



**SERTIT**

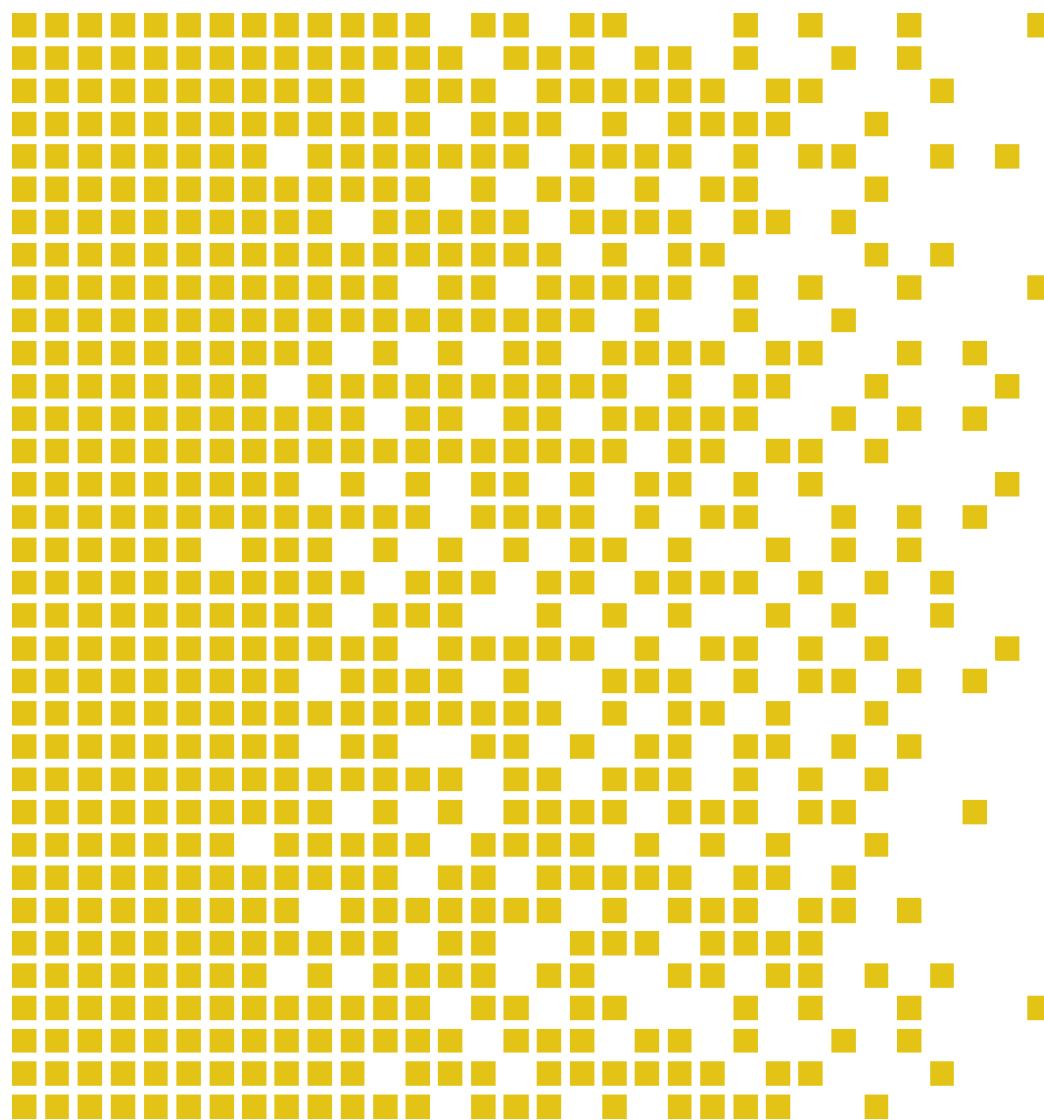
Sertifiseringsmyndigheten for IT-sikkerhet *Norwegian Certification Authority for IT Security*

# SERTIT-111 CR Certification Report

Issue 1.0 1 July 2019

Expiry date 1 July 2024

Ruckus Solution



CERTIFICATION REPORT - SERTIT STANDARD REPORT TEMPLATE ST 009E VERSION 2.5 15.05.2018

**ARRANGEMENT ON THE RECOGNITION OF COMMON CRITERIA CERTIFICATES IN  
THE FIELD OF INFORMATION TECHNOLOGY SECURITY (CCRA)**

SERTIT, the Norwegian Certification Authority for IT Security, is a member of the above Arrangement and as such this confirms that the Common Criteria certificate has been issued by or under the authority of a Party to this Arrangement and is the Party's claim that the certificate has been issued in accordance with the terms of this Arrangement

The judgements contained in the certificate and Certification Report are those of SERTIT which issued it and the evaluation facility (EVIT) which carried out the evaluation. There is no implication of acceptance by other Members of the Agreement Group of liability in respect of those judgements or for loss sustained as a result of reliance placed upon those judgements by a third party.

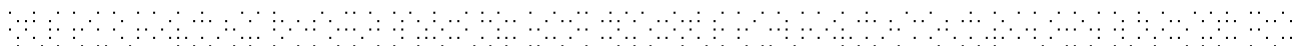
The recognition under CCRA is limited to cPP related assurance packages or components up to EAL 2 with ALC\_FLR CC part 3 components.





## Contents

|     |   |    |
|-----|---|----|
| 1   | Certification Statement                 | 4  |
| 2   | Abbreviations                           | 5  |
| 3   | References                              | 6  |
| 4   | Executive Summary                       | 7  |
| 4.1 | Introduction                            | 7  |
| 4.2 | Evaluated Product                       | 7  |
| 4.3 | TOE scope                               | 8  |
| 4.4 | Protection Profile Conformance          | 8  |
| 4.5 | Security Claims                         | 8  |
| 4.6 | Evaluation Conduct                      | 8  |
| 4.7 | General Points                          | 9  |
| 5   | Evaluation Findings                     | 10 |
| 5.1 | Introduction                            | 10 |
| 5.2 | Delivery                                | 10 |
| 5.3 | Installation and Guidance Documentation | 11 |
| 5.4 | Misuse                                  | 11 |
| 5.5 | Vulnerability Analysis                  | 11 |
| 5.6 | Evaluators' Tests                       | 11 |
| 6   | Evaluation Outcome                      | 12 |
| 6.1 | Certification Result                    | 12 |
| 6.2 | Recommendations                         | 12 |
|     | Annex A: Evaluated Configuration        | 13 |
|     | TOE Identification                      | 13 |
|     | TOE Documentation                       | 13 |
|     | TOE Configuration                       | 14 |



## 1 Certification Statement

Ruckus Solution (Ruckus Solution) is a system of products that are administratively configured to interoperate together to provide a WLAN. The TOE is meant to allow mobile or non-mobile, wireless clients to be roaming hosts on the wireless network, and to connect to the wired network using access points (APs). The TOE provides end-to-end wireless encryption, centralized WLAN management, authentication, authorization, and accounting (AAA) policy enforcement.

Ruckus Solution (versions specified in 4.2 and Annex A) has been evaluated under the terms of the Norwegian Certification Authority for IT Security.

The TOE and ST are conformant with the following specifications: CC Part 2: Security functional components, April 2017, Version 3.1, Revision 4, extended. CC Part 3: Security assurance components, April 2017, Version 3.1, Revision 4, conformant.

The TOE and ST are conformant with collaborative Protection Profile for Network Devices, Version 2.0 + Errata 20180314, 14 March 2018 (CPP\_ND\_V2.0E), and Extended Package for Wireless LAN Access System, v1.0, May 29, 2015 (PP\_WLAN\_AS\_EP\_V1.0). The TOE provides all of the functionality at a level of security corresponding to that identified in the collaborative Protection Profile for Network Devices, Version. 2.0 + Errata 20180314, 14 March 2018 (CPP\_ND\_V2.0E), and Extended Package for Wireless LAN Access System, v1.0, May 29, 2015 (PP\_WLAN\_AS\_EP\_V1.0).

|                    |   |
|--------------------|---|
| Certification team | Arne Høye Rage, SERTIT<br>Lars Borgos, SERTIT |
| Date approved      | 1 July 2019                                   |
| Expiry date        | 1 July 2024                                   |



## 2 Abbreviations

|               |  |
|---------------|--|
| CC            | Common Criteria for Information Technology Security Evaluation(ISO/IEC 15408)                                  |
| CCRA          | Arrangement on the Recognition of Common Criteria Certificates in the Field of Information Technology Security |
| CEM           | Common Methodology for Information Technology Security Evaluation  |
| cPP           | collaborative Protection Profile   |
| EAL           | Evaluation Assurance Level   |
| EOR           | Evaluation Observation Report  |
| ETR           | Evaluation Technical Report  |
| EVIT          | Evaluation Facility under the Norwegian Certification Scheme for IT Security                                   |
| EWP           | Evaluation Work Plan   |
| ISO/IEC 15408 | Information technology -- Security techniques -- Evaluation criteria for IT security                           |
| POC           | Point of Contact   |
| PP            | Protection Profile   |
| QP            | Qualified Participant  |
| SERTIT        | Norwegian Certification Authority for IT Security  |
| SOGIS MRA     | SOGIS Mutual Recognition Agreement of Information Technology Security Evaluation Certificates                  |
| SPM           | Security Policy Model  |
| ST            | Security Target  |
| TOE           | Target of Evaluation   |
| TSF           | TOE Security Functions   |
| TSP           | TOE Security Policy  |



### 3 References

- [1] SERTIT (2018), *The Norwegian Certification Scheme*, SD001E, Version 10.4, SERTIT, 20 February 2018.
- [2] CCRA (2012), *Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and general model*, CCMB-2012-09-001, Version 3.1 R4, CCRA, September 2012.
- [3] CCRA (2012), *Common Criteria for Information Technology Security Evaluation, Part 2: Security functional components*, CCMB-2012-09-002, Version 3.1 R4, CCRA, September 2012.
- [4] CCRA (2012), *Common Criteria for Information Technology Security Evaluation, Part 3: Security assurance components*, CCMB-2012-09-003, Version 3.1 R4, CCRA, September 2012.
- [5] CCRA (2012), *Common Methodology for Information Technology Security Evaluation, Evaluation Methodology*, CCMB-2012-09-004, Version 3.1 R4, CCRA, September 2012.
- [6] CCRA (2006), *ST sanitising for publication*, 2006-04-004, CCRA, April 2006.
- [7] CCRA (2014), *Arrangement on the Recognition of Common Criteria Certificates In the field of Information Technology Security*, CCRA, July 2<sup>nd</sup> 2014.
- [8] Security Target for Ruckus Solution, version 1.2, 14 June 2019.
- [9] Collaborative Protection Profile for Network Devices v 2.0, + Errata 20180314, 14 March 2018
- [10] Extended Package for Wireless LAN Access System, v1.0, May 29, 2015 (pp\_wlan\_as\_ep\_v1.0)
- [11] Evaluation Technical Report ETR for the evaluation project SERTIT-111 version 1.1, 7 June 2019



## 4 Executive Summary

### 4.1 Introduction

This Certification Report states the outcome of the Common Criteria security evaluation of Ruckus Solution (versions detailed in 4.2) to the developer Ruckus Wireless, Inc., and is intended to assist prospective consumers when judging the suitability of the IT security of the product for their particular requirements.

Prospective consumers are advised to read this report in conjunction with the ST[8] which specifies the functional, environmental and assurance evaluation components.

### 4.2 Evaluated Product

The product evaluated was Ruckus Solution and following versions:

#### Wireless Controllers:

Smart Zone 100 (Includes SZ-104 and SZ124 models)

Smart Zone 300 (SZ-300)

Ruckus virtual SmartZone (includes vSZ-E and vSZ-H) running on a specific physical hardware platform (Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz with AES-NI)

Ruckus virtual SmartZone – Data plane (vSZ-D) running on a specific physical hardware platform (Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz with AES-NI)

#### Access Points:

R610

R710

R720

T610 (Including T610S)

T710 (Including T710S)

E510

#### Software version:

5.1.1.3

These products are also described in this report as the Target of Evaluation (TOE). The developer was Ruckus Wireless, Inc.

Details of the evaluated configuration, including the TOE's supporting guidance documentation, are given in Annex A.

### 4.3 TOE scope

The scope of the evaluation includes firmware and hardware that form the TOE and the TOE security functions that are stated in the Security Target[8]

### 4.4 Protection Profile Conformance

The ST[8] claimed conformance to the protection profile:

Collaborative Protection Profile for Network Devices, Version. 2.0 + Errata 20180314, 14 March 2018 (CPP\_ND\_V2.0E).

and

Extended Package for Wireless LAN Access System, v1.0, May 29, 2015 (PP\_WLAN\_AS\_EP\_V1.0).

### 4.5 Security Claims

The Assumptions, Threats, and Organization Security Policies included in the Security Target correspond to the Assumptions, Threats, and Organization Security Policies specified in the collaborative Protection Profile for Network Devices, Version. 2.0 + Errata 20180314, 14 March 2018 (CPP\_ND\_V2.0E), and Extended Package for Wireless LAN Access System, v1.0, May 29, 2015 (PP\_WLAN\_AS\_EP\_V1.0) for which exact conformance is claimed.

The Security Objectives included in the Security Target correspond to the Security Objectives specified in the CPP\_ND\_V2.0E and PP\_WLAN\_AS\_EP\_V1.0, for which exact conformance is claimed.

The Security Functional Requirements included in the Security Target correspond to the Security Functional Requirements specified in the CPP\_ND\_V2.0E and PP\_WLAN\_AS\_EP\_V1.0, for which exact conformance is claimed. Security Assurance Requirements specified in this Security Target are identical to the Security Assurance Requirements included in the CPP\_ND\_V2.0E and PP\_WLAN\_AS\_EP\_V1.0.

### 4.6 Evaluation Conduct

The evaluation was carried out in accordance with the requirements of the Norwegian Certification Scheme for IT Security as described in SERTIT Document SD001E[1]. The Scheme is managed by the Norwegian Certification Authority for IT Security (SERTIT). As stated on page 2 of this Certification Report, SERTIT is a member of the Arrangement on the Recognition of Common Criteria Certificates in the Field of Information





Technology Security, CCRA[7], and the evaluation was conducted in accordance with the term of this Arrangement.

The purpose of the evaluation was to provide assurance about the effectiveness of the TOE in meeting its ST[8], which prospective consumers are advised to read. To ensure that the ST gave an appropriate baseline for a CC evaluation, it was first itself evaluated. The TOE was then evaluated against this baseline. Both parts of the evaluation were performed in accordance with CC Part 3[4] and the Common Evaluation Methodology (CEM)[5].

SERTIT monitored the evaluation in accordance with SD001E[1] which was carried out by the Advanced Data Security Commercial Evaluation Facility (EVIT). The evaluation was completed when the EVIT submitted the final ETR[11] to SERTIT on 7 June 2019. SERTIT then produced this Certification Report.

#### 4.7 General Points

The evaluation addressed the security functionality claimed in the ST[8] with reference to the assumed operating environment specified by the ST[8]. The evaluated configuration was that specified in Annex A. Prospective consumers are advised to check that this matches their identified requirements and give due consideration to the recommendations and caveats of this report.

Certification does not guarantee that the IT product is free from security vulnerabilities. This Certification Report and the belonging Certificate only reflect the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown in this report. This Certification Report is not an endorsement of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report, and no warranty of the IT product by SERTIT or any other organization that recognizes or gives effect to this Certification Report is either expressed or implied.



## 5 Evaluation Findings

The TOE assurance requirements for the ST are listed in the collaborative Protection Profile for Network Devices, Version. 2.0 + Errata 20180314, 14 March 2018 (CPP\_ND\_V2.0E), and Extended Package for Wireless LAN Access System, v1.0, May 29, 2015 (PP\_WLAN\_AS\_EP\_V1.0) and correspond to the set of SARs listed in Common Criteria Version 3.1, Revision 4.

| <b>Assurance Component</b> | <b>Component Name</b>          | <b>Assurance Measures</b>                         |
|----------------------------|--------------------------------|---|
| ADV_FSP.1                  | Basic functional specification | Security Design for the Ruckus Solution           |
| AGD_OPE.1                  | Operational user guidance      | Operational User Guidance for the Ruckus Solution |
| AGD_PRE.1                  | Preparative procedures         | Preparative procedures for the Ruckus Solution    |
| ALC_CMC.1                  | Labeling of the TOE            | CM plan for the Ruckus Solution                   |
| ALC_CMS.1                  | TOE CM coverage                | CM plan for the Ruckus Solution                   |
| ATE_IND.1                  | Independent testing – sample   | EVIT Security Testing of the Ruckus Solution      |
| AVA_VAN.1                  | Vulnerability survey           | Vulnerability survey of the Ruckus Solution       |
| ASE_TSS.1                  | Security Target                | Security Target                                   |

### 5.1 Introduction

The evaluation addressed the requirements specified in the ST[8]. The results of this work were reported in the ETR[11] under the CC Part 3[4] headings. The following sections note considerations that are of particular relevance to either consumers or those involved with subsequent assurance maintenance and re-evaluation of the TOE.

### 5.2 Delivery

On receipt of the TOE, the consumer is recommended to check that the evaluated version has been supplied, and to check that the security of the TOE has not been compromised in delivery.



### 5.3 Installation and Guidance Documentation

Installation of the TOE must be performed completely in accordance with the guidance in the Operational User Guidance documents provided by the developer.

These documents are a collection of all security relevant operations and settings that must be observed to ensure that the TOE operates in a secure manner.

### 5.4 Misuse

There is always a risk of intentional and unintentional misconfigurations that could possibly compromise confidential information. The user should always follow the guidance for the TOE in order to ensure that the TOE operates in a secure manner.

The guidance documents adequately describe the mode of operation of the TOE, all assumptions about the intended environment and all requirements for external security. Sufficient guidance is provided for the consumer to effectively use the TOE's security functions.

### 5.5 Vulnerability Analysis

The Evaluators' vulnerability analysis was based on both public domain sources and the visibility of the TOE given by the evaluation process.

Upon completing penetration tests the verdict is that the TOE is resistant against attackers possessing Basic attack potential. Therefore, the evaluators concluded that the TOE, in its intended environment, is resistant to an attacker possessing a Basic attack potential

### 5.6 Evaluators' Tests

The evaluators have examined the test plan and determined that the TOE test configuration is consistent with the ST. The evaluators have produced test documentation detailed so that the tests are reproducible. The document provides the testing approach, interfaces used to test and observe responses, and initial conditions. The evaluators have conducted the tests and recorded the results. All results are of passing grade. The independent tests concentrated on critical functionality of the TOE.



## 6 Evaluation Outcome

### 6.1 Certification Result

After due consideration of the ETR[11], produced by the Evaluators, and the conduct of the evaluation, as witnessed by the Certifier, SERTIT has determined that Ruckus Solution versions specified in 4.2 and Annex A meet the Common Criteria Part 3 conformant assurance components and the Common Criteria Part 2 extended functionality specified in Protection Profile CPP\_ND\_V2.0E and PP\_WLAN\_AS\_EP\_v1.0 in the specified environment, when running on platforms specified in Annex A.

### 6.2 Recommendations

Prospective consumers of Ruckus Solution, versions specified in 4.2 and Annex A should understand the specific scope of the certification by reading this report in conjunction with the ST[8]. The TOE should be used in accordance with a number of environmental considerations as specified in the ST[8].

Only the evaluated TOE configuration should be installed. This is specified in Annex A with further relevant information given above in Section 4.3 “TOE Scope” and Section 5 “Evaluation Findings”.

The TOE should be used in accordance with the supporting guidance documentation included in the evaluated configuration.



## Annex A: Evaluated Configuration

### TOE Identification

The product evaluated was Ruckus Solution and following versions:

#### Wireless Controllers:

Smart Zone 100 (includes SZ-104 and SZ-124 models)

Smart Zone 300 (SZ-300)

Ruckus virtual SmartZone (includes vSZ-E and vSZ-H) running on a specific physical hardware platform (Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz with AES-NI)

Ruckus virtual SmartZone – Data plane (vSZ-D) running on a specific physical hardware platform (Intel(R) Xeon(R) CPU E5-2620 v4 @ 2.10GHz with AES-NI)

#### Access Points:

R610

R710

R720

T610 (including T610S)

T710 (including T710S)

E510

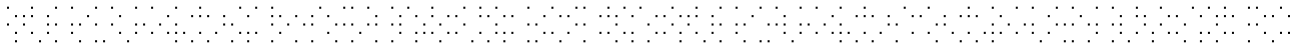
#### Software version:

5.1.1.3

### TOE Documentation

The supporting guidance documents evaluated were:

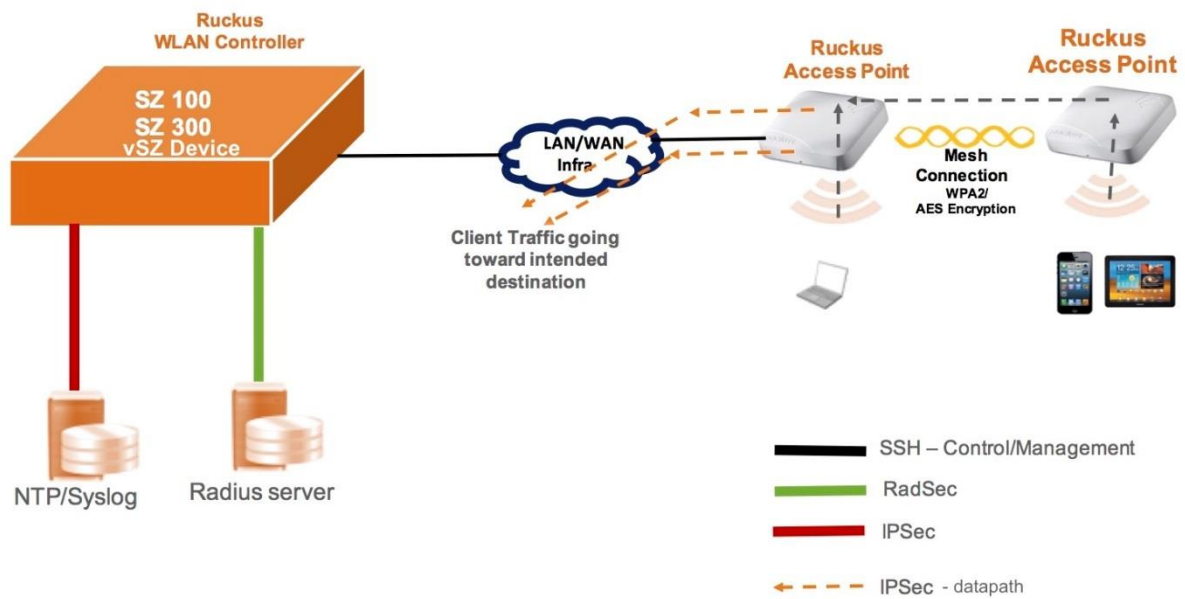
- [a] Security Target for Ruckus Solution, version 1.2, 14 June 2019
- [b] Ruckus FIPS and Common Criteria Configuration Guide for SmartZone and AP, v. 1.0
- [c] Common Criteria Guidance Supplement document, v. 3.0
- [d] Ruckus FIPS Configuration Guide for SmartZone and AP, April 2018
- [e] SCG200 vSZ-H and SZ300 Administrator Guide, November 2017



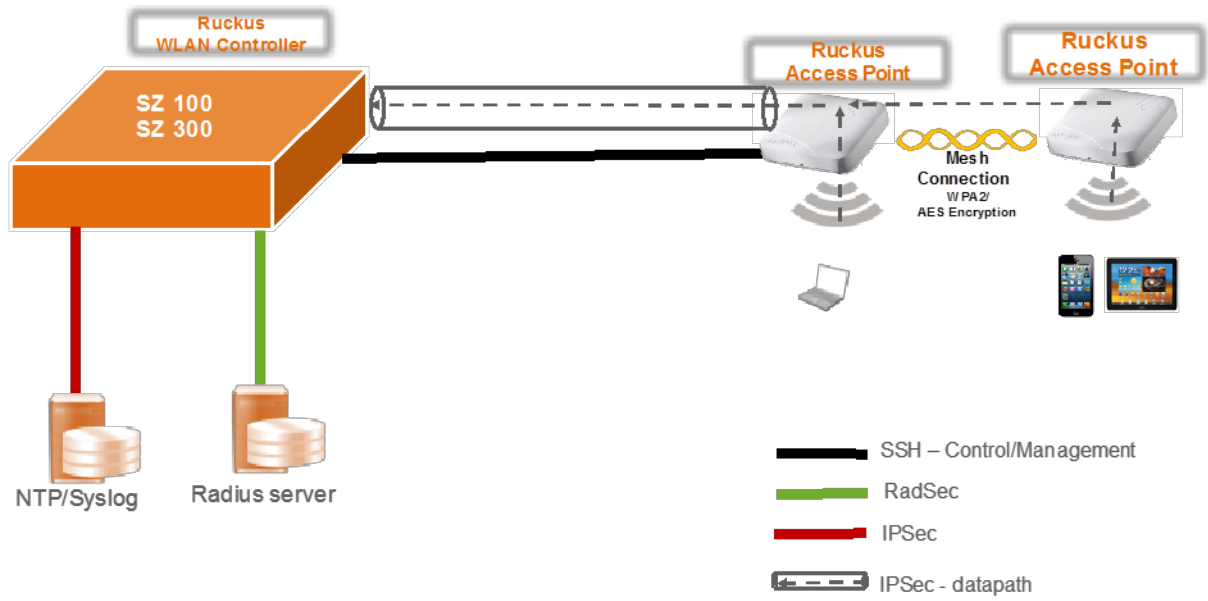
- [f] Ruckus SmartZone 100 and Virtual SmartZone Essentials Administrator Guide, November 2017
- [g] Ruckus SmartZone 100 Getting Started Guide, August 2017
- [h] Ruckus SmartZone 100 Quick Setup Guide, November 2017
- [i] SmartZone 300 Quick Setup Guide, November 2017

### TOE Configuration

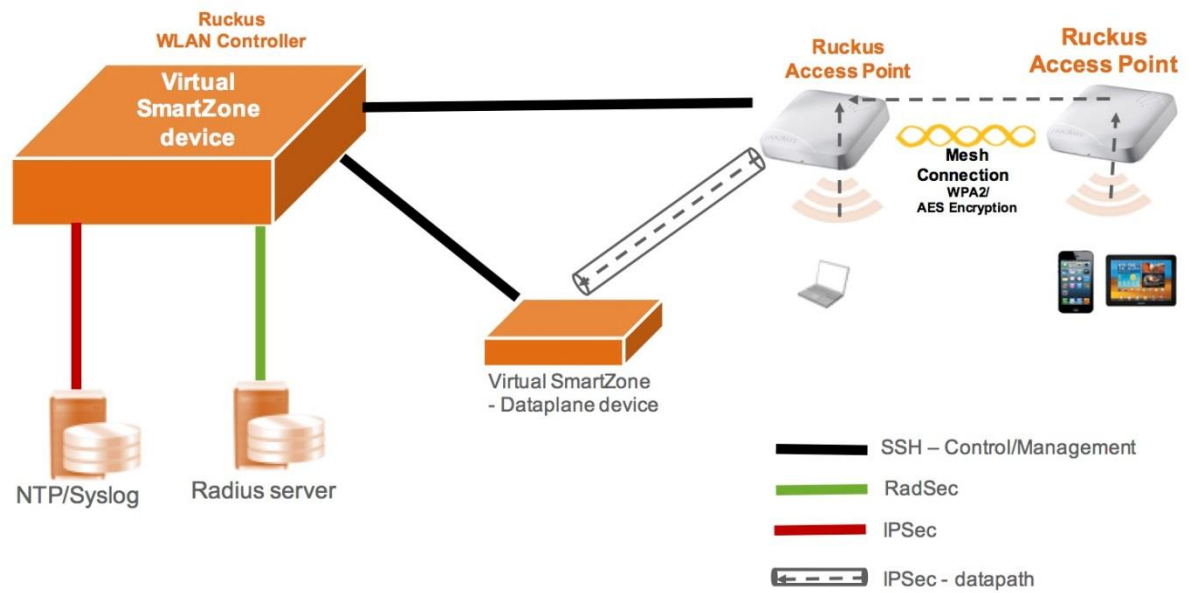
The following configuration was used for testing:



### Distributed Deployment Model



Centralized Deployment Model 1



Centralized Deployment Model 2



# Certificate

*The IT product identified in this certificate has been evaluated at the Norwegian evaluation facility described on this certificate using Common Methodology for IT Security Evaluation, according to the version number described on this certificate, for conformance to the Common Criteria for IT Security Evaluation according to the version number described on this certificate. This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification report. The evaluation has been conducted in accordance with the provisions of The Norwegian Certification Authority for IT Security (SERTIT) and the conclusions of the evaluation technical report are consistent with the evidence adduced. Certification does not guarantee that the IT product is free from security vulnerabilities. This certificate only reflects the view of SERTIT at the time of certification. It is furthermore the responsibility of users (both existing and prospective) to check whether any security vulnerabilities have been discovered since the date shown of this certificate. This certificate is not an endorsement of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, and no warranty of the IT product by SERTIT or by any other organization that recognizes or gives effect to this certificate, is either expressed or implied.*

Certificate Identifier: SERTIT-111 C

Product Name: Ruckus Solution

Version and Release Numbers: See Certification Report

Type of Product: Network and Network-Related Devices and Systems

Product Manufacturer: Ruckus Wireless, Inc.

Assurance Type: CPP\_ND\_V2.0E and PP\_WLAN\_AS\_EP\_V1.0

Evaluation Criteria: Common Criteria Version 3.1 R4

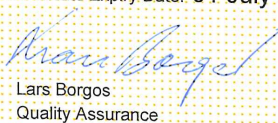
Name of IT Security Evaluation Facility: Advanced Data Security

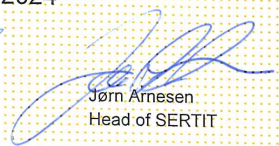
Name of Validation Body and Certification Authority: SERTIT

Certification Report Identifier: SERTIT-111 CR, issue 1.0, 01 July 2019

Certificate Issued Date: 01 July 2019 Certificate Expiry Date: 01 July 2024

  
Arne Høye Røge  
Certifier

  
Lars Borgos  
Quality Assurance

  
Jørn Arnesen  
Head of SERTIT



**SERTIT**

Norwegian Certification Authority for IT Security



CC Recognition Arrangement  
for cPPs or components up to  
EAL 2 and ALC\_FLR