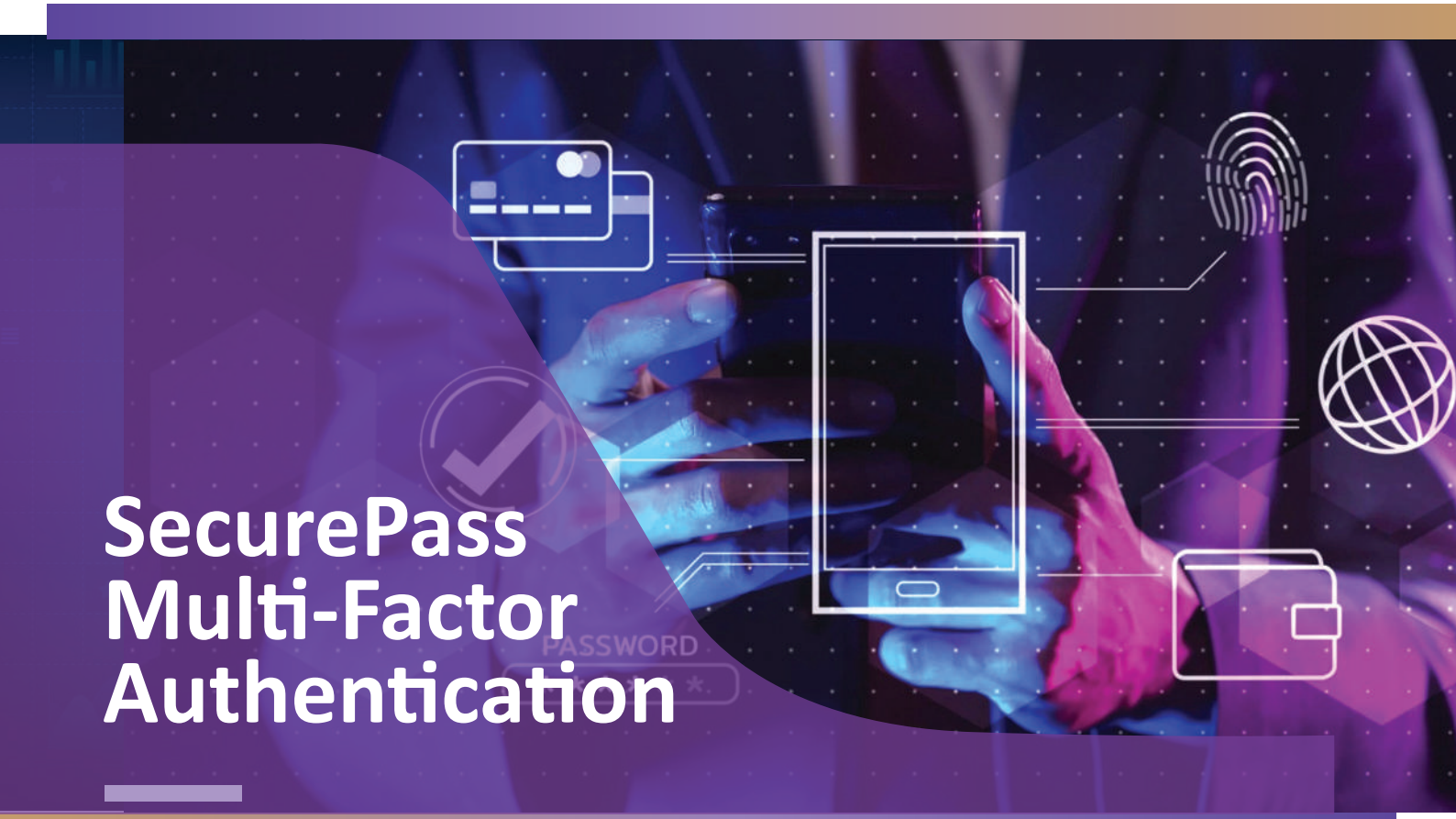
emudhra
Trust Delivered



SecurePass Multi-Factor Authentication

Conventional, credential-based approach for user authentication can only take you so far. It is time to combat security risks with an adaptive approach to risk management using CARTA (Continuous Adaptive Risk and Trust Assessment).

With malware, ransomware and other cyber threats constantly thrown at Enterprises, a holistic security platform is required to securely enable digital identity and transaction management. eMudhra's flagship product eMudhra Authentication Server has been empowering millions of users securely manage their online identity and authentication needs by offering a single holistic security perspective!

Trusted by several large Banks, SecurePass offers a host of strong authentication options that help Enterprises secure physical, mobile, logical access to applications.

15 Factors of Authentication

SecurePass supports 15 factors of authentication - from Digital Certificates, OTP and Biometric factors of authentication to adaptive analytics driven by behavioral insights into how users login.

Risk Based Parameter Definition

SecurePass gives you the flexibility to define the type and layers of authentication based on an individual user risk profile. Risk parameter definition is flexible and can be dependent on a single or a cumulative measure of multiple parameters. SecurePass can also work with any existing system to pull the risk score and invoke relevant authentication layer(s).

fido ALLIANCE MEMBER
CAB CA/BROWSER FORUM
Webtrust Accredited
AATL
CLOUD SIGNATURE CONSORTIUM
Asia PKI Consortium

SecurePass addresses the need of the hour – Mitigating risk for Enterprise and it's end users while keeping it simple

Threats are Multi-Channel

With customers, employees, suppliers accessing applications across web, desktop, mobile and cloud, enterprises have to constantly worry about newer threat dimensions. SecurePass's behavioral analytics module runs machine learning algorithms to detect anomalies and put in place risk mitigation measures.

Cloud Applications Add a New Dimension

With the explosion of cloud offerings and hosting providers and sensitive data on cloud, security officers have to constantly think about how to protect authentication on the cloud. SecurePass's plug and play architecture allows quick addition of newer platforms and factors of authentication.

Ensure Legal Non-Repudiation Using PKI

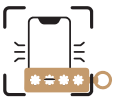
Plain username/passwords & OTPs are today most vulnerable for cyber-attack. SecurePass offers the ability to attach users to a risk profile to allow creation of trusted networks using Public Key Infrastructure offering strongest form of protection to enterprises and its customers.

Behavioral Risk Parameter Detection

SecurePass MFA can be paired with SecurePass Adaptive to build a behavioral model around user-login to provoke authentication layers in line with real-time adjusted risk profile..

Different types of Authentication


Username/ Password


Mobile Soft Token


Digital Signatures – Crypto Token/


Web Token Mob


See What you Sign – SWYS Key


Mobile APP Token


Smart Card


Hardware Token


Bluetooth Token


Grid Card


Mobile Device Certificates


QR Code


Knowledge Based


Biometrics IRIS


Behavioral (uses Anomaly Detection based on Machine Learning)


Face Recognition


Biometrics Fingerprints

emudhra
Trust Delivered

Success Stories

A leading bank with over 16 million customers used our MFA solution to provide comprehensive security across various banking channels including Internet Banking, ATM, Mobile Banking and Treasury

The Result:

Authentication throughput at 7 milliseconds
Savings by replacing hardware tokens by
Near zero fraud reported on digital channels

Product Benefits

Ultra-fast processing of authentication requests

Cost effective deployment of strong authentication across Enterprise

Mobility enabled for leveraging mobile authentication options

Acceptance of global CA certificates for Digital Signature Certificate & Public Key Infrastructure based authentication

Platform agnostic – deployed across Solaris/ Windows Server/ Red Hat Linux/ IBM AIX

Built for the future with FIDO Compliance measures

Technical Specifications

- **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, 7x64; SUSE Enterprise Linux 11 x64 SP2, 12 x64
  Oracle Solaris 11 (SPARC), Oracle Solaris 11x64
  IBM AIX 7.1 (POWER6, POWER8), HP-UX 11i v3
  Oracle Enterprise Linux 6.8 x64 and 7.1 x64

- **DB Compatibility**
  Oracle 10g+, SQL Server 2008+,
  MySQL 5+, DB2 9+, Postgre 9+

- **App Server**
  Apache Tomcat 7+, JBoss 7+, Web Sphere 8+, Web Logic 12+

- **Web Services**
  SOAP, REST

  Protocols
  LDAP, SMPP, HTTP, HTTPS, FTP, WSS, OAuth 2.0, JWT, U2F, EST

- **Java**
  Oracle JDK 1.7+

- **Key Features**
  - Online/Offline CRL Verification
  - User Management
  - Signer Component
  - Self-registration portal
  - Configuration Module
  - Tamper proof logging
  - Advanced Reporting
  - Back office admin module with dashboard

About eMudhra

eMudhra, a global provider of digital identity and cybersecurity solutions, specializes in digital signature certificates, Public Key Infrastructure (PKI) services, and robust authentication protocols. Our impactful presence in India and international presence have allowed us to support governments and enterprises in safeguarding their digital transactions and vital information.

eMudhra offers digital certificates, PKI-based solutions, authentication and identity governance services. With a strong presence in India and a global footprint, eMudhra helps organizations securely manage their digital transactions and protect sensitive information. Being a leading digital identity and cybersecurity solutions provider, eMudhra is now focused on futureproofing cybersecurity using Post Quantum Ready Cryptography and Zero-Trust Identity Governance model.