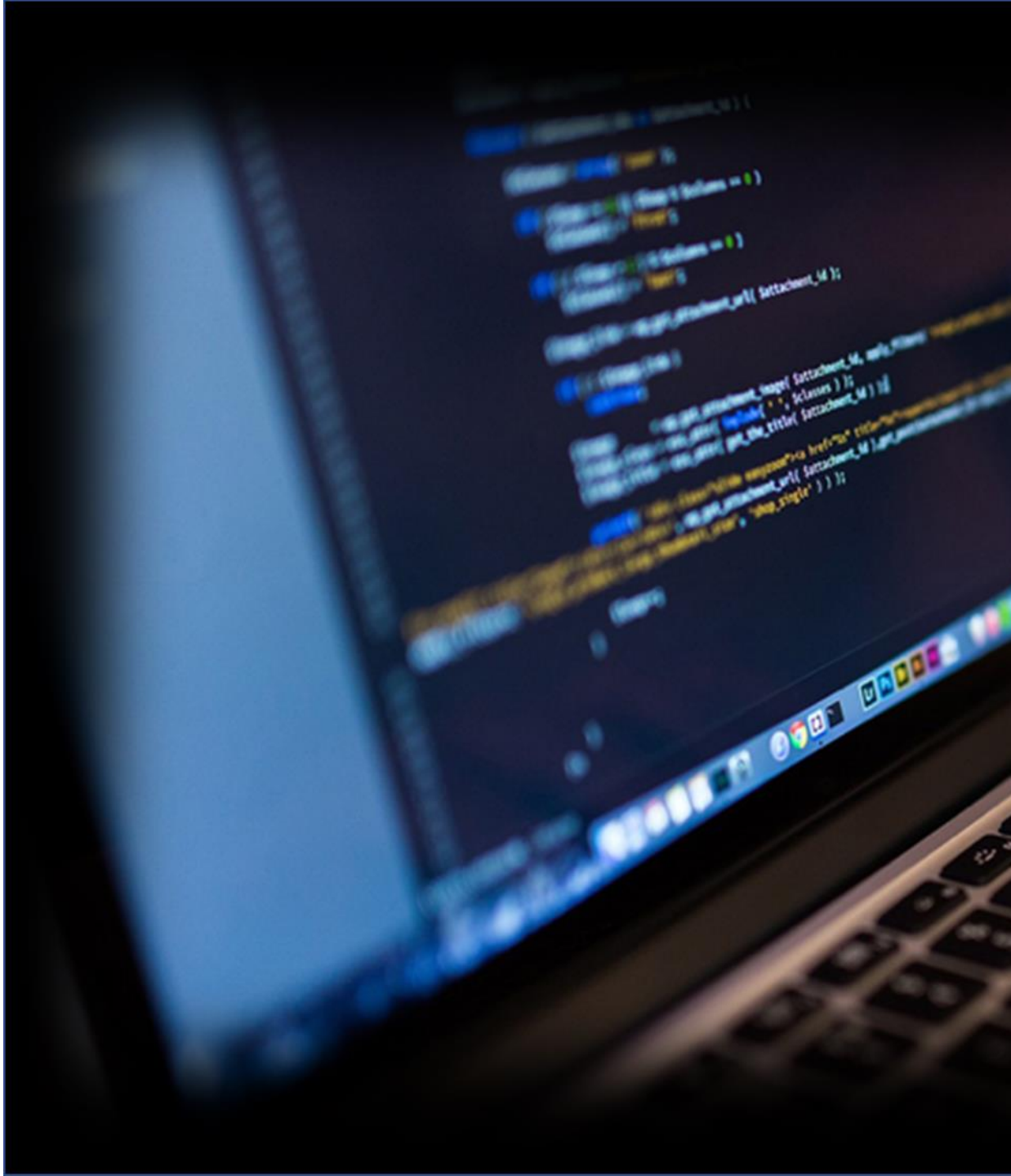
TrustSoT
Solution Intoroduction

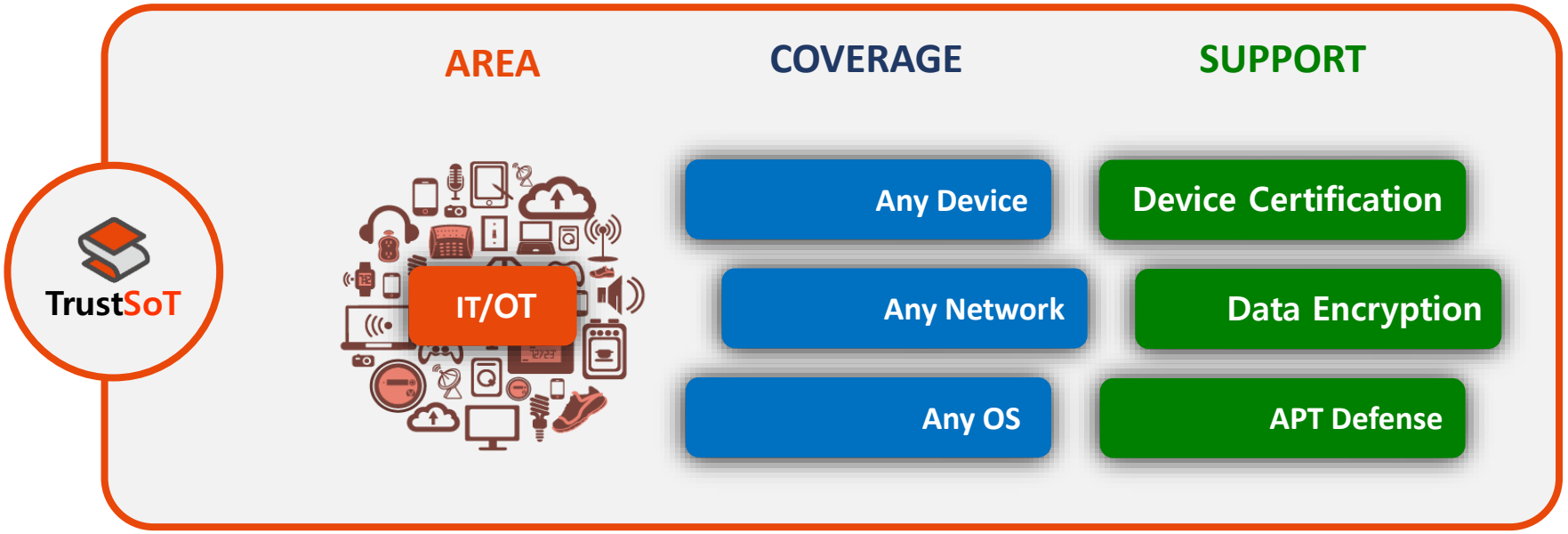
2022



TrustSoT Concept

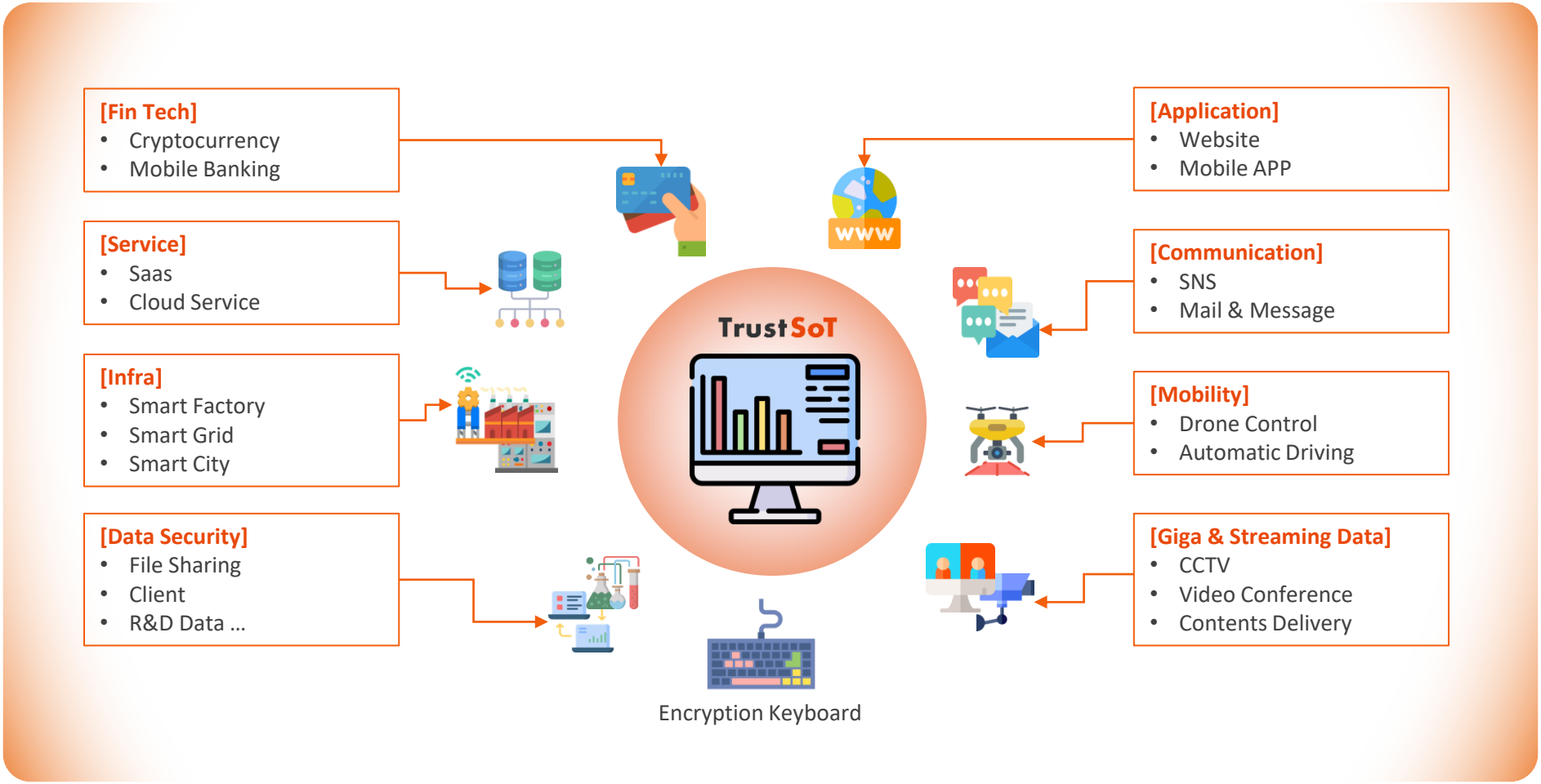
Based on its own patents, **TrustSoT**

- uses「**ultra light software library**」,「**device certification**」, and「**encryption at the point of data genertion**」technologies to
- **regardless** of types of「**Decive**」,「**Network**」, and「**OS**」.
- provide the most optimal security system that satisfies the customer's objectives in「**private information**」,「**confidential information of companies and public institutions**」,「**consignment management information such as Cloud**」, and「**large file streaming videos**」, as well as「**Remote and Automatic Control Industry** (OT/ICS [Note 1)])」and「**Communication Infrastucture Construction**」



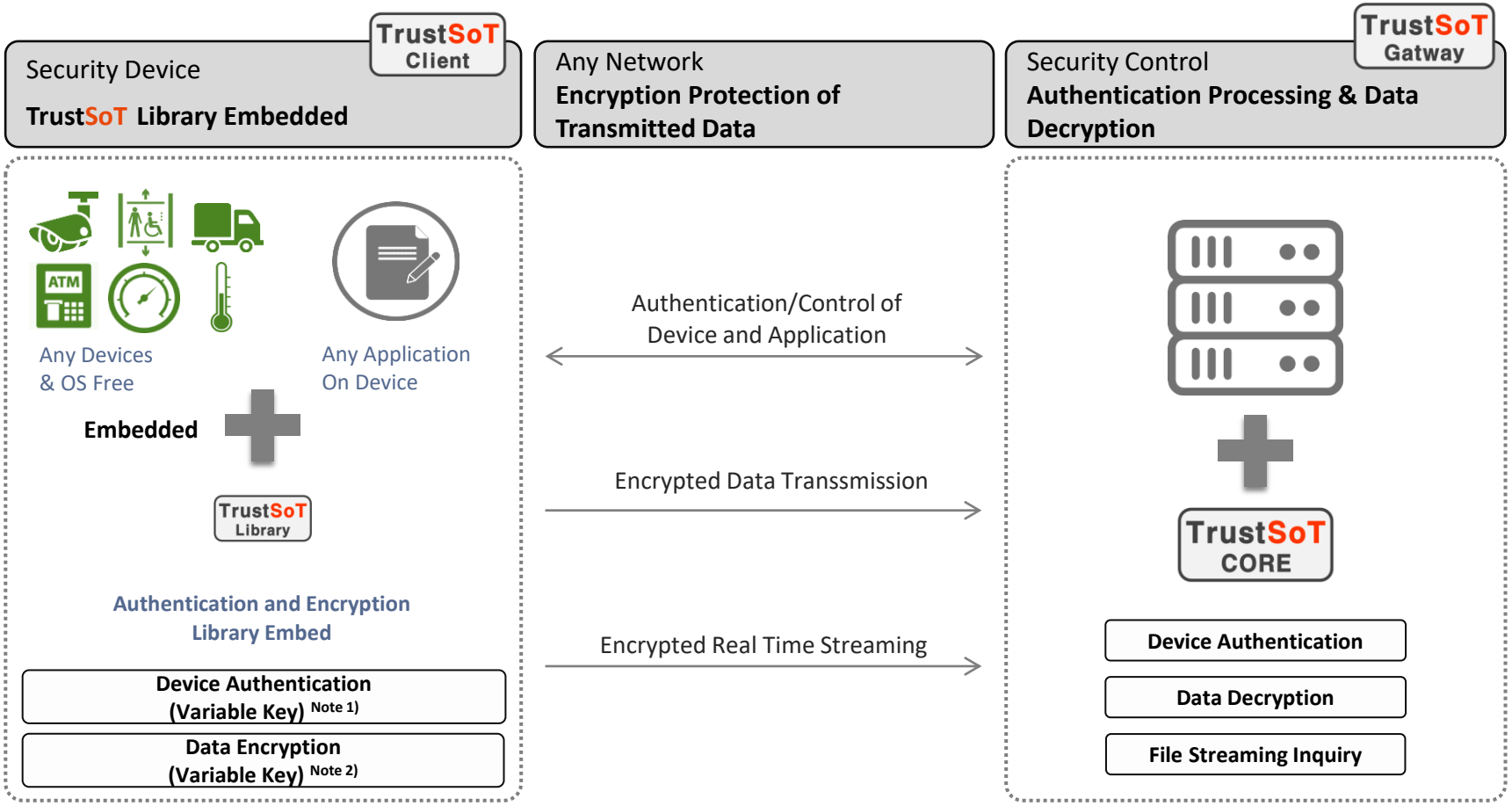
Note 1) OT/ICS : “Operational Technology/Industrial Control System”

■ **TrustSoT** is applicable to all areas and it **encrypts and protects key data and control commands** in various types of networks.



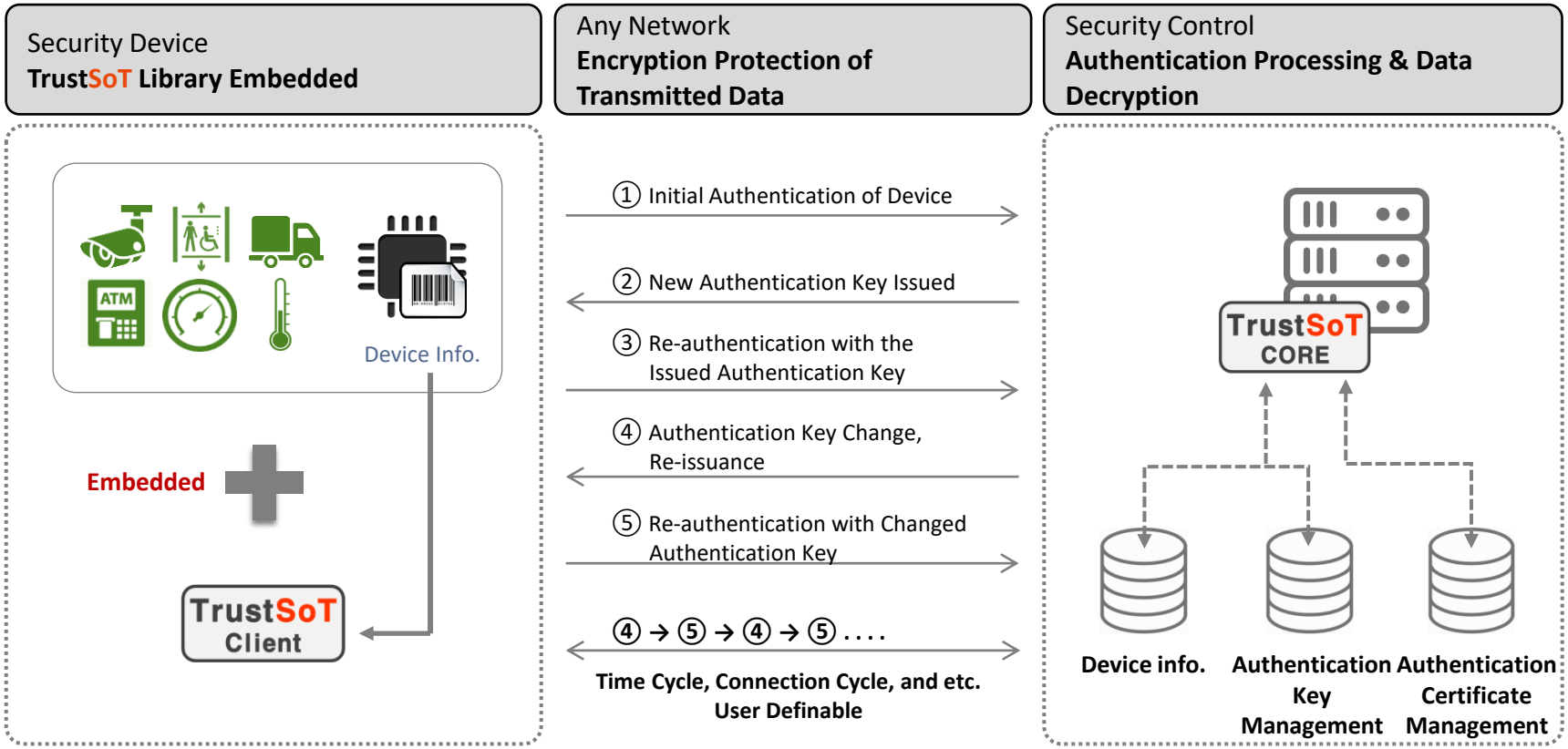
TrustSoT Core Technology

■ Certification/Encryption



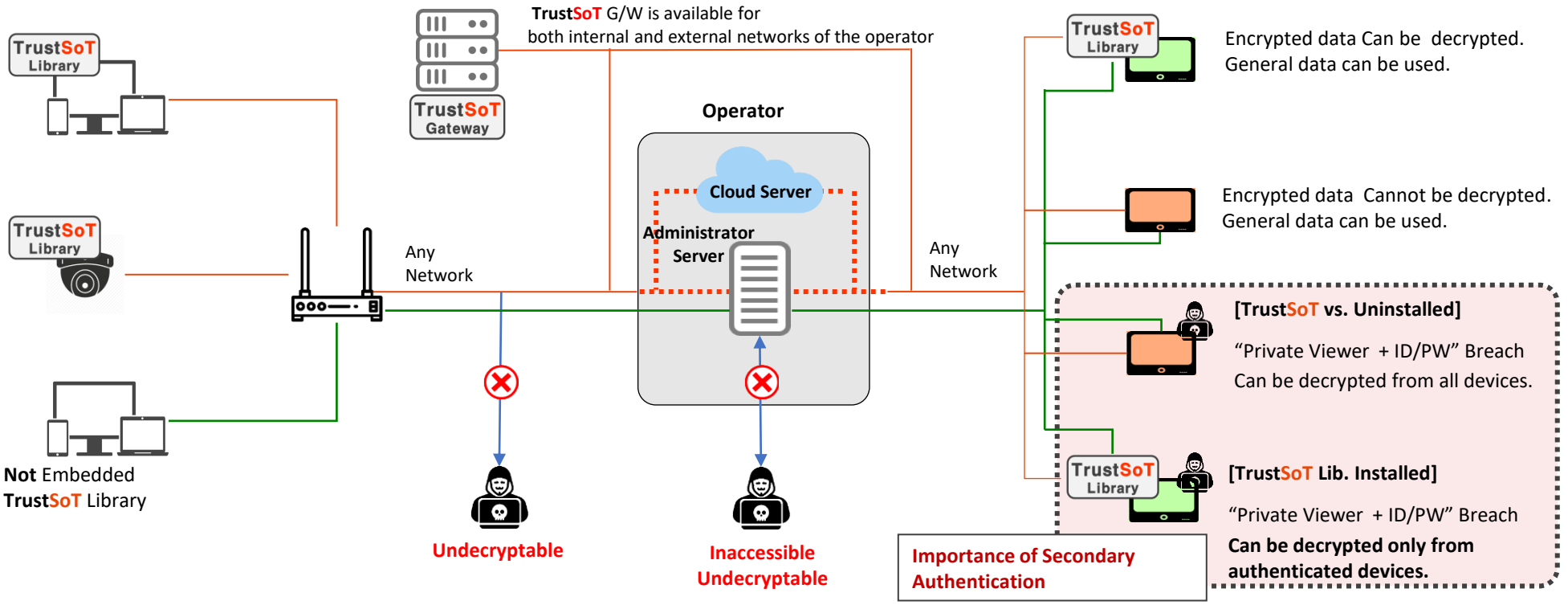
Note 1) Refer to "**Device Authentication**" on Page 7~8
Note 2) Refer to "**Data Encryption**" on Page 9~10

■ Devices to which **TrustSoT** is applied are authenticated based on unique (individual) information of the device, and after initial authentication, a new authentication key is renewed every time the system is connected to maximize authentication reliability.

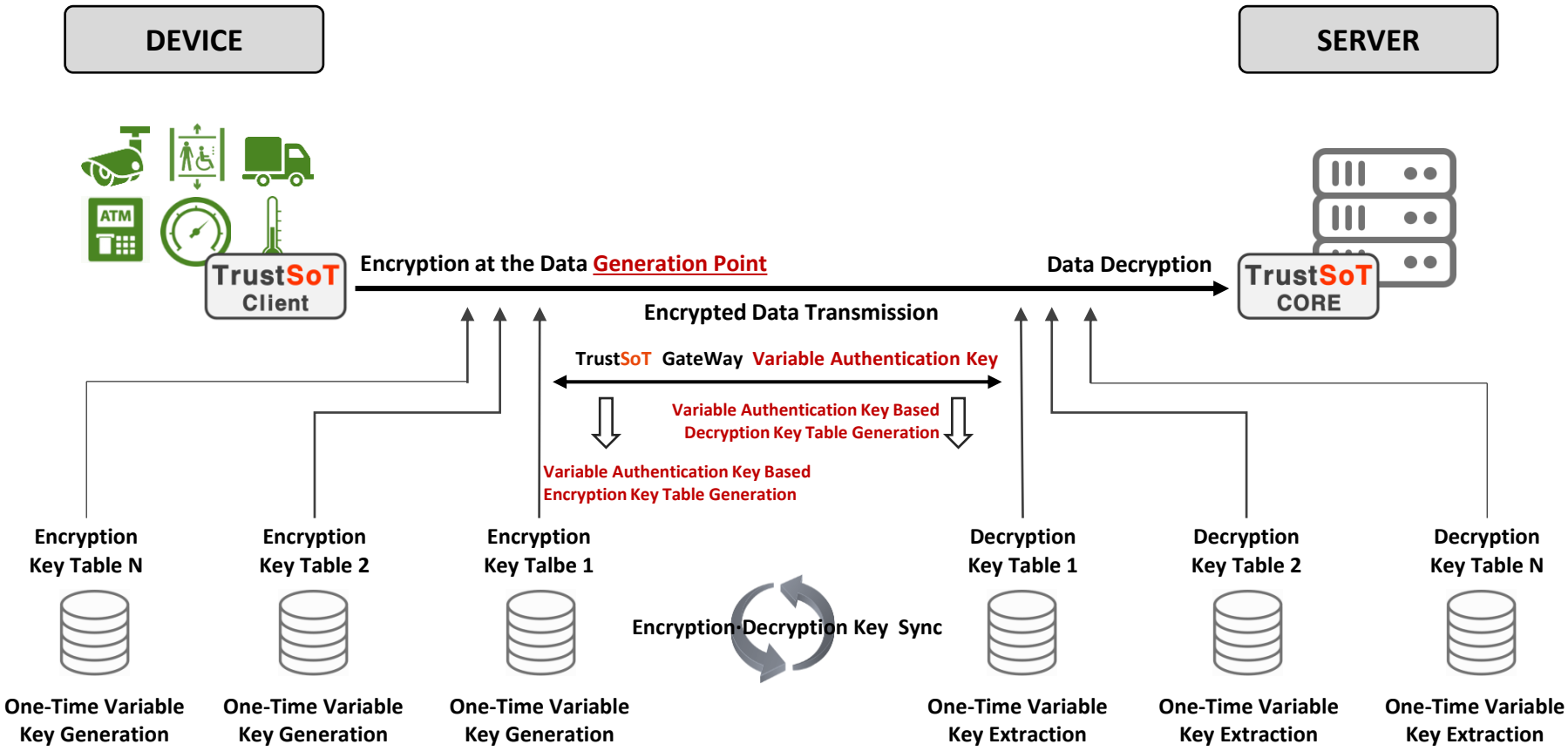


■ Importance of Variable Authentication Key Based Secondary Authentication of TrustSoT

- After the initial authentication, which is in physical form through ID and password, a continuous secondary authentication takes place in accordance with pre-determined policy such as time and connection, without requiring any additional actions by the user.
- Even when ID and PW are stolen, access is not possible except to the authenticated device, and even when ID, PW, and authenticated device are all stolen, video access and information theft are impossible as the device is controlled.



■ A device, on which **TrustSoT** is applied, performs data encryption based on a random one-time variable encryption key from the time of the data generation to completely protect all data that are being transmitted or stored (supports standard authentication encryption module and algorithm).

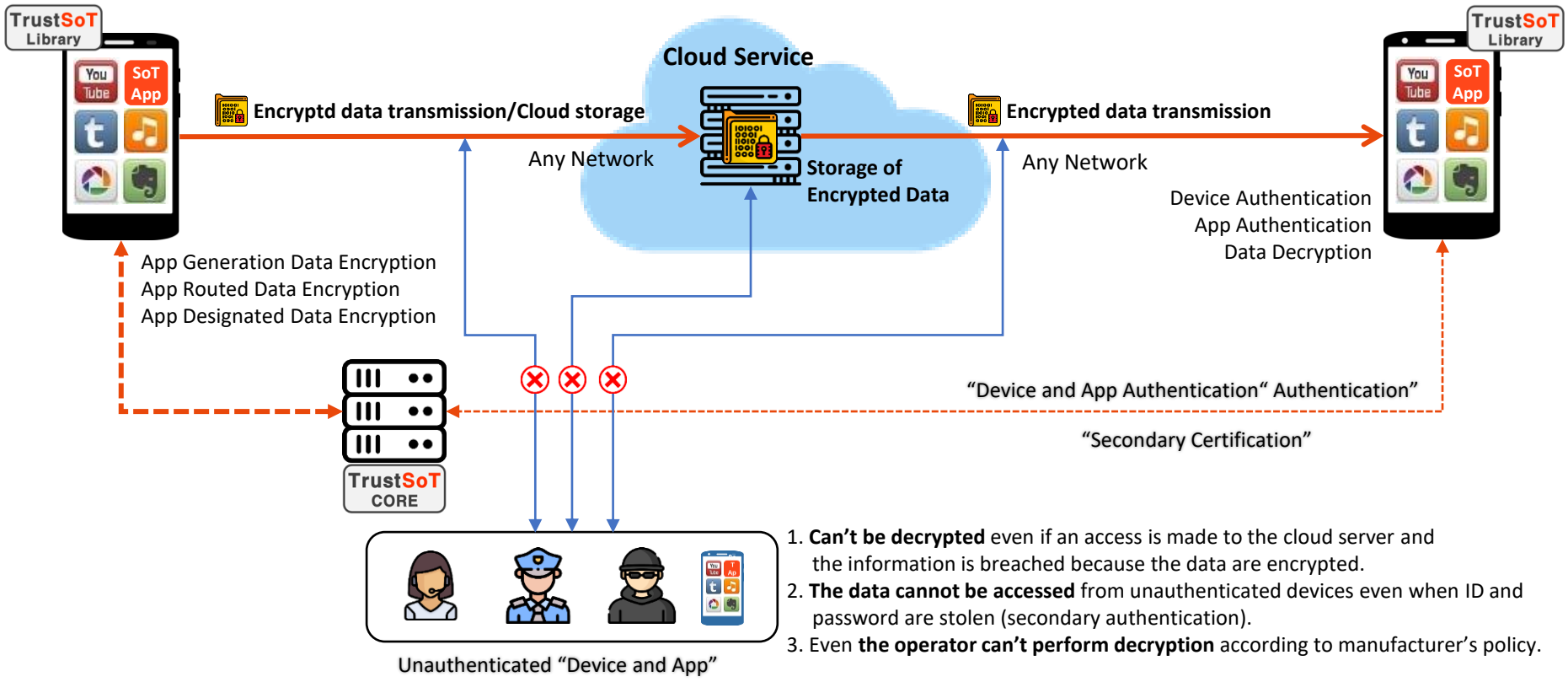


■ TrustSoT vs. Existing Data Encryption

TrustSoT	TPM Method	Chip Method
■ Can be protected through software based authentication and implementing encrypted library. ※ Embedding through updates on previously deployed devices.	□ Hardware production phase must be taken into consideration in the design for TPM authentication.	△ Hardware production phase must be taken into consideration in the design for chip authentication and data encryption.
■ Device authentication based on variable authentication keys.	□ Fixed key based authentication method.	△ Most use fixed key based authentication method. ※ The data can be decrypted when the fixed key is breached.
■ Encryption of generated data and decryption of received data. ※ Variable Encryption Key Sinc Technology	□ Generation data cannot be encrypted.	
■ No need for encryption of communication interval. ※ Can't be decrypted even when it is breached because the transmitted data are encrypted.		
■ Possible to centrally manage document security by using TrustSoT file viewer.		
■ Monitoring and control of authentication and received data status.		
■ Can be operated even in low specification, low power environment like IoT.	□ Difficult to implement in low specification, low power environment.	△ Difficult to implement in low specification, low power environment such as IoT because encryption of communication interval is necessary.

TrustSoT Case Study

■ All data of an application, on which **TrustSoT** is applied, are encrypted and uploaded to a cloud server immediately upon its generation.
Therefore, not only unauthenticated devices, but also the cloud service operator cannot view the customer data.
It is possible to provide a cloud service which resolves security risks of confidential information being stored in a third-party institution.



Encrypted data stored in the cloud cannot be decrypted not only by hackers but also by the cloud operator and during official verification processes.

■ **TrustSoT Cloud Security** vs. Typical Cloud Service

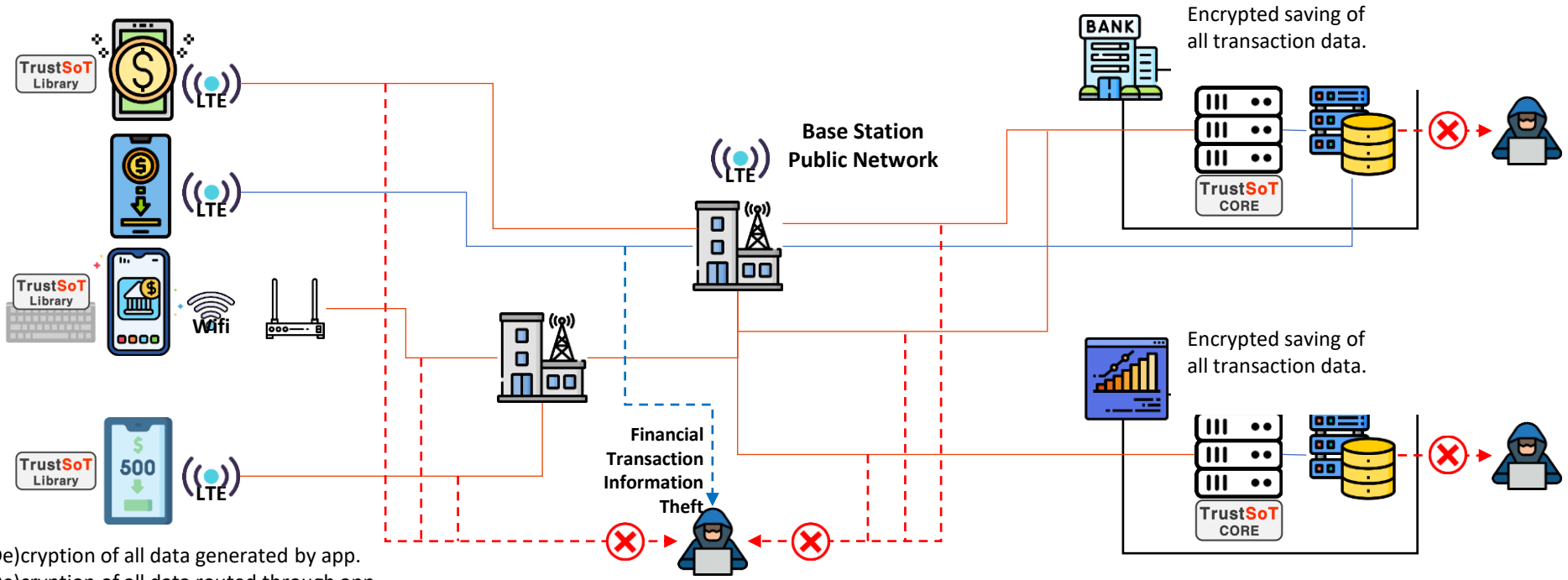
Classification	TrustSoT Cloud Security	Typical Cloud Service
App Authentication Method	**Two-step authentication method** of "terminal + app" through **variable key** of **TrustSoT.**	General authentication method based on "ID and MAC address."
Data Protection	Encryption at the **time of data generation** at **TrustSoT** authentication App.	No other data protection (encryption and etc.) support available.
Network Security	Upload to and download from **data in encrypted form**. (Data can't be decrypted even if they are hacked in the network.)	Data can be breached by network hacking during the upload.
Cloud Hacking Preventive Measures	Data can only be used in authenticated devices (applications) because encrypted data are uploaded to the cloud.	All data are vulnerable to breach when the cloud is hacked (ID and password breach and etc.).
Handling of Stolen Terminals	Complete protection of data uploaded to cloud by **disabling** applications of the **stolen terminal**.	There is no other countermeasuer than but to change the ID and password for accesing the cloud.

■ Solution1

All date generated in banking applications are encrypted at the time of generation by applying **TrustSoT** to provide complete protection of all transactions.

■ Solution2

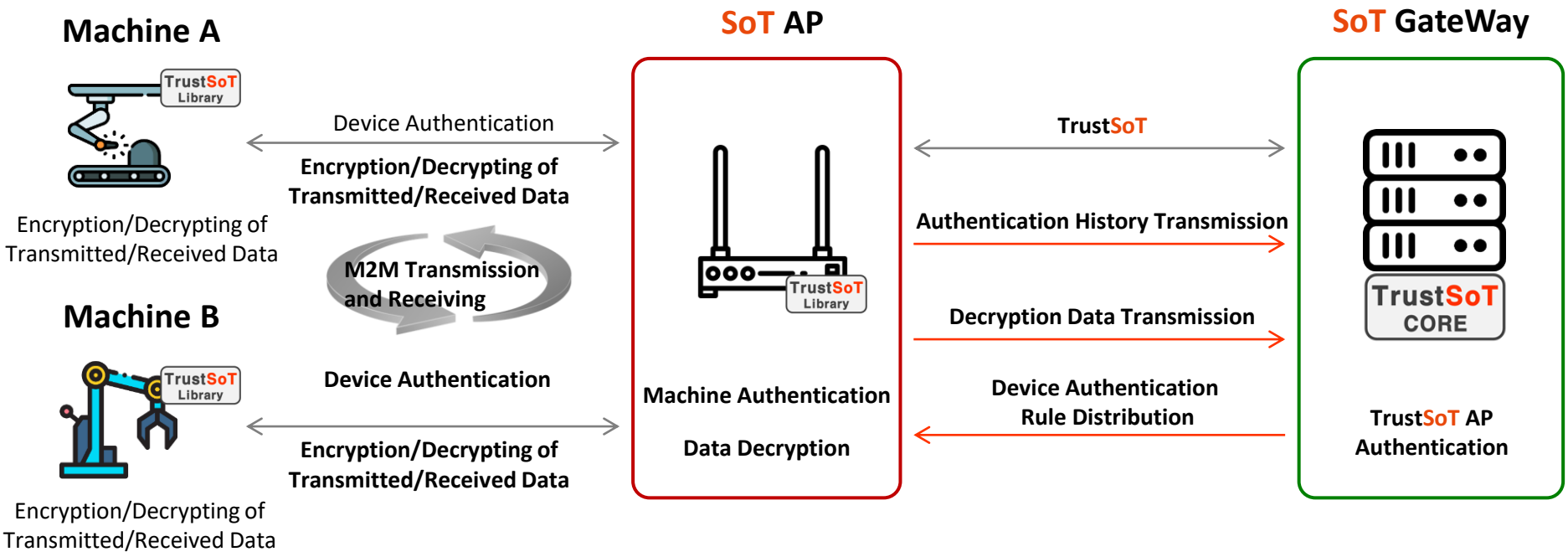
All transactions are completely protected through encryption of all data entered, stored and transmitted by applying **TrustSoT** "**Security Keyboard**" (page21) inside the banking applications.



- En(De)cryption of all data generated by app.
- En(De)cryption of all data routed through app.
- En(De)cryption of all data designated by app.

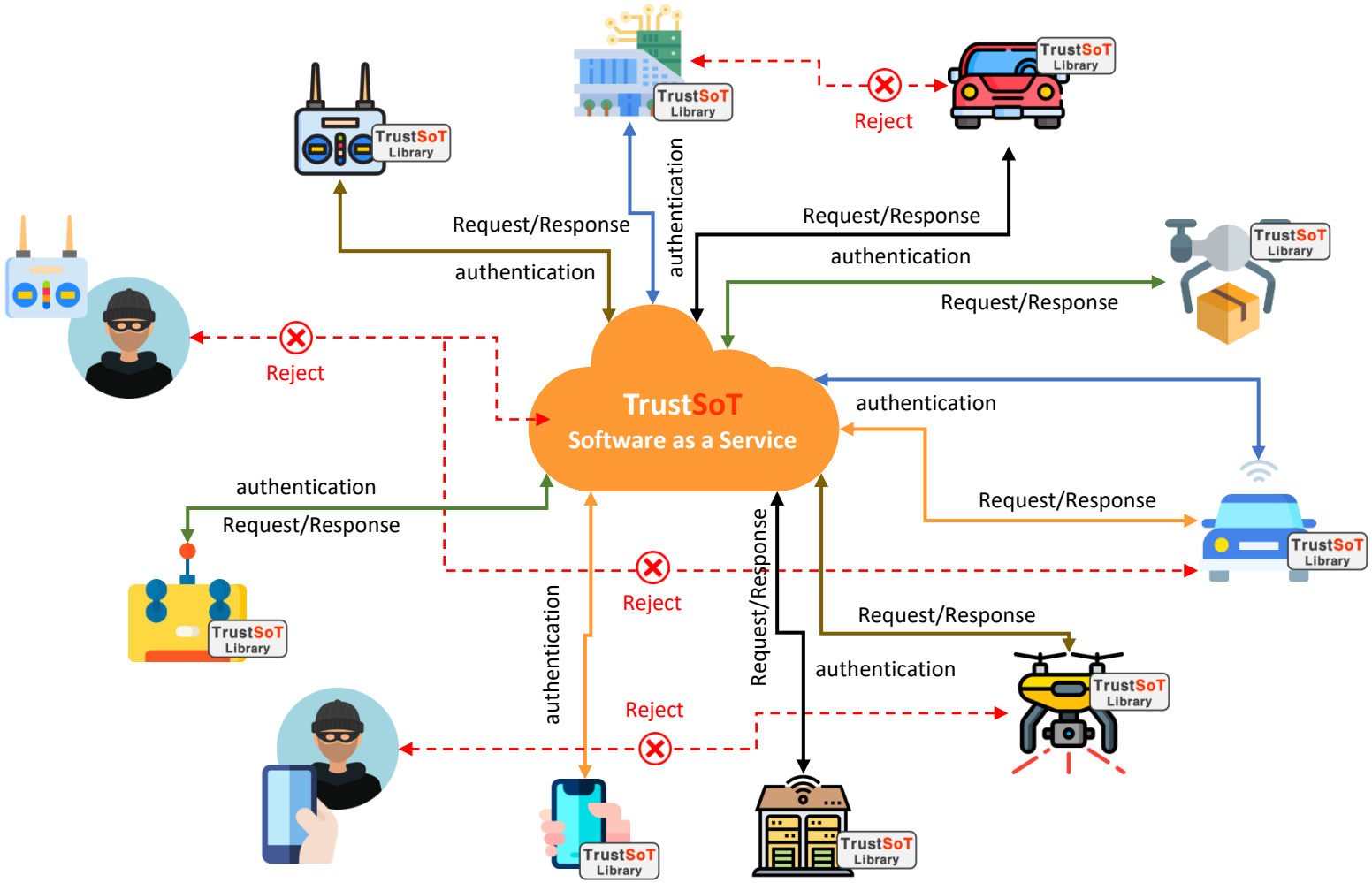
Not only all data being transacted over communication interval but also transaction data being stored are completely protected.
[All data such as ID and password, transaction amount, account number, counterparties of the transaction.]

■ **TrustSoT** supports device authentication and data protection that are optimized for various Iot convergence applications.



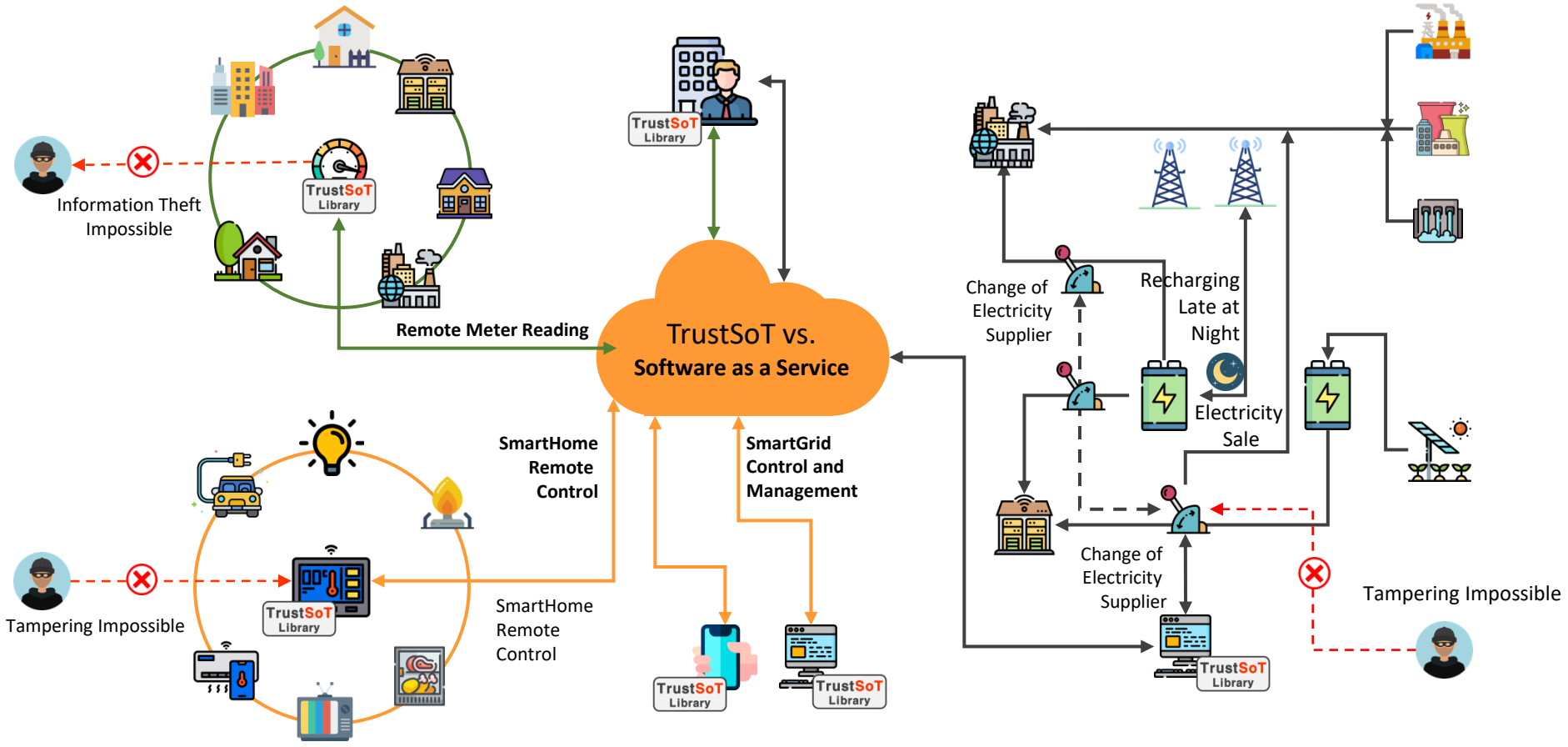
Device to device authentication as well as fundamental protection of communicated data can be provided through implementation of TrustSoT solutions (AP, GateWay, and etc.) in M2M construction of enterprise and public infrastructures.

■ **TrustSoT** supports protection of control signal of various mobile objects and authentication for the control devices.



Misoperation can be preemptively prevented through authentication between mobile objects and controlled devices, and complete protection of control signals.

■ **TrustSoT** supports authentication and protection of data communicated by various types of industrial goods, as well as light duty Iot devices.



Prevention of misoperation and information breach through authentication between devices, as well as complete protection of control signals and device generated data.

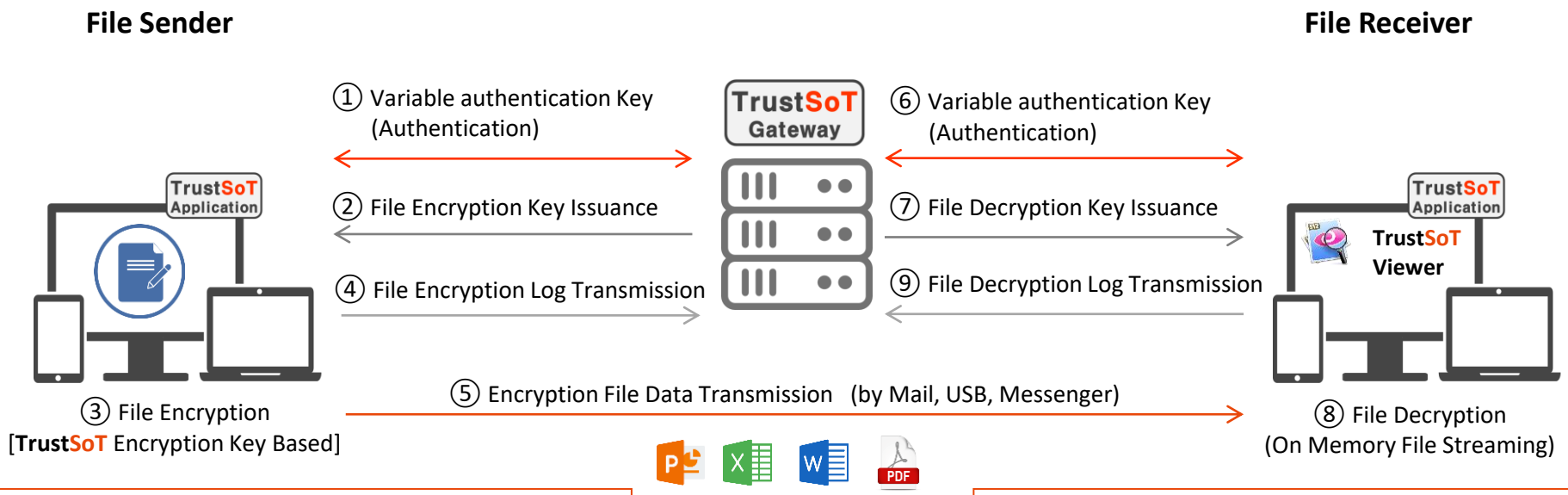
TrustSoT Product

■ By applying **TrustSoT**-based technology to solutions in various fields of IT as well as industrial controls in the OT/ICT field, we continue to work on developing applications and products that can be implemented directly on customer environments.

Software	**TrustSoT CORE** **Gateway** **Devices Authentication/Data Encryption** Supports ultra-light library based security authentication for all devices within the network, as well as complete encryption and decryption of communication data of reciprocally authenticated devices.	**TrustSoT Keyboard** (Keyboard entered data encryption) **Plug in + Gateway** By using a **TrustSoT** technology based virtual keyboard plug in, all texts entered are encrypted, stored, and transmitted without manipulating existing keyboard and therefore all data generated through the keyboard are fundamentally protected.
	TrustSoT File (File Encryption) **Application+Gateway** A file security solution that encrypts and transmits files through an application installed on the device and allows file receivers to stream files by using **TrustSoT** Private File Viewer only.	**TrustSoT IMG** (Video Data Encryption) **Application+Gateway** Provides prevention of illegal reproduction and distribution of video content, such as encryption and decryption of video data, capture prevention, and remote hacking prevention, through an application (agent) installed in cameras.
	TrustSoT Mail (Mail Encryption) **Plug in + Gateway** Fundamentally protects all texts and attached files transmitted through all web mail services by using a **TrustSoT** technology based web browser plug in. Supports sent mail security control even after an email is sent	**TrustSoT OT/ICS** (SCADA/PLC Control Data Encryption) **Application+Gateway** Detects malware, issues relevant warnings, and blocks internal spread of the malware through device authentication, encryption of control data, illegal access monitoring, prevention of information breach, and agent based processes monitoring by using an agent installed on SCADA control devices.
Hardware	**TrustSoT Security Camera** (Security CCTV Camera) with **TrustSoT IMG**	**TrustSoT LTE Router** (Security LTE Router) with **TrustSoT CORE** (Certification/Encryption)

Software

■ A device, with the 「TrustSoT File」application installed, encrypts and transmits files, and a user, with the 「TrustSoT File」application installed, who receives the transmitted files, obtains authentication through 「TrustSoT Gateway」. Additionally, the files can only be decrypted and accessed by using a private 「TrustSoT File Viewer」, without abilities to be saved to devices. Therefore, all transmitted document files are completely secured and can be centrally managed over not only within the internal network but also over all areas.

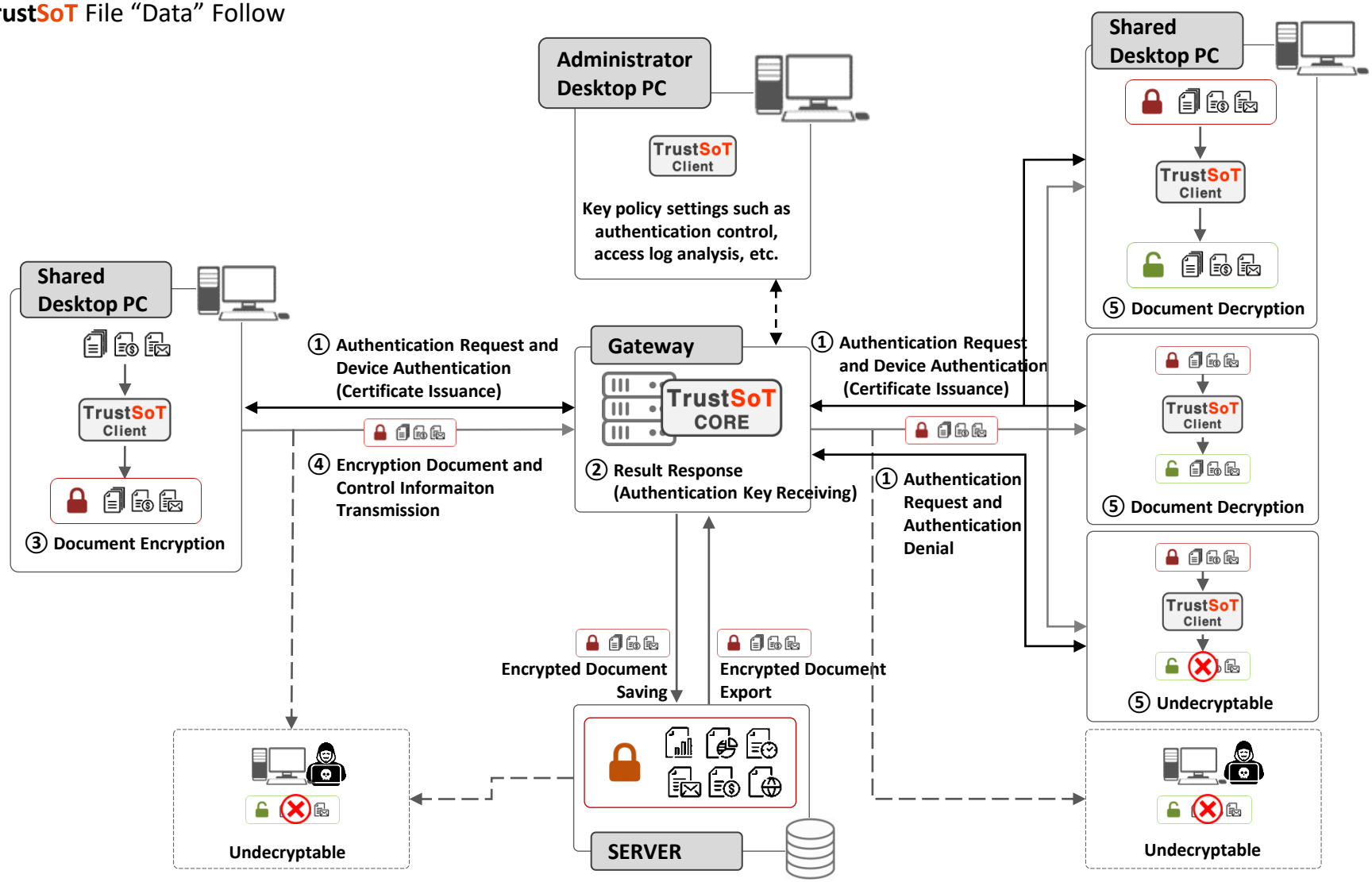


- Specific receiver(s) can be designated during file encryption.
- Only the specified receiver(s) can view the file.

- Decrypted files can only be accessed by using TrustSoT File Viewer.
- Decrypted files cannot be saved onto devices.

Encrypted mails exchanged between 「TrustSoT File」 users cannot be decrypted in TrustSoT Gateway either.

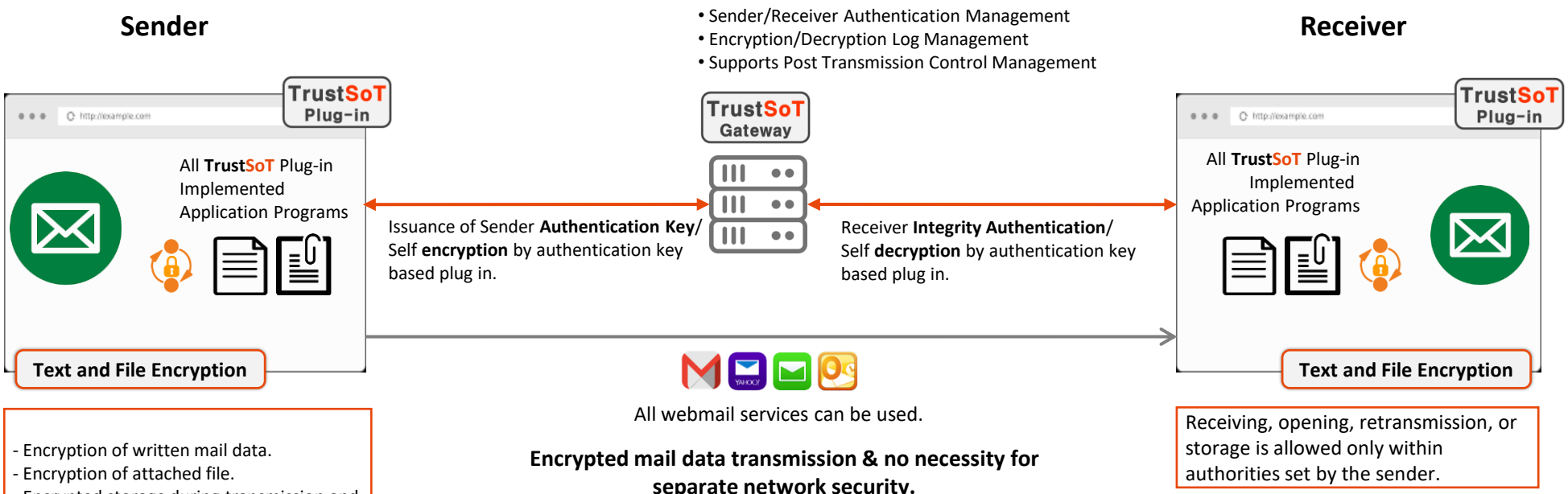
■ TrustSoT File “Data” Follow



■ TrustSoT File vs. General Document Centralization Technology

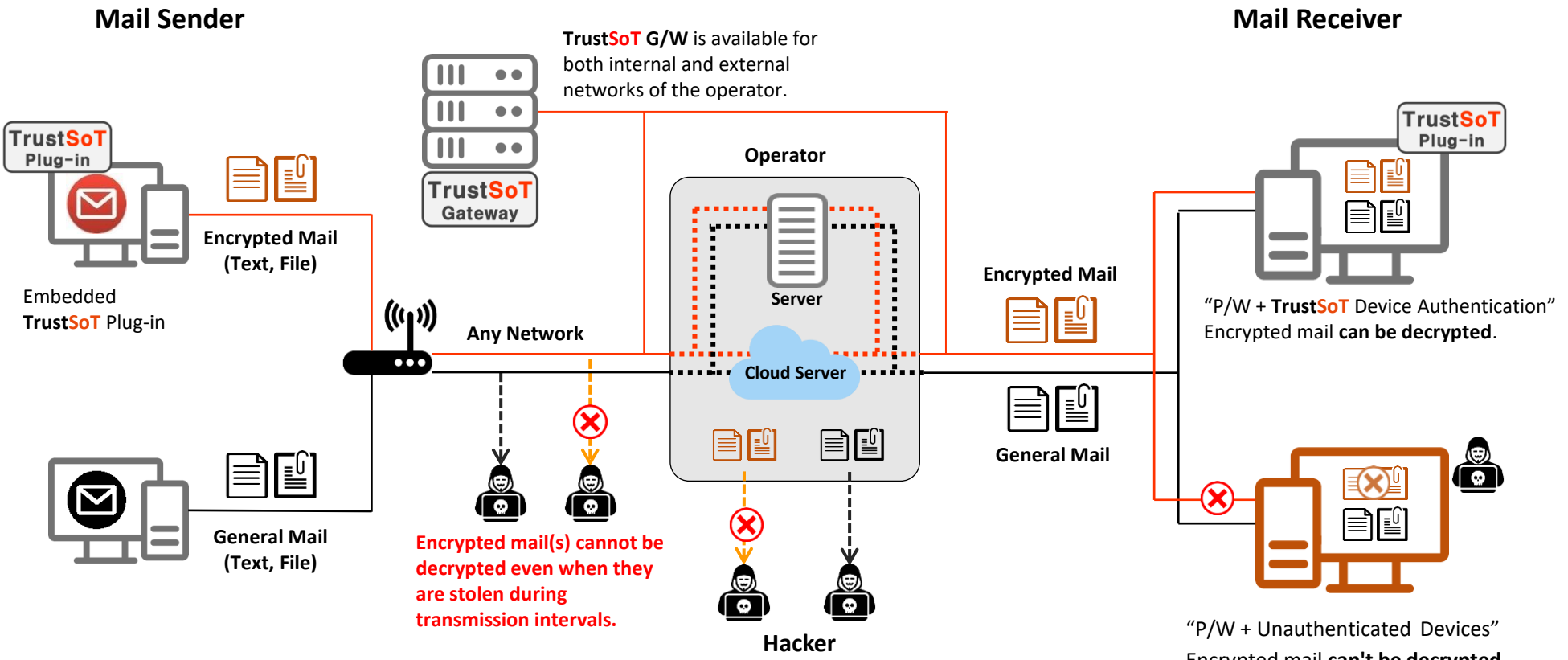
Classification	TrustSoT Gateway	General Document Centralization Method
Transmission Interval Limitation	■ Encryption over data transmission interval is not necessary.	☐ Need to establish internal closed network.
File Encryption	■ When sending files to the outside, the documents are encrypted before transmission ■ File breach can be prevented even when there is hacking attack because encrypted data are transmitted by using variable encryption keys.	☐ File encryption is optional and general encryption method is used. ☐ Permission or authority is required when experting external files.
File Protection	■ A user who encrypts the file can specify receiver(s) and only authenticated receiver(s) can view the file. ■ A receiver can only view decrypted files and can't save the file to private device(s).	☐ Computing environment of external user(s) who receive the file can't be controlled (only export records exist.).

■ Texts and attached files of webmail, SNS, and mobile applications are encrypted through 「**TrustSoT** Mail」's plug in for web browser. Additionally, various types of security control and post management are supported even after the mail transmission. Creation of secured mails and post-transmission management of such mails are possible through **TrustSoT** Library or Plug-in without a separate network security solution.



Encrypted mails exchanged between 「TrustSoT File」 users cannot be decrypted even in TrustSoT Gateway either.

■ TrustSoT Mail "Text & File" Follow



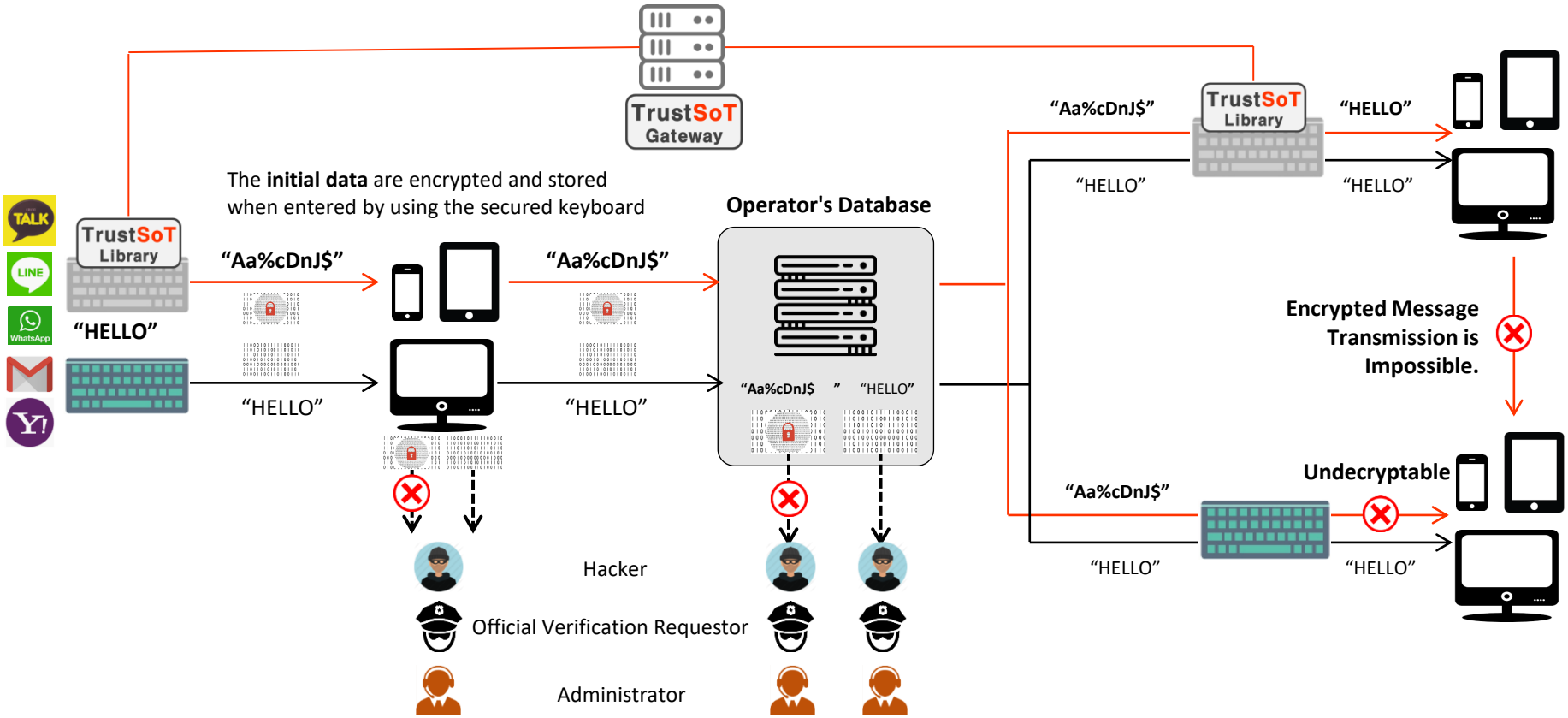
※ Encrypted mail cannot be viewed from unauthenticated device(s) even if the password is stolen.

Encrypted mail(s) that are stored in the operator's server or cloud cannot be decrypted even if they are stolen.
(General mail(s) in storage can be viewed when they are stolen.)

■ **TrustSoT Mail** vs General Secured Mail Solution

Classification	**TrustSoT Mail**	Gmail Security Service (USA, Company 'C')	Information Leak Prevention Solution (KOR, Company 'U')
User Authentication	■ Complex authentication through browser plug in. ■ No need for installation of separate application(s). ■ Complete authentication security through variable authentication.	☐ User authentication through mail receiver's password. ☐ All mails can be viewed if the sender's password is known.	△ Authentication through Agent (Software) Installation.
Date Security	■ All encryption algorithms can be implemented. ■ **TrustSoT** data security technology implementation. ■ Encrypted on mail text browser. ■ Encrypted file is attached through plug in. ■ No limit on attached file size.	☐ Security is based on password(s) set by the mail sender. ☐ Mail text AES25 encoding is supported. ☐ when attaching a file to an email, AES25 encoding is done first and then uploaded/ linked to cloud of the company C. ☐ The maximum size of attached file is limited to 100M.	△ Data is transmitted after encryption by uploading the texts and files to the server. △ Such data can be decrypted in all terminals that have a viewer (agent) installed. △ The server limits size of attached file(s).
Compatibility	■ Compatible with all operating systems and browsers. ■ All mobile application libraries are supported.	☐ Compatible with certain web browsers only Exclusively for Gmail service. ☐ Need to download exclusive mobile application.	△ Only supports operating system provided by the agent. △ An exclusive viewer must be installed for data access.
Solution Deployment ROI	■ **TrustSoT** Gateway and plug in costs are the only expenses. ■ Can be implemented on all mail services.	☐ Service charge of $5.00/month for each user. ☐ Only can be used with Gmail service.	△ Expenses are incurred for the solution deployment (server, agent). △ Expenses are incurred for network and terminal securities when necessary.

■ As an initial input device for all devices, on which 「TrustSoT KeyBoard」 Library is implemented, encryption is applied from the point of data generation to enable complete data protection without interlocking with other security solutions over communication intervals.
Additionally, the encryption is maintained even after the data is shared and decryption of each device is enabled/disabled by “central command(s)”. (Competitive Edge)



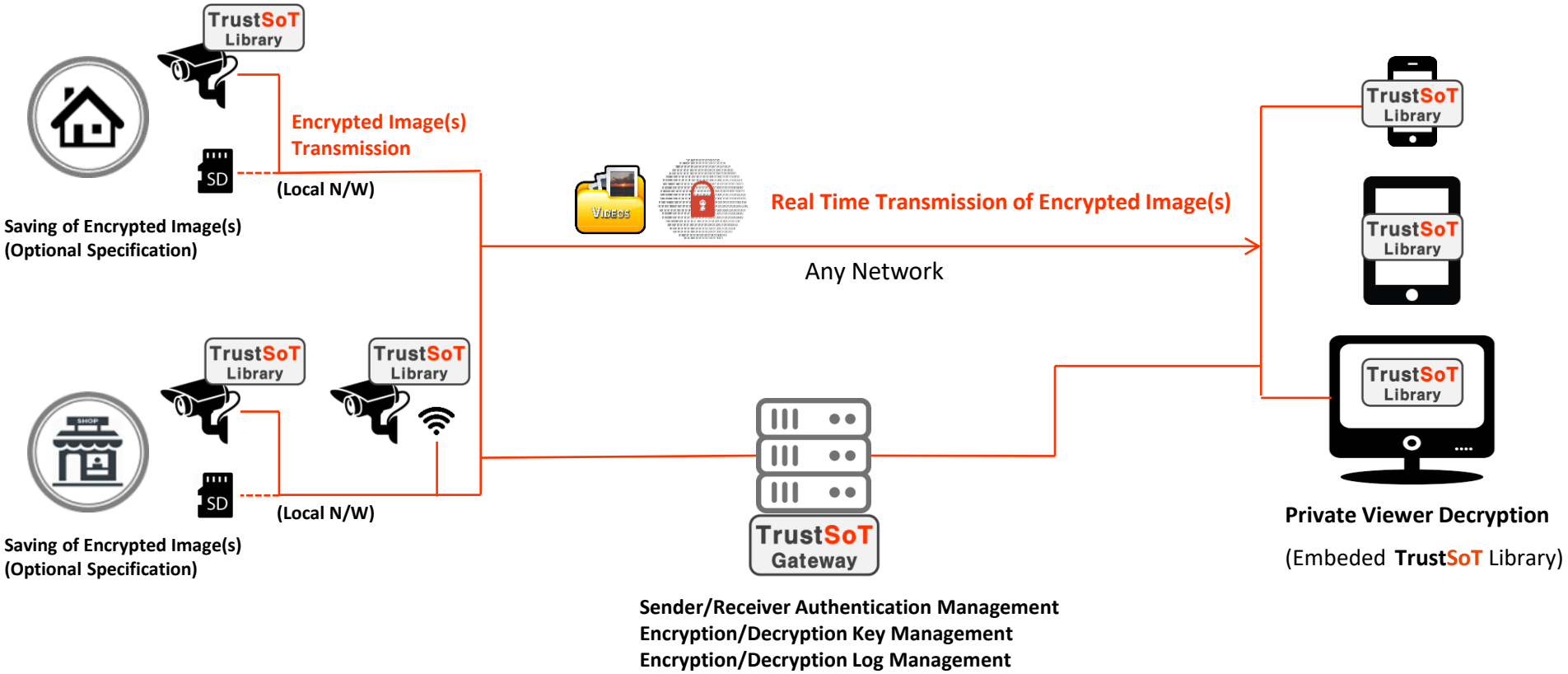
Encrypted data stored in the cloud or in the oprator’s server cannot be decrypted not only by hackers but also by the cloud operator and during official verification processes.

■ Key Functionaities

Classification	Functionalities
Commercial Encrypted Keyboard	☐ All documents and applications, including messenger(s) and mail(s), as well as generated data are encrypted. ☐ Only counterparts (person(s), device(s)) that are designated with decryption authority can decrypt when sharing the encrypted data. ☐ Items such as number and time period of decryption can be limited. ☐ Decryption authority can be revoked. (Even if the decryption authority has been previously given, user(s) whose decryption authority is revoked afterwards cannot decrypt phrase(s) written before and after the revocation of authority.)
Corporate Encrypted Keyboard	☐ All functionalities of general encryption keyboard are implemented. ☐ Collection of keyboard input/encryption/authentication logs. ☐ Partial monitoring of keyboard installed device(s) (such as screen captures and malware operation).
Additional Special Functionalities	☐ Conversion of character strings into image(s) or RGB (saving and sharing). ☐ The members of the messenger window displayed on the screen are automatically recognized (members of private chat rooms, group chat rooms, etc.) by using open API provided by the operator. **-Secure saving and recovery of data through cloud service (backup) of encrypted data.**

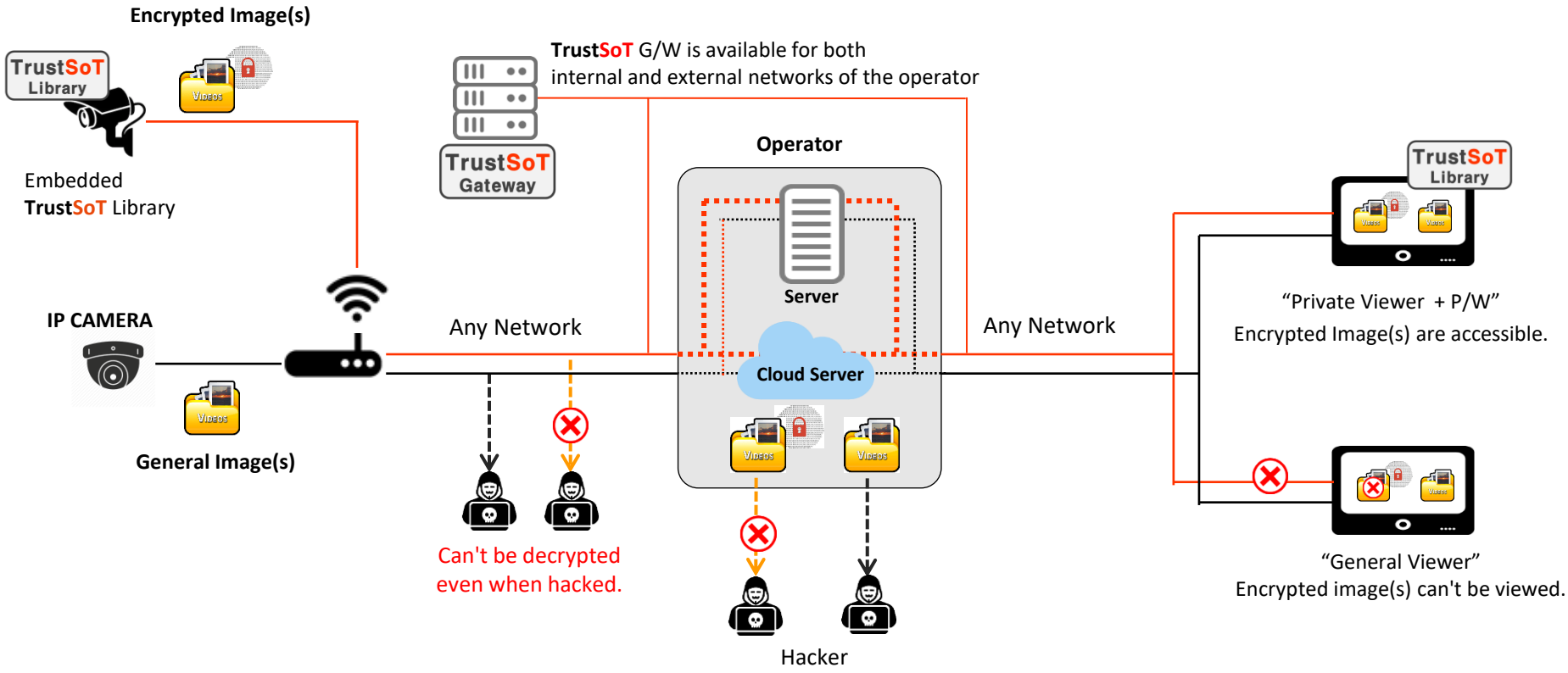
TrustSoT IMG (Video Data Encryption)

■ Illegal theft, reproduction, and distribution of images are fundamentally prevented even if image data is breached because the data of visual data generating device(s) such as CCTV cameras, on which 「TrustSoT IMG」 Library is implemented, are encrypted from the time of data generation.



Encrypted image(s) exchanged between 「TrustSoT IMGl」 users cannot be decrypted in even in TrustSoT Gateway either.

■ **TrustSoT** IMG “Video & Image” Follow



Encrypted image(s) that are stored in the operator’s server or cloud cannot be decrypted even if they are stolen.
(General mail(s) in storage can be viewed when they are stolen.)

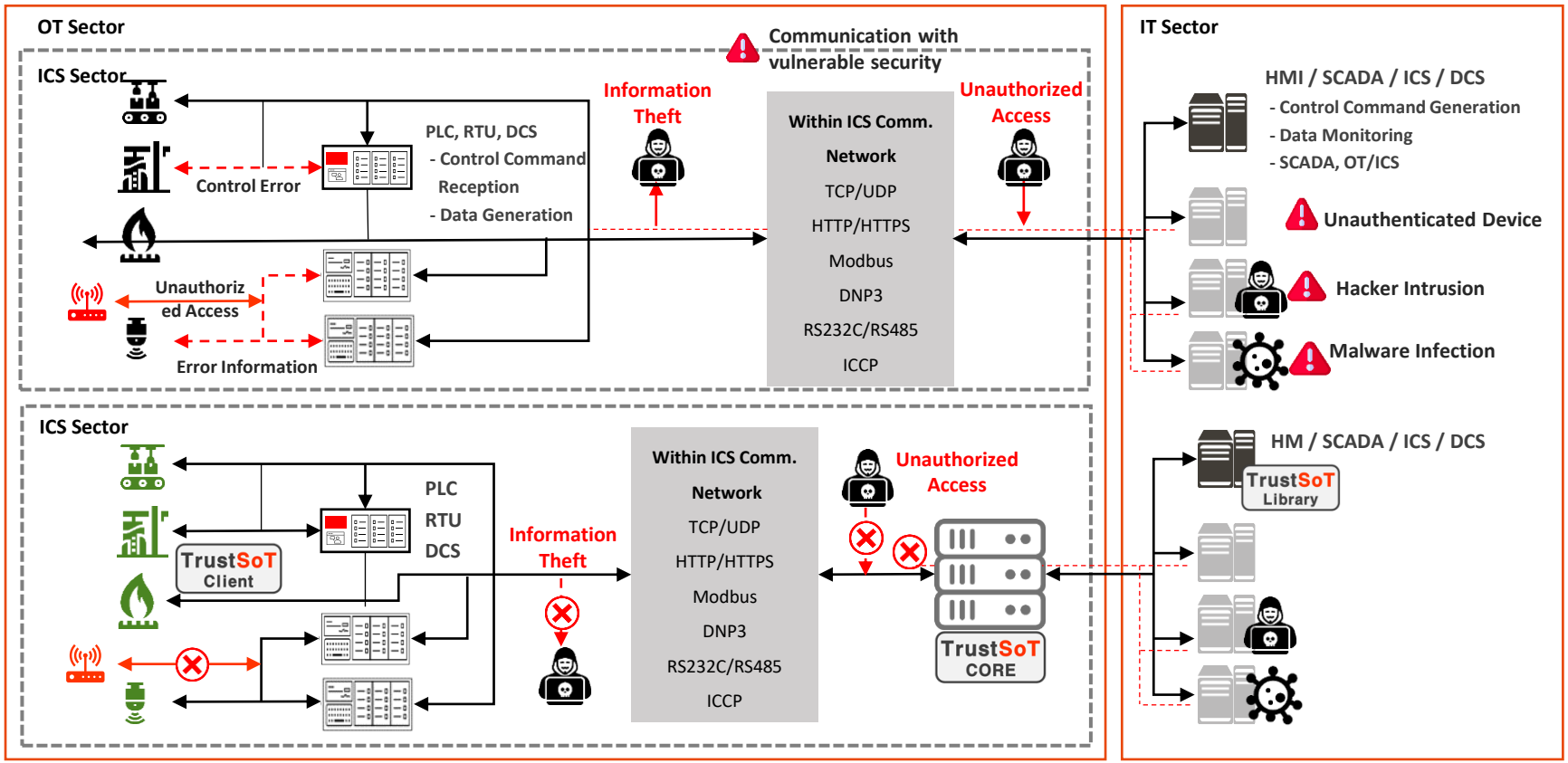
■ **TrustSoT IMG** vs General CCTV Encryption Technologies Comparison

Classification	**TrustSoT vs.**	General CCTV Encryption
Transmission Intervals Limitation	■ Header encryption immediately upon image(s) generation. ■ Encryption over data transmission interval is not necessary.	☐ Encryption of visual data at the time of generation is impossible. ☐ Header encryption within data transmission interval.
Data Preservation	■ Header encryption and self storage immediately upon image(s) generation. ■ Data are preserved within set capacity limit even when the communication is lost.	☐ Encryption method for visual data transmission. ☐ Untransmitted data are lost when the communication is lost.
Data Protection	■ Supports variable authentication key based termianl security authentication. ■ Data breach can be prevented even when there is hacking attack because data that are encrypted in real time are transmitted by using variable encryption keys.	☐ Basic terminal authentication by using IP or MAC address methods. ☐ No data protection is provided when encryption key is compromised because fixed key based header encryption is used over the transmission interval.
Point of Data Encryption	■ The only light load solution that encrypts CCTV image(s) data from the point of date generation (AES256 or above)	☐ Encryption at the point of transmission instead of the point of image(s) generation.

TrustSoT OT/ICS (Industrial Control Signals/Data Encryption)

- 「TrustSoT OT/ICS 」provides protections for OT/ICS (industrial controls) areas, that require various types of protection systems because there is no special protective measures for device controls and monitoring due to characteristics of the network constructions (internal networks/close networks), through such methods as device(s) authentication, data encryption, and event monitoring to resolve various security issues that can occur.

- TrustSoT OT/ICS "Control Signal/Data" Follow



Key Features of Gateway and Module

TrustSoT Slave Module

- Decryption Key Request
- Control Command Decryption and Confirmation
- Certificate Issue/Revocation Request
- Data Generation, Authentication Information Transmission
- Transmission Date Generation/Receiving Date Analysis

TrustSoT Gateway

- Data Proxy
- Authentication and Access Control between
- Master and Slave
- (Authentication, Encryption) Variable Key
- Management
- Transmission Data Analysis Monitoring Log Collection

TrustSoT Master Module

- Encryption Key Request
- Control Command Encryption
- Certificate Issue/Revocation Request
- Data Authentication Information Confirmation
- Transmission Date Generation/Receiving Date Analysis

Additional Functionality in OT/ICS Sector: Prevention of Internal Malware Spreading

Classification	Paloalto	Symantec ATP (Advanced Threat Protection)	TrustSoT
Prevention of internal spread after malware infection	× Open/closed malware blocking	× Open malware blocking	○ Open/closed malware blocking Execution Warning and Prevention of Internal Spread (**Blocking**)
Generation File Protection	×	×	○
ICS (Industrial Controls System) Protocol Support	×	×	○
Device User Monitoring	×	×	○
File Breach Protection	○	×	○
Key Functions	Intrusion Blocking	Intrusion Blocking	Spread Blocking Data Encryption

Hardware

Security Camera (TrustSoT IMG Implemented)

Items		Specifications	Items		Specifications
Wireless		IEEE802.11b/g/n	Motion Detection		Automatically turns on when motion is detected. (Detection Distance: 5m)
Video File Output		HD960P	Lens		3.6mm/90° viewing angle lens (Option : 2.8mm/120°)
Compression Type		H264O	Audio Support		Remote Two-way Audio Transmission and Receiving Function
OS	Smart Phone	Android, iOS	Power Consumption		< 5W
	Desktop Computer	Windows	Bulb Quantity	LED	25 pcs
Storage Memory		2 ~ 64GB micro SD		Infrared	4 pcs (Night Vision 8~10m)
Back Up		Mobile, PC	Socket		272622
Lens Resolution		1.3 mega pixel	Weight		280 g
Alarm		Motion detection, sound, message, lighting	Operating Environment		-20°C ~ 50°C
Storage Time		Upto 24 days/64G micro SD	Power Supply		Weidmuller 100~250V AC

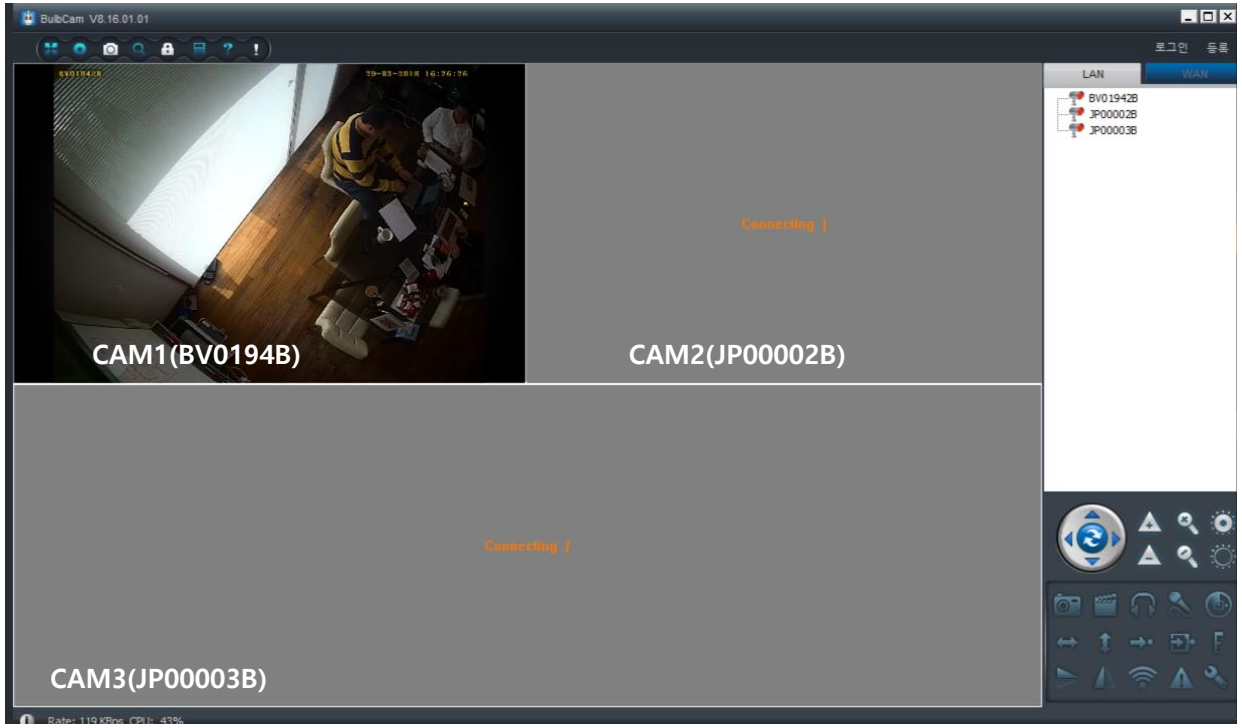
※ The above specifications may be modified during product deployment review phase.

IB-175W [White Light]

IB-175Y [Warm Light]

- General Viewer: Image(s) of “CAM1(BV0194B)”, a camera with no **TrustSoT** Library implementation can be viewed.
  Impossible to access encrypted image(s) of **TrustSoT** Security Camera “CAM2(JP00002B)” and “CAM3(JP00003B)”.

- Exclusive Viewer : Encrypted image(s) of **TrustSoT** Security Camera can be viewed (decryption).



General Viewer (Desktop Computer)

TrustSoT Private Viewer (Android)

■ **TrustSoT** IMG Image(s) Encryption Performance Inspection Results

SoT 処理性能検証結果 (SOT처리성능확인결과)

측정①~암호화(SoT G/W 경유)·LOCAL 연결
測定①～暗号化(SoT G/W経由)・ローカル接続

PC時計	動画	差分	差分（平均）
15:50:53.277	15:50:52.119	00:00:01.158	
15:51:54.529	15:51:53.355	00:00:01.174	
15:52:55.836	15:52:54.685	00:00:01.151	00:00:01.172
15:53:58.118	15:53:56.944	00:00:01.174	
15:54:59.808	15:54:58.604	00:00:01.204	

측정②~비암호화(카메라 직접연결)·LOCAL 연결
測定②～暗号化なし(カメラ直接)・ローカル接続

PC時計	動画	差分	差分（平均）
15:58:01.560	15:58:00.387	00:00:01.173	
15:59:01.930	15:59:00.764	00:00:01.166	
16:00:03.291	16:00:02.132	00:00:01.159	00:00:01.166
16:01:09.404	16:01:08.238	00:00:01.166	
16:02:05.961	16:02:04.795	00:00:01.166	

결과 • 監視カメラ映像の暗号化／復号処理による遅延： 6ミリ秒

암/복호화처리 지연 : 6msec

[참고]측정③~암호화(SoT G/W 경유)·INTERNET 연결
【参考】測定③～暗号化(SoT G/W経由)・インターネット経由

PC時計	動画	差分	差分（平均）
15:45:21.934	15:45:20.733	00:00:01.201	
15:46:23.730	15:46:22.523	00:00:01.207	
15:47:22.212	15:47:20.993	00:00:01.219	00:00:01.222
15:48:22.852	15:48:21.586	00:00:01.266	
15:49:24.069	15:49:22.852	00:00:01.217	

[참고]측정④~비암호화(카메리 직접 연결)·INTERNET 연결
【参考】測定④～暗号化なし(カメラ直接)・インターネット経由

PC時計	動画	差分	差分（平均）
16:03:52.539	16:03:51.258	00:00:01.281	
16:04:55.657	16:04:53.992	00:00:01.665	
16:06:02.528	16:06:00.090	00:00:02.438	00:00:01.640
16:07:00.273	16:06:58.852	00:00:01.421	
16:08:04.168	16:08:02.773	00:00:01.395	

<結果考察及び備考>
- SoT経由（暗号化／復号処理）とカメラ直接間に堅調な遅延影響は認識できず。
- 取得結果にブレが生じている点は、ネットワークの品質もしくはカメラの映像配信処理にも依存している可能性がある。
- インターネット経由での測定は時間帯によるネットワーク遅延の要素が加味されるため、実使用時の参考までとする。

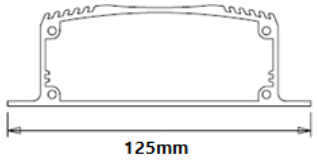
〈결과 고찰 및 비고〉
- SoT 경유(암호화/복호화 처리)와 카메라 직접 연결과의 차이에서 확연한 지연 영향은 확인 할 수 없음
- 검토 결과에 차이가 발생하는 점은, 네트워크의 품질 또는 카메라의 영상 전송 처리에 의한 차이일 가능성이 있음
- 인터넷을 통한 측정시간은 네트워크 지연 요소가 추가되어야 하기 때문에, 실제 사용시에는 참고하여야 함

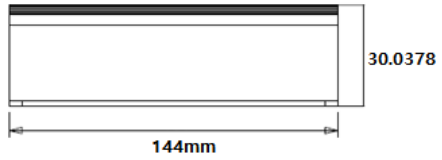
カル接続
測定②～暗号化なし(カメラ直接)・ローカル接続
差分 差分（平均） PC時計 動画 差分 差分（平均）
0:01.158 15:58:01.560 15:58:00.387 00:00:01.173
0:01.174 15:59:01.930 15:59:00.764 00:00:01.166
0:01.151 00:00:01.172 16:00:03.291 16:00:02.132 00:00:01.159 00:00:01.166
0:01.174 16:01:09.404 16:01:08.238 00:00:01.166
0:01.204 16:02:05.961 16:02:04.795 00:00:01.166
監視カメラ映像の暗号化／復号処理による遅延： 6ミリ秒
)・インターネット経由
【参考】測定④～暗号化なし(カメラ直接)・インターネット経由
差分 差分（平均） PC時計 動画 差分 差分（平均）
0:01.201 16:03:52.539 16:03:51.258 00:00:01.281
0:01.207 16:04:55.657 16:04:53.992 00:00:01.665
0:01.219 00:00:01.222 16:06:02.528 16:06:00.090 00:00:02.438 00:00:01.640
0:01.266 16:07:00.273 16:06:58.852 00:00:01.421
0:01.217 16:08:04.168 16:08:02.773 00:00:01.395
<結果考察及び備考>
• SoT経由（暗号化／復号処理）とカメラ直接間に堅調な遅延影響は認識できず。
• 取得結果にブレが生じている点は、ネットワークの品質もしくはカメラの映像配信処理にも依存している可能性がある。
• インターネット経由での測定は時間帯によるネットワーク遅延の要素が加味されるため、実使用時の参考までとする。

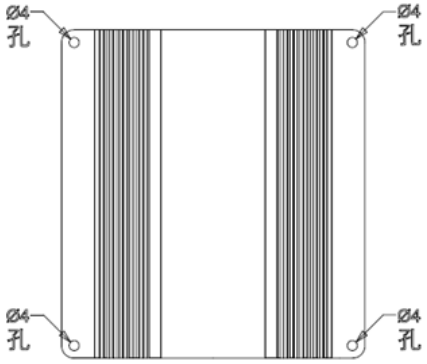
Security LTE Router (TrustSoT CORE Implemented)

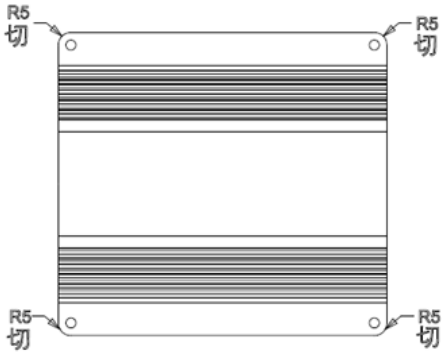
Hardware	Indoor Type with PSE	Remarks
CPU	ARM Cortext-A8 AM3352 (600MHz)	
Memory	512 Mbyte	
Flash Memory	eMMC 4 Gbyte	
LAN	1 x 10/100 Base-T With 35W PSE	
WAN	1 x 10/100 Base-T	
Wi-Fi	IEEE802.11 a/b/g/n 2.4G/5G Dual Band	
3G/LTE Dual Mode	M.2 Con. Support	
LTE Antenna	2dBi, 1T1R Dipole Antenna	
Status LED	1-LTE, 1-LAN, 1-WAN, 1-PWR, 1-WIFI	
USB 2.0	Host port 1	
Console	RS-232 Lite	RX,TX,GND
Surge Protection	10/700μs / 400W	
ESD Protection	Contact : ±8KV, Air : ±15KV	
Operating Temperature	-40 ~ 85℃	
Operating Humidity	10 ~ 90%	Non-condensing
Input Voltage/Current	DC 24V / 2.5A max Adaptor	
Power Consumption	<10W (35W / PSE 1port)	
Dimension	144mmx125mmx32mm	
Weight	< 380g (< 430g in case PSE)	

Software	characteristics
VPN	Multi and Bonding Tunnel
	Split Tunneling
	IPsec, IKE Version 1,2
	Transport/Tunnel Mode
	Crypto Algorithms(3DES, AES123/192/256)
	Authentication Algorithms(MD5,SHA1,SHA2)
	Dead Peer Detection
	NAT Traversal
Firewall	Stateful packet Inspection
	Tuples direction/Type
	Static, Dynamic NAT
	Exclude, Double NAT
Network	Route Mode/ Multipath route
	Policy based routing
	QoS / DHCP Server, Relay
	DDNS/ LLDP
IPv6	IPv6 Routing/Firewall/Ipsec
	6 to 4, ISATAP
Management	SNMP v1/2/3
	CLI, Web UI
	Syslog
	System Firmware update function



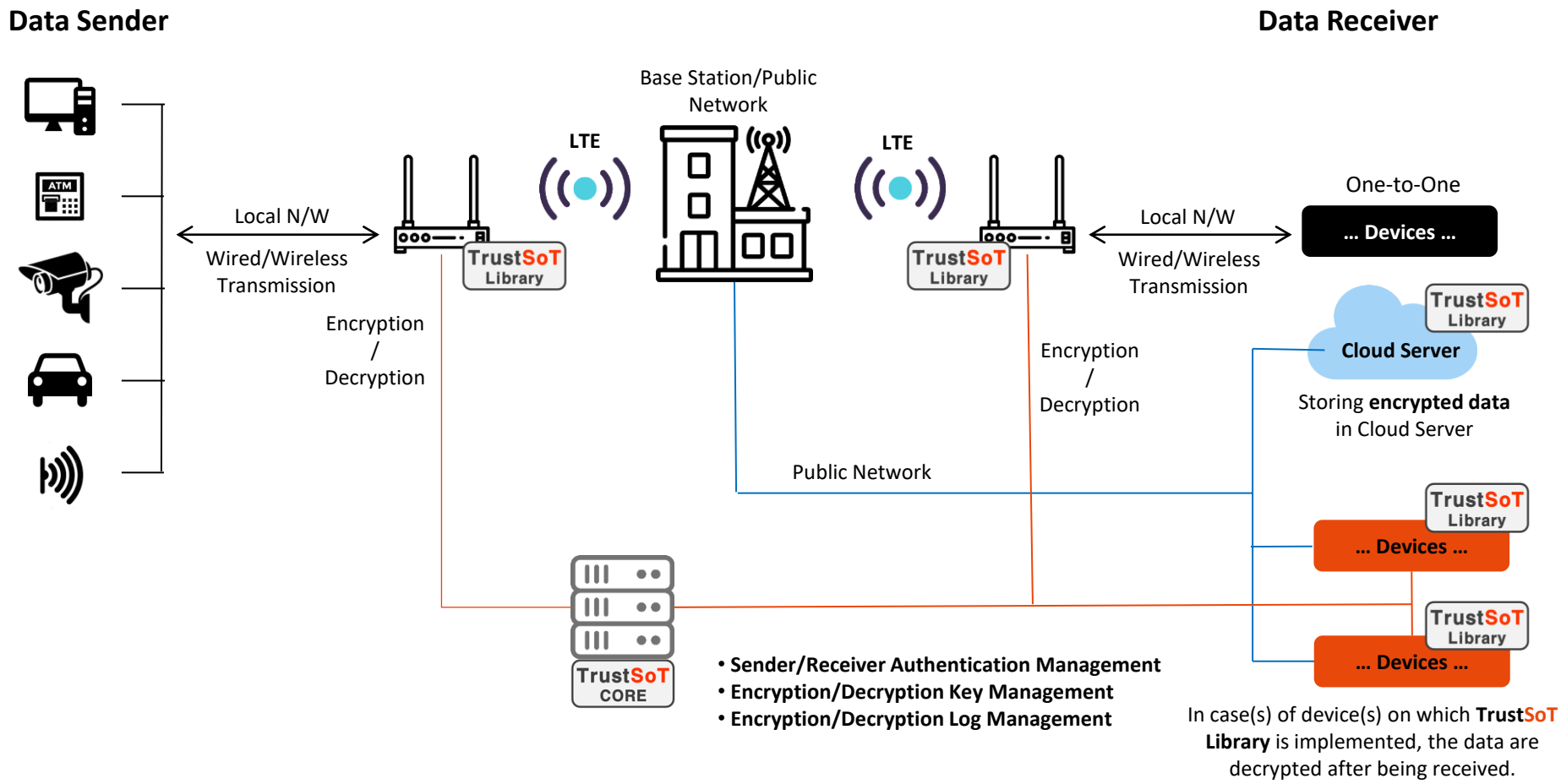






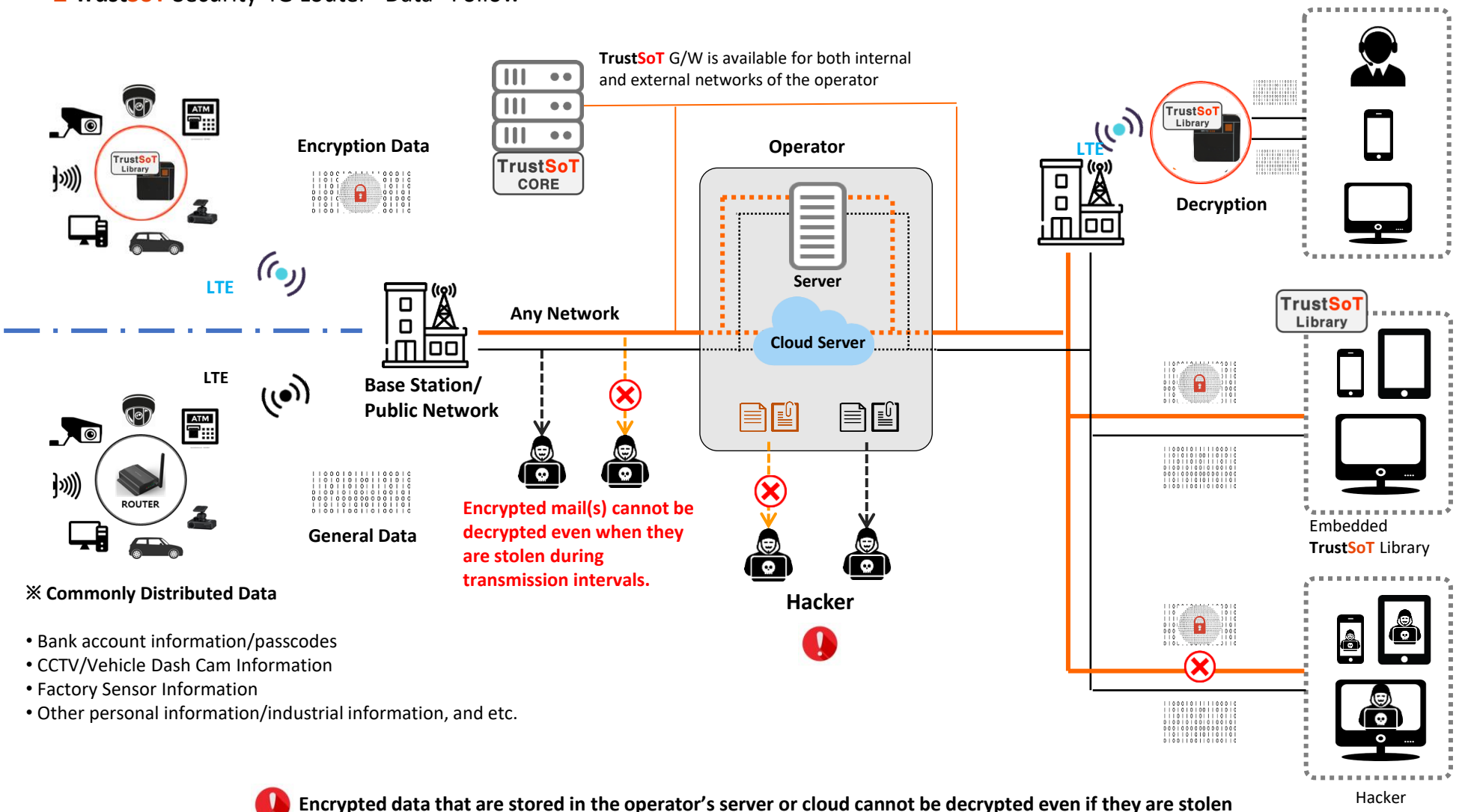
Security LTE Router (TrustSoT CORE Implemented)

■ When data generated by all devices are LTE transmitted through "**TrustSoT** LTE Router",
encrypted transmission and storage of the data are possible even when they are done over a public network or by using cloud service.



Security LTE Router (TrustSoT CORE Implemented)

■ **TrustSoT** Security 4G Louter "Data" Follow



※ Commonly Distributed Data

- Bank account information/passcodes
- CCTV/Vehicle Dash Cam Information
- Factory Sensor Information
- Other personal information/industrial information, and etc.

Encrypted data that are stored in the operator's server or cloud cannot be decrypted even if they are stolen
(General mail(s) in storage can be viewed when they are stolen.)

TrustSoT SCADA/PLC Demo System Software Configuration

Classification	Linux	Windows
Version	Kernel 3.X or higher	7 or higher
Standard Distribution Version	Ubuntu 18.04, CentOS 7.6	Windows 7, Windows 10
Implementation Environment	C/C++, Python 3.X, Shell script	C/C++, Python 3.X, C#
Library	GCC 7.1 or higher	.NET 4.0 or higher
Development Tool	Supports most development tools.	Visual studio 2017 or higher
Database	Postgressql 11 or higher	Postgresql 11 or higher
Packaging Method	Self-execution and Docker	Self-execution and Docker

TrustSoT SCADA/PLC Demo System Hardware Configuration

Classification	Minimum Specification	Standard Specification	Maximum Specification
CPU	4Core	8Core	8Core
CPU Architecture	Intel x86_64	Intel x86_64	Intel Xeon
Memory	8GB	16GB	32GB
SSD	256GB	1TB	1TB x 4EA (RAID)
Network Card	Ethernet 1 Gbps Two or more	Ethernet 1 Gbps Two or more	Ethernet 1 Gbps Two or more
Power Supply	2 EA	2 EA	2 EA
Interface Port	USB 3.0	USB 3.0	USB 3.0
User	less than 1,000	less than 5,000	less than 10,000

■ **TrustSoT** SCADA/PLC Demo System

Classification	Components
CPU	Siemens PLC 315-2 PN/DP
DI	Siemens PLC 321 (32Points)
DO	Siemens PLC 322 (32Points)
DIN Rail	Siemens DIN Rail for CPU 3xx
Power	Weidmuller 100~240V AC
Button	24V DC Input Push Button
Lamp	24V DC Output Lamp

※ Sofrware
Siemens Operation, Engineering and
TrustSoT encrypt communication library

Supply Performance

Key Clients

Samsung Electronics Co., Ltd.	Samsung Heavy Industries Co.,Ltd.	Samsung SDS Co., Ltd.	Samsung Corning Precision Materials CO., Ltd.
Samsung Fire & Marine Insurance	Samsung Life Insurance Co., Ltd.	Samsung Human Resources Development Institute	SAMSUNG ELECTRONICS SERVICE CO., Ltd.
Samsung Securities Co., Ltd.	SAMSUNG C&T CORPORATION	Samsung Display Co., Ltd.	SAMSUNG CORNING ADVANCED GLASS

KEB Hana Bank	HANA CAPITAL CO.,LTD.	Hana Financial Investment CO.,LTD.
KEB Hana Card Co., Ltd.	HANA SAVINGS BANK.	Hana Financial Group Inc.
Hana Life	Hanatrust	HANAMEMBERS.

Veterans Health Service Medical Center	Daejeon Bohun Hospital	Korea Veterans Health Service
Incheon Bohun Hospital	Gwangju Bohun Hospital	
Busan Bohun Hospital	Daegu Bohun Hospital	