Assessors Panel

CREST Certification Examinations
CREST Certified Wireless Specialist
Notes for Candidates

Issued by	CREST Assessors Panel
Document Reference	C-CWS-CN01
Version Number	1.1
Status	Public Release
Issue Date	23 April 2012
Review Date	1 July 2012

Table of Contents

Version History

Version	Date	Authors	Status
1.0	1st April 2012	Technical Committee and Assessors Panel	Public Release
1.1	23rd April 2012	Technical Committee and Assessors Panel	Update Release

Document Review

Reviewer	Position
Chair	Technical Committee / Assessors Panel
Chair	CREST Board

1 Introduction

1.1 Examination

The CREST Certified Wireless Specialist Examination has two components: a written component and a practical component. The two exam parts between them aim to cover all syllabus areas. The CREST Certified Wireless Specialist examination is only available to those who have previously passed one of the core CREST Certification exams. The CREST Wireless Specialist qualification is valid for three (3) years.

Success at the Certification Examination will confer upon candidates the status of one of the following:

1.1.1 CREST Certified Wireless Specialist (CCWS)

The (CCWS) examination tests candidates' knowledge and expertise in analysing wireless systems with a particular focus on 802.11 wireless networks.

1.2 Confidentiality

CREST takes the confidentiality of the Certification Examination very seriously. The retention or dissemination of data relating to the CREST Certification Examination (other than what is contained in the Notes for Candidates and Technical Syllabus documentation that is available from the CREST web site http://www.crest-approved.org/) is not permitted: along with their booking forms, candidates must also send a signed Non-Disclosure Agreement to this effect, or be prepared to sign a Non-Disclosure Agreement before they start the Certification Examination.

It should be noted that prior knowledge of specific Certification Examination configurations will be of little use to candidates, as the Examination is constantly updated and revised.

2 Examination Details (CCWS)

2.1 Format

The CREST Certified Wireless Specialist exam is made up of two sections, a multiple choice exam comprising of one hundred and twenty (120) questions, followed by a practical examination comprising of a number of practical tasks of varying levels of difficulty.

The practical component will comprise a series of stages, split into structured tasks to be carried out against the CREST Certification Wireless Specialist test rig. Please note that the practical components are not designed as replicas of “real world” engagements; rather, they are examinations whose aim is to test the skills and knowledge that security consultants will need to carry out effective security assessment engagements.

As noted above, stages and tasks are designed to examine fundamental testing skills; candidates will be required to complete all of them. Success at each question or task is based on an item or items of information that the candidate must retrieve, acquire or derive from the target systems. The practical components have, wherever possible, been designed so that success at each question or task should *generally* not depend on success at other questions or tasks, however in some cases where system compromise is required before access can be gained, limited “task chaining” will occur.

2.2 Timings

The exam is 3.5 hours in total. In order to allow the candidates maximum flexibility as to how to manage their time, initially the theory multiple choice exam will be conducted as a closed book test: we expect candidates to answer all the theory multiple choice questions at this point. As soon as the candidate notifies the invigilator they wish to start the practical the theory multi choice exam paper is removed and no more changes are allowed to be made.

The written component will last for approximately 1½ hours and the practical component will last for approximately 2 hours in total but the candidate is free to use as much or as little of their 3½ total examination time as they choose to work on the written exam components.

2.3 Open Book /Closed Book

The theory multiple choice part is a closed book test: candidates will not have access to reference material or the Internet for its duration. The practical test is an open book test: candidates will be permitted to use reference material and Internet access will be available.

3 Practical Exam - Specific Notes

3.1 CREST Certified Wireless Specialist (CCWS) Examination

The CCWS assessment been designed to provide the candidate with a series of generic exercises to find, assess and understand.

Candidates will be expected to demonstrate practical knowledge and expertise in the following areas:

Syllabus area	Syllabus area description
D2	**Bluetooth Common Vulnerabilities**
D3	**Bluetooth Common Uses**
E2	**RFID Common Vulnerabilities**
E3	**RFID Common Uses**
F2	**802.11 Networking Common Vulnerabilities**
F3	**802.11 Networking Common Uses**

For further information see the full Technical Syllabus.

Candidates will be expected to analyse network traffic covering these areas as directed by their candidate's worksheet, providing the results onto the supplied media for later review by the Invigilator.

3.2 Integrity Protection

Candidates will not be permitted to connect their test platforms to CREST's Internet connection, and any data transfer between the CREST Certification Network and the Internet will be by means of a USB flash drive supplied by the Invigilator. Any attempt to connect the candidate's test platform to the Internet via any means will be considered a breach of the CREST Certification Examination rules and will result in an instant fail decision. Any attempt to retain data relating to the CREST Certification Examinations either locally or by remote upload will be considered a breach of the CREST Certification Examination rules and will result in an instant fail decision. No refund of fees will be considered in these situations.

Note particularly that external media players such as iPods are not permitted in the Certification Examination, unless candidates are prepared to have these wiped (as with any other media used during the Examination). If you'd like to listen to music, put it on your hard drive.

3.3 Invigilation

A CREST assessor will be present throughout the day as Invigilator. The Invigilator is not there to assess candidates' capabilities: all assessment is via the objective written and practical components. However, the Invigilator will be able to answer any procedural questions that candidates may have, and assist in troubleshooting.

4 Marking Scheme / Pass Mark

The marking scheme is given in the tables below.

4.1 CREST Wireless Specialist

Component	Marks per question	Number of questions	Total Marks	Weight (%)
Written (multiple choice)	1	120	120	50%
Practical	Various	120	120	50%
Total			**240**	**100.0%**

Successful "Crest Certified Wireless Specialist" candidates must score two-thirds of the available marks in each component. That is:

- CCWS
  - at least **80 marks** from the **written component** (Multiple Choice), and
  - at least **80 marks** from the **practical component**.

This represents an overall pass mark of approximately 67%, but note **that candidates must score the minimum number of marks in each section: candidates who score very well in one component but not the others will not pass.**

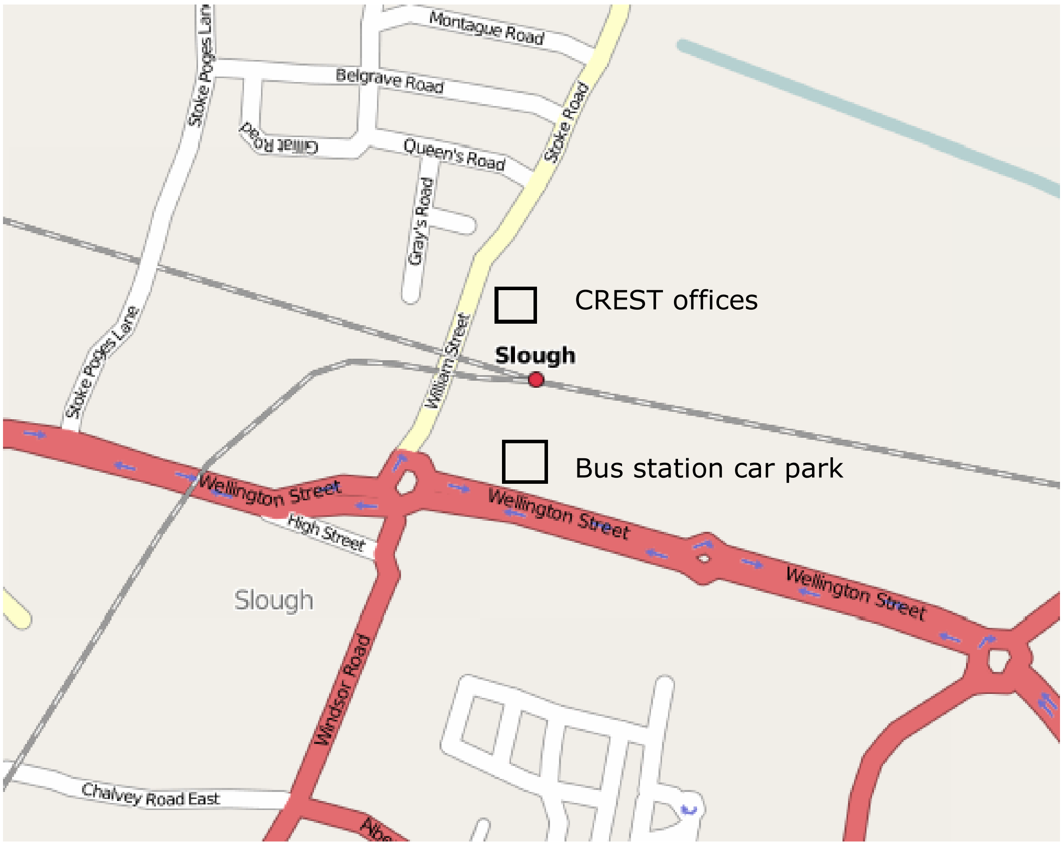
Unsuccessful candidates will be told their final scores in the written and practical components, along with feedback as to the general areas in which they fell short.

5 Examination Logistics

5.1 Location

The Certification Examination will take place at CREST's offices in Slough:

CREST (GB) Ltd
Abbey Business Centres
18-24 Stoke Road
SLOUGH
Berkshire
SL2 5AG



CREST's offices are approximately 10 minutes' walk from Slough train station: come out of the North entrance (from platform 5; not the main entrance), turn left on Railway Terrace and walk up to the main road, Stoke Road. Then turn right, cross over Stanley Cottages, and the CREST offices are in front of you on the right hand side.

Parking is available in the car park for Slough train station.

Full directions can be found online at http://www.abbeyoffices.com/ourlocations/slough/map/, or via Google Maps UK at http://maps.google.co.uk/maps?q=SL2+5AG.

5.2 Before the Certification Examinations starts

Before the Certification Examination starts, candidates will:

- **Have their NDAs collected**. This is to help us maintain the confidentiality of the Certification Examination.
- **Have their ID confirmed**.

5.3 CWS Timing

The general timings of a typical CREST Certification Examination day are as follows, although these should be taken as a guideline only. The only hard time limits are, as laid out above, 3½ hours to complete the exam overall.

Candidate 1
0900: Arrive
0915: Read through worksheet
0930: Start Exam
1300: Finish Exam

If candidates will be late (e.g. traffic problems / late-running trains), the Invigilator should be contacted on 0845 686 5542 as soon as possible.

5.4 Communication of Results

All written and practical component examination scripts will be marked independently will be completed within ten working days of the examination and where possible by the end of the week in which the candidate sits the examination. Results will communicated by letter to the candidate.

A list of all current CREST Consultants in good standing will be available from the CREST web site, http://www.crest-approved.org/.

5.5 Testing Platform Options

5.5.1 Introduction

As noted in previously, CREST takes the confidentiality of the content of the CREST Certification Examinations seriously: candidates are reminded that any attempt to retain data relating to the CREST Certification Examinations either locally or by remote upload will be considered a breach of the CREST Certification Examination rules and will result in an instant fail decision.

In order to help CREST maintain this confidentiality, we do not permit candidates to remove hard disks and writeable media that have been connected to the CREST Certification Network unless they have been securely wiped: we have the facility to do this.

Consequently, CREST requires all candidates to be able (and equipped) to remove their internal hard disk at the end of the exam so that it can be retained by CREST for erasure.

It is the candidate's responsibility to ensure that all disk BIOS passwords (also known as IDE or SATA passwords) are removed before surrendering the hard disk – failure to do so will mean that the disk cannot be erased and thus cannot be returned.

It should be noted that CREST are **UNABLE** to accept responsibility for candidate laptops and only the bare drive will be retained. It is the candidates' responsibility to ensure they are competent to remove the disk.

There is currently only one option available for test platforms.

5.5.2 Option 1: Use own laptop testing platform

Candidates must bring their own testing platform(s) (e.g. laptop with appropriate software toolkit) to the CREST offices.

Any test platform must have an RJ45 Ethernet connection capable of running at a minimum of 100Mbps, configured to obtain an IP address via DHCP.

Additionally, any test platform must be capable of reading from and writing to a USB key formatted with a FAT file system.

It is important to note that candidates choosing to use their own testing platform **must surrender their hard disk and any other writeable media for wiping at the end of the assessment process**. Hard disks, once wiped, will be returned to the candidates: we envisage that this will be **at the latest** within two weeks of completion of the certification examination.

6 Example questions (written component)

6.1 Multiple choice

An example multiple choice question is given below, along with the answer.

6.1.1 Question

Which of the following is NOT a valid DNS record type?

A. SOA – Start of Authority

B. NWS – News Server

C. CNAME – Canonical Name

D. MX – Mail eXchange

E. PTR - Domain Name Pointer

Candidates should clearly indicate their answer by circling the appropriate letter in their test script.

6.1.2 Answer

The correct answer is (B).

6.1.3 Marking scheme

Each multiple choice answer is worth one (1) mark. No points are deducted for incorrect answers.