**Summary of [Name] comments on Thales/Gemalto merger**
**September 2018**

- [Name] is an end user of many different types of HSMs across its operations.

- [Name] is reliant on HSMs to develop its innovations and services, and to ensure it and its customers can securely communicate and retain sensitive data across all areas of business.

- [Name] presently acquires HSMs for its worldwide operations from both Gemalto and Thales; its experience is that Gemalto and Thales units are by far the best-known and highest-performing HSMs in the market.

- [Name] utilises both Gemalto and Thales devices, so as to avoid supplier dependence and maximise its commercial leverage.

- [Name] is very concerned that, if the proposed acquisition proceeds, the merged entity will:

    - have the ability and incentive to withhold supply of HSMs to [Name], or to significantly increase the price for those HSMs in New Zealand.

    - Increase prices to, or reduce choice and innovation for, customers of HSMs like [Name], as there is no threat of marketplace constraint due to the high barriers of entry for new participants.

- Many [Name] products depend on the secure communication and retention of highly-sensitive personal information. A fundamental element of protecting such sensitive data is the hardware which protects the information in question. This information is typically encrypted and protected by a physical security device known as an HSM.

- A fundamental element of protecting such sensitive data is the hardware which protects the information in question. This information is typically encrypted and protected by a physical security device known as an HSM.

- [Name] sees the two merging firms as by far the leading global suppliers of HSMs, in terms of product quality, range width, applications, performance, technology, brand and reputation.

- [Name] estimates that the merger parties' combined share of HSMs worldwide is 50-65% in Europe and about 60% globally, with each rival far behind that figure. It expects the figures in New Zealand would align with those global shares.

- Both Thales and Gemalto supply net HSM and card HSM units, which represent the majority of [Name]'s needs. [Name] frequently solicits offers from both suppliers for its requirements, as well as for recurring yearly support for devices once in-service.

- More generally, [Name]'s experience is that it is too risky to have a sole supplier of HSMs. HSMs are business critical infrastructure, and [Name] has an array of different solutions which require various types and qualities of HSMs. [Name] is presently able to source from both Thales and Gemalto to avoid sole-supplier dependency risk. [Name] believes that many other HSM end users likewise generally adopt a dual-supplier strategy for HSMs, to ensure redundancy and avoid undue reliance on a single supplier.

- [Name] has consistently found Thales and Gemalto to be head and shoulders above all other offerings for its requirements. [Name] does not know of any other suppliers as efficient and credible against these criteria as Thales and Gemalto.

- [Name] does not purchase HSM aaS. It does not believe that HSM aaS or other cloud-based key management solutions are a satisfactory alternative to the dedicated physical Thales and Gemalto net HSMs described above. The use of any cloud-based service requires the communication of sensitive information which introduces risk and enlarges the attack surface. Indeed, [Name]'s clients will typically not accept solutions based on HSMs deployed in the cloud or in which HSM hosting is delegated.

- [Name] also sees high barriers to entry in this market, making it unlikely that a new entrant or expanding firm would emerge to challenge the merged entity within the next 3 to 5 years:

    - **Product range width:** A supplier must be able to offer the widest possible range of products (HSM cards, portable HSM and net HSM) to constitute a credible alternative.

    - **Security reputation paramount:** Not all suppliers are equal in security terms, even if they have reached the same certification. For example, having the secrets kept inside the HSM, or having them encrypted on an external disk, is not the same approach even if both ostensibly meet the certification requirements.

    - **High capital requirements:** HSM production is technically complex and it is difficult to ensure the digital (crypto) and physical security of HSM (such as heat problems inside the tamper-proof case) and requires important investments. For these reasons, HSM development requires significant R&D expenditure to achieve high security.

    - **Certification hard to obtain:** HSM are certified by internationally recognized standards such as Common Criteria (in the EU) or FIPS (in the US) to provide users with independent assurance that the design and implementation of the product and cryptographic algorithms are sound. [Name]'s marketplace experience is that customers are increasingly requiring higher levels of certification, which is a long and costly process. Furthermore, a broad array of diverse auditing and certification scheme exists in different national industries.

    - **Customers are sticky once committed to a HSM brand:** Once an HSM is supplied and installed, the cost to that customer of switching supplier for the relevant HSM applications is high both in investment time and potential exposure to security breaches. In many cases the entire module must be replaced.

- Overall, [Name] sees no real possibility of new entry in the HSM market, given high entry barriers such as high capital investments, the fact that the market is highly consolidated and in view of the consumer expectations of security reputation and trust in HSM products and suppliers.