



---

## **PRODUCT ASSURANCE AT IL3 AND BELOW**

### **A. What is Product Assurance?**

1. HMG customers use product assurance as a mitigation for technical risks to their business activities. CESG operates a number of product assurance schemes which are intended to assure developers' products against certain criteria. Product assurance, therefore, is the act of independently validating that a product implements the security functions it claims to, that these functions represent effective mitigations for the perceived risks, and that the product is designed and developed to a sufficient level of quality to reduce the risk of an adversary successfully attacking the product.

### **B. Background:**

2. Historically, a number of product assurance schemes have developed which CESG either supports or runs in some capacity. Those HMG departments and agencies which handle data solely at IL3 and below have not traditionally seen themselves in a 'high security' environment, and, when combined with a lack of clear guidance on the use of assured products, have generally not required suppliers to deliver assured products in many of its business solutions. Vendors have subsequently been unsure where they should invest their own funds in terms of certification of their products, with the result that in many categories, HMG is undersupplied with products that have undergone appropriate independent assurance.

3. The most effective approach to building a secure business solution is through using products in which we have gained confidence. By failing to supply HMG with a sensible selection of assured products we place HMG data at unnecessary risk, as it is protected by products of unknown provenance and quality, configured and operated without a detailed understanding of their security properties, and included in system architectures without sufficient knowledge of their relative strengths and weaknesses.

4. Our defender's dilemma is that we must defend all avenues of attack – whereas the adversary need only find one way in. When we assume that products defend attacks without evidence to justify that assumption, we make the attacker's job far easier.

## NOT PROTECTIVELY MARKED

5. CESA currently operate or recognise a suite of assurance schemes which have developed organically to solve particular assurance requirements. These do not necessarily represent a coherent whole, and do not always align well with each other – for example, there is no easy way for work performed under one scheme to be used to reduce work in another. Nor is there clarity amongst customers as to when to require certificates from each scheme.

### C. What is Proposed?

6. CESA proposes a series of fundamental changes and improvements to the way HMG approaches product assurance for IL3 and below. The first is a direct change in the way product evaluation works – rather than assure a product as being suitable for protecting a particular business impact level, CESA will instead approve products as being suitable for mitigating certain categories of threats to business. The impact level of data does not accurately capture the real risk to that information – the IL3 emails the Foreign Secretary receives are under much greater risk than the IL3 emails that a local authority worker handles. We seek to address this disparity and ensure that suitably robust products are available for both, balancing the higher cost of operational and developmental security against those higher threat environments, a methodology already employed in the IS1 segmentation model.

7. It is proposed that a two-tier model is adopted, in which HMG customers determine the approximate threat to their data based on the nature of the data itself. Using questions such as *‘is this data of international interest?’* and *‘would serious / organised crime find value in this information?’* information asset owners will be able to identify which tier their data is in Tier A (higher threat) or Tier B (lower threat)<sup>1</sup>. They will then be able to select products which have been evaluated against defined threat models for each tier.

8. Security characteristics for classes of security product will be investigated and defined by CESA’s research area, using the defined threat models to guide their work and illustrate how the proposed types of technical mitigations in products actually solve the threats to Tier A or Tier B data. Importantly, Tier B is a subset of the threats to Tier A, and so Tier A products would also be suitable for the protection of Tier B data – and indeed Tier B products may also be suitable for the protection of Tier A information, if used or deployed in a different way.

9. In addition to security characteristics, CESA will also develop ‘build standards’ for all security products, which will describe those qualities and criteria which are not product category specific. These will cover elements of engineering rigour such as

---

<sup>1</sup> The names ‘Tier A’ and ‘Tier B’ are working titles to illustrate the concept.

## NOT PROTECTIVELY MARKED

configuration control, flaw remediation etc, and describe those requirements which are again required to mitigate the threat to HMG data.

10. Importantly, CESC, as the National Technical Authority for Information Assurance will set the standards for, and operate, this national product evaluation scheme, using our unique knowledge of the threats to HMG data to develop and maintain the important threat models and security characteristics for products.

11. We propose simplifying HMG policy around the use of assured products, to ensure a robust market for vendors, and to encourage departments to differentiate between products on characteristics other than price. CESC will re-examine all product assurance schemes it operates and look to rationalise them wherever possible. Transition plans for products previously evaluated under these schemes will be developed to ensure their continued suitability. We will also look in more detail at how we might make use of evidence generated by external schemes, such as FIPS-140/2 and Common Criteria, where it is available.

12. The Assurance Framework – intrinsic, extrinsic, operational and implementation – will be the basis for this new approach to product assurance. Product evaluation will take explicit account of lifecycle assurance issues – ensuring a product remains secure throughout its deployed life within HMG – and a vendor's approach to development security. CESC will investigate the provision of a scheme by which individual developers or product teams can prove their security engineering competence, which will lead to increased trust in the deliverables provided, and hence reduced costs and timescales for the evaluation effort.

13. Lifecycle assurance activities move from repeated and costly full reassessments to a trust-and-verify model, with spot check audits. This will require vendors to develop with CESC an assurance maintenance plan in advance of their product's certification, which will detail the involvement CESC will need to have with different types of changes to their product in the future, and those changes that the vendor acknowledges will require additional evaluation effort.

14. CESC will also take this opportunity of reassessing product assurance schemes to examine the commercial implications of many of the changes outlined in this paper, and to ensure that the funding models for assurance and assurance maintenance remain appropriate.

15. A forum for senior users of assured products, such as HMG CIOs, will also be developed, with the intention they can learn more about the evaluation process and guide its development; acting as a trusted friend to CESC, advising on future product assurance developments, and representing a forum for CESC and HMG customers to discuss the rationale behind assurance decisions.

16. In addition a suite of improvements and business change activities for the product assurance area, and CESC as an integrated business, are proposed. These are

3 of 4

CESG is part of Government Communications Headquarters

This information is exempt under the Freedom of Information Act 2000 (FOIA) and may be exempt under other UK information legislation. Refer any FOIA queries to GCHQ on 01242 221491 x30306 or [infoleg@gchq.gsi.gov.uk](mailto:infoleg@gchq.gsi.gov.uk)



NOT PROTECTIVELY MARKED



INVESTMENT IN PEOPLE

## NOT PROTECTIVELY MARKED

separate activities which could occur at any time, but we believe that the right time to introduce these is whilst the whole evaluation process is undergoing a revamp. These changes will help increase the professionalization of the evaluator community and improve the tools and training available to them. Opportunities are also identified for improving the service we offer to customers – vendors, HMG users, system integrators and managed service providers – helping to inform them about our product assurance approach, and the value it brings to their information risk management process.

17. During the transition-planning period, all of the CESG Assurance schemes will continue to operate under their agreed Terms and Conditions. There are no current plans to close any existing schemes without offering clear transition arrangements to viable replacement services. Evaluations and Tasks that are currently being undertaken, will continue as planned to achieve to their appropriate completion. It is CESG's current intention that all certifications from existing schemes will continue to be valid as designated by CESG.