CETHERA CTHR-01 SPU

PCIe 기반 보안 가속기

SPU(Security Processing Unit)

To learn more, go to cethera.com/product

www.cethera.com 뉴젠스 NEWGENS

목차

01. 도입 배경

계층화된 하드웨어 기반 보안가속기를 통해
진화하는 사이버 위협과
미래의 양자 컴퓨팅 위협에 대응

양자 컴퓨팅 시대의 위협 가속화

- 양자 컴퓨터 연산 성능 비약적 발전으로 현재의 공개키 암호화 방식 무력화
- 국가 및 기업의 핵심 자산이 미래의 양자 해킹으로부터 자유롭지 못한 'Harvest now, Decrypt later' 위협 증대

위험 요인

"AI 혁명"에 따른 사이버 위협의 진화

- 실시간 피해자 환경을 분석, 표적을 정확하게 타격할 수 있는 악성코드를 생성해 실행하는 적응형 공격 확대
- 탐지 회피를 위한 다양한 변형 코드 생산을 통해 기존 보안 시스템 우회

위험 요인

보안 위협에 따른 지속적인 비용 증가

- 전 세계적으로 사이버범죄 대응을 위해 연간 약 10조 달러 비용 발생
- 데이터 대량 유출, 재무적 손실 및 운영 중단

02. CETHERA CTHR-01 개요

보안저장소 및 키보관소, 자율 사이버 면역 시스템(ACIS)을 탑재한 PCIe 하드웨어 기반 보안가속기

■ SPU(보안 가속기)

- **Security Processor Unit**
- **PCIe 슬롯 제공 모든 PC 및 서버에 적용 가능**
- **하드웨어 기반 양자 보안(QE-BCP) 프로세스 가속기**
- **암호화키 보관소(Secure Key Store)**
  - 하드웨어 수준에서 암호화키 분산 보관
- **중요 프로세스 가속 처리 및 QE-BCP 암호화**
  - DB암호화 및 TLS 서비스 등을 오프로드 하여 가속 처리, SPU 내 모든 데이터는 QE-BCP로 보호됨
  - CPU 코아 및 라이선스 가격 절감(CAPEX 감소)

■ ACIS(자율 사이버 면역 시스템)

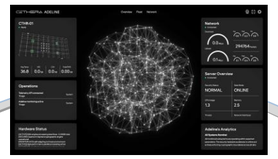
- **Autonomous Cyber Immunization System**
- **유전 알고리즘 AI를 적용**하여 카드 및 트래픽/키 사용패턴/펌웨어 무결성을 모니터링하고 공격 시도를 실시간 모니터링 및 대응
  - SPU 내 가속 기능을 이용함으로써 **ms 이내로 위협 탐지 및 차단(격리 등)**
  - 운영자의 별도 개입 없이 시스템이 자동적으로 공격을 차단함으로써 피해 확산 방지

SPU
(보안 가속기)

QE-BCP
(양자 얽힘 기반 암호화 프로토콜)

CETHERA CTHR-01 솔루션

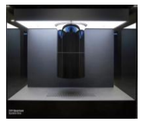
ACIS
(자율 사이버 면역 시스템)



Adeline 모니터링 플랫폼

■ QE-BCP

- **Quantum Entanglement-based Cryptography Protocol**
  - 현존 하드웨어를 통해 양자 역학 개념 구현 (**Quantum-Inspired**)
  - 지속적인 동적 키 변이를 통해 물리적 수준에서 기존 PQC(양자내성암호화)의 보안 강도 향상
  - 무결성 특성을 통해 데이터의 위변조 원천 차단
  - 양자시스템을 통해 프로토콜 시뮬레이션



IBM 양자컴퓨터,
연세대학교

■ Adeline

- 공격 탐지 시, 경보 및 상태 정보 제공
  - ACIS에서 즉시 공격 무력화
  - 내/외부 공격 상태, 대응 상태 기록
- SPU 상태 / 시스템 성능 & 지연 시간
- 시스템 이벤트 로그 제공
- CTHR-01 간 파일 공유용 Secure Channel 제공

뉴젠스 NEWGENS

03. 주요 특징 요약

- **가속 성능**
  - 시스템 속도 저하 없이 기업 규모의 암호화 가속을 위한 최대 8GB의 고대역폭 메모리 제공(316+GB/s 처리 성능)

- **강화된 양자 내성 암호화 (QE-BCP)**
  - 지속적인 암호키 변이(ms), 가속기 내 분산형 키 보관소 제공
  - 하드웨어 레벨에서 암호화 가속. 호스트 OS가 공격당하더라도 보안 프로세스 내부의 데이터와 메모리 영역은 안전하게 격리

- **자율 사이버 면역 시스템(ACIS)**
  - 실시간 비정상 트래픽 탐지 및 하드웨어 레벨 무력화
  - 운영자 대응 최소화

- **Zero-Trust 구조**
  - 모든 데이터는 암호화 상태로 처리됨
  - 키 분산 보관 및 유출에 대한 보호 (메모리 격리)

- **Adeline 사용자 인터페이스(UI)**
  - 보안 상태에 대한 직관적인, 실시간 시각화—위협 모니터링, 인터랙티브 AI 구체(sphere)를 통한 경보 확인

04. CTHR-01 SPU(Security Processor Unit)

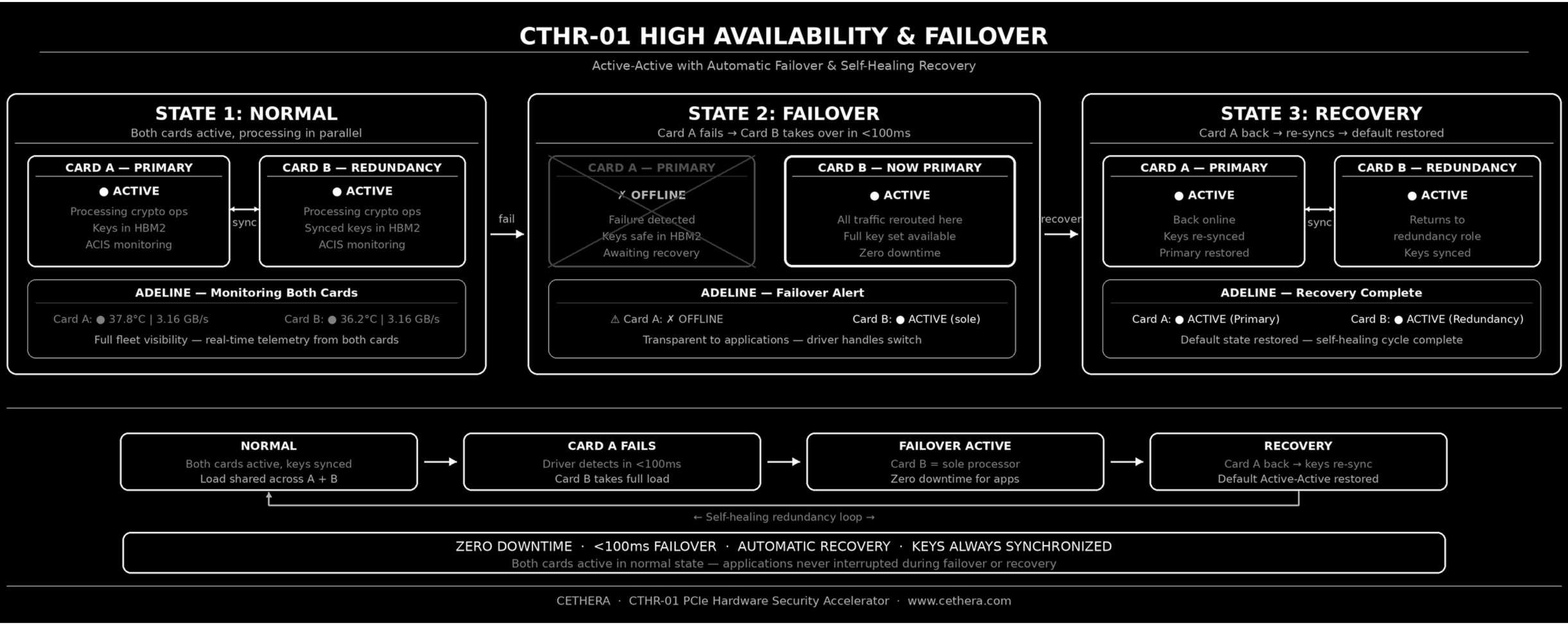
- PCIe 기반 보안 가속기
  - 하드웨어 레벨에서 강력한 보안을 제공하는 PCIe 가속기 솔루션
  - PCIe 슬롯을 제공하는 모든 서버 및 PC에 적용 가능

- QE-BCP를 통해 양자내성암호(PQC) 강화*
  - QE-BCP(Quantum Entanglement-based Cryptography Protocol, 양자얽힘 기반 암호화 프로토콜)
  - 기존 RSA/AES 암호화 방식 대체
  - CETHERA 사 자체 기술로 기존 하드웨어를 통해 양자 역학 기반 암호화 구현(Quantum-inspired)

- 모든 보안 관련 오버헤드를 호스트 CPU로 부터 오프로드하여 가속 수행

*** 기존 양자내성암호(PQC) 문제점**
- 복잡한 수학적 구조(격자 기반코드 기반 등)에 따른 성능 및 효율 저하
- 상대적으로 큰 암호화 키와 서명 데이터의 저장 및 전송 시 고대역폭과 메모리 필요
- 도입 및 전환의 복잡성, 고비용
- 특정 단일 알고리즘에만 전적으로 의존할 경우 발생할 수 있는 취약점과 한계 존재

05. CTHR-01 SPU 이중화(HA) 구조



06. QE-BCP

(Quantum Entanglement-Based Cryptography Protocol)

AES/RSA 대체방안

1

양자 개념 암호화 엔진

양자 역학 원리를 이용하여 지속적으로 진화하며, 비반복적 암호화 키를 통해 독보적인 데이터 보호 구현

2

자율 사이버 면역 시스템(ACIS)

새로운 위협에 실시간으로 적응하며, 사람의 개입 없이 공격을 자율적으로 탐지하고 무력화함

3

고성능 가속

316+ GB/s 의 암호화 처리 성능을 제공하며, 대규모 병렬 처리를 통해 기업 규모의 보안을 신속하게 처리

4

ZERO-TRUST 물리 구조

하드웨어 기반의 암호화키 분산 및 강화된 방어 기술을 통해 제로 평문 노출 및 변조에 즉시 대응 보장

뉴젠스 NEWGENS

07. 위협 모델 및 보안 경계

공격 경로	CTHR-01 SPU 미적용 시	CTHR-01 SPU 적용 시
루트 권한 탈취	키에 대한 전체 접근 권한	키 격리
메모리 스크래핑	메모리(RAM) 내 키 존재	메모리(RAM) 내 키 없음
DMA 공격	가능	카드 로직에 의한 차단
내부자(물리적 공격)	키 탈취 가능	탐지 및 폐기
부채널 공격	취약함	하드웨어 차원 대응

08. ACIS(Autonomous Cyber Immune System)

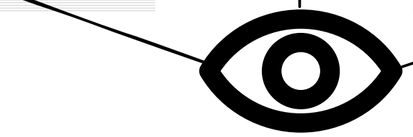
- 자율 사이버 면역 시스템

ACIS 모니터링 & Adeline 전달 항목

- CTHR-01 카드를 대상으로 하는 모든 DMA 읽기/쓰기, 레지스터 접근 및 명령 서술자는 암호화 코어나 HBM2 메모리에 도달 전 전수 조사

- 키 사용 빈도, 프로세스/VM 별 접근 패턴, 펌웨어 상태, 내부 오류 조건, 온도/전력 특성에 대한 실시간 모니터링

- 정의된 키 영역을 벗어난 메모리 주소 접근, 비정상적 데이터 대량 전송, 잘못된 서술자 등에 대해 적대적 공격으로 간주



능동적 하드웨어 경계	CTHR-01 SPU 상에서 PCIe 트래픽, 펌웨어 무결성 및 키 사용 패턴 모니터링
키 추출 원천 차단	HBM2 내 키 영역 외부 노출 차단; 해당 키 영역에 대한 어떠한 접근 시도도 하드웨어 레벨에서 차단
백도어 및 디버깅 경로 차단	양산형 펌웨어의 디버그 및 JTAG 비활성화; ACIS를 통한 물리적 수준에서의 하드웨어 디버그 경로 접근 시도 차단

09. Adeline UI

CTHR-01 SPU시스템 모니터링

“모니터링 사용자인터페이스(UI)”를
제공하는 유일한 보안 가속기”

24/7 프로세서 동작 상태 모니터링
잠재적인 침해 시 경보 제공

다음 페이지 >>

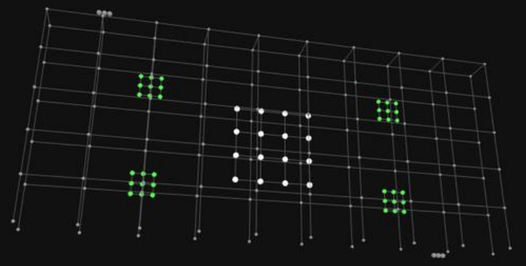
뉴젠스 NEWGENS

CETHERA ADELINE

Overview Fleet Network

CTHR-01

Ready



Avg Temp	H2C	C2H	Total DMA
36.8	0.0 GB	0.0 GB	0.00 GB

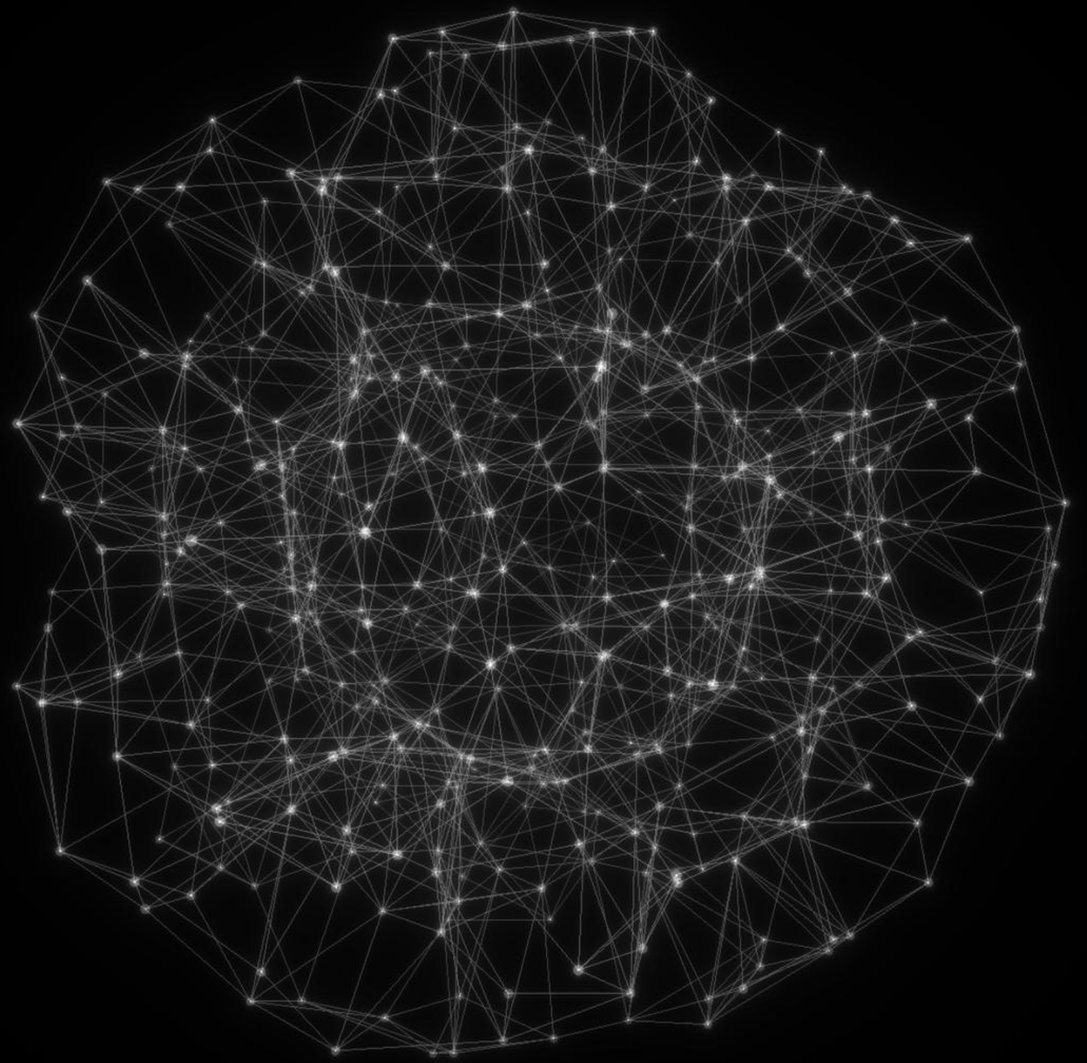
Operations

Telemetry API connected
1h ago — System

Adeline monitoring active
1h ago — System

Hardware Status

[ACTIVE] DMA engine processing data flows - 0.00GB total
[SECURE] Quantum-inspired cryptographic engine operational
[MONITOR] ACIS self-adapting to threat environment
[ACTIVE] High-performance parallel processing active
[SECURE] Physical tamper response systems armed



Network

Connected

Download

Avg	Peak	Min
0.0	0.3	0.0

0.0 Mbps

294764 Packets

Upload

Avg	Peak	Min
0.1	0.4	0.0

0.1 Mbps

Server Overview

Connected

Security Status	Data Mode
NORMAL	ONLINE
CPU Usage	**Memory**
1.3	2.5
Threats	Network Interfaces

Adeline's Analytics

All Systems Nominal

All monitored subsystems are operating within expected parameters. The security hardware accelerator is online and actively enforcing cryptographic boundaries across all data

CTHR-01
Fleet Management System & 네트워크 모니터

다수 서버에 설치된 CTHR-01 카드에 대한 중앙화된 모니터링

다음 페이지 >>

뉴젠스 NEWGENS

Security Subsystems

- System Overview
- Entropy Generator
- Quantum Adapter
- Crypto Utilities
- Homomorphic Engine
- Dynamic Shield
- QE-BCP Processor
- PCIe Integration
- Post-Quantum
- Side-Channel
- Verification

Security Mechanics | Fleet Devices | System Metrics

Fleet Devices

Real-time registry of connected CTHR-01 processors across the secured network

Total Devices	Online	Offline	Active Threats
1	1	0	0

DEVICE LIST

● cethera	BDF: 0000:03:00.0	37.8°C	0.00GB	SECURE

DEVICE STATUS | TECHNICAL DETAILS

DEVICE INFORMATION

Device Name:	cethera
Status:	Online
IP Address:	192.168.0.2
PCIe BDF:	0000:03:00.0
Device Ready:	Yes

THERMAL MONITORING

FPGA Temperature:	37.8°C
Thermal Status:	NORMAL

DMA THROUGHPUT

Host → Card (H2C):	0.000 GB
Card → Host (C2H):	0.000 GB
Total DMA:	0.000 GB
Transfer Rate:	Idle

SECURITY STATUS

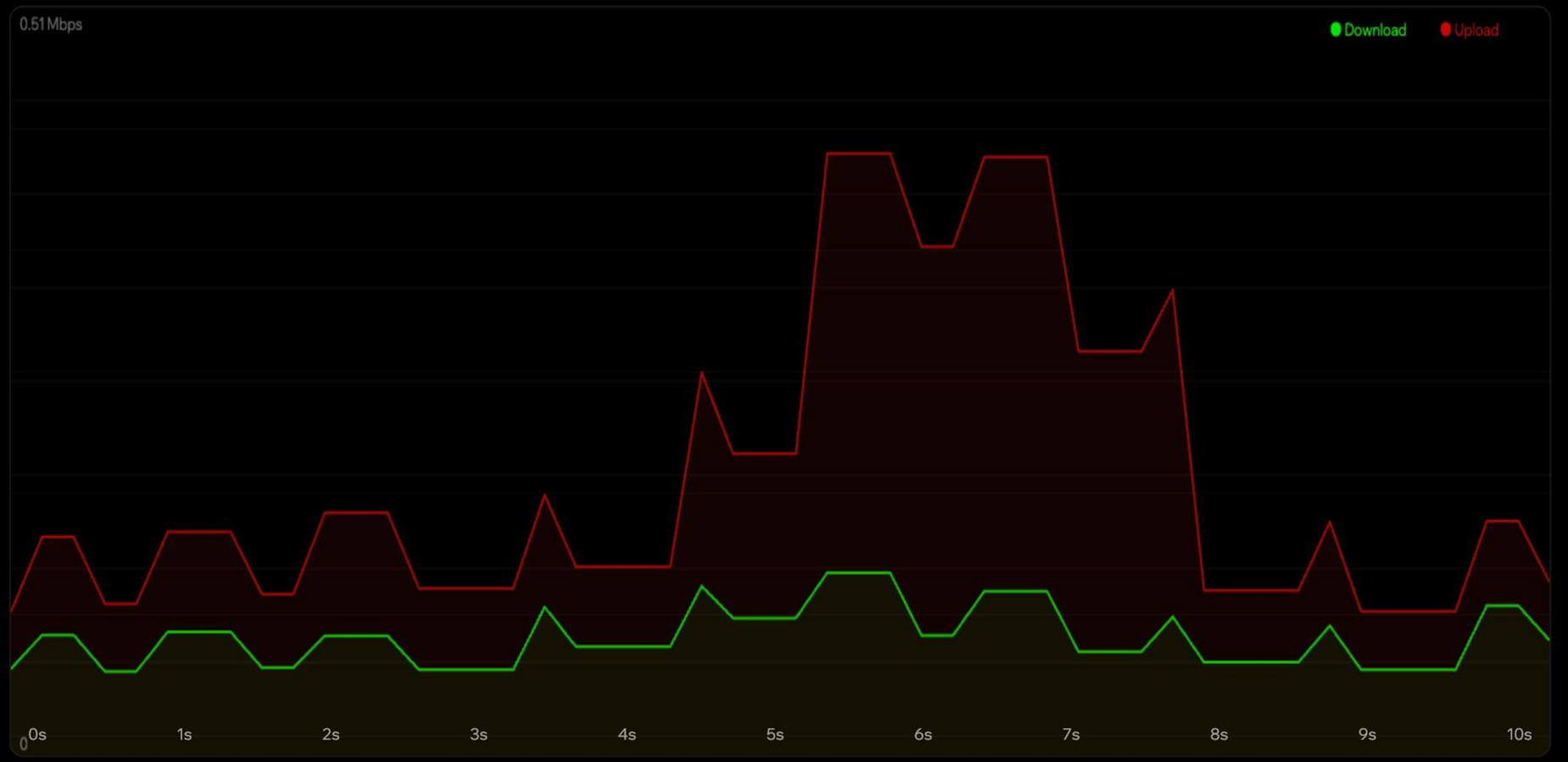
Active Threats:	0
Threat Types:	None

QE-BCP CORE STATUS

QE-BCP Core: STANDBY

CETHERA NETWORK MONITOR

v4.4 | Real-time Network Throughput Analysis



Download:
0.07 Mbps
Trend: ↓

Upload:
0.12 Mbps
Trend: ↓

Average Download:	0.07 Mbps
Average Upload:	0.19 Mbps
Peak Download:	0.47 Mbps
Peak Upload:	2.19 Mbps
Min Download:	0.00 Mbps
Min Upload:	0.00 Mbps
Std Dev Download:	0.14 Mbps
Std Dev Upload:	0.42 Mbps
Coeff. of Variation:	1.90
Active Connections:	13
Packets Received/Sent:	157006/405306

NETWORK RELIABILITY

Consistency: 34%

Classification: Poor

Interpretation: High variance, unstable connection

Variance Coefficient: 1.90x

Upload/Download Ratio: 1.58x

Started: 2026-02-19 07:57:37 | Duration: 36s

CTHR-01 보안 통신 채널

강력한 암호화 통신 채널 | B2G & B2B용 애플리케이션

다음 페이지 >>

뉴젠스 NEWGENS

CTHR-01 SECURE CHANNEL

Hardware-Accelerated Cryptographic Security Platform

DEVICE: DEVICE 5020

SERIAL: 4DAE-0946-E057-C1C2

FILE SELECTION

No file selected

BROWSE

OPERATION MODE

(•) ENCRYPT ( ) DECRYPT

SECURITY OPTIONS

[ ] Enable Device Binding

Target Device ID: 4DAE-0946-E057-C1C2

START PROCESSING

CANCEL

PROCESSING STATUS

0%

READY

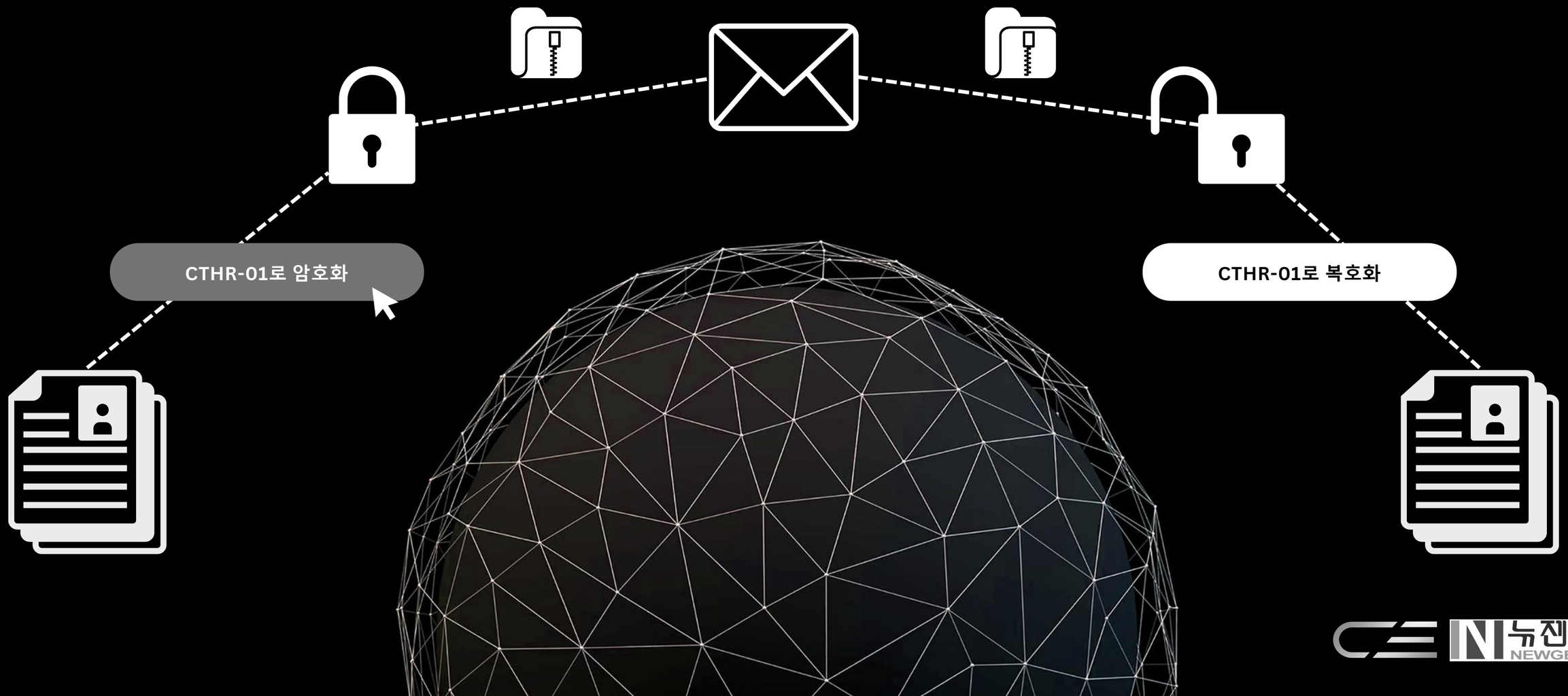
SYSTEM LOG

```
[07:30:25] ✓ System initialized
[07:30:25] » Device: 4DAE-0946-E057-C1C2
[07:30:25] ✓ FPGA: Device 5020 @ 0000:04:00.0
[07:30:25] ✓ Encryption: QE-BCP
```

SECURE CHANNEL

CTHR-01 - CTHR-01 간 암호화된 파일 전송을 위한 부가적인 기능

CTHR-01가 설치된
모든 곳에서 사용 가능



10. 구성 절차

CETHERA CTHR-01
SERIES 1

엔비디아 GPU 구성과 동일

NVIDIA QUADRO
RTX 6000

주문 & 배송

PCIe 슬롯에 장착

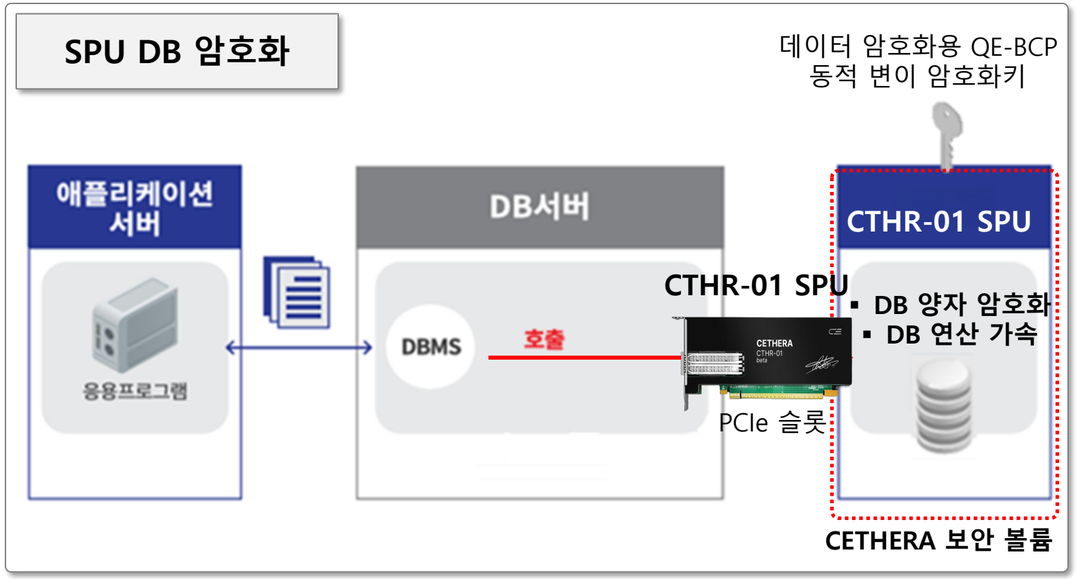
드라이버 및 소프트웨어
(ACIS/Adeline) 설치

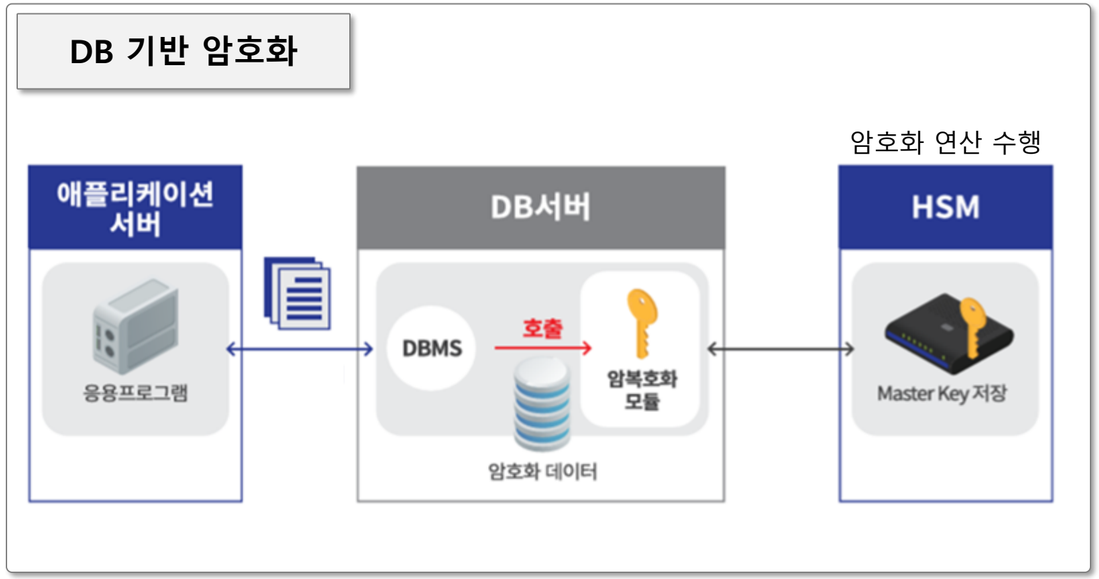
구성 완료

뉴젠스 NEWGENS

11. 적용 방안

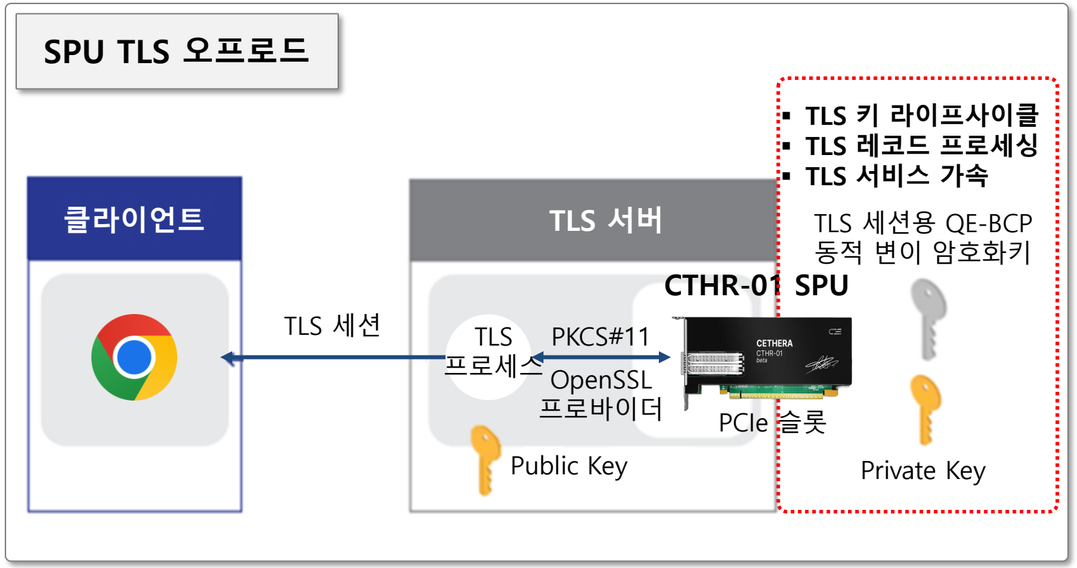
■ DB암호화 가속

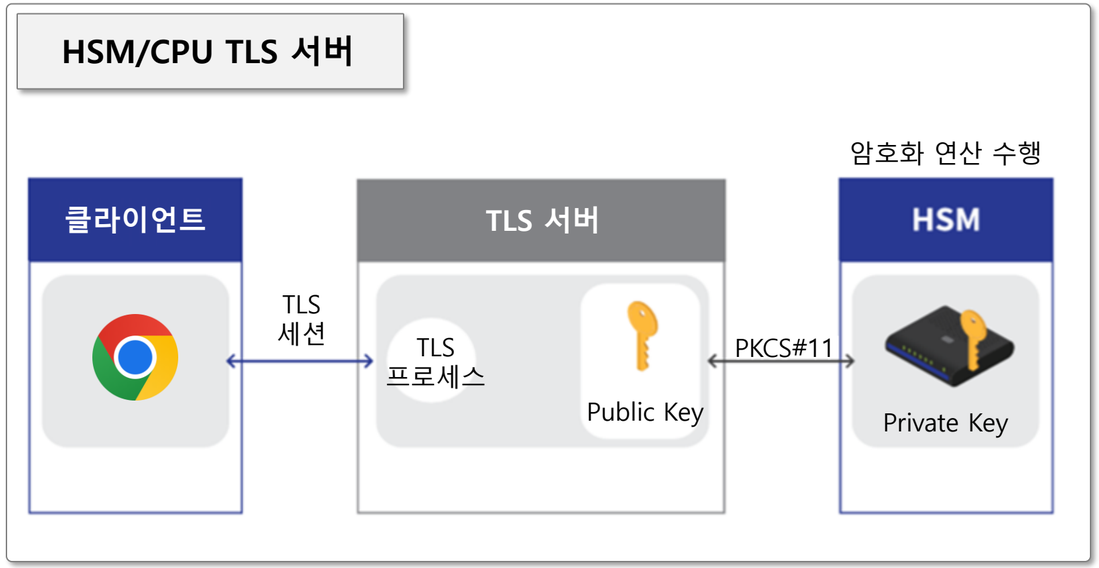




구분	CTHR-01 SPU DB 암호화	일반 TDE DB 암호화
처리 주체	전용 PCIe 가속기(8GB HBM2, 316+GB/s)	서버 메인 CPU
CPU 부하	하드웨어로 오프로딩하여 부하 최소화	암/복호화 시 CPU 점유율 상승
암호화 알고리즘	QE-BCP(양자얽힘 기반) 및 ACIS 적용	AES 등 표준 알고리즘 적용
보안 수준	양자내성암호(PQC) 이상의 강력한 HW 수준 보안 제로-평문 노출 구조	키 유출 및 SW 취약점에 노출 가능성 메모리 내 평문 변환에 따른 탈취 우려
적용 방식	CETHERA 보안 볼륨으로 DB 파일 이전	일반 DBMS 제공 기능
KMS/HSM	불필요	필요
추가 라이선스	불필요	추가 필요(비용 증가)

■ TLS 서비스 오프로드



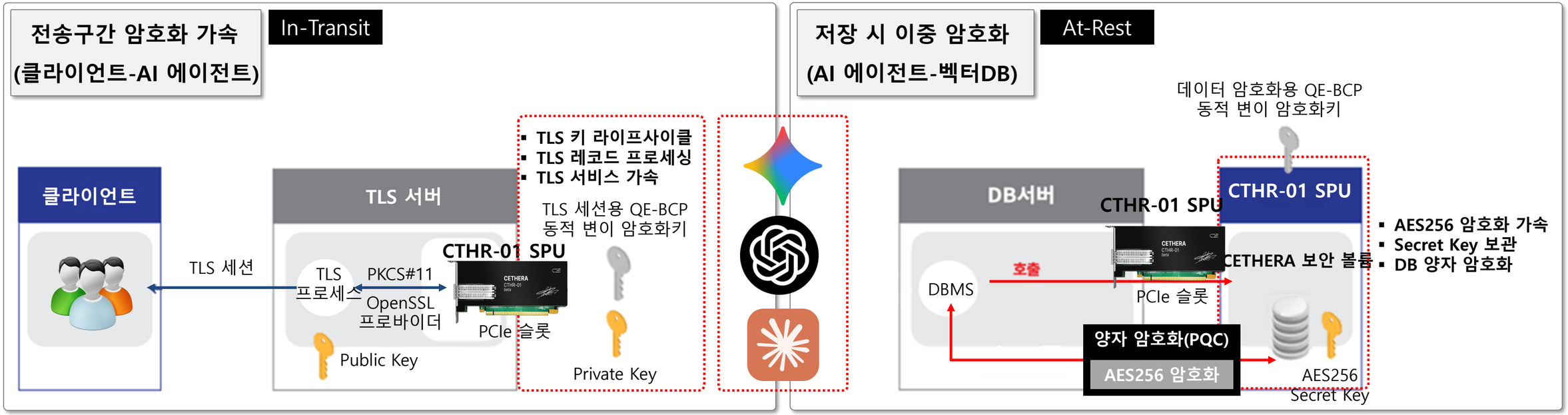


구분	CTHR-01 SPU TLS 오프로드	HSM/CPU TLS
처리 주체 (TLS 1.3 키 스케줄)	전용 PCIe 가속기	서버 메인 CPU
CPU 부하	하드웨어로 오프로딩하여 부하 최소화	CPU 점유율 상승
프라이빗 키 위치	전용 PCIe 가속기 내 보안 저장소	서버 메모리
세션 키 위치	전용 PCIe 가속기 내 메모리	서버 메모리
HSM	불필요	필요

■ AI 데이터 보안 강화

- 저장 시 암호화 (Encryption at Rest)
  - DB 서버의 디스크에 저장되는 벡터 데이터 암호화(AES-256) 가속(호환성 보장)
  - QE-BCP를 통한 개선된 양자내성암호화(PQC) 적용(하드웨어 수준 보안성 강화)

- 전송 시 암호화 (Encryption in Transit)
  - AI 에이전트 - DB 구간, 혹은 사용자 환경 - 서버 구간 암호화 전송을 위한 TLS 서비스 가속
  - TLS 프로토콜(AES-GCM)을 사용해 가로채기 공격(Sniffing) 방지



12. CETHERA 회사 개요

CETHERA는 "CE (Cyber Entropy)와 THERA (테라 섬)"의 합성어로, 변화하는 환경 속에서 엔트로피를 이용해 동적으로 진화하고, 구시대적인 보안 모델을 재정의하겠다는 목표를 추구합니다.

- CPU / GPU / DPU와 차별화된 "보안 처리 장치(SPU, Security Processing Unit)"라는 새로운 형태의 보안 하드웨어 카테고리 산업을 창출하고 있는 대한민국의 딥테크 기업
- AI, 클라우드, 디지털 금융 환경에서 증가하는 보안 위협에 대응하기 위한 새로운 보안 아키텍처 개발
- 기존 소프트웨어 중심 보안 모델의 한계를 넘어 Hardware Root of Trust 기반 보안 플랫폼 지향
- 목표 시장 : 데이터센터, 통신사, 금융기관 등 핵심 인프라 환경

주요 핵심 인력

Nikita Bondarenko

- 연세대학교 창의기술경영(CTM) 전공
- 신경망 & 하드웨어 엔지니어
- CEO & 설립자
- 양자 기술을 통한 보안 시스템 + 지적재산권 보유

Alexey Korepin

- 수석 SW 엔지니어(CSE, Chief Software Engineer)
- 컴퓨터 보안 & 시스템 엔지니어
- Adeline & 보안 프로토콜 통합

Kellen Ray Tanaka

- 연세대학교 창의기술경영(CTM) 전공
- AI 프로그래밍 & 머신러닝 분야 스페셜리스트
- Adeline을 위한 수학적 UI/UX 디자인

이범준 CEO

- 서울대학교 전자공학 전공
- UC 버클리 컴퓨터 과학 석사
- 30년 이상 텔레콤 및 AI 인프라 사업 부문 종사

윤원석 박사

- 인천경제자유구역청 제8대 청장(IFEZ, Incheon Free Economic Zone)
- 대한무역투자진흥공사(KOTRA) 경제통상협력본부장
- 글로벌산업경쟁력포럼 회장
- 한글과컴퓨터그룹 해외사업총괄사장

뉴젠스 NEWGENS

엔지니어링, 랩실 운영 & 국내 영업 총괄(5+ 엔지니어)

Technology Ownership & IP

Security Devices and Systems using Quantum Technology
No. 10-2025-0079734

CONTACT US

World’s First SPU

Executive Vice President of Sales,
BumJun Lee
bj.lee@cethera.com

WWW.CETHERA.COM

General Inquiries
info@cethera.com

Investment Inquiries
ir@cethera.com

Founder, Nikita Bondarenko
nikita@cethera.com