OpenSSL Conference ‘25

The Value of OpenSSL Providers in a Business Context

Date: Oct 7th, 2025

OpenSSL Providers

- **A Provider**: "is a unit that provides one or more algorithm implementations" (OpenSSL-3.0 Design Draft)
- New in OpenSSL-3.0, replacing Engines (along with other functionality) to provide better separation of algorithm implementation and API's (EVP API's).
- Providers can be dynamically loaded or linked into the libcrypto library
- Providers can be
  - built-in (default, null, base)
  - delivered with OpenSSL (legacy, FIPS)
  - third party provided

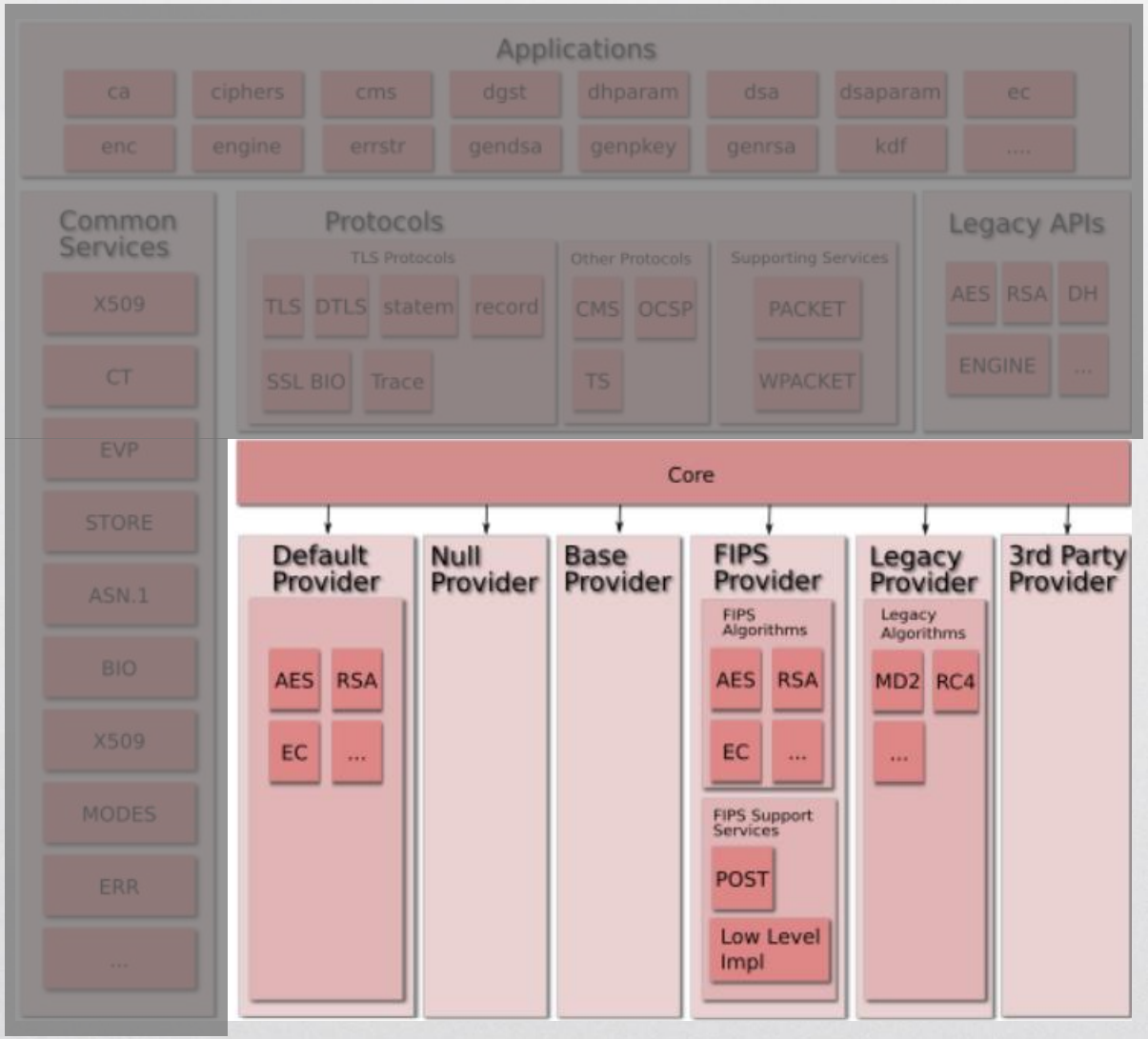


Diagram from OpenSSL 3.0.0 Design (Draft): https://docs.openssl.org/master/OpenSSL300Design/

Agenda

- Power of Providers
- Performance Considerations
- Release Frequency
- FIPS Provider & Isolation
- Post Quantum Cryptography Application Performance
- Dual approach to Enabling
- Difficulties with Providers
- Conclusion

Power of Providers

Performance
Platform-specific optimizations

Flexibility
Independent release timing & updates

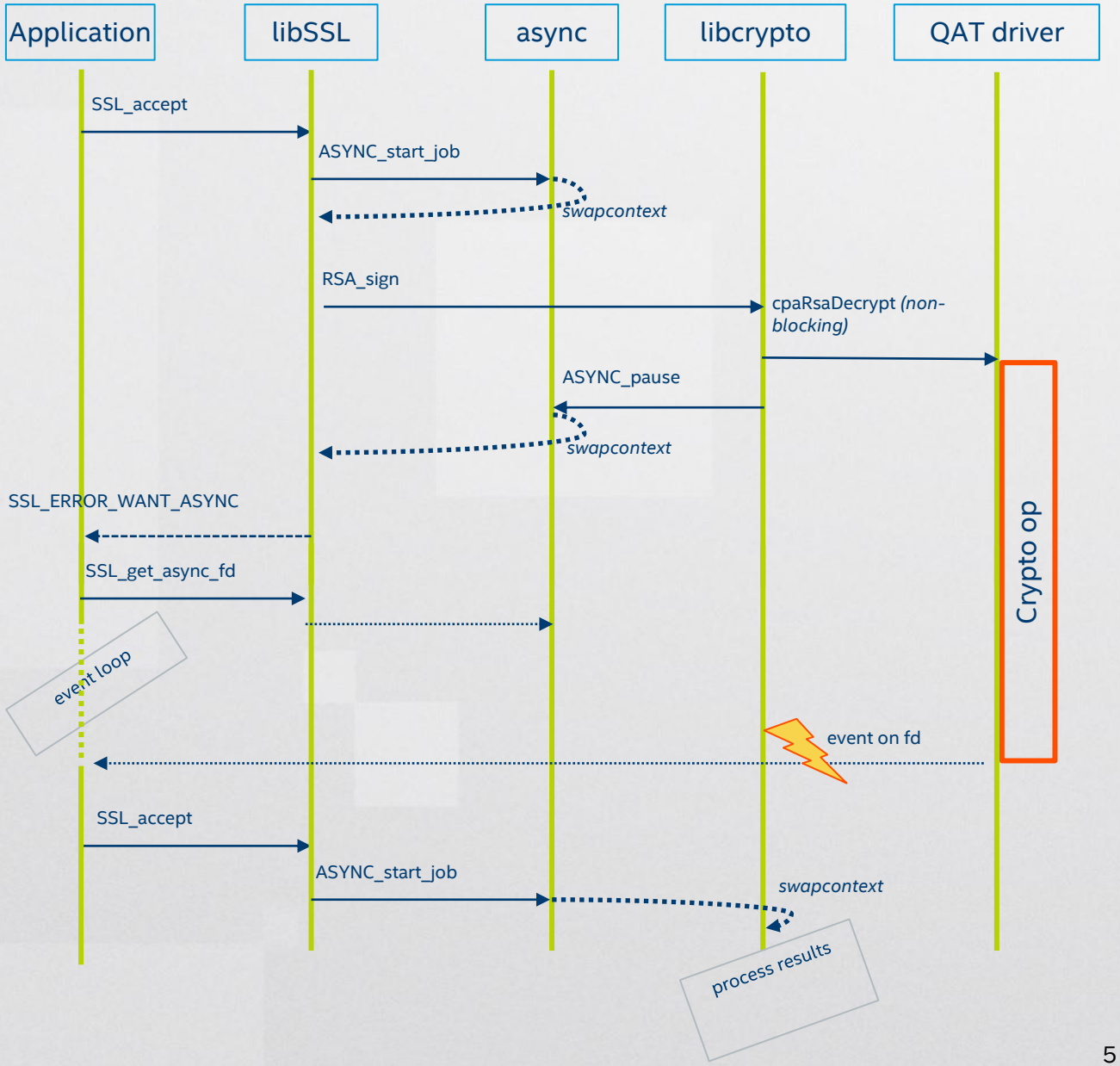
Scalability
Load-balancing across implementations

Compatibility
Version & legacy support

Security
FIPS & isolation

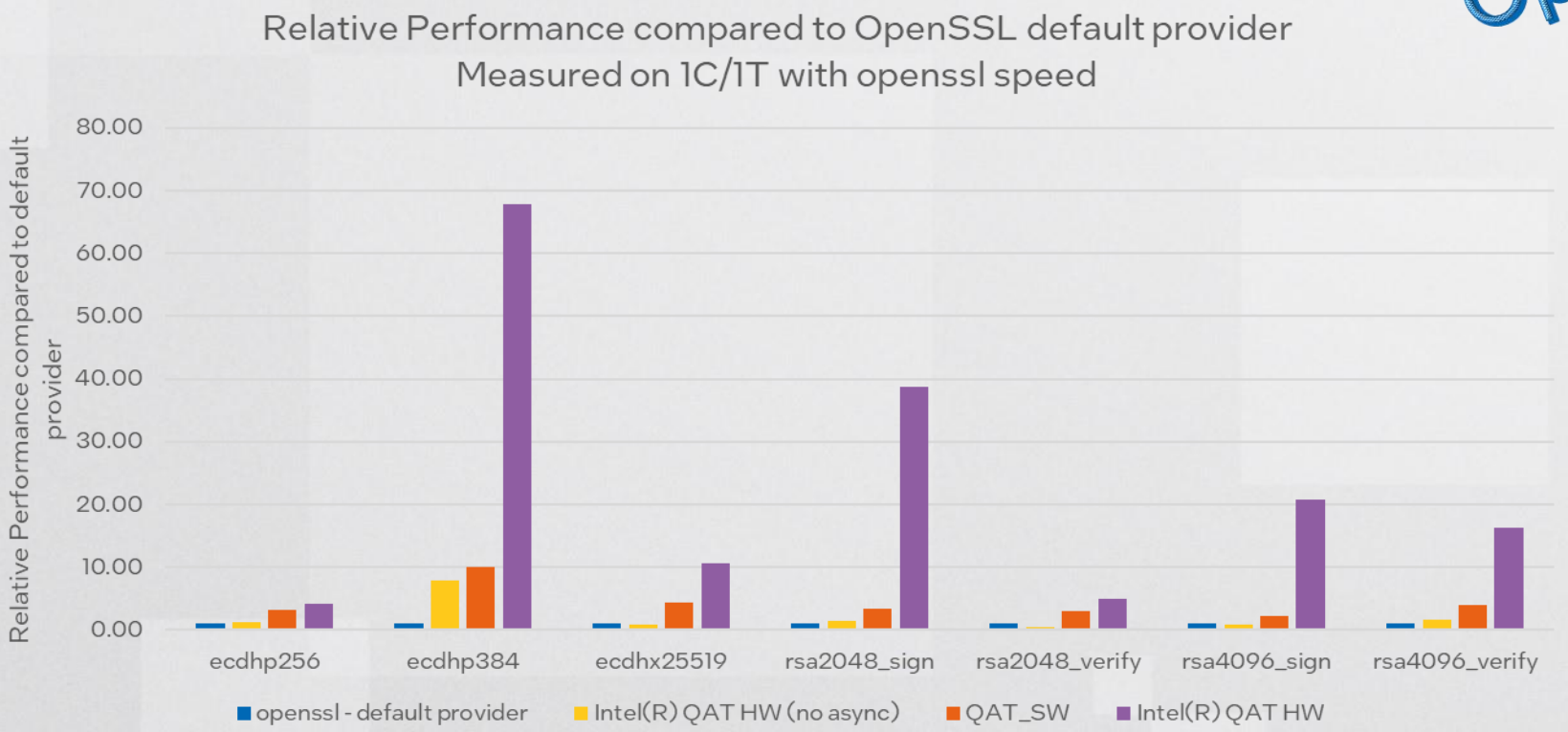
Performance: Asynchronous Processing

- Added to OpenSSL circa 2015 the capability to process operations in an asynchronous fashion, in particular cryptographic operations.
- This allows providers to process crypto operations asynchronously wrt to TLS protocol and application processing.
- This opens many possibilities; two distinct options we use in the qat_engine:
  - Offload to Intel® QAT HW
  - Batch multiple requests for vectorization (multi-buffer) processing
- Providers now have the flexibility to process requests using the most optimal methods



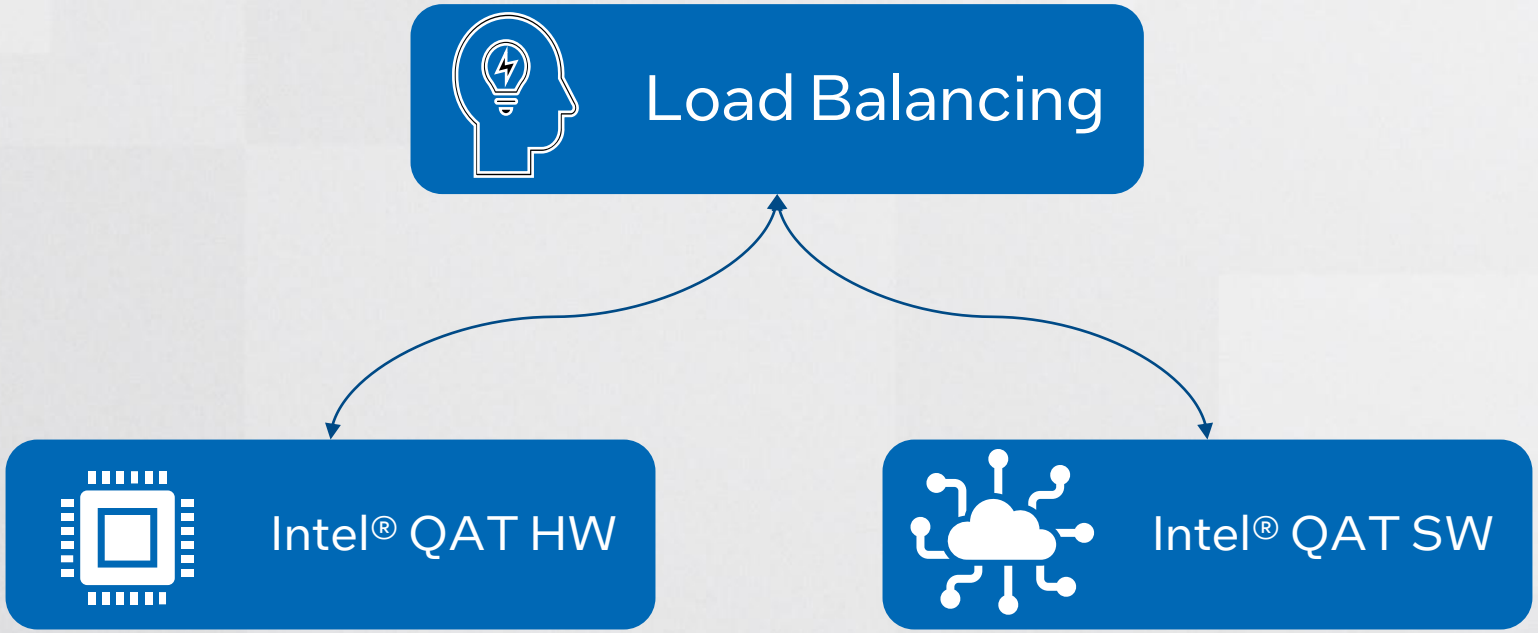
Async Performance

Openssl speed



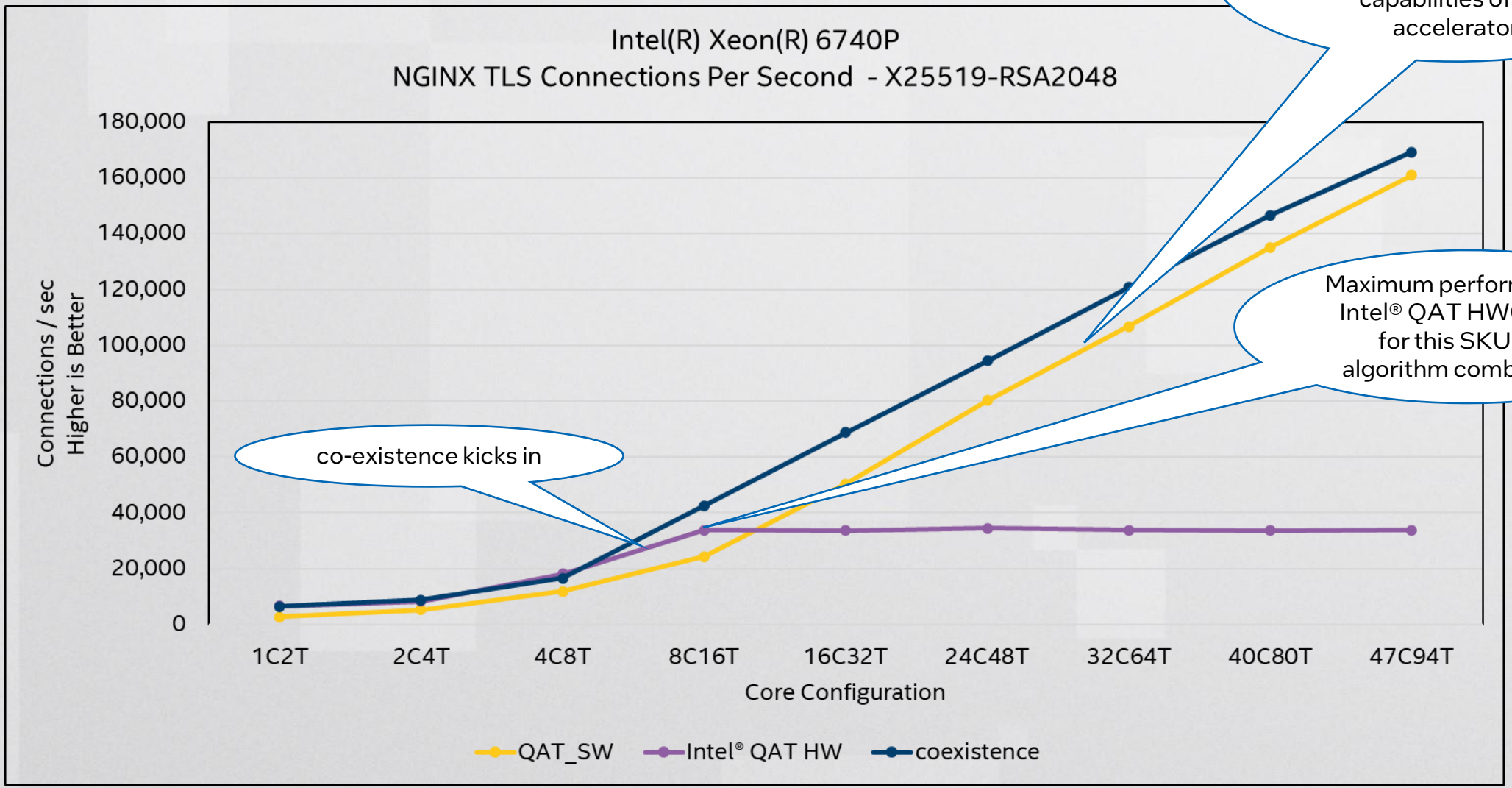
- Async invocation allows speed to submit multiple requests to Intel® QAT HW or QAT_SW
- In sync mode the submission thread needs to block waiting for the response to complete, resulting in significant under utilization.
- For ECDH-P384 this change results in up to **8.5 times better performance per core** moving from sync to async invocation or **up to 67 times better performance when compared to the default openssl provider**.

Performance varies by use, configuration and other factors.
See backup for workloads and configurations. Results may vary.(**System Configuration 1**)



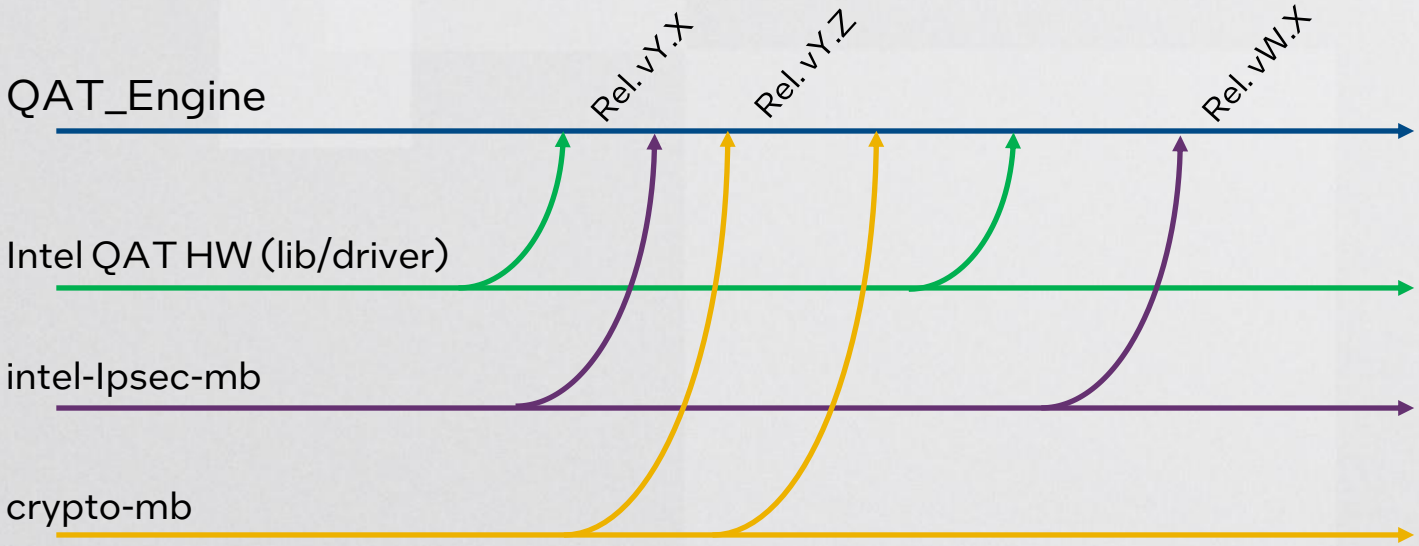
QAT_HW & QAT_SW Co-existence

QAT_HW & QAT_SW Co-existence Performance

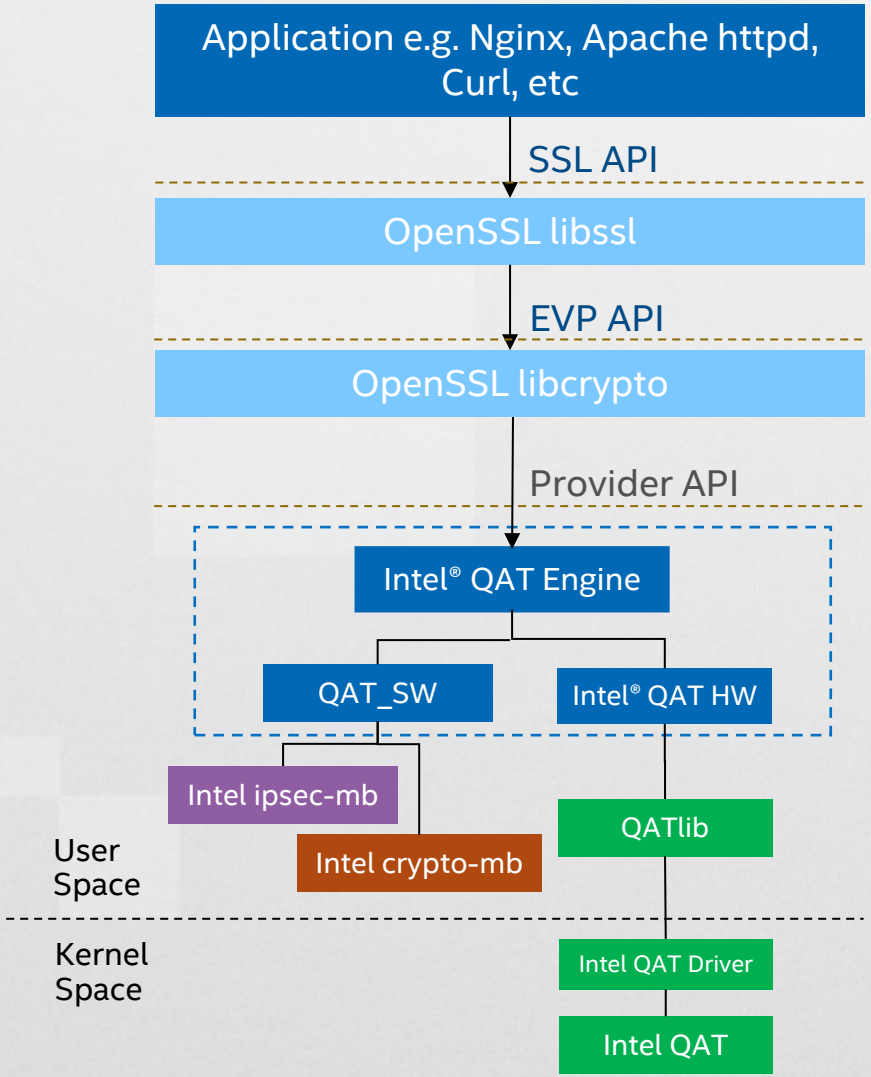


Performance varies by use, configuration and other factors.
See backup for workloads and configurations. Results may vary.(**System Configuration 2**)

Release Frequency & Version Support

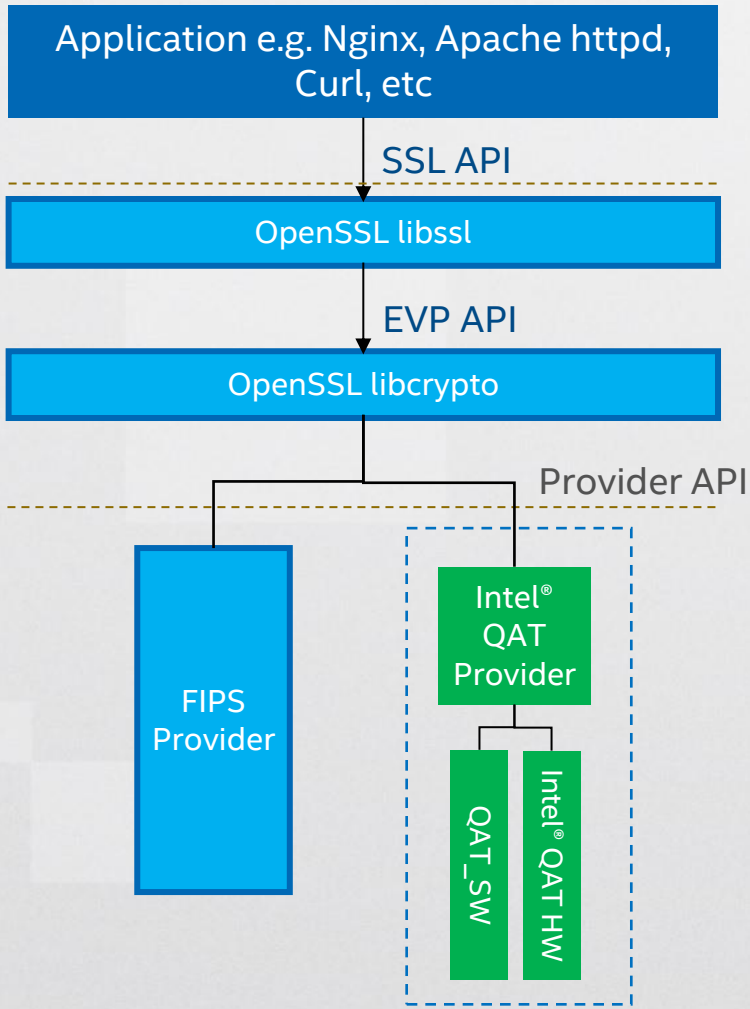


- QAT_Engine encompasses three acceleration technologies:
  - Intel® QAT HW Acceleration
  - QAT_SW Acceleration
    - Intel ipsec-mb
    - Intel crypto-mb

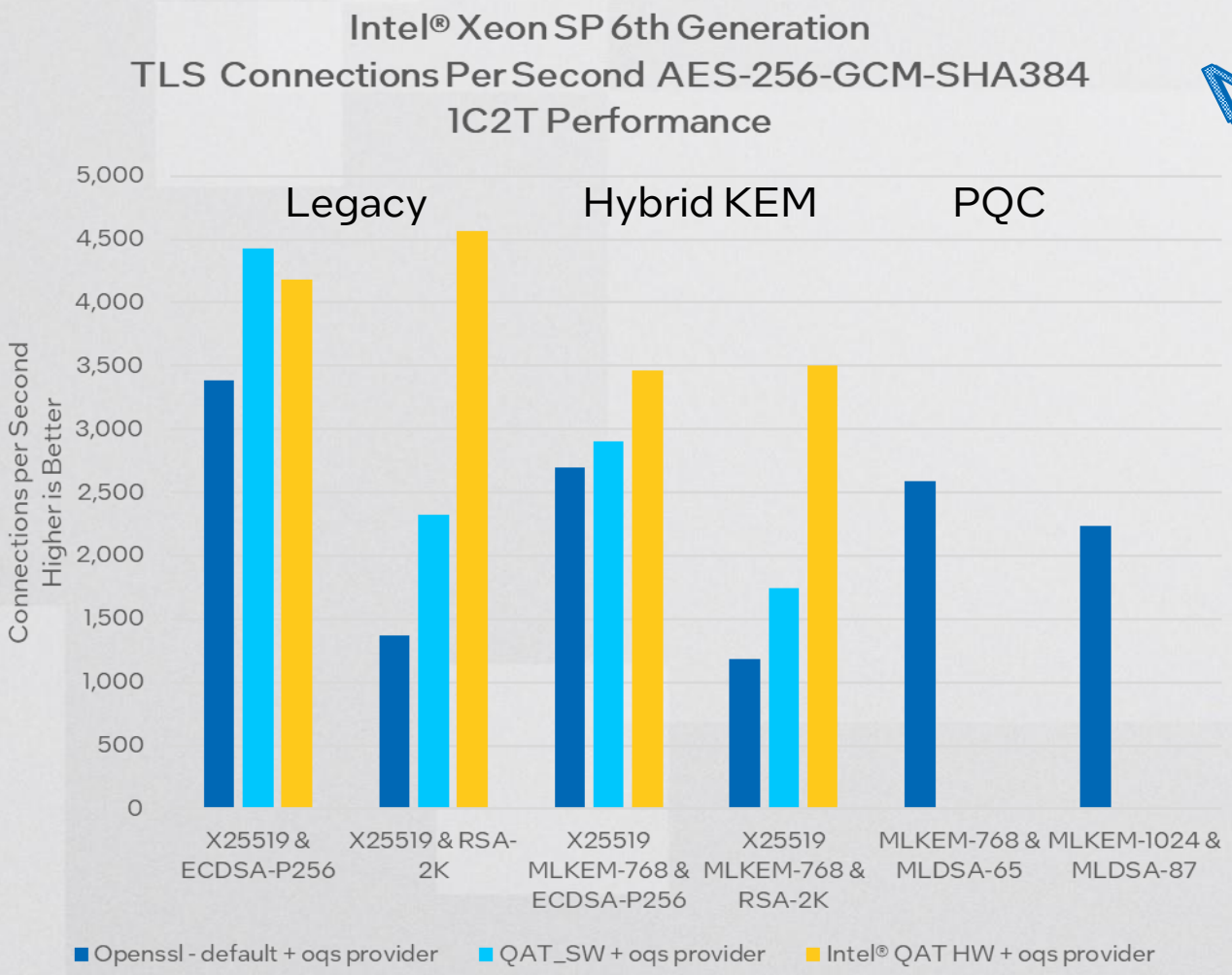


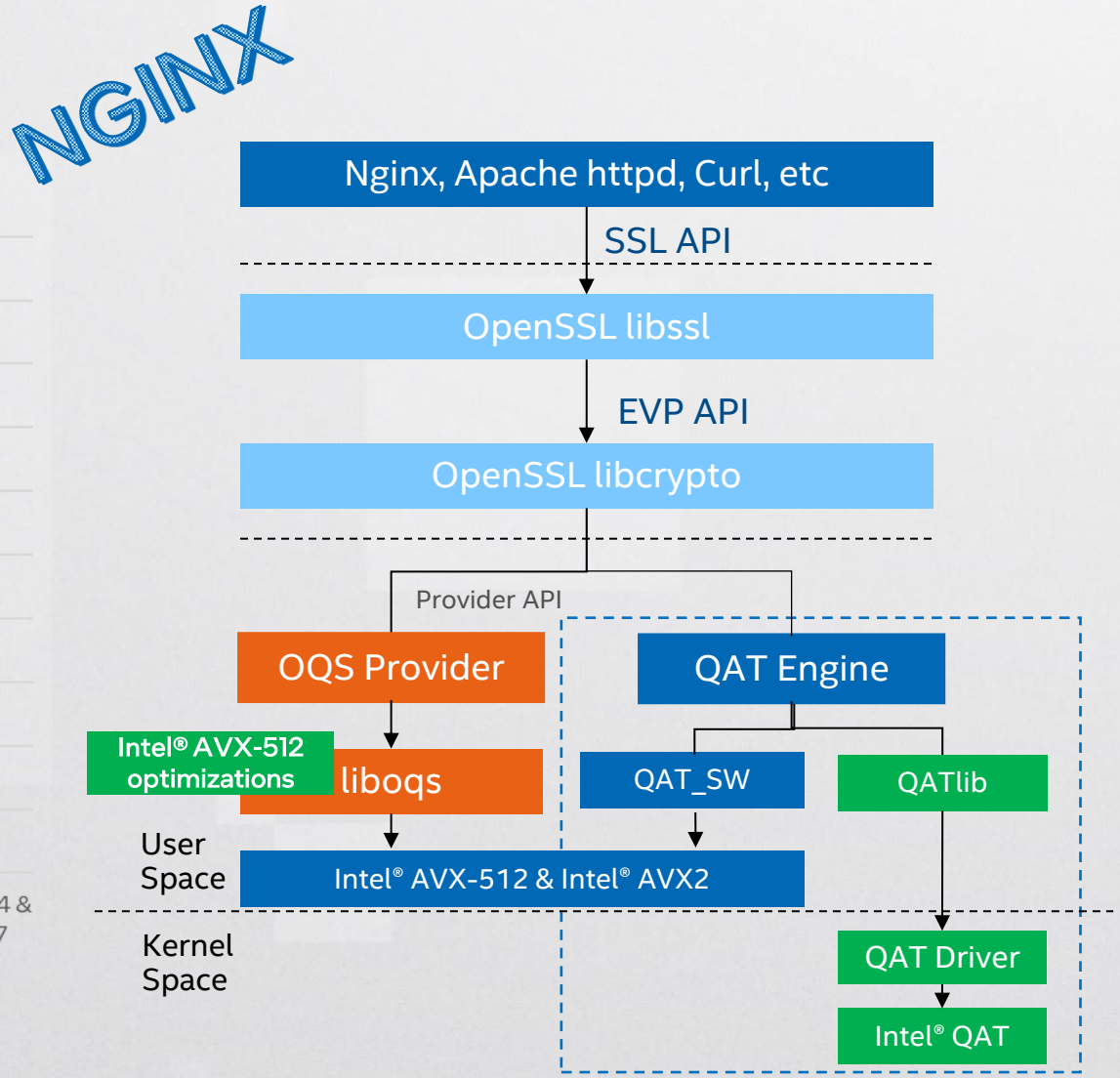
FIPS & Isolation

- FIPS
  - Providers give a clear boundary to attain FIPS certification, separate from libssl and the application.
  - Intel® QuickAssist Technology (QAT) Provider is FIPS 140-3 level 1 certified.
  - Loading with OpenSSL's FIPS provider, allows for an accelerated FIPS solution covering all certified algorithms
- Isolation
  - Due to the clean boundary created by the provider interface.
  - Cryptographic Key processing can be implemented locally, or remotely under more stringent or centralized security measures.
  - Remote communications can be entirely encompassed inside the provider, leveraging ASYNC semantics



Post-Quantum Cryptography (PQC)

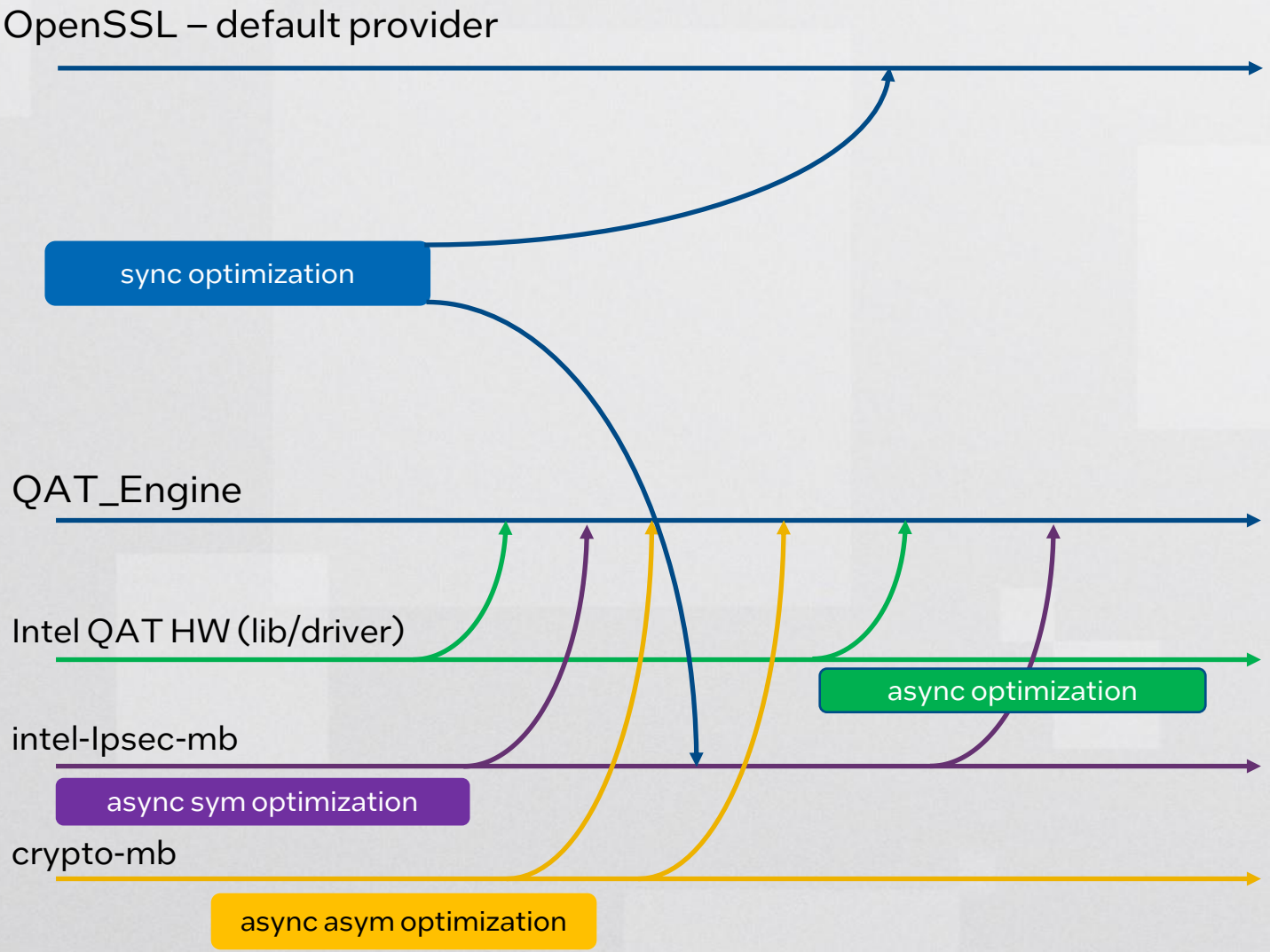




liboqs PR#2167 - Added AVX512VL-Optimized SHA3/SHAKE Implementations

Performance varies by use, configuration and other factors.
See backup for workloads and configurations. Results may vary.(**System Configuration 3**)

Dual Approach to Enabling



Difficulties with Providers & Deployment Considerations

- Deployment and accessibility to customers “ingest” models
  - distributions and package repositories
  - source
- Providers need to release packages into the downstream repositories
  - packages must meet release windows of distribution
  - loading of provider by applications
- Lack of a run time configuration interfaces for providers
  - prevents some models of operation e.g. direct polling of responses
- OpenSSL-3.x provider performance

Conclusion

- Providers are an excellent mechanism to deliver cryptographic innovations, on a provider's timeline.

Composability of provider's delivers flexible solutions

Notices & Disclaimers

Performance varies by use, configuration and other factors. Learn more on the Performance Index site.

Performance results are based on testing as of dates shown in configurations and may not reflect all publicly available updates. See backup for configuration details. No product or component can be absolutely secure.

Your costs and results may vary.

Intel technologies may require enabled hardware, software or service activation.

Backup

System Configuration 1

Date	9/16/2025
System	Intel Corporation BeechnutCity
Baseboard	Intel Corporation BeechnutCity
Chassis	Intel Corporation Rack Mount Chassis
CPU Model	Intel(R) Xeon(R) 6787P
Microarchitecture	Unknown Intel
Sockets	2
Cores per Socket	86
Hyperthreading	Enabled
CPUs	344
Intel Turbo Boost	Disabled
Base Frequency	2.0GHz
All-core Maximum Frequency	3.2GHz
Maximum Frequency	2.0GHz
NUMA Nodes	2
Prefetchers	L2 HW, L2 Adj., DCU HW, DCU IP
PPINs	653e2dc099625dc4,64dc7232e7cbb8d8
Accelerators	QAT:4, DSA:8, IAA:8
Installed Memory	512GB (16x32GB <OUT OF SPEC> 5600 MT/s [5600 MT/s])
Hugepagesize	2048 kB
Transparent Huge Pages	madvise
Automatic NUMA Balancing	Disabled
NIC	1x I210 Gigabit Network Connection
Disk	1x 223.6G INTEL SSDSC2KB240G8
BIOS	BHSDREL1.IPC.3544.P69.2505272019
Microcode	0x810003d0
OS	Ubuntu 24.04.2 LTS
Kernel	6.8.0-58-generic
TDP	350 watts
Power & Perf Policy	Performance
Frequency Governor	schedutil
Frequency Driver	acpi-cpufreq
Max C-State	9
Vulnerability	CVE-2017-5753:OK, CVE-2017-5715:OK, CVE-2017-5754:OK, CVE-2018-3640:OK, CVE-2018-3639:OK, CVE-2018-3615:OK, CVE-2018-3620:OK, CVE-2018-3646:OK, CVE-2018-12126:OK, CVE-2018-12130:OK, CVE-2018-12127:OK, CVE-2019-11091:OK, CVE-2019-11135:OK, CVE-2018-12207:OK, CVE-2020-0543:OK

Performance varies by use, configuration and other factors. Learn more on the Performance Index site

System Configuration 1 (Software)

Workload	Openssl speed
Tools/Compilers	gcc (Ubuntu 13.3.0-6ubuntu2~24.04) 13.3.0
Libraries	OpenSSL 3.5.2 Qat Provider v1.9.0 (provider) QAT20.L.1.2.30-00090 Cryptography Primitives v1.0.1 IPSecMB v2.0
NIC firmware	4.20 0x80017784 1.3346.0
ice driver	ice 1.15.4
Commands used	taskset -c <> openssl speed -multi <>-seconds 30 -async_jobs <num> -provider qatprovider -elapsed <cipher>

System Configuration 2

Date	9/16/2025
System	Intel Corporation BeechnutCity
Baseboard	Intel Corporation BeechnutCity
Chassis	Intel Corporation Rack Mount Chassis
CPU Model	Intel(R) Xeon(R) 6740P
Microarchitecture	GNR_X2
Sockets	2
Cores per Socket	48
Hyperthreading	Enabled
CPUs	192
Intel Turbo Boost	Disabled
Base Frequency	2.1GHz
All-core Maximum Frequency	3.3GHz
Maximum Frequency	2.1GHz
NUMA Nodes	2
Prefetchers	L2 HW: Enabled, L2 Adj.: Enabled, DCU HW: Enabled, DCU IP: Enabled, AMP: Enabled, Homeless: Enabled, LLC: Disabled
PPINs	5c468d64e995db79,5c5f8e64b71ea5d4
Accelerators	DLB 4 [0], DSA 4 [0], IAA 4 [0], QAT 4 [2]
Installed Memory	512GB (16x32GB DDR5 6400 MT/s [6400 MT/s])
Hugepagesize	2048 kB
Transparent Huge Pages	madvise
Automatic NUMA Balancing	Disabled
NIC	10x Ethernet Controller E810-C for QSFP, 1x I210 Gigabit Network Connection
Disk	1x 223.6G KINGSTON SA400S37240G, 1x 240M Disk
BIOS	BHSDCRB1.IPC.3544.P07.2410011105
Microcode	0x81000314
OS	Ubuntu 22.04 LTS
Kernel	5.15.0-27-generic
TDP	270 watts
Power & Perf Policy	Normal (6)
Frequency Governor	Powersave
Frequency Driver	intel_pstate
Max C-State	9
Vulnerability	CVE-2017-5715:OK, CVE-2017-5753:OK, CVE-2017-5754:OK, CVE-2018-12126:OK, CVE-2018-12127:OK, CVE-2018-12130:OK, CVE-2018-12207:OK, CVE-2018-3615:OK, CVE-2018-3620:OK, CVE-2018-3639:OK, CVE-2018-3640:OK, CVE-2018-3646:OK, CVE-2019-11091:OK, CVE-2019-11135:OK, CVE-2020-0543:OK, CVE-2022-40982:OK, CVE-2023-20569:OK, CVE-2023-20593:OK, CVE-2023-23583:OK

Performance varies by use, configuration and other factors. Learn more on the Performance Index site

System Configuration 2 (Software)

Workload	Async Mode for NGINX v0.5.3 (https://github.com/intel/asynch_mode_nginx)
Application	Connections Per Second - ECDHE-X25519-RSA2K
Tools/Compilers	gcc (Ubuntu 11.2.0-19ubuntu1) 11.2.0
Libraries	OpenSSL 3.3.2 Qat Engine v1.8.0 (engine) Cryptography Primitives v1.0.1 IPSecMB v2.0 QAT20.L.1.2.30-00090
NIC firmware	4.20 0x80017784 1.3346.0
ice driver	ice 1.15.4
cores used	47C94T

System Configuration 3

Date	09/11/2024
System	Intel Corporation BeechnutCity
Baseboard	Intel Corporation BeechnutCity
Chassis	Intel Corporation Rack Mount Chassis
CPU Model	Genuine Intel(R) 0000
Microarchitecture	GNR_X2
Sockets	2
Cores per Socket	86
Hyperthreading	Enabled
CPUs	344
Intel Turbo Boost	Enabled
Base Frequency	1.9GHz
All-core Maximum Frequency	2.9GHz
Maximum Frequency	1.9GHz
NUMA Nodes	2
Prefetchers	L2 HW: Enabled, L2 Adj.: Enabled, DCU HW: Enabled, DCU IP: Enabled, AMP: Enabled, Homeless: Enabled, LLC: Disabled
PPINs	22efd25d9b0e20a7,22efcd5dd3bb1f98
Accelerators Available [used]	DLB 8 [0], DSA 8 [0], IAA 8 [0], QAT 8 [0]
Installed Memory	512GB (16x32GB DDR5 5600 MT/s [5600 MT/s])
Hugepagesize	2048 kB
Transparent Huge Pages	madvise
Automatic NUMA Balancing	Disabled
NIC	10x Ethernet Controller E810-C for QSFP, 1x I210 Gigabit Network Connection
Disk	1x 894.3G Micron_7450_MTFDKBG960TFR
BIOS	BHSDCRB1.IPC.0034.D65.2407302252
Microcode	0x810002e0
OS	Ubuntu 24.04 LTS
Kernel	6.8.0-31-generic
TDP	350 watts
Power & Perf Policy	Normal (6)
Frequency Governor	schedutil
Frequency Driver	acpi-cpufreq
Max C-State	9
Vulnerability	CVE-2017-5715:OK, CVE-2017-5753:OK, CVE-2017-5754:OK, CVE-2018-12126:OK, CVE-2018-12127:OK, CVE-2018-12130:OK, CVE-2018-12207:OK, CVE-2018-3615:OK, CVE-2018-3620:OK, CVE-2018-3639:OK, CVE-2018-3640:OK, CVE-2018-3646:OK, CVE-2019-11091:OK, CVE-2019-11135:OK, CVE-2020-0543:OK, CVE-2022-40982:OK, CVE-2023-20569:OK, CVE-2023-20593:OK, CVE-2023-23583:OK

System Configuration 3 (Software)

Workload	Async Mode for NGINX v0.5.1 (https://github.com/intel/asynch_mode_nginx)
Application	Connections Per Second
Tools/Compilers	gcc (Ubuntu 13.2.0-23ubuntu4) 13.2.0
Libraries	OpenSSL 3.3.1 Qat Engine v1.6.1 (provider) Cryptography Primitives v ippcp_2021.12.1 IPSecMB v1.5 libOQS v0.10.1 OQS-Provider v0.6.1 QAT Driver QAT20.L.1.2.30-00078

Performance varies by use, configuration and other factors. Learn more on the Performance Index site


intel