 4.7.4 Notification of New Certificate Issuance to Subscriber

See section 4.3.2.

### 4.7.5 Conduct Constituting Acceptance of a Re-Keyed Certificate

See section 4.4.1.

### 4.7.6 Publication of the Re-keyed Certificate by the CA

See section 4.4.2.

### 4.7.7 Notification of Certificate Issuance by the CA to Other Entities

See section 4.4.3.

## 4.8 Modification

Certificate modification is not allowed at this time.

### 4.8.1 Circumstance for Certificate Modification

Not applicable.

### 4.8.2 Who May Request Certificate Modification

Not applicable.

### 4.8.3 Processing Certificate Modification Requests

Not applicable.

### 4.8.4 Notification of New Certificate Issuance to Subscriber

Not applicable.

### 4.8.5 Conduct Constituting Acceptance of Modified Certificate

Not applicable.

### 4.8.6 Publication of the Modified Certificate by the CA
Not applicable.

### 4.8.7 Notification of Certificate Issuance by the CA to Other Entities
Not applicable.

## 4.9 Certificate Revocation and Suspension

### 4.9.1 Circumstances for Revocation
All Certificates are revoked when the binding between the Subject and the Subject's public key defined within a Certificate is no longer considered valid. Examples of circumstances that invalidate the binding are:

- identifying information or affiliation components of any names in the Certificate become invalid
- the Subscriber can be shown to have violated the stipulations of its Subscriber
  Agreement or Terms and Conditions
- the private key is suspected of compromise and the Subscriber asks for his/her certificate to be revoked
- the Subscriber, Custodian (e.g. HISP), or RA requests Certificate revocation
- the Subscriber did not authorize the original certificate request and did not retroactively grant authorization

Whenever any of the above circumstances occur, the associated Certificate is revoked and placed on the CRL and, when applicable, its' revoked status is reflected in OCSP responses.

### 4.9.2 Who Can Request Revocation
The MedAllies CA, Subscriber, an Authorized Representative, or the RA may request revocation of a Certificate, or the issuing CA may consider requests from a Subscriber or their Authorized Representative to revoke a certificate.

### 4.9.3 Procedure for Revocation Request
All requests for Certificate revocation identify the Certificate to be revoked by serial number and explain the reason for revocation. The MedAllies CA ensure that the Certificate revocation request is not malicious and verifies that the reason for revocation is valid. If the request comes from a third party, the SSC will investigate the report and decide whether the revocation is appropriate.

If the reason for revocation is valid, the MedAllies CA places the Certificate's serial

number and any other required information on its' CRL and/or has its revoked status reflected in OCSP responses.

### 4.9.4 Revocation Request Grace Period

There is no grace period for revocation. Subscribers and other participants must request the revocation of a Certificate as soon as the need for revocation comes to their attention.

### 4.9.5 Time Within Which CA Must Process the Revocation Request

The MedAllies CA processes all revocation requests within 8 hours of receipt. CRL issuance frequency is addressed in section 4.9.7.

### 4.9.6 Revocation Checking Requirements for Relying Parties

No stipulation.

### 4.9.7 CRL Issuance Frequency

All MedAllies CA CRLs are issued and posted to the repository listed in section 2.2.1. The CRL for end entity Certificates are issued every 24 hours with a 25 hour lifespan.

The CRL for CA Certificates are issued every 30 days with a 35 day lifespan. A CRL may be issued more frequently if new entries are made to the CRL.

The MedAllies CA ensures that superseded CRLs are removed from the public repository upon posting of the latest CRL.

### 4.9.8 Maximum Latency of CRLs

CRLs are posted upon generation but within no more than four hours after generation. Furthermore, a new CRL is published no later than the time specified in the nextUpdate field of the most recently published CRL.

### 4.9.9 On-Line Revocation/Status Checking Availability

The MedAllies CA deploys an OCSP responder.

### 4.9.10 On-Line Revocation Checking Requirements

No stipulation.

### 4.9.11 Other Forms of Revocation Advertisements Available

No other form of revocation advertisement are offered.

### 4.9.12 Special Requirements Related to Key Compromise

In the event of a CA Private Key compromise or loss, a CRL shall be published at the earliest feasible time. When a CA Certificate is revoked, or Subscriber Certificate is revoked because of a compromise or suspected compromise of a Private Key, a CRL will

be issued within 18 hours of notification.

### 4.9.13 Circumstances for Suspension
The MedAllies CA does not support Certificate suspension.

### 4.9.14 Who Can Requests 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
The MedAllies CAs support Certificate status services via CRLs and OCSP responders See section 4.10.2 for service availability.

### 4.10.2 Service Availability
Certificate services are available 24x7 without interruption.

### 4.10.3 Optional Features
Responses are digitally signed by an OCSP Certificate which is issued by the same CA as the Certificate under consideration.

## 4.11 End of Subscription
Certificates that have expired prior to or upon end of subscription are not revoked. Subscribers with an expired subscription will have unexpired Certificates revoked.

## 4.12 Key Escrow and Recovery
Key escrow is not supported.

### 4.12.1 Key Escrow and Recovery Policy and Practices
Not applicable.

### 4.12.2 Session Key Encapsulation and Recovery Policy and Practices
Not applicable.

# 5 Facility Management and Operations Controls

## 5.1 Physical Controls

The MedAllies CA and RA equipment are protected from unauthorized access at all times.

### 5.1.1 Site Location and Construction

MedAllies Direct Services production environment is located at a top-tier, 3rd party hosting facility that meets Payment Card Industry Data Security Standard (PCI-DSS), Systems and Organization Controls (SOC) 2, HIPAA, NIST 800-53, Leadership in Energy and Environment Design (LEED), North American Electric Reliability Corporate (NERC), Gramm-Leach-Bliley Act (GLBA), and the Sarbanes-Oxley Act of 2002 (SOX) requirements. The location and construction of the facility housing the CA/RA equipment is consistent with facilities used to house proprietary and sensitive computer systems and networks. The location and construction provides robust protection against unauthorized access to the CA/RA equipment and records.

### 5.1.2 Physical Access

The data center facility utilizes an array of security equipment and procedures to control, monitor, and record access to the facility, including the customer dedicated areas. The data center facilities exteriors may incorporate additional security measures such as masonry and steel construction, ballistics-resistant walls, doors, and windows, and hurricane wind-rate roofs.

All areas of the data center facilities, including cages, are controlled, monitored, and recorded using Closed Circuit Television (CCTV) cameras. The CCTV subsystem provides the display, control, Digital Video Recording (DVR), and playback of live video from cameras throughout the facilities. Each camera is capable of accelerating digital recordings during alarm conditions for better resolution.

The data center facilities are staffed on a 24 hour per day basis by either third party vendor professional security staff or employed personnel, which monitor access points and the electronic security systems. The door entrances to the data center facilitates require a two-factor method authentication, consistent of a biometric scanner and electronic access card swipe or security code. The biometric scanners verify unique geometry images and heat signatures before allowing authorized users access into the facilities and through various doors within the facilities. Through a combination of biometric scanner and electronic access card swipe or security code, users identify themselves to the system and obtain access into certain areas of the data center facilitates based upon the pre-defined user permissions.

### 5.1.3 Power and Air Conditioning

A building monitoring system (BMS) is in place at the data center facilities. The BMS is a

control, monitoring, and reporting system used to monitor and control the environmental systems and alert operations personnel to potential issues. Engineers routinely use it to review operating conditions that include, but are not limited to temperatures, flows, pressures, electronical and mechanical loads, and alarms, looking for abnormal conditions. The BMS also provides long-term data storage to assist in troubleshooting, if needed. The facility environment systems are monitored and managed by employed personnel.

The BMS system monitors / controls the following:

- Power systems, including critical electronic components, generators, transfer switches, main switchgears, power distribution units (PDU), automatic transfer switches (ATS), and uninterruptible power supply
- The Heating, Ventilation, Air Conditioning (HVAC) system, which controls and / or monitors space temperature and humidity within the data center facilities, space pressurization, HVAC equipment status and performance, and outside air conditions.
- Fire detection and suppression equipment, such as very early smoke detection apparatus (VESDA), double interlock pre-action and detection systems, and zoned gaseous-based fire extinguishing system.
- Leak detection systems.

Site personnel perform and log visual checks of poser, environmental, and other system controls, including battery and fuel monitoring systems per defined schedules.

### 5.1.4 Water Exposures

See section 1.5.

### 5.1.5 Fire Prevention and Protection

The data center facilities are constructed with fire detection and suppression system that limit potential damage in the event of a fire. Key features of the fire detection and suppression systems includes a combination of any of the following:

- Dry-pipe double interlock pre-action fire suppression system
- Wet pipe water sprinkler fire suppression system
- Laser-based VESDA
- Zoned gaseous-based fire extinguishing system

Sprinkler systems in the data center facilities are implemented with double interlock pre-action and detection systems. Pre-action detection with intelligent heat detectors are installed in the ceiling of mission critical areas of the data center facilities. Upon activation of any of these heat detectors, audio-visual alarms (horn and/or strobes) will activate throughout the space. A signal is sent to a pre-action valve for the affected fire zone. If the temperature in the at-risk area also reaches levels to melt any of the sprinkler

head fusible links, water is triggered to enter the sprinkler pipes for the affected areas of the data center facility.

Fire extinguishers are provided throughout each data center facility. Dry chemical or clean agent extinguishers are installed in the mission critical space or adjacent areas where one might reasonably expect a person to carry them into the affected areas during an emergency.

The fire suppression system is monitored on a 24 hour per day basis by an external alarm monitoring company which will dispatch the city fire department upon receipt of an alarm. Inside the data center facilities, software is used for fire detection and monitoring, combined with customized floor plan graphics to illustrate detection devices and detection devices and fire zones to aid personnel and the fire department in responding to and coordinating fire control activities.

### 5.1.6 Media Storage

CA/RA media is stored so as to protect it from accidental damage (such as water, fire, electromagnetic, etc.). Media that contains audit, archive, or backup information is duplicated on redundant disks and stored in a secure location separate from the CA/RA equipment. This storage is restricted to authorized custodians.

### 5.1.7 Waste Disposal

Sensitive media and documentation that are no longer needed for CA operations is destroyed by a commercial disposal company. For example, sensitive paper documentation is shredded and rendered unrecoverable.

De-commissioned hard drives are securely erased. They are then handed over to a commercial disposal company. Certificates of destruction are provided by the disposal company.

## 5.2 Procedural Controls

### 5.2.1 Trusted Roles

The MedAllies CAs defines Trusted personnel in terms of four roles:

1. **Administrator** – authorized to install, configure, and maintain the CA; establish and maintain user accounts; configure profiles and audit parameters; and generate component keys
2. **Officer** – authorized to request or approve Certificates or Certificate revocations
3. **Auditor** – authorized to maintain audit logs
4. **Operator** – authorized to perform system backup and recovery

Some roles may be combined. The following subsections provide a detailed description of the responsibilities for each role.

#### 5.2.1.1 Administrator – Chief Technology Officer

The Administrator role is responsible for:

- Installation, configuration, and maintenance of the CA
- Establishing and maintaining CA system accounts
- Configuring Certificate profiles or templates and audit parameters, and generating and backing up CA keys
- Administrators do not issue certificates to Subscribers.

#### 5.2.1.2 Officer – Chief Operating Officer

The Officer role is responsible for issuing Certificates. This includes overseeing:

- Registering new Subscribers and requesting the issuance of Certificates
- Verifying the identity of Subscribers and accuracy of information included in certificates
- Approving and executing the issuance of Certificates, and requesting, approving and executing the revocation of Certificates

#### 5.2.1.3 Auditor – Chief Security Officer

The Auditor role is responsible for overseeing:

- Reviewing, maintaining, and archiving audit logs
- Performing or overseeing internal compliance audits to ensure that the CA is operating in accordance with this CP

#### 5.2.1.4 Operator – Sys Ops Manager

The Operator role is responsible for overseeing:

- The routine operation of the CA equipment and operations such as system back-ups and recovery or changing recording media.

### 5.2.2 Number of Persons Required Per Task

At least two people are trained for each task but only one is required to execute each task.

### 5.2.3 Identification and Authentication for Each Role

A person occupying a Trusted Agent role authenticates himself/herself to the CA system using a MedAllies credential or equivalent.

### 5.2.4 Separation of Roles

Any individual may assume the Operator role. No one individual assumes both the Officer and Administrator roles.

## 5.3 Personnel Controls

### 5.3.1 Background, Qualifications, Experience, and Security Clearance Requirements

All persons filling Trusted Roles are selected on the basis of loyalty, trustworthiness, and integrity. All Trusted Roles are required to be held by persons who are legally eligible to work in the United States.

### 5.3.2 Background Check Procedures

It is MedAllies policy that all offers of employment at MedAllies are contingent upon clear results of a thorough background check. Background checks will be conducted on all applicants after acceptance of a job offer. Background checks are conducted according to the MedAllies Personnel Policy manual.

### 5.3.3 Training Requirements

Persons in a Trusted Role receive comprehensive in all aspects of the role they perform. All persons have a reasonable understanding of PKI principles and operations.

### 5.3.4 Retraining Frequency and Requirements

Individuals responsible for Trusted Roles are notified of changes in CA operation. Any significant change to the operations must include a training plan, and the execution of such plan is documented.

### 5.3.5 Job Rotation Frequency and Sequence

MedAllies has no requirement for job rotation.

### 5.3.6 Sanctions for Unauthorized Actions

The SSC takes appropriate administrative and disciplinary actions against personnel who violate this policy.

### 5.3.7 Independent Contractor Requirements

Contractor personnel employed to perform functions pertaining to the CA meet the personnel requirements set forth in this CP.

### 5.3.8 Documentation Supplied to Personnel

Documentation sufficient to define duties and procedures for each role is provided to the personnel filling that role.

## 5.4 Audit Logging Procedures

Audit log files are generated for all events relating to the security of the CA. All security audit logs, both electronic and non-electronic, are retained and made available during compliance audits.

### 5.4.1 Types of Events Recorded

A message from any source received by the MedAllies CA requesting an action related to the operational state of the CA is an auditable event. At a minimum, each audit record includes the following (either recorded automatically or manually for each auditable event):

- The type of event,
- The date and time the event occurred,
- A success or failure indicator, where appropriate,
- The identity of the entity and/or operator (of the MedAllies CA) that caused the event,

Detailed audit requirements are listed in the table below. All security auditing capabilities of the Issuing CA operating system and CA applications required by this CP are enabled. As a result, most of the events identified in the table are automatically recorded. Where events cannot be automatically recorded, the MedAllies CA implements manual procedures to satisfy this requirement.

| **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 unsuccessful authentication attempts reached 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 the system |
| DATA EXPORT AND OUTPUT |
| All successful and unsuccessful requests for confidential and security-relevant information |
| KEY GENERATION |
| Whenever a CA generates a key (not mandatory for single session or one-time use symmetric keys) |
| PRIVATE KEY LOAD AND STORAGE |
| The loading of Component Private Keys |
| All access to Certificate Subject Private Keys retained within the CA for key recovery |
| TRUSTED PUBLIC KEY ENTRY, DELETION, AND STORAGE |
| Any change to the trusted public keys, including additions and deletions |
| SECRET KEY STORAGE |
| The manual entry of secret keys used for authentication |
| PRIVATE AND SECRET KEY EXPORT |
| The export of private and secret keys (keys used for a single session or message are excluded) |
| CERTIFICATE REGISTRATION |
| All certificate requests, including issuance, re-key, and renewal |
| Certificate issuance |
| CERTIFICATE REVOCATION |
| All certificate revocation requests |
| CERTIFICATE STATUS CHANGE APPROVAL OR REJECTION |

| |
|---|
| CA CONFIGURATION |
| Any security-relevant changes to the configuration of a CA system component |
| 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 |
| REVOCATION PROFILE MANAGEMENT |
| All changes to the revocation profile |
| CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT |
| All changes to the certificate revocation list profile |
| TIME STAMPING |
| A third party time stamp is obtained |
| MISCELLANEOUS |
| Appointment of an individual to a Trusted Role |
| Installation of an Operating System |
| Installation of a PKI Application |
| Installation of a Hardware Security Modules |
| System Start-up |
| Log on attempts to PKI Application |
| Attempts to set passwords |
| Attempts to modify passwords |
| Backup of the internal CA database |

| |
|---|
| Restoration from backup of the internal CA database |
| All Certificate compromise notification requests |
| Zeroizing Hardware Security Modules (HSMs) |
| Re-key of the Component |
| CONFIGURATION CHANGES |
| Hardware |
| Software |
| Operating System |
| Patches |
| PHYSICAL ACCESS / SITE SECURITY |
| Known or suspected violations of physical security |
| ANOMALIES |
| System crashes and hardware failures |
| Software error conditions |
| Software check integrity failures |
| Network attacks (suspected or confirmed) |
| Equipment failure |
| Violations of a CPS or CP |
| Resetting Operating System clock |

### 5.4.2 Frequency of Processing Log

Audit logs are reviewed and monitored by an automated process in real-time. Alerts and exception reports are generated as appropriate.

### 5.4.3 Retention Period for Audit Logs

Security audit log data is available on the CA equipment for a minimum of two months.

### 5.4.4 Protection of Audit Logs

Only authorized personnel who require access for the performance of their job responsibilities have access to the logs, and the right to archive the logs. Access rights management systems and processes enforce these requirements.

### 5.4.5 Audit Log Backup Procedures

The security audit logs are backed up to an offsite location in real-time. All virtual machines are snapshotted nightly and moved offsite daily.

### 5.4.6 Audit Collection System (internal vs. external)

All security audit processes are invoked at CA start-up and cease only at shutdown. Should it become apparent that an automated security audit system has failed, the CA ceases all operation except for revocation processing until the security audit capability can be restored.

### 5.4.7 Notification to Event-Causing Subject

There is no requirement to notify a Subject that an event was audited. Real-time alerts are neither required nor prohibited.

### 5.4.8 Vulnerability Assessments

The CA is subjected to the same vulnerability assessments as other critical systems. The MedAllies CA operator executes external and internal vulnerability scans on a monthly basis.

## 5.5 Records Archival

### 5.5.1 Types of Events Archived

CA archive records are sufficiently detailed as to verify that the CA was properly operated as well as to verify the validity of any Certificate throughout its validity period. The following data is archived:

1. Any accreditation of the MedAllies CA
2. All applicable CPS and CP versions
3. Contractual obligations and other agreements concerning the operation of the CA
4. System and equipment configurations, modifications, and updates
5. Certificate and revocation requests
6. Identity authentication data
7. Any documentation related to the receipt or acceptance of a certificate or token
8. Subscriber Agreements
9. Issued certificates
10. A record of Certificate re-keys

11. CRLs
12. Any data or applications necessary to verify an archive's contents
13. Compliance auditor reports
14. Any changes to the Issuer CA's audit parameters
15. Any attempt to delete or modify audit logs
16. Key generation (excluding session keys)
17. Access to Private Keys for key recovery purposes
18. Changes to trusted public keys
19. Export of Private Keys
20. Approval or rejection of a Certificate status change request
21. Appointment of an individual to a Trusted Role
22. Destruction of a cryptographic module
23. Certificate compromise notifications
24. Remedial action taken as a result of violations of physical security
25. Violations of the CPS or CP.

### 5.5.2 Retention Period for Archive

CA archives are kept for a minimum of seven years and six months.

### 5.5.3 Protection of Archive

All archive data is backed-up daily and stored in an offsite facility. All back-ups are encrypted in transit and at rest.

### 5.5.4 Archive Backup Procedures

The entire image of the production servers containing all MedAllies CA and RA operational artifacts (i.e., Certificates, keys, CRLs, CP, etc.,) is backed-up weekly and stored on redundant live media and tape media in a safe, remote location. Incremental back-ups of the directories containing the CA and RA data are performed daily, and stored on redundant live media and tape media in a safe, remote location. Contractual information (i.e. Business Associate Agreements, Subscriber Agreement, etc.,) is stored in a secure, private folder in the MedAllies enterprise environment and backed up each weekday to redundant live media and disc media in a safe, remote location.

### 5.5.5 Requirements for Time-Stamping of Records

CA archive records are automatically time-stamped using a trusted time service, as they are created. The MedAllies CA runs a local Network Time Protocol (NTP) server that automatically syncs to a trusted NIST.gov NTP server.

### 5.5.6 Archive Collection System (Internal vs. External)

See section 5.5.4.

### 5.5.7 Procedures to Obtain & Verify Archive Information

See section 5.5.4.

## 5.6 Key Changeover

The MedAllies CA will not issue Subscriber Certificates that extend beyond the expiration date of its' own CA certificates and public keys.

The MedAllies CA operator may choose to minimize risk to the PKI through compromised CA keys, the CA private keys may be changed more frequently, and only the new key will be used for Certificate signing purposes from that time. The older, but still valid, Certificate is available to verify old signatures until all of the Subscriber Certificates signed under it have also expired. If the old private key is used to sign CRLs that contain Certificates signed with that key, then the old key is retained and protected.

The CA self-signed root Certificate is valid for no more than 20 years.

## 5.7 Compromise and Disaster Recovery

### 5.7.1 Incident and Compromise Handling Procedures

If a hacking attempt or other form of potential compromise of the MedAllies CA becomes known, it is investigated in order to determine the nature and the degree of damage. If the CA key is suspected of compromise, the procedures outlined in section 5.7.3 are followed. Otherwise the scope of potential damage is assessed in order to determine if the CA needs to be rebuilt, only some Certificates need to be revoked, and/or the CA key needs to be declared compromised.

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

The MedAllies CA maintains back-up copies of system, databases, and private keys in order to rebuild the CA capability in case of software and/or data corruption. Prior to resuming operations, the CA ensures that the system's integrity has been restored.

### 5.7.3 Entity Private Key Compromise Procedures

If the CA key is compromised, the trusted CA Certificate is removed from each Relying Party application, and a new one is distributed via secure out-of-band mechanisms.

### 5.7.4 Business Continuity Capabilities after a Disaster

In the case of a disaster in which the CA equipment is damaged and inoperative, the CA operations is re-established as quickly as possible, giving priority to the ability to revoke Subscriber's Certificates. If the CA cannot re-establish revocation capabilities prior to the next update field in the latest CRL issued by the CA, then the SSC decides whether to declare the CA private signing key as compromised, and reestablish the CA keys and Certificates and all Subscriber Certificates, or allow additional time for re-establishment of the CA's revocation capability.

In the case of a disaster whereby the CA installation is physically damaged and copies of the CA signature key are destroyed as a result, the CA will be completely rebuilt using redundant copies stored in a geographically remote location. The aforementioned procedure will be followed.

## 5.8 CA and RA Termination

In the event the MedAllies CA termination, Certificates signed by it are revoked.

# 6 Technical Security Controls

## 6.1 Key Pair Generation and Installation

### 6.1.1 Key Pair Generation

#### 6.1.1.1 CA Key Pair Generation

The CA cryptographic keying material used to sign Certificates or CRLs are generated on tamper-proof hardware secure modules.

#### 6.1.1.2 Subscriber Key Pair Generation

The CA cryptographic keying material generated for Subscriber Certificates are created on physically secure hardware that rated at a Federal Information Processing Standard (FIPS) 140-2 level 2.

### 6.1.2 Private Key Delivery to Subscriber

Private keys are not delivered to the Subscriber.

### 6.1.3 Public Key Delivery to Certificate Issuer

Public keys that are contained in Direct Certificates are delivered to the MedAllies HISP and publish in Lightweight Directory Access Protocol (LDAP) or Domain Network System (DNS). Public keys in Secure Socket Layer (SSL) Certificates are delivered to the client via email or FTP.

### 6.1.4 CA Public Key Delivery to Relying Parties

MedAllies delivers its public CA Certificates to a repository accessible via the Authority Information Access (AIA) link in its leaf certificates, commonly known as end-entity certificate.

### 6.1.5 Key Sizes

The MedAllies CA generates and uses the following keys, signature algorithms, and hash algorithms for signing Certificates, CRLs, and Certificate status server responses:

Minimum 2048-bit Rivest–Shamir–Adleman (RSA) Key with Secure Hash Algorithm version 2 (SHA-256)

The MedAllies CA only issues end-entity Certificates that contain at least 2048-bit public keys for RSA, Digital Signature Algorithm (DSA), or Diffie-Hellman.

The MedAllies CA may require larger key sizes at its sole discretion.

### 6.1.6 Public Key Parameters Generation and Quality Checking

The MedAllies CA generates public keys via a FIPS 140-2 certified cryptographic library.

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

MedAllies Direct Subscriber public keys that are bound into Certificates are certified for use in signing and encryption of S/MIME packages as required by the DirectTrust. Specifically, Subscriber Certificates assert the following key usage bits:

- digitalSignature
- keyEncipherment

Subscriber Direct Certificates that are held by the HISP do not assert the non-repudiation bit.

Subscriber Certificates assert a basicConstraints of *CA:FALSE*. And also assert an extended key usage not in conflict with the Certificate primary key usage.

The MedAllies Direct root certificate asserts the following key usage bits:

- cRLSign
- digitalSignature
- keyCertSign

The MedAllies Direct CA Certificates also asserts 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 modules are validated to at least the equivalent of the FIPS-140 level identified below for the relevant party:

| | |
|---|---|
| CA | Level 2 |
| RA | Level 1 |
| Custodian (e.g. HISP) | Level 2 |
| Subscriber | Level 1 |

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

Private key control for the MedAllies HSM is 2 out of 5.

### 6.2.3 Private Key Escrow

Private keys (CA or Subscriber) are not escrowed.

### 6.2.4 Private Key Backup

The MedAllies Direct CA private signature key is backed up to a secure offsite location to facilitate disaster recovery. See section 5.7.4.

### 6.2.5 Private Key Archival

MedAllies does not archive private keys.

### 6.2.6 Private Key Transfer into or from a Cryptographic Module

CA private keys live inside the HSM and are never exported. They can be cloned only under the HSM manufacturer's certified procedures. Leaf certificate private keys are wrapped and exported. Wrapped keys are submitted for cryptographic functions inside the HSM. The HSM erases them after usage.

### 6.2.7 Private Key Storage on Cryptographic Module

CA private keys are stored in a cryptographic module that meets the requirements of section 6.2.1. Leaf certificates are wrapped by the cryptographic module and stored in a database.

### 6.2.8 Method of Activating Private Keys

The MedAllies CA activates its Private Keys in accordance with the specifications of its installed cryptographic module manufacturer.

### 6.2.9 Methods of Deactivating Private Keys

MedAllies CA does not deactivate private keys.

### 6.2.10 Method of Destroying Private Keys

Individuals in Trusted Roles destroy their private keys when they are no longer needed.

Subscriber private keys are destroyed when they are no longer needed, or when the Certificates to which they correspond expire or are revoked.

### 6.2.11 Cryptographic Module Rating

See section 6.2.1.

## 6.3 Other Aspects of Key Management

### 6.3.1 Public Key Archival

Public keys are backed-up as part of routine data back-up process. There is no separate archive.

### 6.3.2 Certificate Operational Periods/Key Usage Periods

The MedAllies Direct root private key is valid for a maximum of 20 years. The subordinate issuing CAs private key is valid for a maximum of 20 years and they do not exceed the life

of the root CA. Subscriber private keys can be used for a maximum of 9 years. Subscriber public Certificates expire after a maximum of 3 years.

## 6.4 Activation Data

### 6.4.1 Activation Data Generation and Installation

MedAllies' activation process requires secure Administrator access to the activation server at MedAllies. The Administrator may be an employee or a Trusted Agent of MedAllies. The process requires role-based authentication to the system. The data is generated by the RA and securely transmitted to the CA via the Administrator or the Trusted Agent.

### 6.4.2 Activation Data Protection

Private keys for leaf certificates are wrapped by a FIPS 140-2 level 2 HSM and exported to a secure database. Private keys for the issuing CAs and root CA are not exportable from the HSM.

### 6.4.3 Other Aspects of Activation Data

Not applicable.

## 6.5 Computer Security Controls

### 6.5.1 Specific Computer Security Technical Requirements

The MedAllies CA shall secure its systems, authenticate, and protect communications between its systems and Trusted Roles. MedAllies servers and support workstations run on trustworthy systems that are configured and hardened using industry best practices. MedAllies scans all systems for malicious codes and protects against spyware. Malware, and viruses.

The MedAllies CA configures its CA systems, including any remote workstations, 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.

The MedAllies CA authenticates and protects all communications between a Trusted Role and its CA system.

### 6.5.2 Computer Security Rating

Not applicable.

## 6.6 Life-Cycle Security Controls

### 6.6.1 System Development Controls

CA software is developed or obtained from a vendor and placed in a controlled development environment with modern source code version control. All CA hardware and software is dedicated to performing CA tasks. CA hardware and software containing private keys are protected in HSMs. Hardware and software updates are developed and tested locally, delivered to the version control system. It is then published from the version control system to the QA environment where user acceptance testing is completed. Final versions are then published from the version control system to the production system.

### 6.6.2 Security Management Controls

The configuration of the CA system as well as any modifications and upgrades are documented and controlled through a version control system. A formal configuration management methodology is used for installation and ongoing maintenance of the CA system.

### 6.6.3 Life Cycle Security Ratings

Not applicable.

## 6.7 Network Security Controls

Information transferred from the CA is done through secure networks. The CA employs appropriate security measures to ensure it is guarded against denial of service and intrusion attacks.

## 6.8 Time Stamping

All system clock time for the CA system is derived from NIST public NTP servers. Asserted times are accurate to within three seconds.

# 7 Certificate, CRL, and OCSP Profiles Format

## 7.1 Certificate Profile

The MedAllies CA issues Certificates in accordance with approved DirectTrust Certificate Profiles corresponding to the active DirectTrust CP.

### 7.1.1 Version Numbers

The MedAllies CA issues only X.509 v3 certificates, which means the version field contains the integer 2.

### 7.1.2 Certificate Extensions

The MedAllies CA uses standard certificate extensions that are compliant with IETF RFC 5280. The Key Usage, Extended Key Usage, and Basic Constraints extensions are populated as specified in section 6.1.7. The CRL Distribution Points extension is populated with a CRL Uniform Resoure Locator (URL) as specified in section 2.2.1. The AIA extension may be populated with an OCSP Responder location as specified in section 2.2.1. The Subject Alternative Name extension is populated as specified in section 3.1.1. The Certificate Policies extension is populated as defined in section 7.1.6.

### 7.1.3 Algorithm Object Identifiers

End Entity Certificates signed by the MedAllies CA 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 the MedAllies CA 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

See section 3.1.1.

### 7.1.5 Name Constraints

No constraints other than those specified in section 3.1.

### 7.1.6 Certificate Policy Object Identifier

Certificates shall assert at least one of the policy OIDs in section 1.2 of the CP.

### 7.1.7 Usage of Policy Constraints Extension

MedAllies may add policy constraints as OIDs in the Certificate.

### 7.1.8 Policy Qualifiers Syntax and Semantic

MedAllies may add policy constraints as OIDs in the Certificate.

### 7.1.9 Processing Semantics for the Critical Certificate Policy Extension

The *certificatePolicies* extension may or may not be set to critical. Relying Parties whose client software does not process this extension risk using certificates inappropriately.

## 7.2 CRL Profile

The MedAllies CA generates CRLs in accordance with approved CRL profiles. See section 7.1.

### 7.2.1 Version Numbers

The MedAllies CA issues X.509 version 2 CRLs, which means the version field contains the integer 1.

### 7.2.2 CRL and CRL Entry Extensions

The MedAllies CA conforms to the CRL and CRL Extensions profile defined in IETF RFC 5280.

The MedAllies CA signs the CRL using the SHA-256 signature algorithm and identifies it using the following OID:

sha256WithRSAEncryption: {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}

The CRL contains a CRL Reason Code entry extension for each entry.

## 7.3 OCSP Profile

The MedAllies CA deploys an OCSP responder. The OCSP generates signed responses compliant with RFC 5280.

# 8 Compliance Audits and Other Assessments

MedAllies goes through an annual HITRUST privacy and security audit. The HISP, CA, and RA Accreditation are performed by DirectTrust every two years.

## 8.1 Frequency and Circumstances of Assessment

MedAllies goes through an annual HITRUST privacy and security audit. The HISP, CA, and RA Accreditation are performed by DirectTrust every two years.

## 8.2 Identity/Qualifications of Assessor

Qualified and certified third parties are responsible for the qualifications of the assessor.

## 8.3 Assessor's Relationship to Assessed Entity

MedAllies is a member of DirectTrust, which may perform a portion of the audits.

## 8.4 Topics Covered by Assessment

The DirectTrust Accreditation program certifies the compliance of CAs, RAs, and Custodians (e.g. HISPs), The Accreditation program outlines the topics covered by assessment.

## 8.5 Actions Taken as a Result of Deficiency

The MedAllies CA is not granted the right to claim conformance with reference to this CP unless they are in full compliance with the provisions and requirements of the DirectTrust CP.

## 8.6 Communication of Results

DirectTrust provides a web page or other appropriate means for the MedAllies CA to report the status/results of the compliance assessment and audit process or to reference a location where such reports are available.

# 9 Other Business and Legal Matters

## 9.1 Fees

### 9.1.1 Certificate Issuance/Renewal Fees

MedAllies charges subscriber fees detailed in the Master Services Agreement. MedAllies retains its right to make changes in its fees. MedAllies customers will receive proper notices of price amendments as detailed in their relevant customer agreement.

### 9.1.2 Certificate Access Fees

Not applicable.

### 9.1.3 Revocation or Status Information Access Fee

Not applicable.

### 9.1.4 Fees for other Services

MedAllies provides other services as part of its ongoing business. Pricing is negotiated.

### 9.1.5 Refund Policy

Refund policies are detailed in the Services agreements.

## 9.2 Financial Responsibility

### 9.2.1 Insurance Coverage

Carrier: Sentinel Insurance Company Ltd
Type: General Liability, Automobile Liability, Umbrella Liability
Carrier: Travelers Excess & Surplus Lines Company
Type: Technology E&O Liability

### 9.2.2 Other Assets

Not applicable.

### 9.2.3 Insurance/Warranty Coverage for End-Entities

Subscriber should refer to their individual customer agreement for details.

## 9.3 Confidentiality of Business Information

### 9.3.1 Scope of Confidential Information

MedAllies keeps the following information confidential and maintains reasonable controls to prevent the exposure of such records to non-trusted personnel.

- All private keys
- Any activate data use to active private keys or gain access to the CA system
- Any business continuity, business response, and business disaster recovery plans
- Any security practices, measures, mechanisms, procedures or plans used to protect the confidentiality, integrity, or availability of information
- Any information held by MedAllies in accordance with section 9.4
- Any transaction, audit log, and archive log identified in section 5.4 or 5.5
- Transaction records, financial audit records, external / internal audit trail records, and audit reports.

### 9.3.2 Information not within the scope of Confidential Information

Subscriber application data identified as being published in a digital Certificate is considered public and not within the scope of confidential information. Certificate revocation data is public information and is published periodically by the MedAllies CA.

### 9.3.3 Responsibility to Protect Confidential Information

The MedAllies CA contractually obligates employees, agents, and contractors to protect confidential information. The MedAllies CA provides training to employees on how to handle confidential information.

## 9.4 Privacy of Personal Information

### 9.4.1 Privacy Plan

All identifying information for a Subscriber is protected from unauthorized disclosure. The MedAllies CA creates and follows a publicly posted privacy policy on MedAllies website (www.medallies.com) that specifies how it handles personal information.

### 9.4.2 Information Treated as Private

Information deemed as private shall be defined as such in agreements between the MedAllies CA and its Subscribers.

### 9.4.3 Information included in certificates is not deemed private.

Certificates, CRLs, and personal or corporate information appearing in them are not considered private.

### 9.4.4 Responsibility to Protect Private Information

Each party shall protect the confidentiality of private information that is in its possession, custody or control with the same degree of care that it exercises with respect to its own information of like import, but in no event less than reasonable care, and shall use appropriate safeguards and otherwise exercise reasonable precautions to prevent the unauthorized disclosure of private information.

### 9.4.5 Notice and Consent to Use Private Information

The MedAllies CA uses private information as dictated by the agreements with its Subscribers.

### 9.4.6 Disclosure Pursuant to Judicial/Administrative Process

The MedAllies CA does not disclose private information unless allowed by agreements with its Subscribers or unless required to by law.

### 9.4.7 Other Information Disclosure Circumstances

All personnel in trusted positions handle all information in strictest confidence including those requirements of US Law including protection of personal data.

## 9.5 Intellectual Property Rights

The MedAllies CA and other Business Associates each own their own intellectual property rights associated with their databases, websites, digital certificates and other publications originating from MedAllies.

## 9.6 Representations and Warranties

### 9.6.1 CA Representations and Warranties

The MedAllies CA represents and warrants that it has all the necessary licenses, authorizations and approvals to perform its obligations as detailed in the MedAllies Subscriber Agreement. The MedAllies CA will perform substantially as described in the MedAllies Certification Process Guide.

### 9.6.2 RA Representations and Warranties

The MedAllies RA, and RAs operating on behalf of MedAllies, represent and warrant they have all the necessary licenses, authorizations and approvals to perform its obligations as detailed in the MedAllies Subscriber Agreement. The MedAllies RA, and RAs operating on behalf of MedAllies will perform substantially as described in the MedAllies Certification Process Guide.

### 9.6.3 Subscriber Representations and Warranties

Each Subscriber represents to the MedAllies CA that the Subscriber:

1. Protects its Private Keys from compromise (including if employing MedAllies who uses secure processes against potential compromise),
2. Limits Users to only employees or Affiliates of the organization named in the Certificate subject,
3. Provides accurate and complete information and communication to the MedAllies CA and RA,

4. Confirms the accuracy of Certificate data prior to using the Certificate,
5. Promptly ceases using a Certificate and notifies the MedAllies CA if (i) any information that was submitted to it 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,
6. Uses the Certificate only for authorized and legal purposes, consistent with this CP and Subscriber Agreement, (including only installing device certificates on servers accessible at the domain listed in the certificate), and
7. Promptly ceases using the Certificate and related Private Key after the Certificate's expiration.

### 9.6.4 Relying Parties Representations and Warranties

A Relying Party only uses a MedAllies Certificate for the purpose for which it was intended and checks each Certificate for validity.

### 9.6.5 Representations and Warranties of Affiliated Organizations

Same as 9.6.3.

### 9.6.6 Representations and Warranties of Other Participants

Same as 9.6.4.

## 9.7 Disclaimers of Warranties

Other than the Warranties provided in the MedAllies Subscriber Agreement, the MedAllies network and all services provided by MedAllies are provided "as is" and without any warranties of any kind. All other warranties and representations with regard to the MedAllies network and the services provided by MedAllies are hereby disclaimed, including the implied warranties of the merchantability and fitness for a particular purpose. MedAllies expressly disclaims any warranty that the MedAllies network will meet requirements as detailed in the Network Connectivity Agreement or that it will operate without interruption or be error free.

## 9.8 Limitations of Liabilities

Except as otherwise expressly provided in the MedAllies Subscriber Agreement or the Vendor Network Agreement, The maximum, cumulative and aggregate monetary liability of each party for all claims and actions arising under, or relating to, the client's Agreement at any time or times, notwithstanding the form in which any such claim or action is brought and notwithstanding any failure of essential purpose that might be found or inferred herefrom, shall be limited to the total and aggregate amount of fees paid to MedAllies by vendors under this agreement during the twelve consecutive (12) months immediately preceding the events giving rise to the claim or action.

## 9.9 Indemnities

By accepting or using a Certificate, each Subscriber and Relying Party agrees to indemnify and hold MedAllies, as well as any of its respective parent companies, subsidiaries, directors, officers, employees, agents, and contractors harmless from any acts or omissions resulting in liability, any loss or damage, and any suits and expenses of any kind, including reasonable attorneys' fees, that MedAllies, and/or the above mentioned parties may incur, that are caused by the use or publication of a Certificate, and that arises from that party's: (i) misrepresentation or omission of material fact in order to obtain or use a Certificate, whether or not such misrepresentation or omission was intentional; (ii) violation of the Subscriber Agreement, Relying Party Agreement, this CPS/CP, or any applicable law; (iii) compromise or unauthorized use of a Certificate or Private Key caused by the negligence of that party and not by MedAllies (unless prior to such unauthorized use MedAllies has received an authenticated request to revoke the Certificate); or (iv) misuse of the Certificate or Private Key.

## 9.10 Term and Termination

### 9.10.1 Term

This certification practice statement becomes effective when approved through the SSC consensus process. This certification practice statement has no specified term.

### 9.10.2 Termination

This CP as amended from time to time shall remain in force until it is replaced by a new version or as otherwise terminated in accordance with this section 9.10.

### 9.10.3 Effect of Termination and Survival

The assertions made within this certification practice statement remain in effect through the end of the archive period of the last certificate issued.

## 9.11 Individual Notices and Communications with Participants

MedAllies accepts notices related to this CP by means of digitally signed messages or in paper form addressed to the locations specified in section 2.2 of this CP. Upon receipt of a valid, digitally signed acknowledgment of receipt from MedAllies, the sender of the notice shall deem their communication effective. The sender must receive such acknowledgment within five 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.

### 9.11.1 Procedure for Amendment

The SSC is responsible for approving any changes to the MedAllies CP. Any such changes shall be submitted to the Paralegal for inclusion on the next SSC quarterly agenda for

review, discussion, and approval.

### 9.11.2 Notification Mechanism and Period

The MedAllies CA is notified of a policy change by DirectTrust when an updated version is posted to the DirectTrust website. The effective data and required dates for compliance are as stated in section 1.2.

### 9.11.3 Circumstances Under Which OID Must be Changed

If a change in Certificate policy is deemed by DirectTust to be substantive, a Certificate Policy OID is changed. New OIDs may be introduced or existing OIDs modified or removed with publication of a new CP version.

## 9.12 Dispute Resolution Provisions

Before resorting to any dispute resolution mechanism including adjudication or any type of Alternative Dispute Resolution (including without exception mini-trial, arbitration, mediation, umpire, binding expert's advice, co-operation monitoring and normal expert's advice) the parties agree to notify MedAllies of the dispute with a view to seek dispute resolution.

## 9.13 Governing Law

The CP shall be governed by, subject to, and interpreted in accordance with, the laws of the State of New York, without regard to any conflicts of laws provisions. The exclusive venue for all legal actions or proceedings arising out of, or related to, this CP shall be in an appropriate Federal or State court located in New York, and each Party hereby irrevocably consents to the personal and subject matter jurisdiction of such courts and waives any claim that such courts do not constitute a convenient and appropriate venue for such actions or proceedings.

## 9.14 Compliance with Applicable Law

All PKI participants are required to comply with applicable laws.

## 9.15 Miscellaneous Provisions

### 9.15.1 Entire Agreement

The headings, subheadings, and other captions in this CP are intended for convenience and reference only and shall not be used in interpreting, construing, or enforcing any of the provisions of this CP. Appendices and definitions to this CP are for all purposes an integral and binding part of the CP. If/when this CP conflicts with other rules, guidelines, or contracts, this CP shall prevail and bind the Subscriber and other parties. If there is any conflict between the sections of this CP and any other document that relate to MedAllies, then the sections benefiting MedAllies and preserving MedAllies' best interests, at MedAllies' sole determination, shall prevail and bind the applicable parties. This CP 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 the parties shall also take into account the international scope and application of the services and products of MedAllies as well as the principle of good faith as it is applied in commercial transactions.

### 9.15.2 Assignment

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

### 9.15.3 Severability

Should it be determined that one section of this CP is incorrect or invalid, the other sections of this CP shall remain in effect until the CP is updated.

### 9.15.4 Enforcement (Attorney Fees/Waiver of Rights)

MedAllies 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, no delay or omission by any party to exercise any right, remedy or power it has under this CP 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 shall not be construed to be a waiver of any other or succeeding breach or covenant. Bilateral agreements between MedAllies and the parties to this CP may contain additional provisions governing enforcement.

### 9.15.5 Force Majeure

Neither Party shall be liable or deemed in default for failure to fulfill any of its obligations under this Agreement (other than payment obligations) due to causes beyond its reasonable control. Such causes or conditions shall include, but shall not be limited to, acts of God, acts of government, fires, floods, epidemics, strikes, shortages of labor or materials, earthquakes, hurricanes, floods, electrical power failures, telecommunication or Internet outages, failure of an Internet service provider, or other similar causes beyond such Party's reasonable control.

## 9.16 Other Provisions

Notices given pursuant to the CP shall be addressed to the appropriate Party at the address as indicated in the Subscriber Agreement.