KECS-CR-17-47

KT Secure Vault V1.0

Certification Report

Certification No.: KECS-CISS-0811-2017

2017. 7.

IT Security Certification Center

History of Creation and Revision			
No.	Date	Revised Pages	Description
00	2017.7.26	-	Certification report for KT Secure Vault V1.0 - First documentation

This document is the certification report for KT Secure Vault V1.0 of KT Corp.

The Certification Body

IT Security Certification Center

The Evaluation Facility

Korea System Assurance (KOSYAS)

Table of Contents

1. Executive Summary

This report describes the evaluation result drawn by the certification body on the results of the EAL1 evaluation of KT Secure Vault V1.0 developed by KT Corp with reference to the Common Criteria for Information Technology Security Evaluation (hereinafter “CC”) [1]. It describes the evaluation result and its soundness as well as conformity.

The Target of Evaluation (“TOE” hereinafter) is an information security product that offers encryption/decryption and Access Control Functions for securing files stored in the user PC. The TOE offers encryption/decryption and Access Control Functions to secure files saved on a user PC

TOE consists of KT Secure Vault Client (hereinafter “KClient”) and KT Secure Vault Server (hereinafter “KServer”). KClient is installed on the group user and group administrator’s PCs, and the KServer is installed in the server. TOE communicates between components through the IPv4 network to provide security functions.

The major security features offered by TOE are as follows

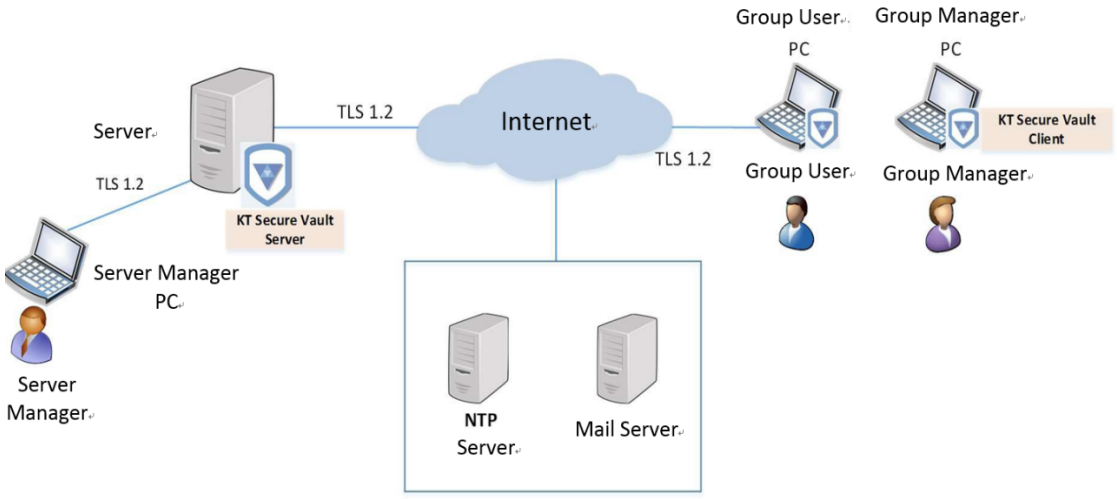
- User file encryption and decryption: Perform file extension-based encryption and decryption
- Volt file access control: Authority level and team id based access control

The evaluation of the TOE has been carried out by Korea System Assurance (KOSYAS) and completed on July 4th, 2017. This report grounds on the evaluation technical report (ETR) [3] that KOSYAS had submitted and the Security Target (ST) [4].

The ST has no conformance claim to the Protection Profile (PP). All Security Assurance Requirements (SARs) in the ST are based only upon assurance component in CC Part 3, and the TOE satisfies the SARs of Evaluation Assurance Level EAL1. Therefore the ST and the resulting TOE is CC Part 3 conformant. The Security Functional Requirements (SFRs) are based upon functional components in CC Part 2 and one SFR (FCS_RBG.1) is newly defined in the chapter of Extended Component of ST. The TOE satisfies the SFRs in the ST. Therefore the ST and the resulting TOE is CC Part 2 conformant.

[Figure 1] shows the operational environment of the TOE. The server administrator only has access from the allowed IP address by using a web browser from the local network where the KT Secure Vault Server is located. HTTPS protocols are used for communication between the server administrator's PC and the KT Secure Vault Server in order to secure any transmitted data. Moreover, communication must operate in a TLS 1.2 communication operating environment to ensure the confidentiality and integrity of data between TOE components.

Mail servers are used when sending mail to the group administrator or group users, and the NTP server is used to synchronize the time in the KT Secure Vault Server. TOE is operated by communicating with components in the ipv4 wired internet network environment.



[Figure 1] TOE Operational Environment

Hardware and software requirements for operating KT Secure Vault Server and KT Secure Vault Client are shown in [Table 1] and [Table 2].

TOE Components	Category	Minimum Requirements
KServer (KT Secure Vault Server)	CPU	Intel® Core™ i7, 4 Core 2.5 Ghz or higher
	RAM	2 GB or higher
	HDD	2 TB or higher
	NIC	Ethernet 10/100/1000 * 1 port
	OS	CentOS 7.3 (Kernel 3.10.0, 64 bit)

TOE Components	Category	Minimum Requirements
	SW	Apache-tomcat 8.5.15 httpd 2.4.25 jdk-8u131 PostgreSQL 9.6.3
	Library	glibc 2.17 openssl 1.0.2l

[Table 1] Non-TOE hardware and software of the KT Secure Vault Server

TOE Components	Category	Minimum requirements
KT Secure Vault Client	CPU	Intel® Core2™ duo 2.2 GHz or higher
	RAM	1 GB or higher
	HDD	500 GB or higher
	NIC	Ethernet 10/100/1000 * 1 port
	OS	Windows 7 Professional (64bit)
	SW	Microsoft Visual C++ 2013 Redistributable (x86) 12.0.30501

[Table 2] Non-TOE hardware and software of the KT Secure Vault Client

Server administrator uses the PC that can operate web browser to use the security management. The minimum requirements for Server administrator PC are shown in [Table 3].

Category	Minimum requirements
CPU	Intel® Core2™ duo 2.2 GHz or higher
RAM	1 GB or higher
NIC	Ethernet 10/100/1000 * 1 port
HDD	500 GB or higher
OS	Windows 7 Professional (64bit)
SW	Firefox 54.0

[Table 3] Non-TOE Hardware and Software of the KT Secure Vault Client

[Table 4] shows external IT entity that is interacted for TOE operation.

Category	Contents
Mail Server(SMTP)	Server for sending e-mails
NTP Server	Server for time synchronization

[Table 4] External IT entities

Certification Validity: The certificate is not an endorsement of the IT product by the government of Republic of Korea or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by the government of Republic of Korea or by any other organization recognizes or gives effect to the certificate, is either expressed or implied.

2. Identification

The TOE reference is identified as follows.

TOE	KT Secure Vault V1.0
Version	V1.0.022
TOE Components	KT Secure Vault Server V1.0.B-022.017 (KT_Secure_Vault_Server_V1.0.B-022.017.tar) KT Secure Vault Client V1.0.B-017.019 (KT Secure Vault Client V1.0.B-017.019.exe)
Guidance Documents	KT Secure Vault V1.0 Users Guidance V1.0.009 (KT Secure Vault V1.0-USR-V1.0.009.pdf) KT Secure Vault V1.0 Preparation V1.0.009 (KT Secure Vault V1.0-PRE-V1.0.009.pdf)

[Table 5] TOE identification

[Table 6] summarizes additional information for scheme, developer, sponsor, evaluation, facility, certification body, etc.

Scheme	Korea Evaluation and Certification Guidelines for IT Security (2016.06.27) Korea Evaluation and Certification Regulation for IT Security (2017.06.26)
TOE	KT Secure Vault V1.0
Common Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012
EAL	EAL1
Protection Profile	ST does not claim conformance to PP
Developer	KT Corp.
Sponsor	KT Corp.
Evaluation Facility	Korea System Assurance (KOSYAS)
Completion Date of Evaluation	July 4th, 2017
Certification Body	IT Security Certification Center

[Table 6] Additional identification information

3. Security Policy

The TOE complies security policies defined in the ST [4] by security objectives and security requirements. The TOE implements policies pertaining to the following security functional classes :

- Security Audit
- Cryptographic Support
- User Data Protection
- Identification and Authentication
- Security Management
- TOE Access

Complete details of the security functional requirements (SFRs) can be found in the Security Target (ST) [4].

4. Assumptions and Clarification of Scope

There are no Assumptions in the Security Problem Definition in the ST. The scope of this evaluation is limited to the functionality and assurance covered in the Security Target. The TOE includes the KT Secure Vault Server that is distributed through a CD and the KT Secure Vault Client that is installed after being downloaded rom the KT Secure Vault Server. It also includes the KT Secure Vault V1.0 Preparation Procedures and the KT Secure Vault V1.0 User Manual that are distributed to end users in the form of a manual so that the TOE can be safely installed and operated.

5. Architectural Information

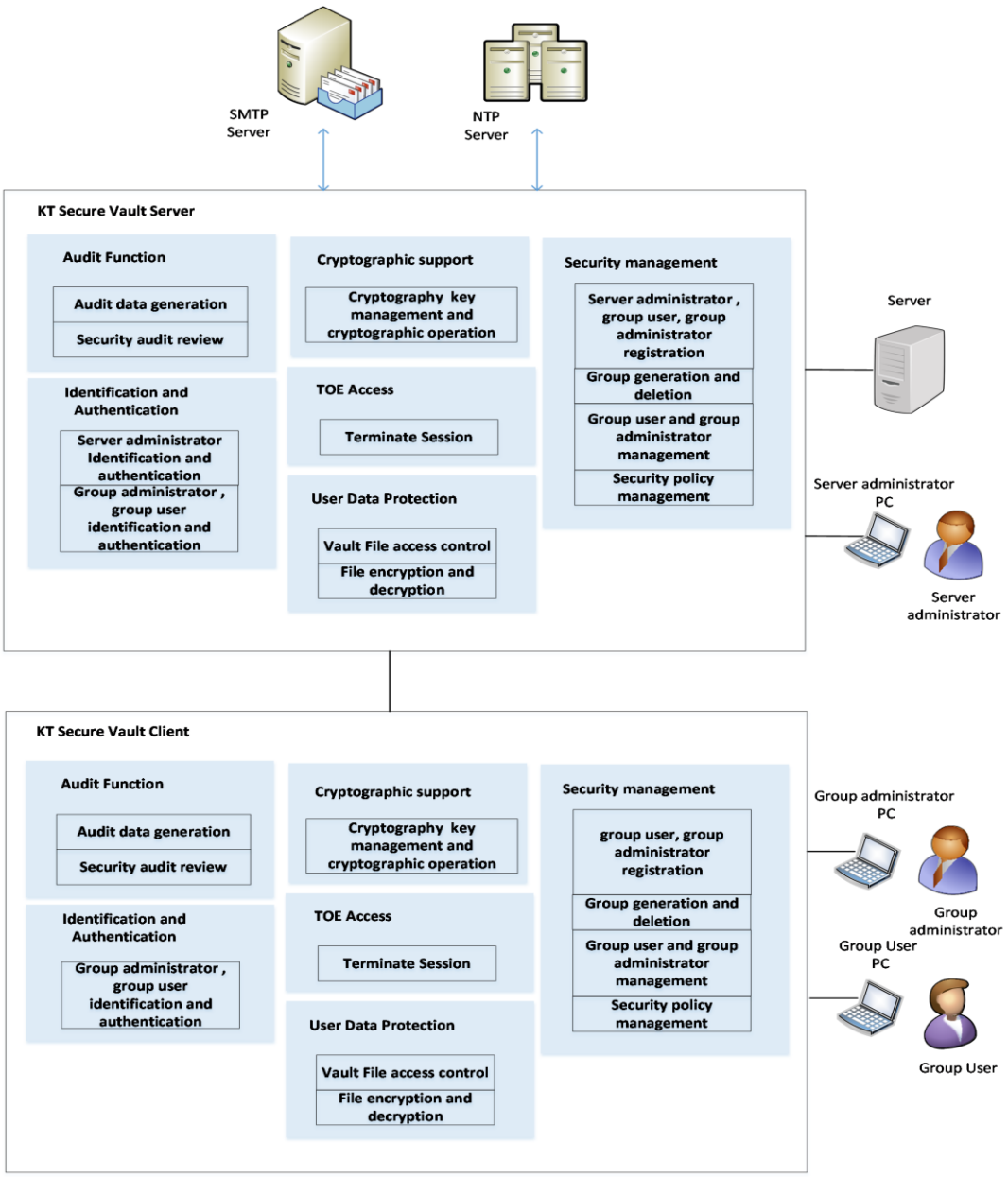
The physical scope of the TOE consists of KT Secure Vault Server and KT Secure Vault Client, which are distributed as software, and manuals such as user Guidance and preparation procedure documents.

Category	Identification	Type
SW	KT Secure Vault Server V1.0.B-022.017 (file: KT_Secure_Vault_Server_V1.0.B-022.017.tar)	SW (CD)
	KT Secure Vault Client V1.0.B-017.019 (file: KT Secure Vault Client V1.0.B-017.019.exe)	SW (Download)

Guidance Documents	KT Secure Vault V1.0 User Guidance V1.0.009 (file: KT Secure Vault V1.0-USR-V1.0.009.pdf)	PDF(CD)
	KT Secure Vault V1.0 Preparation V1.0.009 (file: KT Secure Vault V1.0-PRE-V1.0.009.pdf)	

[Table 7] Physical scope and boundary

Logical scope and boundary of TOE is shown in [Figure 2].



[Figure 2] TOE Logical scope and boundary

6. Documentation

The following documentation is evaluated and provided with the TOE by the developer to the customer.

Identifier	Version	Date
KT Secure Vault V1.0 User Guidance V1.0.009 (KT Secure Vault V1.0-USR-V1.0.009.pdf)	V1.0.009	June 9th, 2017
KT Secure Vault V1.0 Preparation V1.0.009 (KT Secure Vault V1.0-PRE-V1.0.009.pdf)	V1.0.009	June 9th, 2017

[Table 8] Documentation

7. TOE Testing

The evaluator performed independent testing listed in ETR [3], based upon test cases devised by the evaluator. The evaluator took a testing approach based on the security services provided by each TOE components based on the operational environment of the TOE. Each test case includes the following information:

- Test no. and conductor: Identifier of each test case and its conductor
- Test Purpose: Includes the security functions and modules to be tested
- Test Configuration: Details about the test configuration
- Test Procedure detail: Detailed procedures for testing each security function
- Expected result: Result expected from testing
- Actual result: Result obtained by performing testing
- Test result compared to the expected result: Comparison between the expected and actual result

The evaluator set up the test configuration and testing environment consistent with the ST [4]. In addition, the evaluator conducted penetration testing based upon test cases devised by the evaluator resulting from the independent search for potential vulnerabilities. These tests cover weakness analysis of privilege check of executable code, bypassing security functionality, invalid inputs for interfaces, vulnerability scanning using commercial tools, disclosure of secrets, and so on. No exploitable vulnerabilities by attackers possessing basic attack potential were found from penetration testing. The evaluator confirmed that all the actual testing results correspond to the expected testing results. The evaluator testing effort, the testing approach, configuration, depth, and results are summarized in the ETR [3].

8. Evaluated Configuration

The TOE is software and firmware consisting of the following components::

- KT Secure Vault Server V1.0.B-022.017
- KT Secure Vault Client V1.0.B-017.019

The Administrator can identify the complete TOE reference after installation using the product's Info check menu. And the guidance documents listed in this report chapter 6 were evaluated with the TOE.

9. Results of the Evaluation

The evaluation facility provided the evaluation result in the ETR [3] which references Single Evaluation Reports for each assurance requirement and Observation Reports.
The evaluation result was based on the CC [1] and CEM [2].
As a result of the evaluation, the verdict PASS is assigned to all assurance components of EAL1.

9.1 Security Target Evaluation (ASE)

The ST Introduction correctly identifies the ST and the TOE, and describes the TOE in a narrative way at three levels of abstraction (TOE reference, TOE overview and TOE description), and these three descriptions are consistent with each other. Therefore the verdict PASS is assigned to ASE_INT.1.
The Conformance Claim properly describes how the ST and the TOE conform to the CC and how the ST conforms to PPs and packages. Therefore the verdict PASS is assigned to ASE_CCL.1.
The Security Objectives for the operational environment are clearly defined. Therefore the verdict PASS is assigned to ASE_OBJ.1.
Extended Components have been clearly and unambiguously defined, and whether they are necessary, i.e. they may not be clearly expressed using existing CC Part 2 or CC Part 3 components. Therefore the verdict PASS is assigned to ASE_ECD.1.
The SFRs and SARs are clear, unambiguous and well-defined and whether they are internally consistent. Therefore the verdict PASS is assigned to ASE_REQ.1.
The TOE Summary Specification addresses all SFRs, and it is consistent with other

narrative descriptions of the TOE. Therefore the verdict PASS is assigned to ASE_TSS.1.

Thus, the ST is sound and internally consistent, and suitable to be used as the basis for the TOE evaluation.

The verdict PASS is assigned to the assurance class ASE.

9.2 Life Cycle Support Evaluation (ALC)

The developer has clearly identified the TOE. Therefore the verdict PASS is assigned to ALC_CMC.1.

The developer performs configuration management on the TOE and the evaluation evidence. Therefore the verdict PASS is assigned to ALC_CMS.1.

Thus, the security procedures that the developer uses during the development and maintenance of the TOE are adequate. These procedures include life-cycle model used by developer, the configuration management, the security measures used throughout TOE development, and the delivery activity.

The verdict PASS is assigned to the assurance class ALC.

9.3 Guidance Documents Evaluation (AGD)

The procedures and steps for the secure preparation of the TOE have been documented and result in a secure configuration. Therefore the verdict PASS is assigned to AGD_PRE.1.

The operational user guidance describes for each user role the security functionality and interfaces provided by the TSF, provides instructions and guidelines for the secure use of the TOE, addresses secure procedures for all modes of operation, facilitates prevention and detection of insecure TOE states, or it is misleading or unreasonable. Therefore the verdict PASS is assigned to AGD_OPE.1.

Thus, the guidance documents are adequately describing the user can handle the TOE in a secure manner. The guidance documents take into account the various types of users (e.g. those who accept, install, administrate or operate the TOE) whose incorrect actions could adversely affect the security of the TOE or of their own data.

The verdict PASS is assigned to the assurance class AGD.

9.4 Development Evaluation (ADV)

The developer has provided a high-level description of at least the SFR-enforcing TSFIs, in terms of descriptions of their parameters. Therefore the verdict PASS is

assigned to ADV_FSP.1.

The verdict PASS is assigned to the assurance class ADV.

9.5 Test Evaluation (ATE)

By independently testing a subset of the TSFI, the evaluator confirmed that the TOE behaves as specified in the functional specification and guidance documentation. Therefore the verdict PASS is assigned to ATE_IND.1.

Thus, the TOE behaves as described in the ST and as specified in the evaluation evidence (described in the ADV class).

The verdict PASS is assigned to the assurance class ATE.

9.6 Vulnerability Assessment (AVA)

By penetrating testing, the evaluator confirmed that there are no exploitable vulnerabilities by attackers possessing basic attack potential in the operational environment of the TOE. Therefore the verdict PASS is assigned to AVA_VAN.1.

Thus, potential vulnerabilities identified, during the evaluation of the development and anticipated operation of the TOE or by other methods (e.g. by flaw hypotheses), don't allow attackers possessing basic attack potential to violate the SFRs.

The verdict PASS is assigned to the assurance class AVA.

9.7 Evaluation Result Summary

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
ASE	ASE_INT.1	ASE_INT.1.1E	PASS	PASS	PASS
		ASE_INT.1.2E	PASS		
	ASE_CCL.1	ASE_CCL.1.1E	PASS	PASS	
	ASE_OBJ.1	ASE_OBJ.1.1E	PASS	PASS	
	ASE_ECD.1	ASE_ECD.1.1E	PASS	PASS	
		ASE_ECD.1.2E	PASS		
	ASE_REQ.1	ASE_REQ.1.1E	PASS	PASS	
	ASE_TSS.1	ASE_TSS.1.1E	PASS	PASS	
		ASE_TSS.1.2E	PASS		
ALC	ALC_CMS.1	ALC_CMS.1.1E	PASS	PASS	PASS
	ALC_CMC.1	ALC_CMC.1.1E	PASS	PASS	
AGD	AGD_PRE.1	AGD_PRE.1.1E	PASS	PASS	PASS

Assurance Class	Assurance Component	Evaluator Action Elements	Verdict		
			Evaluator Action Elements	Assurance Component	Assurance Class
		AGD_PRE.1.2E	PASS		
	AGD_OPE.1	AGD_OPE.1.1E	PASS	PASS	
ADV	ADV_FSP.1	ADV_FSP.1.1E	PASS	PASS	PASS
		ADV_FSP.1.2E	PASS		
ATE	ATE_IND.1	ATE_IND.1.1E	PASS	PASS	PASS
		ATE_IND.1.2E	PASS		
AVA	AVA_VAN.1	AVA_VAN.1.1E	PASS	PASS	PASS
		AVA_VAN.1.2E	PASS		
		AVA_VAN.1.3E	PASS		

[Table 8] Evaluation Result Summary

10. Recommendations

The TOE security functionality can be ensured only in the evaluated TOE operational environment with the evaluated TOE configuration, thus the TOE shall be operated by complying with the followings:

- The administrator should periodically check the free space of the audit data storage in preparation for the loss of the audit records, and perform backups of the audit records so that the audit records are not exhausted.
- The KT Secure Vault Server must be installed and operated in a physically secure environment that is accessible only to authorized administrators and should not allow remote administration from outside.
- If the group administrator's group key is lost, users may not be able to decrypt the encrypted file stored on the user's PC, so administrator has to be careful with key management

11. Security Target

KT Secure Vault V1.0 Security Target v1.0.023 [4] is included in this report for reference.

12. Acronyms and Glossary

CC	Common Criteria
EAL	Evaluation Assurance Level
PP	Protection Profile
SAR	Security Assurance Requirement
SFR	Security Functional Requirement
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functionality
TSFI	TSF Interface
ETR	Evaluation Technical Report
Authorized Administrator	A user who was authenticated by the server administrator or group administrator and can perform security management functions
Server administrator	Adds, views, revises, deletes group members and group administrators through the server management UI
Group administrator	A group user who uses the administrator functions of the KT Secure Vault Client in the TOE client area. Adds, views users in the group, views, revises information, deletes, etc. within the group. They manage the group user's permissions and are able to set target files for encryption. The group administrator can use all the functions available to group users, hence all explanations regarding group users are applicable to the group administrator without requiring further descriptions
Group user	A user who uses the KT Secure Vault Client in the TOE client area
Authentication Key	A unique symmetric key that is generated for each group user, and used to log by sharing with the server
Group key	A unique group key that is generated when the group is

	registered as a member. It is shared with all users in the group and triggers an encryption key from the encryption key seed that was received from the server
Server key	A unique group key that is generated when a group becomes registered as a member. The identifier is decrypted to verify the file's permissions, the encryption key seed is generated according to the permissions, then sent to the client
PIN	When a group user inputs the pin with their ID upon logging in, a unique authentication key is generated to trigger the authentication process
Vault file	The final file type that is created through the TOE from the original file according to an encryption request. Identifiers are included after the original file is encrypted

13. Bibliography

The certification body has used following documents to produce this report.

[1] Common Criteria for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-001 ~ CCMB-2012-09-003, September 2012

[2] Common Methodology for Information Technology Security Evaluation, Version 3.1 Revision 4, CCMB-2012-09-004, September 2012

[3] KT Secure Vault V1.0 Evaluation Technical Report(ETR) V3.00, July 11, 2017

[4] KT Secure Vault V1.0 Security Target V1.0.023, June 27, 2017