



**emAS**

# emAS Identity and Access Management System

## A Feature Packed IAM Solutions that Enables Digital Trust

We've all heard of IAM's and their importance in maintaining security in your organization. However, we felt that they were inadequate or often needed to plug into different systems for Multi-factor authentication to enable secure sign on. So we created emAS - IAM

### Sophisticated Multifactor Authentication Engine

emAS IAM comes with the ability to authenticate 15+ forms of authentication right up from Advanced Password and Crypto Token/Digital Signature based authentication to Facial, Grid, Behavioral Analytics and QR Code based authentication. Authentication is an important part of security in an IAM so we wanted to ensure nothing is lacking on this end.

### Web Single Sign On with App Dashboard

emAS IAM supports Single Sign On through common protocols such as SAML, OAuth, AD, LDAP with manual or auto provisioning functionality.

### End-to-end Access Management

In emAS IAM, access request workflows can be defined based on the application and resources. Even multi-level approval based access request workflows can be defined where in multiple users (authorized to approve/reject the request) are required to approve the request.

#### Product Benefits

- End-to-end security
- Cost effective deployment supported by one line API integration
- Super-fast processing of authentication requests
- Platform agnostic – easily deployed or migrated across Solaris/Window server/Red Hat Enterprise/ Linux/AI
- Ability to provide managed services
- Mobility enabled for leveraging mobile authentication options
- Acceptance of global CA certificates for Digital Signature Certificate & Public Key Infrastructure based authentication
- Built for the future with FIDO Compliance measures

## Standards Compliant, User Friendly and Easily Deployable IAM System

emAS IAM conforms with all the global standards around Single Sign On, Multi-factor Authentication & PKI. It is extremely user friendly with a quicker than average deployment time and is perhaps one of the few IAM systems with PKI functionality.

### Adaptive Authentication Framework Using Risk Weights and Anomaly Detection

emAS IAM combines state-of-the-art analytics and risk-based authentication technologies to measure the risk associated with a user's login and post-login activities and prompt for additional identity assurance in scenarios that are deemed high risk and/or in violation of rules established by your organization.

### Automated User Provisioning Using LDAP/AD

emAS IAM supports internal and external user provisioning using LDAP/AD. Further, there is the option to enable auto-provisioning where the system will automate the user provisioning entirely. For manual provisioning, users can bulk upload data or go one by one (for smaller organizations).

### Advanced Reporting

emAS IAM supports creation and automation of many reports and extraction of historic data. The reporting module allows role based access to view or edit/create reports.

#### Success Stories

A new age public sector bank offering a broad array of financial products used eMudhra's MFA powered Identity and Access Management solution to mitigate risks involved in supporting alternate banking channels.

"We have been able to take the lead in implementing digital signature enabled strong authentication to provide comprehensive security as well as seamless customer experience, thanks to eMudhra's support."

— **Deputy General Manager, New Age Public Sector Bank**

## Technical Details

### ■ Recommended Hardware

- Processor: 2 \* Quad Core Processors
- RAM: 16 GB
- HDD: 500 GB SAS HDD

### ■ OS Compatibility

- Microsoft Windows 7 x64, 10 x64; Windows Server 2008 R2 x64, 2012 R2 x64, 2016 x64
- Red Hat Enterprise Linux AS/ES 6 x64, 6 x86, 7 x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64
- Oracle Solaris 11 (SPARC), Oracle Solaris 11 x64
- IBM AIX 7.1 (POWER6, POWER8), HP-UX 11i v3
- Oracle Enterprise Linux 6.8 x64 and 7.1 x64

### ■ Single Sign On Protocols

OAuth, SAML, True SSO, Federated SSO

### ■ User Provisioning Methods

Manual user provisioning, auto provisioning, de-provisioning, re-provisioning

### ■ Authentication Mode

SMS OTP, APP OTP, eOTP, QR Code, Digital Signature, 2FA, knowledge based, grid based, smart card, token based, tOTP, Adaptive authentication, biometric, IRIS, parameter based MFA, FIDO U2F

### ■ Access Management

Resource level, Application Level

### ■ Encryption

User data storage encrypted (AES 256)

### ■ Appserver Supported

Apache Tomcat 7+, JBoss 7+, Web Sphere 8+, Web Logic 12+

### ■ Log Management

SIEM Integration supported, en-suite log management

## Modules

### ■ User Creation Engine

Handles user management including user creation and approval workflow for user entitlement

### ■ User Authentication

15+ modes of authentication + SSO supported

### ■ Policy Enforcement

Set resource/app specific policy, define policy matrix, monitor violations, set policy for blocking attempts

### ■ Credential Management

2FA, MFA, admin/user based enrollment, user change/reset password

### ■ Workflow Management

Prevent policy violations, allow 'request for access' requests, rapid deployment with custom applications

### ■ Session Management

Manage multiple application sessions

## About eMudhra:

Much like the name, which is an embodiment of the seal of authenticity in the electronic or digital world, eMudhra is a cyber security solutions company and a trust service provider that is focused on accelerating the world's transition to a secure integrated digital society. With presence in 5 continents and a global delivery center in Bengaluru, India, eMudhra is empowering secure digital transformation of over 45 global banks, several Fortune 100 customers and thousands of SMEs.

