Australian Government
Department of Defence

Australasian Information Security Evaluation Program

Certification Report

Certificate Number: 2009/62

26/10/09

Version 1.0

Amendment Record

Version	Date	Description
1.0	26/10/2009	Public release.

Executive Summary

1 The Target of Evaluation (TOE) is the Senetas Encryptor Range comprising CypherNET Ethernet Encryptor, CypherNET Fibre Channel Encryptor, CypherStream Ethernet Encryptor and CypherManager. It is a product range that is designed to encrypt data in transit at up to 10 Gbps for CypherNET and 10 Mbps for CypherStream.

2 This report describes the findings of the IT security evaluation of the TOE to the Common Criteria (CC) evaluation assurance level EAL4 augmented with ALC_FLR.2 (Flaw reporting procedures). The report concludes that the product has met the target assurance level of EAL4+ and that the evaluation was conducted in accordance with the Common Criteria and the requirements of the Australasian Information Security Evaluation Program (AISEP). The evaluation was performed by CSC and was completed on 28 August 2009.

3 With regard to the secure operation of the TOE, the Australasian Certification Authority (ACA) recommends that:

a) The TOE is used only in its evaluated configurations; and

b) The TOE is operated according to the administrator's guidance.

4 This report includes information about the underlying security policies and architecture of the TOE, and information regarding the conduct of the evaluation.

5 It is the responsibility of the user to ensure that the TOE meets their requirements. For this reason, it is recommended that a prospective user of the TOE refer to the Security Target at Ref [1] and read this Certification Report prior to deciding whether to purchase the product.

Table of Contents

CHAPTER 1 - INTRODUCTION 1

1.1 OVERVIEW 1
1.2 PURPOSE 1
1.3 IDENTIFICATION 1

CHAPTER 2 - TARGET OF EVALUATION 2

2.1 OVERVIEW 2
2.2 DESCRIPTION OF THE TOE 2
2.3 SECURITY POLICY 3
2.4 TOE ARCHITECTURE 3
a) CypherManager Subsystem 3
b) Management Subsystem 3
c) Local and Network Interface Subsystems 4
d) Software Crypto Subsystem 4
e) Low Speed Crypto Subsystem 4
f) FPGA Crypto Subsystem 4
2.5 CLARIFICATION OF SCOPE 4
2.5.1 Evaluated Functionality 5
2.5.2 Non-evaluated Functionality and Systems 5
2.6 USAGE 5
2.6.1 Evaluated Configuration 5
2.6.2 Delivery procedures 7
2.6.3 Determining the Evaluated Configuration 8
2.6.4 Documentation 8
2.6.5 Secure Usage 9

CHAPTER 3 - EVALUATION 10

3.1 OVERVIEW 10
3.2 EVALUATION PROCEDURES 10
3.3 FUNCTIONAL TESTING 10
3.4 PENETRATION TESTING 11

CHAPTER 4 - CERTIFICATION 11

4.1 OVERVIEW 11
4.2 CERTIFICATION RESULT 11
4.3 ASSURANCE LEVEL INFORMATION 12
4.4 RECOMMENDATIONS 12

ANNEX A - REFERENCES AND ABBREVIATIONS 13

A.1 REFERENCES 13
ABBREVIATIONS 15

Chapter 1 - Introduction

1.1 Overview

6 This chapter contains information about the purpose of this document and how to identify the Target of Evaluation (TOE).

1.2 Purpose

7 The purpose of this Certification Report is to:

report the certification of results of the IT security evaluation of the TOE, Senetas Encryptor Range comprising CypherNET Ethernet Encryptor, CypherNET Fibre Channel Encryptor, CypherStream Ethernet Encryptor and CypherManager, against the requirements of the Common Criteria (CC) evaluation assurance level EAL4+, and provide a source of detailed security information about the TOE for any interested parties.

8 This report should be read in conjunction with the TOE's Security Target (Ref [1]) which provides a full description of the security requirements and specifications that were used as the basis of the evaluation.

1.3 Identification

9 Table 1 provides identification details for the evaluation. For details of all components included in the evaluated configuration refer to section 2.6.1 Evaluated Configuration.

Table 1: Identification Information

Item	Identifier
Evaluation Scheme	Australasian Information Security Evaluation Program
TOE	Senetas Encryptor Range comprising CypherNET Ethernet Encryptor, CypherNET Fibre Channel Encryptor, CypherStream Ethernet Encryptor and CypherManager
Software Version	CypherNet Application Software version 2.0.0 CypherStream Application Software version 1.0.6 CypherManager version 6.5.0
Security Target	Security Target for CypherNET Ethernet Encryptor CypherNET Fibre Channel Encryptor CypherStream Ethernet Encryptor CypherManager

Evaluation Level	EAL4+
Evaluation Technical Report	Senetas Encryptor Range Evaluation Technical Report Reference CSC-EFC-T0067-ETR Version 1.0
Criteria	Common Criteria for Information Technology Security Evaluation, Version 3.1, September 2007, with interpretations as of 3 December 2008.
Methodology	Common Methodology for Information Technology Security Evaluation, Evaluation methodology, September 2007, Version 3.1 Revision 2, CCMB-2007-09-004 with interpretations as of 3 December 2008.
Conformance	Common Criteria Part 2 conformant Common Criteria Part 3 Augmented with ALC_FLR.2 (Flaw reporting procedures.)
Sponsor/Developer	Senetas Security Ltd, Level 1 / 11 Queens Rd, Melbourne, Vic 3004
Evaluation Facility	CSC, 217 Northbourne Ave, Turner, ACT 2612

Chapter 2 - Target of Evaluation

2.1 Overview

10 This chapter contains information about the TOE, including: a description of functionality provided; its architecture components; the scope of evaluation; security policies; and its secure usage.

2.2 Description of the TOE

11 The TOE is Senetas Encryptor Range comprising CypherNET Ethernet Encryptor, CypherNET Fibre Channel Encryptor, CypherStream Ethernet Encryptor and CypherManager developed by Senetas. The primary role of the TOE is to encrypt data in transit.

12 The TOE consists of

- CypherNET encryptors;
- CypherStream encryptors; and

- CypherManager software.

13 CypherNET is a high-speed, standards based multi-protocol encryptor specifically designed to secure voice, data and video information transmitted over Ethernet and Fibre Channel data networks at data rates up to 10 Gigabits per second. It also provides access control facilities using access rules for each defined Ethernet or fibre channel connection.

14 CypherStream is a small desktop form factor 10 Mbps Ethernet Encryptor designed to provide an integrated data security solution for point to point or meshed Ethernet links up to 10 Mbps. CypherStream has been designed to integrate transparently and simply into network architectures.

15 CypherManager is a Graphical User Interface (GUI) software package that runs on Windows platforms. It acts as a Certification Authority (CA) for signing X.509 certificates and provides secure remote installation of X.509 certificates into CypherNET and CypherStream using SNMPv3.

2.3 Security Policy

16 The Security Target (Ref [1]) contains no explicit security policy model as the evaluation was performed at EAL4+.

2.4 TOE Architecture

The TOE comprises several major subsystems. These subsystems work together in enforcing the TSP.

a) CypherManager Subsystem

17 The CypherManager Subsystem provides a Graphical User Interface (GUI) for remote management of CypherNET and CypherStream encryptors. The subsystem utilises encrypted SNMPv3 communications over either an out-of-band management interface or in-band via the local and network interfaces. The software is compatible with Windows NT 4.0, 2000 and XP operating systems.

b) Management Subsystem

18 The management subsystem provides the following functionality:

a) Creation and maintenance of the audit log;

b) Audit trail analysis and review;

c) Creation and maintenance of user profiles;

d) Identification and authentication of users;

e) Remote management using SNMPv3;

f) Local management using the RS232 console port;

g) Creation and maintenance of the Connection Action Table (CAT);

h) Random number generation for keys;

i) A real time clock;

j) Running of self-tests during start-up; and

k) Automatic destruction of keys and user passwords if either of the interface cards are removed.

c) Local and Network Interface Subsystems

Both the network and local interface subsystems convert the physical signal received from the network and translates it into a suitable logical format for the frame/cell/bit stream/packet to be processed by the encryptor.

d) Software Crypto Subsystem

The software crypto subsystem provides cryptographic support services to the management subsystem. The subsystem is built using the open source OpenSSL libraries, and provides such functionality as session key establishment, certificate generation, authentication and provision of SNMP authentication and privacy services.

e) Low Speed Crypto Subsystem

The Low Speed Crypto Subsystem provides the encryption and decryption functionalities of the CypherStream encryptor, for traffic transmitted between encryptors. The subsystem is implemented in a software library and is configured by the Management Subsystem with user-desired algorithms and associated parameters.

f) FPGA Crypto Subsystem

CypherNet encryptors use a Field Programmable Gate Array (FPGA)to conduct encryption and decryption of protected traffic between encryptors. The cryptographic functions are performed at very high speed as the process occurs purely in hardware.

2.5 Clarification of Scope

19 The scope of the evaluation was limited to those claims made in the Security Target (Ref [1]). Unlike other encryption devices which provide layer 3 encryption and may contain replay protection, the CypherNET and CypherStream encryptors are layer 2 encryption devices that do not

provide or claim protection against replay of legitimate traffic. The CypherNet and CypherStream encryptors are designed to provide confidentiality of data transmitted across untrusted networks.

2.5.1 Evaluated Functionality

20 The TOE provides the following evaluated security functionality:

a) Security audit;

b) Cryptographic support;

c) User data protection;

d) Identification and authentication;

e) Security management;

f) Protection of the TOE security functions;

g) TOE access; and

h) Trusted path/Channels.

2.5.2 Non-evaluated Functionality and Systems

21 Potential users of the TOE are advised that some functions and services have not been evaluated as part of the evaluation. Potential users of the TOE should carefully consider their requirements for using functions and services outside of the evaluated configuration; Australian Government users should refer to Australian Government Information Security Manual (ISM) (Ref [2]) for policy relating to using an evaluated product in an unevaluated configuration. New Zealand Government users should consult the Government Communications Security Bureau (GCSB).

22 The functions and services that have not been included as part of the evaluation are provided below:

a) The IdQuantique product is not in scope of the TOE. The CypherNet encryptor using QKD keys is in scope. Cerberis (the combination of IdQuantique 5100 and CypherNET) is not considered to have any negative impact on the Cyphernet security functions.

2.6 Usage

2.6.1 Evaluated Configuration

23 This section describes the configurations of the TOE that were included within scope of the evaluation. The assurance gained via evaluation applies specifically to the TOE in these defined evaluated configurations.

Australian Government users should refer to ISM (Ref [2]) to ensure that configurations meet the minimum Australian Government policy requirements. New Zealand Government users should consult the GCSB.

24 The TOE is comprised of the following software components:

a) CypherNet Application Software version 2.0.0

b) CypherStream Application Software version 1.0.6

c) CypherManager 6.5.0

25 The TOE relies on the following hardware:

Table 2 - CypherNET Model Numbers

ID	Description
A5137B	CYPHERNET ETHERNET 100M (SFP+RJ45) AC UNIT
A5139B	CYPHERNET ETHERNET 10M (SFP+RJ45) AC UNIT
A5141B	CYPHERNET ETHERNET 1G (SFP+RJ45) AC UNIT
A5171B	CYPHERNET FIBRE CHANNEL 1G AC UNIT
A5173B	CYPHERNET FIBRE CHANNEL 2G AC UNIT
A5175B	CYPHERNET FIBRE CHANNEL 4G AC UNIT
A5203B	CYPHERNET ETHERNET 10G AC UNIT
A5204B	CYPHERNET ETHERNET 10G DC UNIT
A2153B	CYPHERNET ETHERNET 10M AC UNIT
A2151B	CYPHERNET ETHERNET 100M AC UNIT
A2101B	CYPHERNET ETHERNET 1G AC UNIT
A2159B	CYPHERNET ETHERNET 10M (SFP+RJ45) AC UNIT
A2157B	CYPHERNET ETHERNET 100M (SFP+RJ45) AC UNIT
A2155B	CYPHERNET ETHERNET 1G (SFP+RJ45) AC UNIT
A2165B	CYPHERNET FIBRE CHANNEL 1G AC UNIT
A2163B	CYPHERNET FIBRE CHANNEL 2G AC UNIT

A2161B	CYPHERNET FIBRE CHANNEL 4G AC UNIT
A2202B	CYPHERNET ETHERNET 10G DC UNIT

Table 3 - CypherStream Model Number

ID	Description
A4201B	CYPHERSTREAM ETHERNET 10M (RJ45) AC UNIT

26 The TOE evaluated configuration consists of the CypherNET application software version 2.0.0 loaded onto the applicable encryptor hardware model; the CypherStream application software version loaded onto the applicable encryptor model; and a single version of CypherManager software (6.5.0). The out of scope Quantum Key Distribution System was connected to ensure no adverse effects on the CypherNET security functionality. Although the IdQuantique product is not in scope of the TOE, the CypherNet encryptor using QKD keys is in scope.

Table 4 - Cerberis Model Number

ID	Description
5100	CERBERIS QUANTUM KEY DISTRIBUTION SYSTEM

2.6.2 Delivery procedures

27 When placing an order for the TOE, purchasers should make it clear to their supplier that they wish to receive the evaluated product. They should then receive the correct hardware and software.

a) Hardware

28 Shipment of units from Senetas to the user is via a commercial courier company who will pick up the unit from Senetas and deliver it directly to the user. After placing an order, Senetas will issue an Order Acknowledgement Form listing the assigned user order number, the model number(s), serial number(s) and expected date of delivery. When items are received, the customer must ensure that the serial number on the outside of the packaging, the serial number attached to the encryptor itself and the number listed on the Acknowledgement match. The customer must also verify that the tamper proof seal on the outside of the unit is intact. If the seal is broken then the integrity of the encryptor cannot be assured and Senetas should be informed immediately.

a) Software

29 Before shipping any software upgrades, a ‘Software Upgrade Notice’ will be sent to the user. The software upgrade notice will list the user name, software maintenance agreement number, software identification number, software version number, a random shipment identification number and expected date of delivery.

30 Before shipment of the software, a Shipment Identification Number label is attached to the software media, the software media is sealed in an envelope and a tamper proof seal is attached across the flap of the envelope. Upon delivery, the customer must verify the information in the Shipment Identification Number label matches the Software Upgrade Notice. The customer must also verify that the tamper proof seal is intact. If the seal is broken or the information does not match, Senetas should be informed immediately.

2.6.3 Determining the Evaluated Configuration

31 To ensure the hardware received is the evaluated product the customer must check the models received against the list of TOE hardware models defined in the Security Target [1]. In addition to verifying model numbers for hardware components, the software versions must also be verified by the recipient. Software versions can be checked using the “version” command over an encryptor’s command line interface (CLI).

2.6.4 Documentation

32 It is important that the TOE is used in accordance with guidance documentation (Ref [3]) in order to ensure secure usage. The following documentation is delivered to the consumer along with the TOE for each corresponding configuration:

a) CypherNet

33 Senetas CypherNet Product Manual, Version 2.0, July 2009 the CypherNET Product manual describes the processes and other relevant information for the secure installation and operation of the CypherNET Multiprotocol Encryptor. Additionally this document describes usage assumptions and details technical information regarding the TOE’s use.

b) CypherStream

34 Senetas CypherStream Product Manual, Version 2.0, July 2009 the CypherStream Product manual describes the processes and other relevant information for the secure installation and operation of the CypherStream Encryptor. Additionally this document describes usage assumptions and details technical information regarding the TOE’s use.

c) Cerberis

35 CypherNet QKD Functionality User Manual, Version 0.2, March 2007 The CypherNet QKD Functionality User Manual provides details on installation, configuration and operation of the TOE in the Cerberis configuration. The manual should be read in conjunction with the CypherNet Product Manual, which describes the features, functions and operation of the CypherNet product range.

2.6.5 Secure Usage

36 The evaluation of the TOE took into account certain assumptions about its operational environment. These assumptions must hold in order to ensure the security objectives of the TOE are met.

37 Section 3.1: 'Assumptions' in the Security Target (Ref [1]) provides a full description of the assumptions. Assumptions are made in the following areas:

a) Physical security;

b) Configuration;

c) Administrators;

d) Inspection of audit logs;

e) Restricted access to private key; and

f) Installation.

38 In addition, the following organisational security policies must be in place:

a) All encryption services must conform to the standards specified in the ISM (Ref [2]).

b) Traffic flow is controlled on the basis of the information in the Ethernet frame or fibre channel frame and the action specified in the Connection Action Table. Any Ethernet frame or fibre channel frame for which there is no CAT entry is discarded. By default all unrecognised Ethernet or fibre frames are discarded.

c) Administration of the TOE is controlled through the definition of roles, which assign different privilege levels to different types of authorised users. (administrators, supervisors and operators.) The TOE is administered in accordance with the concept of 'least privilege'.

Chapter 3 - Evaluation

3.1 Overview

39 This chapter contains information about the procedures used in conducting the evaluation and the testing conducted as part of the evaluation.

3.2 Evaluation Procedures

40 The criteria against which the Target of Evaluation (TOE) has been evaluated are contained in the Common Criteria for Information Technology Security Evaluation Version 3.1 Revision 2 (Refs [4], [5] and [6]). The methodology used is described in the Common Methodology for Information Technology Security Evaluation Version 3.1 Revision 2 (CEM) (Ref [7]). The evaluation was carried out in accordance with the operational procedures of the Australasian Information Security Evaluation Program (AISEP) (Refs [8], [9],[10] and [11]). In addition, the conditions outlined in the Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security (Ref [12]) were also upheld.

3.3 Functional Testing

41 To gain confidence that the developer's testing was sufficient to ensure the correct operation of the TOE, the evaluators analysed the evidence of the developer's testing effort. This analysis included examining: test coverage; test plans and procedures; and expected and actual results. The evaluators drew upon this evidence to perform a sample of the developer tests in order to verify that the test results were consistent with those recorded by the developers. Independent evaluator testing was conducted at three sites. Components of the testing that required the use of specialised equipment in relation to Fibre Channel analysis were conducted at Senetas' head office, Level 1/11 Queens Road, St Kilda, Victoria. The majority of functional and penetration testing was conducted at CSC's AISEF Laboratory at 212 Northbourne Avenue, Braddon, ACT. Due to office relocation, the remainder of the testing was performed at CSC's AISEF Laboratory at 217 Northbourne Avenue, Turner, ACT. The evaluators conducted independent and penetration testing between the 5th of June 2009 and the 7th of August 2009. The evaluators chose to repeat a sample of developer tests on a Fibre Channel Device covering the core security functionality associated within the following Functions described in the Security Target (Ref [1]):

a) F.INFORMATION_FLOW_CONTROL

b) F.DATA_EXCHANGE

c) F.KEY_MANAGEMENT

d) F.SELF_PROTECT

42 The evaluators note this core functionality implements 16 of the 37 Security Functional Requirements (SFRs) described in the Security Target(Ref [1]), which covers 43% of the total Security Functional requirements. The evaluators therefore consider the sample large enough to gain confidence that the developers' test results are correct, without the expense of confirming the whole test suite.

3.4 Penetration Testing

43 The developer performed a vulnerability analysis of the TOE in order to identify any obvious vulnerability in the product and to show that the vulnerabilities were not exploitable in the intended environment of the TOE. This analysis included a search for possible vulnerability sources in publicly available information such as:

a) Milw0rm - http://www.milw0rm.com
a) Security Focus - http://www.securityfocus.com
b) Secunia - http://www.secunia.com
c) Packetstorm Security - http://www.packetstormsecurity.org

44 The penetration effort included traffic replay, autodiscovery, portscan, flow control, ARPE Cache poisoning, exploitation of MAC Address Learning, malformed Ethernet traffic, SNMP traffic and etherleak testing, The analysis conducted by the evaluators and the subsequent testing indicated that the TOE will resist an attacker with an attacker potential consistent with the requirements of an EAL 4+ assurance level.

Chapter 4 - Certification

4.1 Overview

45 This chapter contains information about the result of the certification, an overview of the assurance provided by the level chosen, and recommendations made by the certifiers.

4.2 Certification Result

46 After due consideration of the conduct of the evaluation as witnessed by the certifiers and of the Evaluation Technical Report (Ref[13]), the Australasian Certification Authority certifies the evaluation of Senetas Encryptor Range comprising CypherNET Ethernet Encryptor, CypherNET Fibre Channel Encryptor, CypherStream Ethernet Encryptor and CypherManager performed by the Australasian Information Security Evaluation Facility, CSC.

47 CSC has found that Senetas Encryptor Range comprising CypherNET Ethernet Encryptor, CypherNET Fibre Channel Encryptor, CypherStream Ethernet Encryptor and CypherManager upholds the claims made in the Security Target (Ref [1]) and has met the requirements of the Common Criteria (CC) evaluation assurance level EAL4 augmented with ALC_FLR.2 (Flaw reporting procedures).

48 Certification is not a guarantee of freedom from security vulnerabilities.

4.3 Assurance Level Information

49 EAL4 provides assurance by a full security target and an analysis of the SFRs in that Security Target (Ref [1]), using a functional and complete interface specification, guidance documentation, a description of the basic modular design of the TOE, and a subset of the implementation, to understand the security behaviour.

50 The analysis is supported by independent testing of the TSF, evidence of developer testing based on the functional specification and TOE design, selective independent confirmation of the developer test results, and a vulnerability analysis (based upon the functional specification, TOE design, implementation representation, security architecture description and guidance evidence provided) demonstrating resistance to penetration attackers with an Enhanced-Basic attack potential.

51 EAL4 also provides assurance through the use of development environment controls and additional TOE configuration management including automation and evidence of secure delivery procedures.

4.4 Recommendations

52 Not all of the evaluated functionality present in the TOE may be suitable for Australian and New Zealand Government users. For further guidance, Australian Government users should refer to the ISM (Ref [2]) and New Zealand Government users should consult the GCSB.

53 In addition to ensuring that the assumptions concerning the operational environment are fulfilled and the guidance document is followed (Ref [3]), the ACA also recommends that:

a) The TOE is used only in its evaluated configurations; and

b) The TOE is operated according to the administrator's guidance.

Annex A - References and Abbreviations

A.1 References

[1] Security Target for CypherNET Ethernet Encryptor, CypherNET Fibre Channel Encryptor, CypherStream Ethernet Encryptor, CypherManager Version 2.0, 4 August 2009.

[2] Australian Government Information Security Manual (ISM), September 2009, Defence Signals Directorate, (available at www.dsd.gov.au).

[3] User Documentation.

i) Senetas CypherNet Product Manual, Version 2.0, July 2009

ii) Senetas CypherStream Product Manual, Version 2.0, July 2009

iii) CypherNet QKD Functionality User Manual, Version 0.2, March 2007

[4] Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Model (CC), Version 3.1, Revision 1, September 2006, CCMB-2006-09-001, Incorporated with interpretations as of 2008-05-29

[5] Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components (CC), Version 3.1, Revision 2 , September 2007, CCMB-2007-09-002, Incorporated with interpretations as of 2008-05-29

[6] Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components (CC), Version 3.1, Revision 2, September 2007, CCMB-2007-09-003, Incorporated with interpretations as of 2008-05-29

[7] Common Methodology for Information Technology Security Evaluation (CEM), Version 3.1, Revision 2 September 2007, CCMB-2007-09-004 Incorporated with interpretations as of 2008-05-29

[8] AISEP Publication No. 1 – Program Policy, AP 1, Version 3.1, 29 September 2006, Defence Signals Directorate.

[9] AISEP Publication No. 2 – Certifier Guidance, AP 2. Version 3.3, September 2007, Defence Signals Directorate.

[10] AISEP Publication No. 3 – Evaluator Guidance, AP 3. Version 3.1, 29 September 2006, Defence Signals Directorate.

[11] AISEP Publication No. 4 – Sponsor and Consumer Guidance, AP 4. Version 3.1, 29 September 2006, Defence Signals Directorate.

[12] Arrangement on the Recognition of Common Criteria Certificates in the field of Information Technology Security, May 2000

[13] Evaluation Technical Report for Senetas Encryptor Range Version 1.0 28/8/09

Abbreviations

AISEF	Australasian Information Security Evaluation Facility
AISEP	Australasian Information Security Evaluation Program
CAT	Connection Action Table
CC	Common Criteria
CEM	Common Evaluation Methodology
DSD	Defence Signals Directorate
EAL	Evaluation Assurance Level
ETR	Evaluation Technical Report
GCSB	Government Communications Security Bureau
SFP	Security Function Policy
SFR	Security Functional Requirements
ST	Security Target
TOE	Target of Evaluation
TSF	TOE Security Functions
TSP	TOE Security Policy
QKD	Quantum key distribution system