

MedAllies Service Description

Published by

MedAllies, Inc

300 Westage Business Center Drive

Suite 320

Fishkill, NY  12524

[www.medallies.com](http://www.medallies.com/)

MedAllies, Inc.

Proprietary and Confidential

This document is proprietary and confidential information of MedAllies, and may not be reproduced or distributed without the express written consent of MedAllies

# 1. Public service Description

This Service relates to MedAllies’ service known as the MedAllies Registration Authority (RA).

The MedAllies Registration Authority is an identity proofing service that verifies identity information for applicants for Levels 1-3 non-PKI authentication credentials. This Registration Authority implements the MedAllies’ Registration Policy (RP) that provides the requirements related to the identity proofing of individuals seeking level 1-3, 2-factor non-PKI identity credentials as defined under NIST Special Publication 800-63, the Kantara Identity Assurance Framework and the US federal Identity Credentialing and Access Management (FICAM) programs. The proofing performed by the RA is done to verify to the maximum feasible extent in accordance with NIST and FICAM requirements that the individual seeking a credential is actually the person they purport to be. The MedAllies RA works as a partner with other contracted service components (token managers) as part of a full service credential service provider (CSP).

The MedAllies RA operates under the provisions of the MedAllies Registration Policy, V1.0 and the MedAllies Registration Practices Statement, V1.0.

## 1.1 Features and Functions

The RA operates a face to face identity proofing process using trusted agents (TA) designated and trained by MedAllies to verify identities under the MedAllies RP. TAs are employees of MedAllies clients located at client facilities who meet in a face-to-face setting with applicants for credentials and verify their identities by viewing and verifying identity documents. The verified data is then provided to the MedAllies Registration authority that approves the documentation and notifies the token manager that the credential may be issued to the approved applicant.

### 1.2 Intended classes of users

The users of the MedAllies RA include:

 client organization applicants for credentials/Subscribers;

 client TAs;

 the MedAllies RA;

 contracted token managers.

### 1.3 Tasks and usage

The MedAllies RA conducts identity proofing for client-sponsored applicants for non-PKI authentication credentials. Designated and trained TAs perform the actual verification by matching proffered identity documents to the applicants during a face-to-face meeting. The TA collects required data from the offered documents and forwards required data to the RA who reviews the data and approves the application for credential. The TA maintains required data in its repository for the required period of time as directed by the RP.

### 1.4 Checks performed on supplied data

The RA/TA shall inspect the photo-ID, compare picture to Applicant, and record ID number, address and date of birth (DOB). If the photo ID appears valid and the photo matches Applicant and if the ID confirms the address of record, the RA authorizes the CSP shall issue credentials and notice shall be sent to the address of record; OR if ID does not confirm address of record, the CSP shall issue credentials in a manner that confirms the claimed address.
The ID may also be established remotely by verifying information provided by applicant including ID number and account number through record checks either with the applicable agency or institution or through credit bureaus or similar databases.

In both person to person and remote processes the TA/RA shall confirm that: name, Date of Birth (DoB), address and other personal information in records are consistent with the application and sufficient to identify a unique individual.

### 1.5 Applicable restrictions and User characteristics

Applicant’s for credentials must be employees of, or otherwise contractually bound parties to, MedAllies clients.

### 1.6 Nature of User agreements

User agreements are within the purview of the issuing credential service provider/token manager

## 2 Service Topology

The following diagram shows the topology of the MedAllies RA system.

##

## 2.1 Service Platform

**Service Production Inventory List**

 **Hardware**

Dell PowerEdge R720 Server

Dell PowerEdge 1950 Server

Brocade ICX6430-24 Switch

F5 BigIP 2000 Load Balancer

45Drives Storinator S45

Dell PowerVault MD3220i iSCSI Direct Attached Storage

Dell PowerVault MD1200 Direct Attached Storage

BAE Network Security Appliance

Cisco ASA 5510 Firewall

Luna SA 1700 HSM

**Software**

VMware vSphere/vCenter 5.5

Microsoft Windows Server 2008 R2 Datacenter Edition

MySQL 5.7

Java 1.6u25

James Mail Server 3.0

                Apache Tomcat 7.0.22

ESET Endpoint Fileserver 4.5

Nakivo Backup and Replication 5.9

Red Hat Enterprise Linux 6.4

CentOS Linux 6.6
OpenSSL 1.0.0-fips 29 Mar 2010

# 3. Maintenance and of Personally Identifiable Information (PII)

The MedAllies RA operates two geographically dispersed mirror image sites (ref Section 2.3). The system operates in a high availability hot/hot mode with load balancing and instant failover capability.

The information collected during identity verification falls under the definition of PII and requires protection and archival to comply with the requirements of SP 800-63-2, the FBCA CP, and Kantara IAF. In the case of the RA, all data is replicated to both operating locations in near-real-time. Data is encrypted during transmittal and while at rest in the separate databases. In compliance with the noted references, MedAllies and client LRA/TAs maintain data for at least seven and one-half years post credential expiration or revocation.

# 4. Assessors Service Definition

The MedAllies RA provides assurance level 2 and 3 identity proofing services to applicants for identity credentials that are sponsored by MedAllies clients. Identity proofing is currently performed using face to face meetings between the applicants and local registration agents/trusted agents (LRA/TA) who are credential holding employees of MedAllies clients. These personnel are first identity proofed by the MedAllies Registration Agent and trained by MedAllies to perform identity proofing for their sponsored employees and contractors. MedAllies may, in the future, employ a remote proofing process as yet to be designed. The MedAllies RA operates as a component service with a token manager as part of a full service credential service provider. Client entities that provide LRA/TAs are contractually bound to operate according to the MedAllies Registration Policy and Registration Practices Statement. Both documents have been provided to the MedAllies Assessor.