



eMudhra Vulnerability Management Process

Copyright

Copyright © eMudhra Limited. All rights reserved. The information in this document is for the use of intended customer of eMudhra and exclusively for the purpose of the agreement under which the document is submitted. No part of it may be reproduced or transmitted in any form or means without the prior written permission of eMudhra. The document has been prepared to be used by professionals and trained personnel, and the customer assumes full responsibility when using it.

This document and the product it describes are considered protected by copyright according to the applicable laws.

Disclaimer

The information or statements given in this document concerning the suitability, capacity, or performance of the mentioned hardware or software products cannot be considered binding but shall be defined in the agreement made between eMudhra and the customer. However, eMudhra has made all reasonable efforts to ensure that the instructions contained in the document are adequate and free of material errors and omissions. eMudhra will, if necessary, explain issues, which may not be covered by the document.

Feedback

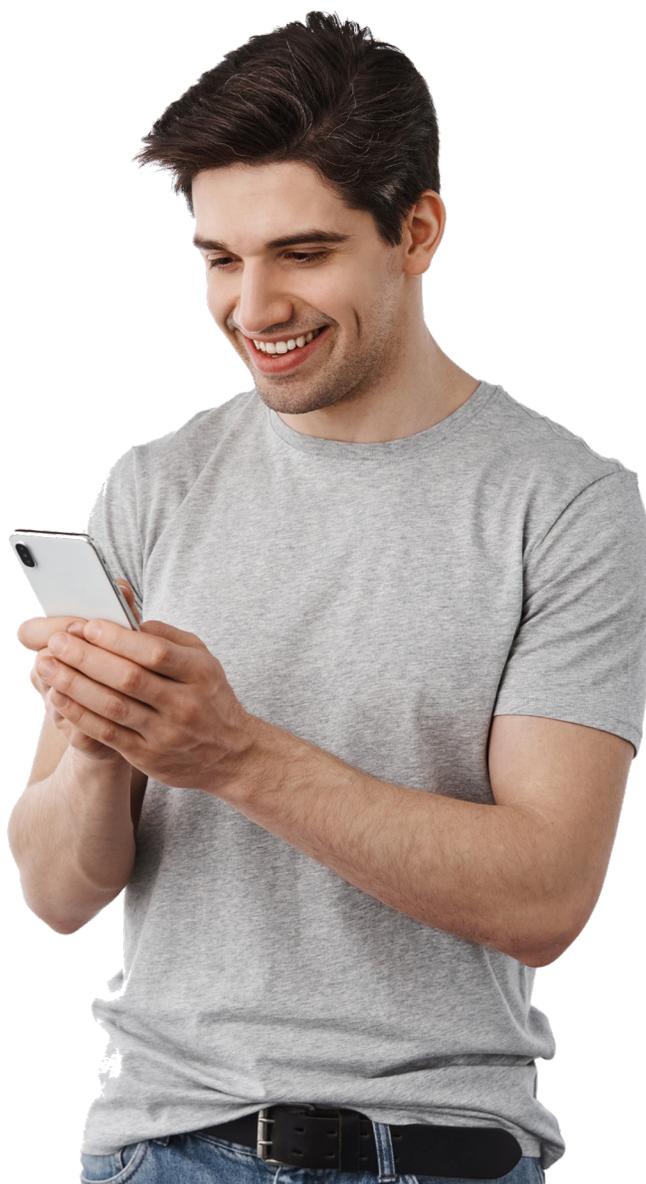
eMudhra welcomes customer comments as a part of the process of continuous development and improvement of the documentation.

Trademarks and Registered Trademarks

Products and product names mentioned in this document may be trademarks or registered trademarks of their individual proprietors.

Table of Contents

Safeguard Your Interests!	4
eMudhra's Vulnerability Management Program	5
Conclusion	8



Safeguard Your Interests!

At eMudhra, we firmly believe that delivering Trust is a full-time job and not a part-time practice! emSigner's security policies have been designed to offer highest level of assurance to its users. Built in industry leading infrastructure and designed with best-in-class security features, emSigner's platforms are rigorously audited to protect customer data.

emSigner's security program is built on the following core principles-



Deliver Trust

We have over 10 years of experience in operating as a trust service provider in global markets. Leveraging this experience and expertise, we deliver trust across consumer and enterprise facing applications.



Cutting Edge Technology to Power Security

emSigner's technology stack uses industry leading techniques in cryptography, latest systems that guard end-points along with a host of security measures at application, network, and database levels to protect sensitive data. This is backed up by round-the-clock monitoring, logging, and continuous training & awareness programs.

eMudhra's Vulnerability Management Program

eMudhra conducts systematic review of security weaknesses in information systems or applications. It evaluates if the system or application is susceptible to any known vulnerabilities, assigns severity levels to those vulnerabilities, and recommends remediation or mitigation, if and whenever needed.

Vulnerability can be a security exposure in an operating system or other system software or application software component including, but not limited to: missing operating system and application patches, inappropriately installed or active applications and services, software flaws and exploits, misconfigurations in systems, etc.

This document establishes the rules for the review, evaluation, application, and verification of system updates to mitigate vulnerabilities in the IT environment/application and the risks associated with them.



Assessment Type

eMudhra follows the Open Web Application Security Project (OWASP) standard — an established standard in application security methodology — for application security. OWASP is a worldwide free and open community focused on improving the security of application software. OWASP's mission is to make application security "visible," so that people and organizations can make informed decisions about application security risks.

We employ third-party security tools to unceasingly and dynamically scan our core applications against common web application security risks, including, but not limited to the OWASP Top 10 security risks.



Scanning Frequency

- Periodic or continuous vulnerability assessment scanning of all supporting assets in the eMudhra Network will be performed by the endpoint security solution
- Application level internal vulnerability assessment will be conducted before every release
- Failed vulnerability scan results rated at Critical or High level will be remediated and re-scanned until all Critical and High risks are resolved
- Any evidence of a compromised or exploited Information Resource found during vulnerability scanning will be reported to the product team for remediation

Penetration Testing

- External and internal penetration testing will be performed on a scheduled basis. The purpose of a penetration test is to verify that the security controls protecting eMudhra assets are working properly
- Testing will also consist of network and application-layer penetration tests
- The Security team will provide the results of penetration tests in detailed reports to the security team constituted by CISO





Remediation

A remediation plan will be developed and implemented for each scanned results. The plan will outline roles, responsibilities and deadlines for remediation. The IT manager will assign appropriate resources to address any vulnerability recommended for remediation by IT security team



Conclusion

eMudhra strives to ensure that emSigner is a product which is devoid of any vulnerabilities by rigorously testing emSigner and the hosting infrastructure. This ensures that the customers data is always protected, which means that all our customers can rest easy.

eMail: support@emsigner.com

Web: www.emsigner.com



About eMudhra

As the world goes Digital, security is ever more crucial to protect identities, data, and enable trust in a digital society. eMudhra focuses on SECURE Digital Transformation to enable organizations to progress and evolve without sacrificing "Trust," which matters most in our society. With an end-to-end stack around trust services, PKI, Paperless transformation, and Digital Authentication, eMudhra is optimally placed to aid digital journeys where identity assertion is critical.

eMudhra chairs the Asia PKI Consortium, is a board member of the Cloud Signature Consortium and a member of the CA Browser Forum. Having been in business for over 12 years and built a reach that spans more than 50 countries, eMudhra is deeply committed to bringing change and helping societies across not just go digital but go digital in a secure way.