

**THALES**

**Application for clearance of a  
business acquisition under s66 of  
the Commerce Act 1986**

Proposed acquisition by Thales S.A. of shares  
in Gemalto N.V.

31 July 2018

# Table of Contents

<b>Part A – Executive Summary</b>	<b>4</b>
Parties	4
Proposed Transaction	4
Overlaps Between the Parties	4
Relevant Markets	5
Counterfactual	5
No Substantial Lessening of Competition for Enterprise Key Management Market	6
No Substantial Lessening of Competition for Enterprise Encryption Software Market	6
<b>Part B – The Parties</b>	<b>8</b>
Acquiring Party	8
Selling Party	8
<b>Part C – Transaction Details</b>	<b>9</b>
Proposed Transaction	9
Rationale for the Proposed Transaction	10
Other Competition Agencies Being Notified	10
Related Transactions	11
<b>Part D – Horizontal Overlap</b>	<b>12</b>
Activities of the Parties to the Proposed Transaction	12
Relevant Overlaps Between the Parties	15
Required Documents / Information	17
<b>Part E – Market Definition</b>	<b>18</b>
Overview of Relevant Markets	18
Enterprise Key Management Market	18
Enterprise Encryption Software Market	22
<b>Part F – Counterfactual</b>	<b>24</b>
<b>Part G – The Industry</b>	<b>25</b>
Overview of Enterprise Data Security and Encryption	25
Enterprise Key Management Products Provided by the Parties	31
Other Industry Participants in Enterprise Key Management	35

Enterprise Encryption Software Products Provided by the Parties	41
Other Industry Participants in Enterprise Encryption Software	43
Recent Merger Activity	45
<b>Part H – Competition Assessment for Enterprise Key Management Market</b>	<b>46</b>
Market Shares	46
Constraint from Existing Competition	50
Constraints on the Merged Entity Post-Acquisition from Potential Competition	53
Countervailing Power from Customers	54
Risk of Coordination Post-Acquisition is Low	55
No Lessening of Competition Even if Market is Limited to Payment HSMs and GP HSMs Only	55
Conclusion	56
<b>Part I – Competition Assessment for Enterprise Encryption Software Market</b>	<b>57</b>
Market Shares	57
Constraints from Existing Competition	59
Constraints on the Merged Entity Post-Acquisition from Potential Competition	60
Countervailing Power from Customers	60
Risk of Coordination Post-Acquisition is Low	61
Conclusion	61
<b>Part J – Confidentiality</b>	<b>62</b>
<b>Part K – Declaration</b>	<b>63</b>
Appendix 1 – Transaction Documents	64
Appendix 2 – Corporate Structure Charts	65
Appendix 3 – Audited Financial Statements and Annual Report	66
Appendix 4 – Total Sales Revenues	67
Appendix 5 – New Zealand Competitors and Industry Associations	68
Appendix 6 – Key Customers	70
Appendix 7 – Methodology and Sources of Market Share Data	73
Appendix 8 – Third Party Market Studies	75
Appendix 9 – Overview of Competing Global Players with Enterprise Key Management Capabilities	76
Appendix 10 – Recent Entrants in the Key Enterprise Management Market	79
Appendix 11 – Glossary	81

## Part A – Executive Summary

1. Thales S.A. (**Thales** or **Thales Group**) is applying for clearance from the Commerce Commission to acquire all issued and outstanding ordinary shares of Gemalto N.V. (**Gemalto**) (together, the **Parties**). The proposed acquisition is part of a global merger, which would include Thales acquiring ownership of Gemalto's operations in New Zealand. This clearance application relates to the proposed acquisition to the extent that it affects New Zealand.

### Parties

2. Thales is an international electronics and communications group that is registered in France and listed on the Euronext Stock Exchange in Paris. It is globally active in five main areas: (i) aeronautics, (ii) space, (iii) ground transportation, (iv) defence and (v) security.
3. Gemalto is an international digital security company registered in the Netherlands and listed on the Euronext Stock Exchange in Paris and Amsterdam. Gemalto is active globally in the development, manufacture or supply of, or the provision of services relating to, data encryption and security technologies and communications systems.

### Proposed Transaction

4. The proposed transaction involves the acquisition of all issued and outstanding ordinary shares of Gemalto by Thales (**Proposed Transaction**) by way of a full public offer subject to the terms and conditions of a Merger Agreement dated 17 December 2017 (the **Merger Agreement**). The Proposed Transaction will result in Gemalto becoming a subsidiary of Thales.

### Overlaps Between the Parties

5. The Proposed Transaction involves the merger of Thales' and Gemalto's highly complementary businesses. Thales is primarily active in aeronautics, space, ground transportation, defence and security, while Gemalto provides secure personal solutions, including smart cards, identification documents, and biometric solutions – with horizontal overlaps at the global level only in the data security space and, in particular, in the enterprise encryption software and enterprise key management markets.
6. Data security is broadly part of both Parties' enterprise cyber security offerings – yet even there the Parties' activities are complementary. While Thales focuses only on software encryption and enterprise key management, Gemalto supplies a wider range of products including strong authentication and software monetisation.
7. The Parties' operations only overlap to a very limited extent in New Zealand, in relation to the supply of:
  - 7.1 Enterprise key management; and
  - 7.2 Enterprise encryption software for data at rest and data in use.

8. Together these overlaps at the global level make up just [ ] of Thales' and [ ] of Gemalto's 2017 global revenues – and they are just a small part of the Parties' overall businesses.

9. In terms of the scale of the Parties' operations in these overlap areas in New Zealand, it is very small. In 2017 the Parties had combined revenue in enterprise key management (including maintenance) in New Zealand of only approximately [ ] (Thales: [ ] and Gemalto: [ ]). The Parties had combined revenue for enterprise encryption software in New Zealand for 2017 of only approximately [ ] (Thales [ ]; Gemalto [ ]). [ ]

].

10. As regards what enterprise encryption and key management entails, encryption involves the transformation of electronic data, programs, images or other information (plain text) into a format that is not understandable by a person or a computer (cipher text). Encryption requires the use of an encryption algorithm and at least one encryption key. Encryption keys in turn need to be managed across their life cycle. This key management activity includes in particular key generation, registration, storage, distribution, installation, use, rotation, backup, recovery, revocation, suspension and deletion. The growing use of encryption in recent years has led to a proliferation of keys within organisations, such that it is not uncommon for enterprises to use thousands, if not hundreds of thousands, of keys (or more) in their daily businesses. This in turn has increased the need for efficient key management.

### Relevant Markets

11. The Parties consider that the relevant markets in this case are:

11.1 The global market for the supply of enterprise key management products and associated maintenance services (the **Enterprise Key Management Market**). The Enterprise Key Management Market includes the supply of both payment hardware security modules (**Payment HSMs**) and general purpose hardware security modules (**GP HSMs**); and

11.2 The global market for the supply of enterprise encryption software for data at rest and in use (the **Enterprise Encryption Software Market**).

12. Even if the Commission takes the view that it must define national New Zealand markets for the supply of enterprise key management products and associated maintenance services, and for the supply of enterprise encryption software for data at rest and in use, then overseas suppliers will still exercise a competitive constraint on the participants in that market. Therefore the global position of the Parties and their competitors remains relevant and information on the global markets is included in the competition assessment.

### Counterfactual

13. The Parties consider that, in the absence of the Proposed Transaction, it is likely that Gemalto will continue to operate as an independent supplier in the relevant markets. [ ]

].

#### **No Substantial Lessening of Competition for Enterprise Key Management Market**

14. The market is highly competitive: The Parties compete fiercely with a large number of other global suppliers across a range of key management solutions. There are at least 60 other suppliers including, among many others, Atos, IBM, Micro Focus, Microsoft, Utimaco and Ultra Electronics. [

].

15. The Parties are not uniquely close competitors: While the Parties are both traditional vendors of HSMs with similar solution designs, they do not pose a unique competitive constraint on each other. The Parties' products have different strengths in terms of functionalities and capabilities, and customers have a wide variety of solutions offered by rival vendors to choose from.

16. The market is highly dynamic and there are low entry barriers: The market for key management solutions has grown rapidly in recent years (estimated at 20% per annum in the last three years) and will continue to do so for the foreseeable future. Customers can choose from a wide range of solutions (such as HSMs aaS and other cloud-based key management solutions and integrated solutions), and options are expected to continue to broaden as new solutions are developed leveraging technologies such as trusted platform modules (TPMs) embedding microprocessors with built-in key management capabilities and multi-party computational software. Low barriers to entry are demonstrated by numerous new entrants globally in recent years including Box, Cavium, Commvault, Device Authority, Equinix Telecity, Fernetix, Fortanix, Infineon, Intel, KeyNexus, NyCypher, PKWARE, Salesforce, Securosys, Sophos, Unbound and Venafi.

17. Customers exert significant constraint on suppliers: Customers are typically highly sophisticated with a clear understanding of their key management and data protection requirements. They can and do switch products and providers readily. Some customers are in a position to sponsor entry. The Parties are further constrained by resellers and system integrators who assist customers in selecting the best solution for their needs and are not tied to a particular supplier.

#### **No Substantial Lessening of Competition for Enterprise Encryption Software Market**

18. The market is highly competitive: [
- ]. There are at least 30 other suppliers competing fiercely for customers globally. These include large, well-established players like Dell EMC, IBM, McAfee and Symantec, fast-growing Cloud powerhouses including AWS, Google and Microsoft Azure, and innovative new entrants like Cloudera, Hashicorp, Ionic Security and Skyhigh. As noted above, the Parties' New Zealand revenues are [

].

19. The Parties are not uniquely close competitors: The Parties are small players in a fragmented market and do not view each other's offerings as particularly close substitutes. All other competing solutions offer largely similar levels of performance, functionality and customer support to the Parties.

20. Customers can readily switch: Most customers are sophisticated buyers with a clear understanding of their data protection requirements and can and do switch easily. Switching is facilitated by resellers who help customers identify and source the right products from a range of suppliers.
  
21. The market is highly dynamic and there are low entry barriers: The market is fast growing and there are numerous examples of entry in recent years. These include, among others, Baffle, Couchbase, DataLocker, DataStax, GCHQ, Google Cloud Platform, HashiCorp, Hortonworks, Ionic Security, Netskope, Protegrity, Pure Storage, SaltStack, Secomba, Sophos and TokenEx. There are no material regulatory barriers to entry. Entry is facilitated by the growing use of open-source encryption software, the lack of need for expensive manufacturing facilities or IP licences, and the limited need for local sales forces.

## Part B – The Parties

### Acquiring Party

22. The acquirer is Thales, or any of its interconnected bodies corporate.

23. This notice is given by:

Thales S.A.  
Tour Carpe Diem  
31 Place des Corolles – CS 20001  
92098 Paris la Defense Cedex  
FRANCE

**Attention:** Isabelle Simon  
Group Secretary and General Counsel  
Telephone: +33 1 5777 8645  
Email: isabelle.simon@thalesgroup.com

### Selling Party

24. The seller is Gemalto. Its contact details are:

Gemalto N.V.  
6 Rue de la Verrerie  
Meudon, Ile-de-France 92197  
FRANCE

**Attention:** Marc Bergmann  
Senior Vice-President & General Counsel of M&A  
Telephone: +33 1 5501 6080  
Email: marc.bergmann@gemalto.com

25. All correspondence and notices to Thales and Gemalto in respect of this application should be directed in the first instance to:

Simpson Grierson  
Lumley Centre  
88 Shortland Street  
Private Bag 92518  
Auckland 1010  
NEW ZEALAND

**Attention:** James Craig / Nina Blomfield  
Telephone: (09) 977 5125  
Mobile: (021) 497 713  
Email: james.craig@simpsongrierson.com  
nina.blomfield@simpsongrierson.com



## Part C – Transaction Details

### Proposed Transaction

26. The Proposed Transaction involves the acquisition of all the issued and outstanding ordinary shares of Gemalto by Thales by way of a full public offer subject to the terms and conditions of the Merger Agreement. A copy of the Merger Agreement is attached at **Appendix 1**.
27. Under the Merger Agreement, Thales and Gemalto agreed to combine their businesses by way of a recommended full public offer in respect of all issued and outstanding ordinary shares of Gemalto to be made by or on behalf of Thales. The Parties have agreed that the price payable by Thales for each share shall be a consideration of €51 in cash, subject to any relevant reduction less any applicable withholding tax payable under mandatory law.
28. [
- ].
29. The Proposed Transaction will consist of the following steps, some of which have already been implemented:
- 29.1 A draft public tender offer was filed with the Dutch Financial Market Authority on 1 February 2018 and approved on 26 March 2018;
- 29.2 The offer document was made available to the public on 27 March 2018 and the acceptance period was initiated on 28 March 2018. The acceptance period, which was initially scheduled to end on 6 June 2018, was extended until 15 August 2018, and may be further extended subject to the Dutch Financial Market Authority's authorisation;
- 29.3 [
- ].
30. [
- ].
31. The Proposed Transaction is subject to the satisfaction or waiver of customary conditions, including but not limited to:
- 31.1 regulatory approvals;
- 31.2 a minimum acceptance level of at least 67% of Gemalto Shares;
- 31.3 no material adverse effect having occurred;
- 31.4 no material breach of the Merger Agreement having occurred; and
- 31.5 no superior offer having been made or agreed upon.

32. The Proposed Transaction is expected to close during the second half of 2018.

**Rationale for the Proposed Transaction**

33. Thales' core business is the powering of its customers' critical decision chains in its five vertical markets: aeronautics, space, ground transportation, defence, and security.

34. Thales is positioning itself as its customers' key strategic partner in their digital transformation, and thus in managing their critical decision chains. Thales has identified four key digital technologies to support this digital journey: connectivity, cyber security, big data and analytics, and artificial intelligence.

35. In the last three years, Thales has significantly increased its focus on digital technologies, investing over €1 billion, including with the acquisitions of Vormetric and Guavus, and the creation of a joint venture with Sysgo. The current Transaction will now allow Thales to further accelerate the development of its digital strategy by reinforcing Thales' digital offering across its five vertical markets [

]. Combined with Gemalto's diverse digital security portfolio, Thales will be ideally positioned to power its customers' full digital decision chains, which will continue to be foundational in ensuring the safety and security of critical solutions.

36. The Proposed Transaction will thus put Thales in a better position to compete for new opportunities in the fast-growing data security space by providing enterprises and governments with a seamless response to the data security challenges that lie at the heart of their digital transformation.

37. [

].

**Other Competition Agencies Being Notified**

38. The Proposed Transaction is conditional on receipt of regulatory approvals and other customary closing conditions. In particular, completion of the Proposed Transaction is conditional on receipt of merger clearance in a number of jurisdictions, including New Zealand [ ]. The table below sets out the current status of merger filings in jurisdictions outside of New Zealand.

[ ]	[ ]
[ ]	[ ]
[ ]	[ ]
[ ]	[ ]
European Union	Filed on 18 June 2018
[ ]	[ ]

[ ]	[ ]
[ ]	[ ]
[ ]	[ ]
[ ]	[ ]
[ ]	[ ]

**Related Transactions**

39. There are no related transactions between Thales and Gemalto affecting New Zealand.

## Part D – Horizontal Overlap

### Activities of the Parties to the Proposed Transaction

#### *Thales*

40. Thales is an international electronics and communications group registered in France and listed on the Euronext Stock Exchange in Paris. Thales provides systems and electronic services globally in five main areas:
- 40.1 aeronautics;
  - 40.2 space;
  - 40.3 ground transportation;
  - 40.4 defence; and
  - 40.5 security.
41. Thales e-Security (**TeS**) is part of the Thales Group, and provides organisations with solutions to protect and manage their data, identities and intellectual property and to meet regulatory compliance. This includes encryption, advanced key management, tokenisation, privileged user control and meeting standards of certification for high assurance solutions.
42. In 2017, the Thales Group had global revenues of [ ] ([ ] of which were from New Zealand), operations in 56 countries and 64,100 employees.
43. Thales has been present in New Zealand for over 20 years and has two offices in Auckland and one office in Wellington ([ ]).
- Its key operations in New Zealand are in three areas: transport, defence and air traffic management.
- 43.1 In transport, Thales developed and delivered a multi-modal and multi-operator ticketing system for Auckland and the Auckland Regional Transport Authority (the AT Hop Card). The system provides Auckland transport customers with seamless movement between trains, buses and ferries using one smartcard ticket.
  - 43.2 In defence, Thales is a longstanding partner of the New Zealand Defence Force. It provides equipment, systems and services to increase operational effectiveness as well as ensuring the highest levels of protection. Thales designs systems for all types of aircraft, naval vessels and land platforms. Its key capabilities are:
    - 43.2.1 Surveillance, detection and intelligence systems: Thales' systems provide all levels of the command and intelligence chain with the most comprehensive understanding of the theatre of operations.
    - 43.2.2 Communication, command and control systems: Thales' systems provide the capability and capacity to transmit secure information to each level of the command chain, a tactical and strategic imperative to meet the requirements of armed forces and security forces.

**43.2.3** Protection systems and mission/combat systems: Thales supports governments as they seek to modernise their force protection, territorial protection and high value asset protection systems, and helps to ensure the highest possible levels of operational effectiveness and precision.

**43.2.4** Mission services and support: After these systems are delivered and integrated, Thales continues to work alongside its customers to provide innovative and extended service solutions – training, lifecycle support, repairs, guaranteed levels of operational availability, upgrades and more. Thales provides a wide range of systems and equipment for the New Zealand Defence Force, supporting personnel in safely conducting their tactical missions. This includes encryption devices, friend or foe identification capabilities, secure tactical radio technology, thermal imaging equipment, electro-optics for the Light Armoured Vehicles, Steyr rifles and small arms ammunition to the New Zealand Army.

**43.3** In air traffic management, Thales (then known as Thomson CSF) won the contract in 1993 to deliver New Zealand's first fully computerised air traffic control centre. Consisting of a fully computerised air traffic control centre, radars across nine sites, air navigation systems and all instrument landing equipment, this program represented one of the most significant investments in air safety in New Zealand's history. Thales continues to provide control radar, en-route radar and secondary radar at multiple sites throughout New Zealand and recently upgraded the radar systems to allow for satellite navigation at 13 locations around the country.

**44.** In addition to these key areas:

**44.1** Thales provides encryption and secure communications technologies supporting electronic transactions in New Zealand; and

**44.2** Thales is the world's second largest provider of simulation-based training solutions for civil, military aircraft and helicopter pilots, and supplies and supports Air New Zealand with full-flight simulators.

**45.** In 2017, Thales' total revenue in New Zealand in relation to the supply of enterprise key management products and associated maintenance services was approximately [ ] (or around [ ] of Thales' total 2017 revenue in New Zealand). Its total revenue in New Zealand in relation to the supply of enterprise encryption software for data at rest and in use was [

].

**46.** Additional information on Thales and its business can be obtained from its website at <https://www.thalesgroup.com/en/countries/asia-pacific/new-zealand>, and its 2017 Registration Document.<sup>1</sup>

<sup>1</sup> Thales' 2017 Registration Document is available at: [https://www.thalesgroup.com/sites/default/files/asset/document/2017\\_registration\\_document.pdf](https://www.thalesgroup.com/sites/default/files/asset/document/2017_registration_document.pdf)

## Gemalto

47. Gemalto is an international digital security company registered in the Netherlands and listed on the Euronext Stock Exchange in Paris and Amsterdam. Gemalto is active globally in six main areas:
- 47.1 mobile platforms and services;
  - 47.2 mobile embedded software and products;
  - 47.3 payment;
  - 47.4 government programs;
  - 47.5 machine to machine (IoT); and
  - 47.6 enterprise security.
48. In 2017, Gemalto had global revenues of approximately €3 billion ([ ]), operations in 47 countries and 15,000 employees.
49. The majority of Gemalto's activities in New Zealand relate to the sale of smart cards (mainly SIM cards and payment cards) and related products and services. Such activities account for over [ ] of Gemalto's overall sales in New Zealand. The remainder of Gemalto's New Zealand activities relate mainly to the sale of machine-to-machine (**M2M**) modules and data security products. In New Zealand, Gemalto's operations are run out of an office in Auckland and include activities in the following main areas:
- 49.1 Mobile: Gemalto supplies a range of solutions to mobile network operators and telecommunications equipment vendors, including mainly SIM cards and associated products and services.
  - 49.2 Banking and Payment: Gemalto provides a range of banking and payment solutions to financial institutions, including payments cards and personalisation services.
  - 49.3 Machine-to-machine and IoT: Gemalto offers a broad portfolio of M2M and IoT solutions and services.
  - 49.4 Government: Gemalto is active in the manufacture and supply of secure identification documents and materials for government applications.
  - 49.5 Enterprise security: Gemalto provides a wide range of solutions that help organisations protect and secure their data, and maximise the uptake and profitability of their software. In New Zealand, this includes software monetisation solutions, enterprise key management solutions, and enterprise encryption software.
50. For enterprise key management in New Zealand, Gemalto sells the SafeNet Luna (SafeNet Luna Network and SafeNet Luna USB) and Protect Server lines of its GP HSMs, and SafeNet Luna EFT Payment HSM.
51. In 2017, Gemalto's total revenue in New Zealand in relation to the supply of enterprise key management products and associated maintenance services was approximately [ ]. Its total revenue in New Zealand in 2017 in relation to the

supply of enterprise encryption software for data at rest and in use was approximately [ ]. [ ].

52. Additional information on Gemalto and its business can be obtained from its website [www.gemalto.com](http://www.gemalto.com) and its 2017 Annual Report.<sup>2</sup>

### Relevant Overlaps Between the Parties

53. The Proposed Transaction involves the merger of Thales' and Gemalto's highly complementary businesses. Thales is primarily active in aeronautics, space, ground transportation, defence and security, while Gemalto provides secure personal solutions, including smart cards, identification documents, and biometric solutions.

54. Data security is broadly part of both Parties' enterprise cyber security offerings – yet even there the Parties' activities are complementary. While Thales focuses only on software encryption and enterprise key management, Gemalto supplies a wider range of products including strong authentication and software monetisation.

55. Within the data security space, the Parties' specific horizontal overlaps in New Zealand are limited to:

55.1 enterprise key management; and

55.2 enterprise encryption software for data at rest and in use ([ ]).

56. Together these overlaps at the global level make up just [ ] of Thales' and [ ] of Gemalto's 2017 global revenues – and are just a small part of the Parties' overall businesses.

57. For completeness, the Parties note that their global operations overlap in two other areas that do not have any direct effect on New Zealand. They are briefly described below but are not otherwise discussed in this application:

57.1 Security evaluation labs: Both Parties provide security testing and evaluation services from their labs in France. There are no such labs operated by the parties in New Zealand.

57.2 Enterprise network encryptors for data in motion (noting the Parties do not provide encryption software for data in motion): Increasingly, data must be sent from one location to another over public networks. To protect such communications, this "data in motion"<sup>3</sup> is encrypted before transit between the originating and receiving location to avoid data loss from attacks during transit. [ ].

2 Gemalto's 2017 Annual Report is available at:

<https://www.gemalto.com/investors-site/Documents/2018/Annual-report-2017.pdf>.

3 The term "data in motion" is further explained below at para. 120 onwards.

## *Enterprise Key Management*

- 58.** As is explained further below, encryption involves the transformation of electronic data, programs, images or other information (plain text) into a format that is not understandable by a person or a computer (cipher text). Encryption requires the use of an encryption algorithm and at least one encryption key. Encryption keys in turn need to be managed across their lifecycle. This key management activity includes, in particular, key generation, registration, storage, distribution, installation, use, rotation, backup, recovery, revocation, suspension, and deletion.
- 59.** The growing use of encryption in recent years has led to a proliferation of keys within organisations, such that it is not uncommon for enterprises to use thousands, if not hundreds of thousands, of keys (or more) in their daily businesses. This in turn has increased the need for efficient key management.
- 60.** Thales is active in offering three types of enterprise key management products:
- 60.1** GP HSMs with Thales' nShield lines;
  - 60.2** Payment HSMs with its payShield lines; and
  - 60.3** Encryption software/hardware with key management capabilities with its Vormetric encryption products.
- 61.** Thales' enterprise key management activities generated worldwide sales of [ ].
- 62.** Gemalto is active in offering four types of enterprise key management products:
- 62.1** GP HSMs with its SafeNet Luna and ProtectServer product lines as well as the SafeNet Crypto Command Center;
  - 62.2** Payment HSMs with its SafeNet Luna EFT product line;
  - 62.3** HSMs as a Service (**HSMs aaS**) with its Data Protection On Demand product (**DPoD**); and
  - 62.4** Encryption software/hardware with key management capabilities with SafeNet KeySecure and SafeNet Virtual KeySecure.<sup>4</sup>
- 63.** Gemalto's enterprise key management activities generated worldwide sales of [ ].

## *Enterprise Encryption Software*

- 64.** The process of encryption and decryption of data (using an encryption algorithm and encryption keys) is performed by encryption software.
- 65.** Thales is active globally in enterprise encryption software, offering the following products: Vormetric Transparent Encryption, Vormetric Transparent Encryption and

<sup>4</sup> For a more detailed overview of Thales' and Gemalto's enterprise key management products see Part G below.



Vormetric Protection for Teradata Database, Vormetric Application Encryption, Vormetric Tokenization and Data Masking, Vormetric Batch Data Transformation, and Static Data Masking products.

66. Thales' activities in enterprise encryption software generated worldwide sales of [                    ]. In New Zealand, Thales' enterprise encryption software revenues were [                    ].
67. Gemalto is also active in enterprise encryption software, offering the following products: SafeNet Protect File, SafeNet Protect V and SafeNet SecureStorage, SafeNet ProtectDB, SafeNet ProtectApp, and Tokenization and Data Masking with its SafeNet Tokenization product.<sup>5</sup>
68. Gemalto's activities in enterprise encryption software generated worldwide sales of [                    ] in 2017. In New Zealand, Gemalto's enterprise encryption software sales were [                    ].

#### **Required Documents / Information**

69. We provide in **Appendices 2 to 6**:
- 69.1 a copy of, or link to, the most recent annual report, audited financial statements and management accounts for the relevant business unit(s);
  - 69.2 each Party's total sales revenues, and volumes;
  - 69.3 the names and contact details for the Parties' main competitors, and any trade or industry associations in which one or both of the Parties participate; and
  - 69.4 the names and contact details for each Party's key customers, and the revenue earned from each customer in the last financial year.

5 For a more detailed overview of Thales' and Gemalto's enterprise encryption software products see Part G below.

## Part E – Market Definition

### Overview of Relevant Markets

70. To the Parties' knowledge, the Commission has not had the opportunity to date to assess the enterprise key management solutions or the enterprise encryption software for data in use/at rest segments.
71. The Parties consider the relevant markets for the purposes of this application in which their overlapping products are supplied are the Enterprise Key Management Market and the Enterprise Encryption Software Market.
72. Even if the Commission takes the view that it must define a national New Zealand market for the supply of enterprise key management products and associated maintenance services, and/or the supply of enterprise encryption software, then overseas suppliers will still exercise a competitive constraint on the participants in those markets. Therefore the global position of the Parties and their competitors remains relevant, and information on the global markets is included in the competition assessment.

### Enterprise Key Management Market

#### *Product Dimension*

73. An enterprise key management solution must, among other factors, be capable of generating, distributing, storing, rotating and deleting the vast number of keys used within an organisation. There are a number of different types of enterprise key management products that fulfill this need. These include:
- 73.1 encryption software/hardware containing key management capabilities;
  - 73.2 dedicated key management software;
  - 73.3 GP HSMs;
  - 73.4 Payment HSMs;
  - 73.5 HSMs aaS;
  - 73.6 Cloud-based encryption solutions with key management capabilities;
  - 73.7 TPMs; and
  - 73.8 microprocessors with key management capabilities.<sup>6</sup>
74. The Parties consider that there is an overall market for the supply of enterprise key management products and associated maintenance services in which a wide range of innovative and dynamic competitors are active.<sup>7</sup>

<sup>6</sup> These are expanded on in the competition assessment in Part H below.

<sup>7</sup> Consistent with the Parties' view, several third-party market studies identify and assess competition on the enterprise key management market, including IDC and MarketsandMarkets, see IDC, *Worldwide Data Security Taxonomy*, 2016, page 5 and MarketsandMarkets, *Enterprise Key Management Market, Global Forecast to 2022*, 2017, page 27 (provided at **Appendix 8**).

**75.** Most of the Parties' offerings in the enterprise key management market are GP HSMs and Payment HSMs, which are seen as quite conventional or traditional on-premise hardware products. However, the Parties consider that GP HSMs and Payment HSMs are appropriately viewed as falling within the same product market as other enterprise key management products. In the Parties' experience, enterprises would turn (and do turn) to key management solutions other than HSMs for new applications. [

].

**76.** From a supply-side substitutability perspective, vendors offer various options within the enterprise key management market and can relatively easily switch to offering additional types of key management products, in no small part because similar software is used across the key management solutions. In particular many vendors offer various options within the enterprise key management market – in fact, more than 15 players are active in more than one key management solution segment.<sup>8</sup> For instance:

**76.1** Intel supplies TPMs and microprocessors with built-in key management capabilities as well as encryption software with key management capabilities;

**76.2** Microsoft offers both encryption software with inherent key management capabilities, cloud-based key management solutions and dedicated key management software;

**76.3** Atos offers both dedicated software and a series of GP and Payment HSMs;

**76.4** Securosys offers both a series of GP HSMs and an HSMs aaS offer (through its product Securosys Clouds HSM);

**76.5** Ultra Electronics offers GP HSMs, Payment HSMs, and a dedicated key management software solution.

**77.** In general, enterprises are not required to choose products certified to any particular standard or to purchase any given type of key management product. Importantly, regulations generally do not require enterprises to use any specific product. Enterprises can choose a solution depending on a number of factors such as: the type and volume of data to be secured; the enterprise's risk tolerance and compliance rules; the complexity of access control management; processing power; cost; and the key management solutions used for existing applications.

**78.** The payment industry is an exception to the observation above that enterprises are not typically required to choose products certified to any particular standard or to

<sup>8</sup> Namely, AWS, Atos, DosuSign, Equinix Telecity, Futurex, Hitachi, IBM, KeyNexus, Micro Focus, Microsoft, Oracle, Realsec, Sophos, Securosys, Symantec, Trend Micro, Ultra Electronics and Ultimaco.

purchase any given type of key management product. Globally, companies processing electronic payment transactions are required to certify their broad data environment for certain payment applications under the Payment Card Industry Data Security Standard (**PCI DSS**). The PCI DSS was established in 2004 by the main payment schemes (i.e. Visa, MasterCard, American Express, JCB, and Discover) to protect payment card transactions and cardholders against misuse of their personal information. It standardises and ensures a consistent minimum level of security in backend processing of payment cards globally. To obtain PCI certification, customers must have their computer system examined by a third-party assessor (or, for small organisations, complete a self-assessment), remediate any vulnerabilities identified during this assessment, and report to their bank and ultimately to the card brands. Even there, however, there is no requirement to use any particular type of encryption or key management. This point is discussed further below.

79. Finally, resellers (including those used by the Parties in New Zealand) usually offer several key management solutions from different vendors and often help customers choose among these different key management solutions depending on their needs. The vast majority of Thales' and Gemalto's top resellers (in terms of sales value) sell more than one key management solution and offer at least two different brands per key management solution.
80. Notwithstanding their view that Payment HSMs are part of the broader Enterprise Key Management Market, for completeness the Parties have provided some specific information in relation to the overlap between them in Payment HSMs and also GP HSMs in the competitive analysis later in this application.

#### *Functional Dimension*

81. The Parties supply both enterprise key management products and associated maintenance services. [ ].

9

].

82. Globally, Thales and Gemalto offer their enterprise key management solutions at a retail level, but the more common scenario is for sales to occur at a wholesale level to resellers who then on-sell to end users. [ ].

].

#### *Geographic Dimension*

83. The Parties consider that the Enterprise Key Management Market is global in scope. The European Commission has consistently defined IT software and related markets as global (or at least EEA-wide).<sup>10</sup>

9 [ ]

].

10 In *Intel/McAfee*, the European Commission found that “the market investigation confirms that the relevant geographic markets for endpoint security are at least EEA-wide. [...] The Commission consider[ed] that endpoint security markets have a worldwide or at least EEA-wide geographic scope.”; see European Commission decision of January 26, 2011, *Intel/McAfee*, case M.5984, paras. 54-55. See also European Commission decision of January 21, 2010, *Oracle/Sun Microsystems*, case M.5529, paras. 112-113.

84. In particular, a local presence may be beneficial but is not essential to supply enterprise key management products in any particular region, because sales can be arranged online or over the phone, and maintenance and technical support services can usually be performed virtually. Where on-the-ground support is required, suppliers can, and do, rely on local resellers and distributors to resell their products to end-customers, and can also fly in temporary support from regional service centres. Resellers and distributors often bundle the vendors' HSMs in large, value-added solutions, and provide basic maintenance support (including, for example, training and product installation) to end-customers. [

].

85. Further, there is nothing material to stop customers from procuring key management products in one country and using them in another – indeed, it is common for companies in Australia and New Zealand to procure products for use in other countries within the Asia-Pacific region.

86. In addition, standards are similar internationally. FIPS and PCI DSS are widely recognised globally, including in New Zealand. As regards Payment HSMs specifically, the global payment schemes (Visa, MasterCard, Amex, etc) require PCI DSS/EMV certification. This applies globally, including in New Zealand. While members of the Australian EFTPOS debit card scheme (e.g. banks, building societies, credit unions and major retailers in Australia) must comply with the Australia-specific standard for certification of Payment HSM products called AS2805, which is developed and managed by AUSPAYNET (formerly known as APCA – the Australian Payment Clearing Association), there is no requirement for Payment HSMs in NZ to satisfy the Australian AS2805 standard. Instead, banks in New Zealand have the choice to procure any Payment HSM that is globally certified against PCI DSS/EMV, and therefore meets the requirements of the global payment schemes. This is evidenced for instance by the Parties' understanding that Utimaco's Atalla product line is not currently certified as compliant with the Australian AS2805 standard, but is still supplied to banks in New Zealand.

87. For these reasons the Parties maintain that the geographic scope of the Enterprise Key Management Market is worldwide (with the exception of China).

88. Even if the Commission takes the view that it must define a national New Zealand market for the supply of enterprise key management products and associated maintenance services, then overseas suppliers will still exercise a competitive constraint on the participants in that market. Therefore the global position of the Parties and their competitors remains relevant and information on the global market is included in the competition assessment.<sup>11</sup>

11 For instance, this was the approach of the Commission in Decision No. 455, Hewlett-Packard Company and Compaq Computer Corporation, 28 February 2002, paras 87-89.

## Enterprise Encryption Software Market

### *Product Dimension*

89. As discussed above, encryption is the process of converting plain text to cipher text using an encryption algorithm and encryption keys. The encryption and decryption of data is performed by encryption software.
90. The Parties consider that enterprise encryption software solutions protecting data at rest and data in use<sup>12</sup> make up a global product market, and that any sub-segmentation of enterprise encryption software down to the level in the data stack at which a user ultimately chooses to encrypt their data would not make sense.
91. There are no regulatory requirements to encrypt data at a particular level. While certain customers may need to follow industry-specific regulatory requirements related to the certification of their data security infrastructure generally, the Parties are not aware of any general requirements that would force a customer to encrypt data at any particular level of the data stack. As such, there are no regulatory requirements preventing customers from choosing one type of encryption software over another.
92. The Parties consider, however, that it is appropriate to treat enterprise encryption software solutions designed to protect data in motion as falling into a separate market. The players active in data in motion encryption products tend to be different from the at rest/in use players – and indeed neither of the Parties is active in offering encryption software for data in motion.

### *Geographic Dimension*

93. The Parties consider that the market for the supply of enterprise encryption software is global in scope, excluding China.
94. Most suppliers and brands are active globally and serve customers globally from a few facilities and customer support centres. Enterprise encryption software products are generally homogeneous across regions (e.g. all of Thales' and Gemalto's encryption software solutions are supplied globally, with very limited region-specific adjustments). [

].<sup>13</sup>

95. Local presence is not a significant requirement to supply enterprise encryption software (including for maintenance services, which can be provided by local resellers and distributors). [

].

96. There are no applicable regulatory or certification requirements for enterprise encryption software at the local level. Transport costs are negligible (software may

<sup>12</sup> These terms are further explained below from para. 120 onwards.

<sup>13</sup> [

].

be provided over the internet at nearly no cost). Finally, there are no quotas, tariffs or other trade barriers that affect the import into New Zealand or export from New Zealand of encryption software.

- 97.** Again, even if the Commission takes the view that it must define a national New Zealand market for the supply of enterprise encryption software, then overseas suppliers will still exercise a competitive constraint on the participants in that market. Therefore the global position of the Parties and their competitors remains relevant and information on the global market is included in the competition assessment.

## Part F – Counterfactual

98. The Parties consider that in the absence of the Proposed Transaction, it is likely that Gemalto will continue to operate as an independent supplier in the relevant markets.<sup>14</sup> [

].

14 [

].



## Part G – The Industry

- 100.** In this section we deal with the following topics:
- 100.1** an overview of enterprise data security and encryption;
  - 100.2** the products provided by the Parties;
  - 100.3** other industry participants;
  - 100.4** current industry trends; and
  - 100.5** recent merger activity in the industry.

### Overview of Enterprise Data Security and Encryption

#### *Enterprise Data Security*

- 101.** Enterprise data security products broadly aim to mitigate security and privacy risks in the creation, storage, and dissemination of data within “enterprises.” Enterprise data security is part of the broader enterprise cyber security space (which encompasses all products improving the security of computers, information systems, communications, transactions, personal devices, physical and cloud environments), and of the broader digital security space (which encompasses all solutions securing identity and reliability of persons, devices as well as connected objects and data).

#### *Encryption*

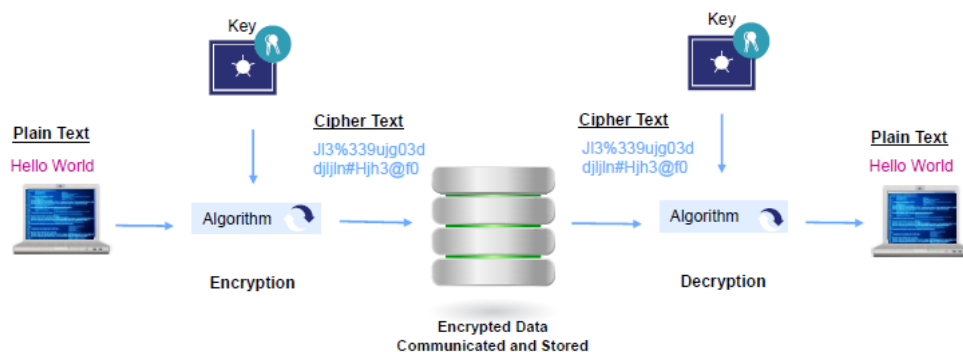
- 102.** Enterprises historically relied on a range of solutions, such as firewalls or basic password protection, to protect their networks. However, with the rise of cyber-attacks<sup>15</sup> and new regulatory requirements, customers have increasingly realised that the risk of data breaches is non-trivial as perimeter-based security is no longer efficient, and that it is therefore more important to protect a company’s data in the event that a breach occurs.
- 103.** Encryption is the most commonly used, and a fast growing, native method for securing electronic data. It has moved from a niche security technology to a mainstream method for protecting sensitive data at multiple locations in traditional, virtualised, and cloud environments. The Parties fully anticipate that encryption’s rapid growth will only continue given the further proliferation of data and the acceleration of digitalisation, including cloud, big data, mobile usage, and the IoT.
- 104.** Encryption involves the transformation of electronic data, programs, images or other information (known as plain text) into a format that is not understandable by a person or a computer (known as cipher text). Conversely, decryption transforms cipher text into plain text. Encryption requires the use of an encryption algorithm and at least one encryption key. Expanding on this:

<sup>15</sup> According to a PwC study, the number of detected security incidents has risen 66% year over year from 2009 to 2014, rising from 3.4 million to 42.8 million (see PwC, “Managing cyber risks in an interconnected world: Key findings from the Global State of Information Security Survey 2015”, page 7).

**104.1** Encryption algorithm: An encryption algorithm is a mathematical formula used to scramble (or encrypt) data. Typically, the formula performs a series of arithmetic steps on the data to be protected using the encryption key (known as the key), resulting in scrambled (or encrypted) data. Only someone with the right key can unscramble (or decrypt) the scrambled data. Encryption algorithms differ in the kind of formulas and keys they use to encrypt data. The type of formula (in terms of complexity and speed) and key (in terms of length) used to encrypt data may vary depending on how the protected data is used. Encryption algorithms are generally standardised and specified, so that two different parties can send and receive (and encrypt or decrypt) encrypted messages as long as they use the same formulas and have exchanged keys in a specified way.<sup>16</sup> In a world of standardised algorithms, the strength of the key (which determines the level of data scrambling) is critical to ensuring strong data protection. Thus, hackers generally turn their attention to “cracking” keys used to encrypt and decrypt data (rather than attempting to crack the encryption algorithm as such).

**104.2** Encryption key: Unlike encryption algorithms, which are public, an encryption key is a secret code, usually a random series of numbers or a pair of randomly chosen prime numbers, which is used by an algorithm to encrypt or decrypt data. The strength of the encryption depends on the randomness of the key generation, the length of the key (the longer the key the greater the computation effort and time required to crack it), the algorithm used, and how the data is entered into the algorithm. If the key generation process is not truly random, a new key can be predicted from knowledge of previous keys or the key generation itself. Protection of a key is essential in data security. If an encryption key is lost without backup, there is no way to decipher data encrypted with the lost key.

**105.** The following figure illustrates the interaction of the encryption algorithm and key to encrypt and decrypt data.



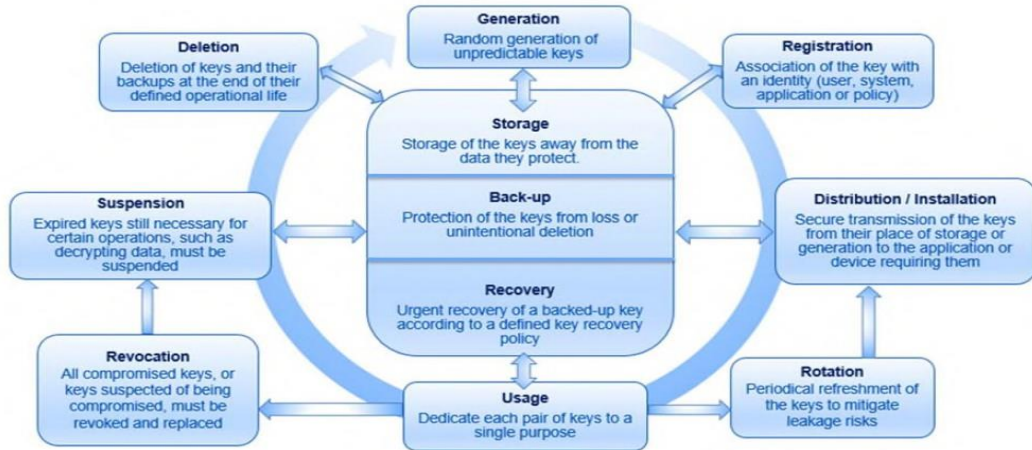
### *Encryption and Key Management*

**106.** Given the importance of keys to the encryption process, proper management of encryption keys is critical to ensure that any use of encryption delivers robust data security. Indeed, the growing use of encryption has led to a proliferation of keys within organisations. It is not uncommon for enterprises to use thousands, if not

<sup>16</sup> Advanced Encryption Standard (**AES**), Data Encryption Standard (**DES**), Blowfish, and Rivest, Shamir and Adleman (**RSA**) are examples of such standardized algorithms.

hundreds of thousands, of keys (or more) in their daily businesses. This has increased the need for efficient key management.

107. The diagram below displays a typical key life cycle. Key life cycles vary depending on the "use case", such that the ordering of phases may be altered and certain phases may be skipped completely.



Source: The Parties

108. Key management therefore comprises professional key management systems that provide encryption keys across a variety of operating systems and databases. This is necessary for most organisations collecting credit card information, names and addresses, or protected health information. For example, a network might be comprised of several different versions of Microsoft SQL Server as well as IBM, Linux, UNIX, or Oracle servers, as well as backup tapes and data stored in the cloud. The encryption key manager needs to be able to communicate simultaneously with all of these locations in order to provide encryption keys, decrypt, and rotate keys.

#### *Different Types of Enterprise Key Management Solutions*

109. There are several different types of enterprise key management products. These include:

Key Management Product	Description
<b>Encryption software/hardware containing key management capabilities</b>	Key management capabilities inherently included in encryption software/hardware products or integrated as part of a broader solution including one or several encryption software/hardware products
<b>Dedicated key management software</b>	Dedicated key management software, running on a physical or cloud server, used either stand-alone or in combination with hardware to further increase the level of security.
<b>GP HSM</b>	A dedicated hardware appliance running on encryption software to generate, protect, and manage keys in a secure tamper-resistant module.
<b>Payment HSM</b>	Similar to a GP HSM, but designed to provide high level payment-related functionality (e.g. PIN processing) and to perform a high volume of payment operations rapidly.
<b>HSM aaS</b>	HSM services purchased on a pay per use basis in lieu of physical, on-premise HSMs, offered either by CSPs or traditional HSM vendors.
<b>Cloud-based encryption solutions with key management capabilities</b>	Key management solutions inherently included in cloud-based encryption solutions deployed by CSPs to secure data stored on their cloud.
<b>TPMs and microprocessors with key management capabilities</b>	<p>A trusted platform module (<b>TPM</b>) is a dedicated security chip mounted as a motherboard component on various computing platforms (e.g. PCs, servers, phones, tablets), which provides a secure hardware enclave to store encryption keys and perform certain key management functions. Similarly, microprocessors with a secure enclave allow users to create a dedicated secure operating environment which functions under different (and more secure) operating principles than the traditional microprocessor's environment.</p> <p>For the avoidance of doubt, TPMs/microprocessors are not enterprise key management solutions in their own right, but they are used with key management software.</p>

*Sources of Revenue for Enterprise Key Management*

- 110. Depending on the particular product category, vendors' revenues are typically derived from a combination of the purchase price of hardware, license fees for software, and maintenance fees.
- 111. The proportion of revenue attributable to each varies not only based on the type of key management solution, but also on vendors' business models. For example, some vendors may charge a higher up-front purchase price but a lower ongoing software license fee. Similarly, an initial contract generally includes a period of maintenance, with the customer having the option of extending the maintenance contract at a later date. Vendors only provide maintenance for their own products, and maintenance fees typically represent a significant portion of vendors' revenues.
- 112. Maintenance contracts generally cover the provision of ongoing support for the user of the product, repairs to the product if required, and the provision of software upgrades during the period of the contract. The contracts would not ordinarily cover the replacement of existing hardware, other than when repairs are required.
- 113. [ ]:
- 113.1 [ ];

113.2 [ ];

113.3 [ ].

114. [ ].

115. [ ].

#### *Enterprise Encryption Software*

116. Enterprise encryption is a comprehensive data protection platform that includes strong encryption to secure and control access to high-value information, and centralised enterprise key management to secure, manage, and prove ownership of an organisation's keys to ensure sensitive data is not at risk.

117. The encryption and decryption of data is performed by encryption software. Encryption software solutions may be sold as:

117.1 standalone encryption software products;

117.2 native parts of underlying IT products (such as databases, data storage solutions, or operating systems and applications) which may also inherently include some key management capabilities; or

117.3 as a combination of different types of encryption software (or hardware), potentially combined with other capabilities such as centralised key and policy management.

118. The bulk of encryption software sold today is natively part of other software or hardware products that customers buy. Customers can generally enable or license the native encryption function in these products, thereby removing the need for additional dedicated encryption software to run over the top of those products. For example, native encryption capability is provided today as part of the standard cloud-based package of services offered by Amazon, Dropbox and Google; it comes with most databases (e.g. IBM DB2, Microsoft SQL, MongoDB, Oracle, and SAP); and is built into many operating systems, including Windows and Linux.

119. A substantial part of encryption software today is what is known as "open source".<sup>17</sup> Larger enterprise customers in particular often have internal development capabilities and thus regularly threaten to develop an encryption solution on their own using open source products.

120. There are three basic types of data that encryption software is designed to protect:

120.1 Data at rest which is not actively moving from device to device or network to network but is stored in one place;

17 Open source enterprise encryption software includes, for example, Apache Hadoop, AxCrypt, MySQL, PostgreSQL, SaltStack Enterprise Operations Framework, SQLCipher, Ubuntu, Vault Enterprise, and VeraCrypt.

- 120.2** Data in use which is stored in a non-persistent digital state in the computer memory or processed applications, and is generally accessible to several persons and devices; and
- 120.3** Data in motion (also called “in transit”) which is data actively moving from one location to another (such as via the internet, private network, or cloud).<sup>18</sup> Encryption software designed to protect data in motion is also called communication encryption software. Neither Thales nor Gemalto is active in offering encryption software for data in motion/communication encryption software, and as such the remainder of this section focuses on enterprise encryption software for data at rest or in use.
- 121.** The remainder of this section focuses on enterprise encryption software for data at rest or in use.
- 122.** Enterprise encryption software encrypts data at rest or in use at various levels or layers – including, in particular, at the storage/disk, file/folder, database, or application level:
- 122.1** Storage/disk encryption: Storage/disk encryption enciphers data in storage devices, such as hard disks, removable media, USBs, or CDs/DVDs. Disk encryption tends to offer protection primarily against theft or accidental loss of a physical drive, preventing an unauthorised party from accessing data on the encrypted disk. Storage encryption is a type of disk encryption applied at the network or shared drive level to encrypt large repositories of data. Neither of the Parties offer a disk or storage encryption solution.
- 122.2** File/folder encryption: File/folder encryption software secures sensitive files or folders stored, for example, in local PCs, servers, or on business networks. Rather than encrypting the entire disk, which might have millions of files protected with a single key based all-or-nothing approach, file/folder encryption allows information on the disk to be secured in a compartmentalised way. This makes it easier to differentiate levels of protection across the different files/folders on a disk. Both Thales and Gemalto offer file/folder encryption solutions.
- 122.3** Database encryption: Database encryption solutions encipher data stored in databases. Both Thales and Gemalto offer database-level encryption software.
- 122.4** Application-level encryption: Application-level encryption software encrypts data at the highest level in the data stack, such that each of the other layers “see” the data only in enciphered form. Application-level encryption is performed within the application that introduces the data into the system. This means that the data is encrypted as it moves around the network and cannot be understood even by database administrators. This is different from disk encryption, where the data is only encrypted when it is saved to the disk, but can be seen as it moves around. Application-level encryption typically protects specific subsets of data (such as primary account numbers or fields in a database). Both Thales and Gemalto offer application-level encryption software. Several of the Parties’ competitors

18 Examples include data as it moves across the internet to a cloud service provider or files transferred over File Transfer Protocol (FTP), and might include calls, mails, or instant messaging. The Secure Sockets Layer (SSL) protocol standard (also known as Transport Layer Security or TLS) is the default form of protection for Internet communications to secure data in transit across untrusted networks.

offer hybrid application level encryption products that are specifically advertised as being able to encrypt data at the application level and/or another level.<sup>19</sup>

- 123.** Further variants of encryption software include:
- 123.1** Tokenisation: Tokenisation is the process of protecting data by replacing sensitive numbers/information with random numbers or letters, and is used most commonly to protect credit card numbers: it converts or replaces cardholder data with a unique token ID to be used for one or more transactions. Both Thales and Gemalto have tokenisation solutions;
  - 123.2** Format preserving encryption (FPE): FPE is encryption that uses algorithms dedicated to particular data formats, such as credit card numbers. It enciphers data without changing the underlying format, e.g. maintaining a 16 digit number for a credit card. FPE allows encryption to be truly invisible to other systems that may need to process the encrypted data. Neither Thales nor Gemalto offer a stand-alone dedicated FPE product, but they both use the FPE technique as part of other products;
  - 123.3** Data masking: Data masking, rather than enciphering particular data fields, masks specific data elements in databases and file systems using random numbers, patterns, or letters while keeping the data structure. Thales offers a data masking product, but Gemalto does not.
- 124.** Because tokenisation, FPE, and data masking take place at the application level of the data stack, these techniques could be viewed as a form of application encryption software, but conservatively these products are discussed separately in this application. All three of these techniques are commonly used in the financial sector and for other sensitive personal identifiers (for example, a tax file number).






## **Enterprise Key Management Products Provided by the Parties**

### *Thales*



- 125.** Thales is active in three key enterprise management segments in New Zealand:
- 125.1** General Purpose HSMs with its nShield lines;
  - 125.2** Payment HSMs with its payShield lines; and
  - 125.3** encryption software with key management capabilities with its Vormetric encryption products.
- 126.** The table below summarises Thales' enterprise key management products globally:

<sup>19</sup> Below are some illustrative examples:  
*CipherCloud Cloud Access Security Broker Platform*: This solution offers application and file/folder encryption, as well as tokenisation and data masking. It is described as the "industry's first and most complete [Cloud Access Security Broker] solution". See: [https://docs.wixstatic.com/ugd/08e241\\_da9b556ad49b4077b51f5a599cd14e4b.pdf](https://docs.wixstatic.com/ugd/08e241_da9b556ad49b4077b51f5a599cd14e4b.pdf)  
*Google Cloud Platform*: This solution offers a native cloud encryption product performing application, disk/storage, database and file/folder encryption. See: <https://cloud.google.com/security/encryption-at-rest/default-encryption/resources/encryption-whitepaper.pdf>

Enterprise key management products offered by Thales

Category	Product	Description	Example	Global Revenue (excluding maintenance and support) 2017
General Purpose HSMs	nShield Connect	Thales' nShield Connect solution delivers HSM and key management services to applications distributed across an enterprise's network. nShield Connect HSMs are available in two series: classic nShield Connect+ HSMs, and the high-performance nShield Connect XC HSM series.		[ ]
	nShield Edge	The nShield Edge is a portable HSM designed for low-volume transaction environments. It is a USB-connected device that delivers key management capabilities and is ideally suited for off-line key generation for certificate authorities (CAs) as well as development environments.		[ ]
	nShield Solo	nShield Solo HSMs are low-profile, embedded PCI-Express cards that provide key management services to one or more applications hosted on a single server or appliance. nShield Solo HSMs are available in two series: classic nShield Solo+ HSMs, and the high performance nShield Solo XC HSM series.		[ ]
	CipherTrust Cloud Key Manager	The CipherTrust Cloud Key Manager delivers key management either as a service in the cloud based on a virtual DSM or as an on-premises deployment using the Vormetric Data Security Manager to securely manage keys.		[ ]
	nShield Bring Your Own Key (BYOK)	nShield Bring Your Own Key (BYOK) allows users to use their own keys in cloud applications, regardless of whether on Amazon Web Services (AWS), Google Cloud Platform (GCP) or Microsoft Azure. This allows users to retain closer control of key management in an nShield HSM while still taking advantage of the flexibility and economy of cloud services.		[ ]



<b>Payment HSMs</b>	<b>payShield 9000</b>	The payShield 9000 is a payment HSM designed specifically for payment applications, including PIN protection and validation, transaction processing, mobile and payment card issuance, and key management. It delivers high assurance protection for automated teller machine (ATM) and point of sale (POS) credit and debit card transactions and works with all major banking sector payment authorization applications.		[ ]
<b>Encryption Software or Hardware with Key Management Capabilities</b>	<b>Vormetric DSM</b>	The Vormetric Data Security Manager (“DSM”) also provides centralized key management. The Vormetric Data Security Manager is available in different form factors, as a virtual appliance, in private and public clouds or as a hardware.		[ ]


*Gemalto*






127. Gemalto is active in four key enterprise management segments in New Zealand:

- 127.1 General Purpose HSMs with its SafeNet Luna and ProtectServer product lines as well as SafeNet Crypto Command Center;
- 127.2 Payment HSMs with its SafeNet Luna EFT product line;
- 127.3 HSMs aaS with DPoD; and
- 127.4 encryption software with key management capabilities with SafeNet KeySecure and SafeNet Virtual KeySecure.

128. The table below summarises Gemalto’s enterprise key management products globally:

*Enterprise key management products offered by Gemalto*

Category	Product	Description	Example	Global Revenue (excluding maintenance and support) 2017
<b>General Purpose HSMs</b>	<b>SafeNet Luna Network HSM</b>	The SafeNet Luna Network HSM is Gemalto’s network-attached HSM and key management solution. SafeNet Luna Network HSMs come in Series A and S (which offers multi-factor authentication), and within those series in three different models to meet users’ performance needs.		[ ]

	<b>SafeNet Luna PCIe HSM</b>	The SafeNet Luna PCIe HSM is a card that can be embedded directly in an appliance or appliance server for an easy-to-integrate HSM and key management solution. The PCIe too comes in A and S series and in three models within those series.		[ ]
	<b>SafeNet USB HSM</b>	The SafeNet USB HSM solution delivers key management in a portable appliance with an USB interface. Its small size makes it especially attractive to customers who need to physically remove and store the appliance.		[ ]
	<b>Gemalto's ProtectServer HSMs</b>	Gemalto's ProtectServer HSMs are an alternate line of GP HSMs providing HSM and key management services. They offer a unique level of flexibility for application developers to create their own firmware and execute it within the secure confines of the HSM. ProtectServer HSMs exist as network connected versions or as PCI cards.		[ ]
	<b>SafeNet Crypto Command Center</b>	The SafeNet Crypto Command Center ("3C") provides a complete, centralized solution for the management of encryption HSM resources in the cloud. As an HSMs as a service, customers can quickly and cost-effectively provide and remotely manage single or groups of SafeNet Luna Network HSMs from one central location.	 SafeNet Crypto Command Center	[ ]
<b>Payment HSMs</b>	<b>SafeNet Luna EFT Payment HSM</b>	In Payment HSMs, Gemalto offers its SafeNet Luna EFT Payment HSM, a network-attached HSM designed for retail payment system processing environment for credit, debit, e-wallet and chip cards, as well and Internet payment applications. It offers secure PIN and card processing, message authentication, comprehensive key management, and general purpose cryptographic processing.		[ ]

HSMs aaS

**Data Protection On Demand<sup>20</sup>**

The Data Protection On Demand (DPoD) solution is a cloud-based platform that provides a wide range of on-demand encryption and key management services through a simple online marketplace. DPoD allows customers to deploy and manage encryption, key management and HSM services, on-demand and from the cloud. Since DPoD is based on a pay-as-you-grow pricing, customers can grow HSM and key management capacity and encryption resources without limitation.



[ ]

**Encryption Software or Hardware with Key Management Capabilities**

**SafeNet KeySecure**

The SafeNet KeySecure solution provides a central platform to manage keys and applications (while also serving as a broader platform offering encryption software solutions). SafeNet Key Secure can be deployed in physical, virtualized infrastructure, and public cloud environments.



[ ]<sup>21</sup>

**SafeNet Virtual KeySecure**

The SafeNet Virtual KeySecure solution provides centralised cryptographic processing, security policy and key management in a virtual (non-hardware) security appliance. It offers scalable key management and secure encryption at remote facilities or cloud infrastructures such as VMware or AWS Market place.



[ ]

### Other Industry Participants in Enterprise Key Management

- 129. In addition to the Parties, there are multiple other suppliers of enterprise key management solutions, both around the world and in New Zealand.
- 130. **Appendix 5** to this application sets out key New Zealand competitors, while **Appendix 9** sets out additional global competitors.
- 131. Some of the largest competitors and recent entrants in this segment are described below.

#### *Microsoft Corporation*

- 132. Microsoft is the world's largest software maker by revenue. For the past four years, Microsoft has been recognised as a leader for its Cloud infrastructure-as-a-service

<sup>20</sup> [ ]

<sup>21</sup> Please note that KeySecure is a "hybrid solution". As such, it is primarily sold for encryption purposes, but contains key management functionality. [ ]

(IaaS), with peer reviews praising its high growth rate, its agility, and its overall attractiveness.<sup>22</sup> Microsoft achieved turnovers of US\$90 billion in 2017.<sup>23</sup>

133. In enterprise key management, Microsoft is active in three segments:
- 133.1 dedicated key management software with its Key Management Server;
  - 133.2 cloud-based key management solutions with its Microsoft Azure product; and
  - 133.3 encryption software or hardware with key management capabilities with various software solutions.
134. Its Microsoft Azure solution is a cloud-based service used for building, testing, deploying and managing applications and services through a global network of data centres managed by Microsoft.<sup>24</sup>
135. Microsoft Azure includes Key Vault, which (among other things) encrypts keys and small secrets like passwords that use keys stored in HSMs.<sup>25</sup> Microsoft Azure is available online directly from Microsoft, or from a wide range of Microsoft partners in New Zealand.<sup>26</sup>
136. More information about Microsoft Corporation is available at [www.microsoft.com](http://www.microsoft.com).

#### *Micro Focus*

137. Micro Focus is a multinational software and information technology business based in England. It is listed on the New York Stock Exchange, the London Stock Exchange and is a constituent of the FTSE 100 Index.<sup>27</sup> Following its recent merger with HPE Software in September 2017, it is now the seventh largest pure-play software company in the world with more than 5,800 employees in research and development.<sup>28</sup>
138. Micro Focus offers a range of data security and encryption solutions. One of those solutions is Enterprise Secure Key Manager, which provides a centralised key management hardware-based solution for unifying and automating a customer's encryption key controls by creating, protecting, serving and auditing access to encryption keys.<sup>29</sup> Enterprise Secure Key Manager is distributed in New Zealand through Micro Focus' preferred distributor for New Zealand and Australia, NEXTGEN. NEXTGEN has offices in Sydney, Melbourne and Auckland.
139. In May 2018 it was announced that Utimaco is to acquire Micro Focus' Atalla portfolio, which would make the combined entity the third largest Payment HSMs provider worldwide.<sup>30</sup>
140. More information about Micro Focus is available at <https://www.microfocus.com/>.

22 See <https://www.gartner.com/doc/reprints?id=1-2G45TQU&ct=150519&st=sb>.

23 See <https://www.microsoft.com/investor/reports/ar17/index.html>.

24 See [https://en.wikipedia.org/wiki/Microsoft\\_Azure](https://en.wikipedia.org/wiki/Microsoft_Azure)

25 See <https://azure.microsoft.com/en-us/services/key-vault/>

26 See <https://azure.microsoft.com/en-us/pricing/purchase-options/>

27 See [https://en.wikipedia.org/wiki/Micro\\_Focus](https://en.wikipedia.org/wiki/Micro_Focus)

28 See <https://www.microfocus.com/about/>

29 See <http://files.asset.microfocus.com/4aa6-5089/en/4aa6-5089.pdf>

30 See <https://hsm.utimaco.com/news/utimaco-announces-intent-to-acquire-atalla-from-micro-focus/> and <https://www.microfocus.com/de-de/about/press-room/article/2018/micro-focus-announces-agreement-with-utimaco-to-divest-atalla-portfolio/>

### *Protegrity*

- 141. Protegrity was founded in 1996 and is based in Connecticut, United States. It provides data security solutions.<sup>31</sup> It has offices in the United Kingdom, Sweden, and India, as well as many regional locations throughout Europe.<sup>32</sup>
- 142. It provides the Enterprise Security Administrator, which is an interface for the centralised, visual administration of data security policies, key management, auditing and reporting of sensitive data assets across the customer's organisation. In relation to key management, Enterprise Security Administrator allows keys to be managed from a single centralised repository, key state management and the flexibility to integrate with external HSM systems.<sup>33</sup>
- 143. More information about Protegrity is available at [www.protegrity.com](http://www.protegrity.com).

### *Venafi*

- 144. Venafi (formerly known as IMCentric) is a cyber-security company founded in 2000 and headquartered in Utah, United States. It provides enterprise key and certificate management security solutions to organisations in the financial services, insurance, high-tech, telecommunications, aerospace, manufacturing, healthcare and retail sectors worldwide.<sup>34</sup>
- 145. The Venafi Trust Protection Platform secures and protects keys and certificates in the data centre, on desktops, on mobile and IoT devices, and in the cloud. It supports Venafi TrustAuthority, Venafi TrustForce and Venafi TrustNet, all of which contribute to the key management process.<sup>35</sup> The Venafi Trust Protection Platform is available in New Zealand through a reseller, Scientific Software & Systems (**SSS**).
- 146. More information about Venafi is available at [www.venafi.com](http://www.venafi.com).

### *SSH Communication*

- 147. SSH Communications Security (**SSH**) is a cybersecurity company founded in 1995 that is focused on encryption and access control solutions, with a particular focus on SSH (secure shell) key management. It has offices in the United States, Hong Kong, Germany and Finland, and is listed on the Nasdaq Nordic.<sup>36</sup>
- 148. SSH offers the Universal Key Manager solution, which allows users to analyse their SSH key environment, take control with centralised key management and automate the key lifecycle process.<sup>37</sup>
- 149. More information about SSH is available at [www.ssh.com](http://www.ssh.com).

### *Amazon Web Services*

- 150. Amazon Web Services (**AWS**) is a subsidiary of Amazon.com. It was founded in 2006 and is headquartered in Washington, DC. AWS is the leading CSP globally

31 See <https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=779830>

32 See <https://www.protegrity.com/company/location/>

33 See [http://info.protegrity.com/l/49532/2016-03-09/2zjq52/49532/55063/Protegrity\\_Enterprise\\_Security\\_Administrator\\_Data\\_Sheet.pdf](http://info.protegrity.com/l/49532/2016-03-09/2zjq52/49532/55063/Protegrity_Enterprise_Security_Administrator_Data_Sheet.pdf)

34 See <https://www.bloomberg.com/research/stocks/private/snapshot.asp?privcapId=20703557>

35 See [https://www.venafi.com/assets/pdf/ds/Venafi\\_Trust\\_Protection\\_Platform\\_datasheet.pdf](https://www.venafi.com/assets/pdf/ds/Venafi_Trust_Protection_Platform_datasheet.pdf)

36 See [https://en.wikipedia.org/wiki/SSH\\_Communications\\_Security](https://en.wikipedia.org/wiki/SSH_Communications_Security)

37 See <https://www.ssh.com/products/universal-ssh-key-manager/>

and operates in more than 190 countries, with large data centres located in the United States, Europe, Brazil, Singapore, Japan and Australia. Amazon achieved turnovers of US\$18.4 billion in 2017.<sup>38</sup>

151. AWS offers its cloud customers agile, standard-compliant, and fully managed key management services integrated with a range of other cloud storage services. AWS is globally distinguished for its IaaS products, which are backed by highly-responsive customer support. In enterprise key management, AWS is active in two segments: HSMsaaS through its CloudHSM offer and cloud-based key management solutions through its Key Management Service offer. These are available directly from AWS online.
152. More information about AWS is available at <http://aws.amazon.com/>.

#### *IBM*

153. IBM is a multinational technology company founded in 1911, headquartered in California and listed on the New York Stock Exchange. It has operations in more than 170 countries. It manufactures and markets computer hardware, middleware and software, as well as providing hosting and consulting services.<sup>39</sup>
154. IBM offers the IBM Security Key Lifecycle Manager, which centralises, simplifies and automates encryption key management.<sup>40</sup> The IBM Security Key Lifecycle Manager is available in New Zealand through a reseller, Liquid IT.
155. More information about IBM is available at [www.ibm.com](http://www.ibm.com).

#### *Oracle Corporation*

156. Oracle Corporation (**Oracle**) is a multinational computer technology corporation founded in 1977, headquartered in California and listed on the New York Stock Exchange. It specialises in developing and marketing database software and technology, cloud engineered systems and enterprise software products. It also develops and builds tools for database development and systems of middle-tier software, enterprise resource planning software, and customer relationship and supply chain management software.<sup>41</sup>
157. Oracle offers the Oracle Key Vault, which enables customers to deploy encryption and other security solutions through the central management of encryption keys.<sup>42</sup> The parties understand that Oracle Key Vault is available directly from Oracle.
158. More information about Oracle is available at [www.oracle.com](http://www.oracle.com).

#### *Google*

159. Google is a multinational technology company founded in 1998 and headquartered in California. It specialises in Internet-related products and service, including online advertising technologies, search engine, cloud computing, software and hardware.<sup>43</sup>

38 See <http://phx.corporate-ir.net/phoenix.zhtml?c=97664&p=irol-newsArticle&ID=2329885>

39 See <https://en.wikipedia.org/wiki/IBM>

40 See <https://www.ibm.com/us-en/marketplace/ibm-security-key-lifecycle-manager>

41 See [https://en.wikipedia.org/wiki/Oracle\\_Corporation](https://en.wikipedia.org/wiki/Oracle_Corporation)

42 See <http://www.oracle.com/technetwork/database/options/key-management/overview/index.html>

43 See <https://en.wikipedia.org/wiki/Google>

160. Google offers the Cloud KMS solution, a cloud-hosted key management service that allows users to generate, use, rotate and destroy encryption keys for cloud services.<sup>44</sup> Cloud KMS is available directly from Google online.

161. More information about Google is available at <https://www.google.com/about/our-company/>.

#### *Salesforce*

162. Salesforce is an American cloud computing company founded in 1999, headquartered in San Francisco and listed on the New York Stock Exchange.<sup>45</sup> Salesforce states that it provides the world's leading customer relationship management platform and has offices in Asia Pacific, the Americas, the Middle East, Europe and Africa.<sup>46</sup>

163. Salesforce offers a related product known as Salesforce Shield, a set of integrated services built natively into the Salesforce platform which allow customers to monitor and encrypt sensitive cloud data at rest.<sup>47</sup> Data encryption keys are not stored in Salesforce, but instead derived from the master secret and tenant secret whenever a key is needed to encrypt or decrypt data. Customers have three options for setting up their data encryption key material:<sup>48</sup>

163.1 Use the Shield Key Management Service to generate an organisation-specific tenant secret (from which data encryption keys are derived).

163.2 Use the infrastructure of their choice (such as an on-premises HSM) to generate and manage their tenant secret outside of Salesforce and then upload the tenant secret to the Shield Key Management Service.

163.3 Opt out of the Shield Key Management Service key derivation process with the Bring Your Own Key service – this allows customers to use the infrastructure of their choice.

164. The Shield Key Management Service is available directly from Salesforce.

165. More information about Salesforce is available at <https://www.salesforce.com/>.

#### *Entrust DataCard*

166. Entrust Datacard is a privately-held technology company, which was founded in 1969 and is headquartered in Minnesota, United States. It has more than 2,000 employees in 34 locations worldwide and generates over US\$600 million in annual revenue.<sup>49</sup>

167. Entrust Datacard's public key infrastructure (**PKI**) products include:<sup>50</sup>

167.1 PKI Based Authentication – an integrated security infrastructure for encryption, digital signatures and certificate authentication.

44 See <https://cloud.google.com/kms/>

45 See <https://en.wikipedia.org/wiki/Salesforce.com>

46 See <https://www.salesforce.com/> and <https://www.salesforce.com/au/company/locations/>

47 See <https://www.salesforce.com/blog/2016/07/bring-your-own-key-encryption-salesforce-platform.html>

48 See [https://help.salesforce.com/articleView?id=security\\_pe\\_byok\\_why.htm&type=5](https://help.salesforce.com/articleView?id=security_pe_byok_why.htm&type=5)

49 See <https://www.entrustdatacard.com/about/overview>

50 See <https://www.entrustdatacard.com/products/categories/pki>

- 167.2** Entelligence Security Provider Digital Identity Management – automatic management of an organisation’s digital IDs.
- 167.3** Managed PKI Service (Entrust Cloud PKI) – provides reliable service with continuous protection housed in established secure facilities.
- 168.** Entrust Datacard’s public key infrastructure products are available in New Zealand through a reseller, SSS.<sup>51</sup>
- 169.** More information about Entrust Datacard is available at [www.entrustdatacard.com](http://www.entrustdatacard.com).

*Randtronics*

- 170.** Randtronics is a privately-owned company founded in 2002 that develops data encryption solutions. It has offices in Australia and the United States.<sup>52</sup>
- 171.** Randtronics’ core technology is the Data Privacy Manager, which provides a number of data security solutions including the DPM Key Manager.<sup>53</sup> The DPM Key Manager offers a central place to manage encryption keys and straightforward integration with an HSM.<sup>54</sup>
- 172.** More information about Randtronics is available at [www.randtronics.com](http://www.randtronics.com).

*Salt Group*

- 173.** Salt Group is an Australian IT security company that has been operating since 2002. It provides a robust security infrastructure to support the authentication of mobile and embedded devices, users and transaction. Salt Group’s products are available in Australia, Asia Pacific and Europe.<sup>55</sup>
- 174.** Products offered by Salt Group include:<sup>56</sup>
  - 174.1** Salt Mobile – digital identity security tokens and SDK enable high assurance trust and authentication of devices, user and transactions.
  - 174.2** Echidna – an enterprise grade security platform that provides a single trust anchor for organisations to authenticate user identities across a variety of contexts and channels.
  - 174.3** Third Party – third party hardware and software products to complement Echidna and Salt Mobile, including Thales nShield HSMs, Thales Vormetric and Intercede MyID.
- 175.** The parties understand that these products are available in New Zealand directly.
- 176.** More information about Salt Group is available at <http://www.saltgroup.com.au/>

51 See <https://www.sss.co.nz/solutions/security-products/public-key-infrastructure-and-key-management/>  
52 See <https://www.randtronics.com/about-us/company>  
53 See <https://www.randtronics.com/products/products-overview>  
54 See [https://www.randtronics.com/images/Datasheets/Randtronics\\_DPM\\_Technology\\_V13\\_US.pdf](https://www.randtronics.com/images/Datasheets/Randtronics_DPM_Technology_V13_US.pdf)  
55 See <http://www.saltgroup.com.au/about/>  
56 See <http://www.saltgroup.com.au/products/>



## Cogito Group

177. Cogito Group is an Australian-owned ICT company that provides organisations with digital security solutions and assists organisations with their digital security and authentication requirements.<sup>57</sup> It has offices in Australia and New Zealand.<sup>58</sup>
178. Cogito Group offers a modular solution known as Jellyfish, which is a cyber-security platform that integrates security services and products (in other words, it is an aggregator).<sup>59</sup> In providing this solution, Cogito Group partners with a number of other technology providers, including Thales and Gemalto.<sup>60</sup> Jellyfish is available in New Zealand.
179. More information about Cogito Group is available at <https://cogitogroup.com.au/>.

## Enterprise Encryption Software Products Provided by the Parties

180. The table below summarises the levels of the "data stack" for which the Parties offer enterprise encryption software.

Level of Encryption	Does Thales Offer a Product?	Does Gemalto Offer a Product?
Storage/disk	No	No
File/folder	Yes	Yes
Database	Yes	Yes
Application-level	Yes	Yes
Tokenisation	Yes	Yes
FPE	No	No
Data masking	Yes	No

Source: The Parties

## Thales

181. Within the encryption software segment, Thales supplies its Vormetric enterprise encryption solutions, and Gemalto supplies its SafeNet enterprise encryption solutions. In 2017, Thales' activities in enterprise encryption software generated global sales of [ ]). In 2017, Gemalto's activities in enterprise encryption software generated global sales of [ ]).
182. The table below summarises Thales' enterprise encryption software products supplied globally.

57 See <https://cogitogroup.com.au/about/>  
58 See <https://cogitogroup.com.au/contact/>  
59 See <https://cogitogroup.com.au/jellyfish/>  
60 See <https://cogitogroup.com.au/partners/>

Product name	Product description
Vormetric Transparent Encryption	Delivers data at rest encryption with centralised key management, wherever the data reside (i.e. across multiple clouds, on-premises or within big data and container environments). This solution's transparent approach enables organisations to implement encryption without having to make changes to applications, infrastructure or business practices.
Vormetric Application Encryption	Encrypts specific files in databases, big data nodes and "platform-as-a-service" environments.
Vormetric Cloud Encryption Gateway	This is Thales' cloud encryption solution, encrypting sensitive data – file/folder or databases – before they leave the user's premises to be saved in the cloud storage environments. It also offers key management and access control to its users.
Vormetric Protection for Teradata Database	Offers centrally managed encryption of sensitive data in the user's Teradata environment without altering their format.
Vormetric Tokenization and Data Masking	Tokenises data and masks sensitive assets no matter where they reside (e.g. cloud, data centre, outsourced environment, etc.) without requiring extensive changes to applications, network systems or storage architecture.
Vormetric Batch Data Transformation	Works with other Vormetric applications to facilitate and fasten the encryption or tokenisation of high volumes of sensitive data.
Vormetric Data Security Platform	The Vormetric Data Security Platform is composed of several products which can be deployed individually, namely, the Vormetric Data Security Manager ( <b>DSM</b> ) and one or more Vormetric solutions (called "agents"). The DSM is a centralised key manager device connected to all applications and devices of the organisation. While the DSM is used to store the root key like an HSM (discussed below), it also has (i) enterprise key management capabilities which support Vormetric applications, (ii) policy management capabilities (ie, it contains the company's data policies used to configure the software solutions), (iii) central logging capabilities (ie, it gives instructions to all devices to grant users access to the encrypted data), and (iv) a common user interface (which makes it easier to keep qualified staff trained).

Source: Thales

183. [

].

Gemalto

184. The table below summarises Gemalto's enterprise encryption software products globally.

Product name	Product description
SafeNet ProtectFile	Provides transparent and automated file system level encryption in several environments (i.e. physical, virtual and cloud environments), as well as centralised key management.
SafeNet ProtectV	Provides virtual machine encryption for a variety of cloud environments, including Amazon Web Services, IBM SoftLayer Cloud, Microsoft Azure and VMware.
SafeNet ProtectDB	Encrypts structured sensitive data (i.e. credit cards, passwords and email addresses) residing in all types of data centres (i.e. on-premises, virtual and public cloud environments).
SafeNet ProtectApp	Provides an interphase for key management operations and application-level encryption of sensitive data during their entire lifecycle. It can be deployed in various environments (i.e. physical, virtual and cloud environments).
SafeNet Tokenization	This is Gemalto's tokenisation solution. SafeNet Tokenization tokenises sensitive data and can be deployed in various environments (i.e. on-premises, virtual and public cloud).
SafeNet KeySecure	SafeNet KeySecure is Gemalto's integrated data security solution. SafeNet KeySecure is a platform composed of a hardware appliance and a SafeNet Luna HSM and can interoperate with one or more encryption solutions, including Gemalto (e.g. Safenet ProtectApp Encryptor or SafeNet ProtectFile Encryptor) and third-party software. The platform offers simplified centralised key management for all encryption solutions to which it is connected and which can be deployed over diverse centres or infrastructures, such as public, private or hybrid cloud environments.

Source: Gemalto

185. [

].

### Other Industry Participants in Enterprise Encryption Software

186. In addition to the Parties, there are multiple other suppliers of enterprise encryption software, both globally and in New Zealand specifically. We identify below the Parties' largest competitors globally (well over 30 in total), together with their estimated market shares for the supply of enterprise encryption software for data at rest/in use.

187. Some of the largest competitors in this segment are described below.

#### *Microsoft*

188. Microsoft is a public United States company. It was founded in 1975, and is headquartered in Redmond, Washington.

189. Microsoft is the world's largest software maker by revenue (achieving turnover of USD 90 billion in 2017), and one of the major vendors of encryption software. It develops, manufactures, licenses, supports and sells computer software, consumer electronics, personal computers, services, cloud-based software and hardware appliances, and is active in more than 190 countries. Microsoft is active in disk/storage, database, and file/folder encryption as well as in tokenisation/data masking.
190. In addition, Microsoft offers Microsoft Azure Service Encryption for data at rest, a cloud-based service. This solution helps users protect their data to meet organisational security and compliance commitments.
191. More information can be found at: [www.microsoft.com](http://www.microsoft.com).

#### Oracle

192. Oracle is a public United States company. It was founded in 1977, and is headquartered in Redwood Shores, California. Oracle offers "*the world's first database*",<sup>61</sup> and is specialised in developing and marketing database software and technology, cloud engineering systems and enterprise software products. It is particularly renowned for its Transparent Data Encryption offering, and has more than 480,000 customers and 25,000 partners in 175 countries. Oracle achieved a turnover of USD 37.7 billion in 2017.
193. In encryption software, Oracle is active in database and application encryption and in data masking. In addition, Oracle offers a data security platform: Oracle Enterprise Manager. This solution provides a single pane of glass for managing all of a customer's Oracle deployments, whether they are located in the user's data centre or in the Oracle Cloud.<sup>62</sup>
194. More information can be found at: [www.oracle.com](http://www.oracle.com).

#### Dell EMC

195. RSA Security, also known under the name Dell EMC, is a United States company, which has been part of the Dell Technologies family of brands since 2016. It was founded in 1984, and is headquartered in Hopkinton, Massachusetts. RSA provides solutions for advanced threat detection and cyber incident response. It has more than 30,000 customers globally, including nearly half of the global Fortune 500 companies.
196. In encryption software, Dell EMC is active in disk/storage, file/folder and application encryption as well as in tokenisation, with some of its products offered in the cloud. In addition, Dell EMC offers Data Protection Cloud Edition. This solution provides data control through transparent client-side encryption. Data Protection Cloud Edition encrypts traffic captured as it moves into the cloud and decrypts traffic captured as it moves out of the cloud.<sup>63</sup>
197. More information can be found at: [www.rsa.com](http://www.rsa.com).

61 See <http://www.oracle.com/us/corporate/oracle-fact-sheet-079219.pdf>.

62 See <http://www.oracle.com/technetwork/oem/enterprise-manager/overview/index.html>.

63 See [http://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/Dell\\_Data\\_Protection\\_Cloud\\_Edition\\_Data\\_Sheet.pdf](http://i.dell.com/sites/doccontent/shared-content/data-sheets/en/Documents/Dell_Data_Protection_Cloud_Edition_Data_Sheet.pdf).

## *Seagate Technology*

- 198.** Seagate is a public United States company. It was founded in 1979, and is headquartered in Cupertino, California. Seagate is the "global leader in data storage solutions".<sup>64</sup> It provides electronic data storage technology and solutions and its main products are hard disk drives. Seagate achieved a turnover of USD 10.8 billion in 2017.
- 199.** In encryption software, Seagate is active in disk encryption with its Seagate Secure Self-Encrypting Drive. This solution provides native encryption of all the data in the hard disk drive, and it automatically locks the hard disk drive and secures its data the instant a drive is removed from a system, or the moment the drive or system is turned off. Seagate Secure Self-Encrypting Drive protects data at rest, reduces IT drive retirement costs and is Federal Information Processing Standardisation (FIPS) 140-2 validated.<sup>65</sup>
- 200.** More information can be found at: [www.seagate.com](http://www.seagate.com).
- 201.** In addition to the competitors described above, companies also supplying these services into New Zealand include: ESET, McAfee, Netscape, Nuvola, Randtronics, Sky High, Trend Micro, Townsend and ToxenX.

## **Recent Merger Activity**

- 202.** In May 2018 it was announced that Utimaco is to acquire Micro Focus' Atalla portfolio, which would make the combined entity the third largest Payment HSMS provider worldwide.<sup>66</sup>
- 203.** In January 2018, Thales, through its German company Sysgo, formed a joint venture with Vector, a Germany-based specialist for automotive embedded electronics.
- 204.** In December 2017, Thales completed the acquisition of Guavus, a provider of real-time big data analytics.
- 205.** In September 2017, UK-based Micro Focus completed the acquisition of HPE Software. The combined company became the world's seventh largest pure-play software company.
- 206.** In March 2016, Thales completed the acquisition of Vormetric, a provider of data protection solutions.

64 See <https://www.seagate.com/qb/en/about-seagate/>.

65 See <https://www.seagate.com/qb/en/tech-insights/protect-data-with-seagate-secure-self-encrypting-drives-master-ti/>.

66 See: <https://hsm.utimaco.com/news/utimaco-announces-intent-to-acquire-atalla-from-micro-focus/> and <https://www.microfocus.com/de-de/about/press-room/article/2018/micro-focus-announces-agreement-with-utimaco-to-divest-atalla-portfolio/>

## Part H – Competition Assessment for Enterprise Key Management Market

208. In this section, we deal with:
- 208.1 The relevant market shares of the key participants in the Enterprise Key Management Market;
  - 208.2 The constraints on the merged entity post-acquisition from existing competition;
  - 208.3 The constraints on the merged entity post-acquisition from potential competition;
  - 208.4 Countervailing power from major customers;
  - 208.5 Why the risk of coordination post-acquisition is low; and
  - 208.6 Why there would be no lessening of competition even if there were separate markets for Payment HSMs or GP HSMs only (contrary to the Parties' position that these are both segments of the wider Enterprise Key Management Market).
209. For the reasons set out below, the Parties maintain that any attempt by Thales to increase the price of its enterprise key management solutions, or decrease the quality of its service in relation to those products, in New Zealand post-Proposed Transaction will be rapidly defeated. Thales will have no ability or incentive to maintain a price increase because it will lose customers to one of the many existing alternative suppliers in the market, or to a competitor with a new product as substantial innovation continues to change competitive dynamics in the market. As a result, the Proposed Transaction will have no effect on the competitive conditions in the Enterprise Key Management Market.

### Market Shares

210. The Parties provide share data below for the Enterprise Key Management Market. In case the Commission wishes to consider narrower market segments (despite the Parties' contentions to the contrary), share data is also provided for Payment HSMs and GP HSMs. Share data is provided on a global level only as the parties do not have reliable assessments of market shares for New Zealand. However, the Parties do provide their New Zealand revenue figures for both markets to assist the Commission.
211. The methodology and sources of the market share data used are expanded on in **Appendix 7**.

### *Enterprise Key Management*

212. The Parties and their primary competitors' estimated global<sup>67</sup> value-based market shares in enterprise key management between 2015 and 2017 are provided in the table below.<sup>68</sup>

67 In each case excluding China (as set out in Part E above under Geographic Dimension).

68 Market share data is based on IDC data. For an overview of the methodology and sources used to calculate this market share data see **Appendix 7**.

**Global market shares by value for the supply of enterprise key management solutions  
(2015-2017)**

Company	2015		2016		2017	
	Revenue (Mn €)	Share (%)	Revenue (Mn €)	Share (%)	Revenue (Mn €)	Share (%)
Thales	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Gemalto	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
<b>Combined</b>	<b>[ ]</b>	<b>[ ]</b>	<b>[ ]</b>	<b>[ ]</b>	<b>[ ]</b>	<b>[ ]</b>
Veritas	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
AWS	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Microsoft	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Commvault	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Veeam	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
IBM	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Fujitsu	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Atos	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Oracle	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
NetApp	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Symantec	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Sophos	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
RSA (Dell EMC)	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Hitachi	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
McAfee	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Utimaco	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Ultra Electronics	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Quantum	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Trend Micro	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
DocuSign	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Futurex	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Protegrity	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Zix	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Tokheim	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Huawei	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Venafi	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Box	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Others	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
<b>Total</b>	[ ]	<b>100%</b>	[ ]	<b>100%</b>	[ ]	<b>100%</b>

Source: IDC and the Parties

213. In 2017, the Parties' combined market shares (in value) amounted to just under [ ] worldwide (Thales: [ ]; Gemalto: [ ]). This is within the Commission's concentration indicator threshold.

214. The Parties' global market shares have [

].

215. In 2017, the Parties had combined revenue in enterprise key management (including maintenance) in New Zealand of approximately [ ] (Thales: [ ] and Gemalto: [ ]).

216. The Parties' main competitors worldwide include Veritas ([ ]), AWS ([ ]), Microsoft ([ ]), Commvault ([ ]), Veeam ([ ]), and a myriad of small players (eg IBM, Fujitsu, Atos etc).

#### Payment HSMs

217. The Parties and their primary competitors' estimated global value-based market shares in Payment HSMs in 2017 are provided in the table below.

Company	Sales (€million)	Share
Thales	[ ]	[ ]
Gemalto	[ ]	[ ]
<i>Combined</i>	<i>[ ]</i>	<i>[ ]</i>
Atos	[ ]	[ ]
Micro Focus	[ ]	[ ]
Tokheim	[ ]	[ ]
DocuSign	[ ]	[ ]
Futurex	[ ]	[ ]
Cryptera	[ ]	[ ]
Realsec	[ ]	[ ]
Ultra Electronics	[ ]	[ ]



CCV	[ ]	[ ]
HID	[ ]	[ ]
Prism	[ ]	[ ]
Utimaco	[ ]	[ ]
Others	[ ]	[ ]
<b>Total</b>	<b>[ ]</b>	<b>100%</b>

Source: IDC and The Parties

- 218.** The Parties' combined segment shares (in value) amounted to [ ] on a worldwide level. Moreover, the Proposed Transaction will bring a limited increment, with Gemalto's limited market presence ([ ] worldwide in 2017).
- 219.** The Parties compete with numerous other players worldwide, including Atos ([ ]), Tokheim ([ ]), Micro Focus ([ ]), DocuSign ([ ]), and Futurex ([ ]), and a number of smaller players (e.g. CCV, Cryptera, HID, Prism, Realsec, Utimaco etc).
- 220.** The Parties' combined supply shares have [ ].
- ]. This is due to:
- 220.1** the cyclical nature of Payment HSM vendors' sales, which peak when they release a new version of a Payment HSM; and
- 220.2** the recent expansion of several competitors, including [ ].
- 221.** The Parties' combined Payment HSMs revenue in New Zealand in 2017 including maintenance was approximately [ ] (Thales: [ ] and Gemalto: [ ]).

#### GP HSMs

- 222.** The Parties and their primary competitors' estimated global value-based segment shares in GP HSMs in 2017 are provided in the table below. These sales and shares include HSMs aaS sales.

Company	Revenue (€m)	Shares (%)
Thales	[ ]	[ ]
Gemalto	[ ]	[ ]
<b>Combined</b>	<b>[ ]</b>	<b>[ ]</b>
Atos Group	[ ]	[ ]
Utimaco	[ ]	[ ]
Ultra Electronics	[ ]	[ ]
IBM	[ ]	[ ]

Securosys	[ ]	[ ]
Futurex	[ ]	[ ]
Cavium	[ ]	[ ]
DocuSign	[ ]	[ ]
AWS	[ ]	[ ]
Microsoft	[ ]	[ ]
Others	[ ]	[ ]
<b>Total</b>	<b>[ ]</b>	<b>100%</b>

Source: IDC and the Parties

223. In 2017, the Parties' combined GP HSM shares (in value) amounted to [ ] on a worldwide level (Thales: [ ]; Gemalto: [ ]). The Parties' main competitors on a worldwide-level are: Atos ([ ]); IBM ([ ]); Ultra Electronics ([ ]); and Utimaco ([ ]). The Parties also compete with a number of other players (including Amazon, Cavium, DocuSign, Futurex, Microsoft, Realsec, Securosys, and Yubico).

224. [

].

225. In 2017, the Parties' combined revenue for GP HSMs in New Zealand including maintenance was approximately [ ] (Thales: [ ] and Gemalto: [ ]).

### Constraint from Existing Competition

226. The Parties consider that there will be strong constraints on them post-acquisition from existing competition. The reasons for this are set out below.

#### *The Enterprise Key Management Market is Highly Competitive*

227. The Parties compete with a broad range of players across a range of key management solutions from traditional HSMs, cloud-based HSMs aaS, dedicated key management software, encryption software containing key management capabilities, microprocessors with built-in key management capabilities, TPMs with key management capabilities, cloud-based encryption solutions with key management capabilities, as well as multi-party computational software. To name just a few such competitors, Atos, IBM, Micro Focus, Microsoft, Utimaco and Ultra Electronics, are all active in at least three different key management solution categories globally (similar to the Parties), while many others focus on one or two solutions.<sup>69</sup> As noted above, in May 2018 it was announced that Utimaco is to acquire Micro Focus' Atalla portfolio, which would make the combined entity the third largest Payment HSMs provider worldwide.<sup>70</sup>

69 For an overview of the activities of the Parties' competitors with Enterprise Key Management capabilities see **Appendix 9**.

70 See <https://hsm.utimaco.com/news/utimaco-announces-intent-to-acquire-atalla-from-micro-focus/> and

Key management solutions	Description	Selected competitors
<b>GP HSMs</b>	Dedicated hardware solution with tamper-proof features	Atos, Cavium, DocuSign, Futurex, IBM, Micro Focus, Realsec, Securosys, Utimaco, Townsend, Ultra Electronics, and Yubico
<b>Payment HSMs</b>	Dedicated hardware solution with tamper-proof features including built-in software layer to perform higher frequency payment-related functions and operations	Atos, CCV, Cryptera, DocuSign, Futurex, HID, Micro Focus, Prism, Realsec, Utimaco, Tokheim, Townsend and Ultra Electronics
<b>Dedicated key management software</b>	Dedicated software solution that can be used as stand-alone or in combination with hardware to increase the level of security	Atos, Box, Cryptomathic, Device Authority, Fometix, Fortanix, KeyNexus, Microsoft, Oracle, Quantum, Trend Micro, Ultra Electronics and Unbound
<b>Cloud-based HSMs as a service</b>	Cloud-based native encryption services including KM capabilities offered by cloud service providers	AWS, Bluefin, Equinix Telecity, Securosys, and Virtru
<b>Cloud-based encryption solutions with key management capabilities</b>	Cloud-based native encryption services including KM capabilities offered by cloud service providers	Alibaba Cloud, AWS, Dropbox, Equinix Telecity, Google, Hitachi, Huawei, IBM, KeyNexus, McAfee, Microsoft, NuCypher, Salesforce, Sepior, and Symantec
<b>Encryption software containing key management capabilities</b>	Underlying/native encryption software including KM capabilities, and Integrated software solution with centralized key management capabilities	Check Point Software, Commvault, DataLocker, Eruces, Fujitsu, Hitachi, IBM, Micro Focus, Microsoft, NetApp, Oracle, PKWARE, Protegrity, RSA, Utimaco, Symantec, Trend Micro, Veeam, Venafi, WinMagic, and Zix
<b>TPMs with key management capabilities</b>	Dedicated hardware solution (security chip) fitting as a motherboard component on a laptop or desktop	Asus, Gigabyte, HPE, Infineon, Intel, Microchip, Nuvoton, and ST Microelectronics
<b>Microprocess or with built-in key management capabilities</b>	Dedicated hardware solution (standard microprocessors) embedding a security enclave for physical key storage	Arm, Intel and Qualcomm

228. Further information on the competing players with enterprise key management capabilities is set out in **Appendix 9**.

<https://www.microfocus.com/de-de/about/press-room/article/2018/micro-focus-announces-agreement-with-utimaco-to-divest-atalla-portfolio/>

- 229.** Given the large number of competitive solutions that will continue to constrain the Parties worldwide and in New Zealand, including fast growing cloud-based technologies and other innovative solutions, the Parties' limited size as compared to these other big players, and the lack of unique competitive constraints that the Parties impose on one another, the Parties believe the Proposed Transaction will not result in any impediment to effective competition in the markets involved. Quite to the contrary, the Proposed Transaction will allow the combined entity to compete more effectively in the ever-changing data security space.

*Market Shares Overstate Parties' Competitive Position*

- 230.** Further, the market share estimates above likely overstate the Parties' combined position in the supply of key management solutions.
- 231.** The market share estimates do not take account of the revenues earned by suppliers of TPMs and microprocessors with built-in key management capabilities, nor multi-party computational software.
- 232.** The data may also not accurately reflect the full revenues resulting from key management capabilities of third parties that have been included within other products, sold by system integrators, or sold through value-added resellers.
- 233.** Nor does the data for new entrants reflect ongoing maintenance arrangements, whereas this is taken into account in the figures for Thales and Gemalto. [

]:

Party	Country	Year	Product	Maintenance share
Gemalto	New Zealand	2017	GP HSM	[ ]
Gemalto	New Zealand	2017	Payment HSM	[ ]
Thales	New Zealand	2017	GP HSM	[ ]
Thales	New Zealand	2017	Payment HSM	[ ]

*The Parties Do Not Exercise a Unique Competitive Constraint on One Another*

- 234.** While the Parties are both traditional vendors with similar solution designs (e.g. both offer on-premise HSM products as their major products in this market), Thales and Gemalto do not impose a unique competitive constraint on one another. The Parties' products have different strengths in terms of functionalities and capabilities. [ ]
- 235.** Further, when launching a new key management infrastructure project, customers can turn to a wide panel of alternatives to the Parties' solutions. In New Zealand specifically, this includes:

- 235.1** Vendors of encryption software or hardware with inherent key management capabilities (e.g. IBM, Microsoft and Oracle) or of integrated solutions (e.g. Oracle);
- 235.2** Dedicated key management software players (e.g. Microsoft and Trend Micro);
- 235.3** Other GP HSM players (e.g. Utimaco);
- 235.4** Other Payment HSM players (e.g. Utimaco through its acquisition of the Atalla product line);<sup>71</sup> and
- 235.5** Vendors of cloud-based key management solutions (e.g. AWS, Dropbox and Microsoft).

*The Market is Highly Dynamic*

- 236.** The global market for enterprise key management has grown substantially over the last decade (i.e. about 20% annually from 2015 to 2017), enriched by new key management solutions and growing use of existing key management solutions. Enterprises can now manage their keys by choosing among a wider panel of options, including HSMs aaS and other cloud-based key management solutions offered by CSPs as well as integrated solutions. Customer choices will broaden further as new solutions leverage technologies such as TPMs embedding microprocessors with built-in key management capabilities and multi-party computational software, which permit pure software and combined hardware and software solutions to offer security levels equal to those of traditional GP HSMs and Payment HSMs. These options were not available at all or as fully-fledged key management solutions a decade ago.

*No Capacity Constraints in the Industry*

- 237.** Should Thales attempt to increase the price for the Parties' enterprise key management products post-Proposed Transaction, competitors could easily step in and increase their sales to the Parties' customers because there are no relevant capacity constraints in the industry. Many of the key management solutions are software based, with regard to which the suppliers' marginal costs are close to zero. With respect to HSMs and other hardware based solutions, vendors generally source significant hardware from third-party suppliers without any capacity constraints. New market entrants that do not have any manufacturing capabilities have access to a number of OEMs from whom they could acquire finished product for limited investment and without material capacity constraints, as the Parties themselves do.

**Constraints on the Merged Entity Post-Acquisition from Potential Competition**

*Limited Barriers to Entry – Aggressive New Competitors*

- 238.** The merged entity will not inhibit competitors from expanding. Quite to the contrary, the Parties will continue to face a number of aggressive competitors, including many

71 The Parties believe that the Atalla product line is not currently certified as compliant with the Australian AS2805 standard, but for the reasons discussed above and further below, this will not pose any material barrier to Utimaco (following its acquisition of the Atalla products) competing head to head with Thales post-Proposed Transaction, and acting as a strong competitive constraint on Thales' supply of Payment HSMs. In particular, as noted above, there is no requirement for Payment HSMs in New Zealand to satisfy the AS2805 standard, as evidenced by the fact that the Atalla product is already supplied in New Zealand.

recent entrants such as the large CSPs, who will look to take advantage of the Proposed Transaction to continue their growth.<sup>72</sup>

239. Evidence of the limited barriers to new entry can be found in the fact that there have been around 35 new entrants in the Enterprise Key Management Market globally in recent times. A list of the new entrants and their approximate date of market entry is set out in **Appendix 10**, divided into global and New Zealand new entrants.

*The Proposed Transaction Will Not Affect Expected Rate Of Expansion Of New Entrants*

240. The Proposed Transaction will not in any way slow the growth of new competitors' entry or expansion. The Parties do not have control over any essential facility or necessary IP rights, nor do they (or could they) require resellers or integrators to work exclusively with them.

**Countervailing Power from Customers**

241. The Parties' customers for enterprise key management solutions are typically highly sophisticated, have a clear understanding of their key management and data protection requirements, and can and will switch between suppliers if required.  
[

].

242. Customers in the financial services sector have in the past been in a good position to sponsor new entry. [

].

243. When launching a new application or expanding an existing application involving large purchases of key management solutions, customers can easily switch from one key management solution to another and, within each key management segment, from one supplier to one of the many other suppliers. Customers will be assisted in identifying suitable alternative solutions by resellers and system integrators, who are often not tied to one brand or supplier and will make a recommendation based on the enterprise's requirements.

244. [

].

72 For a list of recent entrants in the Enterprise Key Management market see **Appendix 10**.

## Risk of Coordination Post-Acquisition is Low

245. The Proposed Transaction will not increase the risk of coordinated conduct. The Enterprise Key Management Market is a fragmented, non-transparent, and highly innovative market with a large number of competitors offering a large variety of heterogeneous products to meet customer demand. This means that any risk of tacit collusion is marginal.

## No Substantial Lessening of Competition Even if Market is Limited to Payment HSMs or GP HSMs Only

### *Payment HSMs*

246. For the reasons outlined above, the Parties do not consider that the supply of Payment HSMs should be viewed as a separate market. The Parties have set out in this section, for completeness, the reasons why there is unlikely to be a substantial lessening of competition in the Payment HSMs segment of the Enterprise Key Management Market post-Proposed Transaction.

247. Thales will have no ability or incentive to increase the price of the Parties' Payment HSMs, or decrease the service that it provides in relation to those HSMs (e.g. technical support, maintenance and repairs etc) post-Proposed Transaction for the following reasons:

- 247.1 The Parties' combined share globally is not substantial, and the Parties are subject to constraints globally: Companies supply the same products around the world, all sourced from manufacturing sites in the Northern Hemisphere and often sold into multiple countries with no on-the-ground personnel. [

]. This reflects the fact that the size of this part of Gemalto's business in New Zealand is [ ] and, as expanded on further below, there are not contestable sales of Payment HSMs each year in New Zealand in any event.

- 247.2 Other competitors exist in New Zealand: The Parties understand that Micro Focus (now Utimaco) already supplies its Atalla Payment HSMs in New Zealand. [

].

- 247.3 Other barriers to entry are also low: A company currently supplying Payment HSMs overseas could easily commence sales into New Zealand in a short period of time. Payment HSM suppliers are active globally, have global supply chains, and can generally serve customers remotely. By way of example, Thales services its New Zealand Payment HSM business with [

]. Further, a new entrant need not seek to undertake local sales directly at all. It could readily commence supplying Payment HSMs in New Zealand through a local reseller ([ ]), of which there are many

available, thereby taking advantage of the reseller's existing experience and customer contacts.

**247.4** As previously discussed, issues such as transportation costs or import barriers (e.g. quotas) will not cause any problems for a new entrant into New Zealand, and there will not be any need to develop new products for the local market since the existing globally-supplied products are already perfectly suited to local requirements. [

].

**247.5** Customers exercise substantial countervailing buyer power: Customers that acquire Payment HSMs in New Zealand are typically large and sophisticated – primarily comprising the major banks and other organisations in the financial services sector – and will have several options available to them to constrain Thales' conduct post-Proposed Transaction as noted above.

**247.6** Future innovation will decrease role of Payment HSMs: As mentioned above, Payment HSM aaS is already offered by competitors outside New Zealand, and the Parties are aware that others, including AWS, are also likely to offer HSM aaS solutions for payment applications to replace on-premise Payment HSMs. It is likely that those competing solutions will become widely accepted and ultimately certified in the future, thereby putting even more pressure on suppliers of conventional Payment HSMs.

#### *GP HSMs*

- 248.** GP HSMs have similar characteristics to Payment HSMs (e.g. on-premise hardware devices), but are not specialised for payment applications.
- 249.** In respect of GP HSMs, Thales and Gemalto compete, and post-Proposed Transaction will continue to compete, with a number of strong suppliers both globally and in New Zealand (including for instance AEP, HP, IBM, Ultra Electronics, Utimaco and Yubico, and others such as the aggressive new entrant Hashicorp). The GP HSM space is therefore highly competitive.
- 250.** Moreover, in the near future, the Parties believe that the disruptive nature of the new HSM aaS and other key management solutions (e.g. cloud-based solutions, dedicated software based on multi-party computation or microprocessors) will have a direct impact on competitive conditions even for on-premise GP HSMs, and this is already evident today. As a result, the Parties believe that the Proposed Transaction will not give rise to any lessening of competition in respect of GP HSMs, even if the supply of GP HSMs was viewed as a separate product market (which, for all the reasons previously discussed, the Parties consider would not be the correct way to view the market).

#### **Conclusion**

- 251.** For all the reasons described above, particularly the highly innovative and competitive nature of all of the relevant markets and the large number of major alternative suppliers in each segment, the Parties are confident that the Proposed Transaction will not give rise to any lessening of competition for enterprise key management now, or in the foreseeable future.



## Part I – Competition Assessment for Enterprise Encryption Software Market

252. In this section, we deal with:
- 252.1 The relevant market shares of the key participants in the Enterprise Encryption Software Market;
  - 252.2 The constraints on the merged entity post-acquisition from existing competition;
  - 252.3 The constraints on the merged entity post-acquisition from potential competition;
  - 252.4 Countervailing power from major customers; and
  - 252.5 Why the risk of coordination post-acquisition is low.
253. For the reasons outlined below, the Parties are confident there will be no lessening of competition, let alone a substantial lessening of competition, in relation to the supply of enterprise encryption software for data at rest and in use, either globally or in New Zealand in particular, as a result of the combination of their operations through the Proposed Transaction.

### Market Shares

254. The Parties provide share data below for the Enterprise Encryption Software Market. Share data is provided on a global level, as there is no reliable local New Zealand share data.
255. The methodology and sources of the market share data used are expanded on in **Appendix 7**.
256. The Parties' and their primary competitors' estimated global<sup>73</sup> value-based market shares in enterprise encryption software between 2015 and 2017 are provided in the table below.<sup>74</sup>

Global market shares by value for the supply of enterprise encryption software for data at rest/in use (2015-2017)						
Company	2015		2016		2017	
	Revenue (Mn €)	Share (%)	Revenue (Mn €)	Share (%)	Revenue (Mn €)	Share (%)
Thales	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Gemalto	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
<b>Combined</b>	<b>[ ]</b>	<b>[ ]</b>	<b>[ ]</b>	<b>[ ]</b>	<b>[ ]</b>	<b>[ ]</b>

73 In each case excluding China (as set out in Part E above under Geographic Dimension).

74 Market share data is based on IDC data. For an overview of the methodology and sources used to calculate this market share data see **Appendix 7**.

Microsoft	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Oracle	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Dell	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Seagate SEDs	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
IBM	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Micro Focus	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Symantec	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
McAfee	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Red Hat	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Check Point	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Sophos	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Veritas	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Protegrity	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Informatica	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Teradata	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
WinMagic	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Hitachi	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
NetApp	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Ionic Security	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Trend Micro	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
First Data	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Fujitsu	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
BlackBerry	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Liaison Techn.	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Futurex	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Cloudera	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Intuit Porticore	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Imperva	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
PKWARE	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

Zix Corp	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
InterSystems	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
HyTrust	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Mocana	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
CA Technologies	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
Others	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
<b>Total</b>	<b>[ ]</b>	<b>100%</b>	<b>[ ]</b>	<b>100%</b>	<b>[ ]</b>	<b>100%</b>

Source: IDC and the Parties

**257.** In 2017, the Parties' combined market shares (in value) amounted to [ ] worldwide (Thales [ ]; Gemalto [ ]). This is within the Commission's concentration indicator threshold.

**258.** The Parties global shares have remained relatively consistent over the last three years (from 2015 to 2017), as have their competitors' shares.

**259.** In 2017, the Parties had combined revenue for enterprise encryption software in New Zealand of approximately [ ] (Thales [ ]; Gemalto [ ]). The Parties' presence in New Zealand for enterprise encryption software is therefore minimal.

### Constraints from Existing Competition

**260.** The Parties consider that there will be strong constraints on the merged entity post-acquisition from existing competition. The reasons for this are set out below.

#### *The Enterprise Encryption Software Market is Highly Competitive*

**261.** The Parties are small players (with a combined global share in 2017 of only [ ]) in a market dominated by large, well-established competitors such as Dell EMC, IBM, McAfee and Symantec, fast-growing cloud powerhouses including AWS, Google Cloud Platform, and Microsoft Azure, and innovative new entrants such as Cloudera, Hashicorp, Ionic Security, and Skyhigh. As shown in the table below, there are currently more than 30 suppliers of encryption software to which customers, including those in New Zealand, could turn for products and services.

#### *No Capacity Constraints in the Industry*

**262.** There are no relevant capacity constraints in the production of enterprise encryption software products. The production of encryption software does not require significant investment in production facilities.

#### *The Parties do not exercise a unique competitive constraint on one another*

**263.** The Parties are small players in this market, and do not view each other's products in enterprise encryption software as particularly close substitutes. Indeed, all or most enterprise encryption software solutions offer largely similar levels of performance, functionality and customer support. In the Parties' view, standalone

encryption software vendors such as IBM, Micro Focus (Voltage), and Protegrity; cloud-based vendors such as AWS, Azure KMS, and Google Cloud Platform; and native operating system encryption such as Linux LUKS and Microsoft BitLocker all offer similar types of software encryption use cases as the Parties' products.

264. This is consistent with the Parties' market position. Even when viewed at the data application level, the Parties' global combined share remains very modest: [ ] for file/folder encryption software, [ ] for application-level encryption software, [ ] for database encryption software and less than [ ] for tokenisation/data masking software.

### **Constraints on the Merged Entity Post-Acquisition from Potential Competition**

265. The market for enterprise encryption software is a fast growing and dynamic market characterised by low entry barriers and significant recent entry. New suppliers can – and do – enter the market. Entry is facilitated by the growing use of open-source encryption software, the lack of a need for expensive manufacturing facilities or intellectual property licenses, the limited need for local sales forces ([ ]), and the lack of legal barriers to entry. Examples of new entrants globally since 2015 alone include Baffle, Couchbase, DataLocker, DataStax, GCHQ, HashiCorp, Hortonworks, Ionic Security, Netskope, Protegrity, Pure Storage, SaltStack, Secomba, Sophos and TokenEx.

### **Countervailing Power from Customers**

266. Customers can readily switch between suppliers and solutions. The Parties' customers for enterprise encryption software are typically highly sophisticated, have a clear understanding of their data protection requirements, and can and will switch between encryption software suppliers relatively easily.
267. They may be aided in this process by channel distributors or resellers, who assist customers to identify the right products and services for their requirements from a range of different suppliers. Resellers provide a wide range solution set around IT Security products and services, including alternative solutions from those offered by the Parties.
268. A number of Thales' customers globally have recently switched suppliers including, but not limited to, the following:

268.1 [

].

268.2 [

].

268.3 [

].

268.4 [

].

268.5 [

].

#### **Risk of Coordination Post-Acquisition is Low**

269. The Proposed Transaction will not increase the risk of coordinated conduct. Like the Enterprise Key Management Market, the Enterprise Encryption Market is a fragmented, non-transparent, and highly innovative market with a large number of competitors offering a large variety of heterogeneous products to meet customer demand. This means that any risk of tacit collusion is marginal.

#### **Conclusion**

270. As a result of the matters described above, any attempt by Thales to increase the price of its enterprise encryption software, or decrease the quality of its service in relation to that software, in New Zealand post-Proposed Transaction will be rapidly defeated. Thales will have no ability or incentive to maintain a price increase because it will lose customers to one of the many alternative suppliers in the market. As a result, the Proposed Transaction will have no effect on the competitive conditions in this market.

## Part J – Confidentiality

- 271.** Both public and confidential versions of this clearance application have been provided to the Commission.
- 272.** Confidentiality is sought in respect of the information in the confidential version of this application that is highlighted in coloured shading. Confidentiality is sought for the purposes of section 9(2)(b) of the Official Information Act 1982 on the grounds that:
- 272.1** the information is commercially sensitive and contains valuable information which is confidential to either or both of the merger parties; and
  - 272.2** disclosure of it is likely to prejudice unreasonably the commercial position of the merger parties.
- 273.** Thales requests that it be notified of any request made to the Commission under the Official Information Act for release of the confidential information, and that the Commission seeks its views (and those of Gemalto where applicable) as to whether the information remains confidential and commercially sensitive at the time responses to those requests are being considered.
- 274.** The above applies equally in respect of any additional information provided to the Commission that is expressed to be confidential.

## Part K – Declaration

I, Isabelle Simon, have prepared, or supervised the preparation, of this notice seeking clearance.

To the best of my knowledge, I confirm that:

- all information specified by the Commission has been supplied;
- if information has not been supplied, reasons have been included as to why the information has not been supplied;
- all information known to me that is relevant to the consideration of this notice has been supplied; and
- all information supplied is correct as at the date of this notice.

I undertake to advise the Commission immediately of any material change in circumstances relating to the notice.

I understand that it is an offence under the Commerce Act to attempt to deceive or knowingly mislead the Commission in respect of any matter before the Commission, including in these documents.

I am an officer of the company and am duly authorised to submit this notice.

### **Name and title of person authorised to sign:**

Isabelle Simon  
Group Secretary and General Counsel  
Thales S.A.

**Sign:** \_\_\_\_\_

**Date:** \_\_\_\_\_

## Appendix 1 – Transaction Documents

- Merger Agreement between Thales and Gemalto regarding the combination of Thales and Gemalto through a public offer by Thales for all issued and outstanding ordinary shares of Gemalto, dated 17 December 2017



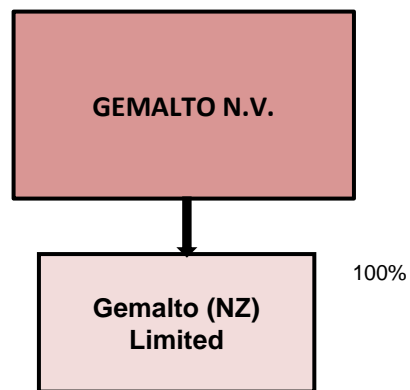
## Appendix 2 – Corporate Structure Charts

### Current ownership of Thales

The current ownership of Thales is set out in the **attached** corporate structure chart.

### Current ownership of Gemalto

The current ownership of Gemalto is set out below.



## Appendix 3 – Audited Financial Statements and Annual Report

### Thales

The latest quarterly, consolidated, unaudited financial information of Thales can be found here: <https://www.thalesgroup.com/en/worldwide/press-release/2017-full-year-results>.

The Annual Report and Accounts for Thales (for the year ending 31 December 2016) can be found here: [https://www.thalesgroup.com/sites/default/files/database/document/2018-05/2017\\_registration\\_document.pdf](https://www.thalesgroup.com/sites/default/files/database/document/2018-05/2017_registration_document.pdf).

### Gemalto

The latest audited financial statements of Gemalto NZ (for the year ended 31 December 2017) are **attached**.

Gemalto N.V.'s most recent Annual Report can be found here: <https://www.gemalto.com/investors-site/Documents/2018/Annual-report-2017.pdf>.

## Appendix 4 – Total Sales Revenues

### Thales

Thales' audited 2016 and 2017 turnover in New Zealand was:

- [ ];
- [ ].

This included revenue of:

Product	2016 Revenue (€)	2017 Revenue (€)
Payment HSMs (including allocated maintenance revenue)	[ ]	[ ]
General Purpose HSMs (including allocated maintenance revenue)	[ ]	[ ]
Enterprise Encryption Software	[ ]	[ ]
<b>Total</b>	<b>[ ]</b>	<b>[ ]</b>

### Gemalto

Gemalto NZ's 2016 and 2017 audited revenue was:

- [ ];
- [ ].

This included revenue of:

Product	2016 Revenue (€)	2017 Revenue (€)
Payment HSMs (including allocated maintenance revenue)	[ ]	[ ]
General Purpose HSMs (including allocated maintenance revenue)	[ ]	[ ]
Enterprise Encryption Software	[ ]	[ ]
	[ ]	[ ]
Network Encryptors	[ ]	[ ]
Other	[ ]	[ ]
<b>Total</b>	<b>[ ]</b>	<b>[ ]</b>

## Appendix 5 – New Zealand Competitors and Industry Associations

### NZ Competitors

Competitors	Contact Details
<b>Microsoft (Azure)</b>	Contact Person: Barrie Sheers (Managing Director) Address: Viaduct Harbour Avenue, Auckland, 1010, New Zealand Tel: +64 936 25800 Email: bsheers@microsoft.com
<b>Micro Focus (Voltage)</b>	Contact Person: Glen Stenbeck (New Zealand Territory Manager) Address: 23-29 Albert Street, Auckland, 1010, New Zealand Tel: +1 801 861 7000 Email: glen.stenbeck@microfocus.com
<b>Protegrity</b>	Contact Person: Alissandra Burack (Vice President) Address: 333 Ludlow Street Windsor Road, CT 06902, Stamford (Berkshire), United Kingdom Tel: +44 149 485 7762 Email: alissandra.burack@protegrity.com
<b>Venafi</b>	Contact Person: Jeff Hudson (Chief Executive Officer) Address: 175 E 400 S, Suite 300, Salt Lake City, UT 84111, United States Tel: +1 801 676 6900 Email: jeff.hudson@venafi.com
<b>SSH Communication (Cert+ &amp; UKM)</b>	Contact Person: Markku Karppi (General Counsel) Address: Kometintie 3, 00380, Helsinki Tel: +358 205 007 000 Email: markku.karppi@ssh.com
<b>AWS (KMS)</b>	Contact Person: Tom Dacombe-Bird (Country Manager New Zealand) Address: 89 Quay Street, Auckland, 1010, New Zealand Tel: Not Available Email: dacombebird@amazon.com
<b>IBM (KMS)</b>	Contact Person: Mike Smith (Managing Director New Zealand) Address: 30 Gaunt Street, PO Box 6840, Wellesley Street, Auckland, 1010, New Zealand Tel: +64 4576 5999 Email: mike.smith@nz.ibm.com
<b>Oracle (KMS)</b>	Contact Person: Robert Gosling (Managing Director New Zealand) Address: 162 Victoria Street West, Auckland, 1010, New Zealand Tel: +64 9977 2100 Email: robert.gosling@oracle.com
<b>Google (KMS)</b>	Contact Person: Caroline Rainsford (Country Director New Zealand) Tel: Not Available Email: crainsford@google.com
<b>Salesforce (Shield KMS)</b>	Contact Person: Craig Skinner (Commercial Sales Director) Address: 55 Collins Street, Melbourne, Victoria, 3000, Australia Tel: +64 9601 8900 Email: skinnercraig@salesforce.com
<b>Entrust DataCard</b>	Contact Person: Michael Robertson (Regional Director for South Pacific)

	<p>Address: 14-22 Triton Drive, Albany, 0632, New Zealand  Tel: +64 9451 9555  Email: michael.robertson@entrustdatacard.com</p>
<b>Randtronics</b>	<p>Contact Person: Serge Knezevic (Sales Director)  Address: North Ryde, NSW, 2113, Australia  Tel: +61 421 739 828  Email: serge.knezevic@randtronics.com</p>
<b>Salt Group (Echidna KMS)</b>	<p>Contact Person: Ross Oakley (CEO and Founder)  Address: 459, Collins Street, Melbourne, Victoria, 3000, Australia  Tel: +61 396 144 416  Email: roackley@saltgroup.com.au</p>
<b>Cogito</b>	<p>Contact Person: Richard Brown (Managing Director)  Address: 9 Sydney Avenue, Barton, 2600, Australia  Tel: +61 417 832 021  Email: richard.brown@cogitogroup.net</p>

## NZ Industry Associations

Association	Contact Details
<b>Biometrics Institute</b>	<p>P O Box 576  Crows Nest NSW 1585  Australia  Phone: +61 2 9431 8688  www.biometricsinstitute.org</p>

## Appendix 6 – Key Customers

### Thales Key Resellers

[

].

Reseller	Contact	2017 Order Intake Value (US)
[ ]	[ ]	[ ]
[ ]	[ ]	[ ]
[ ]	[ ]	[ ]
[ ]	[ ]	[ ]
[ ]	[ ]	[ ]
[ ]	[ ]	[ ]

[

]

*Enterprise Key Management*

End user	Contact person	Position	Email address	Telephone number	Business/ Postal address	2017 Order Intake Value (US)
<b>Payment HSM (payShield)</b>						
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
<b>GP HSM (nShield)</b>						
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

## Gemalto Key Customers

### Payment HSMs

Customer	Contact person	Email address	Telephone number	Business/ Postal address	2017 Revenue	Type of customer
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]

### General Purpose HSMs

Customer	Contact person	Email address	Telephone number	Business/ Postal address	2017 Revenue	Type of customer
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]
[ ]	[ ]	[ ]	[ ]	[ ]	[ ]	[ ]



## Appendix 7 – Methodology and Sources of Market Share Data

275. [

]:

275.1 [

].

275.2 [

]:

275.2.1 [

];

275.2.2 [

];

275.2.3 [

].

275.3 [

].

276. [

].

277. [

].

278. [

,<sup>75</sup>

].

75 [

]

[ ]

279. [ ]:

279.1 [ ];

279.2 [ ];

279.3 [ ];

279.4 [ ];

279.5 [ ];

279.6 [ ];

279.7 [ ]

].

280. [ ]

].

281. [ ]

].

282. [ ]

].

## Appendix 8 – Third Party Market Studies

- IDC, Worldwide Data Security Taxonomy, 2016
- MarketsandMarkets, Enterprise Key Management Market, Global Forecast to 2022

## Appendix 9 – Overview of Competing Global Players with Enterprise Key Management Capabilities

Company	Encryption Software Or Hardware With Key Management Capabilities	Dedicated Key Management Software	General Purpose HSMs	Payment HSMs	HSMs aaS	Cloud-Based Key Management Solutions	TPMs And Microprocessors With Built-In Key Management Capabilities
Thales	✓	✗	✓	✓	✗	✗	✗
Gemalto	✓	✗	✓	✓	✓	✗	✗
Alibaba Cloud	✗	✗	✗	✗	✗	✓	✗
AWS	✗	✗	✗	✗	✓	✓	✗
Arm	✗	✗	✗	✗	✗	✗	✓
Asus	✗	✗	✗	✗	✗	✗	✓
Atos	✗	✓	✓	✓	✗	✗	✗
Bluefin	✗	✗	✗	✗	✓	✗	✗
Bloombase	✓	✗	✗	✗	✗	✗	✗
Box	✗	✓	✗	✗	✗	✗	✗
Cavium	✗	✗	✓	✗	✗	✗	✗
CCV	✗	✗	✗	✓	✗	✗	✗
Check Point Software Technologies	✓	✗	✗	✗	✗	✗	✗
CipherCloud	✓	✗	✗	✗	✗	✗	✗
Commvault	✓	✗	✗	✗	✗	✗	✗
Cryptera	✗	✗	✗	✓	✗	✗	✗
Cryptomathic	✗	✓	✗	✗	✗	✗	✗
DataLocker	✓	✗	✗	✗	✗	✗	✗
Device Authority	✗	✓	✗	✗	✗	✗	✗

DocuSign	x	x	✓	✓	x	x	x
Dropbox	x	x	x	x	x	✓	x
Eruces	✓	x	x	x	x	x	x
Equinix Telecity	x	x	x	x	✓	✓	x
Fornetix	x	✓	x	x	x	x	x
Fortanix	x	✓	x	x	x	x	x
Fujitsu	✓	x	x	x	x	x	x
Futurex	x	x	✓	✓	x	x	x
Gigabyte	x	x	x	x	x	x	✓
Google	x	x	x	x	x	✓	x
Hewlett Packard Enterprise	x	x	x	x	x	x	✓
HID	x	x	x	✓	x	x	x
Hitachi	✓	x	x	x	x	✓	x
Huawei	x	x	x	x	x	✓	x
IBM	✓	x	✓	x	✓	✓	x
Infineon	x	x	x	x	x	x	✓
Intel	x	x	x	x	x	x	✓
Ionic Security	✓	x	x	x	x	x	x
KeyNexus	x	✓	x	x	x	✓	x
McAfee <sup>76</sup>	x	x	x	x	x	✓	x
Microchip	x	x	x	x	x	x	✓
Micro Focus	✓	x	✓	✓	x	x	x
Microsoft	✓	✓	x	x	x	✓	x
NetApp	✓	x	x	x	x	x	x
NuCypher	x	x	x	x	x	✓	x

76 McAfee was owned by Intel from 2011 until Intel sold its majority stake in McAfee to TPG Capital and Thoma Bravo in 2017. Thus, in the sales and market shares for 2014-2017 provided below, McAfee's sales are included in Intel's sales.

Nuvoton	x	x	x	x	x	x	✓
Oracle	✓	✓	x	x	x	x	x
PKWARE	✓	x	x	x	x	x	x
Prism	x	x	x	✓	x	x	x
Protegrity	✓	x	x	x	x	x	x
Qualcomm	x	x	x	x	x	x	✓
Quantum	x	✓	x	x	x	x	x
Realsec	x	x	✓	✓	x	x	x
RSA Security (Dell EMC)	✓	x	x	x	x	x	x
Salesforce	x	x	x	x	x	✓	x
Securosys	x	x	✓	x	✓	x	x
Sepior	x	x	x	x	x	✓	x
Sophos	✓	x	x	x	x	x	x
ST Microelectronics	x	x	x	x	x	x	✓
Symantec	✓	x	x	x	x	✓	x
Tokheim	x	x	x	✓	x	x	x
Townsend	x	x	✓	x	x	x	x
Trend Micro	✓	✓	x	x	x	x	x
Ultra Electronics	x	✓	✓	✓	x	x	x
Unbound	x	✓	x	x	x	x	x
Utimaco	x	x	✓	✓	✓	x	x
Veeam	✓	x	x	x	x	x	x
Venafi	x	✓	x	x	x	x	x
Veritas	✓	x	x	x	x	x	x
WinMagic	✓	x	x	x	x	x	x
Yubico	x	x	✓	x	x	x	x
Zix	✓	x	x	x	x	x	x
<b>Total suppliers (at least)</b>	<b>26</b>	<b>14</b>	<b>14</b>	<b>14</b>	<b>7</b>	<b>15</b>	<b>10</b>

Source: The Parties

## Appendix 10 – Recent Entrants in the Key Enterprise Management Market

### Worldwide

Company	Year of entrance
Alibaba Cloud	Founded in 2009
AWS	2006
Arm	2008
Bluefin	Founded in 2007
Box	2016
Cavium	2015
Commvault	2017
DataLocker	Founded in 2007
Device Authority	2016
Dropbox	Founded in 2007
Equinix Telecity	2017
Fornetix	Founded in 2014
Fortanix	2017
Google	2011
IBM	2007
Infineon	2013
Intel	2013
KeyNexus	2013
Microsoft Azure	2010
NuCypher	Founded in 2016
Nuvoton	Founded in 2008
Oracle	2007
PKWARE	2016
Qualcomm	2008
Realsec	2001

Salesforce	2016
Securosys	2014
Sepior	2014
Sophos	2016
Trend Micro	2010
Unbound	Founded in 2014
Venafi	2014
Yubico	Founded in 2007
<b>Total new entrants (at least)</b>	<b>33</b>

## New Zealand

Company	Year of Entrance to NZ (where known)
Microsoft (Azure)	2014
Micro Focus (Voltage)	
Protegrity	
AWS (KMS)	2012
IBM (KMS)	2016
Oracle (KMS)	2014
Google (KMS)	
Salesforce (Shield KMS)	



## Appendix 11 – Glossary

Term	Definition
<b>ANSSI</b>	Agence National de la Sécurité des Systèmes d'Information
<b>AES</b>	Advanced Encryption Standard, an example of a standardised algorithm
<b>Cloud-based encryption solutions with key management capabilities</b>	Key management solutions inherently included in cloud-based encryption solutions deployed by cloud service providers to secure data stored on their cloud
<b>Communication, command and control systems</b>	Systems providing the capability and capacity to transmit secure information to each level of the command chain, a tactical and strategic imperative to meet the requirements of armed forces and security forces
<b>CSPs</b>	Cloud Service Providers
<b>Data at rest</b>	Data which is not actively moving from device to device or network to network but is stored in one place
<b>Data in motion</b>	Data actively moving from one location to another, via the internet, private network or the cloud, for example (also called "in transit")
<b>Data in use</b>	Data which is stored in a non-persistent digital state in the computer memory or processed applications and is generally accessible to several persons and devices
<b>Data masking</b>	Masking of specific data elements in databases and file systems using random numbers, patterns, or letters while keeping the data structure.
<b>Dedicated key management software</b>	Runs on a physical or cloud server, used either stand-alone or in combination with hardware to further increase the level of security
<b>DES</b>	Data Encryption Standard, an example of a standardised algorithm
<b>DPoD</b>	Data Protection on Demand: a cloud-based platform that provides a wide range of on-demand encryption and key management services through a simple online marketplace
<b>DSM</b>	Data Security Manager

<b>Encryption software/hardware containing key management capabilities</b>	Key management capabilities inherently included in encryption software/hardware products or integrated as part of a broader solution including one or several encryption software/hardware products
<b>FPE</b>	Format Preserving Encryption: encryption that uses algorithms dedicated to particular data formats (eg credit card numbers), and works by enciphering data without changing the underlying format, for example by maintaining a 16-digit number for a credit card
<b>FTP</b>	File Transfer Protocol
<b>GDPR</b>	European Union General Data Protection Regulation
<b>GP HSM</b>	A dedicated hardware appliance running encryption software to generate, protect, and manage keys in a secure tamper-resistant module
<b>Gemalto</b>	Gemalto N.V.
<b>HSM</b>	Hardware Security Module
<b>HSM aaS</b>	HSM services purchased on a pay per-use basis in lieu of physical, on-premise HSMs, offered either by cloud service providers to secure data stored on their cloud
<b>IaaS</b>	Infrastructure-as-a-service
<b>IoT</b>	Internet of Things
<b>M2M</b>	Machine-to-Machine
<b>Merger Agreement</b>	The agreement entered into on 17 December 2017 between Thales S.A. and Gemalto N.V. for a binding Merger Agreement in respect of the Proposed Transaction
<b>Microprocessors with key management capabilities</b>	Similar to TPMs, in that they provide a secure enclave allowing users to create a dedicated secure operating environment which functions under different (and more secure) operating principles than the traditional microprocessor's environment
<b>Mission services support</b>	After sale support including innovative and extended service solutions - training, life cycle support, repairs, guaranteed levels of operational availability, upgrades and more, including encryption devices, friend or foe identification capabilities, secure tactical radio technology, thermal imaging equipment and electro-optics.

<b>OEM</b>	Original Equipment Manufacturer
<b>Payment HSM</b>	Similar to a GP HSM, but designed to provide high level payment-related functionality (eg PIN processing) and to perform a high volume of payment operations rapidly
<b>PKI</b>	Public Key Infrastructure
<b>Proposed Transaction</b>	Thales' proposed acquisition of 100% of the issued and outstanding shares in Gemalto
<b>Protection systems and mission/combat systems</b>	Systems providing territorial protection and high value asset protection, helping to ensure the highest possible levels of operational effectiveness and precision
<b>RSA</b>	Rivest, Shamir and Adelman, an example of a standardised algorithm
<b>SSL</b>	Secure Sockets Layer: is the default form of protection for Internet communications to secure data in transit across untrusted networks
<b>Surveillance, detection and intelligence systems</b>	Systems that provide all levels of the command and intelligence chain with the most comprehensive understanding of the theatre of operations
<b>TeS</b>	Thales e-Security
<b>Thales or Thales Group</b>	Thales S.A.
<b>Tokenisation</b>	The process of protecting data by replacing sensitive numbers or information with random numbers or letters, and is used most commonly to protect credit card numbers
<b>TPM</b>	Trusted Platform Module: a dedicated security chip mounted as a motherboard component on various computing platforms (e.g. PCs, phones, tablets) which provides a secure hardware enclave to store encryption keys and perform certain key management functions
<b>TLS</b>	Transport Layer Security: encryption protocols that provide communications security over a computer network