SECURITY MECHANISM OF TELTONIKA REMOTE MANAGEMENT SYSTEM

SUMMARY

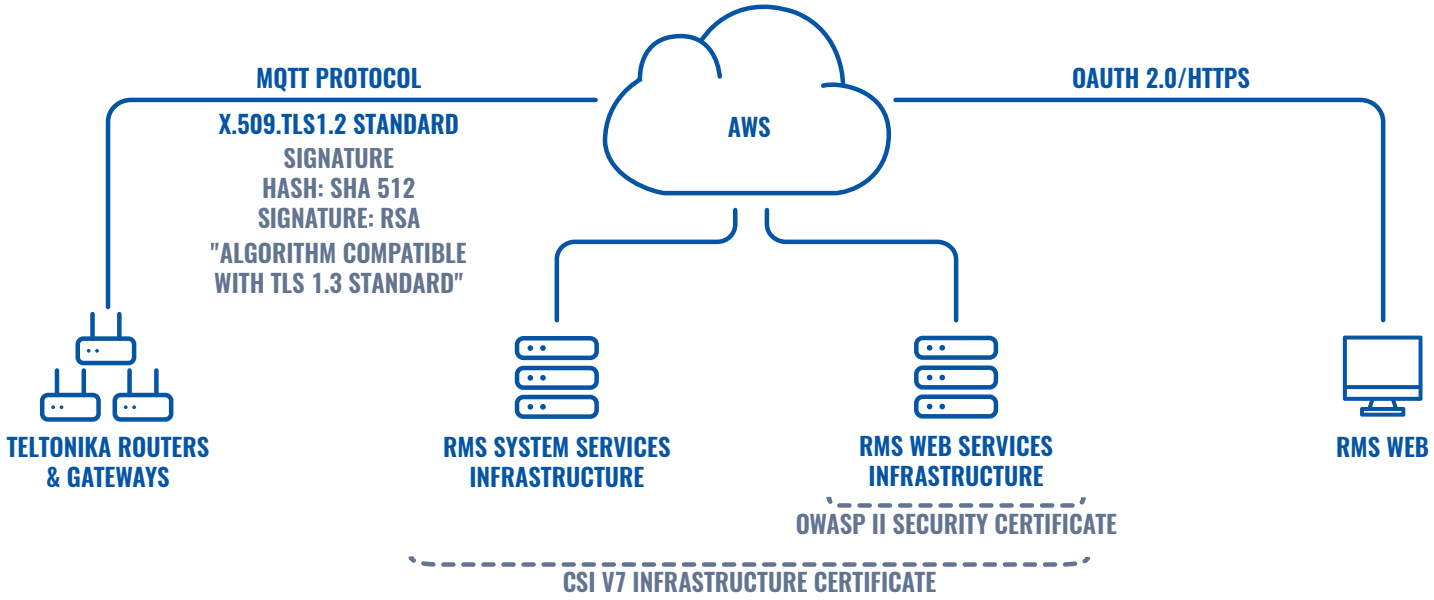
The world of the Internet of Things is rapidly evolving and is changing the way we interact with people, devices, and infrastructure. The growth of the number of connected IoT devices is unprecedented and is forecasted to reach over 50 billion by the end of 2020. They say that data is the new oil and we can see analogies between the two not only in terms of value but also in terms of its attractiveness for theft and interception. According to numerous security experts, cybercrimes in 2018 have generated upwards of 1.5 trillion USD. Cybersecurity threats will inevitably become more relevant and dangerous as the number of connected devices increases. Teltonika Networks have deployed hundreds of thousands of Industrial Cellular routers & gateways, which are keeping the world's most sensitive infrastructure securely connected.

Security is a priority for Teltonika Networks product development team, and our Remote Management System (RMS) is no exception. RMS is a cloud-based platform used daily by thousands of businesses globally which use the system to stay in control of their mission-critical network infrastructure conveniently. Below we will outline a few of the steps we take to make sure our RMS users are secure from any cyber-attacks and unauthorized access.

WHAT IS RMS SECURITY MECHANISM?

Remote Management System (RMS) is a proprietary software solution developed by Teltonika Networks and hosted on AWS (Amazon Web Services). AWS has more than a million active enterprise users, including companies like Samsung, Netflix & NASA. It is arguably the safest cloud available today with a multitude of certifications and attestations including SOC-1/2/3 which makes AWS even safer than most On-Premise server configurations.

TOPOLOGY



HOW DOES TELTONIKA NETWORKS DEVICES COMMUNICATE WITH RMS?

Routers & Gateways by Teltonika Networks communicate with RMS platform using MQTT (Message Queuing Telemetry Transport) protocol which was chosen because of its security features. MQTT is secured with TLS protocol protected according to X.509 TLS 1.2 Standard signature algorithm. All communication between the device and the RMS is hashed and signed with RSA signature. Combined, this method of interaction complies with TLS 1.3 protocol requirements which ensures unparalleled privacy and performance compared to previous versions of TLS and non-secure HTTP.

HOW SECURE IS RMS CLIENT CONNECTIONS TO THE SYSTEM?

All clients access RMS via HTTPS; therefore, all communication is encrypted, making sure that no one will be able to intercept your login details and gain unauthorized access to the client's account. To make the access even more secure, we have implemented OAuth 2.0 authentication method with 2-way verification which will prevent unauthorized access even in an event if your login credentials are compromised or stolen.

WHAT CYBER-SECURITY CERTIFICATION RMS COMPLIES WITH?

Because all servers running RMS are hosted by AWS, RMS complies with CIS v7 infrastructure security certificate developed to align with the latest cyber threat data and reflect today's current threat environment. Moreover, RMS has been awarded OWASP 2 security certificate, which is popular amongst banks and other financial institutions.