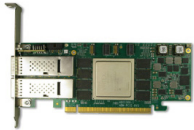


Ferrara2™

Product Brief



The DRC Ferrara2 crypto engine provides an ultra-high speed, inline encryption and data security capability. Industry standard encryption techniques with a patented information dispersal algorithm delivers an ultra-secure data-in-motion, data-at-rest and application protection capability, scalable to 100s of gigabits per second.



Ferrara2 cryptonet engine

- High performance – 40+ Gbps
- Very low latency – 20 microseconds
- Unique bit split capability
- Full Linux Support
- Highly scalable

Background. High performance inline encryption is an essential requirement to protecting your IT environment. Ensuring that no data is in the clear whether its at rest or in motion is no longer an optional requirement.

Solution. The DRC Ferrara2 cryptonet engine delivers encryption and authentication at line rates of 40+ Gbps. Additionally it can create “shares” of the data and transmit those down alternative paths or store those on geographically distributed systems – each share has no discernable data.

Single or Multiple Engines. Ferrara2 engines are available as PCIe add-in boards for integration into application servers, communication systems or storage systems. For very high bandwidth applications multiple Ferrara2 boards can be placed in one system.

Encrypted at Source. By placing the Ferrara2 PCIe board in the system that generates or stores the data it ensures that no data is visible in the clear. It also minimizes latency and maximizes performance.

Storage Integrated. By placing the Ferrara2 PCIe engine inside the storage controller all data can be encrypted and decrypted within the storage system. This provides the highest level of data integrity available combined with lowest latency.

Server Integrated. The Ferrara2 PCIe engine can be integrated into any application server and can be used to encrypt and decrypt data and applications at point of capture and analysis.

Comm Integrated. The Ferrara2 PCIe engine can be integrated into a communications switch for encrypting and decrypting data within and between networks.

Cloud ready. Ferrara2 engines are cloud ready.

FIPS140-2 compliant. Ferrara2 is based on the original Ferrara product that is FIPS certified.

Flexible Encryption. Standard encryption is AES-256 however a user specified encryption technique can be substituted.

Unique Cryptography. Ferrara2 combines standards based AES-256 and authentication cryptography with a unique bit-splitting capability from Security First Corporation (SFC). The bit-splitting information dispersal algorithm (IDA) patented by SFC secures cleartext data by splitting it at the bit level into n shares (n is user selectable). None of the shares contain discernable data. In addition the user has the option to specify a number m ($m < n$) where m denotes the number of shares required to reconstitute the original cleartext data. The n shares can be geographically distributed and so combined with $m < n$ this delivers a very high-availability solution. With Ferrara2 the n shares can be distributed over different communications links or phases in a fiber optic network.

Specification (per Ferrara2 engine):

Throughput	Sustained 60+ Gbps
Latency	< 20 microseconds
Encryption	AES-256
Data Assurance	SFC Bitsplit
Authentication	HMAC and SHA-256
Configuration	PCIe Gen 3 x 16, Single slot
Power Consumption	<20 watts

Highly Secure Gateway. The algorithms are coded on the onboard FPGA. For an even more secure environment the FPGA can be made to prevent reconfiguration. This provides a highly secure gateway in and out of the system that can not be hacked or modified.

The DRC Difference

With over 200 man-years of experience in developing low latency, high capacity solutions DRC has a unique talent in big data applications.

Made in America

DRC is a US based company with all its staff US citizens, and all its engineering and product sourcing conducted in the US.

DRC COMPUTER CORP
3375 Scott Blvd, Suite 206
Santa Clara, CA 95054

PHONE
+1. 408.562.0000

WEB
drccomputer.com