

CDEF Co., Ltd. — Company Profile

2026.07



CONTENTS

1. Company Overview
2. Background of the Proposal
3. CDEF Core Technology
4. Business Status

Company Overview - General Status



CDEF currently sells a SEED-algorithm-based file encryption solution [API license], and has launched **SHIFT-S [IDS + Stealth HDD]**, a hardware-based data-leakage-prevention solution.

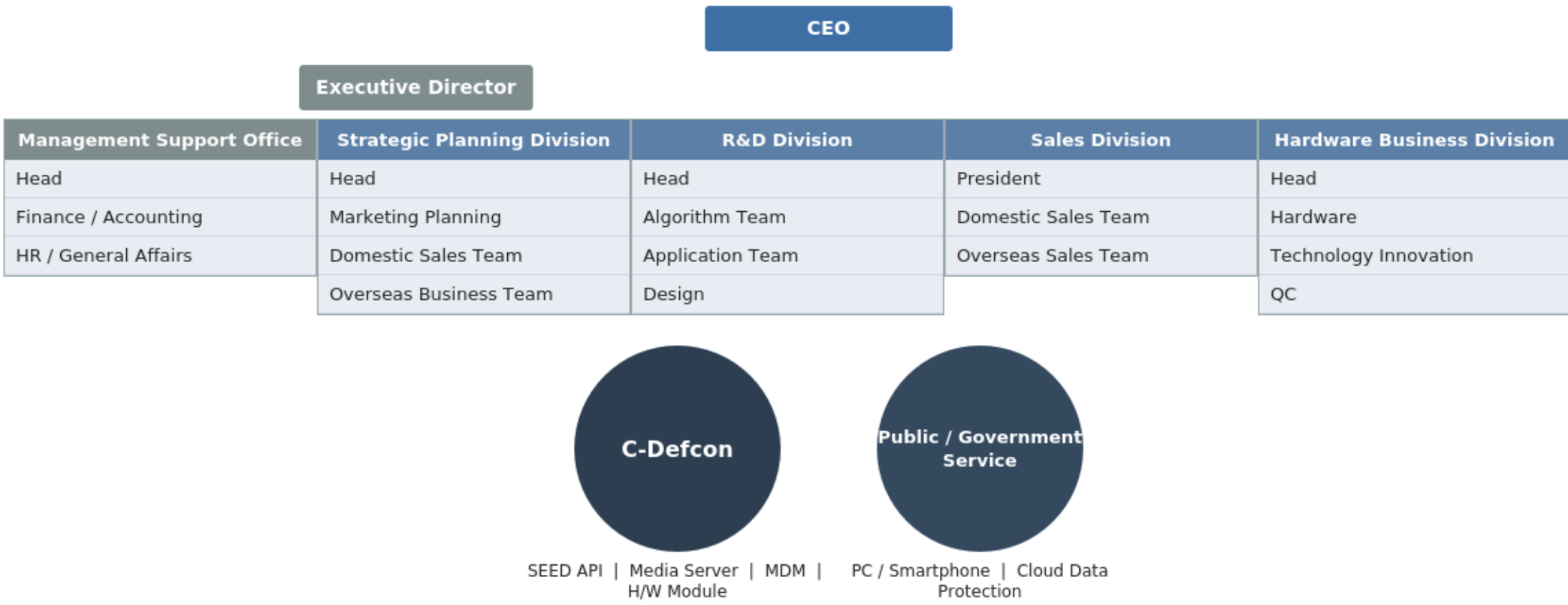
Company Name	CDEF Co., Ltd.	Founded	April 21, 2020
CEO	Ko Hee-gun	Employees	4 (as of Jan. 2023)
Corporate Reg. No.	761-81-02024	Business Reg. No.	483-88-01196
Capital		Industry	Applied Software Development
Address	Rm. 914, ACE High-End Tower 9, 233 Gasan Digital 1-ro, Geumcheon-gu, Seoul, Korea		
Main Products	• SEED Encryption High-Speed Algorithm Engine • Non-Encoding Media Streaming Server • Live Commerce (Open Mall / Closed Mall) • Hardware-based IDS/IPS information-security solution – ERP, SI/SM		
New Business Products	• Real-time CCTV encryption/decryption • WebRTC encrypted video conferencing • Modified SEED Encrypt/Decrypt Engine (API) • Blockchain DID document exchange (hospitals, government offices, certifications, etc.)		

IDS: Intrusion Detection System IPS: Intrusion Prevention System MDM: Mobile Device Management

Company Overview - Organization Chart



The business organization consists of **4 business divisions and 1 support office** (encryption algorithm field, applied applications).



Business Foundation Period (2016-2018)

1996-2017: Foundation

- 01: CDEF [corporate entity] – encryption algorithm development, WELL function applied
- 02: ERP encryption operations transferred
- 03: DB encryption operations transferred

«Key Achievements»

- In-house ERP builds (Dongyang Machinery, Goje, Outback, etc.)
- Patent-Net 3rd phase build
- Defense ATCIS 3rd phase build
- Joint Chiefs simulated-combat system build
- Korea Institute for Defense Analyses system build
- CJ Distribution integrated dev. build (VIPS, Tous Les Jours, Hancook, Seafood)
- Indonesia / China Lotte Mart build
- China Zhonggong Network messenger dev.
- Lotte Mall build (Gimpo, Dongdaemun, Jamsil, Suwon)

2018

- 01: SEED encryption engine dev. begins
- 02: SEED algorithm dev. begins
- 03: SEED video-encryption V1.0 developed

Growth Foundation Period (2019-2020)

2019

- 01: CDEF Co., Ltd. established
- 02: SEED video-encryption V1.1 completed
- 03: Ghost HDD solution dev. begins
- 04: SEED file-encryption API sales begin
- 05: Ghost HDD PCIe Card 1st dev. / Agent S/W test version
- 06: MDM (SMB) dev. begins / Media Server update
- 07: IDS/IPS Agent dev.

2020

- 01: IDS/IPS Agent beta test
- 02: Live Media Server v1.0 launched
- 03: Real-time CCTV encrypt/decrypt
- 04: IO Community distribution corp. established

Growth Leap Period (2021-2024)

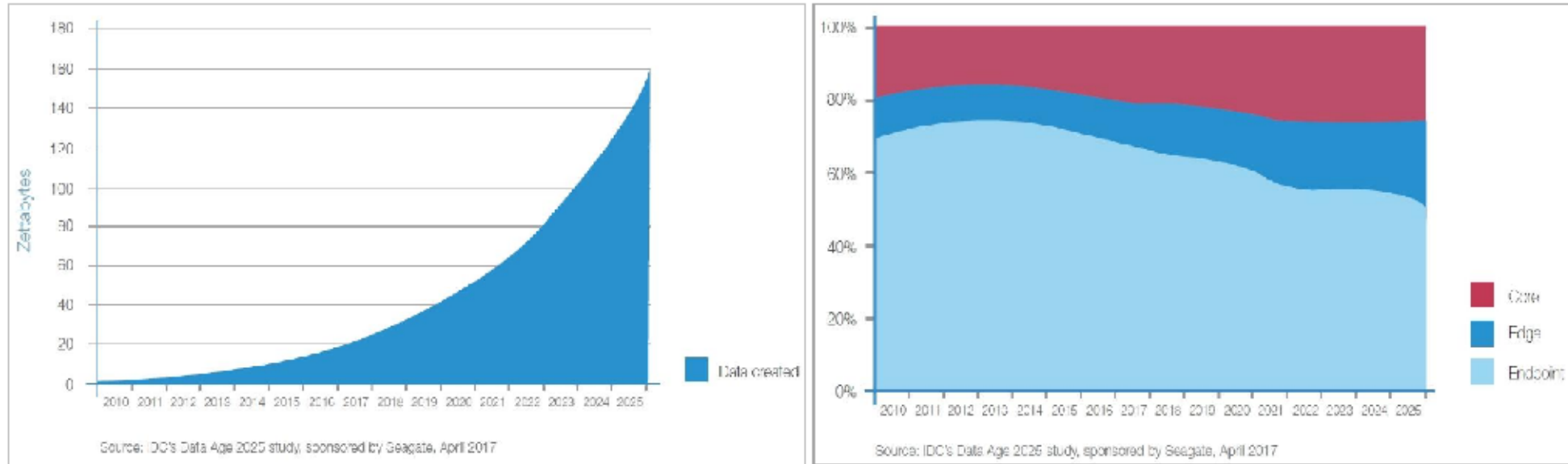
2021-2023

- 01: Video encryption dev.
- 02: Document encryption dev. completed
- 03: CCTV encryption module completed
- 04: Image encryption module completed
- 05: PCI-type Ghost HDD H/W & S/W dev.
- 06: R&D center established
- 07: Core encryption tech. performance improved
- 08: Hanwha Techwin AI camera real-time encryption dev.

2024-2025

- 01: AI-accelerated original SEED tech. dev.
 - 02: Integrated encryption messenger tech. dev. (purchasing agency)
 - 03: CDEF NFT COIN dev.
 - 04: TTA GS certification submitted (planned)
 - 05: GS certification acquisition (planned)
 - 06: KCMVP certification acquired
 - 07: K-POP Mall dev.
 - 08: K-Youth Business Group Mall dev.
 - 09: Military PX Mall dev. – in negotiation
- 2025:** Additional patents/certifications; K-POP Mall purchasing-agency service (May); official launch of encryption coin

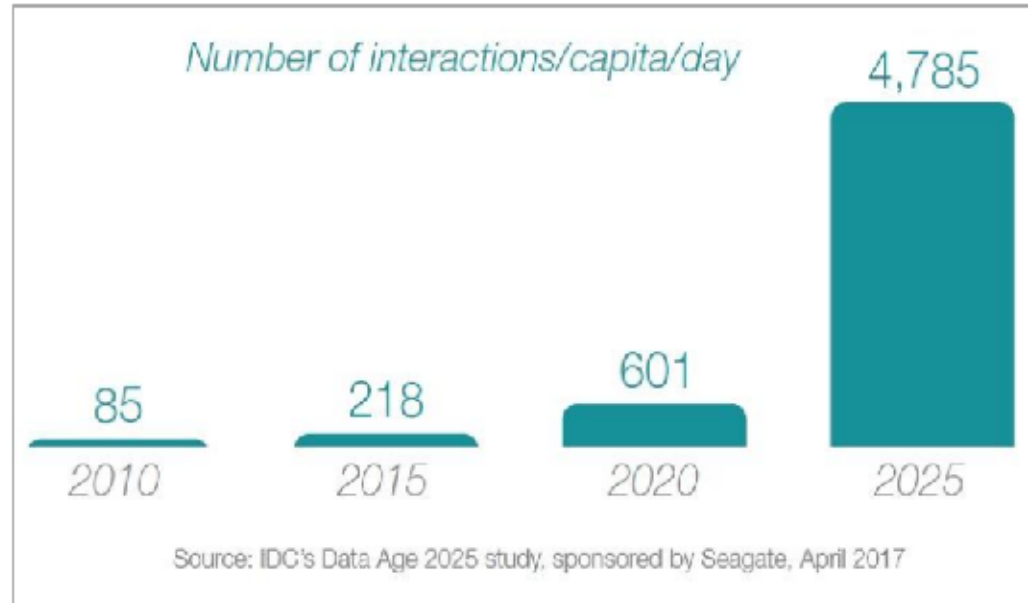
IDC “Global data volume in 2025 forecast at 175ZB, growing at 61% CAGR”



- IDC projects total worldwide data volume will grow from 33ZB in 2018 to 175ZB by 2025 – a 61% average annual increase
- The 2017 IDC 'Data Age 2025' White Paper forecast of 163ZB was revised up 9% to 175ZB in the 2018 outlook
- Data-creation sources fall into Endpoint (Web, PC, Mobile) / Edge (IoT, CCTV, autonomous driving) / Core (Data Center, Cloud, Big Data, AI)
- Edge and Core data are expected to see explosive growth going forward
- 1 Zettabyte (ZB) = 1,024 Exabytes (EB) = 1.1 trillion Gigabytes (GB) – enough to store 28.15 trillion 3MB MP3 songs

Background of the Proposal - Interaction & Data-Driven Business

“By 2025, a data interaction will occur roughly every 8 seconds - explosive growth of data-driven business”



- Daily data interactions per capita from the Internet, mobile, and IoT grew from an average of 85/day in 2015 to a projected 4,785/day by 2025 - about once every 8 seconds
- Explosive growth of data-driven business such as Industry 4.0 & Smart Factory, Smart City
- Rapid data growth is creating simultaneous issues in infrastructure, traffic, and **security**

Background of the Proposal - Data Security Issues

*“Ever-growing data volume / rapid traffic increase / increasingly complex infrastructure / **speed issues**”*



Video | Audio | Image
Document | Sensing | Etc.

- Security issues arising from massive data volumes generated by numerous devices and systems
- Speed issues that emerge when applying security to large-volume, ultra-high-speed, hyper-connected environments
- Structural limitations in the encryption/decryption process of encryption algorithms – the core element of security

“Parallel-processing encryption algorithm / pure software-based / real-time large-volume data encryption & decryption”

C-DEFCON Encryption Engine

C-DEFCON Encryption Engine

- NIS(National Intelligence Service)-certified standard encryption algorithm applied
- SEED, ARIA 128-bit / 256-bit encryption
- Parallel-processing, expandable encryption/decryption structure
- Large-volume, real-time ultra-high-speed encryption/decryption

Network Protocol Control

- Supports multiple communication protocols (TCP/UDP/RTCP/RTP)
- Real-time streaming support
- Memory-based ultra-high-speed transmission

C-DEFCON Key Management

- Key-management module stored separately (key leakage impossible)
- C-DEFCON's proprietary encryption-key management
- Proprietary Nonce and WELL algorithm applied
- Dedicated decryption-management program

Data Control

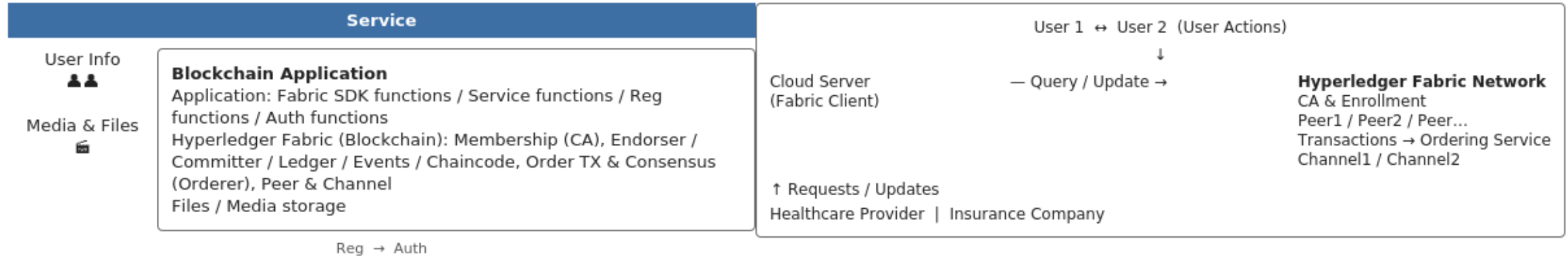
- High-speed transmission - matrix media-balancing engine
- Video/audio object-analysis structure (OpenCV-based)
- Encryption/decryption by payload (I/P/B-Frame)
- Supports any data format (video, audio, document, etc.)

“Parallel-processing encryption structure / pure software-based / real-time large-volume data encryption & decryption”

Data Source	C-DEFCON Encryption & Decryption Architecture			Supported
CCTV & IP Camera	Encryption & Decryption Core Engine Parallel threads (Thread-01..04), each performing SEED/ARIA block encryption in parallel (“Thread+α” expandable structure)	KEY Management Unique Key (IV) – “Key = like an OTP”. NONCE + WELL combination, per-thread individual key. NONCE: KEY(IV) attribute, User No/USIM ID, Time Stamp/GPS, MAC/Bluetooth. WELL: duplicate-prevention algorithm, random-function generation, expanded distribution range.	Data Control Matrix media-balancing engine. Video/audio object analysis (OpenCV). Any-data-format transmission. Encrypt/decrypt by payload (I/P/B-Frame).	iOS & Android
Video, Audio, Image				Cross Browsing
Document, Drawing, Graphic				All Devices
Cloud, AI, Big Data		Network Protocol Control TCP/UDP/RTCP/RTP. Real-time streaming transmission. Memory-based transmission.	C-DEFCON API Web / Mobile / Embedded. Multi-OS (Windows, Linux). Any data format supported.	Multi-OS

- Parallel-processing thread structure for encryption/decryption, expandable in parallel – “Thread+α”
- Proprietary key-management structure (Nonce, WELL applied)
- Supports all data sources, devices, and multiple OS

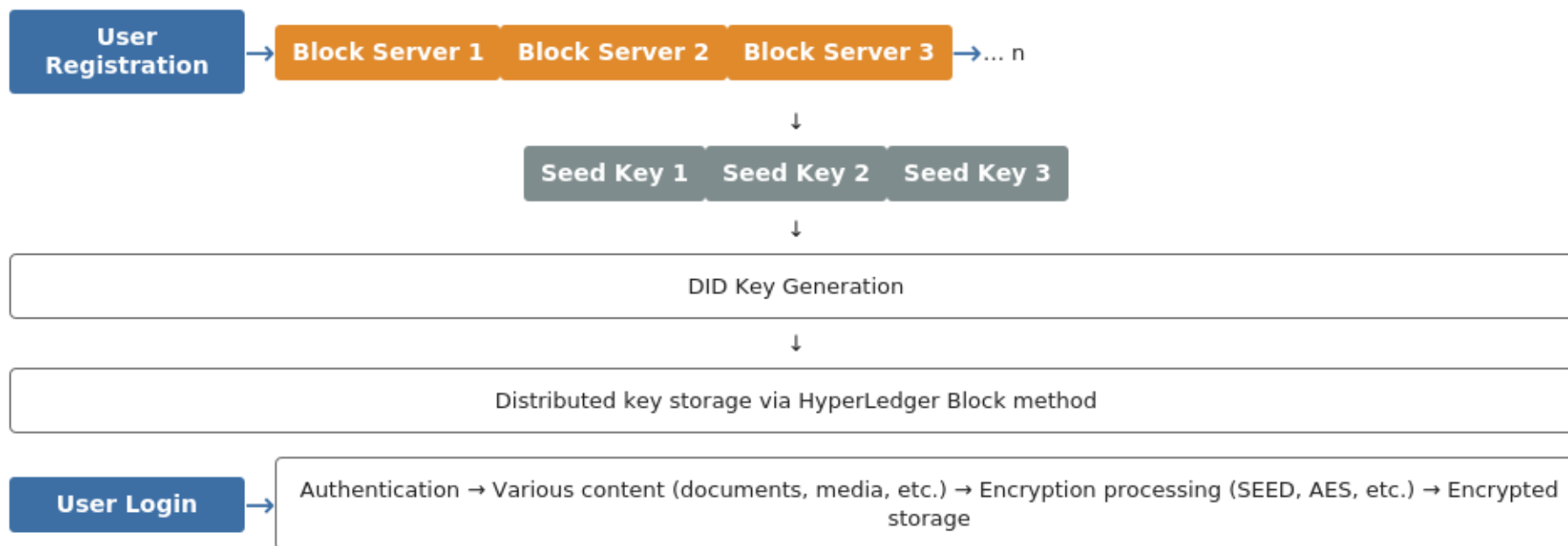
“Distributed storage of encryption keys via HyperLedger Blockchain DID generation”



- Encryption keys are distributed across cloud servers, so decryption is impossible unless **all** servers are compromised in an attack
- Existing blockchains use a minimal ledger-based approach for fast Digital ID access
- Adopts next-generation quantum theory (quantum code), enabling an expandable DID technology with unlimited random-number processing when generating server keys

"Issuance of encryption keys via HyperLedger Blockchain DID generation"

- 👤 User
- 📱 iOS & Android
- 🌐 Cross Browsing
- 🖨 All Devices
- 🖥 Multi-OS



CDEF Core Technology - Live Commerce H/W Configuration



Internet / PSTN → Firewall → Internal Network

Broadcast Studio

Filming Equipment (real-time): 4K+ camera, lighting / mic / prompter

Broadcast Editing Equipment: Editing PC / 32" monitor

OS: Windows 10+, CPU: Xeon Dual, RAM: 64GB, HDD: 2TB, WAS: Apache/Tomcat

Blockchain DID Server 1 / 2 / 3

OS: Linux/Windows 10+ CPU: i7

RAM: 32GB HDD: 2TB

WAS Server

OS: Linux/Windows 10+ CPU: Xeon Dual

RAM: 64GB HDD: 2TB WAS: Apache/Tomcat

DB Server

OS: Linux/Windows 10+ CPU: Xeon Dual

RAM: 64GB HDD: 2TB DB: MySQL

Media Server

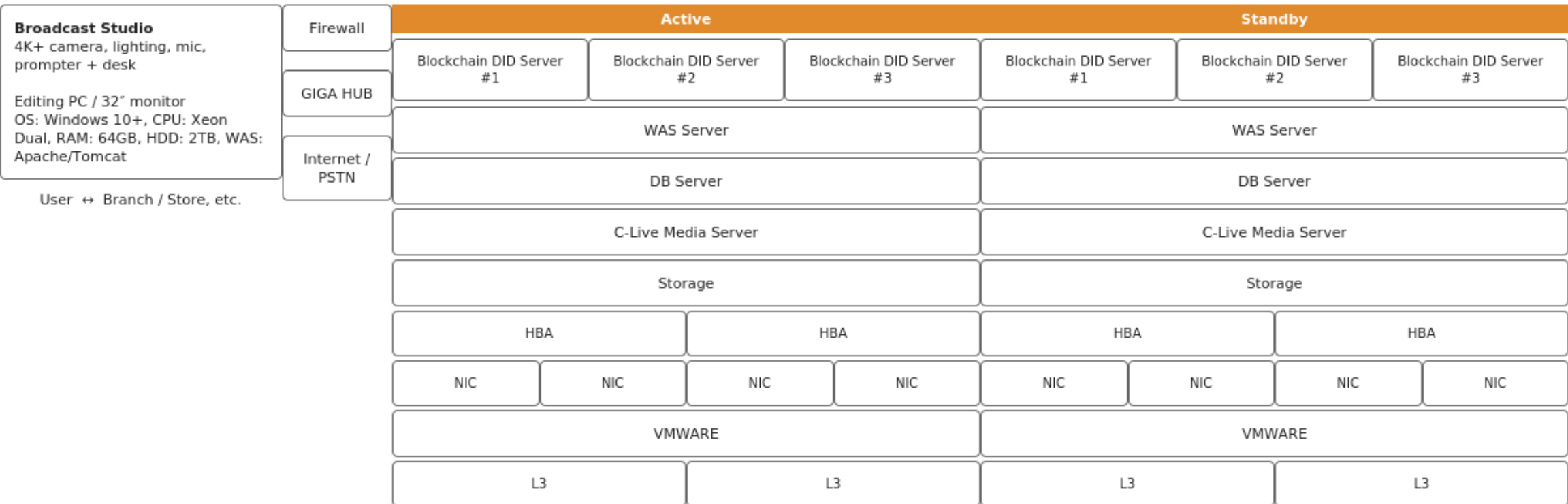
OS: Linux/Windows 10+ CPU: Xeon Dual

RAM: 128GB HDD: 10TB Supports 1,500 concurrent connections

Storage

WAS, DB, Media - 10TB total

CDEF Core Technology - Live Commerce Redundant (Failover) H/W Configuration



“Parallel matrix data transmission / memory-based transmission & computation / OpenCV object analysis”

Existing Method



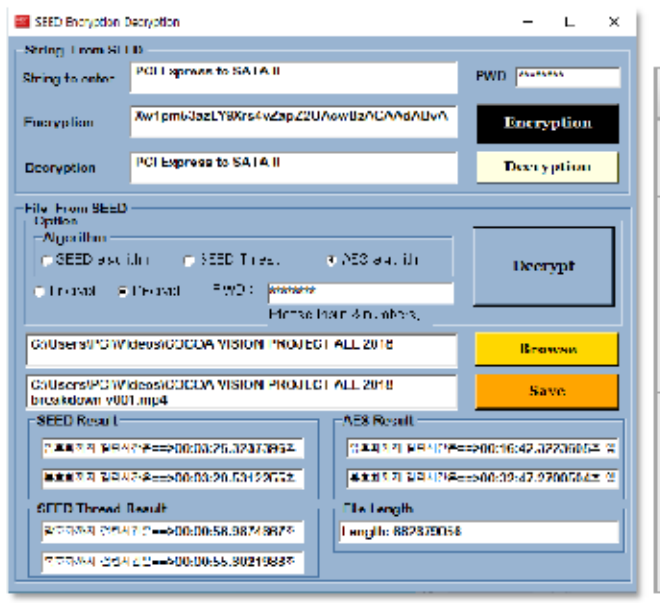
- Video/audio transmission via file streaming results in large data volume (serial format, e.g. 010010101010101100110)
- The VMS server requires CPU computation to parse frame, coordinate, and RGB data
- Speed issues occur during data transmission and parsing
- Real-time encryption/decryption is not possible when encryption is applied to this method – most current video encryption uses VMS asynchronous encrypt/decrypt

C-DEFCON



- Parallel matrix transmission results in small data volume (matrix packets include frame, coordinate, RGB data together)
- No separate parsing required – memory-based transmission and computation enable high-speed transfer
- OpenCV structure applied / object analysis possible (CDEF patent registered)
- Real-time encryption/decryption and transmission possible

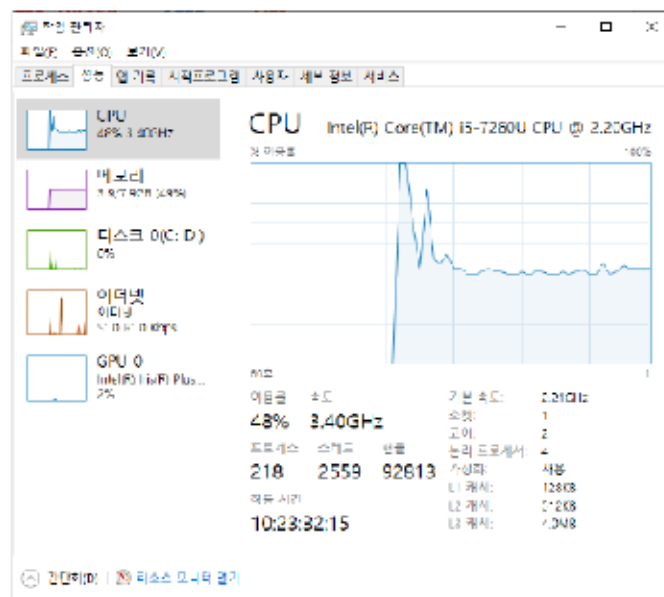
“Parallel-processing encryption structure / pure software-based / real-time large-volume data encryption & decryption”



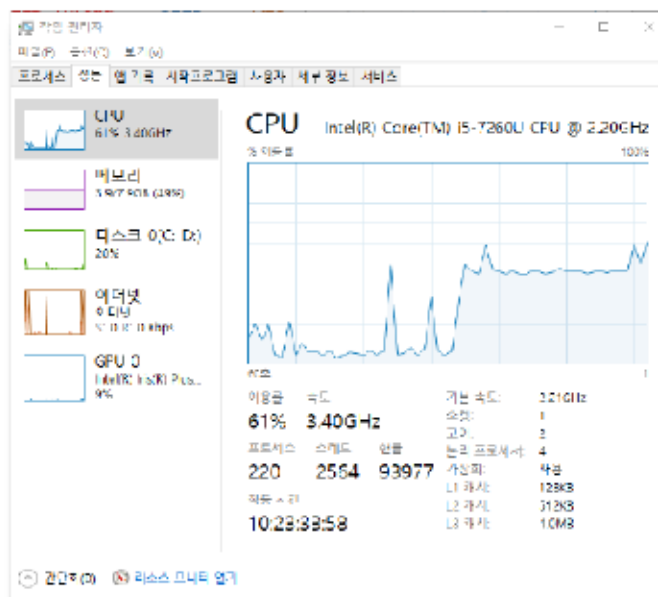
Data Source	650MB video MP4 file – encryption/decryption performance evaluation
Encryption Performance	C-DEFCON Algorithm: 56.98 sec SEED Algorithm: 3 min 25 sec AES Algorithm: 16 min 42 sec C-DEFCON → 3.6× faster than SEED, 16.8× faster than AES
Decryption Performance	C-DEFCON Algorithm: 55.30 sec SEED Algorithm: 3 min 20 sec AES Algorithm: 32 min 47 sec C-DEFCON → 3.5× faster than SEED, 33.7× faster than AES

- C-DEFCON: based on 4-thread parallel SEED algorithm encryption/decryption (performance scales with additional threads)
- Simultaneous parallel encryption/decryption of a single file using multiple threads (C-DEFCON's proprietary feature)
- Outstanding performance compared to existing SEED and AES algorithms – the gap widens further as data volume increases

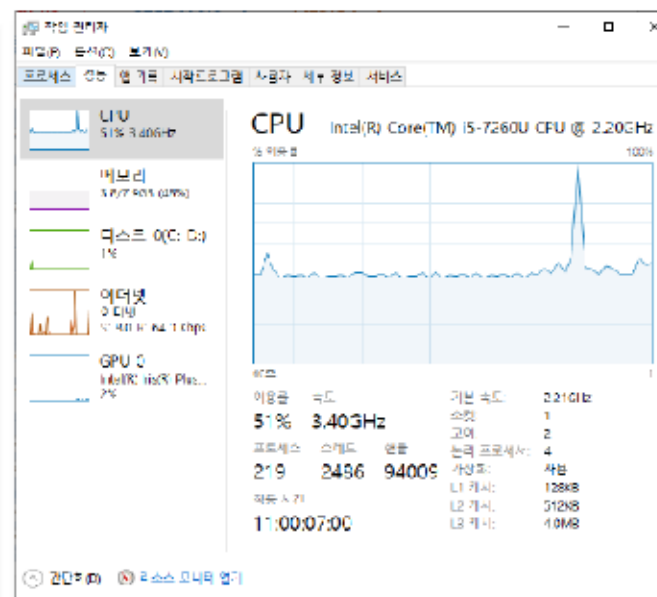
“Parallel-processing encryption structure / pure software-based / real-time large-volume data encryption & decryption”



[C-DEFCON]



[SEED]

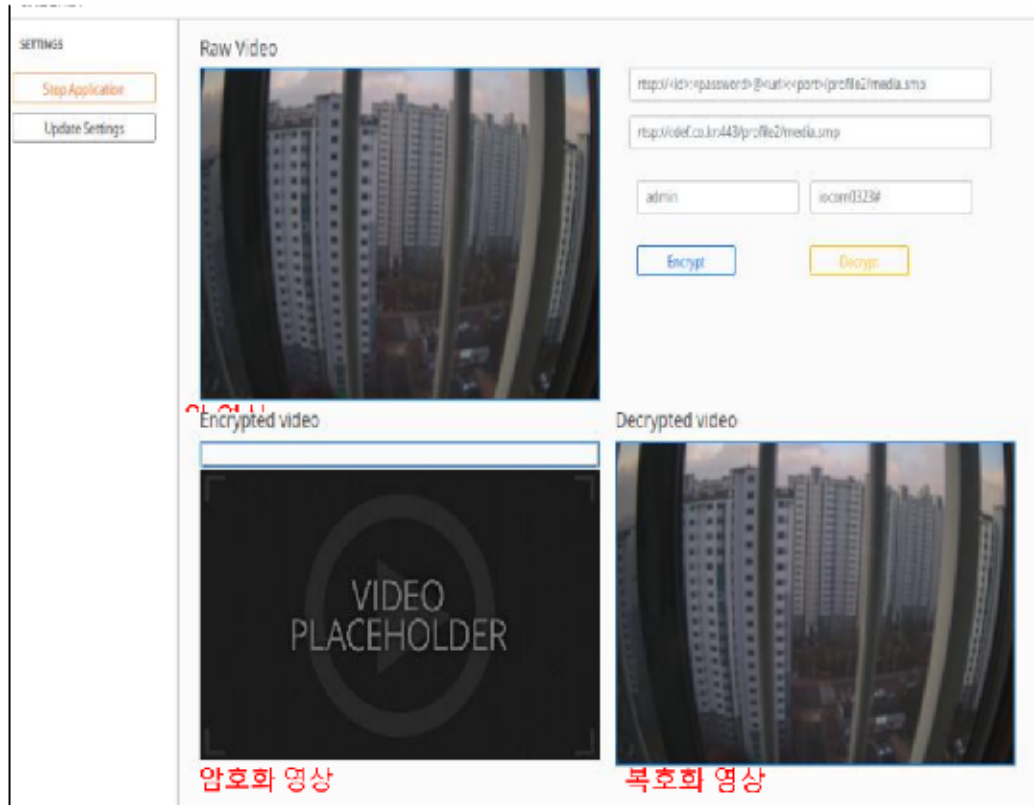


[AES]

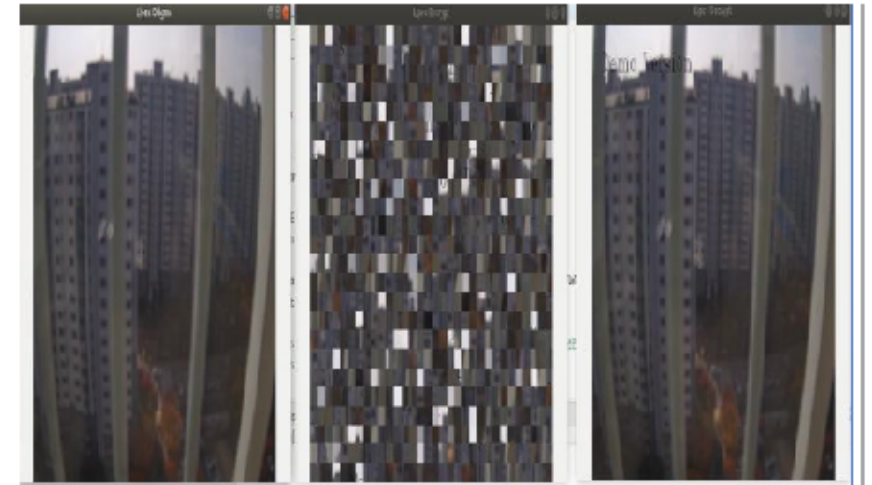
- When evaluating encryption/decryption performance, CPU and other resource usage show minimal difference versus other encryption algorithms

“Real-time video encryption/decryption footage”

◆ Camera Firmware in Operation



◆ Encrypted / Decrypted Footage



Left to right: Original • Encrypted • Decrypted

“World’s first HDD physical security / hardware-based data security / rapid data protection”

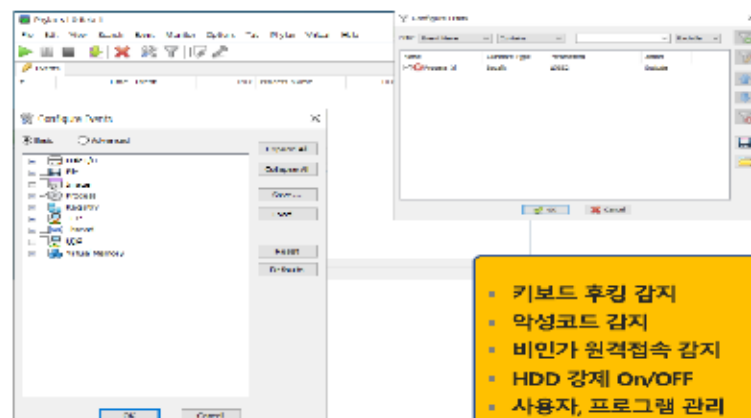
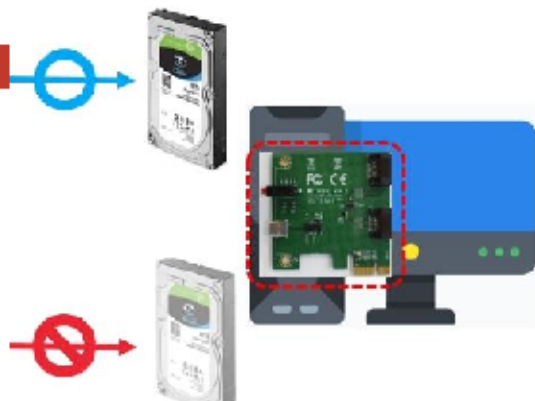
Authorized Programs



Unauthorized Programs



Malware, unauthorized remote access, etc.



- Keyboard-hooking detection
- Malware detection
- Unauthorized remote-access detection
- Forced HDD On/Off
- User & program management

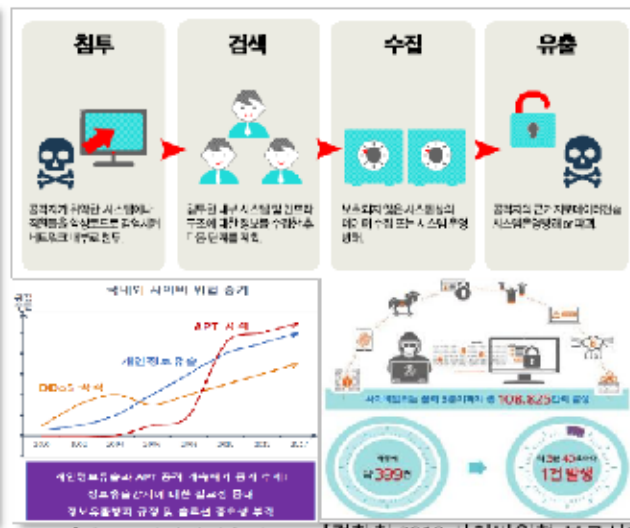
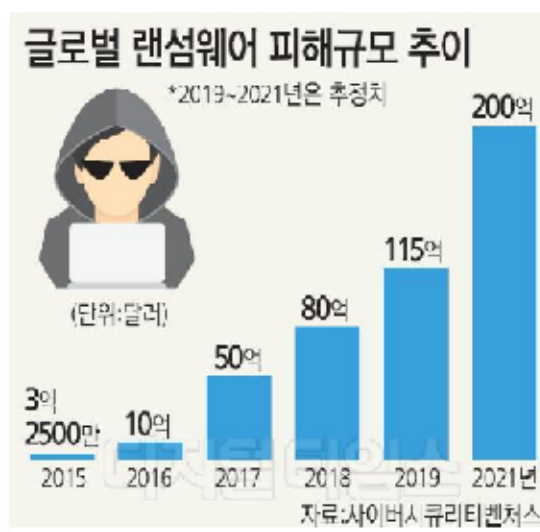
- When an issue occurs, the HDD is physically disconnected to fundamentally prevent data damage or leakage
- A Ghost HDD management PCI board connects to existing or new HDDs on the PC; a PC Agent continuously monitors for keyboard hooking, malware, and unauthorized remote access
- On anomaly detection, a blacklisted-program launch, or access by an unregistered user, the HDD connected to the Ghost HDD PCI board is disconnected
- Available in STA / PCI hardware form factors

연도별 국내 랜섬웨어 피해 규모

○ 접수건수(건)
■ 총피해금액(억원)

연도	접수건수(건)	총피해금액(억원)
2015	2,678	1,090
2016	3,255	3,000
2017	4,475	7,000
2018년(예상)	8,000	15,000

자료: 한국랜섬웨어청해대응센터



- Data damage and leakage from ransomware and other malware continues to increase, both domestically and internationally
- Anti-virus, firewall, and intrusion-prevention products offer only about 30-50% protection
- 87% of cyberattacks were blocked, yet the actual number of data-leak incidents did not decrease

“Expansion of QR-code-based simple payments / Qshing countermeasure security / financial payment & O2O business growth”

Forged/altered QR codes cause financial theft and malware distribution

Normal QR Code → forged/altered → Malicious QR Code

↓ user scans (step 2) ↓

User Device → (3) accesses hacking site → Hacking Site (malicious)
or → Normal Site (if unaltered)

(1) QR code forged/altered • (2) QR code scanned • (3) hacking site accessed



- Starting in China, the QR-code-based simple-payment market continues to grow (QR payments account for 78.5% of all payments in China); domestically expanding via ZeroPay
- QR codes are vulnerable to forgery/alteration and carry high security risk from “Qshing” (QR + Phishing); general users cannot tell a forged code from a genuine one just by looking
- A fundamental security solution for QR codes is required. Qshing exploits forged/altered QR codes to cause financial theft and malware distribution

“QR-code-based simple payment expansion / Qshing countermeasure security / financial payment & O2O business growth”



Existing QR Code

C-DEFCON Encryption

C-QR Code



Merchant ↔ Server (auth-code & QR-module generation, real-time C-QR send/receive) ↔ Buyer

Flow: (1) Server requests QR code from authentication center → (2) C-DEFCON encryption applied (QR Code + auth code) → (3) C-DEFCON auth-code generation server & QR data-module generation server → (4-5) Buyer selects product, bank transfer from buyer's bank to merchant's bank → (6-7) QR code verified → (8) transfer approved after verification → (9) C-QR code sent/received in real time

- QR-code encryption via C-DEFCON SEED block encryption – hacking impossible
- Unique-key generation and duplicate prevention based on C-DEFCON's proprietary Nonce and WELL algorithms
- C-QR Code uses parallel processing, so recognition speed is nearly identical to existing QR codes – 100% compatible with existing QR scanners and equipment

✓ A foreign resident in Korea promotes a product → a friend abroad pays

- Cosmetics, clothing, luxury goods
- Local specialty products



- ① Sender
- ② Product info
- ③ Price info
- ④ Pay

- (1) Info sent
- (2) Payment
- (3) QR sent
- (4) QR match check & product receipt
- (5) Funds deposited

- ① Select product
- ② Proxy payment
- ③ Info sent

✓ Deliver item to a friend in Korea → ship abroad

- Confirm recipient → deliver item
- Overseas shipping → customs duty refund

Domestic Foreign
Resident

Overseas
Foreigner

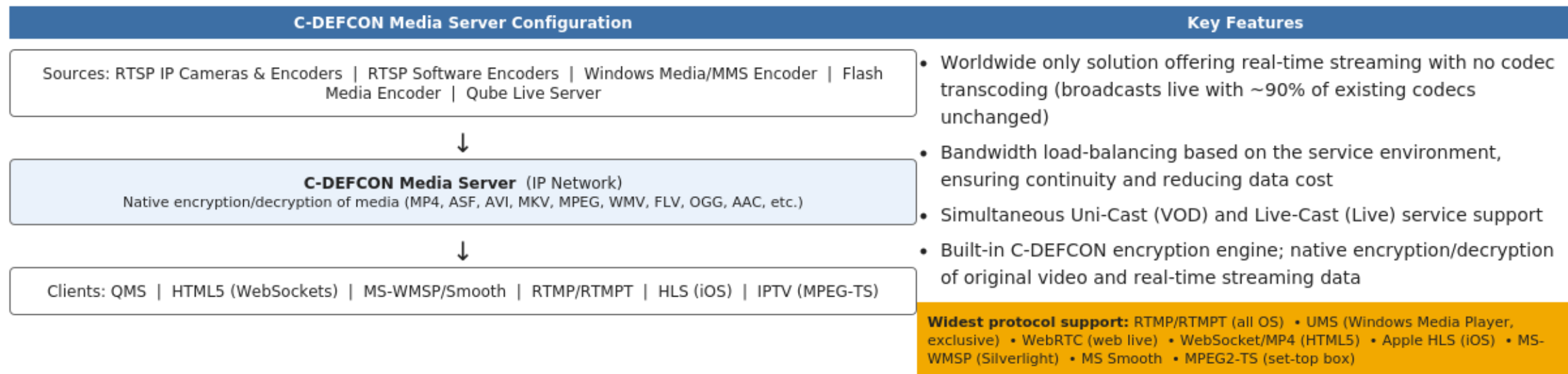
Merchant

- The domestic foreign resident visits the merchant, scans the QR code of the product of interest, and sends it to a friend abroad [merchant, product, price, payment screen, etc.]
- The overseas friend completes payment via the payment screen, entering the domestic recipient's phone number → a 'payment confirmed' message is sent to them, and the QR code is sent to both the merchant's tablet PC and the domestic recipient's phone
- The domestic recipient scans their received QR code on the merchant's tablet PC, which compares it against the QR code it received
- If the two match, the product is handed over to the domestic recipient, and a delivery confirmation is sent to the overseas friend

Notes:

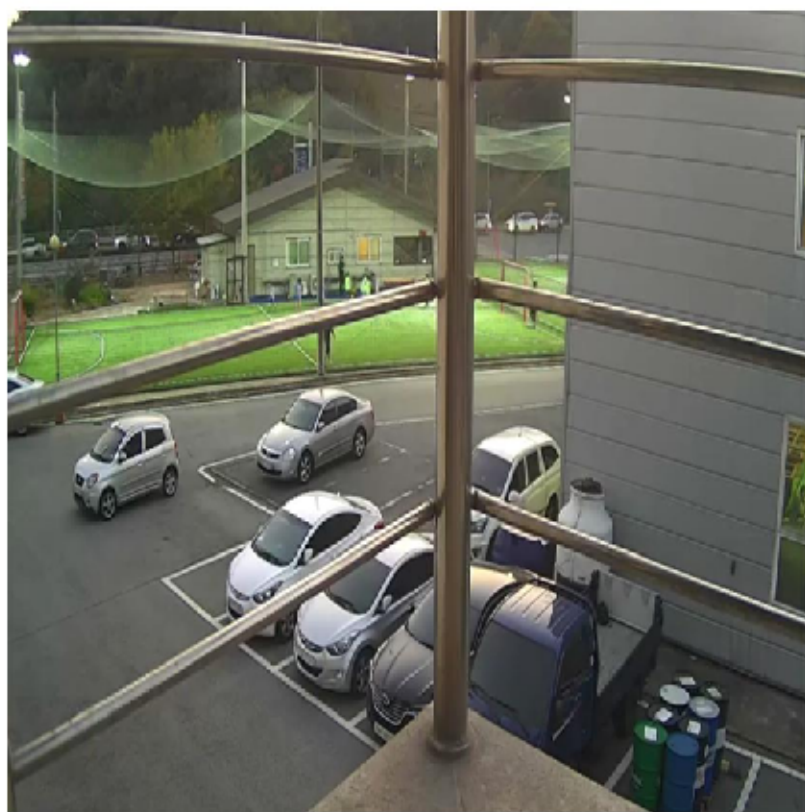
1. The QR codes sent to the merchant and the recipient include a matching code (e.g., a PIN) to confirm the two correspond
2. The tablet PC holds multiple recipient QR codes
3. It checks whether a QR code matching the one the recipient scans exists among them
4. When the tablet PC's QR code matches the recipient's, the purchase and hand-over are complete

“No-transcoding real-time streaming / native encryption of original & streaming data / broadest codec support”

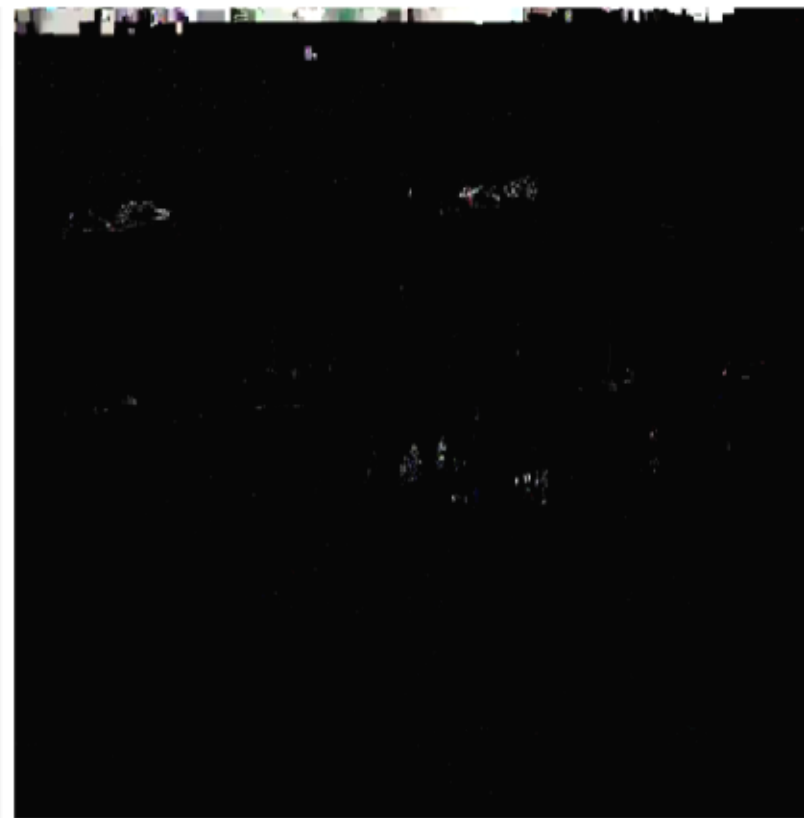


“Real-time video encryption/decryption footage”

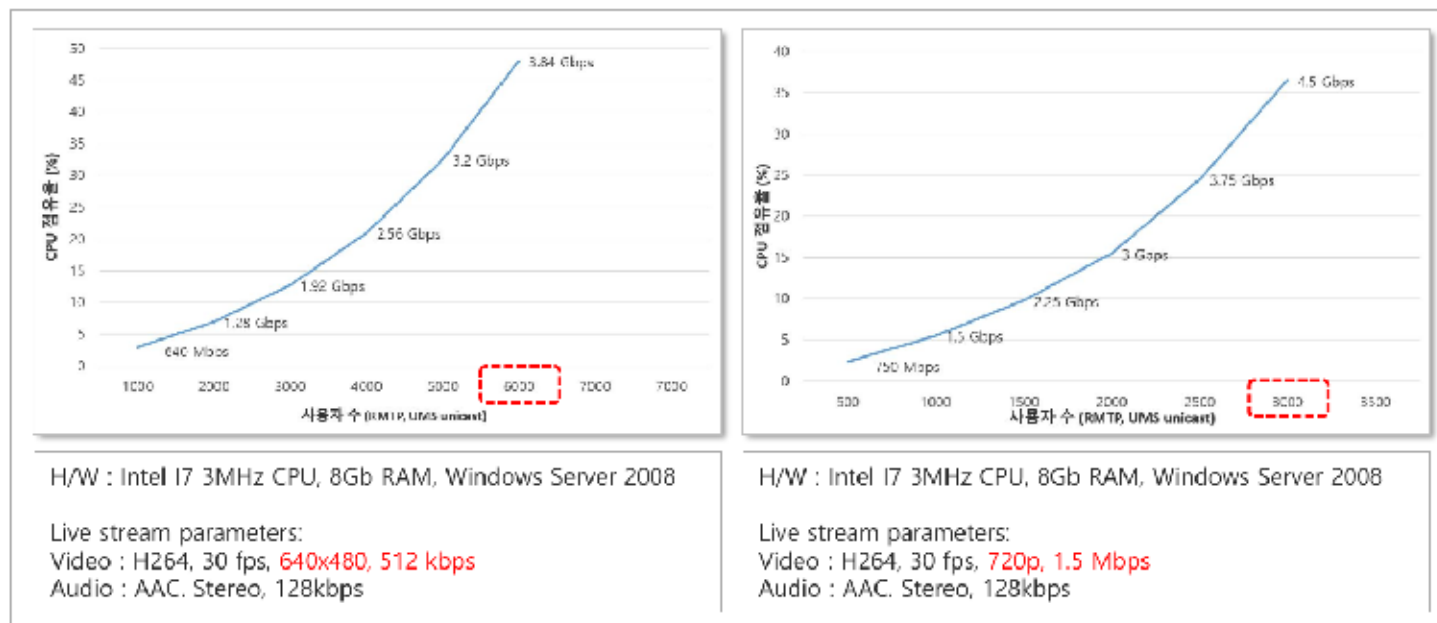
◆ Original Footage



◆ Encrypted Footage



“No-transcoding real-time streaming / native encryption of original & streaming data / broadest codec support”



- A PC-class server (Intel i7, 3MHz CPU, 8GB RAM, Windows Server 2008) can handle 3,000–6,000 concurrent unicast users depending on stream bitrate (512kbps @ 640x480 vs. 1.5Mbps @ 720p)
- Large-scale connections and service are possible even on low-spec hardware, and remain stable even on low-bandwidth networks

 **Have you seen the various security technologies above?**

Engine

Accelerated encryption/decryption engine

Content

Real-time video/content encryption & decryption

Simple Payment

Encrypted QR

Commerce

International purchasing agency



**CDEFCON
-TRADIFY**

- ❖ Confidence and trust in your own assets and the wallet you use.
- ❖ Use your own assets anytime, anywhere – easily and safely.

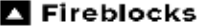
An integrated, community-based encrypted service platform providing customers with USD bank accounts, making it easy to exchange and use digital assets.

Tradify.live

- Weak security of exchange platforms
- Most exchanges operate illegally, without a license
- Limited service offering (Crypto to Crypto only)
- Limited liquidity (trading volume insufficient)
- Unable to exchange to FIAT currency
- Limited number of coins offered
- Unspecialized, one-size-fits-all platforms
- Unspecialized support systems

An integrated blockchain technology that solves the current problems of cryptocurrency exchanges →

- Tradify holds an exchange license and can legally operate by sharing that license.
- We prioritize security using technology also used on NASDAQ.
- Connected with 30+ exchanges, providing abundant liquidity.
- Our platform is a proven, award-winning platform (Digiday Technology Award 2020).
- Provides wallets for 500+ coins.
- FIAT exchange gateway.

Core Function	Details
Wallets 	◆ Tradify has partnered with Fireblocks to provide a world-class SEED-encrypted wallet that guarantees safety. ◆ Companies using the platform can use Fireblocks at no additional cost, giving customers a trustworthy wallet.
Prepaid Card  	◆ All companies using Tradify can pay out to customers via our prepaid card. ◆ A business card is provided in Korea, with a solution allowing companies to manage it directly.

CDEF Core Technology - Why the Integrated Model CDEFOCN-TRADIFY?



“Cryptocurrency, like cash and cards, is only truly electronic money when it has fairness and anonymity.”
“True currency is one with an ecosystem that can be immediately converted to cash (or reward points).”



 **Fireblocks**

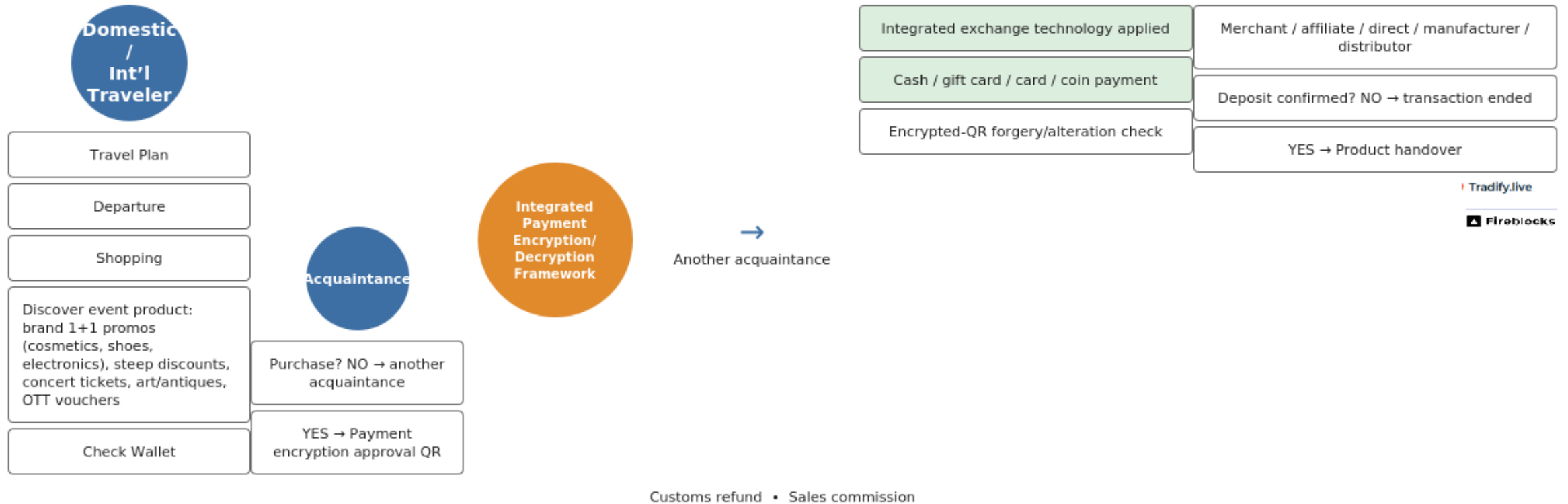
CDEFCON Encrypt Wallets

- ✓ A foreign resident in Korea promotes a product → a friend abroad pays (cosmetics, clothing, luxury, local specialties)
- ✓ Deliver item to a friend in Korea → ship abroad (confirm recipient, customs duty refund)

Tradify.live



CDEF Core Technology - CDEFOCN-TRADIFY Flow



Tradify.live



BΔNXΔ

mercuryo

 Fireblocks

 TREZOR

NIUM

 efficacious

 debanc.

intercash

TECHR∞

 aerapass

CDEF Core Technology - Drone Video Encryption



Storage (crash-proof: if the drone crashes, encrypted storage cannot be decrypted)



C-DEFCON

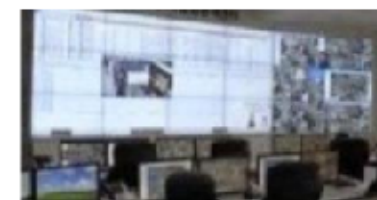
Real-time footage encryption



LTE/5G/RF/Any Protocol •
Video/control/location module



Stream Media Server



Remote monitoring control room -
real-time decrypted playback



THANK YOU