ORYX EMBEDDED

CycloneSSH

RA Ecosystem Partner Solution

ORYX EMBEDDED - CycloneSSH

Embedded SSH / SFTP / SCP Library

1.Solution Summary

CycloneSSH is a SSHv2 library dedicated to embedded applications. It can be used to operate network services such as remote shell and file transfer over an unsecured network. The authentication layer of SSH uses public-key cryptography to authenticate the remote machine. The transport layer of SSH provides confidentiality and integrity of data exchanged between the client and server. CycloneSSH supports several Renesas products including RA MCUs.

2. Features/Benefits

- SSH version 2.0 implementation
- Client and server modes of operation
- Password and public key user authentication methods
- Secure shell client and server (for remote execution of commands)
- SCP client and serve & SFTP client and server
- Key exchange using Diffie-Hellman, ECDH, Curve25519 and Curve448 algorithms
- RSA, DSA, ECDSA, Ed25519 and Ed448 host key algorithms
- 3DES, AES, Camellia, SEED and Chacha20Poly1305 encryption algorithms
- Legacy support for RC4, IDEA and Blowfish encryption algorithms
- CBC, CTR and GCM encryption modes
- HMAC using SHA-1, SHA-256 or SHA512
- Legacy support for MD5 and RIPEMD-160 algorithms
- Supports Encrypt-then-MAC (EtM) construction
- Elliptic Curve Cryptography (ECC) supported
- Flexible memory footprint. Built-time configuration to embed only the necessary features
- Portable architecture (no processor dependencies)
- The library is distributed as a full ANSI C and highly maintainable source code

3. Diagrams/Graphics

4. Target Markets and Applications

- Industrial IoT Systems
- Home & Building Automation
- Security & Defence Systems
- Smart Meters & Energy Storage

https://www.oryx-embedded.com/products/CycloneSSH

2021.08

Company Name	ORYX EMBEDDED
Address	165 rue Louis Barran, ZA Centr'Alp 2, 38430 Saint-Jean-de-Moirans - FRANCE
Date of Creation	2014
Business Description	Secure Networking Solutions for Embedded Systems
Product Offering	CycloneTCP (Embedded TCP/IP Stack, IPv4 & IPv6) CycloneSSL (Embedded TLS 1.3 / DTLS 1.2 Library) CycloneSSH (Embedded SSH / SFTP / SCP Library) CycloneCRYPTO (Embedded Crypto Library) CycloneSTP (STP & RSTP Protocols) CycloneACME (ACME client Library) Our products are available either as open source (GPLv2 license) or under a royalty-free commercial license (non-GPL license). We also propose an evaluation license (90-day license in source form) with technical support for an easier onboarding and effective evaluation of our software: https://www.oryx-embedded.com/download/
Renesas Partner Page	https://www.oryx-embedded.com/partners/renesas.html
Website	https://www.oryx-embedded.com
Contact	info@oryx-embedded.com