TrustSoT

APT Security (OT8/ICS Sector)

2022

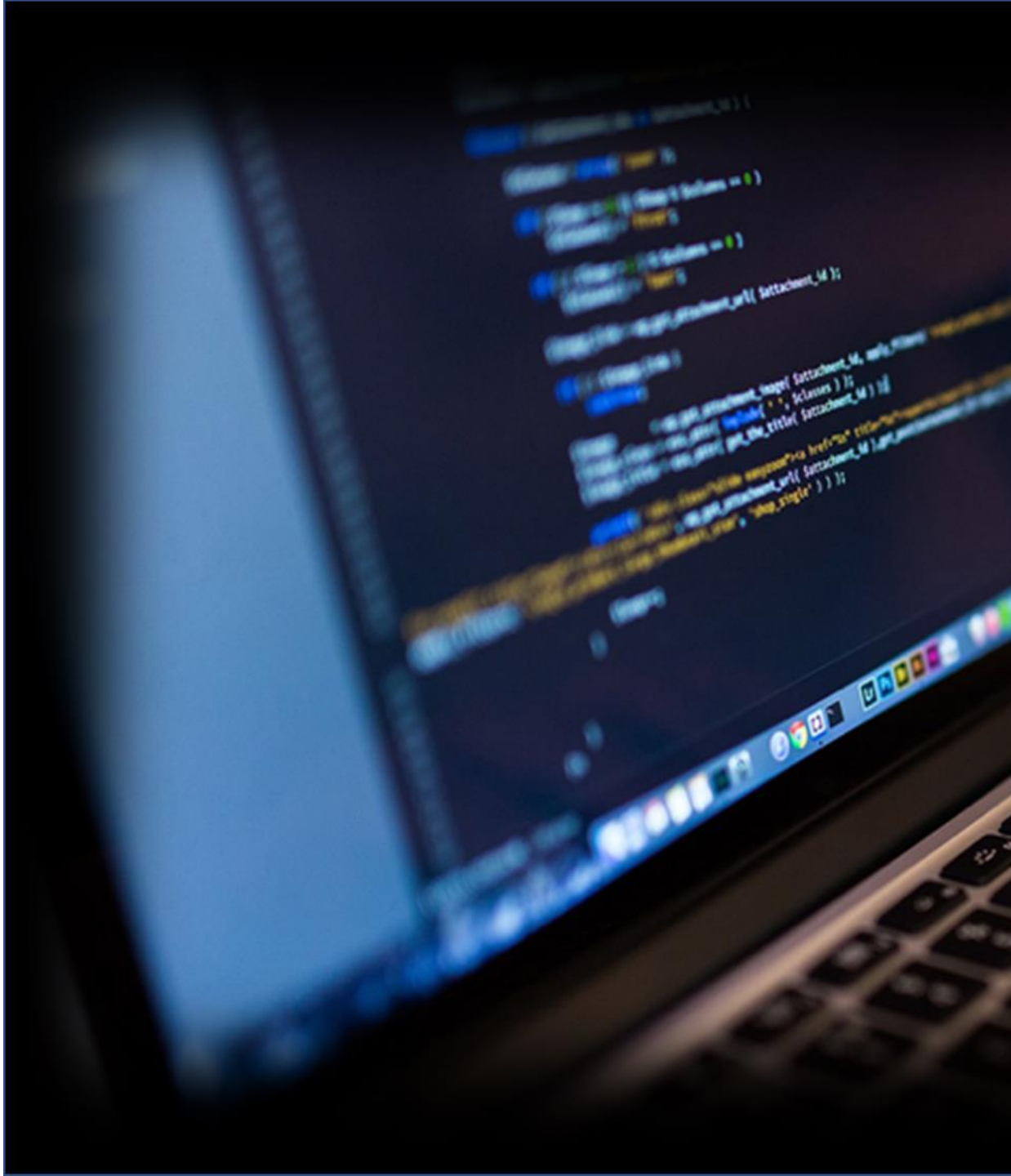


Table of Contents

Chapter 1 TrustSoT Introduction
About TrustSoT Solution ---- 04
Core Technology ---- 05
Core Technology “Device Authentication” ---- 06
Core Technology “Data Encryption” ---- 07
Software Structure and Functionality ---- 08
Product Configuration ---- 09
Applications ---- 10

Chapter 2 New Security Environment (APT)
Advanced Persistent Threats ---- 12
Differences Between IT and OT/ICS Environments ---- 14
Common APT Threat Routes for OT/ICS ---- 15
APT Attack Vulnerability of OT/ICS Area ---- 16
Key APT Attack Examples ---- 17

Chapter 3 TrustSoT‘s Response for OT/ICS APT Attacks
TrustSoT for OT/ICS Security ---- 19
TrustSoT vs. Similar Solutions ---- 22
Role as Reciprocity Supplement of TrustSoT & VPN ---- 23
Definitions of TrustSoT Functionalities ---- 24

Chapter 4 TrustNET Introduction ---- 25

Chapter 5 Uses and Functionalities of Different Components of TrustNET ---- 31

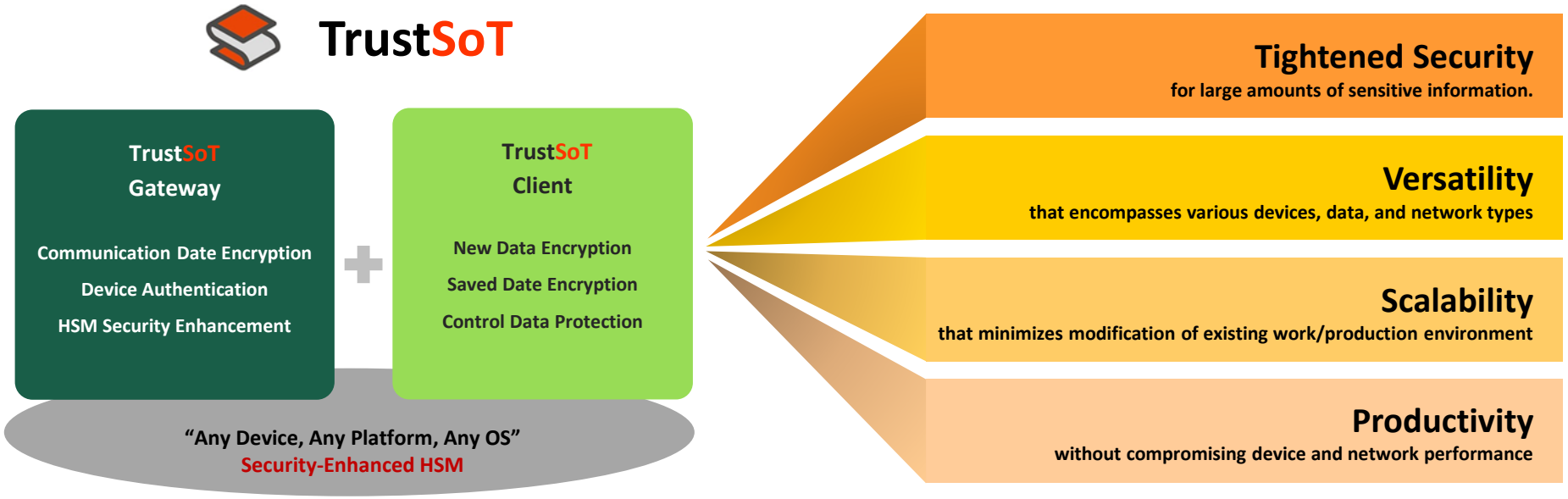
※ Attachment 1 Key Features of TrustNET ---- 49
※ Attachment 2 Key Clients ---- 53

About TrustSoT

Realization of security and integration under next-generation network environments with minimal investment.

Authentication and management of IoT devices and sensors with an ultra-light Cilent Library.
Interactive encryption of data and control signals.

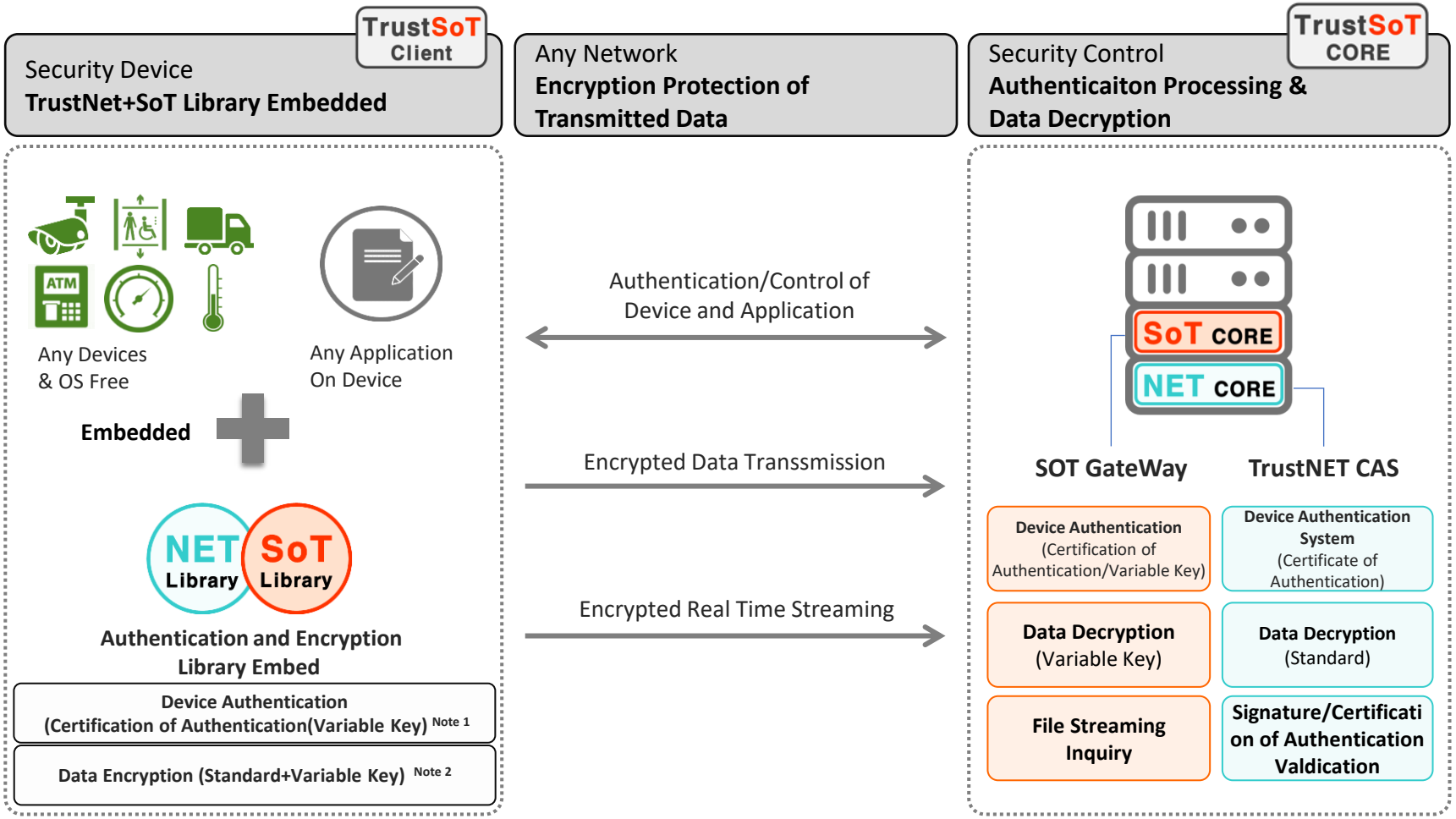
The most effective solution for responding to APT Note 1 Attacks



Provides complete protection for sensitive data across various devices and network types.

※ Note 1 APT : "Advanced Persistent Threats", in other words, "threats that are intelligent and persistent" (Refer to Chapter 2)

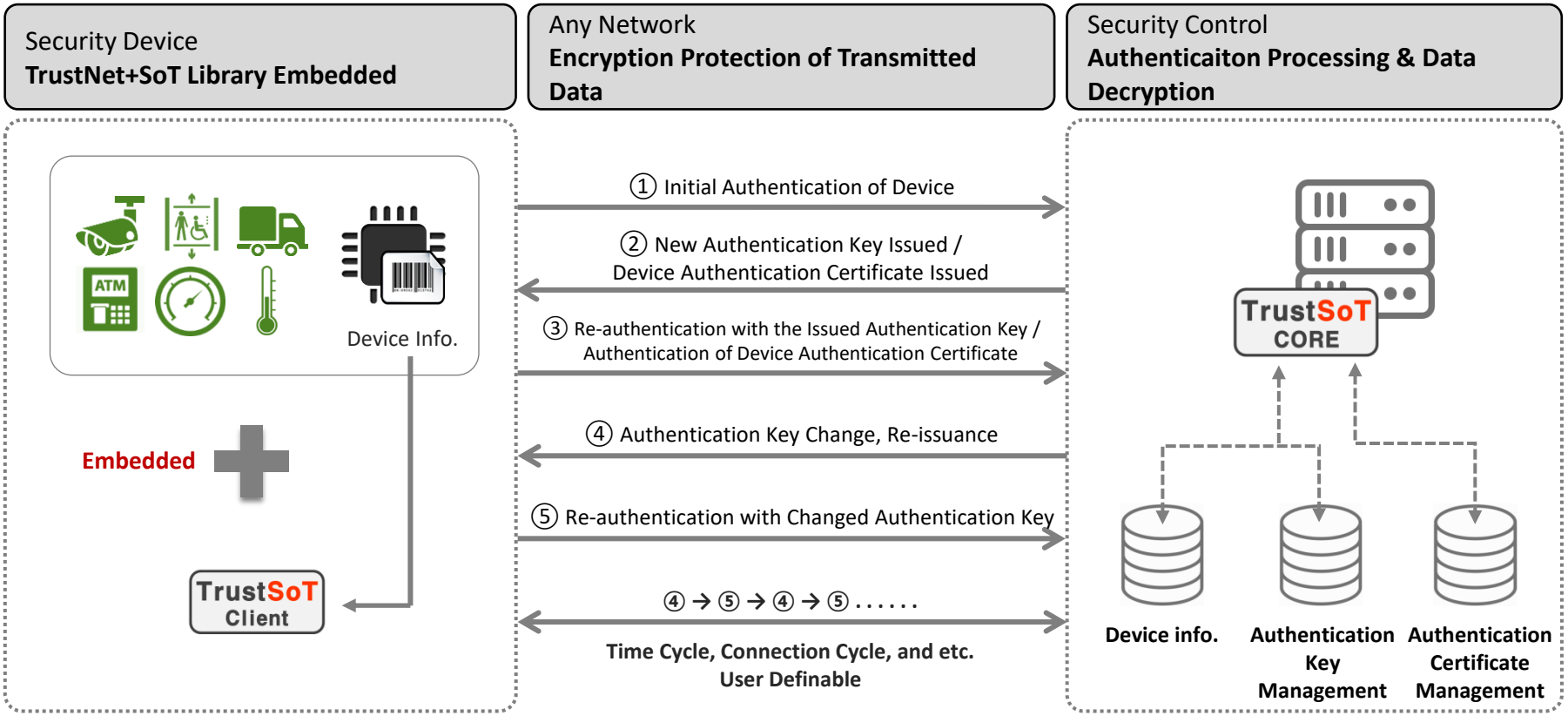
Authenticaion and Encryption



Note 1 Refer to "**Device Authentication**" on Page 6
Note 2 Refer to "**Data Encryption**" on Page 7

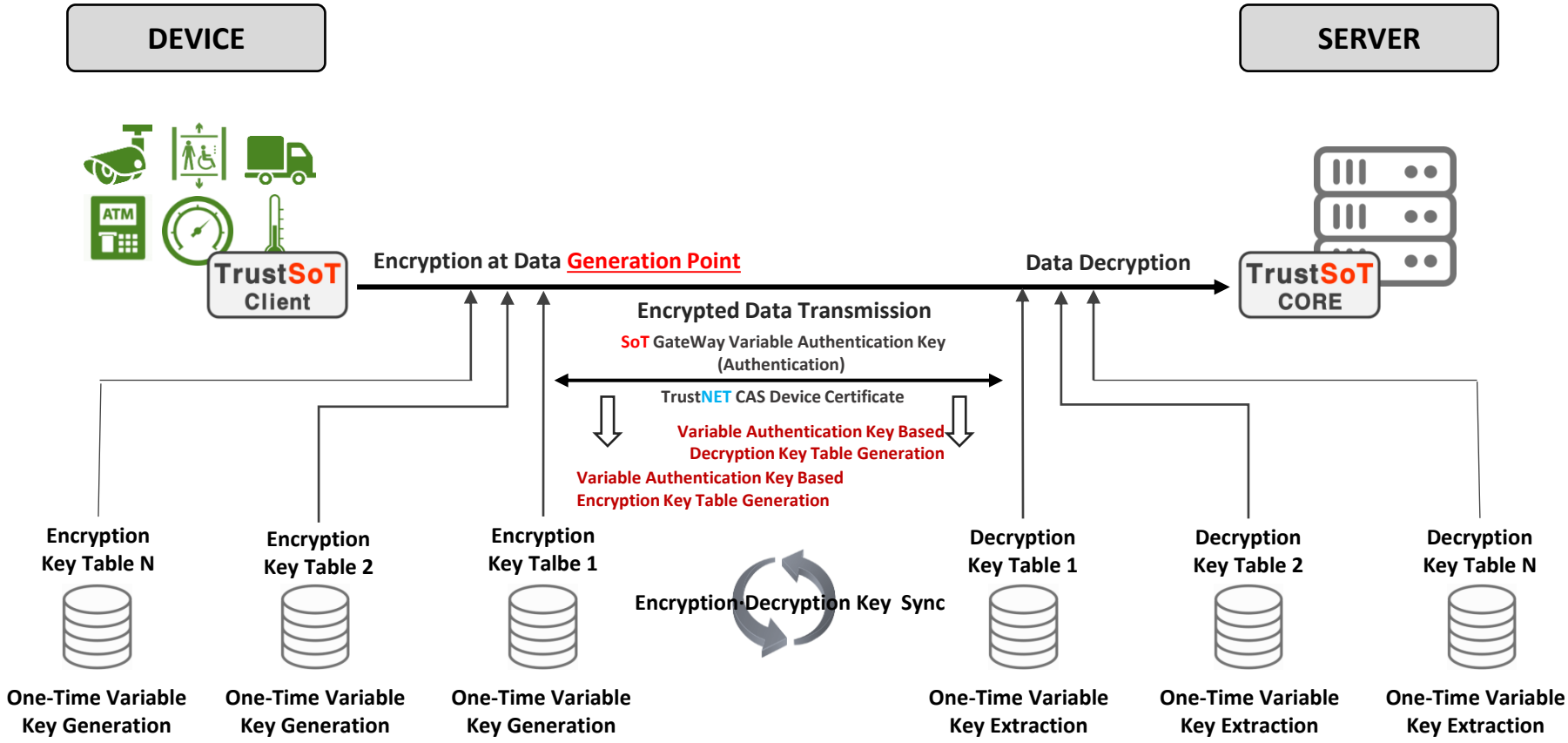
Core Technology “Device Authentication”

Devices in which **TrustNET CAS & SoT** is applied are authenticated based on unique information of the devices and the authentication reliability is maximized by updating new authentication keys every time the system is connected after the initial authentication (Ability to support Device Authentication Certificate).



Core Technology "Data Encryption"

Devices on which **TrustNET & SoT** is applied perform data encryption based on a one-time variable encryption key from the time of the data generation to completely protect all data that are being transmitted or stored (support standard authentication encryption module and algorithm).

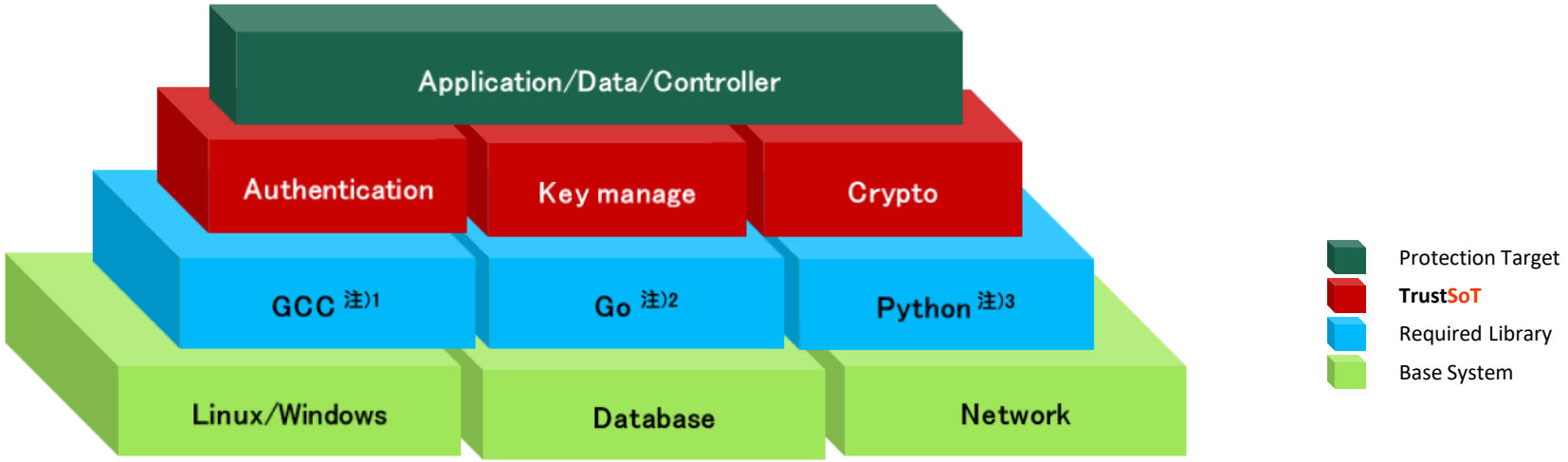


S/W Configuration and Functionality

TrustSoT S/W

Consists of 100% self-developed engines and libraries based on 100% of proprietary patents.

- Koeran Patent: Encryption method and system using authorization key of device (NO. 10-2028151)
- Japanese Patent No. 2017-563588, US Patent: 16/603,339



Note 1 GCC
A library for C/C++ languages and is mainly used for development of various data processing that requires speed.

Note 2 Go
A development language for web-based user screen / Javascript or HTML for web is internally used, but the core operating language is Go language

Note 3 Python
Responsible for log analysis collection and application of artificial intelligence module. / Most log analysis collection, artificial intelligence module are provided with this Python.

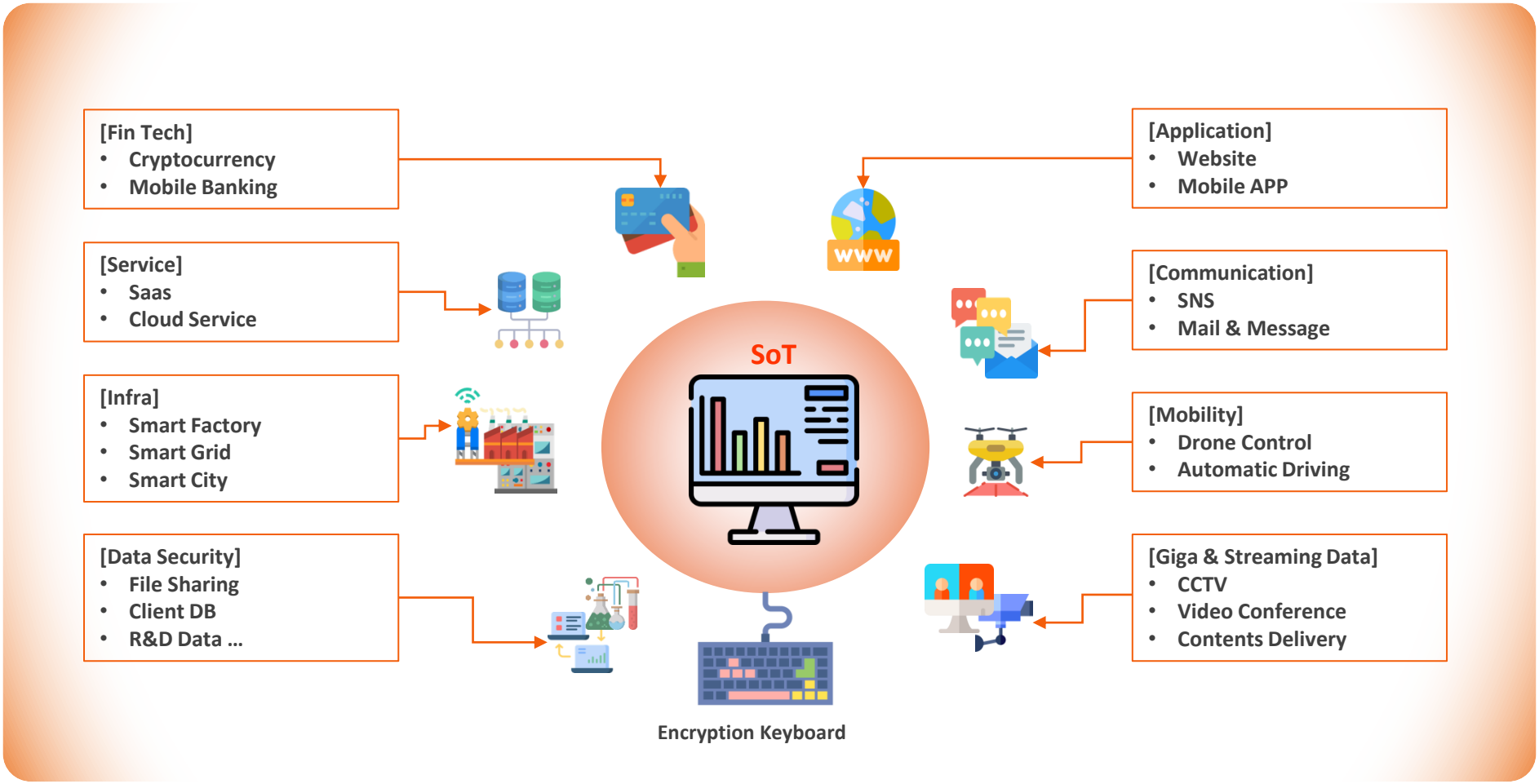
Software Configuration

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

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 1Gbps Two or more	Ethernet 1Gbps Two or more	Ethernet 1Gbps 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 is applicable to all areas and it encrypts and protects key data and control commands in various types of networks

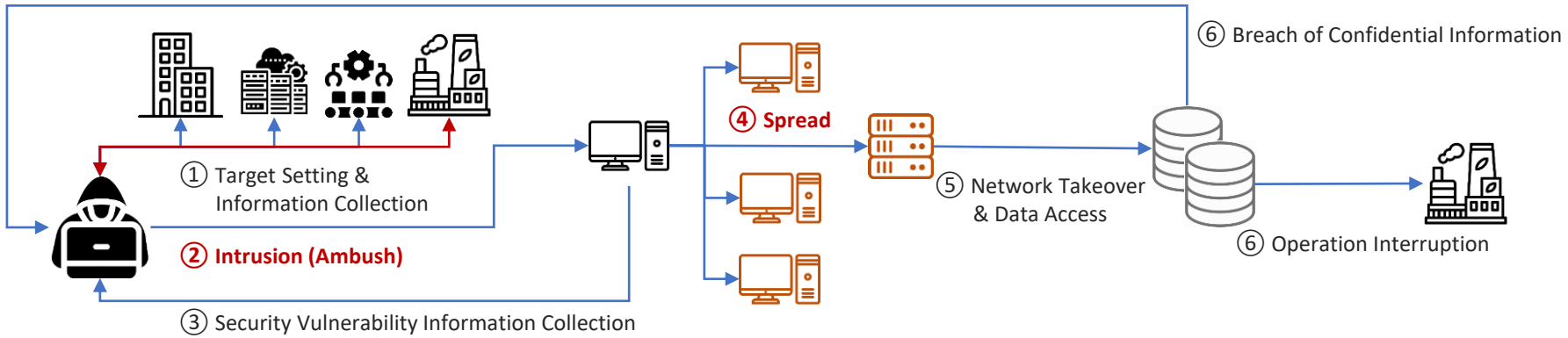


New Security Environment

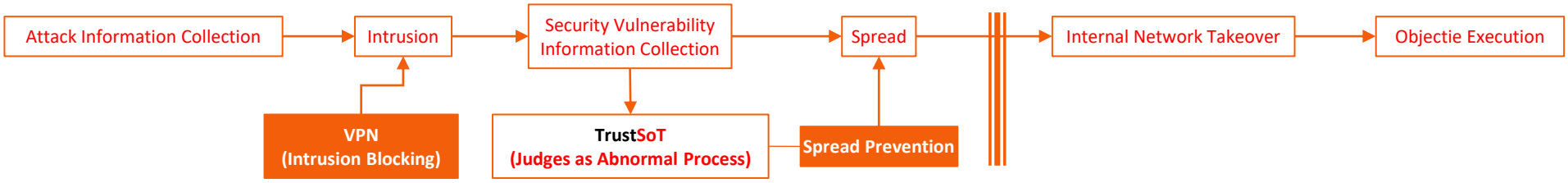
(APT : Advanced Persistent Threats)

APT Threat that neutralize most security solutions such as PKI(SSL/TLS), VPN, and etc.

- "Advanced Persistent Threats" i.e. "**Intelligent and Persistent Threats**"
- Unlike past attacks that targeted unspecified random targets, APT attacks target **one single target** and **continue the attack** by producing multiple security threats based on various IT technologies and attack methods until they succeed in intrusion into the target.
- After successfully **intrusion** into the inside, they establish strategic bases and **spreads** to normal internal systems (desktop computers, servers, and etc.) by using the collected **security vulnerabilities**.
- After taking control of the internal system, they perform **intrusion purposes** such as collection of confidential information, suspension of operations, and system paralysis.
- Used as means of most recent hackings and they target velnerabilities of PKI's and VPN's in particular.



"TrustSoT" and "VPN" are reciprocity supplements that can be used to implement perfect security solution against APT attacks.



(Refer to "Role as Reciprocity Supplement of TrustSoT & VPN " on page 23.)

APT Differences in APT Attacks and Previous Malware Attacks

Characteristics of APT Attacks that are Different from Previous Malware Attacks

① **Advanced** (Intelligent)

② **Persistent** (Persistent)

③ **Motivated** (Motivated)

④ **Targeted** (Targeted)

Classification	Malware Attacks	APT Attacks
Attack Distribution	Unspecified, random attacks	**Detailed and organized plans**
Attack Targets	Unspecified mass	**Government agencies, organizations, and companies**
Attack Frequencies	One-time	**Continuity**
Attack Technology	Malware Design	**Use of highly intelligent security threats at the same time**
Detection Rate	99% detection rate if discovered within 1 month.	**Below 10% if discovered within 1 month.**
Attack Results	Malicious code infection, breach of personal data.	**Breach of confidential information, inoperative system, Paralysis of social infrastructure**

Diffrences between IT and OT/ICS Environments

IT(Information Technology) : Open network such as internet, and information communication techlogies that uses such network.
OT(Operational Technology) : Technologies for management of industrial machineries or processes that have been operated within closed network, but gradually being expanded into open network area.
ICS(Industrial Control System) : Systems for controlling various types of machineries and processes that are operated within closed network. **Security awareness are rather low** because most use specifically designed specifications such as customized hardwares, operation systems, and softwares.

Classification		IT	ICS
Hardware	Device Configuration	Standard Device (Desktop Computer, Server)	**Standard Device, Process Specific Device**
	Configuration Modification Cycle	Short	**Almost No Modification**
	Patch and Maintenance	Occurs frequently for performance enhancement	**Almost none because of operation time**
Software	Operation System (OS)	Universal OS	**Control Device (Windows) Control Target (Customized Embedded OS)**
	Mainly Used Software	Commercially available for business and self developed	**Commercially available for customization and self developed**
	Update Cycle	Frequent patches for functional errors and security	**No patches except for functional errors**
Security	Security Objectives	Prevent breach of critical data and service interruption.	**Prevent possibilities of production and process interruption.**
	Influence of Security Incidents	Damage caused by the importance of breached data.	**Direct damage from production and process interruption.**
		Legal issues and defamed company reliability.	**Defamed product reliability.**

Common APT Threat Routes for OT/ICS

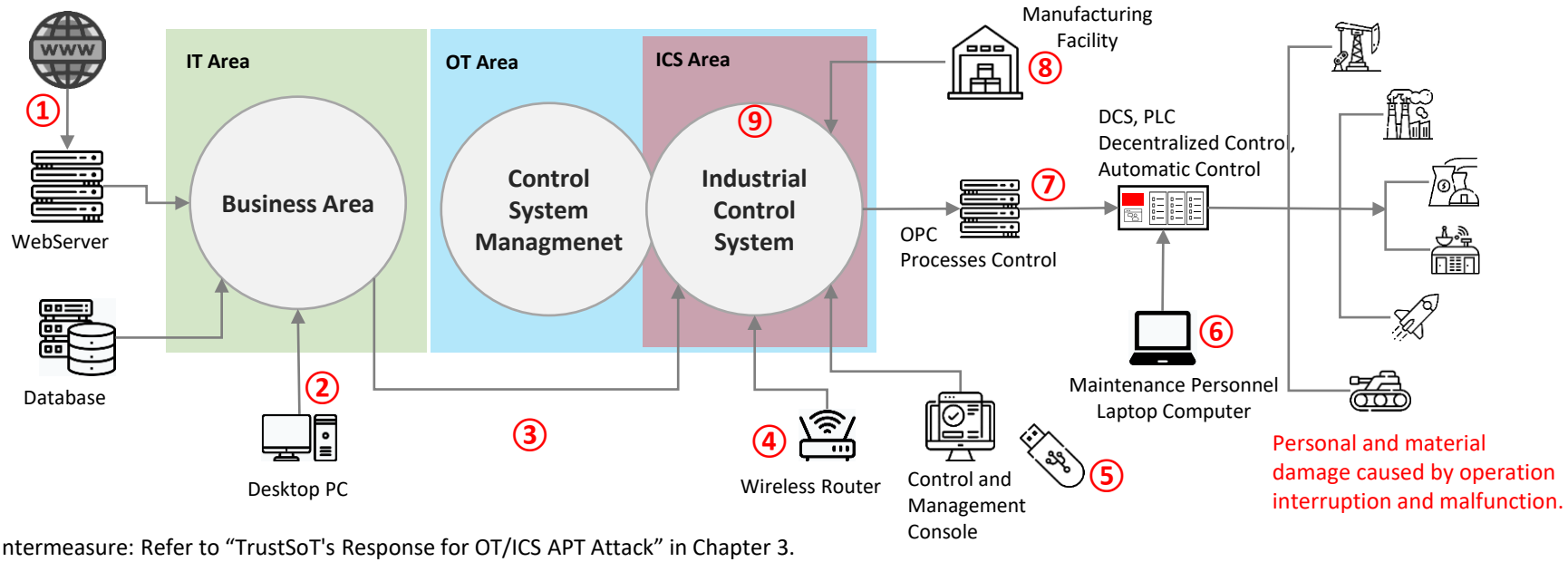
Network Area Classifications

- **IT** (business) area where executives and employees perform their duties.
- **OT** (Control System Management) area for product production.
- **ICS** (Industrial Control System) area that control manufacturing processes and produces products.

Various Security Threats

- IT Security Threats (Hacking, Malware Infection, APT Attack)
- Collects internal information by infiltrating into business area first, and then attacks ICS area.
- Attack by illegal ICS intrusion.

	APT Threat Routes	TrustSoT
①	IT security threats such as hacking, APT attacks, and etc.	
②	Spreads within Network after malware infection.	○
③	Abuse of unauthorized connection from business network to ICS network.	
④	Remote authentication bypass and vulnerability attack within ICS network.	
⑤	Malicious code distribution and breach of critical information by using USB.	○
⑥	Infected laptop computers of outsourced/maintenance personnel.	○
⑦	Control command tampering and protocol information leakage	○
⑧	Abuse of manufacturer's remote maintenance channels.	○
⑨	Single network failure (duplexing not applied).	



※ Countermeasure: Refer to “TrustSoT's Response for OT/ICS APT Attack” in Chapter 3.

Neglection of OS Update (Security Patches)

Most industries operate without OS upgrades (security patches).

- Cause 1) **Security patches can often be neglected** due to characteristic of prolonged operation under closed (independent) network environment.
- Cause 2) Because real-time performance and uninterrupted operation are very important in industrial control, any possibility of **operation interruption are avoided by the industry.**
  In particular, **SCADA program is Windows version**, and **security patches through upgrades are absolutely necessary in the case of Windows OS**.

※ Daily Security (Feb 14, 2021)
- Details of cyberattack on water treatment facilities in Florida have been disclosed.
- An **attack was intended to increase sodium hydroxide input to a dangerous level** by remotely accessing SCADA system of the water treatment facility.
  (Fortunately, a personnel was able to identify abnormal situation and take necessary actions to resolve the situation.)
- Intrusion Method : Access to a SCADA (Supervisory Control and Data Acquisition) system through TeamViewer software installed on one of many computers in the facility connected to the control system.
- Vulnerability : Windows 7 32 bit version with no upgrade was in use (**No update** since January 14, 2020)
  A same password was internally shared for remote access**.**
  Firewall protection function was not installed.
- Solution : Maintain computers, devices, and applications, including all software and programs, patched and up to date.
  Use of two-step authentication with strong passwords.

※ **Response of TrustSoT** (Refer to pages 18~24)

Response 1) OS Regardless of OS upgrade, all ports and packets occurring on client desktop computers, server (SCADA) are monitored and an alarm is triggered or the network is blocked when any abnormality is detected.

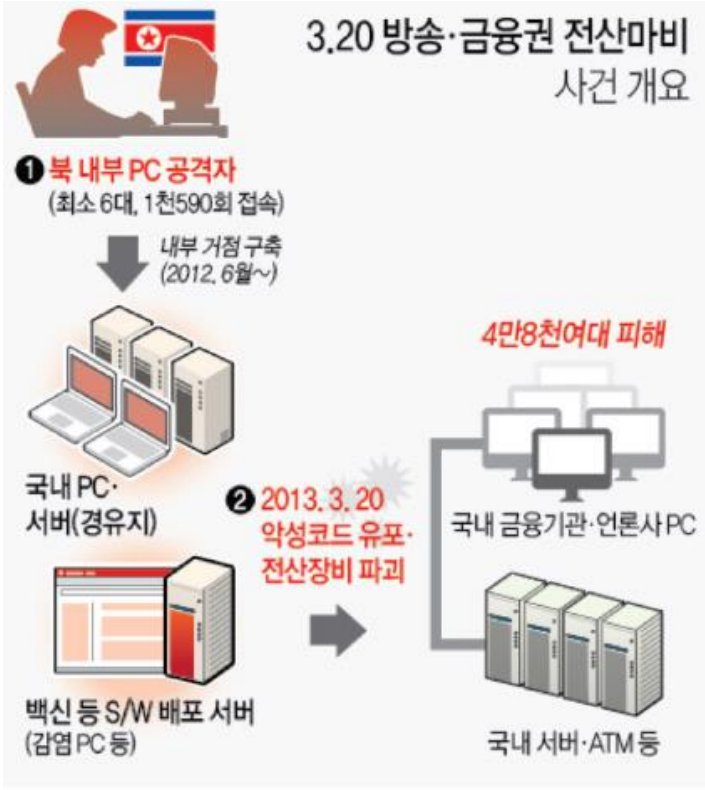
Response 2) Even if any ID/password is shared or stolen, access other than from an authenticated terminal is blocked (control command impossible).

☐ **March 2020 Computer Network Failure** - South Korea
- Infiltrated the network by bypassing vaccine company's update server and initiated the attack after incubating for more than one year (North Korean Intelligence Agency).
- The computer network was paralyzed due to destruction of the booting area (about 48,000 systems such as desktop computers and ATMs were destroyed.)
- Broadcast companies (KBS, MBC, YTN) / Financial institutions (Shinhan Bank, Nonghyup)

☐ **Pyeongchang Olympic Opening Ceremony Attack** – South Korea
- The target was at 8 p.m. of February 9, 2018, the time of the opening ceremony and 50 core servers were destroyed.
  . Infected 300 desktop computers after hacking a router in the computer room of the Olympic Operation Headquarters a month before the opening ceremony, gained an access to the server by stealing 44 account information.
- Olympic related websites were paralyzed, and Wi-Fi services at the Olympic sites and IPTV of the media center was interrupted.
  Ticket sale was suspended after 8 o'clock (resulted in some empty seats at the opening ceremony).
- Russian Main Intelligence Directorate (Disguised as an act of North Korea)

☐ **Interruption of Colonial Pipeline Operation** – United States of America
- Ransomware attack, suspected as an act of Russian Darkside.
- Oil prices rose 5-6% due to paralysis of oil pipeline and 3 million barrels/day supply disruptions.

☐ **What is Stuxnet?** - Iran
- Sophisticated and **military-grade malicious computer worm designed to target Siemens SCADA system**.
- Causes malfunction of control systems of major industrial infrastructure such as nuclear power, electrical, steel, semiconductor, and chemical industries.
- Interference of Iranian nuclear power plant operation in July 2010 (Siemens SCADA System).



TrustSoT's Response for OT/ICS APT Attacks

"Monitoring and detection" and "Network blocking (technical defense) and Risk Warnings (administrative defense)" against APT Attacks

TrustSoT **monitors and detects** APT spread paths on all routes, while **blocking and issuing warnings** when any anomalies are detected.

[Monitoring and Detection]

☐ **Client**
- Behavioral Period Analysis : **TrustSoT** Agent monitors events such as abnormal processes and patterns for all files received from external sources when such files are executed.

☐ **Network**
- Port Scanning : Monitors abnormal services that occur between IP and port.
- Traffic Analysis : Monitors abnormal patterns for increase and decrease of traffics.

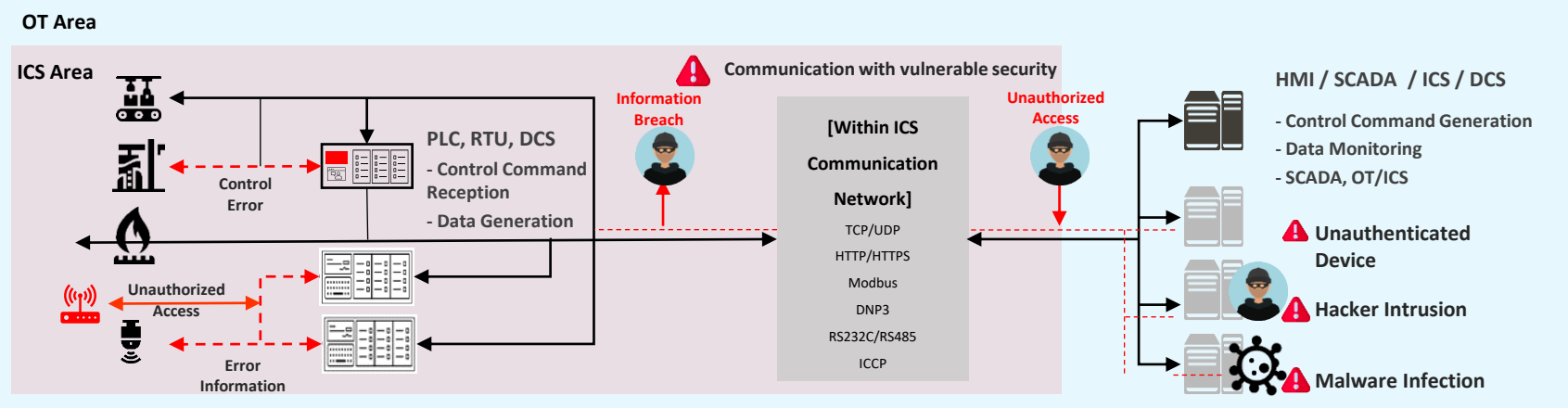
☐ **Server**
- Security Information/Event Management (SIEM) : Implements proactive measures by analyzing collected abnormalities data.
- Log Analysis : Monitors attacks by organizing system logs and timelines.
- Monitors unauthenticated client access (blocks unauthenticated clients regardless of user information such as ID's and passwords).

[Blocking and Warning]

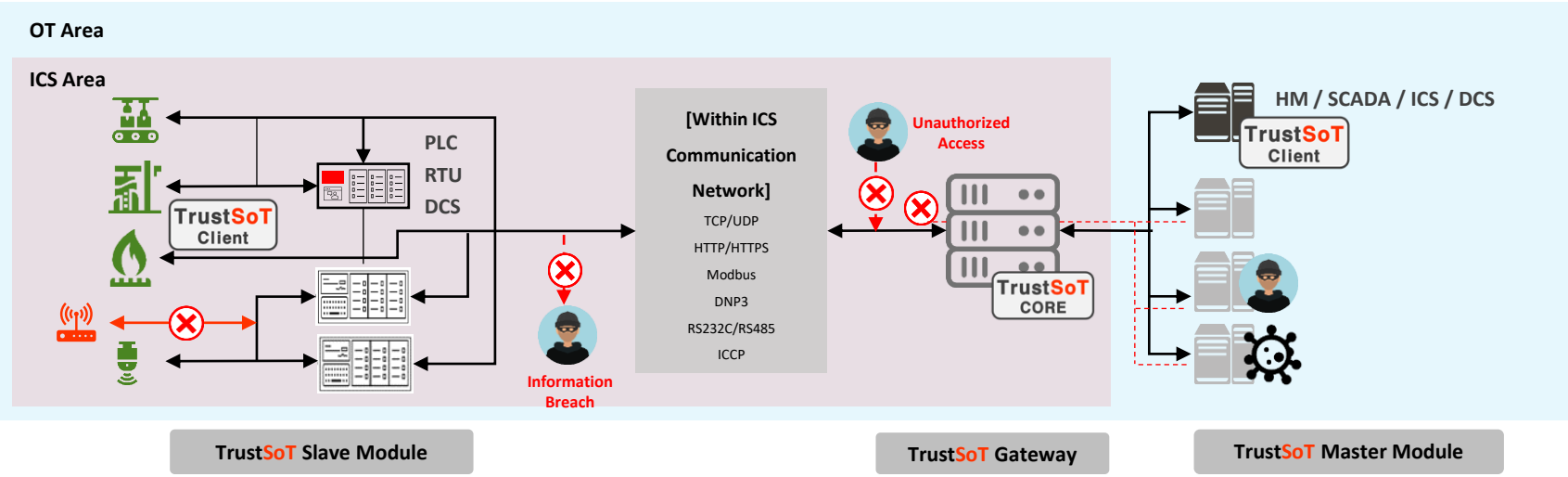
☐ Monitors and detects any abnormalities for the abovementioned attack targets in real-time, while blocking the network and issuing warnings to prevent spreads of infected data from the corresponding client when any abnormalities are detected.

※ Current Responses to APT Attacks
- Although warnings about APT attacks have been issued since 2019, it has been confirmed that the only defense solutions that have been implemented are issuing of warning messages before execution of files attached to emails and developments of vaccines through analysis of previous infection cases (an opinion of Korea Internet and Security Agency).

AS-IS Configurations of current OT/ICS (Industrial Control Systems) field do not have adequate protection plans for device control and monitoring that are conducted internally. Therefore, a different protection system is required for each sector.



TO-BE In order to solve various security problems that may arise in OT/ICS (Industrial Control) sector, TrustSoT protects the control sector through device authentication, data encryption, and event monitoring.



Key Features of Gateway and Module

TrustSoT Slave Module

- Decryption Key Request
- Control Command Decryption & 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 & 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

DEMO Device

Classification	Configuration
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

"SIEMENS Korea" Validation : Confirmed safe protection of control data and normal control operation through "encryption of control data" and "decryption of receiver side" using SIEMENS PLC (Confirmed by technical and sales teams of SIEMENS Korea)

Key Differences

While existing APT security solutions focus on **defense against installation (intrusion)** of malware,
TrustSoT secures differentiation/superiority compared to other products by **focusing on preventing spreads from infected devices and protecting important data (encryption)**.

Classification	Paloalto	Symantec ATP (Advanced Threat Protection)	TrustSoT
Application Monitoring	○	○	○
URL-based Malware Intrusion Blocking	○	○	×
Email Malware Detection	○	○	×
Defense Against Network Attack	○	○	△ Device Port Monitoring
Internal spreads prevention after malware infection.	× **Application** Based Monitoring Policy establishment (such as permission and **Blocking**) Open/closed malware blocking	× **Port** Based Monitoring Policy establishment (such as permission and **blocking**) Open malware blocking	○ **Agent Based Processor Monitoring** Against all open/closed malware (all abnormal processes) **Execution Warning and Internal Spread Prevention (Blocking)**
Generation File Protection	×	×	○ Agent Based File Execution Event Monitoring
ICS (Industrial Control System) Protocol Support	×	×	○
Device User Monitoring	×	×	○
File Breach Protection	○	×	○
Key Features	**Intrusion Blocking**	**Intrusion Blocking**	**Spread Blocking** **Data Encryption**

Role as Reciprocity Supplement of TrustSoT & VPN

Features by Security Solutions

Solution	Feature
PKI	A solution for access and encryption of communication intervals.
VPN	A solution that implements a virtual private network in order to make **it impossible to access the protected network from outside**.
TrustSoT	Unlike PKI and VPN, which can only control access to communication intervals, **TrustSoT** provides **security from within** devices or software that connect to networks through **authentication and encryption at application levels**.

Capabilities of Security Solutions to Respond to Different Security Threats

Attack Types	Ratio (%)	PKI	VPN (Network Based)	TrustSoT (Device Based)	Response of TrustSoT
Document Based **Maleware Distribution**	90%	×	○	◯	Checks whether or not the document is generated by a device and an application that are authenticated by the user. **(Blocks Spread when Infected)**
DDos Attack by Malware	3%	○	○	△	Blocks anything but that are **packets of authenticated types** (Prevents service interruptions.)
Backdoor Based **Unauthorized Intrusion**	2%	×	○	△	Access is only given to encrypted data through **authenticated devices** and patented encryption technology.
File/Data Stealing	2%	×	○	◯	Variable key-based authentication encryption for each file and data is encrypted with different information for each encryption, **allowing only authenticated devices and users to decrypt.**
Industrial Control Lightings **Various Tampering/Forgery of Protocols**	1%	×	×	◯	Encryption of data at the time of protocol generation and **authentication and protocol analysis blocking** at the time of decryption at the receiving end.

Functions by Security Solutions

Classification		Functions	Description
TrustSoT	Gateway (Administrative Functions)	Authentication	Authenticates and controls accesses for users, devices, applications, data and files.
		Encryption	Operates encryption module and encryption key for data encryption generated from users, devices, and applications.
		Client Control	Executes and controls access of dedicated clients such as TrustSoT Agent and TrustSoT SCADA.
		Logs	Collects and monitors various logs.
	Workstation (General Business)	Encryption	Encrypts designated files and data.
		Process Monitoring	Monitors, notifies, and blocks device executed processes.
		Event Monitoring	Monitors, notifies, and blocks events of device's operating system.
		Communication Monitoring	Monitors, notifies, and blocks any port developments other than the designated ports.
	ICS (Control Network)	Control Command Protection	Authenticates/Encrypts transmitted from control unit to PLC.
		Protocol Monitoring	Blocks transmission/reception of protocols other than designated protocols.
		Access Control	Blocks control networks other than authorized users, devices, and applications.
		Status Management	Provides status monitoring and management information on various equipment and operating systems of connected control network.
TrustNet		PKI	Open Key Based Authentication Solution
		KMS (HMS)	Software (Hardware) Type Key Management Solution
		Official authentication encryption module	Encryption module certified by South Korean government (KCMVP)

TrustNET

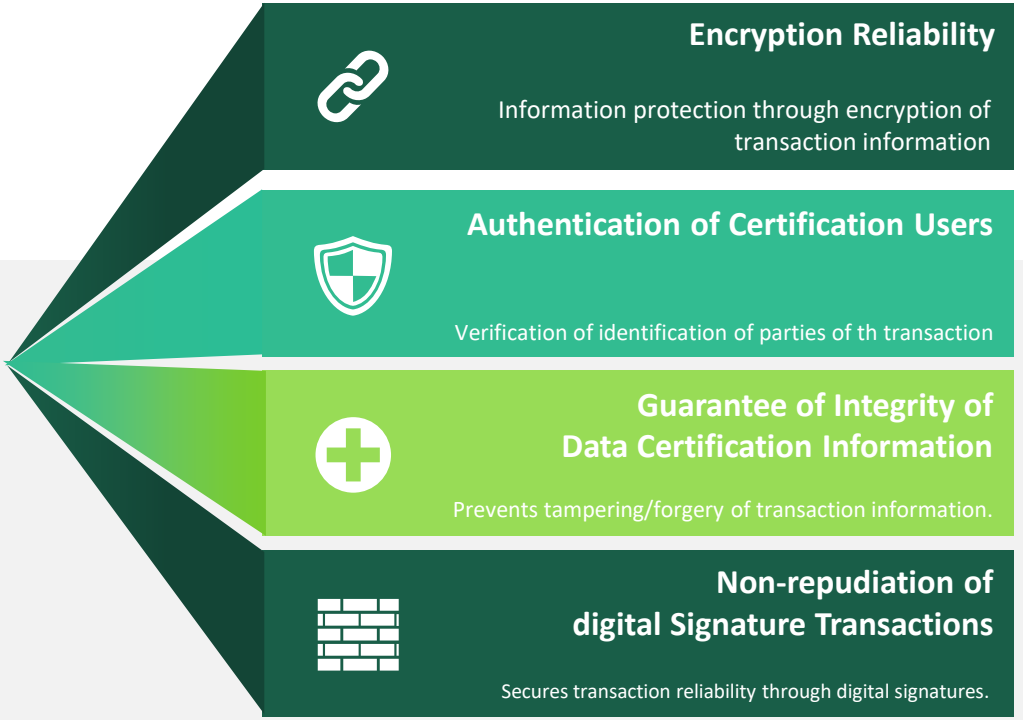
PKI

- Public Key Infrastructure a security technology that guarantees transaction secrets on the Internet while verifying identities of parties of transactions.
- Public key type certificates can be issued without installation of separate client programs.

TrustNET

Public Key Infrastructure

An electronic authentication based technology system that uses a public key method to give safety to information systems such as e-commerce systems and to give authentication functions for users and messages connected to the network.



Needs

Needs for information protection increases as more and more businesses are executed through data exchange in distributed systems environment, while information exchanges through various communication environments and terminals always poses risks of information breaches.

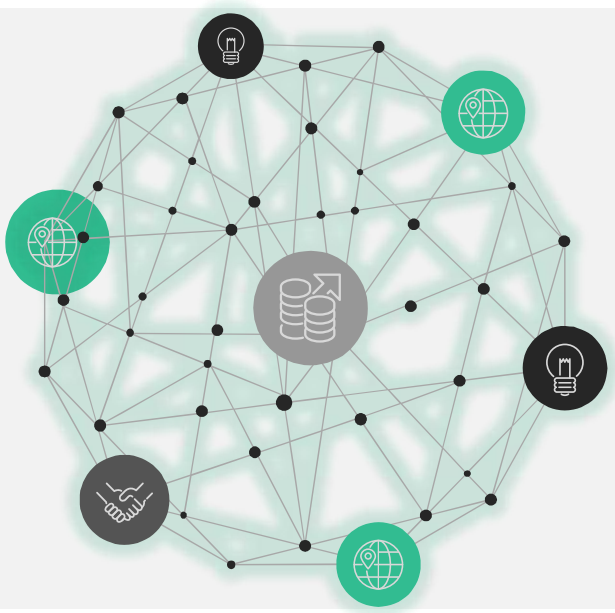
Data integrity and confidentiality must be guaranteed and secure infrastructure that can facilitate scalability of businesses executed through secure information exchange.

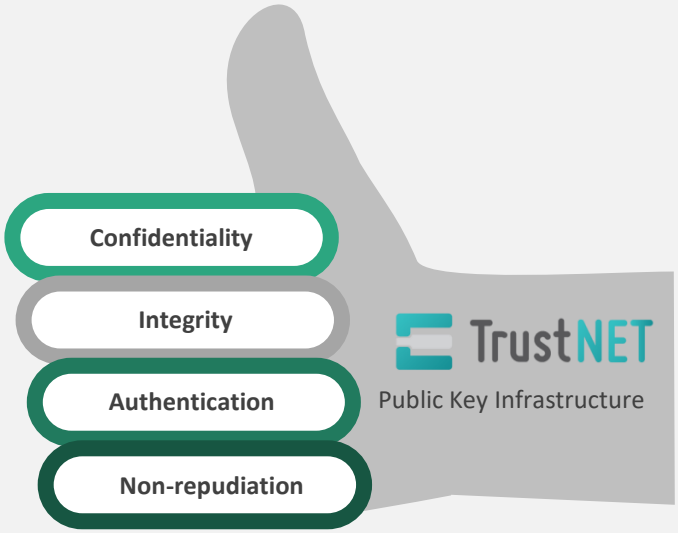
Background

Advancement of the Internet, and increases in distribution of personal information and corporate information assets.

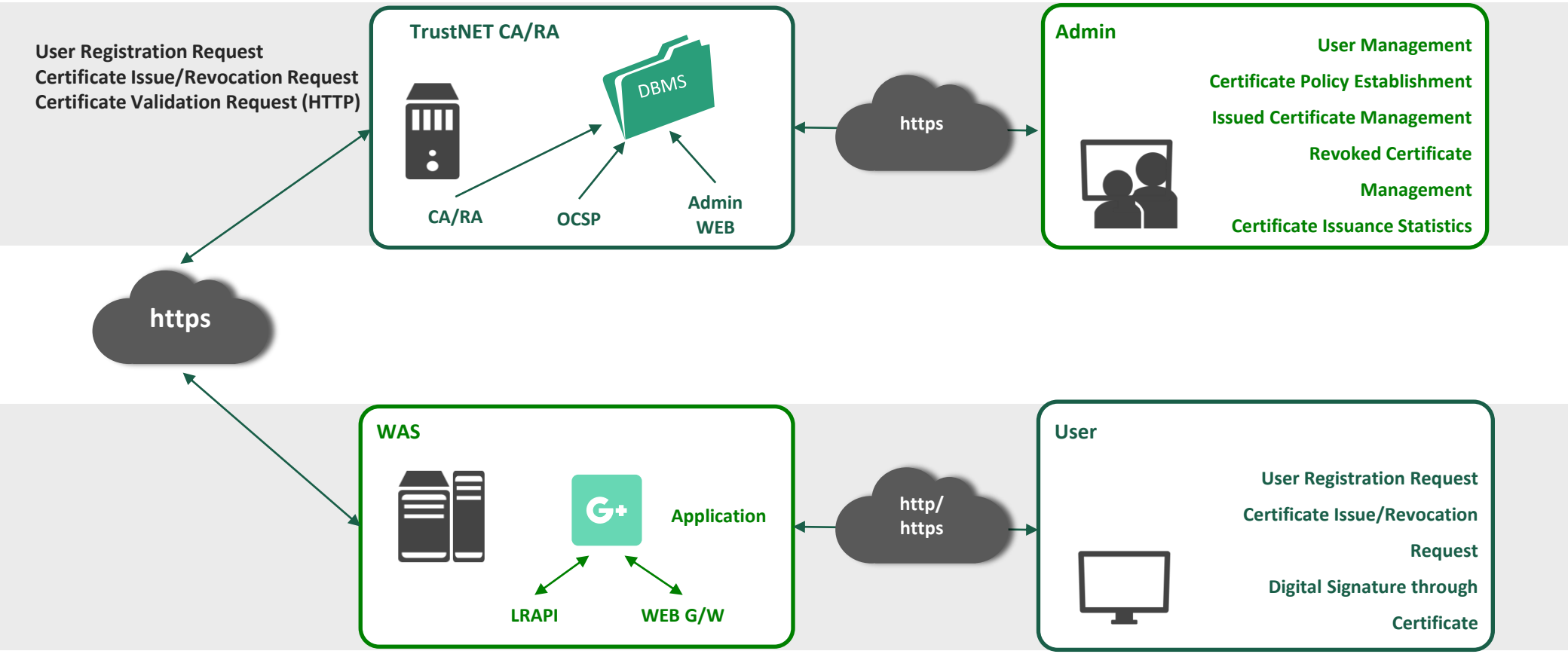
Issues

Eavesdropping of communication details,
Illegal user data tampering,
Repudiation of transmission and receipt.





Product Configuration Diagram



Product Configuration and Key Functionalities

Classification			Functions	Remark
Server	TrustNET CA/RA		Core PKI system that performs functions of registering user information and generating, revoking, and suspending certificates.	Certificate validation is based on OCSP in TrustNET.
	TrustNET OCSP		A system that verifies certificate validity in real time.	RDB handled by CA and OCSP server is separately required.
	Administrator Web Console		Establishes, issues, and revokes certificate policies, and verifies statistical information.	LDAP is separately required when CRL is used.
Applications	TrustNET LRAPI, Web Gateway	ActiveX client	A library used for registering users, deleting users, and performing certificate revocation functions to issue certificates to TrustNET CA/RA servers.	TrustNET CA client must be installed.
Client	TrustNET CA-Client For Desktop Computer	ActiveX Client	A control that is installed on desktop computer of a user, and issues and manages certificates in Windows IE environment.	
		Multi client	A control that is installed on desktop computer of a user, and issues and manages certificates in Windows, Linux, and Mac environment.	Non Plug-in Client is used. Active X is also used in IE.
	TrustNET CA-Client For Mobile	Internal Storage	Certificates and private keys are stored in internal storage, while being provided in forms of applications and it is possible to be used by VPN App or other apps that require such certificates.	Supports Android and iOS Environment
		External Storage	Certificates and private keys are stored in external storage, while being provided in forms of libraries, and certificate issuance and management are performed in external storage.	Supports Android and iOS Environment
	TrustNET Non-Native CA-Client		Performs client functions on the web without installing a separate client module.	All web browsers tha support HTML5.

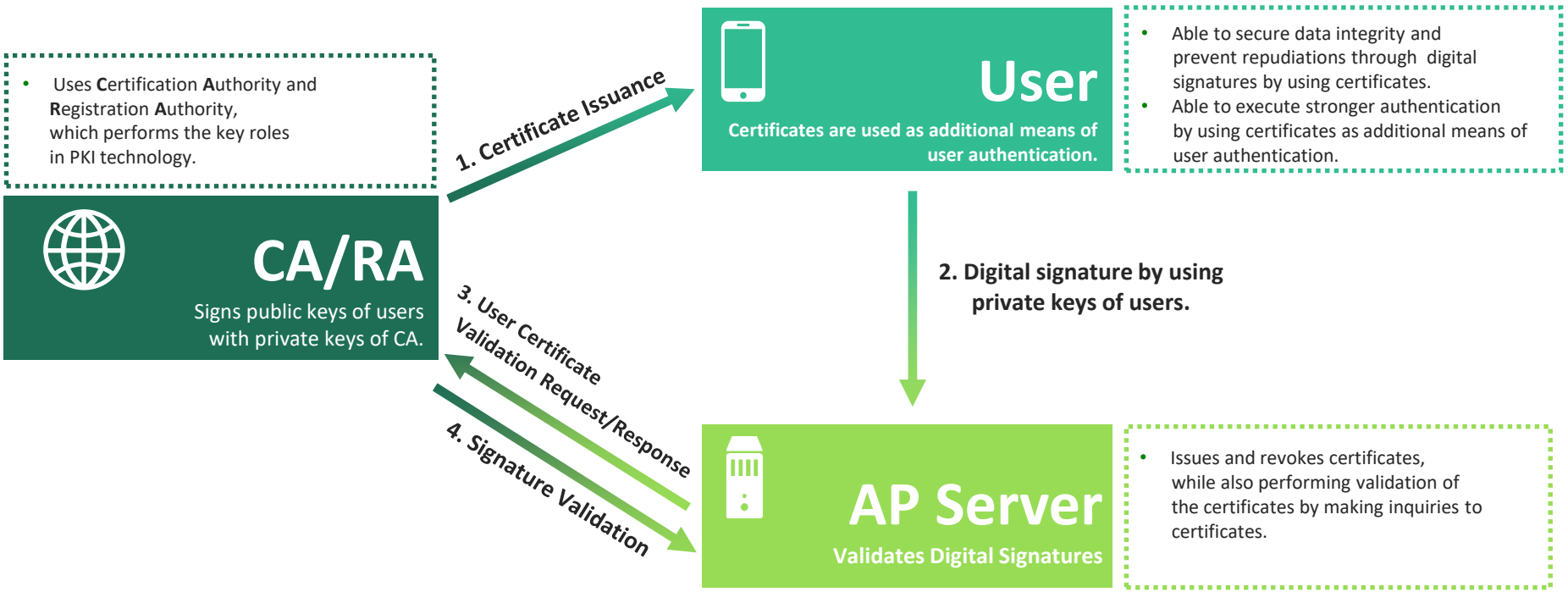
TrustNET Client Toolkit

Classification		Functions
Toolkit	**TrustNET Toolkit for JAVA**	Security libraries that are implemented in C/S application operation Environment
	TrustNET Toolkit for C/S	JAVA classes that are implemented in JAVA integrated environment.
	TrustNET Toolkit for ASP	Security libraries that are implemented in ASP web server for NT environment.
	TrustNET Toolkit for .NET	Security libraries that are implemented in .NET application environment.
	TrustNET Toolkit for PHP	Security libraries that are implemented in PHP based web server environment.

Uses and Functionalities of Different Components of TrustNET

Uses

- Assigns users DN through user information registration, and issues reference numbers and authorization codes for issuing certificates.
- Actively applies international standard technologies and the latest technologies.



Key Functionalities

Certificate Management

Issues, re-issues, revokes all certificates.

Manges certificate by using RFC 2510 CMP.

Stores certificate regardless of DBMS types.

(Uses MariaDB when no separate DBMS is used.)

Publishes certificate through LDAP sever sync.

Certificate Policy Establishment

Sets certificate expiration, key lengths, and key uses.

Sets single or multi certificate(s) per user policy.

Sets certificate preservation period.

Sets CRL renewal interval.

CRL Generation and Management Support

OCSP is provided as a standard for certificate validation,
but CRL generation and LDAP publishing functions are
also provided when there are separate requests.
Update is made periodically in accordance with a CRL update cycle
setting, and the CRL publishing location is attached to the certificate.

User Management and Statistics

Performs user registration and deletion by classifying users.

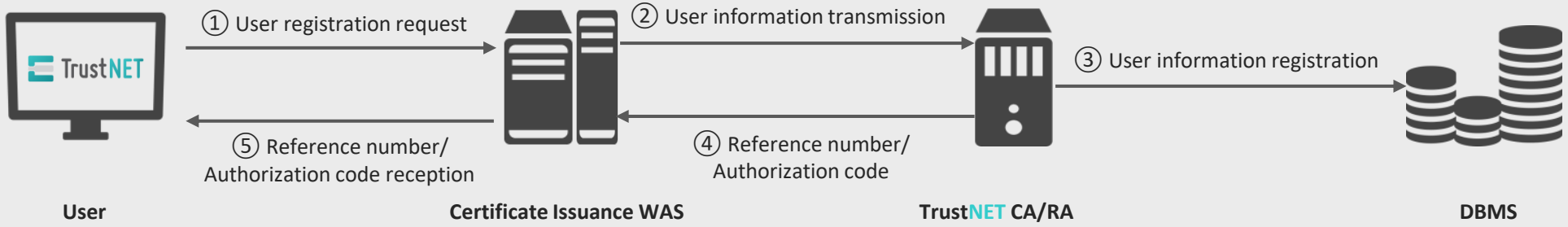
Provides certificate revocation functions due to resignation
such as certificate information (such as status, SN, DN)
inquiries and resignation.

Monthly user registration statistics function.

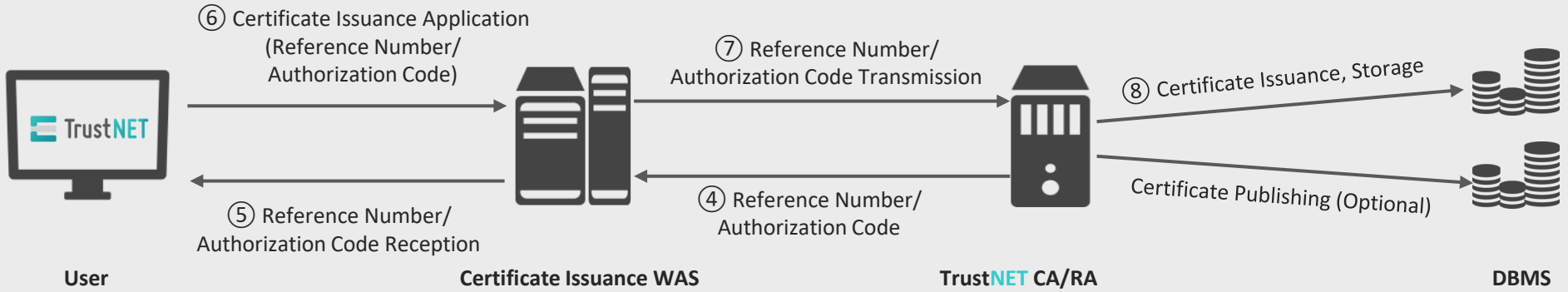
Monthly certificate issuance and revocation statistics function.

Certificate Issuance Processes

User Registration

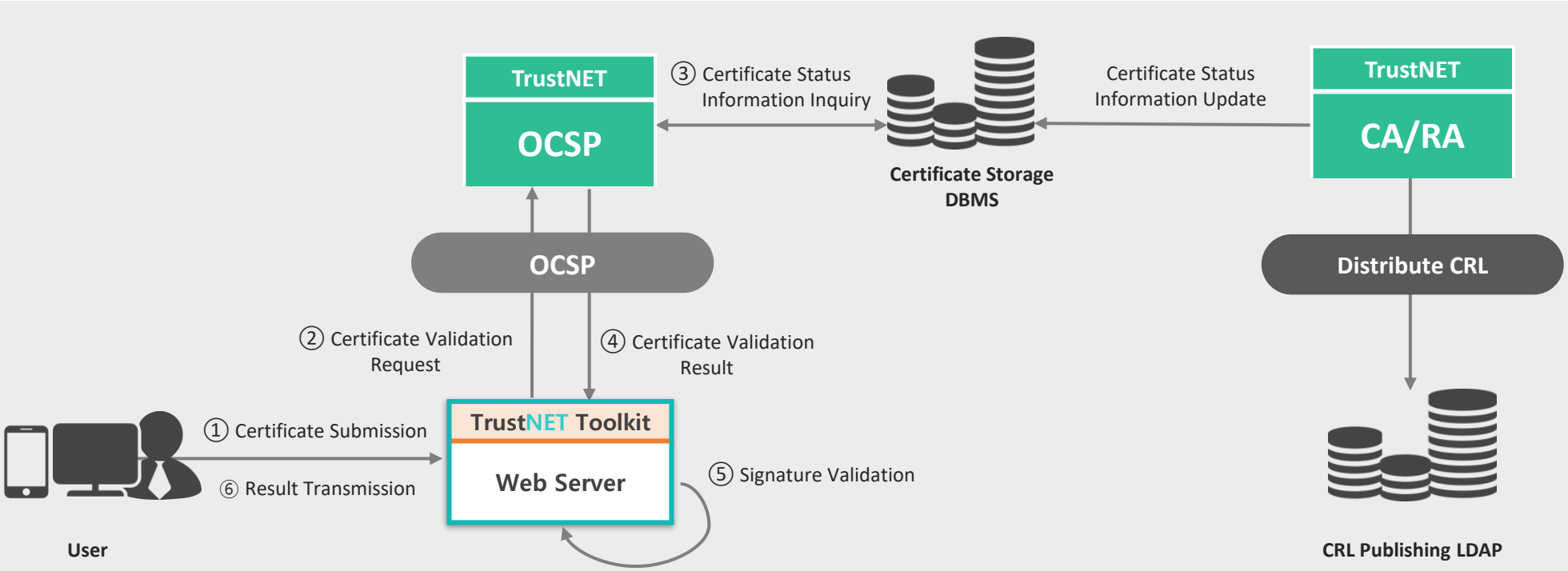


Certificate Issuance



Uses

- OCSP is a system that can validate certificates in real time without making requests for CRLs (Certificate Revocation Lists).
- It also provides functions to perform CRL validation by configuring LDAP upon requests of customers.



Key Functionalities

- A system that allows **real time validation** of certificate.

Real Time Certificate Status Verification

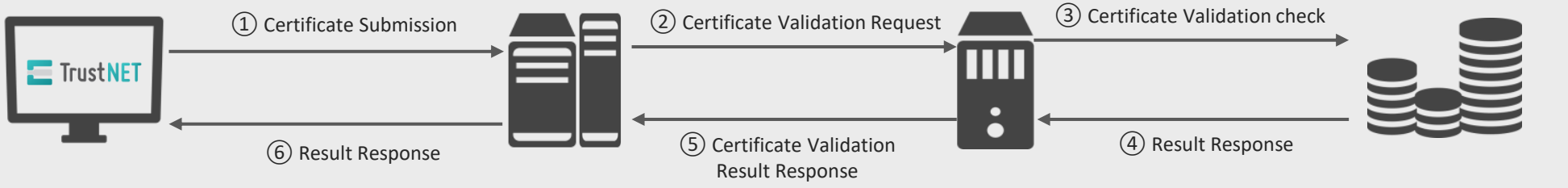
- ✓ A function that checks status of validation request certificate for the OCSP validation request.
- ✓ Information on date and time of revocation, as well as reason for the revocation of revoked certificate can be obtained.
- ✓ A function that records causes of certificate **validation** failures.

OCSP Information Validation Function

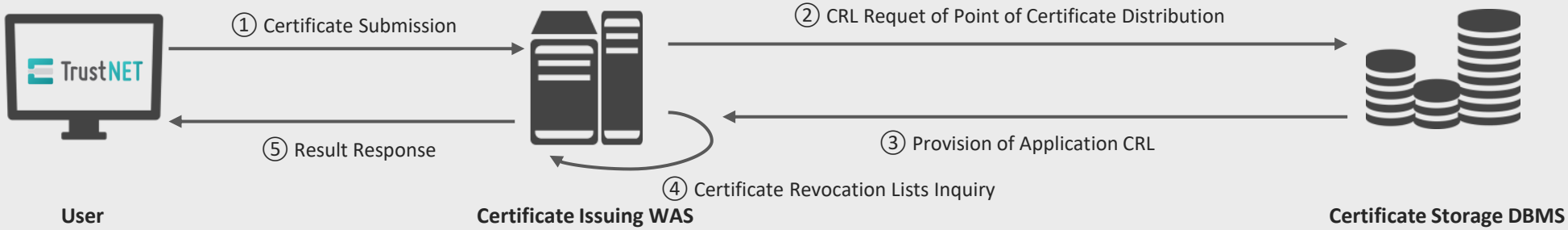
- ✓ A function to verify signatures for the OCSP request information itself.
- ✓ Validates whether or not the certificate is signed by the issuing authority by validating the OCSP requestor's certificate with public keys of the issuing authority.
- ✓ Checks whether or not the OCSP requestor's certificate is a certificate of a subordinate authority by comparing the certificate against the issuing authority's database information.
- ✓ A function that validates whether or not a certificate is one that is issued by an issuing authority by comparing issuer information of a certificate to be validated with an issued certificate of an issuing authority.

Certificate Validation Processes

OCSP Validation

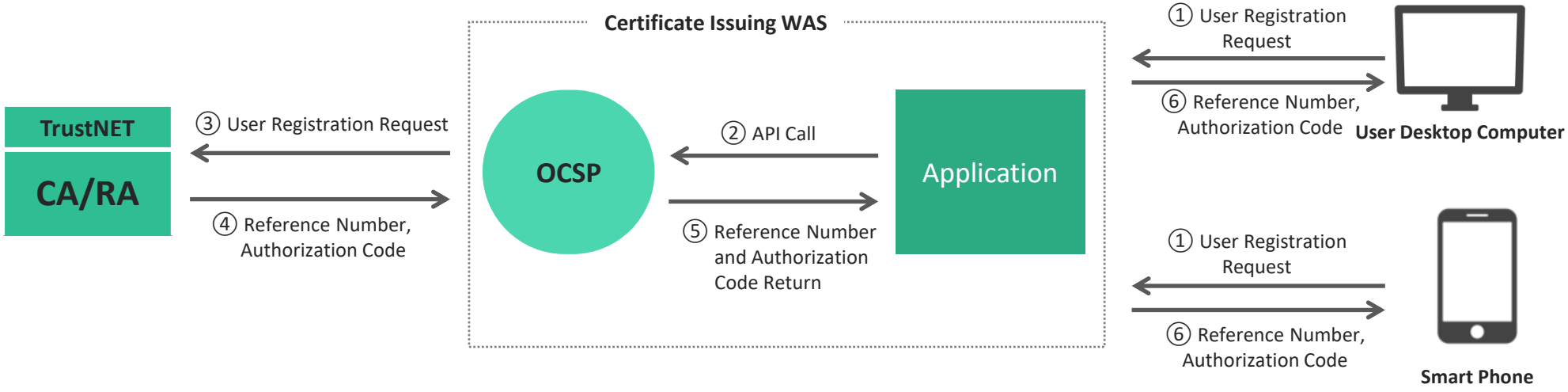


CRL Validation



LRAPI Usage

- API library form to perform the function of user registration, user deleting, and certificate revocation for issuing certificates to TrustNET CA/RA server. It also provides functions to perform CRL validation by configuring LDAP upon requests of product customers.
- An application program calls and uses corresponding API when creating a web screen for certificate issuance.



Key Functionalities

- **Provides API functionality** so that the TrustNET CA/RA server can perform necessary tasks for issuing certificates.

Real Time Certificate Status Verification

- ✓ Executes encrypted (https) communication with TrustNET CA/RA server.
- ✓ Makes user registration/re-registration and deletion requests to TrustNET CA/RA server.
- ✓ Makes certificate revocation request to TrustNET CA/RA server.
- ✓ Can be used in all environment that is JAVA 1.3 or higher.

OCSP Information Validation Function

- ✓ Executes encrypted (https) communication with TrustNET CA/RA server.
- ✓ Makes integrity validation requests to TrustNET CA Client for TrustNET CA/RA server response.
- ✓ Issues and re-issues certificates by using reference numbers and authorization codes which are the user registration result values.
- ✓ CA Client must be installed and operating on the client.
- ✓ Can be used in all environment that is JAVA 1.3 or higher.

Desktop Computer Client

ActiveX Client

- ✓ Activex type development and distribution
- ✓ Can only be used in Windows Internet Explorer
- ✓ After a private certificate issued, it is saved as a file in the desktop computer.
- ✓ Supports management function of issued private certificates.

TrustNET CA Desktop Computer Client

Issued certificates are stored in a form of files in local directories and are divided into two types, ActiveX and non plug-in methods, depending on web browser or operating system type.

ActiveX modules are installed in Windows – Internet Explorer environment, and non plug-in modules are installed and operated in all other browsers (Chrome, Safari, Opera, Firefox, and Edge) or other operating systems.
Functionalities supported by each module are the same.

ActiveX
Non Plug-in
2 Ways

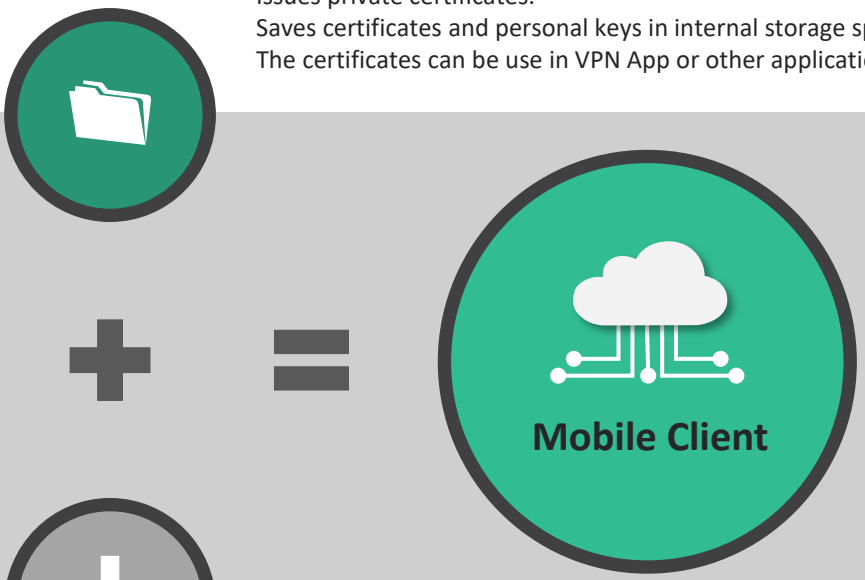
Non Plug-in Client

- ✓ Non plug-in type development and distribution
- ✓ Used in browsers, including Internet Explorer environments, and Windows and other OS (Linux, MacOS) environments.
- ✓ After a private certificate issued, it is saved as a file in the desktop computer.
- ✓ Supports management function of issued private certificates.

Mobile Client

Internal Storage Ver.

Issues private certificates.
Saves certificates and personal keys in internal storage space.
The certificates can be use in VPN App or other applications that require corresponding certificates.



TrustNET CA Mobile Client provides smartphone mobile apps with functionalities to issue and manage private certificates.

It is divided into two versions of internal storage and external storage in accordance with saving types of the issued certificates.

The internal storage version saves certificates issued from the client in an internal storage space that can be recognized by an operating system and allows other applications and operating systems to use the certificates

and the external storage version provides functionalities that allow uses of certificates by saving them in internal folders created within SD cards or application itself.

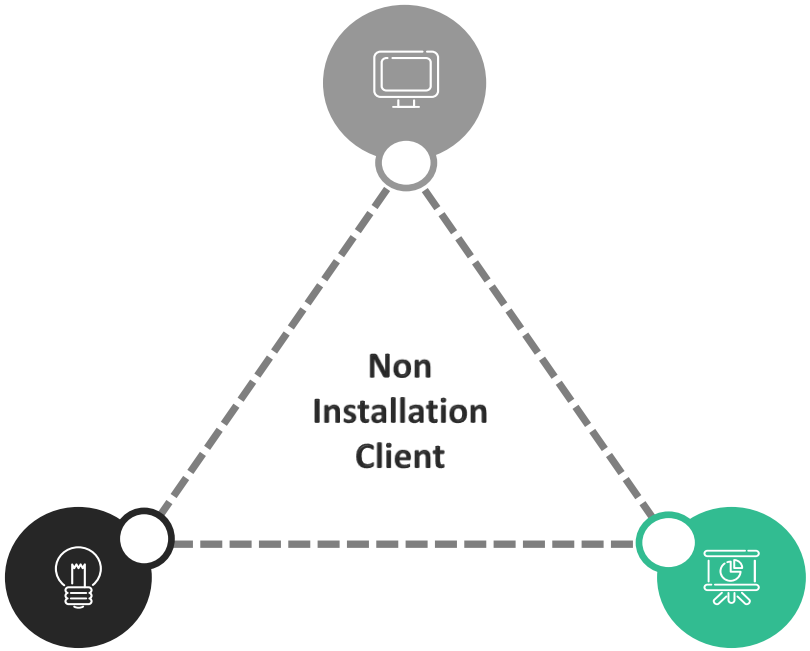
External Storage Ver.

Issues private certificates.
Saves certificates and personal keys in external storage area.
Changes personal key passwords.
Deletes keys/certificates.

Non Installation Client

- Performs client functions without native codes based on JavaScript and HTML5 technologies.

JavaScript codes that perform critical logics are obfuscated and encrypted in real-time.



Certificates and personal keys are saved in internal storage space within web browsers. Encrypts and stores in its own way.

Issues private certificates.

- TrustNET Non-Native CA-Client is a client that can be used equally in desktop computer and mobile environments without needs to install separate modules by using JavaScript and HTML5 Technologies.
- The issued certificate are used after being saved within web browsers.
- They are securely encrypted and stored, so there is no risk of being breached or misused.

Key Functionalities

- Provides API functionality so that the TrustNET CA/RA server can perform necessary tasks for issuing certificates.

Desktop Computer Client

- ✓ A function to validate data integrity with TrustNET CA/RA server.
- ✓ Functions to generate certificate generation request information that are necessary for issuing certificates and to save certificates/private keys.
- ✓ Functionalities of certificates/private keys deleting and private key passwords change.

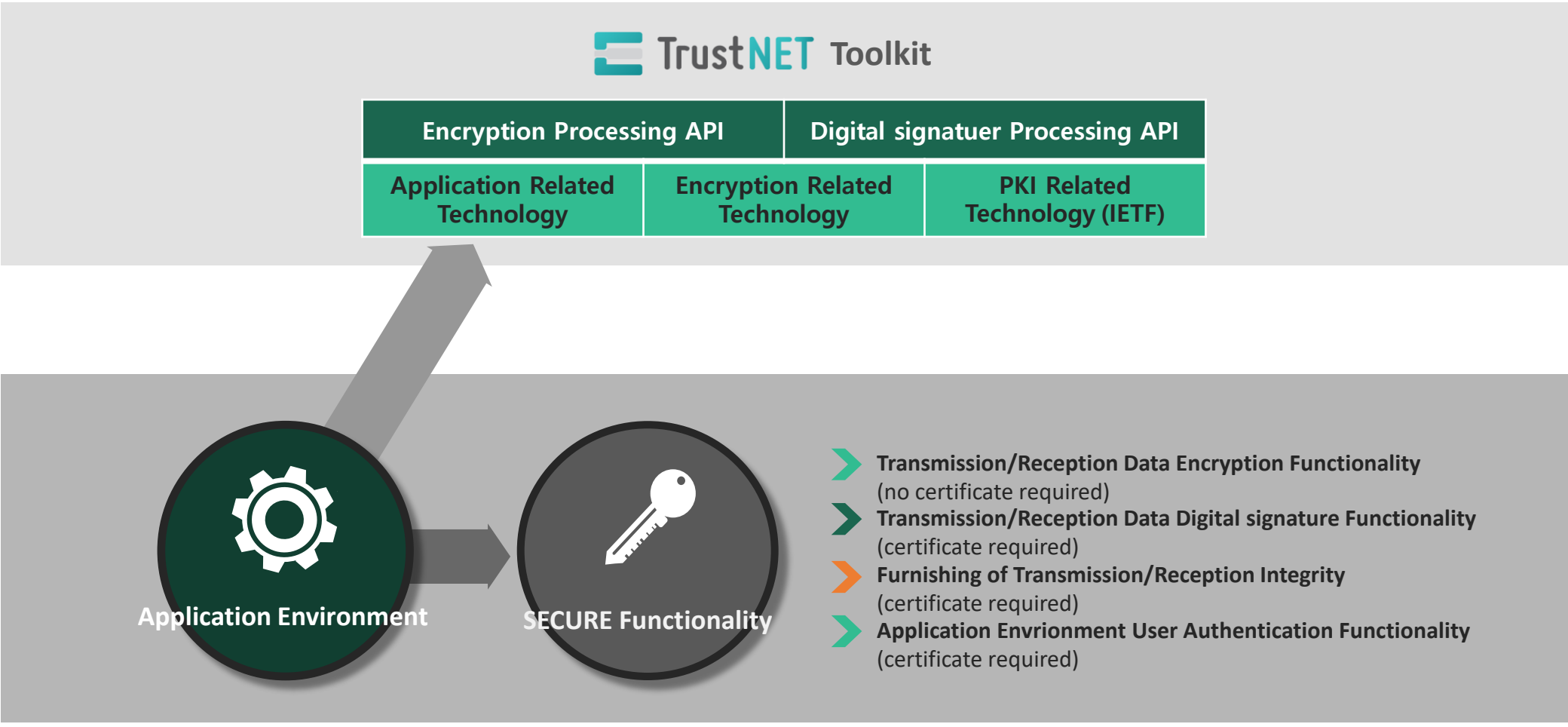
Mobile Client

- ✓ A function to validate data integrity with TrustNET CA/RA server.
- ✓ Functions to generate certificate generation request information that are necessary for issuing certificates and to save certificates/private keys.
- ✓ A function to save certificate sets in internal storage so that certificates can be used by VPN App or other applications.
- ✓ Functionalities of certificates/private keys deleting and private key passwords change when the certificates are saved in external storage.

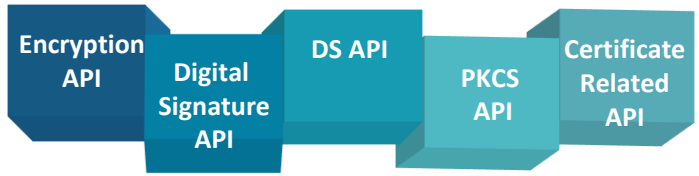
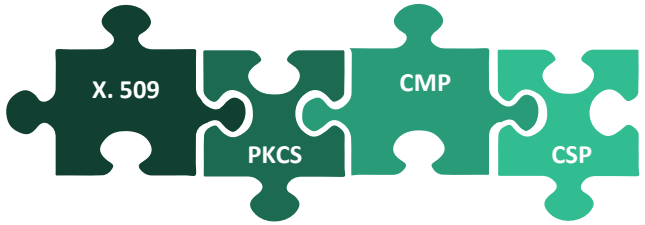
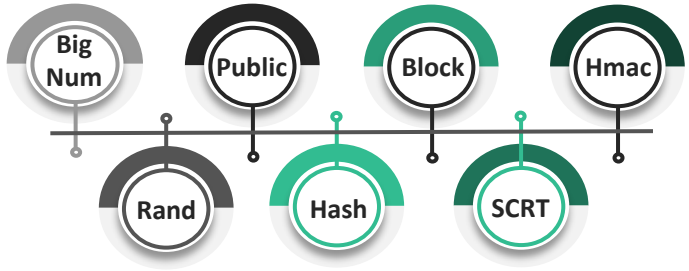
TrustNET Non-Native CA-Client

- ✓ A function to validate data integrity with TrustNET CA/RA server.
- ✓ Functions to generate certificate generation request information that are necessary for issuing certificates and to save certificates/private keys.
- ✓ Functionalities of certificates/private keys deleting and private key passwords change.
- ✓ Provides certificate inport and export functionalities.

Uses



Product Configuration

Classification	Linux	Windows
Toolkit (API)		■ Provides various encryption algorithm. (such as password, digital signature, hash, and random number generation)
Cert Library		■ Certificate (X509) validation and path inquiry functionalities. ■ Encrypted phrase processing functionality. ■ CA interface functionalities such as certificate request and revocation. ■ Encryption and decryption data encoding and decoding.
Crypto Library		■ Provides functionalities for encryption and decryption in server application programs. ■ Provides functionalities digital signature and validation in server application programs. ■ Supports registry and smart card interface.

Key Functionalities

Classification	Functions	Characteristics
Encryption and Decryption Functionalities	A functionality to encrypt and decrypt specific data by using symmetric key algorithms and public key algorithms.	▪ Encryption and decryption of both specific and random data are possible. ▪ Encryption and decryption functionalities for attached files.
Digital Signature Functionality	Functionalities for generating e-signature values for specific data and validating the signature values.	▪ A digital-signature functionality for attached files.
Encryption Key Generation And Key Exchange Functionalities	Provides functionalities for securely generating and exchanging (sharing) session keys (encrypted keys) used for encryption and decryption.	▪ Same methods as the key exchange functionality in SSL V3 and TLS V1.1.
Certificate I/O Functionality	Functionalities to back up and recover certificates and private keys to such media as registries, hard disks, smart cards, and USB ports.	▪ Provides various types of storage methods. (PKCS#12, PEM, DER Encoding and Decoding Functionalities) ▪ Management of PKCS#8 type secret keys.
PKCS#7 Message (Digital Envelope) Functionality	Supports encryption and decryption in RSA standard format, and digital signature generation and recovery functionalities.	▪ Provides scalability for secured mail, XML, and etc.
Certificate Validation Functionality	Provides functionalities for validating (path validation) for certificates issued by various certification agencies.	
Digital Signature Authentication Center Certificate Synchronization Functionality	Provides functionalities for integrating and interfacing intra-company private certificates and digital signature authentication certificates.	▪ Processes interfacing of certificates of the six major digital signature authentication centers and the digital signature validation centers.

Key Functionalities

Classification	Functions	Characteristics
Certificate Management Functionality	Provides functionalities for certificate issuance application, certificate revocation, certificate renewal, certificate password change, and certificate export and import by CMP[Note 1)] method which is the certificate issuance request protocol.	▪ Can be interfaced with all certification agencies (including the digital signature certification center) that conforms to CMP standards. ▪ Provides interfacing with various media such as smart cards, and USB ports.
Certificate GUI (Graphical User Interface) Functionality	Provides convenient screen interface functionality for selecting certificates and obtaining private keys for different storage media.	▪ Processes certificates of the digital signature certification center. ▪ Provides auto certificate selection functionality.
Provides clients in various forms.	Client products that can be used in various environments such as ActiveX, mobile, and non-native environments can be provided.	▪ Able to support almost any environment used in desktop computers or mobile environments. ▪ The non-native enabled client must be a web browser that supports HTML5 functionality.

Note 1) CMP: Certificate Management Protocol

Characteristics and Advantages

Provides customizable toolkit.

The toolkit can be easily reconstructed with a light load of functionalities that are desired by the customer since the toolkit structure consists of three layers.

Fully supports all relevant standards.

Supports domestic standard algorithm while fully complying with other public key algorithms and cryptographic standard.

Public Certificates Processing

Currently processes certificates for five different digital signature authentication centers. (Supports encryption and decryption, digital signature, interface, and smart cards.)

Secured Speed and Stability

Ensured safety and processing speed accomplished by a design that encompasses multi-thread environment
(about 0.03 seconds for K-digital signature/validation).

Supports Various Environments

Supports various structures and application environments
such as web to web browser, client to server, and server to server.

Various Establishment Experience

Experience in establishmentof various PKIs of product clients.
(Establishment of public and large scale certification centers and interfacing of various digital signature certification centers.)

Key Features of TrustNET

Applicable Standards

Classification	Technical Elements	Basis of the Standard	Descriptions
Certification	Certificate Specification	**X.509 v3, RFC3280**	The implemented technology adopts the RFC 2459 certificate specification, which is the Internet standard, to have the minimum functionality required for interfacing with other PKI areas.
	Certificate Revocation List Standard	**X.509 v2, RFC3280**	RFC 2459, the internet standard, is implemented as in the case of the certificates, and interfaces are established between the companies.
	Certificate Management Procedures	**RFC 2510, RFC 2511 draft-ietf-pkix-cmp-transport-protocols-01**	End-to-end interface is established by implementing RFC 2510, an Internet standard for certificate issuance, revocation, and renewal area of mutual messaging, and draft-ietf-pkix-cmp-transport-protocols-01, an Internet standard for the transmission of actual messages.
	Certificate Validation	**RFC 3280**	The route certification part for validation of certificates establishes interoperability for certificate validation during mutual certification by adapting an Internet standard RFC 2459.
	Certificate Distribution	**RFC 2559, RFC 2585, RFC2587**	"LDAP is supported through a standardized directory structure to distribute issued certificates, and RFC 2585 is applied for accessors through HTTP or FTP or other network protocols to promote distribution convenience."
Communication Protocol	CRMF	**RFC 2511**	Certificate Request
	CMP	**RFC 2510**	Internal messaging cross certification
	SSL	**RFC 6101**	Secure Socket Layer
	X.509 PKI-OCSP	**RFC 2560**	Online Certificate Status Protocol
	CMS	**RFC 2630**	Cryptographic Message Syntax
	LDAP	**LDAP**	Communication LDAP
	SQL	**SQL**	Internal Communication
	HTML5	**World Wide Web Consortium**	HTML5

Classification	Technical Elements	Basis of the Standard	Descriptions
Technologies	RSA Encryption	**PKCS #1**	Supports the industry standards related to data encryption and digital signature generation that use RSA algorithms.
	Password Based Data Encryption	**PKCS #5 v2.0**	Supports PBES2 by using PBKDF2, a key-derived function for password-based encryption, and a block password key that is longer than 8 bytes.
	Certificate Extension Structure	**PKCS #6**	As an industry standard to support extended certificate structures, attachment functionality is supported in signature messages, and etc.
	Digital signature and Encrypted Data	**PKCS #7, RFC 2630, RFC 2634**	Supports standards of electronic documents such as digital signature messages, encrypted messages, and digest messages, by using a public key encryption method.
	Private Key Structure	**PKCS #8**	Supports message types and encrypted private key standards for storage and migration of private keys.
	Certificate Request Format	**PKCS #10, RFC 2511**	As a standard structure of certificate issuance request message, RFC 2511, of which the POP and structure are improved in comparison with PKCS#10, is additionally supported.
	User Information Exchange	**PKCS #12**	As a standard for migration, storage, and transmission format of user private keys, certificates, and other security data, PKCS#12 is supported for a mean of certificate migration in desktop computers.

Products			Supported Environment
Server	TrustNET CA/RA TrustNET OCSP Administrator Web Console		Supports all operating system environments that are JAVA 1.7 or higher. DBMS: Supports Oracle, MS-SQL, MySQL, MariaDB, and TiberoDB (Other DBMS can be supported by porting.)
Applications	TrustNET LRAPI, Web Gateway	ActiveX Client	Supports all operating system environments that are JAVA 1.3 or higher.
Client	TrustNET CA-Client For Desktop Computer	ActiveX Client	Browser : Internet Explorer OS : Windows (except for Windows 8.1 tile UI)
		Multi client	Browser : Chrome, Safari, Opera, Firefox, Edge OS : Windows, Mac, Linux
	TrustNET CA-Client For Mobile	iOS	iOS 6.0 or higher
		Android	Android 4.0 (Ice Cream Sandwich) or higher (Per Internal Storage Version)
	TrustNET JavaScript CA-Client		All web browsers that support HTML5.

Key Clients

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	