1 Peer review – adsec03

Description	Max possible	Awarded
A Report structure	2	1
B Product description + design requirements	3	1
C Assumptions	3	1
D High-level architectural overview		
D1 General	4	2
D2 TOE and ST	5	1
E Security evaluation of design + summary		
E1 General	5	0
E2 Evaluation	4	0
Total:	26	6
Score:	8	2

1.1 Deduction motivations

General note: *The amount of whitespace used in this report in order to try to stretch it over the requirement (which it doesn't?) is really pushing it. Don't really know how this should be handled since the grading only says that; under 4.5 pages (lower-bound) or under 5.25 pages (higher-bound) is "not OK", is that failing the whole report or something else?*

Section only lists motivations for deductions to save space.

- **A** Really thin on information, but technically has all sections except summary (-1). Not clear how second assumption relates to security.
- **B** Vague environment description (-1). Missing requirements stated in project document (-1).
- **C** "out-of-hands-reach" assumption not referenced in security evaluation (-1). Authentication specified without assumption/specification (-1).
- **D1** No life-cykel management (-1). No TPM secret/auth values mentioned (-1).
- **D2** Unclear what "send the information to the user securely" entails (-1). TOE is a laundry-list of components without descriptions of relevant security impact (-2). ST is only a list of statements, no descriptions or reasoning (-1).
- **E1** No descriptions of the evaluation/threats except names in table (-2). Summary missing (-2). Final result/rational unclear (-1).
- **E2** Not covering all the stated threats (-2). SECURE BOOT not described in architecture (-2).