

Evaluation results and vulnerability analysis in USB Storage Drive Management System

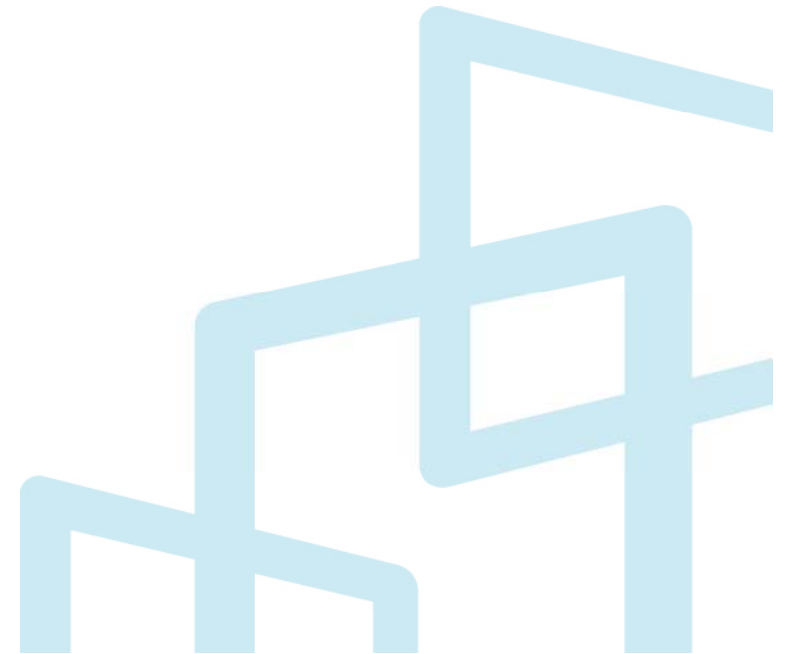
2009. 9. 24
KISA
HyeonMee Pak

10 ICC



Index

1. **USB Storage Drive**
2. **USB Storage Drive Management System**
3. **Results of Evaluation**



1. USB Storage Drive

1. USB Storage Drive



1. USB Storage Drive?

- a. USB drives or thumb drives or flash drives



2. Benefits of USB Storage Drive(USB)

- a. Can store large amounts of data
- b. easy to use
- c. Inexpensive
- d. quick at transmission speed

2. Threat of USB Storage Drive

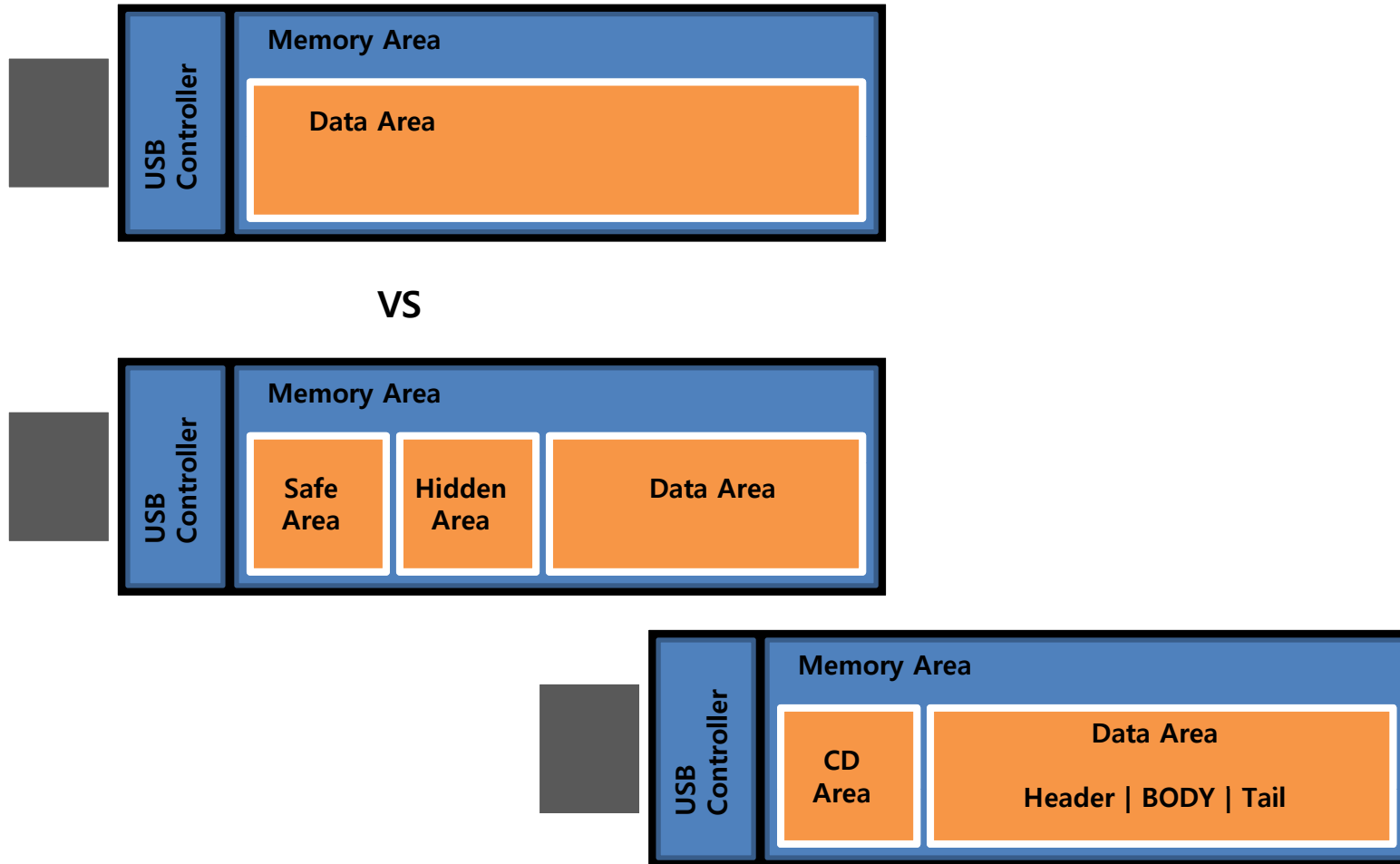


1. Threat of USB Storage Drive

- a. Spread of Virus
- b. Deletion of Data
- c. Loss of Data
- d. Loss of Device
- e. Loss of confidentiality

3. Secure USB Storage Drive

1. Structure of Secure USB Storage Drive



2. USB Storage Drive Management System

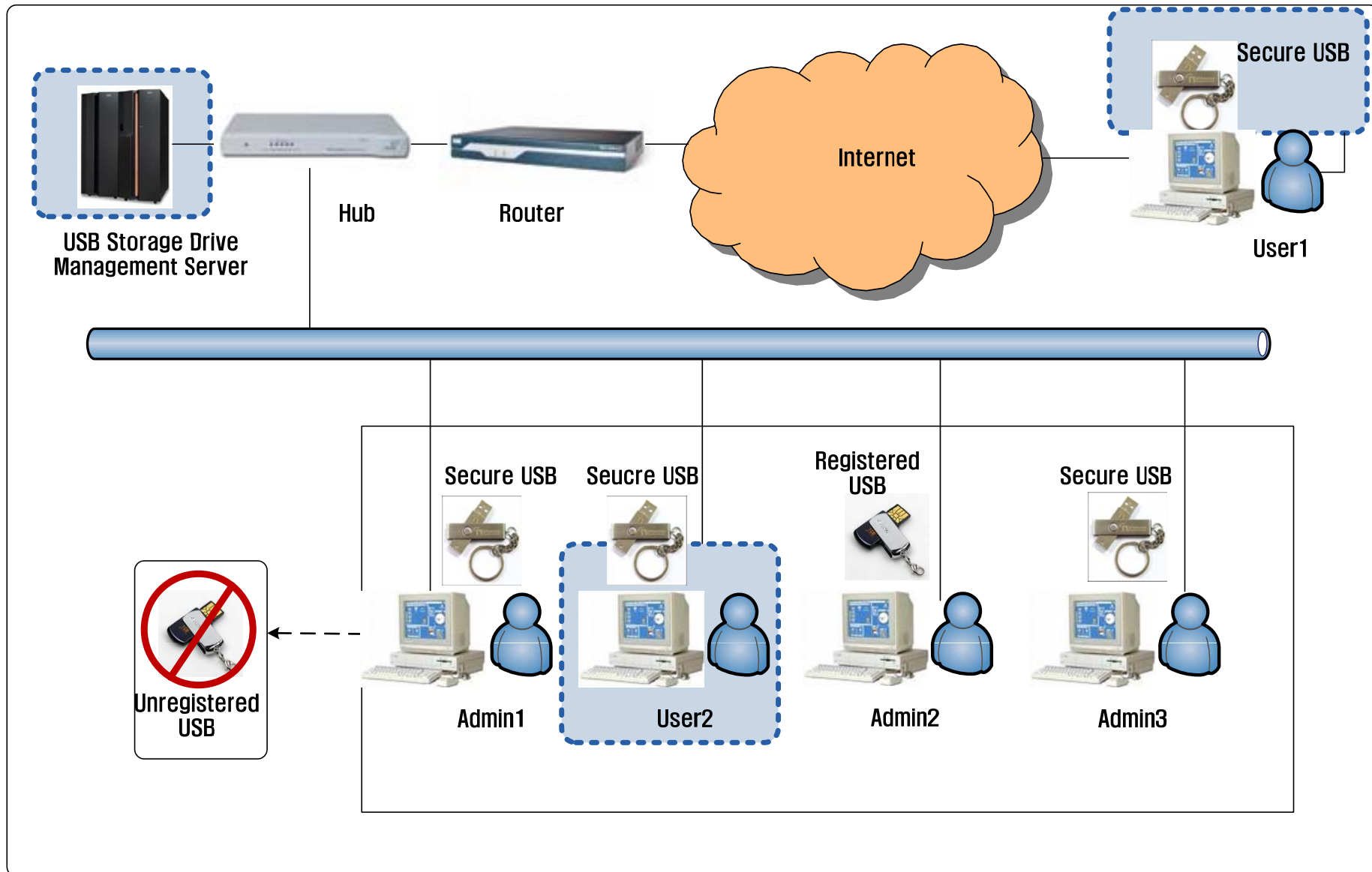
1. USB Storage Drive Management System



1. USB Storage Drive Management System?

- a. Can control USB Storage device permissions
- b. Offers control over a broad range of host devices and ports

2. Concept of operations



3. TSF of USB Storage Drive Management System



1. Management Server

- a. Identification and Authentication
- b. Audit data generation, review
- c. Management of Access control policy
- d. ...



2. Client Agent

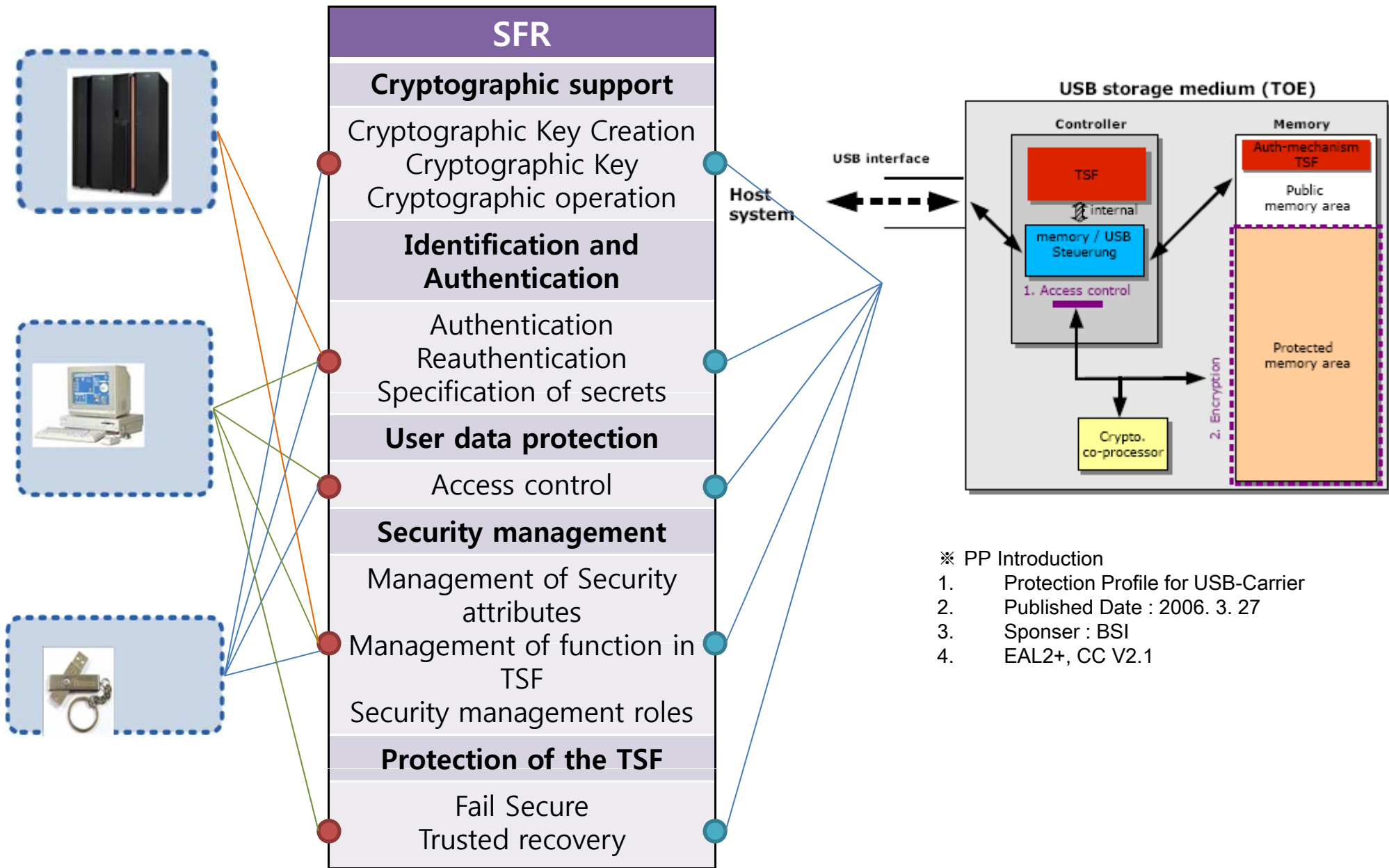
- a. Identification and Authentication
- b. Access control function
- c. Fail Secure
- d. Recovery
- e. ...



3. USB Agent

- a. Identification and Authentication
- b. USB Access control
- c. secure deletion operation
- d. encryption/decryption of stored data
- e. ...

3. TSF of Management System vs. PP for USB-Carrier



※ PP Introduction

1. Protection Profile for USB-Carrier
2. Published Date : 2006. 3. 27
3. Sponser : BSI
4. EAL2+, CC V2.1

3. Evaluation Results

1. General Results



1. **Situation – Why certification need?**
 - a. **Secure USB products need CC for National Agency**
 - b. **“Guideline of Security Management for auxiliary storage Device” – NIS, Jan 2007**

2. Evaluation Results

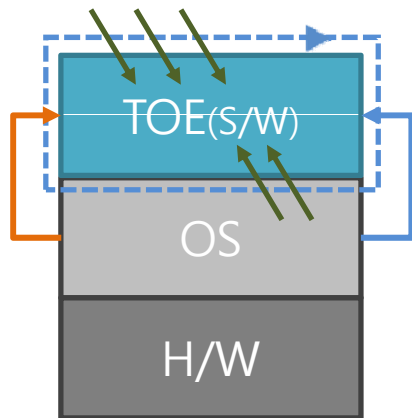
	Passed	In Evaluating	Ready
Number	3	3	2
Level	EAL2	EAL2	EAL2
Scheme	NIS(KECS)	NIS(KECS)	NIS(KECS)
Scope of Activity	Domestic	Domestic	Domestic
CC	V3.1 r2	V3.1 r2	V3.1 r2

2. Vulnerability Analysis (1/2)

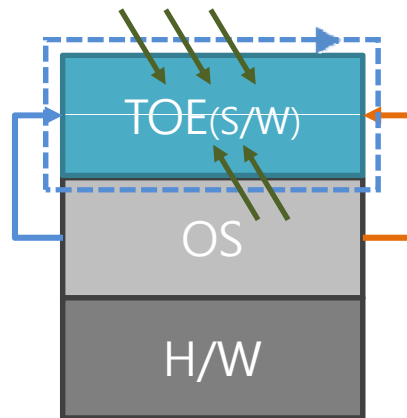


1. Goal of Vulnerability Analysis

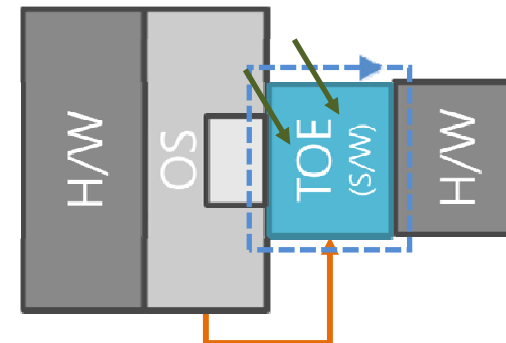
- domain isolation
- self-protection
- non-bypassability



Server



Client



Secure USB

2. Vulnerability Analysis (2/2)



2. Extract Vulnerabilities

	Vulnerability
1	Unload TOE's Driver
2	Terminate Process
3	Be Powerless TOE's Service
4	Modify Registries
5	Forge TOE's Files
6	Difference between Loading Times at booting
7	Expose data using Virtual Machine
8	Destroy TOE and Expose date On Safe Mode

Thank You !!!

Korea Internet & Security Agency