



emSecure

IoT Security Platform for trusted communication



Webtrust Certified Company



9001:2008 27001:2013 20000-1:2011



Certified Company

In a connected world, where devices increasingly influence our life, security of IoT is as important as IoT itself.

It is safe to say that IT is undergoing a paradigm shift where dependability on devices is increasing drastically and we, as people are increasingly relying on 'things' directly or indirectly in our daily lives. IoT, can broadly be defined as the interconnectivity of 'smart' devices to share and execute data and commands based on specific parameters.

Sounds easy enough. There is no question that this already does and will continue to add immense value to humanity. From Smart Cities to Smart Cars, it already does. However, IoT ecosystems in the wrong hands can be equally detrimental to its stakeholders.

emSecure is eMudhra's answer to address this very problem in an effective and scalable manner. Attacks are getting more sophisticated day by day. Most of them capitalize on inadequate identification standards and loops in the authentication layer to penetrate the entire IoT ecosystem through a single rogue device. The Marai Botnet attack used factory default and reset passwords to penetrate millions of devices.

Product Benefits

- **Botnet Attacks, No more!**
We've all heard of botnet attacks causing a havoc across various IoT ecosystems with standard manufacturer passwords. With emSecure, this is no longer a worry!
- **Security at its best!**
emSecure uses PKI to issue device certificates and user certificates across an IoT ecosystem. This brings full accountability and mitigates risk of penetration since only the corresponding key of the asymmetric key pair will authenticate a request.
- **Protect your financial risk**
The cost of a breach can be compounded significantly in an IoT ecosystem. All it takes is one device to infiltrate the network and the losses subsequently, can be catastrophic on your business.
- **R&D to make life better**
eMudhra labs works with leading chip manufacturers (Infineon, etc) to solve the IoT gap at the manufacturing level itself. Everyday, we try to reduce the size of TPM's, explore long range LoRA devices, and more to ensure that our tech gets better everyday.

'Trusted' communication is an important element in a secure IoT network. PKI is the global standard of 'trust' in the digital world
PKI and Encryption Technology

emSecure uses Public Key Cryptography to digitally sign and encrypt all communication in the IoT network. By issuing device certificates and user certificates, it ensures that all data transmitted is secure and un-hackable.

Digital Signature Authentication is required and used in emSecure to protect and confirm sensor data and enforce any specific automated actions based on this data. Key provisioning, deployment and management is also part of the solution.

Hardware that supports scalability

eMudhra is working with leading manufacturers of chips, TPM's, and LoRA devices globally to really go the extra mile and ensure that our offering is complete and capable regardless of the scale of our customers' requirements.

emSecure uses trusted platform modules for the PKI, and LoRA (Wifi/4G also supported) for connectivity of devices.

Use Cases

- **Smart Cities:**
Usage of Information and Communication Technology to meet public needs and foster development in a multistakeholder environment
- **Smart Buildings:**
Offers IoT building blocks that simplify how building systems talk to the cloud and exhaustively analyze building data to uncover new business insights capable of driving real value and greater performance
- **Smart Logistics:**
Combines real-time analysis of vendors, suppliers, environmental sensors, traffic, telematics, geopolitical risk etc. to optimize operations, customer expectations and protect margins
- **Smart Parking:**
Optimizes parking space usage, improves efficiency of parking operations and helps traffic flow more freely with the next generation parking
- **Smart Lighting:**
Saves energy in modern workspaces where every light point is connected to an intelligent system that delivers high-quality, reliable illumination
- **Smart Energy:**
Gives you the platform to control and optimize energy consumption, ensuring that energy is used only when needed

Technical Details

■ Recommended hardware

Processor: 2 * Quad core Processors
RAM: 64 GB
HDD: 1 TB SAS HDD

■ Minimum hardware required

Processor: 2 * Quad core Processors
RAM: 16 GB
HDD: 500 GB SAS HDD

■ OS compatibility

Windows Server 2008+ Enterprise, RHEL 5+,
AIX 7+, Suse 12+ and Solaris 10+

■ 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+

■ Algorithms and standards

- SHA-1, SHA-2 Family, MAC, HMAC, RSA Signing, ECDSA, AES 256
- PKCS 7, X.509 v3

■ Web services

SOAP, REST

■ Protocols

SMPP, WSS

■ Java

Oracle JDK 1.7+

■ Key Modules

- Registration Module
- Certificate Life Cycle Management Module
- Auto Enrollment
- Digital signature generation Module
- Authentication Module
- Tamper proof logging
- Key Generation system
- Ability to generate key pair on Trusted Platform Module
- Encrypted Communication
- Secure Key pair storage

About eMudhra:

eMudhra is a global entity and leading trust service provider focusing on Digital Transformation and Cybersecurity initiatives. Headquartered in Bengaluru, India, eMudhra has global offices across 5 continents catering to thousands of customers across the globe. eMudhra also holds the Vice chairmanship of Asia PKI Consortium, Chairmanship of the India PKI Consortium, and is a member of the UN council on Blockchain.



USA | India | Singapore | UAE | Mauritius | Colombia