

White Paper

# Rocket Boost Your Data Encryption with Intel® QAT Card NA 1000-L2X



## Background: companies need big data to succeed

From the early days of data mining to today's artificial intelligence, the value and importance of big data has steadily increased. Through data accumulation and analysis, businesses have discovered diverse yet invaluable patterns to enhance service quality, make marketing more precise, improve workflow, and reduce operational costs. Without doubt, it will eventually bring enterprises more profits and make them more competitive. It can be said then that big data has become the modern-day business environment's gold mine, and just like an actual gold mine, companies that obtain exclusive mining rights can also earn endless profits, so protecting important data has become a most critical task.

In the era of big data, information is so valuable that criminals can take advantage of any leakage as the starting point to commit online fraud. With leaked information, a criminal can pretend to be a specific person, using lifelike letters and instant messaging to defraud – or for other illegal purposes.

## Challenge: data encryption has become the foundation of information security

When it comes to information security, three basic tenets are C.I.A.: Confidentiality, Integrity, and Availability. Confidentiality is the prevention of unauthorized users from intentionally or unintentionally obtaining data content. Common practice is to encrypt transmitted data and decrypt when it is used; in this way, even if data is accidentally leaked, the acquirer still cannot analyze the data content nor conduct any inappropriate use. However, if the data is highly valued, the acquirer may still have an incentive to try

and decrypt it. Although using a longer key increases the difficulty of cracking it, it also increases the cost of data encryption.

Encryption includes the costs of computing power and time. It is a repetitive and tedious operation that, first, consumes CPU computing power that should be reserved for higher-value applications and, secondly, is not suitable for general-purpose CPU hardware architecture. Therefore, although general-purpose CPUs can complete encryption computing tasks, it also creates two major issues: incalculable costs and data processing delays. When the amount of transmitted data increases, it subsequently decreases the efficacy of the CPU in processing other applications. Thus, when encryption becomes information security's main action, how to complete data encryption efficiently and at a low cost becomes an issue that an information security platform urgently needs to resolve.

## Solution: NEXCOM NSA 5181 + NA 1000-L2X encryption card


In order to resolve the aforementioned data encryption issue, the best way is to speed up encryption operations through dedicated hardware and, thus, offload CPU usage. Through this mode of isolating different computing needs, it allows the CPU's computing resources to focus on important applications in the upper layers, so that any increase in data traffic that needs encryption will not encumber the information security platform's application resources and will instead maintain high-efficiency encryption computing capabilities.

For this reason, NEXCOM has launched the NA 1000-L2X encryption card, which can be used as a cryptographic accelerator with NEXCOM's NSA 5181 network security


platform. More specifically, NA 1000-L26 is based on Intel's Lewisburg platform (C626), embedded with two Intel® QAT (QuickAssist Technology) engines, and connected to the CPU through the PCIe x8 interface. Intel® QAT includes symmetric encryption and authentication, asymmetric encryption, digital signatures, RSA, DH, and ECC, and lossless data compression.

In demonstrating the NA 1000-L26 accelerator card's encryption capabilities, Table I below shows the performance test system configuration of NEXCOM's NSA 5181 paired with NA 1000-L26. Table II shows the results. From the test results, one can see that NSA5181 with NA 1000-L26 QAT, whether utilizing AES128-CBC or AES256-CBC algorithms, can achieve a throughput (Mix) of nearly 40 Gbps.

**TABLE I  
CONFIGURATION FOR NSA 5181 QAT PERFORMANCE TEST**

NSA 5181	Item	Description
	CPU	Intel® Xeon® E-2126G CPU @ 3.30GHz
	Memory	8GiB DIMM DDR4 Synchronous 2133 MHz (0.5 ns)
	Intel® QAT Card	NA 1000-L26
	Intel® QAT Driver	1.7-L.4.4.0-00023
	Linux OS Version	Red Hat Enterprise Linux Server Release 7.6 (Maipo)

**TABLE II  
RESULTS FOR NA 1000-L26 QAT PERFORMANCE TEST**

NA 1000-L26	Algorithm/ Packet Size (Byte)	64	128	256	512	1024	2048	4096	Mix (40%-64B 20%- 752B 35% 1504B 5%-8892B)
	AES 128-CBC Speed (Gbps)	5.2	11	19.9	32.9	44.2	47.8	51	41.1
	AES 256-CBC Speed (Gbps)	5.6	10.2	20.3	32.1	40.7	46.5	50.8	39.2

## Conclusion

With the advent of big data and the heightened role that information security plays, encrypting transmitted data has become a basic requirement for secure communications but substantially increases CPU load. In addition to multiplying computing power costs, it also causes delays in application services. NEXCOM's NCS Group resolves these user issues through the NA 1000-L2X accelerator card, which can

pair with NEXCOM's NSA information security platform series. Through the NA1000-L2X's hardware acceleration function, you can offload the CPU load and greatly enhance the system's encryption throughput.

As a reliable partner and industry leader in information security platforms, NEXCOM is always thinking about the next step for our valued customers.



---

Founded in 1992, NEXCOM integrates its capabilities and operates eight global businesses, which are Industrial Mesh, Intelligent Platform @ Smart City, Intelligent Video Security, Mobile Computing Solutions, Medical and Healthcare Informatics, Network and Communication Solutions, Smart Manufacturing, and Open Robotics and Machinery. This strategic deployment enables NEXCOM to offer time-to-market, time-to-solution products and services without compromising cost.

[www.nexcom.com](http://www.nexcom.com)



---

NEXCOM is an Associate member of the Intel® Internet of Things Solutions Alliance. From modular components to market-ready systems, Intel and the 600+ global member companies of the Intel® Internet of Things Solutions Alliance provide scalable, interoperable solutions that accelerate deployment of intelligent devices and end-to-end analytics. Close collaboration with Intel and each other enables Alliance members to innovate with the latest technologies, helping developers deliver first-in-market solutions.

Learn more at: [intel.com/iotsolutionsalliance](http://intel.com/iotsolutionsalliance)

Intel and Atom are registered trademarks of Intel Corporation in the United States and other countries.