EUROPEAN COMMISSION
DG Competition

CASE M.8797 THALES/ GEMALTO

(Only the English text is authentic)

MERGER PROCEDURE
REGULATION (EC) 139/2004

Article 8(2) Regulation (EC) 139/2004

Date: 11/12/2018

EUROPEAN
COMMISSION

Brussels, 11.12.2018
C(2018) 8401 final

PUBLIC VERSION

COMMISSION DECISION

of 11.12.2018

declaring a concentration to be compatible with the internal market and the EEA agreement

(Case M.8797 Thales / Gemalto)

(Only the English text is authentic)

TABLE OF CONTENTS

COMMISSION DECISION

of 11.12.2018

declaring a concentration to be compatible with the internal market and the EEA agreement

(Case M.8797 Thales / Gemalto)

(Only the English text is authentic)

THE EUROPEAN COMMISSION,

Having regard to the Treaty on the Functioning of the European Union,

Having regard to the Agreement on the European Economic Area, and in particular Article 57 thereof,

Having regard to Council Regulation (EC) No 139/2004 of 20.1.2004 on the control of concentrations between undertakings[1], and in particular Article 8(2) thereof,

Having regard to the Commission's decision of 23 July 2018 to initiate proceedings in this case,

Having regard to the opinion of the Advisory Committee on Concentrations[2],

Having regard to the final report of the Hearing Officer in this case[3],

Whereas:

1. INTRODUCTION

(1) On 18 June 2018, the European Commission ("Commission") received notification of a concentration pursuant to Article 4 of Council Regulation (EC) No 139/2004 (the "Merger Regulation")[4] that would result from the proposed acquisition by Thales S.A. ("Thales" or the "Notifying Party", France), of sole control of Gemalto N.V. ("Gemalto", Netherlands) within the meaning of Article 3(1)(b) of the Merger Regulation (the "Transaction").[5] Thales and Gemalto are hereinafter collectively referred to as the "Parties".

(2) The recitals in this Decision are arranged as follows. Section 2 describes the Parties and explains why the Transaction would result in a concentration. Section 3 explains why the concentration brought about by the Transaction has a Union dimension. Section 4 describes the procedure followed in this case. Section 5 describes the

---

1 OJ L 24, 29.1.2004, p. 1 ("the Merger Regulation"). With effect from 1 December 2009, the Treaty on the Functioning of the European Union ("TFEU") has introduced certain changes, such as the replacement of "Community" by "Union" and "common market" by "internal market". The terminology of the TFEU is used throughout this decision.

2 OJ C ...,...200. , p....

3 OJ C ...,...200. , p....

4 OJ L 24, 29.1.2004, p. 1. With effect from 1 December 2009, the Treaty on the Functioning of the European Union ("TFEU") has introduced certain changes, such as the replacement of "Community" by "Union" and "common market" by "internal market". The terminology of the TFEU is used throughout this Decision.

5 Prior notification of a concentration (Case M.8797 — Thales/Gemalto) Publication in the Official Journal of the European Union No (OJ C 222, 26.06.2018, p. 19.).

investigation undertaken by the Commission into the Transaction. Section 6 provides an overview of the enterprise key management solutions sector. Section 7 defines the relevant product and geographic markets. Section 8 sets out the Commission's assessment of whether the Transaction is likely to significantly impede effective competition. Section 9 contains the Commission's assessment of the commitments. Section 10 contains the Commission's conclusions.

2. THE PARTIES AND THE TRANSACTION

(3) Thales is an international group registered in France and listed on the Euronext Stock Exchange in Paris. Thales is active globally in five main areas: (i) aeronautics; (ii) space; (iii) ground transportation; (iv) defence; and (v) security. In 2017, it had global revenues of EUR 15.8 billion (EUR […] of which in the European Union ("the Union")), operations in 56 countries and 64,100 employees.

(4) 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: (i) mobile platforms & services; (ii) mobile embedded software and products; (iii) payment; (iv) government programs; (v) machine to machine (Internet of Things or "IoT"); and (vi) enterprise security. Gemalto was formed in 2006 as a result of the combination of Axalto Holding N.V. and Gemplus International S.A. In 2017, Gemalto had global revenues of approximately EUR 3 billion (EUR […] of which in the Union), operations in 47 countries and 15,000 employees.

(5) According to a merger agreement entered into on 17 December 2017 (the "Merger Agreement"), Thales will acquire all issued and outstanding ordinary shares and American depository shares in Gemalto by way of a recommended full public offer governed by Dutch law, which will be extended in particular to France and the United States of America ("U.S.A"). The Merger Agreement is subject to the satisfaction or waiver of customary conditions, including but not limited to: (i) regulatory approvals; (ii) a minimum acceptance level of at least 67% of Gemalto shares; (iii) no material adverse effect having occurred; (iv) no material breach of the Merger Agreement having occurred; and (v) no superior offer having been made or agreed upon.

(6) Therefore, the Transaction would result in a concentration within the meaning of Article 3(1)(b) of the Merger Regulation.

3. UNION DIMENSION

(7) The undertakings concerned have a combined aggregate world-wide turnover of more than EUR 5 000 million (Thales: EUR 15 795 million; Gemalto: EUR 2 972 million; combined: EUR 18 767 million; in 2017). Each of them has an Union-wide turnover in excess of EUR 250 million (Thales: EUR […]; Gemalto: EUR […]; in 2017). Neither Thales nor Gemalto achieves more than two-thirds of their aggregate Union-wide turnover within one Member State.

(8) Therefore, the concentration brought about by the Transaction has a Union dimension within the meaning of Article 1(2) of the Merger Regulation.

4. THE PROCEDURE

(9) The Transaction was notified on 18 June 2018.

(10) After a preliminary examination of the notification and based on the first phase market investigation, the Commission concluded that the Transaction raised serious doubts as to its compatibility with the internal market as regards the market for Hardware Security Modules and adopted a decision to initiate proceedings pursuant to Article 6(1)(c) of the Merger Regulation on 23 July 2018 (the "Article 6(1)(c) Decision").

(11) On 26 July 2018, the second phase investigation period was extended by 20 working days at the request of the Notifying Party pursuant to the first sentence of the second subparagraph of Article 10(3) of the Merger Regulation.

(12) On 21 August 2018, the Notifying Party submitted its written comments to the Article 6(1)(c) Decision (the "Article 6(1)(c) Response").

(13) On 10 October 2018, the Notifying Party submitted commitments pursuant to Article 8(2) of the Merger Regulation in order to address the competition concerns identified by the Commission.

(14) On 7 November 2018, the Notifying Party submitted revised commitments pursuant to Article 8(2) of the Merger Regulation in order to address the competition concerns identified by the Commission.

(15) The Advisory Committee discussed the draft of this Decision on 28 November 2018 and issued a unanimous positive opinion.[6]

5. THE INVESTIGATION

(16) Prior to the notification of the Transaction, the Commission sent 7 requests for information ("RFIs") to the Parties, responses to which were included in that notification. The Commission also conducted several interviews with the Parties' customers and competitors.

(17) During the first phase investigation the Commission sent 3 RFIs to the Parties. The Commission also conducted several interviews with the Parties' customers and competitors.

(18) During the second phase investigation, the Commission sent over 17 RFIs to the Parties' competitors, customers and resellers. 13 RFIs were sent to the Parties, including two detailed internal documents requests, resulting in the submission of about 2.3 million internal documents from Thales and Gemalto. Further, the Commission conducted several interviews with the Parties' customers, competitors and resellers. On 23 August 2018 and 13 September technical meetings took place with the Parties to further the understanding of the Parties' products and offering.

6. THE ENTERPRISE KEY MANAGEMENT SOLUTION SECTOR

(19) In this Section, the Commission provides an overview of the enterprise key management solutions ("KMS") sector where the Parties' activities overlap. The purpose of this Section is to set the framework and provide the context for the assessment undertaken in Sections 7 and 8.

---

[6] At the Advisory Committee 10 present Member States agreed that that the Transaction must be declared compatible with the internal market and the EEA Agreement in accordance with Article 2(2) and 8(2) of the Merger Regulation and Article 57 of the EEA Agreement.

6.1. Introduction

(20) Encryption is the most common method for securing data. Encryption transforms plain text into cypher text and requires an encryption algorithm and at least one encryption key. Efficient encryption requires effective encryption key management, that is a solution that manages the lifecycle of the keys that protect sensitive data.

(21) Enterprises can create, store, and manage their encryption keys in a variety of different ways, depending on their security needs, which are either required by regulation or by the industry. KMS can be stand-alone software or hardware products or part of broader encryption software with key management functionality. The following segments can be distinguished for KMS: (i) encryption software or hardware with key management capabilities, (ii) dedicated key management software, (iii) on-premise General Purpose Hardware Security Modules ("GP HSMs"), (iv) on-premise payment HSMs ("Payment HSMs"), (v) HSMs as a service ("HSMs aaS"), (vi) cloud-based KMS, and (vii) trusted platform modules ("TPMs") and microprocessors with built-in key management capabilities.

6.1.1. HSMs

(22) GP HSM is a dedicated hardware appliance running on encryption software to generate, protect, and manage keys in a secure tamper-resistant module. GP HSMs are deployed for various applications similar to those in which dedicated key management software is used, including, for example, authentication and verification, code and document signing, public key infrastructure or credential management, key protection, application-level or database encryption.

(23) For certain specific payment processing functions (including PIN processing and P2PE) enterprises may use Payment HSMs. Payment HSMs provide high level payment-related functionality and are designed to perform a high volume of payment operations rapidly. Apart from general certifications (discussed further in Section 6.5), they are certified to industry-specific standards such as PCI-HSM standards to conform to industry requirements.[7]

(24) Customers purchase HSMs from vendors, such as the Parties, as well as through resellers, system integrators, and distributors. Value-added resellers provide services to assist end-customers with efficient implementation and integration (such as consulting, deployment, and support services) on top of the KMS, while system integrators integrate key management solutions (including HSMs) in larger solutions and often also provide additional services on top of these solutions.

6.1.2. HSMs aaS and cloud-based key management solutions offered aaS

(25) Customers moving data to the cloud can rely on the data security solution provided by the Cloud Service Providers ("CSPs") as part of their cloud storage service offering. Customers can purchase key management aaS, including HSMs aaS and cloud-based KMS offered aaS from HSM aaS vendors or CSPs.

(26) HSMs aaS are based on physical GP HSMs installed on the vendors' premises. HSM aaS vendors either offer customers exclusive access to an entire GP HSM, so-called "single-tenancy," or divide a GP HSM into multiple separate HSM instances, thereby allowing two or more (up to 50) customers ("tenants") to share a single HSM box, i.e. "multi-tenancy." HSM aaS allows for a separation of duties between the

[7] Payment Card Industry (PCI).

company, which controls the keys, and the vendor, who monitors and manages the HSMs.

(27) Customers willing to port keys across cloud providers can use cloud agnostic solutions. For example, customers can use Bring Your Own Key ("BYOK") solutions and use keys held in their own on-premise KMS and HSMs for data run in cloud applications. Customers can also use cloud-agnostic HSM aaS such as Gemalto's Data Protection on Demand ("DPoD") offering to manage keys across different CSP environments (discussed further in Section 6.4).

6.2. Manufacturers of HSMs

(28) The main manufacturers of HSMs are discussed in turn in the recitals (29)-(41).

(29) In 2016, Thales acquired Vormetric, a supplier of data protection solutions in physical, virtual and cloud infrastructures. In addition, in 2008 Thales acquired NCipher through which Thales became active in HSMs. Thales is active in three key management segments: (i) GP HSMs with its nShield lines; (ii) Payment HSMs with its payShield lines; and (iii) encryption software/hardware with key management capabilities with its Vormetric encryption products.

(30) In 2015, Gemalto acquired SafeNet, thereby becoming active in enterprise key management. Gemalto sells its SafeNet Luna and Protect Server GP HSMs, Safenet Luna EFT Payment HSMs, HSM management and monitoring solutions, and a DPoD solution (i.e. HSM aaS). With regard to Payment HSMs in particular, Gemalto became active in this segment through Eracom, a company acquired by SafeNet in 2005, which was mainly active in the Asia-Pacific region.

(31) Utimaco is a German-based company that provides hardware-based, high-security appliances (HSMs) and compliance solutions for telecommunication provider regulations. After developing GP HSMs, Utimaco released an HSM aaS solution (April 2018) and launched its in-house Payment HSM line (2017). Utimaco has also recently acquired MicroFocus' Payment HSM business unit (Atalla).[8]

(32) Atos is a French-based company that provides global digital services. Its global solutions involve Consulting & Systems Integration services, Managed Services & Business Process Outsourcing, Cloud operations, Big Data & Cyber-security solutions.[9] Atos offers cyber security and online payment solutions through its Bull and Worldline offerings, including GP and Payment HSMs and KMS.[10] In addition to being a competitor of the Parties, Atos has also had a supplier and customer relationship with Thales and Gemalto in the past decade.[11]

(33) Cavium is an electronics component company active in infrastructure solutions, security, storage, connectivity and baseband processing, which is based in the U.S.A.[12] GP HSMs constitute one of the products which are deployed, manufactured and supplied by Cavium's solutions business unit. Cavium's GP HSMs are used by OEM customers, as well as CSPs (to offer HSM aaS and cloud based KMS).[13]

(34) DocuSign is a company that provides solutions in response to digital transaction management and digital signature issues, which is based in the U.S.A. The

---

8 https://hsm.utimaco.com/news/utimaco-cleared-to-complete-acquisition-of-atalla/

9 Replies to Questionnaire Q1 – competitors of 19 June 2018, question A.1.

10 Non-confidential minutes of conference calls with Atos of 30 May and 5 June 2018.

11 Non-confidential minutes of conference calls with Atos of 30 May and 5 June 2018.

12 Annex R to Article 6(1)(c), Response, para 15.

13 Annex R to Article 6(1)(c), Response, para 17.

acquisition of Algorithmic Research (2015) allowed Docusign to add GP HSMs to its offering.[14]

(35) Futurex is a company that provides security solutions, including secure encryption, storage, and transmission of sensitive data. Originally active in Payment HSMs in the U.S.A. and South Africa, Futurex has started to expand in GP HSMs globally (including Europe). It is based in the U.S.A.[15]

(36) IBM is a company that provides hardware, software, hosting solutions, GP HSMs (from Gemalto) and consulting services.[16] It is based in the U.S.A. IBM's GP HSMs are distributed as part of a complete integrated IT solution or as a stand-alone product.[17]

(37) MicroFocus is a company that provides a large range of IT solutions, based in the United Kingdom ("UK"). Its enterprise security division includes Voltage (encryption software) and Atalla product line (HSMs and hardware-based KMS). MicroFocus does not provide hosted services (HSM aaS and cloud-based KMS).[18]

(38) Prism is a South African-based subsidiary of Net1. Prism develops HSMs and associated security products for the company's proprietary Universal Electronic Payment System ("UEPS") as well as for banks, electronic payments switches, retail, mobile and utility systems. The majority of the HSM sales are in Africa, however the utility market is global with a focus on emerging markets where new electricity and water infrastructure is being rolled out.[19]

(39) Realsec is a Spanish-based company that provides KMS and (GP and Payment) HSMs since 2001.[20] Both GP and Payment HSMs are manufactured by its own product line and distributed with the support of business partners (Ultra Electronics).[21] Realsec's HSMs are used by enterprise and government customers for applications purposes, including PKI, email encryption, digital signing, and time stamping.[22]

(40) Securosys is a Swiss-based company that entered the GP HSMs market in 2015. Its GP HSMs are manufactured in Switzerland and mainly sold to Swiss customers.[23]

(41) Yubico is a company that provides authentication solutions, encryption software and, since 2017, also GP HSMs. It is based in the U.S.A. Yubico's products are used by CSPs, IT companies and other large companies.[24]

6.3. Distribution channels

(42) The purchasing process enterprises apply in choosing their KMS varies from customer to customer. Enterprises with experience managing their own data centres tend to interact directly with the vendors in selecting a product, although they may ultimately purchase the product from a reseller or distributor with whom they work

---

14 Annex R to Article 6(1)(c) Response, para 28.
15 Annex R to Article 6(1)(c), Response, section B
16 Annex R to Article 6(1)(c), Response, para 41.
17 Annex R to Article 6(1)(c), Response, para 44.
18 Replies to Questionnaire Q1 – competitors of 19 June 2018, question A.1.
19 Replies to questionnaire Q4 of 10 September 2018, question 1.
20 Annex R to Article 6(1)(c) Response, para 50.
21 Annex R to Article 6(1)(c) Response, para 51.
22 Annex R to Article 6(1)(c) Response, para 50.
23 Annex R to Article 6(1)(c) Response, para 55.
24 Annex R to Article 6(1)(c), Response, para 83.

as well. In such enterprises, the selection is typically made by a Chief Technology or Chief Data Security Officer or the equivalent. Other, possibly less technically sophisticated enterprises, may also rely on value-added resellers, system integrators or distributors. Value-added resellers and system integrators can advise enterprises on the options available and recommend an appropriate choice for the enterprise's needs, often including a whole range of services and other products required for a complete data security solution. These resellers and system integrators, as well as distributors reselling KMS without added value, typically offer a number of competing KMS and do not have exclusive relationships with their suppliers.

(43) Sales of KMS through value-added resellers, integrators, and distributors account for a significant portion of vendors' sales. For example, between 2015 and 2017, approximately [50-60]% of Thales' and [60-70]% of Gemalto's KMS were sold through resellers and distributors globally. Thales sells […] in the EEA, while the vast majority of its sales in the US are […]. Gemalto sells […] in the EEA and roughly […] in the US.

6.4. Cloud service providers

(44) CSPs purchase HSMs from HSM manufacturers and often combine these with hardware and software features to create their own HSM aaS offering.

(45) Amazon Web Services ("AWS") launched a pioneer HSM aaS solution, based on Gemalto HSMs, in 2013 and released an upgraded version, based on Cavium HSM, in 2017.[25] In 2013, AWS also released a KMS cloud-based solution.

(46) Microsoft launched Azure (set of cloud services) in 2010 and released Key Vault in June 2015 (cloud-based KMS) in which customers can store cryptographic keys for encrypted data.[26]

(47) Google Cloud Platform was launched in 2011 and Google released its KMS in January 2017,[27] which provides encryption and decryption capabilities that facilitate its integration with other cloud services, as well as provides the ability to manage symmetric encryption keys in a cloud-hosted solution.[28] In July 2018, Google also released a HSM aaS […].[29]

(48) IBM Cloud HSM is a HSM aaS offering, launched in 2016, which provides dedicated, single-tenant encryption, key management, and storage using HSMs.[30]

(49) Traditional HSM manufacturers also introduced HSM aaS offerings and cloud-agnostic solutions as described in recitals (50)-(54).

(50) Gemalto's DPoD is a HSM aaS, launched in 2017, which allows customers to use the capacity of GP HSMs owned and managed by Gemalto and located in Gemalto data centers around the world (e.g. Ottawa, Frankfurt, Dallas). DPoD allows customers to use AWS, Azure, or any other clouds or a combination of cloud and on-premise solutions.[31]

---

25 Form CO, Sections 6-7, Chapters I-II para 126

26 Replies to Questionnaire Q7 – Cloud Service Providers of 11 September 2018, question 4 and Form CO, Sections 6-7, Chapters I-II para 80.

27 Form CO, Sections 6-7, Chapters I-II para 278.

28 Replies to Questionnaire Q7 – Cloud Service Providers of 11 September 2018, question 4.

29 Article 6(1)(c) Response, para 128.

30 https://console.bluemix.net/docs/infrastructure/hardware-security-modules/about html#about-ibm-cloud-hsm

31 Form CO, Sections 6-7, Chapters I-II para 73.

(51) Securosys Cloud HSM is a HSM aaS offering, launched in 2017, based on Securosys Primus HSMs. Companies have full control over their HSM partition(s) and can access these using Decanus, Securosys' secure remote control.[32]

(52) Equinix' SmartKey, launched in 2017, is a HSM aaS powered by Fortanix, based on Intel Software Guard Extensions (SGX). Equinix' offering is a cloud-independent, programmable key management and cryptography service hosted on Platform Equinix.[33]

(53) Utimaco's CryptoServer Cloud HSM, launched in 2018, is a HSM aaS offering on vXchnge, a data center services provider. vXchnge customers can store their keys in Utimaco's HSM premise-based appliance in a separate location, independent of the cloud service provider.[34]

(54) Thales offers a solution for public clouds – "nShield BYOK". This solution allows customers to use their nShield HSMs to generate, store, and manage their keys with a view to securing their cloud-hosted applications and databases, regardless of whether the customer is using clouds offered by AWS, Google Cloud Platform or Microsoft Azure. According to the Notifying Party, most if not all GP HSMs have the capability to export key material and as such can be used in a BYOK structure (although a given GP HSM may not support the format used by a particular CSP).

6.5. Standards and certification

(55) Various certification standards exist to differentiate between the levels of security offered by different types of KMS and HSM offered across vendors.

(56) The most recognised certification standards on a worldwide level include the Federal Information Processing Standards ("FIPS") and the Common Criteria ("CC"). The FIPS and the CC ensure that the vendor's claims about the security attributes of the product have been independently verified.

(57) There is no direct correspondence between FIPS levels and CC evaluation assurance levels ("EALs"). FIPS are a set of enterprise standards originating in the US and Canada, while CC certification harmonised pre-existing independent and national security certification standards, developed through the Common Criteria Recognition Agreement ("CCRA"), which was adopted by 28 countries across the world.[35] CC certification may occur under (i) the European approach and (ii) the North American approach.[36] The European approach entails that in addition to the EU Member States which are signatories to the Common Criteria Recognition agreement ("CCRA"), the

---

32 Form CO, Sections 6-7, Chapters I-II para 73.

33 Form CO, Sections 6-7, Chapters I-II para 73 and para 278.

34 Form CO, Sections 6-7, Chapters I-II para 73.

35 The 28 signatories of the CCRA are composed of (i) 17 "authorising" countries, where licensed laboratories can deliver CC certificates and recognise CC certificates issued by other "authorising" countries (i.e. Australia, Canada, France, Germany, India, Italy, Japan, Malaysia, the Netherlands, New Zealand, Norway, Republic of Korea, Spain, Sweden, Turkey, the UK, and the US); and (ii) 11 "consuming" countries, which recognise CC certificates issued by the "authorising" countries (i.e., Austria, the Czech Republic, Denmark, Ethiopia, Finland, Greece, Hungary, Israel, Pakistan, Qatar, and Singapore).

36 The North American approach is less complex than the European approach. National bodies in the "authorising" countries issue certifications of security properties which map to a collaborative Protection Profile ("cPP"). The cPP does not provide for explicit levels and requires minimal evidence from vendors (e.g. no source code review or site visits are required). The certifications are then recognised by all the signatories of the CCRA up to a particular cPP. Common Criteria, as applied under the North American approach, are less widely used.

European countries have established a mutual recognition system applicable only in Europe (i.e. EU and EFTA): the Senior Official Group Information Systems Security ("SOGIS"). The aim of the SOGIS is to coordinate the standardisation of CC certification policies between European certification bodies. The SOGIS sets forth "protection profiles" under which CC verification is performed and ensures the recognition of certificates by all the signatories to the SOGIS.

6.6. Regulatory developments

(58) The regulatory requirements have further boosted the demand for encryption and KMS globally. In particular, the General Data Protection Regulation[37] ("GDPR") recognises the role of encryption in mitigating data security risks and expressly refers to encryption as an appropriate technical measure for data protection. According to third parties' research reports, the GDPR will impact the adoption of encryption solutions and services in non-regulated industries which, in turn, will boost the adoption of both encryption software and KMS.

(59) The GDPR, however, does not require the implementation of specific encryption or KMS, or compliance with any particular certification standard.

(60) The eIDAS Regulation[38] creates a framework for cross-border electronic identification and transactions across EU Member States, establishing consistent standards for (i) electronic identification, (ii) trust services, and (iii) electronic documents. These requirements have led governments and commercial entities to adopt new solutions certified to the relevant standards. Pursuant to the eIDAS Regulation, electronic signature and seal creation devices must meet certain security requirements and be certified under the common criteria protection profiles for secure signature common devices.

(61) The Notifying Party acknowledges that the eIDAS Regulation has created some demand for GP HSMs certified to the relevant Common Criteria's protection profiles. However, the Notifying Party argues that the eIDAS Regulation applies to a limited number of use cases (i.e. citizen-to-government interactions or business-to-government interactions) and it therefore affects less than [10-20]% of GP HSMs sales in the EEA.

(62) By contrast, according to a report available on Thales' website,[39] HSMs (such as Thales' nshield HSM) play an important role in securing services that come under the eIDAS Regulation. In addition for the traditional use of HSMs for public key certification services, they can be used for the electronic seals and remote signing services introduced by the eIDAS Regulation.

---

37 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, OJ L 119, 4.5.2016, p. 1–88.

38 The eIDAS Regulation replaced the previous eSignature Directive, adopted in 1999, which was intended to encourage the use of electronic signatures across the EU, but did not require each EU Member State to follow common standards. See Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC, OJ L 257, 28.8.2014, p. 73–114.

39 https://www.thalesesecurity.com/solutions/compliance/emea/eidas.

7. RELEVANT MARKETS

7.1. Introduction

(63) Market definition is a tool to identify and define the boundaries of competition between firms.[40] It has both a product and a geographic dimension.

(64) A relevant product market comprises all those products and/or services which are regarded as interchangeable or substitutable, by reason of the products' characteristics, their prices and their intended use. In defining the relevant product market, the Commission assesses demand substitution by determining the range of products which are viewed as substitutes by the consumers. Demand-side substitutability is the focus of the Commission's assessment when defining the relevant markets.[41]

(65) The Commission may also take into account supply-side substitutability, namely when its effects are equivalent to those of demand substitution in terms of effectiveness and immediacy. This is the case when suppliers are able to switch production to the relevant products and market them in the short term without incurring significant additional costs or risks in response to small and permanent changes in relative prices.[42]

(66) The relevant geographic market comprises the area in which the undertakings concerned are involved in the supply and demand of products or services, in which the conditions of competition are sufficiently homogeneous and which can be distinguished from neighbouring areas because the conditions of competition are appreciably different in those areas.[43]

(67) It is within the analytical framework that the Commission has assessed the relevant market definitions.

7.2. Hardware Security Modules

7.2.1. Product market definition

7.2.1.1. Commission precedents

(68) There are no Commission decisions addressing the HSM market.

(69) In 2006, the UK Office of Fair Trading (the "OFT") reviewed the proposed acquisition of nCipher by SafeNet. The deal was ultimately abandoned. In 2008 the OFT reviewed the proposed acquisition of nCipher by Thales. In both cases the OFT considered a separate market for HSMs and a possible sub-segmentation between GP and Payment HSMs but ultimately left the market definition open.

7.2.1.2. Notifying Party's views

A. Overall market for KMS

(70) The Notifying Party considers that there is an overall market for KMS, which includes traditional Payment HSMs, traditional GP HSMs, HSM aaS, encryption software or hardware with key management capabilities, dedicated key management

---

40 Commission Notice on the definition of relevant market for the purposes of Community competition law ("Market Definition Notice"), OJ C 372, 09.12.1997, para 2.

41 Market Definition Notice, points 7 and 15.

42 Market Definition Notice, point 20.

43 Market Definition Notice, point 8.

software, cloud-based KMS, and TPMs and microprocessors with built-in key management capabilities.[44]

(71) In the Form CO, the Notifying Party indicates that a number of substitutes to HSMs have been developed and brought to the market over the last decade. The Notifying Party considers that customers can choose from a wider panel of options, including HSMs aaS and other cloud-based KMS offered by CSPs, as well as integrated solutions, TPMs embedding microprocessors with built-in key management capabilities and multi-party computational software. According to the Notifying Party, these pure software and combined hardware and software solutions offer security levels equal to those of traditional GP and Payment HSMs.

(72) According to the Notifying Party, the majority of HSM customers are not required to install on-premise HSMs and can switch to alternative solutions for new applications. The Notifying Party considers that as customers move data and applications to the cloud, they are progressively replacing their on-premise HSMs with cloud-based key management solutions provided by CSPs.

(73) The Notifying Party argues that a number of new KMS provide the same level of security, functionality, and certification as on-premise HSMs, in particular HSMs aaS, dedicated key management software solutions, or integrated solutions.

(74) Regarding HSM aaS, the Notifying Party argues that they offer the same level of security as traditional, on-premise HSMs as they are based on physical GP or Payment HSMs installed on the premises of vendors. In addition, HSMs aaS offer enhanced support provided by the vendor, in particular CSPs, compared to physical HSMs managed by the end-customer on its own premises. CSPs also offer high availability, backup and disaster recovery services which limit the need for additional on-premise HSMs.

(75) In the Form CO, the Notifying Party submits that further segmentation according to the FIPS levels of security and CC standards (EALs) is not meaningful. According to the Notifying Party, certification is not a key purchasing criterion for customers and certification of particular KMS varies from vendor to vendor.

(76) In the Notifying Party's view, customers are not required by regulation to purchase any specific KMS certified to a given standard, with few exceptions.[45] Enterprises can choose a solution depending on a number of factors, for instance 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.

(77) In the Notifying Party's view, from the supply side, vendors (and their sales and marketing teams) as well as resellers offer various options within the enterprise key management market, notably because similar software is used in a range of KMS.

---

44 Form CO, Sections 6-7, Chapter II, paras 109-113; Article 6(1)(c) Response, para 6.

45 Pursuant to the eIDAS Regulation (Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC), electronic signature and seal creation devices must meet certain security requirements and be certified under the Common Criteria protection profiles for secure signature creation devices. The eIDAS Regulation applies to a limited number of use cases (i.e. citizen-to-government interactions or business-to-government interactions).

(78) The Notifying Party seeks to rely on third-party market studies, notably IDC[46] and Market and Market[47], which in the Notifying Party's view support the conclusion that there is an overall KMS market.

B. GP and Payment HSMs

(79) While the Notifying Party disagrees with the Commission's preliminary conclusions expressed in the Article 6(1)(c) Decision that there is a separate market for HSMs, it argues that, to the extent the Commission rejects an overall enterprise key management market on demand- and supply-side substitutability grounds, it must consistently treat GP and Payment HSMs as making up separate markets. In the Article 6(1)(c) Response, the Notifying Party argues that there is no (or only limited) demand- and supply- side substitutability between Payment and GP HSMs.

(80) As regards demand side substitutability, the Notifying Party argues that there is no demand side substitutability since (i) GP and Payment HSMs are designed and certified for different use cases, (ii) payment of GP HSMs are technically very different, (iii) Payment and GP HSMs have different commercial propositions, (iv) differentiated pricing between GP and Payment HSMs reflect their different functionalities/propositions, (v) customers of GP and Payment HSMs have different purchasing patterns.

(81) As regards supply side substitutability, the Parties argue that there is no supply-side substitutability since (i) GP and Payment HSM designs involve different technologies, (ii) suppliers of GP and payment HSMs undergo different certification process, (iii) GP and Payment HSM competitors are different, (iv) competitors active in GP or Payment HSMs could not easily or quickly switch to supplying the other HSM type in response to a price increase.

(82) In the Notifying Party's view, other KMS (such as HSM aaS, even if in their early stages of growth), already exert a significant competitive constraint, including in particular on vendors of on-premise GP HSMs. According to the Notifying Party, both CSPs and resellers/distributors purchase HSMs from vendors like the Parties and compete with such vendors for the business of end-user customers.

7.2.1.3. Commission's assessment

(83) The Commission has assessed whether other solutions (HSM aaS, other cloud-based KMS, TPM and microprocessors) can be considered to be a substitute to HSMs.

A. HSMs and other cloud-based KMS

(84) With respect to the question whether other cloud-based KMS should be considered from the demand side as an alternative to HSMs, the majority of the respondents to the market investigation do not consider this to be an alternative solution and express a reluctance to move to the cloud. The vast majority of customers replied in the negative to a question whether they were planning to move their entire IT system, including KMS to cloud-based solutions in the next two to five years.[48] Customers considered to have more control with a physical, on-premise HSM and were unsure about the reliability of cloud services.[49] A clear majority of the respondents

---

46 IDC, *Worldwide Data Security Taxotomy*, 2016 and IDC, *Worldwide Hardware Security Modules Revenue Forecast*, 2017-2021.

47 Markets and Markets, *Enterprise Key Management Market, Global Forecast to 2022*, 2017.

48 Replies to Questionnaire Q5 – customers of 7 September 2018, section B.

49 Replies to Questionnaire Q2 – customers of 19 June 2018, question 10; replies to Questionnaire Q2 – customers of 19 June 2018, question 18.

considered that certain levels of security can be achieved only by relying on an HSM.[50]

(85) As regards supply side substitutability, respondents confirmed that this is a high complexity market and a company offering cloud-based KMS would not be able to develop and start supplying HSMs without significant investment and within a limited timeframe. The results of the market investigation confirmed that HSM and cloud-based KMS products require development of different interfaces and technologies.[51]

B. HSMs and other KMS (TPM or microprocessors)

(86) With respect to the question whether other KMS should be considered from the demand side as an alternative to HSMs, the results of the market investigation indicate that they are not. Market participants explained that in general, TPMs or microprocessors do not reach the level of HSMs in terms of security, functionalities and performances. Customers consider them in terms of parallel use, rather than as alternatives.[52]

(87) As regards supply side substitutability, the respondents provided the same indications as for cloud-based KMS and generally confirmed that separate, complex technologies are required for HSMs and that starting to offer HSMs in addition to TPMs or microprocessors would require significant investment and time.[53]

C. HSMs and HSM aaS

(88) With respect to the question whether HSM aaS should be considered from the demand side as an alternative to on-premise HSMs, the results of the market investigation indicate that the substitution between the two is limited, especially if a minimum level of security needs to be achieved. The majority of the customers and competitors do not consider that HSMs can be substituted with HSM aaS or consider that it would depend on the customer requirements and their particular situation. The competitors explained that when using an HSM aaS, the client does not own the "keys" of the system (which are with the HSM aaS provider), which adds to the risk of a security leakage.[54] Moreover, they considered that many customers may not be willing to share such a critical infrastructure with other customers,[55] given that the HSM aaS provider may use the same HSM for multiple customers. Similarly, customers indicated that for high security applications it is not an option to use HSMs deported in the cloud, or to delegate the hosting of HSMs in any other way and that HSMs could not be substituted by HSM aaS.[56] Resellers provided the same explanation as to why they do not consider HSM and HSM aaS to be alternatives, pointing to lack of trust on the part of the customers.[57]

(89) As regards supply side substitutability, respondents generally confirmed that HSM aaS providers do not manufacture HSMs themselves, but purchase them from the

---

50 Replies to Questionnaire Q1 – competitors of 19 June 2018, question B.A.14; replies to Questionnaire Q2 – customers of 19 June 2018, question 18; replies to Questionnaire Q3 – resellers of 21 June 2018, question 19.

51 Replies to Questionnaire Q1 – competitors of 19 June 2018, question B.A.17.

52 Replies to Questionnaire Q2 – customers of 19 June 2018, question 17.

53 Replies to Questionnaire Q1 – competitors of 19 June 2018, question B.A.17.

54 Replies to Questionnaire Q1 – competitors of 19 June 2018, question B.A.1.

55 Replies to Questionnaire Q1 – competitors of 19 June 2018, question B.A.1.

56 Replies to Questionnaire Q2 – customers of 19 June 2018, question 9.1.

57 Replies to Questionnaire Q3 – resellers of 21 June 2018, questions 6.1 and 6.2.

HSM manufacturers.[58] As explained by one of the competitors, designing and building HSM is an entirely different process compared to connecting to a hardware device.[59] In the opinion of competitors, in-house digital security products involve very sophisticated technology requiring specialised skills and certifications, so it would be difficult to develop and take these products to market without significant investment and within a limited timeframe, even by a service provider.[60]

D. GP HSMs and Payment HSMs

(90) The Commission also assessed whether, within HSMs, a distinction should be made between GP HSMs and Payment HSMs.

(91) As regards the question whether GP HSMs and Payment HSMs should be considered from the demand side as substitutes, the results of the market investigation generally indicate that they are not.[61] The majority of the respondents considered that there is a difference in functionality between Payment and GP HSMs and that they are intended for different use cases. Respondents pointed to the fact that GP HSMs are more expensive and more flexible, while Payment HSMs are more case-oriented. It was also explained that GP HSMs must support standardised programmatic application program interfaces ("APIs") whereas Payment HSMs present proprietary APIs that do not allow any interoperability.[62] In addition, customers of Payment HSMs require additional PCI-HSM certifications for the HSMs they purchase. Consequently, the offerings of the Parties and their competitors are divided between Payment and GP HSM products.

(92) However, it appears that in some limited cases a GP HSM could be used instead of a Payment HSM.[63] Card issuance is a particular use case for which both a Payment and a GP HSM could be used.[64]

(93) As regards supply side substitutability, the market investigation generally confirmed that GP and Payment HSMs are designed differently, both when it comes to hardware and software. As explained by one of the respondents to the market investigation "*[i]ndustry standards require that hardware in Payment HSMs provide specific functionalities and meet specific requirements, in order to provide the level of security needed in the payment industry. Hardware in GP HSMs is not manufactured or designed to meet these payment industry requirements*".[65] However, some competitors suggest that the differences in hardware might not be as clear-cut, with Securosys claiming that it could start building a Payment HSM based on its GP HSM platform.[66] Similarly, Futurex considers that the differences are rather with the software and firmware than hardware.[67] While the differences in hardware might not be as pronounced, it is the software which constitutes the significantly bigger part of

---

58 Replies to Questionnaire Q1 – competitors of 19 June 2018, question B.A.12; replies to Questionnaire Q2 – customers of 19 June 2018, question 20; non-confidential minutes of telephone conference with Barclays of 19 June 2018.

59 Replies to Questionnaire Q1 – competitors of 19 June 2018, question B.A.17.

60 Replies to Questionnaire Q1 – competitors of 19 June 2018, question B.A.17.

61 Replies to Questionnaire Q5 – customers of 7 September 2018, questions 37 and 38; replies to questionnaire Q2 – customers of 19 June 2018, question 20.

62 Replies to Questionnaire Q1 – competitors of 19 June 2018.

63 Replies to Questionnaire Q1 – competitors of 19 June 2018, question B.A.15; Replies to Questionnaire Q2 – customers of 19 June 2018, question 23.

64 Reply to RFI 17, question 9, reply to RFI 18, question 8.

65 Replies to Questionnaire Q5 – customers of 7 September 2018, question 39.1.

66 Non-confidential minutes of conference calls with Securosys of 6 September 2018.

67 Replies to Questionnaire Q1 – competitors of 19 June 2018, question B.A.18.1.

the investment effort and which appears to be clearly different to serve distinct use cases.

(94) To obtain PCI-HSM certification, Payment HSMs must meet strict physical and logical security requirements. Obtaining a PCI-HSM certification requires about […] on average and costs around USD […].[68] Market investigation generally confirms that competitors active in GP or Payment HSMs could not easily or quickly switch to supplying the other HSM. [69] The fact that most cases of expansion from one HSM market to another in recent years took place through acquisitions further supports the argument that developing the other type of HSMs when already manufacturing one of them is not easy.

(95) In the course of the market investigation, however, it was indicated to the Commission that the boundaries between the two types of HSM may become increasingly blurred with time.[70] Some attempts have been made at developing HSMs that can serve both Payment and other general purposes, with Futurex already offering such solution on the market.

7.2.1.4. Conclusion on the product market definition

(96) In light of the above, for the purposes of the present Decision, the Commission concludes that the relevant product markets for the assessment of the Transaction are:

(a) GP HSMs

(b) Payment HSMs

(97) To the extent that other products (such as HSM aaS and software with key management capabilities) would be likely to constrain the merged entity from exercising market power in relation to the supply of HSMs this is considered in the competitive assessment in Section 8.2.4.

7.2.2. Geographic market definition

7.2.2.1. Commission precedents

(98) There are no Commission decisions addressing the HSM market. In previous decisions, the Commission has generally concluded that the geographic market in cases concerning the IT sector is at least EEA-wide, if not global.[71]

(99) In Safenet/nCipher (2006) the OFT considered that the geographic market for HSMs was "wider than national, if not global". The OFT noted that no regulatory barriers affected trade of commercial HSMs and 80% of nCipher's sales were made outside the UK. In that case, the Parties submitted that it was not necessary to have a physical presence in a country to be able to win contracts for supplies of HSMs. However, the OFT noted certain customers appeared to hold some preferences for

68 RFI 18, reply to question 7.

69 Replies to questionnaire Q1 – competitors of 19 June 2018, question B.A.18; replies to questionnaire Q4 of 10 September 2018, questions 82-84.

70 Non-confidential minutes of telephone conference with Utimaco of 22 May 2018.

71 See Case M.5984, Commission decision of 26 January 2011, Intel/McAfee, Case M.5529, Commission decision of 21 January 2010, Oracle/Sun Microsystems; see also Case M.4942, Commission decision of 2 July 2008, Nokia/Navteq; Case COMP/C-3/37.792, Commission decision of 24 March 2004, Microsoft.

national HSM suppliers. Similarly, in Thales/nCipher (2008), the OFT left the geographic market definition open after pointing to substantially the same factors.[72]

7.2.2.2. Notifying Party's views

(100) In the Form CO,[73] the Notifying Party submits that, in line with the approach taken by the Commission in other cases concerning the IT software and related markets, the Transaction should be assessed on the basis that the enterprise key management market (and any plausible sub-segment thereof) is worldwide, or at least EEA-wide.

(101) The Notifying Party indicates that customers purchase products from suppliers active globally and KMS are homogenous across regions.

(102) Regarding the importance of local presence of a supplier, the Notifying Party considers that it may be beneficial, even if it is not essential. Vendors, including the Parties, typically have a global centralised sales structure and rely on local resellers and distributors in case they do not have local presence in a given country.

(103) The Notifying Party submits that certification requirements are similar internationally. In the Notifying Party's view, FIPS are recognised globally, while the CC provide framework under which national bodies publish security profiles describing how they will assess EAL requirements – such that national certifications are generally aligned. Based on the system of equivalencies in Europe (the SOGIS), a certification delivered in one country is recognised in other countries.

(104) Transportation costs are negligible and there are no relevant trade or regulatory barriers limiting foreign companies' ability to supply KMS, with the exception of China and Russia.[74]

(105) In the Article 6(1)(c) Response, the Parties do not provide further arguments concerning the geographic scope of the market.

7.2.2.3. Commission's assessment

(106) The results of the market investigation have generally indicated that the geographic scope of the market for HSMs is at least EEA-wide. The majority of the customers responding to the market investigation consider that non-EEA players could compete on an equal footing with established EEA players. While some respondents value having support based locally, many rely on global solutions and on-call support. Competitors, in turn, provided mixed views on the need for local support. Some of the respondents pointed out that the importance of providing local support hinges upon customers' preferences, while others consider that being able to provide local maintenance and support is crucial for customers.

(107) Review of the internal documents of the Parties further confirms that the market is at least EEA-wide. Both Thales and Gemalto make their strategic discussions regarding both Payment and GP HSM products lines on […].

7.2.2.4. Conclusion on the geographic market definition

(108) In light of the above, the Commission concludes, for the purposes of the present Decision, that the geographic market for GP HSMs and Payment HSMs could be at least EEA-wide or worldwide in scope. However, the exact geographic market

---

72 https://assets.publishing.service.gov.uk/media/555de37c40f0b666a200008e/Thales.pdf.

73 Form CO, Sections 6-7, Chapter II, paras 145-147.

74 China has erected regulatory barriers and Russia imposes a licensing regime on imports of key management solutions.

definition can be left open as the competitive assessment remains the same for both an EEA-wide and a worldwide geographic market.

7.2.3. Overall conclusion on market definition

(109) In light of the above, in this Decision the Commission assesses the effects of the Transaction with respect to the market for GP HSMs and Payment HSMs. The geographic scope of these product markets is at least EEA-wide or worldwide but can be left open for the purposes of this case as the competitive assessment does not change for the different geographic levels.

7.3. Enterprise Encryption Software

(110) The process of encrypting data by converting plain text to cipher text using an encryption algorithm and encryption keys is performed by encryption software. Data generally exists in one of three different forms: at rest, in use, or in motion. Enterprises can decide to encrypt their data in any of these three forms. While enterprise encryption software ("ES") generally relates to data at rest and data in use, enterprises may separately also choose to encrypt data while it is in motion.

(111) Data at rest are data not actively moving from device to device or network to network – but rather stored in one place (i.e. in a user's database, file systems, storage infrastructure, or cloud).

(112) Data in use are data stored in a non-persistent digital state in the computer memory or processed applications, and are generally accessible to several persons and devices. Data in use can be in the process of being generated, amended or updated, erased or viewed through various interface endpoints.

(113) ES encrypts data at rest or in use at various levels– including, in particular, at the storage/disk, file/folder, database, or application level. Tokenization, format preserving and data masking are further variants of ES, which take place at the application level of the data stack.[75]

(114) Data in motion, also called "data in transit", are data actively moving from one location to another over the network (such as via the internet, private network, or cloud).[76] To protect such communication, data in motion is encrypted before transit between the originating and receiving location to avoid data loss from attacks during transit. ES designed to protect data in motion is also called communication encryption software.

(115) The type of communication network technology that is supported by network encryption product generally depends on the layer at which encryption takes place. Networks are commonly divided into seven layers[77]: (i) physical[78], (ii) data link[79],

---

[75] File/folder encryption software secures sensitive files or folders stored, for example, in local PCs, servers, or on business networks. Database encryption solutions encrypt data stored in databases. 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. This is different from disk encryption, where the data are only encrypted when they are saved to the disk, but can be seen as they move around. Tokenization 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 transaction. Both Thales and Gemalto have tokenization solutions.

[76] Examples include data as it moves across the internet to a cloud service provider or files transferred over File Transfer Protocol, and might include calls, emails, or instant messaging.

[77] Based on a model developed by the International Standards Organisation in the framework of the Open Systems Interconnection project.

(iii) network[80], (iv) transport[81], (v) session and (vi) presentation[82], and (vii) application[83]. A network encryptor is a hardware appliance that runs encryption software to encrypt the data stream going on to, or coming off of, the network. Data in motion are typically encrypted in Layers 1-3 of enterprise networks.[84]

(116) ES solutions may be sold as (i) stand-alone products, (ii) native parts of underlying IT products (such as databases, data storage solutions, or operating systems and applications), or (iii) as a combination of different types of encryption software (or hardware), potentially combined with other capabilities such as centralised key and policy management. According to the Notifying Party, competitors who offer solutions across various (typically more than one) levels/layers of encryption, in some cases with a single product offering, are referred to as "generalists". Other vendors – "non-generalists" or "specialists" – focus on a specific sub-segment of the ES market and develop products for encrypting data at just one (or two) levels of the data stack.

(117) Thales is active in ES for data at rest/in use with its Vormetric product line.[85] Gemalto is active in ES for data at rest/in use with SafeNet Protect File, SafeNet ProtectV, SafeNet StorageSecure, SafeNet ProtectDB product, SafeNet ProtectApp, and SafeNet Tokenization.

(118) Thales and Gemalto are not active in offering ES for data in motion/communication ES. Thales and Gemalto derive limited revenues from the resale of products designed and manufactured by other players for the protection of data in motion in enterprise networks at Layer 2.[86]

7.3.1. Product market definition

7.3.1.1. Commission precedents

(119) There are no Commission decisions addressing the ES market.

---

78 Layer 1, the physical layer, conveys a stream of bits though the network and includes network adapters, repeaters, network hubs, modems, and fibre media converters. Layer 1 encryption can be integrated into optical switches and offers low-cost data security capable of handling multiple protocols.

79 Layer 2, the data link layer, transfers data from one node to another over the physical layer. Layer 2 encryption can be integrated into routers and switches and offers low cost, efficient and certified data security.

80 Layer 3, the network layer, decides which physical path the data should take based on network conditions, priority of service, and other factors. Layer 3 encryption is integrated into routers and offers a widely understood and accepted technology, especially at low speeds (typically 1 Gb/s or less).

81 Gateways and firewalls operating at Layer 4 provide encryption functionality, so there has not traditionally been demand for stand-alone network encryption devices operating at Layer 4.

82 The "presentation layer" responds to service requests and interacts with the session layer. Although encryption can be done at Layer 5 and 6, it is at the file level (e.g., GIF, JPEG, etc.), rather than for bulk transfers.

83 Encryption at Layer 7 is normally used in the public Internet domain (e.g. user information).

84 Customers do not commonly use Layer 4 to 7 network encryptors to encrypt data in motion as at these layers encryption tends to use TLS/SSL protocols more suited to the public Internet, gateways, and firewalls, than to large bulk data transfers that need to be encrypted over a private link.

85 Thales' Vormetric ES for data at rest and data in use include Vormetric Transparent Encryption, Vormetric Application Encryption, Vormetric Cloud Encryption Gateway, Vormetric Protection for Teradata Database, Vormetric Tokenization and Data Masking, and Vormetric Batch Data Transformation.

86 The network encryption product sold by Thales is known as Datacryptor. Datacryptor products […]. Gemalto's network encryption family of products is known as SafeNet High Speed Encryptors and includes the SafeNet CN4000, CN6000, CN8000, and CN9000 Series. Gemalto's network encryption products […].

7.3.1.2. Notifying Party's views

(120) In the Form CO,[87] the Notifying Party argues that the various ES protecting data at rest or data in use make up a single market for ES. The Notifying Party considers that ES designed to protect data in motion should not be treated as part of this same market for the following reasons: (i) ES protecting data in motion operates and functions very differently (ii) it is mostly used to complement ES protecting data at rest/in use and (iii) the market players active in data in motion encryption products tend to be very different from the companies active in offering ES for data in use/at rest.

(121) In the Notifying Party's view, further segmentation of ES products for data at rest or data in use by level of encryption (e.g. for storage/disk encryption, file/folder encryption, database encryption, application encryption and tokenization & data masking segments) is not justified. The Notifying Party considers that from the demand side, customers may choose to encrypt data at the storage/disk level only, instead decide to encrypt at the file/folder or database level, go a level higher and encrypt at the application level or apply specific masking tools such as tokenization, format-preserving encryption, and data masking to protect any given set of data. The Notifying Party considers that customers can and do switch to ES solutions working at different levels to meet their encryption needs.

(122) From the supply side, the Notifying Party considers that vendors typically provide a wide range of ES solutions for data at rest/in use. Several vendors offer a single product capable of encrypting data at various levels.[88] The Notifying Party considers that ES suppliers typically offer a range of ES products and can easily expand from supplying one specific type of ES (e.g. file/folder) to another (e.g. storage/disk encryption) in view of the low costs involved and based on API development and open source encryption. In the Notifying Party's view, the different types of ES are generally part of the same business unit (regarding e.g. sales, support and R&D activities).

(123) The Notifying Party considers that its arguments regarding the relevant product market definition are supported by third party reports, according to which the various levels of encryption form part of a single ES market.[89]

(124) Regarding data in motion, the Notifying Party argues that the relevant market for the assessment is the market for network encryption products. In the Notifying Party's view, any further segmentation based on network design or the network layer at which encryption takes place would not be appropriate.

(125) First, according to the Notifying Party, from the demand side, enterprises use a number of different technologies in building their networks and they have multiple options to encrypt data in motion.

(126) Second, from the supply side, the Notifying Party considers that there are many companies offering data-in-motion encryption solutions which may target individual

---

87 Form CO, Sections 6-7, Chapters III-IV.

88 Examples are IBM with its product Guardium which performs database, application and file encryption or Oracle with its products Oracle TDE and My SQL Enterprise Encryption which perform database and application encryption). Furthermore, according to the Notifying Party, Thales' products Vormetric Transparent Encryption and Vormetric Cloud Encryption Gateway are used for both file/folder and database encryption.

89 Markets and Markets (Encryption Software Report – Global Forecast to 2022 and Cloud Encryption Market – Global Forecast to 2022) and IDC (Worldwide Security Products Taxonomy).

network layers or provide integrated solutions across two or more layers (e.g. Ciena, Cisco, Nokia, Certes' Zero Trust).[90] Furthermore, the Notifying Party considers that the same players are active in the supply of network encryptors for local-area networks ("LAN"), wide-area networks ("WAN"), and and metropolitan-area networks ("MAN") (at Layer 2 or any other layer).

7.3.1.3. Commission's assessment

(127) The Commission has assessed whether ES solutions for data at rest, data in use and data in motion form part of the same product market and whether further segmentation based on the level and layers of encryption would be appropriate.

(128) The market investigation provided mixed results regarding the question whether there is a single ES market comprising all solutions encrypting data at rest, data in use and data in motion.

(129) As regards demand-side substitutability, a majority of customers responding to the market investigation indicated that they would purchase one single solution to encrypt different stacks of data.[91] This is also confirmed by competitors and resellers which indicated that customers increasingly seek end-to-end encryption and a holistic approach to protect data as it moves between the three areas (at rest, in use and in motion).[92] According to one reseller, "*format-preserving encryption and tokenization are examples of an approach to protect data either at rest or in motion*".[93] Some respondents consider that from the supply side, ES vendor could and do develop products containing all necessary tools and protocols for the three data states.[94]

(130) According to some respondents, a possible further segmentation of the market would include a separate market for data at rest and data in use and a separate market for data in motion due to the different protocols, tools and trust models required for the encryption of data in motion.[95] Some respondents indicate that different players provide ES solutions for data in motion (e.g. communication equipment manufacturers).[96]

(131) The market investigation suggests that a further segmentation of ES for data at rest/in use by level of encryption (at the storage/disk, file/folder, database or application level etc.) would not be appropriate.[97] According to some customers who responded to the market investigation, the different levels of encryption do not exist in distinct silos but are often used in parallel and are closely inter-related from a technical point of view.[98] A respondent to the market investigation expressed the view that "*suppliers are expected to present solution-based approach that encrypts data at one*

---

90 Ciena offers network encryption products that operate at Layers 1 and 2, Cisco offers products that operate at Layers 1, 2 and 3. Nokia (former Alcatel/Lucent) offers products that operate at Layer 1 and 3 and Certes' Zero Trust WAN product operates at Layers 2 and 3 (as well as Layer 4).

91 Replies to Questionnaire Q2 – customers of 19 June 2018, question 63.1.

92 Replies to Questionnaire Q1 – competitors of 19 June 2018, question C.A.2.1; replies to Questionnaire Q3 – resellers of 21 June 2018, question 74.1.

93 Replies to Questionnaire Q3 – resellers of 21 June 2018, question 76.1.

94 Replies to Questionnaire Q2 – customers of 19 June 2018, question 63.1.

95 Replies to Questionnaire Q2 – customers of 19 June 2018, question 65.1, replies to Questionnaire Q3 – resellers of 21 June 2018, question 76.1; replies to Questionnaire Q1 – competitors of 19 June 2018, question C.A.4.1.

96 Replies to Questionnaire Q1 – competitors of 19 June 2018, question C.A.2.1.

97 Replies to Questionnaire Q2 – customers of 19 June 2018, question 66.1.

98 Replies to Questionnaire Q2 – customers of 19 June 2018, question 66.1.

or multiple layers".[99] Some respondents however point out that different technologies are needed to encrypt data at each stage or layer.[100]

(132) Regarding the question whether encryption at different layers can be distinguished as separate markets within the market for network encryptors, the Commission has the following observations.

(133) First, the market investigation did not indicate whether ES for data in motion should be further sub-segmented based on layers of encryption.

(134) Second, based on the Notifying's Party submission, the Commission considers that from the demand side customers can and do use network encryptors to encrypt data at Layers 1, 2 and/or 3 of their computer networks alone or in combination. Customers can choose between products focusing on different layers of their network or multiple layers at once, depending on their requirements (i.e. nature of their data, structure of networks, data usage patterns).

(135) From the supply side, based on the Notifying Party's submission, many companies offer data-in-motion encryption solutions, which may target individual network layers or provide integrated solutions across two or more layers.

7.3.1.4. Conclusion on the product market definition

(136) For the purposes of the present Decision, the exact product market definition can be left open as the Transaction would not significantly impede effective competition under any plausible market definition, including the narrowest possible markets for (i) ES for data at rest/in use and possible further sub-segments by level of encryption (at the storage/disk, file/folder, database or application level, tokenization and data masking etc.) and (ii) network encryptors for data in motion and possible sub-segments based on the layer on which the network encryption takes place.

7.3.2. Geographic market definition

(137) There are no Commission decisions addressing the ES market. In previous decisions, the geographic market in cases concerning the IT sector is considered at least EEA-wide, if not global.[101]

7.3.2.1. Notifying Party's views

(138) The Notifying Party submits that, in line with the Commission's decisional practice, the relevant market for the ES market is global, excluding China or at least EEA-wide.

(139) In the Notifying Party's view, customers generally buy globally across regions and ES products are generally homogenous across regions (e.g. all of Thales' and Gemalto's ES solutions are supplied globally). The Notifying Party further considers that there are no material differences in the way in which ES is sold and distributed within the EEA and in other parts of the world. Most suppliers and brands are active globally and serve customers globally from a few facilities and customer support centres.

---

99 Replies to Questionnaire Q3 – resellers of 21 June 2018, question 77.1.

100 Replies to Questionnaire Q3 – resellers of 21 June 2018, question 77.1.

101 See Case M.5984, Commission decision of 26 January 2011, Intel/McAfee; Case M.5529, Commission decision of 21 January 2010, Oracle/Sun Microsystems; see also Case M.4942, Commission decision of 2 July 2008, Nokia/Navteq; Case COMP/C-3/37.792, Commission decision of 24 March 2004, Microsoft.

(140) Regarding the importance of local presence of a supplier, the Notifying Party considers that it is not required (also for maintenance which is provided remotely). According to the Notifying Party, price and costs of use are broadly consistent globally and discount policies generally do not vary from one region to another. Transport costs are negligible and there are no quotas, tariffs or other trade barriers which affect the import into the EEA or export from the EEA of encryption software.

(141) Regarding the possible market for network encryptors for data in motion, the Notifying Party submits that in line with Commission's decisional practice[102], which concerned various markets in broadband communication equipment and the communications network industry, the relevant market is at least EEA-wide if not global due to the existence of international standards, lack of significant transport costs, and the presence of large equipment manufacturers that are active on a pan-European (and often broader) basis. The Notifying Party considers that the market for network encryptors is dominated by large market equipment manufacturers, such as Ciena, Cisco, Juniper, and Nokia (formerly Alcatel/Lucent), which provide network encryptors as part of their networking devices, and vendors such as AT Media, Rhode & Schwarz, Secunet, Securosys, and Viasat which are active on an EEA-wide or even worldwide basis. Furthermore, end-user customers of network encryptors are often large companies active at an EEA-wide and often worldwide level.

7.3.2.2. Commission's assessment

(142) The Commission considers that the relevant geographic market for ES and network encryptors is global or at least EEA-wide for the reasons set out in recitals (143)-(144).

(143) First, with regard to the geographic scope of the market for ES, the majority of the respondents to the market investigation considers that customers procure ES products based on their characteristics and price, irrespective of the location of the vendor (e.g. in the EEA or outside the EEA).[103] Some respondents point out that maintenance and support provided by local partners can be taken into account, depending on customers' preferences.[104]

(144) Second, the market investigation indicated that the geographic scope of the market may be wider than EEA, as a majority of ES suppliers can supply customers located both in the EEA and outside the EEA.[105]

7.3.2.3. Conclusion on the geographic market definition

(145) For the purposes of the present Decision, the question whether the relevant geographic market definition is EEA-wide or global can be left open as the Transaction would not significantly impede effective competition under any plausible geographic market definition, including the narrowest possible market at the EEA level.

---

102 See Case M.5669, Commission decision of 29 March 2010, Cisco/Tandberg; Case M.4214, Commission decision of 24 July 2006, Alcatel/Lucent Technologies; see also Case M.4063, Commission decision of 22 February 2006, Cisco/Scientific Atlanta.

103 Replies to Questionnaire Q2 – customers of 19 June 2018, questions 67-70.

104 Replies to Questionnaire Q1 – competitors of 19 June 2018, question C.B.5.

105 Replies to Questionnaire Q1 – competitors of 19 June 2018, questions C.B.2 and C.B.3.

7.3.3. Overall conclusion on market definition

(146) In light of the above, for the purpose of this Decision, the exact product and geographic market definition can be left open, since the Transaction would not significantly impede effective competition under any plausible market definition, including the narrowest possible market at the EEA level for (i) ES for data at rest/in use and possible further sub-segments by level of encryption (at the storage/disk, file/folder, database or application level, tokenization and data masking etc.) and (ii) network encryptors for data in motion and possible sub-segments based on the layer on which the network encryption takes place.

7.4. Security evaluation services

7.4.1. Product market definition

7.4.1.1. Notifying Party's views

(147) Security evaluation refers to the examination of a system to determine its degree of compliance with a stated security model, security standard or specification. The evaluation may be conducted by (i) analysing the detailed design, especially of the software, often using verification and validation; (ii) observing the functional behaviour of the system; or (iii) attempting to penetrate the system using techniques available to attack the system. Vendors wishing to certify their products to a particular standard need to have these products tested at independent evaluation centres (labs) which must be accredited by the relevant accreditation bodies. To be accredited, a lab must undergo specific audits on its evaluation methodologies and the security of its sites.

(148) In the Form CO,[106] the Notifying Party submits that Thales and Gemalto have evaluation labs accredited to perform security evaluations under certain standards. According to the Notifying Party, there are over 65 Common Criteria accredited labs around the world, half of which are in the EEA. Evaluation labs are accredited by national IT security agencies (such as the Agence Nationale de la Sécurité des Systèmes d'Information ("ANSSI") in France; or the Bundesamt für Sicherheit in der Informationstechnik ("BSI") in Germany).

(149) Thales' lab – TCS – is accredited by ANSSI to perform security evaluations of electronic and microelectronic components, as well as of embedded software under the Common Criteria and Information Technology Security Evaluation Criteria ("ITSEC"). TCS also holds ANSSI accreditation for First Level Security Certification ("CSPN" – Certification de Sécurité de Premier Niveau)[107] and focuses on testing hardware and associated embedded software.[108]

(150) Gemalto's lab – Trusted Labs – is also accredited by ANSSI, but focuses on testing of software. In addition, Trusted Labs is certified to conduct security evaluations of

---

106 Form CO, Section 6, Chapter IV.

107 CSPN is a French scheme that was introduced by ANSSI to provide an alternative to the Common Criteria evaluations to assess the security resistance of a product to a moderate level of attack. The scope of CSPN is similar to the vulnerability analysis performed within Common Criteria, but with faster testing timelines. The range of products that can receive CSPN certificates is very wide, including embedded hardware and software, mobile applications, connected devices, and open-source software and libraries. CSPN currently applies only in France.

108 TCS is also certified by Mastercard, Visa, EMVCo, American Express, Discover and JCB for security evaluation of banking cards.

mobile payment applications under the Bancontact/Mister Cash security certification scheme.

(151) The Notifying Party submits that the Parties' activities should be considered as part of a market for (cyber) security evaluation services and should not be further divided by certification or security standards. From the demand side, companies are generally not required to certify their products to a particular standard and can choose between a number of different certification options depending on the product application, the desired level of security assurance, time constraints and costs. The Notifying Party considers that from the supply side, most large evaluation labs are typically accredited to perform evaluation services under several security standards.

(152) The Notifying Party argues that Thales and Gemalto compete with regard to CSPN security evaluations (for connected devices) for which both Parties are accredited by ANSSI.

(153) The Notifying Party submits that there is no need to reach a conclusion as to whether there is an overall (cyber) security evaluation market or a separate market for CSPN security evaluation services as the Transaction would not significantly impede effective competition under any plausible market definition.

7.4.1.2. Commission's assessment

(154) There are no Commission precedents addressing the market for security evaluation services.

(155) In 2013, *SDNV/Germanisher Lloyd*[109], the Commission considered an acquisition concerning two companies which were both active in testing, inspection, certification/verification/classification ("TIC") services in the maritime and oil & gas sectors. The Commission noted that testing, inspection, and certification services are highly interrelated and to be distinguished from consultancy services.

(156) Based on the Notifying Party's submission, the Commission considers that the companies typically have a choice between several certification standards against which to certify their products. From the supply side, labs need to be accredited in order to carry out security evaluations.

7.4.1.3. Conclusion on the product market definition

(157) For the purpose of the present Decision, the question whether the product market consists of all (cyber) security evaluation services or whether separate markets exist for any segmentation of these services based on the certification for which the lab was accredited can be left open as the Transaction would not significantly impede effective competition under any plausible market definition, including the narrowest possible market for CSPN security evaluation services.

7.4.2. Geographic market definition

7.4.2.1. Notifying Party's views

(158) The Notifying Party submits that the geographic market for security evaluation services is worldwide or at least EEA-wide.

7.4.2.2. Commission's assessment

(159) The Commission considers, based on the Notifying Party's submission, that most evaluation labs, including the Parties' (located in France) service customers from

[109] See Case M.6885, Commission decision of 15 July 2013, SDNV/Germanischer Lloyd.

around the world and not only those located in France. Most standards are international or at least widely recognised due to mutual recognition agreements such as CCRA.

7.4.2.3. Conclusion on the geographic market definition

(160) For the purpose of the present Decision, the question whether the geographic market for (cyber) security evaluation services is global or EEA-wide can be left open as the Transaction would not significantly impede effective competition under any plausible geographic market definition, including the narrowest possible EEA-wide market.

7.4.3. Overall conclusion on market definition

(161) In light of the above, for the purpose of this Decision, the exact product and geographic market definition can be left open, since the Transaction would not significantly impede effective competition under any plausible market definition, including the narrowest possible market for CSPN security evaluation services at the EEA-wide market.

7.5. SIM Cards, OTA SIM Card Administration and GSM-R integration

7.5.1. Product market definition

7.5.1.1. Notifying Party's views

(162) Gemalto provides SIM cards and Over-the-air ("OTA") SIM administration platforms, which are vertically related to Thales' activities in GSM-R integration.

(163) GSM-R, also referred to as GSM-Railway, is an international wireless communications standard for railway communication and applications. A subsystem of the European Rail Traffic Management System ("ERTMS"), it is used for communication between staff, trains and control centres. It is based on GSM and EIRENE – MORANE specifications that guarantee performance at speeds up to 500 km/h (310 mph) without any communication loss.

(164) SIM cards are used in GSM-R handsets and GSM-R cab radio modules, which are installed inside the cab control unit of a driving cab. OTA SIM card administration platforms are used to allow mobile device operators to communicate with, download applications to, and manage SIM cards without being connected physically to the card (i.e. the OTA platform formats the request of the mobile device into a message that can be understood by the recipient SIM card).

(165) As part of its […] business, Thales has a very limited activity globally in the design, integration and installation of GSM-R systems – and no presence at all in the EEA. For some of its GSM-R integration projects outside of the EEA […], Thales has purchased […].

(166) In the Form CO,[110] the Notifying Party submits that in line with the Commission's findings in *Advent International/Morpho*,[111] the relevant product market is the market for the manufacture and supply of SIM cards.

(167) The Notifying Party submits that the relevant product market is the market for the provision of OTA SIM card administration and services platforms in line with the Commission's decision in *Axalto/Gemplus.*[112]

---

110 Form CO, Section 6, Chapter IV.

111 See Case M.8258, Commission decision of 19 April 2017, Advent International/Morpho.

(168) Regarding GSM-R, the Notifying Party submits that in line with the Commission's prior decisional practice[113] on railway signalling projects and the fact that GSM-R systems are usually tendered separately from signalling systems, GSM-R integration projects are likely to belong to a separate product market. According to the Notifying Party, while Thales has participated in […].

7.5.1.2. Commission's assessment

(169) In previous decisions (see recital (166)), the Commission analysed the transaction by distinguishing between the market for the manufacture and supply of SIM cards from the overall market for plastic cards, ultimately leaving the question open.

(170) In line with previous decisional practice (see recital (167)), the Commission considers that the provision of OTA SIM card administration and services platforms constitutes a distinct product market from general operation and support system ("OSS") market in which traditional software vendors provide telecommunication operators with IT-solutions (including call completion, messaging solutions, delivery of data).

(171) With regard to GSM-R, the Commission considers that there are indications that GSM-R integration projects constitute a separate product market from railway signalling systems due to the following factors: (i) the presence of specialised providers of GSM-R solutions, such as Nokia or Kapsch, who are not active in other subsystems for railway signalling, (ii) railway signalling suppliers such as Thales, Siemens and Alstom frequently bid in consortia with these specialised GSM-R providers so that they do not directly supply GSM-R systems, (iii) the specialised nature of the GSM-R standards and the underlying technologies, which are different from other railway signalling technologies (such ETCS, the other component of ERTMS).

7.5.1.3. Conclusion on the product market definition

(172) For the purpose of the present Decision, the Commission in line with its decisional practice confirms that the relevant product market is the market for the provision of OTA SIM card administration and services platforms. The Commission leaves open the question whether the market for the manufacture and supply of SIM cards constitutes a separate market and whether GSM-R integration constitutes a separate market as the Transaction would not significantly impede effective competition under any plausible market definition, including the narrowest possible market for the manufacture and supply of SIM cards and GSM-R integration.

7.5.2. Geographic market definition

7.5.2.1. Notifying Party's views

(173) Regarding the manufacture and supply of SIM cards, the Notifying Party submits that in line with the Commission's previous decisional practice, the relevant geographic market is at least EEA-wide in scope.

(174) Regarding the OTA SIM card administration and services platforms, the Notifying Party submits that that the relevant geographic market is worldwide or at least EEA-

---

112 See Case M.3998, Commission decision of 19 May 19 2006, Axalto/Gemplus.

113 See Case IV/M.685, Commission decision of 8 February 1996, Siemens/Lagardère; Case M.2694, Commission decision of 21 June 2002, Metronet/Infraco; Case M.4337, Commission decision of 7 November 2006, Thales/Alcatel; Case M.6843, Commission decision of 18 May 2013, Siemens/Invensys Rail.

wide in scope. In the Notifying Party's view, there are no barriers to entry, as customers may be supplied from any country regardless of the country where actual manufacturing is undertaken. The Notifying Party considers that the exact geographic market definition can be left open in this case as the Transaction raises no competition concerns regardless of how the market is defined.

(175) Regarding GSM-R, the Notifying Party submits that the geographic scope of the market for GSM-R integration is likely national. According to the Notifying Party, while the equipment from GSM-R OEMs is the same throughout the EEA, the GSM-R network design is affected by local regulations and rules put in place by operators and infrastructure owners. In addition, GSM-R OEM suppliers must go through a qualification process, which is conducted at a national level. The Notifying Party considers that the exact geographic market definition can be left open as the Transaction raises no competition concerns regardless of how the market is defined.

7.5.2.2. Commission's assessment

(176) In line with previous decisional practice (see recitals (167)-(168)), the Commission considers, for the purposes of this Decision, that the relevant geographic market for (i) the manufacture and supply of SIM cards, (ii) OTA SIM card administration and services platform is at least EEA-wide, if not global.

(177) In relation to the geographic scope of the market for GSM-R integration, the Commission considers that, while there are elements that could point to a national geographic scope (see recital (175)), other considerations, such the presence of the same players across different EEA countries and the presence of the GSM-R standard (see recital (163)) suggest an EEA-wide or global geographic market.

7.5.2.3. Conclusion on the geographic market definition

(178) For the purpose of the present Decision, the exact geographic market definition can be left open as the Transaction would not significantly impede effective competition under any plausible market definition, including the narrowest possible market at the EEA level for the manufacture and supply of SIM cards and OTA SIM card administration and services platform, and at a national level for GSM-R integration.

7.5.3. Overall conclusion on market definition

(179) In light of the above, for the purpose of this Decision, the exact product and geographic market definition can be left open, since the Transaction would not significantly impede effective competition under any plausible market definition, including the narrowest possible market for (i) the manufacture and supply of SIM cards at the EEA level and (ii) the market for GSM-R integration at a national level. In line with previous decisional practice, for the purpose of the present Decision, the Commission concludes that the relevant product market is the market for OTA SIM card administration and services platform but leaves open the question whether the relevant geographic market is global or EEA-wide as the Transaction would not significantly impede effective competition under any plausible geographic market definition.

7.6. Access control smart cards

7.6.1. Product market definition

7.6.1.1. Notifying Party's views

(180) Gemalto sells a wide variety of smart cards for multiple applications, including for physical and logical access control. Thales purchases access control smart cards […] for use with its […].[114]

(181) Access control systems are tools and protocols used to protect hardware from unauthorised users. They include tools and protocols for identification, authentication, authorisation and accountability in IT systems. Access control systems can provide a user with "physical" or "logical" access. While "physical" access control limits access to buildings, rooms, areas and IT assets, "logical" access control limits connections to computer networks, system files and data, and is often needed for remote access of hardware. The line between physical and logical access control can, however, be blurred when physical access is controlled by software. For example, entry to a room may be controlled by a smart card and an electronic lock controlled by software. Only those in possession of an appropriate card and with knowledge of the PIN are permitted to enter the room. On swiping the card into a card reader and entering the correct PIN, the user's access rights/security level are checked against a security database and compared to the access rights/security level required to enter the room. Having logical access controlled centrally in software allows a user's physical access permissions to be rapidly amended or revoked.

(182) In the Form CO,[115] the Notifying Party submits that even if there are no Commission precedents specifically discussing access control smart cards (such as those used for remote administration of HSMs), in line with the Commission's findings in the *Axalto/Gemplus* and *Advent International/Morpho* cases, such cards could belong to a distinct product market, which at its narrowest would include all physical and logical access control microprocessor chip cards (regardless of their form factor e.g. traditional plastic cards, key fobs, or USB-based tokens).

(183) In the Notifying Party's view, from the demand side, various access control cards are purchased by the same customers and serve the same purpose – protecting hardware from unauthorised access (whether through physical or logical access control, or both). According to the Notifying Party, from the supply side, the process of manufacturing physical and logical access control smart cards is substantially the same.

(184) The Notifying Party considers that the exact product market definition can be left open in this case as the Transaction raises no competition concerns regardless of how the market is defined.

7.6.1.2. Commission's assessment

(185) Based on the Notifying Party's submission, from the demand side the line between physical and logical access control are possibly blurred when physical access is controlled by software, such as in the case of a smart card. From the supply side, vendors are increasingly offering dual-use access control cards that can simultaneously provide logical and physical access control (i.e. enabling the same credentials to both open a door and access a computer system).

---

114 [Description of Thales' product].

115 Form CO, Section 6, Chapter V.

7.6.1.3. Conclusion on the product market definition

(186) For the purpose of the present Decision, the exact product market definition can be left open as the Transaction would not significantly impede effective competition under any plausible market definition, including the narrowest possible market including for (i) physical and (ii) logical access control microprocessor chip cards.

7.6.2. Geographic market definition

7.6.2.1. Notifying Party's views

(187) The Notifying Party submits that the relevant geographic market is worldwide or at least EEA-wide. In the Notifying Party's view, the market is not national in scope as the same (access control) cards are sold in the EEA and globally. Furthermore, they also serve the same range of applications and use cases regardless of the country. According to the Notifying Party, customers do not have any specific requirements or preferences that vary depending on the country and buyers tend to select providers on the basis of global (or at least Union-wide) tenders, and they qualify bidders irrespective of their location. Most major access control smart card providers, including Assa Abloy/HID Global, FEITIAN, G&D, IDEMIA, and Paragon ID, are active globally (including in the EEA).

(188) The Notifying Party considers that the exact geographic market definition can be left open in this case as the Transaction raises no competition concerns regardless of how the market is defined.

7.6.2.2. Commission's assessment

(189) Based on the Notifying Party's submission, the Commission considers that there are indications that the relevant geographic market is global or at least EEA-wide.

7.6.2.3. Conclusion on the geographic market definition

(190) For the purpose of the present Decision, the exact geographic market definition can be left open as the Transaction does would not significantly impede effective competition under any plausible market definition, including the narrowest possible market at the EEA level.

7.6.2.4. Overall conclusion on market definition

(191) In light of the above, for the purpose of this Decision, the exact product and geographic market definition can be left open, since the Transaction would not significantly impede effective competition under any plausible market definition, including the narrowest possible market for physical or logical access control cards at the EEA-level.

7.7. Affected markets

7.7.1. Horizontally affected markets

(192) The Transaction gives rise to the following horizontally affected markets:

(1) The market for GP HSMs

(2) The market for Payment HSMs

(3) The potential market for network encryptors and the narrowest possible sub-segment for data in motion at Layer 2 at the EEA-wide market.[116]

7.7.2. Vertically affected markets

(193) The Transaction gives rise to vertically affected markets in relation to the links between the following markets[117]:

(1) the upstream EEA market for the manufacture and supply of SIM cards (where Gemalto's market share is [30-40]%) and the downstream national or EEA-wide market for GSM-R integration.

(2) the upstream EEA market for OTA SIM card administration platforms (where Gemalto's market share is around [40-50]%) and the downstream national or EEA-wide market for GSM-R integration.

(3) the upstream EEA market for access control smart cards (including a possible sub-segmentation based on physical or logical access control cards) for use in remote HSM administration and the downstream markets for GP HSMs and Payment HSMs where Thales market share is [40-50]% and [40-50]%, respectively, in 2017 (see Tables 5 and 10).

8. COMPETITIVE ASSESSMENT

(194) In this Section, the Commission carries out its competitive assessment with respect to the horizontal non-coordinated and coordinated effects of the Transaction in the

---

116 The Transaction does not give rise to a horizontally affected market for ES for data at rest/in use even if the Commission were to take into account the narrowest possible sub-segmentation. The Parties' combined market share in ES for data at rest/in use does not exceed [5-10]% on the worldwide level and would not exceed [0-5]% on the EEA level. For file/folder encryption level, the Parties' combined share does not exceed [10-20]% on the worldwide level and would not exceed [5-10]% on the EEA level. For database encryption, the Parties' combined market share would not exceed [10-20]% on the worldwide level and would not exceed [0-5]% on the EEA level. For application encryption, the Parties' combined market share would not exceed [10-20]% on the worldwide level and would not exceed [0-5]% on the EEA level. The limited revenues which the Parties derive from ES in tokenization and data masking would amount to a combined market share below [0-5]% both on the worldwide and EEA level. The Parties are not active in disk/storage encryption. The horizontal overlap in the supply of ES solutions for data at rest/in use will therefore no longer be discussed in Section 8. The Transaction similarly does not give rise to a horizontally affected market in the supply of (cyber) security evaluation services. Irrespective of the exact product and geographic market definition, the Parties estimate that their revenues from the sale of such services account for less than [10-20]% of the market for the provision of (cyber) security evaluation services. On the possible market for CSPN evaluation services, the Notifying Party submits that there are nine French labs in addition to those of the Parties that have been accredited by ANSSI for the evaluation of products under CSPN. As companies operate these labs as part of their broader R&D/technical capabilities rather than as a stand-alone profit centres, they do not publish revenue figures. The Notifying Party estimates that the Parties' combined market share would be well below [20-30]% globally and in the EEA. Therefore, the horizontal overlap in the supply of (cyber) security evaluation services will also not be further discussed in Section 8.

117 In the Form CO, the Notifying Party has identified a number of other potential vertical links. However, these possible vertical links will not be further discussed in Section 8 for the following reasons: (i) regarding the vertical link between Gemalto's activities on the upstream market for transport cards and Thales' activities on the downstream market for ticketing systems, […]; (ii) regarding the vertical link between Thales' activities on the upstream market for the provision of security evaluation and Gemalto's need for evaluation of its smart cards, […]; (iii) […], Gemalto became active in the provision of biometric solutions (with its Live Face Identification system – "LIVE") which could theoretically be used as a plug-in in video surveillance systems – an area where Thales is active. However, […]; (iv) in 2013 Gemalto acquired Invia, […]. This vertical relationship is *de minimis* […]. The Transaction will not affect the market structure and any potential foreclosure concerns can be excluded.

affected markets identified in Section 7.7. To this aim, Section 8.1 discusses the relevant legal test. Sections 8.2 – 8.4 assess the likely effects of the Transaction, respectively, on the EEA-wide or worldwide market for GP HSMs, Payment HSMs, and Encryption Software. Section 8.5 addresses the non-horizontal overlaps arising from the Transaction.

8.1. Legal test

(195) Under paragraphs 2 and 3 of Article 2 of the Merger Regulation, the Commission must assess whether a proposed concentration would significantly impede effective competition in the internal market or in a substantial part of it, in particular through the creation or strengthening of a dominant position. In this respect, a merger may entail horizontal and/or vertical effects.

(196) Horizontal effects are those deriving from a concentration where the undertakings concerned are actual or potential competitors of each other in one or more of the relevant markets concerned. Vertical effects are those deriving from a concentration where the undertakings concerned are active on different or multiple levels of the supply chain.

8.1.1. Horizontal non-coordinated effects

(197) The Horizontal Merger Guidelines[118] distinguish between two main ways in which mergers between actual or potential competitors on the same relevant market may significantly impede effective competition, namely non-coordinated and coordinated effects.

(198) The Horizontal Merger Guidelines describe horizontal non-coordinated effects as follows: "*A merger may significantly impede effective competition in a market by removing important competitive constraints on one or more sellers who consequently have increased market power. The most direct effect of the merger will be the loss of competition between the merging firms. For example, if prior to the merger one of the merging firms had raised its price, it would have lost some sales to the other merging firm. The merger removes this particular constraint. Non-merging firms in the same market can also benefit from the reduction of competitive pressure that results from the merger, since the merging firms' price increase may switch some demand to the rival firms, which, in turn, may find it profitable to increase their prices. The reduction in these competitive constraints could lead to significant price increases in the relevant market.*"[119]

(199) Therefore, a merger giving rise to such non-coordinated effects might significantly impede effective competition by creating or strengthening the dominant position of a single firm, one which, typically, would have an appreciably larger market share than the next competitor post-merger.

(200) However, under the substantive test set out in Article 2(2) and (3) of the Merger Regulation, also mergers that do not lead to the creation or the strengthening the dominant position of a single firm may create competition concerns. Indeed, the Merger Regulation recognises that in oligopolistic markets, it is all the more necessary to maintain effective competition.[120] This is in view of the more significant consequences that mergers may have on such markets. For this reason, the Merger

---

[118] Guidelines on the assessment of horizontal mergers under the Council Regulation on the control of concentrations between undertakings OJC 31, 05.02.2004 ("Horizontal Merger Guidelines").

[119] Horizontal Merger Guidelines, para 24.

[120] Merger Regulation, para. 25.

Regulation provides that "*under certain circumstances, concentrations involving the elimination of important competitive constraints that the merging parties had exerted upon each other, as well as a reduction of competitive pressure on the remaining competitors, may, even in the absence of a likelihood of coordination between the members of the oligopoly, result in a significant impediment to effective competition*".[121]

(201) The Horizontal Merger Guidelines list a number of factors which may influence whether or not significant horizontal non-coordinated effects are likely to result from a merger, such as the large market shares of the merging firms, the fact that the merging firms are close competitors, the limited possibilities for customers to switch suppliers, or the fact that the merger would eliminate an important competitive force.[122] That list of factors applies equally regardless of whether a merger would create or strengthen a dominant position, or would otherwise significantly impede effective competition due to non-coordinated effects. Furthermore, not all of these factors need to be present to make significant non-coordinated effects likely and it is not an exhaustive list.[123]

(202) Finally, the Horizontal Merger Guidelines describe a number of factors, which could counteract the harmful effects of the merger on competition, including the likelihood of buyer power, entry and efficiencies.

8.1.2. Horizontal coordinated effects

(203) A merger in a concentrated market may significantly impede effective competition due to horizontal coordinated effects if, through the creation or strengthening of a collective dominant position, it increases the likelihood that firms are able to coordinate their behaviour in this way and raise prices, even without entering into an agreement or resorting to a concerted practice within the meaning of Article 101 TFEU.[124] A merger may also make coordination easier, more stable or more effective for firms that were already coordinating before the merger, either by making the coordination more robust or by permitting firms to coordinate on even higher prices.[125]

8.1.3. Vertical effects

(204) Vertical mergers involve companies operating at different levels of the same supply chain. For instance, a vertical merger occurs when a manufacturer of a certain product merges with one of its distributors.

(205) Pursuant to the Commission Guidelines on the assessment of non-horizontal mergers under the Council Regulation on the control of concentrations between undertakings (the "Non-Horizontal Merger Guidelines"),[126] vertical mergers do not entail the loss of direct competition between merging firms in the same relevant market and provide scope for efficiencies.

---

121 Merger Regulation, para. 25.
122 Horizontal Merger Guidelines, paras 27 et seq.
123 Horizontal Merger Guidelines, para 26.
124 Horizontal Merger Guidelines, para 39.
125 Horizontal Merger Guidelines, para 39.
126 OJ C 265, 18.10.2008, p. 6.

(206) However, there are circumstances in which vertical mergers may significantly impede effective competition. This is in particular the case if they give rise to foreclosure.[127]

(207) The Non-Horizontal Merger Guidelines distinguish between two forms of foreclosure: input foreclosure, where the merger is likely to raise costs of downstream rivals by restricting their access to an important input, and customer foreclosure, where the merger is likely to foreclose upstream rivals by restricting their access to a sufficient customer base.[128]

(208) Pursuant to the Non-Horizontal Merger Guidelines, input foreclosure arises where, post-merger, the new entity would be likely to restrict access to the products or services that it would have otherwise supplied absent the merger, thereby raising its downstream rivals' costs by making it harder for them to obtain supplies of the input under similar prices and conditions as absent the merger.[129]

(209) For input foreclosure to be a concern, the merged entity should have a significant degree of market power in the upstream market. Only when the merged entity has such a significant degree of market power, can it be expected that it will significantly influence the conditions of competition in the upstream market and thus, possibly, the prices and supply conditions in the downstream market.[130]

(210) Pursuant to the Non-Horizontal Merger Guidelines, customer foreclosure may occur when a supplier integrates with an important customer in the downstream market and because of this downstream presence, the merged entity may foreclose access to a sufficient customer base to its actual or potential rivals in the upstream market (the input market) and reduce their ability or incentive to compete which in turn, may raise downstream rivals' costs by making it harder for them to obtain supplies of the input under similar prices and conditions as absent the merger. This may allow the merged entity profitably to establish higher prices on the downstream market.[131]

(211) For customer foreclosure to be a concern, a vertical merger must involve a company which is an important customer with a significant degree of market power in the downstream market. If, on the contrary, there is a sufficiently large customer base, at present or in the future, that is likely to turn to independent suppliers, the Commission is unlikely to raise competition concerns on that ground.[132]

8.1.4. Conglomerate non-coordinated effects

(212) Conglomerate mergers consist of mergers between companies that are active in closely related markets, for instance suppliers of complementary products or of products which belong to a range of products that is generally purchased by the same set of customers for the same end use.[133]

(213) Pursuant to the Non-Horizontal Merger Guidelines, in most circumstances, conglomerate mergers do not lead to any competition problems. However, foreclosure effects may arise when the combination of products in related markets may confer on the merged entity the ability and incentive to leverage a strong market

127 Non-Horizontal Merger Guidelines, para 18.
128 Non-Horizontal Merger Guidelines, para 30.
129 Non-Horizontal Merger Guidelines, para 31.
130 Non-Horizontal Merger Guidelines, para 35.
131 Non-Horizontal Merger Guidelines, para 58.
132 Non-Horizontal Merger Guidelines, para 61.
133 Non-Horizontal Merger Guidelines, para 91.

position from one market to another closely related market by means of tying or bundling or other exclusionary practices.[134]

(214) The Non-Horizontal Merger Guidelines distinguish between bundling, which usually refers to the way products are offered and priced by the merged entity and tying, usually referring to situations where customers that purchase one good (the tying good) are required to also purchase another good from the producer (the tied good).[135]

(215) Within bundling practices, a distinction is also made between pure bundling and mixed bundling. In the case of pure bundling the products are only sold jointly in fixed proportions. With mixed bundling the products are also available separately, but the sum of the stand-alone prices is higher than the bundled price.[136]

(216) Tying can take place on a technical or contractual basis. For instance, technical tying occurs when the tying product is designed in such a way that it only works with the tied product (and not with the alternatives offered by competitors).

(217) While tying and bundling have often no anticompetitive consequences, in certain circumstances such practices may lead to a reduction in actual or potential competitors' ability or incentive to compete. This may reduce the competitive pressure on the merged entity allowing it to increase prices or deteriorate supply conditions in other ways.[137]

(218) In assessing the likelihood of such a scenario, the Commission examines, first, whether the merged firm would have the ability to foreclose its rivals[138], second, whether it would have the economic incentive to do so[139] and, third, whether a foreclosure strategy would have a significant detrimental effect on competition, thus causing harm to consumers.[140] In practice, these factors are often examined together as they are closely intertwined.

8.2. GP HSMs

8.2.1. Market shares and concentration levels

8.2.1.1. Introduction

(219) According to the Horizontal Merger Guidelines,[141] market shares constitute useful first indications of the market structure and of the competitive importance of the market players. The Horizontal Merger Guidelines explain that the larger the market share, the more likely a firm is to possess market power.[142] Furthermore, the larger the addition of market share (or "increment") brought by the transaction, the more likely it is that a merger will lead to a significant increase in market power. Post-merger market shares are calculated on the assumption that the post-merger combined market share of the Parties is the sum of their pre-merger market shares. Although market shares and additions of market shares only provide first indications

134 Non-Horizontal Merger Guidelines, para 93.
135 Non-Horizontal Merger Guidelines, para 97.
136 Non-Horizontal Merger Guidelines, para 96.
137 Non-Horizontal Merger Guidelines, para 93.
138 Non-Horizontal Merger Guidelines, paras 95 to 104.
139 Non-Horizontal Merger Guidelines, paras 105 to 110.
140 Non-Horizontal Merger Guidelines, paras 111 to 118.
141 Horizontal Merger Guidelines, para 14.
142 Horizontal Merger Guidelines, para 27.

of market power and increases in market power, they are normally important factors in the competitive assessment.

8.2.1.2. Market shares provided by the Notifying Party

(220) The Notifying Party has worked together with the International Data Corporation ("IDC") to provide market shares for the purpose of the assessment of this Transaction.

(221) IDC used a number of different inputs to estimate market shares: (i) existing and historical IDC forecasts of security products and data protection markets (e.g., software as a service, IT infrastructure for the public cloud, and cloud professional services), (ii) public information about encryption, tokenization, and key management markets as well as IT cloud services providers' revenue, product mixes, customer segmentation, and strategies, (iii) IDC end-user surveys about encryption, data protection, cloud drivers, inhibitors, and adoption plans, (iv) IDC discussions with suppliers, security resellers, consultancies, and service providers about their strategies and plans, (v) IDC models of historical information technology adoption/diffusion and IDC models of vendor market share concentration in similar markets.[143]

(222) At Thales' request, IDC prepared similar estimates for the years 2014-2016.

(223) IDC then estimated splits for this overall key management market by region, including, in particular for the EEA, the US, and all other jurisdictions combined.[144]

(224) After having estimated the total market and segment sizes, globally and by region for each of the last four years, IDC then split out estimates for individual competitor sizes using supply-side data, demand-side data, industry trends, and the economic outlook to generate a model of the IT opportunity by company.

(225) IDC also took into account the Parties' actual sales as well as input provided by the Parties based on their knowledge of the market. For the Parties' competitors, IDC generally estimated revenues using financial reports, SEC documents, analyst presentations, public and private guidance, historical performance, the financial press, blogs, competitors' comments, and IDC's internal knowledge.

(226) The market shares were at a final stage adjusted based on the own market knowledge of the Parties.

8.2.1.3. Market shares for GP HSMs as provided by the Notifying Party

(227) Based on the data provided by the Notifying Party, the market shares of the Parties in the market for GP HSMs are provided in Tables 1-3. The table presents the market shares for GP HSMs, excluding HSM aaS.

---

143 In addition to these sources and IDC's software tracker database, IDC leveraged the methodology used in the compilation of the Worldwide Enterprise Black Book, which is based on IDC's research taxonomy and is the basis for covering updated forecasts for IT spending (across hardware, software, and services).

144 IDC also split out segment size estimates both globally and by region for both GP HSMs and Payment HSMs. IDC took into account existing manufacturer products and capabilities, publicly available information from the Payment Card Industry Security Standards Council on cryptographic modules validated for payment transactions and publicly available information provided by the National Institute of Standards and Technology (NIST) cryptographic module validation program.

Table 1: Worldwide and EEA market for GP HSMs (excluding HSMs aaS) (2017)

Company	Worldwide		EEA	
	Shares	Revenues (MEUR)	Shares	Revenues (MEUR)
Thales	[20-30]%	[…]	[20-30]%	[…]
Gemalto	[30-40]%	[…]	[20-30]%	[…]
Combined	***[50-60]%***	***[…]***	***[50-60]%***	***[…]***
Atos	[5-10]%	[…]	[10-20]%	[…]
Utimaco	[5-10]%	[…]	[10-20]%	[…]
Ultra Electronics	[5-10]%	[…]	[0-5]%	[…]
Others	[20-30]%	[…]	[20-30]%	[…]

Source: Form CO

Table 2: Worldwide and EEA market for GP HSMs (excluding HSMs aaS) (2016)

Company	Worldwide		EEA	
	Shares (%)	Revenues (MEUR)	Shares (%)	Revenues (MEUR)
Thales	[30-40]%	[…]	[20-30]%	[…]
Gemalto	[30-40]%	[…]	[20-30]%	[…]
Combined	***[60-70]%***	***[…]***	***[50-60]%***	***[…]***
Atos	[5-10]%	[…]	[10-20]%	[…]
Utimaco	[5-10]%	[…]	[10-20]%	[…]
Ultra Electronics	[5-10]%	[…]	[0-5]%	[…]
Others	[20-30]%	[…]	[20-30]%	[…]

Source: Form CO

Table 3: Worldwide and EEA market for GP HSMs (excluding HSMs aaS) (2015)

Company	Worldwide		EEA	
	Shares (%)	Revenues (MEUR)	Shares (%)	Revenues (MEUR)
Thales	[30-40]%	[…]	[20-30]%	[…]
Gemalto	[30-40]%	[…]	[30-40]%	[…]
Combined	***[60-70]%***	***[…]***	***[50-60]%***	***[…]***
Atos	[5-10]%	[…]	[10-20]%	[…]
Utimaco	[5-10]%	[…]	[10-20]%	[…]
Ultra Electronics	[5-10]%	[…]	[0-5]%	[…]
Others	[10-20]%	[…]	[10-20]%	[…]

Source: Form CO

(228) When considering the market for GP HSMs, Table 1 shows that post-Transaction, the combined market share of the Parties in 2017 was [50-60]% and [50-60]% on the worldwide and the EEA-wide market respectively.

(229) The next largest competitors have significantly lower market shares. Atos has a market share of [5-10]% at worldwide level and [10-20]% at EEA level, whereas Utimaco's worldwide and EEA market share is [5-10]% and [10-20]% respectively. The Commission understands Atos' market share might be in reality significantly lower than the one provided by the Notifying Party.

(230) Tables 2 and 3 show that the market shares of Thales and Gemalto in 2016 amounted to [60-70]% and [50-60]% at worldwide and EEA level respectively, whereas in 2015 it amounted to [60-70]% and [50-60]% at worldwide and EEA level respectively. The […] trend over the period 2015-2017 appears mainly due to the increasing revenues of Atos, according to the Notifying Party. However, as explained in recital (244), Atos' revenues appear to be overstated.

(231) The post-transaction HHI on the market for GP HSMs is […] on the worldwide and […] on the EEA market for 2017. The delta brought by the Transaction is […] on the worldwide and […] on the EEA market. According to the Horizontal Merger Guidelines, both the post-merger HHI and the delta of the Transaction are likely to raise competition concerns.

8.2.1.4. Submission on contestability of customers provided by the Notifying Party

(232) Further to their market shares estimates, the Notifying Party's economic advisers have submitted an economic report that analyses the contestability of sales and tries to quantify the extent of customer switching between the Parties. To that effect, the study assesses Thales and Gemalto's EEA sales data in the GP HSM segment for the years 2015-2017.

(233) First, the study tries to assess the portion of end-customers that are contestable over the period in question. The study finds that only [20-30]% of Thales' sales revenues and [10-20]% of Gemalto's revenues are not coming from repeat customers over the 3 years period assessed (2015, 2016 and 2017). From this, it concludes that the vast majority of the Parties' sales are not competitively contestable. Hence, the study argues, there can be no restriction of competition brought about by the Transaction.

(234) Second, the study tries to assess the proportion of contestable sales that switched from one of the Parties to the respective other Party rather than to third parties. It finds that only [5-10]% of Thales's revenues were switched to Gemalto. Conversely, only [10-20]% of Gemalto's revenues were switched to Thales. The study concludes from this that competitive diversion between the Parties is far smaller than one would expect given their high market shares. The Parties' market position therefore overstates the actual, limited degree of competitive interaction between them.

(235) The Commission considers that this study is methodologically flawed, of limited evidentiary value and does not permit any of the inferences drawn from it for the reasons set out in recitals (236)-(242).

(236) First, the study assumes that repeat purchasers should generally be considered as non-contestable and thus impervious to competition. However, the fact that customers have purchased from the same supplier before does not mean that there is no competition between vendors to restrict.

(237) Second, given the short time frame considered by the study, it is unclear why one should expect any more switching activity in this market even if customers were fully contestable. Specifically, the study considers potential switching in only two years (2016 and 2017). However, in a durable goods industry such as GP HSM, where multi-year customer relationships are the norm, only a limited proportion of contracts will come up for renewal and only a limited number of customers will consider purchasing new hardware in any given year.

(238) Third, even if customers were entirely locked-in with their supplier once they have made an initial purchase for a given application, this would not imply that safeguarding competition between suppliers becomes irrelevant. On the contrary, the economic literature on switching costs shows quite clearly that such vendor lock-in merely relocates the locus of competition towards the stage of initial purchases for new applications, where the continued availability of competitive alternatives then becomes all the more critical.

(239) Fourth, where customers experience some degree of ex-post lock-in, the availability of alternative suppliers is what protects customers from prices rising even higher. Such customers may not be inclined to switch away from their original vendor for legacy use cases. But it is the theoretical possibility of doing so that stops suppliers from extracting even larger rents from locked-in customers.

(240) Fifth, the study wrongly interprets any instance where a customer stopped purchasing from one of the Parties and did not start purchasing from the other Party as a "switch away" towards third party rivals.[145] This introduces a further bias into the assessment

[145] See p.6 of the report "Analysis of Constestable Sales and Switching Customers in the GP HSM segment in the EEA" for an acknowledgment from the Parties' economists on the difficulty of interpreting a customer that stops buying as switching away "[w]e do not know whether a customer actually switched away its purchase (e.g., to a third party vendor), simply stopped purchasing GP HSM-related products from either Party or went out of business."

that will tend to understate the actual switching activity between the Parties (and potentially severely so).

(241) Sixth, the study's definition of switching entirely ignores the possibility of dual sourcing and only counts customers as switching to the respective merging partner if sales with the previous supplier are reduced to zero. The study therefore does not account for the various forms of partial switching between the Parties by multi-sourcing customers.

(242) Finally, the study's main claims regarding closeness of competition between the Parties are also inconsistent with the large body of evidence uncovered during the market investigation. In particular, the Parties' own internal documents portray the respective merging partner as an important competitive rival. Moreover, customers explain that competition between the Parties is particularly intense (not remote, as the study alleges without providing any reliable evidence to that effect).

(243) For the reasons set out in recitals (236)-(242), the Commission considers that the economic study does not show, as it purports to do, that the competitive interaction between Thales and Gemalto is of no relevance for customers and the competitive process. It is not possible to conclude from the submitted evidence that the majority of customers are not contestable. Nor is it possible to infer from it that the Parties are no close competitors for contestable sales. The Commission therefore strongly questions the study's conclusions due to lack of its factual basis.

8.2.1.5. Market reconstruction undertaken by the Commission

(244) In the Article 6(1)(c) Decision, the Commission considered that the data provided and the underlying methodology give rise to a number of issues that could potentially lead to a misrepresentation of the Parties' market shares, such as the following:

(a) with regard to a possible overall HSM market, market share data include revenues from providers of HSM aaS, which the Commission understands are customers of HSMs and would create a double counting of revenue;[146]

(b) some of the competitors listed in IDC tables have not confirmed the market shares and have provided much lower revenue figures, which would significantly reduce their actual presence in the market, such as Atos, which reports their worldwide revenues from GP HSMs to be EUR [0-20] million and from Payment HSMs EUR [0-20] million;[147]

(c) some competitors listed in the tables do not seem to supply HSMs as such, such as Tokheim and Cryptera;[148]

(d) some competitors listed in the tables sell to another company which is also included in the table listing the competitors (such as Cavium selling to AWS)[149], hence its inclusion in the overall market is at least debatable; and

(e) the IDC methodology relies on a high number of assumptions that are unknown to the Commission, especially in relation to revenue figures of some competitors, and the estimated market size.[150]

---

146 For example, the revenues of both AWS (HSM aaS provider) and Cavium (its HSM provider) are counted in the market shares submitted by the Notifying Party.

147 Replies to Questionnaire Q1 – competitors of 19 June 2018, question A.4.

148 Notifying Party's reply to the Commission's RFI 7: […].

149 See recital 45.

150 [Description of IDC's methodology].

(245) Moreover, during its investigation the Commission found evidence from internal documents that the Parties' actual market shares differ significantly from those estimated by IDC.

(246) In a Thales internal document dating from August 2017 assessing competition in the overall HSM market[151], Gemalto and Thales are presented as HSM vendors of similar market share, circa [40-50]%. According to this document the Parties would have a combined market share of [80-90]% worldwide. In another Thales internal document, an executive of Thales e-Security confirms combined worldwide market shares of [90-100]% in GP HSMs for the Parties in 2016 seem reasonable.[152]

(247) The Commission therefore considers that the Parties' market shares are likely to be significantly higher than the ones presented by the Notifying Party. As a result, during the in-depth investigation the Commission undertook a market reconstruction exercise.

8.2.1.6. The Commission's market reconstruction exercise

(248) The Commission contacted HSMs manufacturers identified by the Notifying Party in its market shares submissions during the in-depth investigation to request them to provide revenue information at the EEA and worldwide level, differentiating between Payment and GP HSMs, for 2015, 2016, 2017 and the period January to August 2018.

(249) All competitors actually active in the HSM business except one have provided such information to the Commission.[153] Some third Parties identified by the Notifying Party as active in the HSM business have explained to the Commission that they are not active in this sector or that they are customers of HSM manufacturers.[154]

(250) Revenue data was then aggregated across firms to provide overall market sizes for GP HSMs and Payment HSMs, at the EEA and worldwide levels, which were used to compute market shares of the Parties and their competitors.

8.2.1.7. Market shares for GP HSMs based on the Commission's market reconstruction

(251) The market shares for GP HSMs obtained on the basis of the Commission's market reconstruction are presented in Table 4.

---

151 [Reference to internal documents].

152 [Reference to internal documents].

153 The competitor which did not provide disaggregated information however provided an overall revenue figure for its HSM business worldwide, for 2017. In order to approximate disaggregated revenues of the competitor per geography and product (Payment and GP), the Commission used the Parties' estimates, rescaling by the overall revenues provided by the competitor.

154 See email exchange with CCV of 13/09/2018.

Table 4: Evolution of GP HSMs revenue market shares based on the Commission's market reconstruction

		Market shares		Market size (mEUR)	
		Worldwide	**EEA**	**Worldwide**	**EEA**
Jan-Aug 2018	**Thales**	[30-40]%	[30-40]%	[…]	[…]
	Gemalto	[40-50]%	[30-40]%		
	Combined	**[70-80]%**	**[70-80]%**		
2017	**Thales**	[30-40]%	[40-50]%	[…]	[…]
	Gemalto	[40-50]%	[30-40]%		
	Combined	**[70-80]%**	**[70-80]%**		
2016	**Thales**	[40-50]%	[30-40]%	[…]	[…]
	Gemalto	[40-50]%	[30-40]%		
	Combined	**[80-90]%**	**[70-80]%**		
2015	**Thales**	[40-50]%	[30-40]%	[…]	[…]
	Gemalto	[40-50]%	[40-50]%		
	Combined	**[80-90]%**	**[80-90]%**		

(252) The combined market shares reconstructed by the Commission are consistent with evidence obtained during the market investigation from internal documents review (see recital (246)) indicating a combined market share of [80-90]%. Combined market shares range from [80-90]% in 2015 to [70-80]% in 2017 for in the EEA, from [80-90]% in 2015 to [70-80]% in 2017 worldwide.

(253) The market reconstruction for GP HSMs undertaken by the Commission in its in-depth investigation confirms the doubts expressed by the Commission in the Article 6(1)(c) Decision (see recital (244)), i.e. that the Parties' actual market shares are significantly higher than the estimates provided by the Notifying Party.[155]

155 See Article 6(1)(c) Decision of 23 July 2018, paras 94-96.

(254) The Parties' combined market share in the EEA, […], remains above [70-80]% which in itself may show evidence of the creation of a dominant market position due to the Transaction.[156]

(255) Competitors' 2017 market shares based on the Commission's market reconstruction are presented in Table 5.

Table 5: GP HSMs market shares of the Parties and competitors, for 2017, based on the Commission's market reconstruction

2017	GP HSMs	
	WW	EEA
Thales	[30-40]%	[30-40]%
Gemalto	[40-50]%	[30-40]%
Combined	[70-80]%	[70-80]%
Utimaco	[0-12]%	[0-23]%
Atos	[0-3]%	[0-9]%
Cavium	[0-18]%	
Others	[0-10]%	[0-10]%

8.2.1.8. Conclusion on market shares and concentration levels

(256) On the basis of the Commission's market reconstruction, post-transaction HHI on the market for GP HSMs is […] on the worldwide and […] on the EEA market for 2017. The delta brought by the Transaction is […] on the worldwide and […] on the EEA market. These HHI and delta brought by the Transaction far exceed those computed on the market shares (see recital (231)). According to the Horizontal Merger Guidelines, both the post-merger HHI and the delta of the Transaction are likely to raise competition concerns.

(257) Following the results of the market investigation, the competitive assessment is carried out at the narrower, at least EEA-wide level, which is followed by an assessment at worldwide level.

8.2.2. Non-coordinated horizontal effects on the EEA-wide market for GP HSMs

(258) In this Section the Commission assesses the likelihood of anticompetitive horizontal non-coordinated effects in the EEA-wide market for GP HSMs. To this aim, Section 8.2.2.1 presents the competitive conditions of the market pre-Transaction. Sections 8.2.2.2 to 8.2.2.4 assess the competitive constraints exerted by the Parties on each

156 Horizontal Merger Guidelines, para 17.

other and on their competitors. Sections 8.2.3 and 8.2.4 assess the other competitive constraints which will remain post-Transaction, and the likelihood that they off-set the anticompetitive effects of the Transaction. Section 8.2.5 draws conclusions.

8.2.2.1. Competitive conditions pre-Transaction

(259) GP HSMs are highly differentiated goods, and the parameters of competition on which the Parties compete are not limited to price, but rather pertain to functionality and security of the devices offered as well as the level of service.

(260) The Commission considers that when selecting GP HSM suppliers and offerings customers take into account a number of factors, price being only one of them. Therefore, the alleged price benefit to customers which in the view of the Notifying Party results from the constraint that CSPs exert on on-premise GP HSMs only addresses one aspect of competition. The Commission considers that it cannot compensate for the removal of the important competitive constraints which the Parties exerted on each other pre-Transaction for the reasons set out in recitals (261)-(269).

(261) First, in the course of the market investigation[157], customers indicated that price is not the only and decisive parameter on which customers rely when selecting a GP HSM supplier and a GP HSM solution. One customer stated that they consider "*features, benefits, quality, and price as part of our holistic review of potential HSM suppliers*".[158]

(262) Other factors include functionality, certification and security level as well as software compatibility and ease of integration with existing applications. Customers also view as important the ability of the suppliers to provide maintenance and support. A number of customers also value local presence and support.

(263) Customers also refer to track record, reputation, market shares and financial stability as important parameters when selecting a GP HSM supplier. Some customers attach specific importance to reputation and track record when selecting a GP HSM supplier: "*they need to be a reputable company, there are only two of these Thales and Gemalto*".[159]

(264) Second, customers consider that the strengths of Thales are that they are an "*established and respected company*", with "*track record, price, quality, support knowledge and overall good service*".[160] A customer explains that "*Thales' strengths include (i) that it is a centrally-managed solution, (ii) its innovative capabilities, (iii) the firm provides complete solutions, (iv) its ability to obtain necessary certifications and support for working with other vendor applications, and (v) the stringht of its customer support*".[161]

(265) Third, for Gemalto, customers consider that its strengths include "*brand, quality and price*" and that "*Gemalto has a very scalable and easy-to-manage HSM offering compared to other suppliers. They are easy to deploy, have a solid track record, and good support*".[162]

---

157 Replies to Questionnaire Q2 – customers of 19 June 2018, question 30.
158 Replies to Questionnaire Q2 – customers of 19 June 2018, question 30.
159 Replies to Questionnaire Q2 – customers of 19 June 2018, question 33.
160 Replies to Questionnaire Q2 – customers of 19 June 2018, question 46.
161 Replies to Questionnaire Q2 – customers of 19 June 2018, question 46.
162 Replies to Questionnaire Q2 – customers of 19 June 2018, question 47.

(266) Fourth, Thales and Gemalto are both considered by customers to be strong in quality, price, innovative capabilities, logistical capabilities, ability to offer complete solutions, as well as in their track record and extent of past references, local presence in various EEA countries, and their ability to obtain and update the required certifications. [163]

(267) Fifth, innovation in the market for HSMs plays a very important role, particularly due to the emerging cloud-based solutions and the gradual switch of customers to hybrid environments as further explained in Section 8.2.4.

(268) As outlined in recital (263), reputation and track record are among the main parameters that customers take into account when selecting a GP HSM provider. Customers have identified Thales and Gemalto as the main, if not the only, two players on the market with a proven track record and reputation.[164]

(269) Similarly, after sales support and maintenance, preferably 24/7, are of significant importance for customers of GP HSMs. Thales and Gemalto are the two manufacturers that are in a position to offer after-market services around the globe either directly or through specialised resellers.[165] Based on the data provided by the Parties, the revenues from after-market sales represented around [40-50]% of their revenue sales in 2017 for the GP HSM market.[166]

8.2.2.2. Competitive constraints exerted by the Parties

A. Closeness of competition between Thales and Gemalto

Notifying Party's views

(270) The Notifying Party submits that the Parties are not each other's closest competitors. A detailed analysis of the Parties' overlapping customers demonstrate that the majority of Thales' and Gemalto's customers do not source GP HSMs from both Parties and to the extent customers do source GP HSMs from both Parties, they typically concentrate most of their purchases on one of the two vendors, suggesting that customers use the Parties' HSMs for different use cases. Separately, a further assessment of customer switching between the Parties conducted by […] on the basis of the Parties transactional data suggests, according to the Notifying party, that switching/diversion ratios between the Parties are well below what one might expect given the Parties respective historical shares, again suggesting a lack of closeness in competition.

Commission's assessment

(271) The Commission considers that Thales and Gemalto are close competitors in the market for GP HSMs on the EEA-wide or worldwide geographic market. This finding is based on a consistent body of evidence presented in the recitals (272)-(292).

---

163 Replies to Questionnaire Q2 – customers of 19 June 2018, questions 46 and 47.

164 Replies to Questionnaire Q2 – customers of 19 June 2018, questions 30-32.

165 Replies to Questionnaire Q2 – customers of 19 June 2018, questions 32 and 46.

166 For Thales, after-market sales for GP HSM in the EEA in 2017 were equal EUR […] ([…]% of total revenues), and EUR […] worldwide ([…]% of total revenues). For Gemalto, after-market sales for GP HSM in the EEA in 2017 were equal EUR […] ([…]% of total revenues), and EUR […] worldwide ([…]% of total revenues).

(i) Both Thales and Gemalto are traditional vendors with a strong track record

(272) Thales and Gemalto are the clear market leaders, offering solutions with a global reach. Thales is active worldwide with its nShield lines of GP HSMs, selling directly to end-customers or through resellers. Similarly, Gemalto sells its Safenet GP HSMs globally also directly or through resellers.

(273) The offering of the alternative manufacturers present on the HSM market does not match that of Thales and Gemalto. Utimaco is also a GP HSM provider with global reach, however it appears to be active predominantly in Germany and neighbouring countries.[167] From Thales' internal documents it also appears that Utimaco is viewed as a competitor but only in specific geographic areas.[168] Respondents to the market investigation have indicated that Utimaco has a focus in Germany and its products lack of security reputation and financial stability as it is controlled by Private equity funds.[169] Atos' GP HSMs are described to have a very limited capacity for the storage keys whereas the company is focused geographically in France, Belgium and Luxembourg.

(ii) Both Thales and Gemalto offer a wide range of neighbouring solutions

(274) 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. 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 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. These cards perform encryption, digital signing and key generation on behalf of an extensive range of commercial and custom-built applications, including certificate authorities, code signing and more. nShield Solo HSMs are available in two series: classic nShield Solo+ HSMs, and the high performance nShield Solo XC HSM series. The CipherTrust Cloud Key Manager delivers key management either as a service in the cloud based on a virtual DSM or as an on-premise deployment using the Vormetric Data Security Manager to securely manage keys. nShield Bring Your Own Key (BYOK) allows users to use their own keys in cloud applications, regardless of whether on AWS, Google Cloud Platform 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.

(275) Gemalto's SafeNet Luna Network HSM is a 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. 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. The SafeNet USB HSM solution delivers key

---

167 Idemia's non-confidential submission entitled" Case M.8797 - Thales / Gemalto - competition concerns for IDEMIA", dated 3 July 2018.

168 [Reference to internal documents].

169 Idemia's non-confidential submission entitled" Case M.8797 - Thales / Gemalto - competition concerns for IDEMIA", dated 3 July 2018.

management in a portable appliance with a USB interface. Its small size makes it especially attractive to customers who need to physically remove and store the appliance. 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. Known as functionality modules, special toolkits provide a comprehensive facility to develop and deploy custom firmware on the HSM. ProtectServer HSMs exist as network connected versions or as PCI cards. The SafeNet Crypto Command Center ("CCC") provides a complete, centralised solution for the management of encryption HSM resources in the cloud. As an HSMs as a service, customers can quickly and cost effectively provision and remotely manage single or groups of SafeNet Luna Network HSMs from one central location. Encrypted resources can be provisioned on demand for one to thousands of HSMs simultaneously. Customers can also monitor encrypted resources, generate reports, and get continuous updates on the status of their appliances. Customers benefit from cost savings, and simplified management and administration.

(iii) Thales and Gemalto compete head-to-head

(276) The Commission considers that Thales and Gemalto compete head-to-head, notably with regard to their traditional GP HSMs offerings. Being the main GP HSMs manufacturers, Thales and Gemalto also perceive each other as main competitors in relation to innovation and getting ready for the cloud and cooperation with CSPs.

(277) First, the GP HSMs of the two parties are in direct competition. Internal documents of Thales and Gemalto show that each party perceives the other as their closest competitor.

(278) In a power point presentation created in 2017, in which Thales discusses the competitive strengths of various GP HSM manufacturers, Thales names […].[170] In an internal document, Thales comments on a report published by 451 research stating that *"[...]"*.[171]

(279) An internal power point presentation of 2017 refers to Thales as "*[...]*" and states that "*[...]*".[172] Another internal document of Gemalto of 2016 refers to Thales as its "*[...]*" in the GP HSM segment.[173] An internal Gemalto email in reaction to Thales' acquisition of Vormetric states that: "*[...]*".[174] An internal presentation of Gemalto of 2015 on HSM competition indicates that "*[...]*".[175] Gemalto further considers in an internal document analysing market requirements that "*[...]*".[176]

(280) In an internal document of 2017, discussing specifically the US market, Gemalto considers that "*[...]*".[177]

(281) Second, the Parties are close competitors also in terms of innovation competition in light of getting ready for data moving to the cloud.

---

170 [Reference to internal documents].
171 [Reference to internal documents].
172 Annex 5 Q 1 b (30) to the Form CO
173 Document entitled […].
174 [Reference to internal documents].
175 [Reference to internal documents].
176 [Reference to internal documents].
177 [Reference to internal documents].

(282) The Commission considers that traditional HSM manufacturers such as Thales, Gemalto and Utimaco, Equinix have an important role in developing cloud-agnostic and one-stop shop solutions suitable for customers who wish to share data (and therefore access to encryption keys) across on-premise and cloud environments. Such solutions allow customers the flexibility to migrate workloads and avoid vendor lock-ins (mainly with CSPs). These offerings also seem to enable traditional GP HSM manufacturers to make their HSMs more prominent and to further increase their role in the cloud and hybrid environment.

(283) Further, the Commission considers that internal documents confirm that the Parties view each other as close competitors also in terms of innovation for cloud-friendly solutions. In an internal email exchange of November 2017, Thales states that "*[…]*".[178] In an email of Thales of 2017, it is also stated: "*[…]*".[179] Another Thales email of April 2017 stresses that "*[…]*".*[180]* According to another Thales' email of 2017: "*[…]*".[181]

(284) In another internal document, Thales' executives provide comments on a press release issued in response to Gemalto's launch of a cloud-agnostic HSM aaS offering, i.e. DPoD (see recital 50). According to internal comments to a draft press release of November 2017, "*[…]*".[182]

(285) In the context of developing BYOK (Thales' cloud-agnostic offering, see recital 274), in an internal email of 2017, Thales states "*[…]*".[183] Regarding BYOK, a Gemalto internal email exchange of 2017 refers to […].[184]

(286) In an internal power point presentation, Thales also compares its cloud-friendly solutions with […], which is another cloud-agnostic HSM aaS offering of a traditional HSM manufacturer.[185]

(287) Third, the Commission considers that Thales also viewed Gemalto as its main competitor regarding cooperation and partnerships with CSPs.

(288) As indicated by the Notifying Party, CSPs purchase and integrate GP HSMs in their cloud-offerings, most notably in HSM aaS and in certain KMS aaS solutions backed by a GP HSM. Before switching to Cavium, AWS purchased GP HSMs from Gemalto, while Thales supplied Microsoft with GP HSMs to be used in its Azure cloud offering.

(289) Internal documents indicate that Thales viewed Gemalto as its main competitor regarding the supply of GP HSMs to CSPs. Thales internal email of 2017 mentions that Thales is […][186]A Thales email of January 2017 discussed that […].[187]

(290) Another Thales email of 2017 discusses possible strategies to […].*[188]*

---

178 [Reference to internal documents].
179 [Reference to internal documents].
180 [Reference to internal documents].
181 [Reference to internal documents].
182 [Reference to internal documents].
183 [Reference to internal documents].
184 [Reference to internal documents].
185 [Reference to internal documents].
186 [Reference to internal documents].
187 [Reference to internal documents].
188 [Reference to internal documents].

(iv) Thales and Gemalto are considered close competitors by third parties

(291) Thales and Gemalto were identified as close competitors with regard to GP HSMs by all respondents to the market investigation. Other market players are not considered to be equally close competitors. The next closest competitor in the GP HSM segment is considered to be Utimaco but it is not recognised as offering the same level of performance.[189] According to some customers, Thales and Gemalto are "*the only real players*"[190] on the HSM market.

(292) The closeness of competition between the Parties is also confirmed by third parties reports. "451 Research"[191] states in its analysis of the Transaction that "*the number one and two hardware security module (HSM) vendors effectively turn a duopoly into a monopoly*".[192] The analysis further explains that the market for HSMs is dominated by Thales and Gemalto, and that the merged entity will have a dominant share of the overall HSM market, without though further distinguishing between GP and Payment HSMs.

Conclusion on closeness of competition

(293) Based on the evidence set out in recitals (272)-(292), the Commission concludes that the Parties are close competitors on the EEA-wide or worldwide market for GP HSMs.

8.2.2.3. Specific assessment of the competitive constraint exerted by Thales

A. Notifying Party's views

(294) The Notifying Party submits that the Parties' are not each other's only constraint and that for any given use case or application there are a range of other competitors who offer comparable (or better) solutions that the Parties. While the Parties are both traditional vendors with similar solution designs (e.g. both offer on-premise HSM products), there are no customers for whom Thales and Gemalto pose a unique competitive constraint on one another. Further, the Parties' products have different strengths in terms of functionalities and capabilities, and are priced differently.

B. Commission's assessment

(295) The Commission considers that Thales exerts an important competitive constraint in an EEA-wide market for GP HSMs. The same analysis applies when considering a worldwide GP HSM market. This finding is based on a consistent body of evidence presented in recitals (296)-(299).

(296) First, Thales is a market leader on the market for GP HSMs, both at EEA-level and at the worldwide level. It is the second largest company in terms of revenues worldwide with EUR […] and the largest in the EEA with EUR […] for 2017. Its global reach, local presence, direct or through resellers, certifications, track record and reputation place Thales as a significant competitive constraint on the market.

(297) Second, Thales' R&D spending is another indication of the competitive constraint that the company exerts on the market. In 2017, the R&D for GP HSMs amounted to approximately EUR […]. Thales carries out its R&D activities at […].

---

189 Replies to Questionnaire Q2 – customers of 19 June 2018, question 45.

190 Replies to Questionnaire Q2 – customers of 19 June 2018, question 45.

191 451 Research is a global IT research and advisory firm.

192 "Thales rocks the infosec world with $5.7bn bid for encryption rival Gemalto", 451 Research, Garrett Bekker, 18 December 2018.

(298) Third, when asked to describe Thales' competitive strengths, customers responding to the questionnaire indicated proven track record, reputation, quality, local presence in many countries, customer base, scale, breadth of solution, innovative capabilities, customer support, performance, ability to obtain and update the required certifications.[193] All of these qualities indicate that Thales exerts a strong competitive constraint on the market.

(299) Fourth, as described in recitals (285)-(292) Gemalto states in its internal documents that Thales exerts a significant competitive constraint.

C. Conclusion on competitive constraint exerted by Thales

(300) Based on the evidence set out in recitals (270)-(299), the Commission considers that Thales exerts an important competitive constraint in an EEA-wide or a worldwide market for GP HSMs which can be qualified as an important competitive force within the meaning of recital 37 of the Horizontal Merger Guidelines.

8.2.2.4. Specific assessment of the competitive constraint exerted by Gemalto

A. Notifying Party's views

(301) As explained in recital (294), the Notifying Party submits that the Parties do not exert a significant competitive constraint on each other on the GP HSM market.

B. Commission's assessment

(302) The Commission considers that Gemalto exerts an important competitive constraint in the EEA-wide market for GP HSMs. This finding is based on a consistent body of evidence presented in recitals (303)-(306).

(303) First, Gemalto is a market leader on the market for GP HSMs, both at EEA-level and at the worldwide level. It is the largest company on the market in terms of revenues worldwide with EUR […] and the second largest in the EEA with EUR […] for 2017.

(304) Second, Gemalto's R&D spending is another indication of the competitive constraint that the company exerts on the market. In 2017, the R&D for GP HSMs amounted to approximately EUR […]. Gemalto has […] R&D employees in Canada, […] in the US, […] in India, […] in Australia, and [..] in France. They are responsible for both key management and encryption software solutions, generally with no clear allocation to either of the two areas.

(305) Third, when asked to describe Gemalto' competitive strengths, customers responding to the questionnaire indicated proven track record, local presence, customer base, quality, price, innovative capabilities, as well as good support service.[194]

(306) Fourth, as described in recitals (285)-(292), Thales considers in its internal documents that Gemalto exerts a significant competitive constraint.

C. Conclusion on competitive constraint exerted by Gemalto

(307) Based on the evidence set out in recitals (302)-(306), the Commission considers that Gemalto exerts an important competitive constraint in the EEA-wide or the worldwide market for GP HSMs which can be qualified as an important competitive force within the meaning of paragraph 37 of the Horizontal Merger Guidelines.

---

193 Replies to Questionnaire Q5 –customers of 6 September 2018, question 64; replies to Questionnaire Q2 – customers of 19 June 2018, question 46.

194 Replies to Questionnaire Q5 –customers of 6 September 2018, question 65.

8.2.3. Competitive constraints from other GP HSM manufacturers

(308) As mentioned in Section 6, the other traditional GP HSM manufacturers are Utimaco, Atos, Cavium, DocuSign, Futurex, IBM, MicroFocus, Prism, Realsec, Securosys, and Yubico.

A. Notifying Party's views

(309) The Notifying Party submits that post-Transaction the merged entity would continue to face strong competition from all the manufacturers referred to in recital (308).

B. Commission's assessment

(310) A merger is unlikely to harm competition where the reaction of the remaining competitors would discipline the behaviour of the merged entity. On the other hand, competition would be harmed if the remaining competitors may not be willing or able to compete sufficiently post-Transaction so as to compensate for the loss of competition.

(311) The Commission considers that competing GP HSM manufacturers have limited ability and incentive to compete post-Transaction so as to compensate for the loss of competition. This finding is based on a consistent body of evidence presented in recitals (312)-(327).

(312) First, the number of players present on the GP HSM market is limited. The market investigation confirmed that, apart from Thales and Gemalto, there is only a limited number of alternative GP HSM suppliers: Utimaco, Atos, Realsec IBM and Ultra Electronics (see Section 6.2).

(313) Second, the offering of the alternative suppliers present on the HSM market does not match that of Thales and Gemalto, which are clear market leaders, offering solutions with a global reach.

(314) Third, based on the market reconstruction undertaken by the Commission (see Section 8.2.1) the market shares of competitors are significantly lower than the market shares of the Parties. Additionally, in view of the projected growth on the HSM market (see recital (346)), they need to expand their offering in order to maintain their market shares.

(315) Regarding the ability of the other GP HSMs competitors to compete with the post-merger entity, the Commission notes that none of the HSM manufacturers listed in the recitals (316)-(326) below can replace the competitive constraints which Thales and Gemalto exert on each other. Notably, the remaining players on the GP HSM market have significantly smaller market shares, a more limited geographic reach in comparison with the Parties, and in some instances also inferior offerings.

(316) Utimaco is the third largest competitor following Thales and Gemalto. Utimaco's market share is limited to [0-23]% in the EEA in 2017. In an internal presentation, Thales describes Utimaco as […]. Thales further indicates that […]. Nevertheless, Utimaco's offering is considered to be geographically limited, presenting lower performance solutions and not having the sales channel and support structure of Thales and Gemalto.

(317) Atos is similarly considered to be geographically limited and does not offer customisable HSMs.[195] Thales in an internal presentation refers to Atos as "*[...]*". In

[195] Replies to Questionnaire Q2 – customers of 19 June 2018, question 43.

comparison with Atos, Thales is considered as offering "*[…]*", according to the same internal document of Gemalto.[196]

(318) Cavium is a manufacturer and supplier of GP HSMs to CSPs (such as AWS). The Commission considers that Cavium is not a credible competitor for the Parties' end customers. Serving end-customers requires the ability of the suppliers to provide maintenance and support, including in some cases also local presence and support (see recital (262)).

(319) DocuSign has only a very limited presence in GP HSMs through the acquisition of Algorithmic Research in 2015. As explained by the company itself "*DocuSign has only one HSM product, PrivateServer, which provides a network-attached, industry-certified HSM and key management hardware solution. This product was originally developed by an Israeli company called Algorithmic Research Ltd (ARX), which DocuSign acquired in 2015. DocuSign primarily acquired ARX for its other offerings […]*". Therefore Docusign does not view itself and is not a material competitor to the Parties in this area.[197]

(320) Futurex is mainly focusing on Payment HSMs and has been indicated by the vast majority of the customers as a distant competitor of the Parties in GP HSMs.[198] It is mainly active in the US with more limited presence in the EEA.

(321) IBM considers itself as a reseller rather than as a competitor in the GP HSM market. Furthermore, in view of the customers, does not provide a full range of products.[199] In internal documents, IBM is only mentioned as selling […].

(322) MicroFocus is only focusing on Payment HSMs. The company has no intention of expanding to GP HSMs as it is actually in the process of selling its HSM business (Atalla) to Utimaco.

(323) Realsec's position is even more limited, with EEA sales only in Spain and lacking some of the necessary certifications. This is […] by Thales in an internal document, describing Realsec as having […]. In the same document, Thales compares its offering with that of Realsec and concludes that "*[…]*".[200]

(324) Prism is not a GP HSM player with a global presence. In an internal power point presentation, Thales indicated that Prism […].[201]

(325) Securosys indicated by the Notifying Party as […], appears to have limited presence mainly focused on the Swiss market (and primarily working for the Swiss banks). Securosys described itself as a very small player focusing on the needs of the Swiss banking system and does not consider itself to be comparable to either Thales or Gemalto.[202]

(326) Yubico is only manufacturing a USB size HSM device. Thales internal email of 2017 refers to Yubico as "*[…]*".[203]

---

196 [Reference to internal documents].
197 See email of Docusign of 13 November 2018, ID1811.
198 Replies to Questionnaire Q5 – customers of 6 September 2018, question 63.
199 Replies to Questionnaire Q2 – customers of 19 June 2018, question 43.
200 [Reference to internal documents].
201 [Reference to internal documents].
202 [Reference to internal documents].
203 [Reference to internal documents].

(327) Fourth, existing competitors are unlikely to be able to increase their supply substantially if prices increase. Some vendors manufacture their HSMs using a combination of in-house and third-party components while others […] subcontract the manufacturing of their HSMs to third parties. The market investigation[204] has shown that the scarcity of components (e.g. servers, memory, storage etc.) and of skilled workforce negatively influences the ability of existing competitors to expand their capacity for the production of HSMs.

C. Conclusion

(328) The Commission considers that competing HSM manufacturers have limited ability and incentive to compete post-Transaction so as to compensate for the loss of competition.

8.2.4. Competitive constraint from CSPs

A. Notifying Party's views

(329) In the Article 6(1)(c) Response, the Notifying Party argues that CSPs and HSM aaS providers exert competitive pressure on traditional GP HSM providers both as direct competitors and as powerful customers.

(330) The Notifying Party estimates that the vast majority of companies will likely rely on "hybrid" environments (i.e. maintaining some data on-premise while moving other data to the cloud). In the Notifying Party's view, HSM aaS, unlike other cloud-based solutions, can be used for the vast majority of use cases as HSM aaS (i) provides same level of security as on-premise HSMs, (ii) complies with the highest certification standards and (iii) offers strong commercial and technical advantages also for customers relying on purely on-premise HSMs for some of their applications.

(331) According to the Notifying Party, virtually all use cases will gradually move to HSM aaS within the next two to five years. For some limited use cases customers will tend to keep on-premise HSMs and will likely move to HSM aaS over a slightly longer term. The Notifying Party submits that customers across a wide range of industries would be open to switching to cloud-based solutions aaS.

(332) The Notifying Party argues that all customers will benefit from the competitive constraint exerted by GP HSM aaS. Thales and Gemalto will not be able to price discriminate against customers who are less willing to switch to HSM aaS. […], the Parties have no means of consistently identifying the use case for which the customer is buying GP HSMs and whether it is willing to switch to HSM aaS for that use case.

B. Commission's assessment

(333) The Commission considers that CSPs have limited ability and incentive to compete post-Transaction so as to compensate for the loss of competition. This finding is based on a consistent body of evidence presented in recitals (334)-(355).

(i) Alleged competitive constraint currently exerted by CSPs on GP HSM manufacturers

(334) The Commission considers that today CSPs and HSM aaS vendors do not exert competitive constraints on on-premise HSM manufacturers, which could compensate the loss of competition as a result of the Transaction. Irrespective of the slow move to the cloud and its expected growth, cloud-based solutions are still in their infancy.

---

[204] Replies to Questionnaire Q1 – competitors, Question B.C.C.11 of 19 June 2018.

Customers do not consider HSM aaS, KMS aaS or other cloud-based solutions as an alternative to on-premise HSMs.

(335) First, based on the market investigation results,[205] the vast majority of the customers continue to locate their data on-premise. The vast majority of the customers use on-premise HSMs for all use cases listed by the Commission, i.e. PKI[206], customs apps[207], digital signing[208], SSL/TLS[209], Code Signing[210], Generic Key Vault[211], Cyber Ark[212], LoRa[213], Blockchain[214].

(336) Second, the market investigation confirmed that the vast majority of the customers which responded have not switched in the last two years from on-premise HSMs to HSM aaS or KMS aaS (only 1 customer indicated that they have switched to HSM aaS in the last 2 years and only 2 customers indicated that they have started using KMS aaS in the last 2 years only for limited applications).[215]

(337) Third, in view of the findings of the market investigation, as of now, the majority of the customers do not consider HSMs aaS or KMS aaS as alternatives to on-premise HSMs.

(338) A number of customers explained that HSM aaS, KMS aaS or other cloud-based solutions are not mature enough: "*[…] does not consider the HSM aaS offerings as mature enough for such critical use cases that typically involve HSMs*"[216]; "*HSM aaS offerings are not mature*"[217].

(339) Nearly half of the customers consider that HSM aaS does not provide the same level of security as on-premise HSMs. In this regard, the respondents do not refer to the parameters mentioned by the Notifying Party such as level of certification of the HSMs which back up the HSM aaS offering. Customers also do not seem to place

---

205 Replies to Questionnaire Q5 – customers of 6 September 2018, question 5.

206 Public Key Infrastructures (PKIs) include by way of example Authentication, Identity and Access Management use cases, Manufacturing (unique identities & device authenticity to prevent counterfeiting, IoT), Digital Cinema (authentication between playback devices and servers, content encryption, watermarking). PKI is used for e-commerce, online banking, internet gaming, smartphones, and cloud computing all rely on the use of digital certificates to represent the digital identity of users, connected devices, web services, and business applications.

207 Customs applications are typically used for (i) end-to-end encryption, by decrypting sensitive data coming from the Internet (e.g., PINs, passwords) inside the HSM and re-encrypting it before it is processed in the business applications run on premises or in the cloud; (ii) time stamping and other secure clock related applications; or (iii) trusted counters (e.g., counting how many products are manufactured on a given assembly line.

208 Digital signing by way of example includes signing barcodes used in electronic transactions, such as e-tickets for sporting events or airlines. Digital signatures go beyond electronic versions of traditional signatures by invoking cryptographic techniques to dramatically increase security and transparency, both of which are critical in establishing a trust and legal validity.

209 SSL and TLS is the standard for secure communications on the internet. Web traffic is becoming by default encrypted with SSL/TLS, which provides for proper authentication of Web services. The security of SSL/TLS deployments depends on the security of the associated master keys.

210 Code signing is an efficient way to provide code integrity and prevent tampering.

211 Generic Kay Vault is a tool enabling customers to quickly deploy encryption and other security solutions by centrally managing encryption keys.

212 Cyber Ark is a tool protecting sensitive data from cyber attacks.

213 LoRa is a digital wireless data communication technology permitting long-range connectivity for Internet of Things (IoT) devices in rural, remote and offshore industries.

214 Blockchain is a technology for cryptography mainly used in cryptocurrency.

215 Replies to Questionnaire Q5 – customers of 6 September 2018, questions 12 and 13.

216 Replies to Questionnaire Q5 – customers of 6 September 2018, question 12.

217 Replies to Questionnaire Q5 – customers of 6 September 2018, question 57.

the focus on whether from a technical point of view customers have exclusive access and control over keys when using HSM aaS (in view of the defined separation of duties between the customer and the CSP).

(340) Instead, customers point out that using HSM aaS provides a lower level of security as a third party is involved in their keys management which entails that customers relinquish some control over their keys.[218] Some customers stated that "*giving [the keys] to someone else automatically brings in more risk to your business*" or that "*a bit of control goes out of end user hands to provider*". Other customers consider that "*on-premise location offers a stronger protection*" and that "*it is preferable to keep your most precious keys close by, rather than trust a third party*".[219] According to another customer, "*locally supported and dedicated hardware with local physical security would provide a higher level of security*". Another customer considers that "*under HSM aaS, some controls are, by definition, operated by a third party – this reduces the level of control over the setup*". In the view of another customer, "*any use of HSM aaS means giving potentially some level of control over cryptographic keys to a non-[company] entity. It would require trusting this non-[company] third party with highly sensitive material, which is at the very core of [company's] business*". Another customer considers that "*some customers do not like the idea of [keys] being held in the cloud or shared*".[220]

(341) The market investigation results indicate that HSM aaS is not considered as an alternative to on-premise HSMs for highly sensitive data and high-security applications: "*HSM aaS can be used in some cases where the level of security requirements is low*".[221] Another customer points out that using HSM aaS "*requires a network connection, which is prohibited in many high level applications*".[222] According to another customer, "*if [the data] is too sensitive to store it or process it on the cloud, then HSM aaS is not a valid alternative*".[223]

(342) Some customers also indicate that compliance requirements cannot be fulfilled by using HSM aaS, KMS aaS or other cloud-based solutions: "*security controls [mandate] HSMs on premise*"[224], "*cloud-based solutions do not currently meet required compliance standard*"[225]; "*they are currently compliance issues with HSM aaS*"[226].

(343) Competitors and resellers also confirm that, in their view, HSM aaS and KMS aaS are not alternatives to on-premise HSMs. A competitor considers that "*in numerous circumstances, HSM aaS cannot be substituted with HSM aaS*".[227] By way of example one competitor expressed the view that the use of HSM aaS and other cloud-based solutions depends "*on the risk tolerance of the customer and potential regulatory requirements*".[228]

---

218 Replies to Questionnaire Q2 – customers of 19 June 2018, questions 12 and 12.1
219 Replies to Questionnaire Q2 – customers of 19 June 2018, question 12.1.
220 Replies to Questionnaire Q5 – customers of 6 September 2018, question 7.
221 Replies to Questionnaire Q5 – customers of 6 September 2018, question 7.
222 Replies to Questionnaire Q2 – end-customers of 19 June 2018, question 12.1.
223 Replies to Questionnaire Q5 – customers of 6 September 2018, question 7.
224 Replies to Questionnaire Q5 – customers of 6 September 2018, question 15.
225 Replies to Questionnaire Q5 – customers of 6 September 2018, question 18.
226 Replies to Questionnaire Q5 – customers of 6 September 2018, question 58.
227 Replies to Questionnaire Q4 – competitors of 10 September 2018, question 4.
228 Replies to Questionnaire Q4 – competitors of 10 September 2018, question 4.

(344) Internal documents of the Parties also confirm that the Parties recognise that customers do not consider cloud-based solutions as alternative to on-premise HSMs. An email of 2017 of Thales explains that "*[…]*".[229]

(ii) Alleged competitive constraint expected to be exerted by CSPs on GP HSM manufacturers in the near future

(345) The Commission considers that demand for on-premise HSMs will remain in the foreseeable future as regards protection of sensitive data and critical applications. While a number of new applications have slowly started moving towards the cloud, this move concerns mostly non-sensitive, low risk data. Demand for on-premise HSMs will remain both due to legacy issues as well as due to reasons of trust and the need to ensure maximum security for the keys and the encrypted data.

(346) First, the Commission considers that the market for GP HSMs will grow by approximately 10% year-on-year in the coming years. The reasons behind the market growth are the new regulatory frameworks on data protection and data security such as the GDPR and the eIDAS Regulation, as well as the ever increasing risks of cyber-attacks. This is also confirmed by the market investigation[230] as well as by independent third-party reports and the Parties' websites[231].

(347) Second, even if customers will move some workloads to the cloud and/or rely on a "hybrid environment", the Commission considers that on-premise HSMs will remain a necessary component for key management in the next two to five years.

(348) According to the market investigation findings, the ratio of data stored on-premise, and in the public and/or private clouds will change and some workloads will be moved away from on-premise data centres.[232] Only 2 customers consider that all the current IT workloads will remain on-premise in the next five years. The majority of the respondents indicate that at least some of the data/workloads will move to public, private or hybrid clouds (the actual percentages vary drastically from 95% moving to the public, private or hybrid cloud to more moderate estimations in the area of 5-10% of IT workloads moving to the cloud).

(349) The market investigation results indicate that the majority of the customers consider that GP HSMs will remain a necessary component for data protection in the next two to five years.[233] The majority of the customers expect to maintain HSMs on-premise irrespective of the location of workloads.

(350) The vast majority of customers replied that it is highly likely they will start using on-premise HSMs in the next 5 years for most use cases listed by the Commission such as PKI, custom apps, digital signing, SSL/TLS and code signing.

(351) However, the vast majority of customers replied that it is highly unlikely they will start using HSM aaS in the next 5 years for all listed use cases. The vast majority of customers replied that it is highly unlikely they will start using KMS aaS in the next

229 [Reference to internal documents].

230 Replies to Questionnaire Q1 – competitors, question B.C.A.12 of 19 June 2018; replies to Questionnaire 2 – customers, question 39; replies to Questionnaire Q3 – resellers of 21 June 2018, question 43 where the majority of respondents indicate that the HSM market will increase in the next 2-5 years.

231 For instance, https://www.thalesesecurity.com/resources/research-reports-and-white-papers/impact-european-eidas-regulation.

232 Replies to Questionnaire Q5 – customers of 6 September 2018, question 5.1.

233 Replies to Questionnaire Q5 – customers of 6 September 2018, question 58.

5 years for all listed use cases. A number of customers replied that this concerns both legacy and new applications and use cases.

(352) Third, in the course of the market investigation, a number of customers stated that generally HSM aaS, KMS aaS and other cloud-based solutions are relatively new options and that they are at very early stages of analysing and evaluating the possibility to use HSM aaS, KMS aaS or other cloud-based solutions in view of their company's needs. According to some customers, the use of HSM aaS or KMS aaS is "*subject to further study*".[234] Other customers replied that "*[they have] never seriously considered using HSM aaS because HSM aaS was – and still is – a relatively new option*"[235] or that "*[they] have not made any decisions on the potential use of HSM aaS yet*"[236]. Another customer stated that "[they are] *in the early stages of evaluating and exploring options but cannot comment at this point in time*".[237] Another customer explained that "*this option is under investigation but no real progress has been made yet, ie no plans underway*".[238] According to another customer, "*[they do] not have an agreed position on the topic*".[239]

(353) Fourth, some customers expressed the view that that for some workloads (which are cloud-hosted or involve low risk data) they may consider using HSM aaS, KMS aaS or other cloud-based solutions. Some customers indicate that the move to cloud-based solutions will most likely affect new applications as legacy applications remain tied to the existing on-premise HSM-based infrastructure.

(354) Fifth, the findings of the market investigation, namely that demand for on-premise HSMs will remain, […]. In a Thales presentation of 2017 it is mentioned that "*[…]*".[240]

(iii) Price discrimination

(355) With regard to the Notifying Party's argument that the merged entity will not be able to price discriminate against customers who are less willing to switch to HSM aaS (see recital (332)), the Commission considers that when selecting GP HSM suppliers and offerings customers take into account a myriad of factors, price being only one of them (see recital (262)). Therefore, the alleged price benefit to customers which in the view of the Notifying Party results from the constraint that CSPs exert on on-premise GP HSMs only addresses one aspect of competition. The Commission considers that it cannot compensate for the removal of the important competitive constraints which the Parties exerted on each other pre-Transaction.

C. Conclusion

(356) The Commission considers that CSPs have limited ability and incentive to compete post-Transaction so as to compensate for the loss of competition.

---

234 Replies to Questionnaire Q5 – customers of 6 September 2018, question 6.
235 Replies to Questionnaire Q5 – customers of 6 September 2018, question 7.1.
236 Replies to Questionnaire Q5 – customers of 6 September 2018, question 6.
237 Replies to Questionnaire Q5 – customers of 6 September 2018, question 6.
238 Replies to Questionnaire Q5 – customers of 6 September 2018, question 6.
239 Replies to Questionnaire Q5 – customers of 6 September 2018, question 6.
240 [Reference to internal documents].

8.2.5. Conclusion on non-coordinated horizontal effects on the EEA-wide and worldwide market for GP HSMs

(357) The Commission therefore considers that the Transaction would give rise to a significant impediment of effective competition in relation to the EEA-wide market for GP HSMs.

(358) As explained in Section 7, the market for GP HSMs is at least EEA-wide, if not global. The competitive assessment at a worldwide level would be the same as for the EEA-wide level given the Parties' market shares, as well as the fact that the same competitive conditions would apply at worldwide level. Thales and Gemalto are the two largest GP HSM players [241] exerting significant competitive constraints on each other with closely competing products, whereas the remaining GP HSMs players have significantly lower shares. In view of this, the Commission considers that the Transaction would also give rise to a significant impediment of effective competition in relation to the worldwide market for GP HSMs.

8.2.6. Countervailing factors

(359) In this Section the Commission assesses whether the anticompetitive effects of the Transaction ascertained in Sections 8.3 and 8.4 are likely to be offset by entry, countervailing buyer power or efficiencies.

8.2.6.1. Entry

(360) According to the Horizontal Merger Guidelines, when entering a market is sufficiently easy, a merger is unlikely to pose any significant anti-competitive risk. Therefore, entry analysis constitutes an important element of the overall competitive assessment. For entry to be considered a sufficient competitive constraint on the merging parties, it must be shown to be likely, timely and sufficient to deter or defeat any potential anti-competitive effects of the merger.[242]

A. Notifying Party's views

(361) The Notifying Party considers that as demonstrated by the substantial entry in recent years, entry in key management is relatively easy with limited barriers to entry.[243]

(362) In the Notifying Party's view, a new competitor can effectively enter with a single product across a wide range of industries and applications.

(363) Furthermore, the Notifying Party submits that new market entrants are not required to invest heavily in manufacturing facilities. Even for solutions that are based on hardware components, entrants have access to a number of original equipment manufacturers ("OEMs") who can supply components and even finished products for a limited investment. As regards HSMs, Thales […].

(364) According to the Notifying Party, a local sales presence may be beneficial but is not essential. Vendors do not have sales representatives in all countries. Most of them have a centralised sales structure and operate from one or a few sales hubs worldwide. Similarly, the Notifying Party considers that vendors do not need to have local sales presence in the EEA to supply key management products across the EEA.

(365) The Notifying Party indicates that partnerships with distributors are easy to develop, even for small and recent entrants, which can rapidly develop a worldwide network.

---

241 [30-40]% and [40-50]% respectively for 2017.

242 Horizontal Merger Guidelines, para 68.

243 Form CO, Sections 6-7, Chapter II, paras 221-224.

Furthermore, distributors generally do not enter into exclusive agreements with vendors but resell KMS from several vendors.

(366) The Notifying Party further submits that research and development costs are not prohibitive. The Parties estimate that a new entrant would need to incur about EUR 5-10 million to develop a key management solution based on Intel SGX microprocessors (as Fortanix did), and about EUR 10-20 million to develop from scratch the technology required to supply GP HSMs. Even if costs vary from one key management solution to another, a GP HSM vendor can start supplying Payment HSMs relatively easily, with investments of minimum EUR 3-5 million (including about EUR […] for certification costs).

(367) According to the Notifying Party, new entrants do not need to obtain access to patents or other intellectual property rights. A number of key management components are off-the-shelf hardware products. KMS comply with common standards, while most patents are focused on features offering specific capabilities, developed by vendors to differentiate offerings.

(368) In the Notifying Party's view, there are generally no legal or regulatory barriers to entry (except in China and Russia).

(369) The Notifying Party submits that although customers do take into account vendors' reputation and track record, the number of successful recent entries in enterprise key management (including in HSMs) show that reputation and track record do not constitute barriers to access customers.

(370) In the Article 6(1)(c) Response, the Notifying Party submitted that (i) there are recent examples of market entry (Cavium, Securosys, Yubico, Envieta) that demonstrate that entry is possible and common, (ii) new entrants can source components from third parties and work with them to manufacture and develop HSMs.[244]

B. Commission's assessment

(371) For the reasons set out in recitals (371)-(376), the Commission considers that the threat of entry would not be a sufficient competitive constraint on the merged entity to reduce the risk of anti-competitive effects arising from the Transaction.

(372) First, R&D expenditure and investments to develop GP HSM solutions are significant, as shown by the Parties' own estimates of EUR 5 million – EUR 20 million required to develop a key management solution.[245] Along these lines, a competitor submits that it is essential to maintain a constant R&D investment around GP HSM and KMS topics. The state of the art in terms of algorithmic developments (Quantum safe cryptography, homomorphic cryptography, multi-party cryptography, Attribute based encryption), in terms of possible attacks (fault attack, Differential Power analysis, fuzzing etc.), in terms of functionality and performance as well as the need to obtain updated certifications require a technological watch and a recurring investment in R&D.[246] Market investigation results indicate that entering the HSM market, even from neighbouring markets, requires significant investment and time.[247]

---

244 Article 6(1)(c) Response, paras 187-190.
245 Form CO, Sections 6-7, Chapter II, para 221.
246 Replies to Questionnaire Q1 – competitors of 19 June 2018, question A.5.
247 Replies to Questionnaire Q1 – competitors of 19 June 2018, question B.C.C.1.

(373) Second, the need for certification of HSMs under the relevant security standards, which is necessary to enhance the cyber-security conditions for end customers, whether required by regulation or not, is likely to represent a significant barrier to entry both in terms of cost and time. For example, the Parties submit that the time needed for a provider of enterprise KMS to have a product PCI-certified is about […]. There is a myriad of security standards that GP HSM providers are requested to comply with, which are in constant evolution. Therefore, timely compliance with the relevant standard and being up to date increases the costs to enter in the GP HSM market.[248] Consequently, the need for certification was identified by the respondents of the market investigation as one of the barriers to entry.

(374) Third, customers point at track record and reputation as an important factor to choose a GP HSM provider. A potential entrant would therefore face a comparatively worse track record and reputation compared to the Parties. Such difference would increase post-Transaction after the combination of the Parties' track record and reputation. Most customers mention that security reputation is an important factor they consider when assessing alternative suppliers.[249] Indeed, trust and references are essential and existing installed base from a provider can be a decisive criterion.[250]

(375) Competitors also indicate that a potential entrant would have to face key "stickiness" as moving keys from one GP HSM provider to other GP HSM provider is not easy and customers typically select their existing GP HSM supplier when expanding their application.[251]

(376) Fourth, the Commission considers that the entrants mentioned by the Notifying Party cannot credibly replace the competitive constraint exerted by Gemalto, for the reasons set out in recitals (377)-(380).

(377) As indicated at recital (318), Cavium supplies GP HSMs to CSPs such as AWS and is not considered as a credible competitor for the Parties' end customers.

(378) Yubico targets a different price point and lacks security certification (currently offers a USB GP HSM without FIPS certification).[252] Therefore, the Parties' do not consider Yubico […]."[253][…].[254]

(379) Securosys, a new entrant whose operations are limited to Switzerland, stated that it is not considering expansion to countries where Thales and Gemalto are already established, as it does not have comparable resources for marketing. Securosys also confirmed that the lack of local presence and 24/7 support, and lock-in acted as barriers to entry.[255] Furthermore, the Commission considers that Securosys became successful in Switzerland against Thales and Gemalto due to the fact that it is manufactured in Switzerland (where it won a contract with the Swiss banking

---

248 E.g. see Non-confidential minutes of telephone conference with Oracle of 15 May 2018; replies to Questionnaire Q1 – competitors of 19 June 2018, question B.A.17.

249 Replies to Questionnaire Q2 – customers of 19 June 2018, questions 31 and 32.

250 Idemia's non-confidential submission entitled "Case M.8797 - Thales / Gemalto - competition concerns for IDEMIA", dated 3 July 2018.

251 Replies to Questionnaire Q1 – competitors of 19 June 2018, question B.C.A.5

252 Notifying Party's reply to RFI 5, Annex RFI 5 Q1.b(32) (451 Research report on Yubico): "[…]"

253 [Reference to internal documents].

254 [Reference to internal documents].

255 Non-confidential minutes of telephone conference with Securosys of 6 September 2018.

system). In a possible expansion in other European countries, Securosys would not have this advantage. […][256]. […].

(380) Envieta, […], cannot be understood to replace the competitive constraint exerted by Gemalto because it lacks the resources, customer support, experience and reputation of the Parties. According to Envieta's data sheet, its GP HSM solution appears to lack FIPS or other security certifications.[257] Furthermore, the customers, competitors and resellers who responded to the in-depth market investigation consider Envieta a distant competitor of the Parties.[258] Finally, Envieta […], which could undermine Envieta's incentive to become a credible competitor to the Parties. [259]

C. Conclusion on entry

The Commission therefore takes the view that barriers to entry are high and that no entry of sufficient scope is likely to take place in time to counter the anticompetitive non-coordinated effects of the Transaction on the EEA-wide or worldwide market for GP HSMs.

8.2.6.2. Buyer power

(381) According to the Horizontal Merger Guidelines, the competitive pressure on a supplier is not only exercised by competitors but can also come from its customers. Even firms with very high market shares may not be in a position, post-merger, to significantly impede effective competition, in particular by acting to an appreciable extent independently of their customers, if the latter possess countervailing buyer power. Countervailing buyer power in that context should be understood as the bargaining strength that the buyer has vis-à-vis the seller in commercial negotiations due to its size, its commercial significance to the seller and its ability.[260]

A. Notifying Party's views

(382) The Notifying Party considers that customers exert significant constraints on key management suppliers and would be able to disrupt any hypothetical unilateral effects stemming from the Transaction, including by sponsoring new entrants and turning to more cost-efficient and innovative technologies. The Notifying Party refers to the following examples: Cavium entered the market for GP HSMs in 2001, according to the Notifying Party, sponsored by AWS, Goldman Sachs and Citigroup. Unbound's sponsors also include Goldman Sachs and Citigroup. While it will typically be the larger customers with significant resources who will be able to sponsor entry, smaller customers too will benefit from such new competing solutions in the Notifying Party's view.[261]

(383) The Notifying Party argues that customers design their data security strategy and select those products that best covers their data security needs. In other words, they do not select a specific vendor or the ability of a single vendor to provide one comprehensive key management solution. Most customers mix and match KMS, including GP HSMs.

---

256 [Reference to internal documents].
257 Article 6(1)(c) Response, footnote 396.
258 Replies to questionnaires Q4 to competitors, questions 59 and 60, Q5 to customers, questions 62 and 63, and Q6 to resellers, questions 60 and 61.
259 [Reference to internal documents].
260 Horizontal Merger Guidelines, para 64.
261 Form CO, Sections 6-7, Chapter II, para 231.

(384) In Article 6(1)(c) Response, the Notifying Party submitted that (i) large customers constitute the vast majority of the Parties' sales (top 10 customers are […]% of Thales' EEA GP HSM sales and […]% of Gemalto's), […], (ii) these large customers can credibly threaten to resort to alternative suppliers or integrate into the upstream market of GP HSMs, (iii) large customers can sponsor entry.[262]

B. Commission's assessment

(385) The Commission takes the view that buyer power in the GP HSM market is limited for the reasons set out in recitals (385)-(394).

(386) First, customers can only exercise buyer power to the extent that there are available alternative suppliers of GP HSMs on the market. Post-Transaction, the two leading suppliers of GP HSMs will become one, which will significantly reduce customers' choice of supplier.

(387) Second, customer switching is extremely difficult, at least for a given application. Changing the provider of KMS in general and of GP HSMs in particular is difficult, given that migrating the keys, on which the full functioning of the application relies is extremely challenging as it entails compatibility issues and a significant period of testing in order to ensure the correct functioning of the new application.

(388) The results of the in-depth market investigation confirm that switching in the GP HSM market is limited.

(389) The majority of customers who gave a meaningful answer to the in-depth market investigation indicated that switching is not common. A number of respondents submitted that switching suppliers and systems occurs only in some cases. Costs, time, training, integration, etc. were mentioned as factors that make switching GP HSM provider challenging.[263] The majority of resellers that gave a meaningful response also submitted that switching is not common.[264]

(390) As customers confirm that switching is difficult, this means that buyer power is reduced. Customers explain that the GP HSM market is constantly growing. However, demand side switching is difficult. Indeed, once a GP HSM had been supplied to a customer, the cost to that customer of switching supplier for that application in terms of exposure to security breaches, as well as changing protocol is high. Also, the vendor switching cost is high, as the entire module needs to be replaced. As a result of this, the buyer's bargaining power is limited.[265]

(391) Third, the Parties' customer base is extremely fragmented and each customer typically represents a small share of the Parties' revenues. If the whole enterprise key management area is considered, the Notifying Party reports that in 2017 it had sales to […] customers (of which […] were value-added resellers, system integrators and distributors), while Gemalto sold to […] customers (of which […] were resellers). Of these customers, Thales' top 10 end-customers accounted for […]% of its total enterprise key management sales. For Gemalto, the top 10 end customers accounted for […]% of its enterprise key management sales. The Notifying Party submits that most GP HSMs contracts have a relatively low value, about approximately EUR […] on average.

---

262 Article 6(1)(c) Response, paras 179-186.

263 Replies to Questionnaire Q2 – customers of 19 June 2018, question 37.

264 Replies to Questionnaire Q3 – resellers of 21 June 2018, question 41.

265 Idemia's non-confidential submission entitled" Case M.8797 - Thales / Gemalto - competition concerns for IDEMIA", dated 3 July 2018.

(392) The in-depth market investigation confirmed that switching is extremely difficult for customers, at least for existing applications. Competitors have also confirmed that, despite the existence of some large customers, the customer base is very fragmented. Indeed, the Parties' extended data on their customer base show only a few customers having more than […]% of each Party's total revenues from HSMs. For example, only […] of Thales' customers of or GP HSMs represent individually over […]% of revenues in that category. On the other hand, there is a long tail of customers each representing less than […]% of revenues. […] to Gemalto's GP HSM customer base.[266]

(393) The Commission considers that these figures reflect a very fragmented customer base, which is on average very unlikely to exert countervailing buyer power on the Parties. In the Commission's view, even if there were to be some countervailing buyer power by some large customers, most of them would remain unprotected given the extremely limited size of its individual purchases from the Parties.

(394) A further aggravating factor that points at no or very low bargaining power by customers is that the low value of most contracts is likely to represent a small fraction of a customer's overall turnover and IT spending, which would further reduce the incentive of customers to exert countervailing buyer power.

C. Conclusion on buyer power

(395) Based on the above, the Commission takes the view that post-Transaction, the merged entity will not face sufficient competitive constraints from customers to counter the anticompetitive non-coordinated effects of the Transaction on the EEA-wide or worldwide market for GP HSMs.

8.2.6.3. Efficiencies

(396) The Notifying Party submits that the Transaction provides substantial scope for pro-competitive efficiencies.[267]

(397) In assessing any claims regarding efficiencies, the Commission applies the Horizontal Merger Guidelines which establish a cumulative set of requirements to take efficiencies into consideration.[268]

(398) First, the "relevant benchmark" in the assessment of efficiency claims is that consumers should be no worse off as a result of the merger. For that purpose, efficiencies have to be substantial and timely, and should, in principle, benefit consumers in those relevant markets where it is otherwise likely that competition concerns would occur.[269]

(399) In general, efficiencies that lead to reductions in variable or marginal costs are more likely to be relevant for the assessment of efficiencies than reductions in fixed costs as they are more likely to result in lower prices for consumers. Cost reductions, which merely result from anti-competitive reductions in output, cannot be considered as efficiencies benefiting consumers.[270]

(400) Any efficiency should be passed on to consumers. The scope for pass-on is often related to the existence of competitive pressure from the remaining firms in the

---

266 Thales' top 200 clients and Gemalto's to 200 clients, see Thales' response to RFI 13 of 30 August 2018.
267 Form CO, Section 9.
268 Horizontal Merger Guidelines, para 78.
269 Horizontal Merger Guidelines, para 79.
270 Horizontal Merger Guidelines, para 80.

market and from potential entry. The greater the possible negative effects on competition, the more the Commission has to be sure that the claimed efficiencies are substantial, likely to be realised, and to be passed on, to a sufficient degree, to the consumer.[271]

(401) Second, efficiencies should be merger specific and it should not be possible for them to be achieved to a similar extent by less anticompetitive alternatives.[272]

(402) Finally, the efficiencies should be verifiable so that the Commission can be reasonably certain that the efficiencies are likely to materialize, and be substantial enough to counteract a merger's potential harm to consumers.[273]

(403) It is incumbent upon the Notifying Parties to provide the Commission in due time with all the relevant information necessary to demonstrate that any claimed efficiencies are merger-specific and likely to be realised and that the efficiencies are likely to counteract any adverse effects on competition that might otherwise result from the merger, and that the claimed efficiencies therefore benefit consumers.[274] However, the Notifying Party did not provide any relevant information in regard to the possible efficiencies brought about by the merger.

8.2.7. Coordinated horizontal effects on the EEA-wide market for GP HSMs

(404) A merger in a concentrated market may significantly impede effective competition due to horizontal coordinated effects if, through the creation or strengthening of a collective dominant position, it increases the likelihood that firms are able to coordinate their behaviour in this way and raise prices, even without entering into an agreement or resorting to a concerted practice within the meaning of Article 101 TFEU.[275] A merger may also make coordination easier, more stable or more effective for firms that were already coordinating before the merger, either by making the coordination more robust or by permitting firms to coordinate on even higher prices.[276]

8.2.7.1. Notifying Party's views

(405) The Notifying Party submits that the Transaction is unlikely to increase the risk of coordinated conduct.[277] It considers that in a rather fragment, non-transparent, and innovative market with several competitors, there is no risk of tacit collusion.[278] It submits that the number of competitors makes tacit coordination unlikely and also that it would be difficult to monitor deviations from coordination or to establish credible deterrent mechanisms in this non-transparent market. In addition, outsiders and other KMS, including HSM aaS, would jeopardise any possible coordination.[279]

8.2.7.2. Commission's assessment

(406) Based on the results of the market investigation, the Commission does not consider that the change brought about by the Transaction is likely to make coordination more likely in the industry.

---

271 Horizontal Merger Guidelines, para 84.
272 Horizontal Merger Guidelines, para 85.
273 Horizontal Merger Guidelines, para 86.
274 Horizontal Merger Guidelines, para 87.
275 Horizontal Merger Guidelines, para 39.
276 Horizontal Merger Guidelines, para 39.
277 Form CO, para 225.
278 Form CO, para 284.
279 Form CO, para 284.

(407) First, the affected market presents characteristics which make coordination difficult. In the market for GP HSMs demand is highly fragmented. There is limited transparency on the market as these markets are characterised by infrequent, one-off orders rarely awarded through a bidding process. Rather, transactions are confidentially negotiated between buyers and sellers with prices and conditions agreed individually. The Transaction does not diminish these market characteristics which make coordination difficult.

(408) Second, the Transaction does not significantly increase symmetry in the market. Based on the market share figures presented in Table 4, the market will remain relatively asymmetrical post-Transaction.

(409) Third, the market investigation did not indicate that either of the Parties is viewed as a maverick player, the removal of which as a competitive player would increase the likelihood or significance of coordinated effects in other ways.

(410) The Commission therefore considers that the Transaction would not give rise to significant coordinated horizontal effects on the EEA-wide or worldwide market for GP HSMs.

8.3. Payment HSMs

8.3.1. Market shares and concentration levels

8.3.1.1. Market shares for Payment HSMs as provided by the Notifying Party

(411) Based on the data provided by the Notifying Party, the market shares of the Parties and their largest competitors in the market for Payment HSMs are provided in Tables 6-8.

Table 6: Worldwide and EEA-wide market for Payment HSMs (2017)

Company	Worldwide		EEA	
	Shares (%)	Revenues (MEUR)	Shares (%)	Revenues (MEUR)
Thales	[20-30]%	[…]	[10-20]%	[…]
Gemalto	[5-10]%	[…]	[0-5]%	[…]
Combined	***[30-40]%***	***[…]***	***[20-30]%***	***[…]***
Atos	[20-30]%	[…]	[40-50]%	[…]
Micro Focus	[5-10]%	[…]	[0-5]%	[…]
DocuSign	[5-10]%	[…]	[0-5]%	[…]
Others	[20-30]%	[…]	[30-40]%	[…]

Source: Form CO

Table 7: Worldwide and EEA-wide market for Payment HSMs (2016)

Company	Worldwide		EEA	
	Shares (%)	Revenues (MEUR)	Shares (%)	Revenues (MEUR)
Thales	[30-40]%	[…]	[20-30]%	[…]
Gemalto	[5-10]%	[…]	[0-5]%	[…]
Combined	***[30-40]%***	***[…]***	***[20-30]%***	***[…]***
Atos	[20-30]%	[…]	[40-50]%	[…]
Micro Focus	[5-10]%	[…]	[0-5]%	[…]
DocuSign	[5-10]%	[…]	[0-5]%	[…]
Others	[20-30]%	[…]	[20-30]%	[…]

Source: Form CO

Table 8: Worldwide and EEA-wide market for Payment HSMs (2015)

Company	Worldwide		EEA	
	Shares (%)	Revenues (MEUR)	Shares (%)	Revenues (MEUR)
Thales	[40-50]%	[…]	[30-40]%	[…]
Gemalto	[5-10]%	[…]	[0-5]%	[…]
Combined	***[40-50]%***	***[…]***	***[30-40]%***	***[…]***
Atos	[10-20]%	[…]	[30-40]%	[…]
Micro Focus	[5-10]%	[…]	[0-5]%	[…]
DocuSign	[5-10]%	[…]	[0-5]%	[…]
Others	[20-30]%	[…]	[20-30]%	[…]

Source: Form CO

(412) When considering the market segment for Payment HSMs, Table 6 shows that post-Transaction, the combined market share of the Parties in 2017 was [30-40]% and [20-30]% on the worldwide and the EEA-wide market, respectively.

(413) The next largest competitor is indicated to be Atos with [20-30]% and [40-50]% at worldwide and EEA level, respectively. In particular for the market segment for

Payment HSMs, there are strong indications that the market share of Atos might be in reality significantly lower than the one provided by the Notifying Party.[280]

(414) Tables 7 and 8 show that the combined market shares of Thales and Gemalto in 2016 amounted to [30-40]% and [20-30]% at worldwide and EEA level respectively, whereas in 2015 it amounted to [40-50]% and [30-40]% at worldwide and EEA level respectively. The […] trend over the period 2015-2017 appears mainly due to the […] revenues of Atos, according to the Notifying Party.

(415) The post-transaction HHI on the market for Payment HSMs is […] on the worldwide and […] on the EEA-wide market for 2017. The delta brought by the Transaction is […] on the worldwide and […] on the EEA-wide market. According to the Horizontal Merger Guidelines, both the post-merger HHI and the delta of the Transaction are likely to raise competition concerns.

8.3.1.2. Market shares for Payment HSMs based on the Commission's market reconstruction

(416) For reasons outlined in Section 8.2.1.5 the Commission has undertaken a market reconstruction for GP as well as Payment HSMs, an exercise described in Section 8.2.1.6.

(417) The market shares for Payment HSMs obtained thanks to the Commission's market reconstruction are presented in Table 9.

Table 9: Evolution of Payment HSMs market shares and market size based on the Commission's market reconstruction

		Market shares		**Market size (mEUR)**	
		WW	**EEA**	**WW**	**EEA**
Jan-Aug 2018	**Thales**	[50-60]%	[40-50]%	**[…]**	**[…]**
	Gemalto	[10-20]%	[10-20]%		
	Combined	**[60-70]%**	**[50-60]%**		
2017	**Thales**	[50-60]%	[50-60]%	**[…]**	**[…]**
	Gemalto	[10-20]%	[5-10]%		
	Combined	**[60-70]%**	**[50-60]%**		
2016	**Thales**	[50-60]%	[40-50]%	**[…]**	**[…]**
	Gemalto	[10-20]%	[5-10]%		

[280] The Notifying Party provided an estimate of […] worldwide revenues in Payment HSMs of EUR […] million in 2017 whereas, in reality those revenues are EUR [0 – 20] million.

	Combined	**[60-70]%**	**[50-60]%**		
2015	**Thales**	[60-70]%	[60-70]%	**[…]**	**[…]**
	Gemalto	[5-10]%	[5-10]%		
	Combined	**[70-80]%**	**[60-70]%**		

(418) In a similar way to the market reconstruction on GP HSMs, the market reconstruction on Payment HSMs shows the Notifying Party's market shares underestimate the position of the Parties (see Table 6, Table 7 and Table 8).

(419) In a stagnating (worldwide) or slightly declining market (EEA-wide), the Parties combined shares have […] between 2015 and Jan-Aug 2018, from [60-70]% to [50-60]% in the EEA and from [70-80]% to [60-70]% worldwide. This decline can be attributed to Thales, which has gone from a [60-70]% market share in 2015 to a [40-50]% market share in Jan-Aug 2018, in the EEA.

(420) Revenues of Gemalto in the EEA […] from 2015 to 2017 in the EEA at around EUR […]. However, due to the decline in the overall market size, their […], from [5-10]% in 2015 to [10-20]% in Jan-Aug 2018. Worldwide, Gemalto's sales have […], as has its market share, from [5-10]% in 2015 to [10-20]% for the January-August 2018 period.

(421) Competitors of the Parties in Payment HSMs have different strength depending on the geography. As shown in Table 10, Atos is a much stronger player in the EEA than worldwide, while MicroFocus is stronger worldwide than in the EEA.

Table 10: Payment HSMs market shares of the Parties and competitors, for 2017, based on the Commission's market reconstruction

2017	**Payment HSMs**	
	WW	**EEA**
Thales	[50-60]%	[40-50]%
Gemalto	[10-20]%	[5-10]%
Combined	[60-70]%	[50-60]%
Atos	[0-9]%	[0-34]%
MicroFocus	[0-15]%	[0-8]%
Utimaco	[0-6]%	[0-5]%
Others	[0-10]%	[0-10]%

8.3.1.3. Conclusion on market shares and concentration levels

(422) On the basis of the Commission's market reconstruction, post-transaction HHI on the market for Payment HSMs is […] on the worldwide and […] on the EEA-wide market for 2017. The delta brought by the Transaction is […] on the worldwide and […] on the EEA-wide market. These HHI and delta brought by the Transaction exceed those computed on the market shares provided by the Notifying Party (see recital (415)). According to the Horizontal Merger Guidelines, both the post-merger HHI and the delta of the Transaction are likely to raise competition concerns.

(423) Following the results of the market investigation, the competitive assessment is carried out at the narrower, EEA level, which is followed by an assessment at worldwide level.

8.3.2. Non-coordinated horizontal effects on the EEA-wide market for Payment HSMs

(424) In this Section, the Commission assesses the likelihood of anticompetitive horizontal non-coordinated effects in the EEA-wide market for Payment HSMs. To this aim, Section 8.3.2.1 presents the competitive conditions of the market pre-Transaction. Section 8.3.2.2 assesses the competitive constraints exerted by the Parties on each other and on their competitors. Section 8.3.2.3 assesses the other competitive constraints which will remain post-Transaction, and the likelihood that they off-set any potential anticompetitive effects of the Transaction. Sections 8.3.2.4 and 8.3.2.5 draw conclusions.

8.3.2.1. Competitive conditions pre-Transaction

(425) The parties' market shares in Payment HSMs both at EEA and worldwide level indicate that Thales is the main player in this market whereas Gemalto holds a significantly lower market share and has generated […] revenues in the EEA (around EUR […] including support and maintenance), which have […] in the last three years.

8.3.2.2. Competitive constraints exerted by the Parties

A. Closeness of competition between Thales and Gemalto

Notifying Party's views

(426) The Notifying Party submits that the Parties are far from being close competitors. Other players such as Atos, Micro Focus/Atalla, and Futurex are far closer to Thales in size and product line-up than is Gemalto. A detailed analysis of the Parties' overlapping customers demonstrate that the majority of Thales' and Gemalto's customers do not source Payment HSMs from both Parties and to the extent customers do source Payment HSMs from both Parties, they typically concentrate most of their purchases on one of the two vendors, suggesting that customers use the Parties' HSMs for different use cases.

Commission's assessment

(427) The Commission considers that Thales and Gemalto are not close competitors in the market for Payment HSMs in an EEA-wide geographical market on the basis of the body of evidence presented in recitals (428)-(449).

(i) Gemalto is a small player in the market for Payment HSMs

(428) Gemalto has traditionally been a small player in Payment HSMs in the EEA as well as worldwide. As the market share figures show, Gemato holds [5-10]% in the EEA whereas at worldwide level Gemalto has a market share of [10-20]%.

(429) Gemalto's total Payment HSM hardware revenues in the EEA are […] and have […] in the last five years.

Year	Revenue (million EUR)
2013	[…] [281]
2014	[…]
2015	[…]
2016	[…]
2017	[…]

Source: Gemalto

(430) Gemalto's sales of Payment HSMs to new customers have consistently been below EUR […]. This amounted to sales of between […] 40 new Payment HSMs sold EEA-wide per year. In the last 2 years, for example, Gemalto's HSM hardware sales to new customers were:

Year	Gemalto's Sales to New Payment HSM Customers
2016	EUR […]
2017	EUR […]

Source: Gemalto

(431) It has not been established that, absent the Transaction, Gemalto would be in a position in the foreseeable future to increase its market share in Payment HSMs. Gemalto has not been able to leverage its position in GP HSMs to achieve higher sales of Payment HSMs. Although SafeNet entered the Payment HSM business when it acquired Eracom Technologies in 2005, it was never able to leverage its position in GP HSMs to improve its sales of Payment HSMs. This is mainly due to the fact that GP and Payment HSM customers do not typically buy these products together.[282]

(ii) The Parties do not view each other as close competitors

Thales' internal documents

(432) Thales does not view Gemalto as one of its key or primary competitors in Payment HSMs. To the extent Gemalto is mentioned at all as a Payment HSM competitor in Thales' internal documents, they tend to describe Gemalto as a marginal or struggling competitor in Payment HSMs.

(433) A 2015 Thales "[…]" notes that Gemalto's "*[...]*"[283]

---

281 This figure is for Gemalto's Payment HSM sales in EMEA, as data for the EEA is not available. Gemalto estimates that the EEA accounts for around […]% of the EMEA sales.

282 [Reference to internal documents].

283 [Reference to internal documents].

(434) A 2015 Thales "[…]" further compares […] and notes that […]."[284]

(435) A 2016 Thales "[…]" notes: "*[…]*".[285]

(436) The 2016 Thales "[…]" notes: "*[…]*. ".[286]

(437) The 2017 Thales "[…]" similarly notes that "*[…]*."[287]

(438) Another Thales email states "*[…]*".[288]

Gemalto's internal documents

(439) Gemalto's internal documents confirm that it views itself as […] Payment HSM players in the Union and suggest that it […].

(440) Gemalto's internal documents show […]. Indeed, several other internal Gemalto documents from 2017 suggest it competes most closely with […].[289]

(441) A 2013 "[…]"[290].

(442) A 2013 Gemalto internal email states […].[291]

(443) A 2016 Gemalto slide deck "*[…]*." [292]

(ii) Gemalto does not view its product as unique

(444) Gemalto does not offer any material unique features in payment HSMs that are not also offered by other competitors.

(445) Some Gemalto documents contain a reference to it being a leader in […]. […].

(446) As described at recitals (440)-(445), there is no evidence that Gemalto views its product as unique. In another 2017 internal document, […]. [293]

Market investigation

(447) Respondents to the market investigation share the view that in the market for Payment HSMs, Gemalto is not a significant player.

(448) A competitor explains that "*this market is dominated by Thales and Micro Focus, to lesser extent Futurex*".[294] Another explains that Gemalto is perceived more as a provider of GP HSMs and Thales as provider of Payment HSMs adding that "*most probably the two product lines will continue to co-exist and as such just the name of the brands might change*".[295] Similarly, a respondent states that "*Payment HSMs is a core business of Thales not from Gemalto/Safenet*".[296]

---

284 [Reference to internal documents].
285 [Reference to internal documents].
286 [Reference to internal documents].
287 [Reference to internal documents].
288 [Reference to internal documents].
289 [Reference to internal documents].
290 [Reference to internal documents].
291 [Reference to internal documents].
292 [Reference to internal documents].
293 [Reference to internal documents].
294 Replies to Questionnaire Q1 – competitors, question (B.C.B.2.3.1).
295 Replies to Questionnaire Q1 – competitors, question (B.D.2.1).
296 Replies to Questionnaire Q1 – competitors, question (B.D.3.1).

(449) When asked to rank Thales' close competitors, respondents that gave a meaningful reply to the market investigation see Futurex and Microfocus as the dominant vendors of Payment HSMs along with Thales.[297]

8.3.2.3. Competitive constraint from other Payment HSM manufacturers

(450) As mentioned in Section 6, the other traditional Payment HSM manufacturers are Atos, DocuSign, Futurex, MicroFocus, Prism, Realsec, Ultra Electronics, and Utimaco.

A. Notifying Party's views

(451) The Notifying Party submits that post-Transaction the merged entity would continue to face strong competition from all of the above-mentioned manufacturers.

B. Commission's assessment

(452) As stated in Section 8.2 in relation to GP HSMs, a merger is unlikely to harm competition where the reaction of the remaining competitors would discipline the behaviour of the merged entity. On the other hand, competition would be harmed if the remaining competitors may not be willing or able to compete sufficiently post-Transaction so as to compensate for the loss of competition.

(453) The Commission considers that the Transaction will not significantly change the existing competitive landscape and that post-Transaction there will remain a sufficient number of competitors with the ability and incentive to constrain the merged entity.

(454) The vast majority of competitors present on the Payment HSM market offer the same or higher certification levels. The main competitors all offer FIPS 140-2 Level 3 certification, with Atos and Utimaco offering also level 4 for physical security.[298] Similarly, with one exception,[299] they are all PCI HSM v2 certified or meet PCI HSM requirements (DocuSign).

(455) Product offerings of the remaining competitors allow them to effectively compete with the merged entity, since the performance levels of their products are comparable and sometimes superior to those offered by Thales and Gemalto. […].

(456) […].[300] Equally, Thales considers it a "*[...]*"[301] And that its product […][302] Thales' Payment HSM. They also state that […].[303]

(457) Utimaco, has recently acquired the Atalla Payment HSM business from Micro Focus […].[304]. This acquisition confirms its incentive to continue to compete in that market. […]. They consider that they should […] and that they are […][305][…].[306]

(458) While Futurex and Utimaco are both global players, Atos is a strong regional player, and the second biggest competitive force on the EEA-wide market, as confirmed by the market reconstruction (see Section 8.2.1). As such, it will continue to constrain

297 Replies to Questionnaire Q1 – competitors, question (B.C.B.1.3.1).
298 Article 6(1)(c) Response, Table 11.
299 MicroFocus is v1 PCI HSM certified, just like Thales.
300 [Reference to internal documents].
301 [Reference to internal documents].
302 Annex to RFI 5 Q.1.a.1
303 [Reference to internal documents].
304 https://hsm.utimaco.com/news/utimaco-cleared-to-complete-acquisition-of-atalla/.
305 [Reference to internal documents].
306 Annex to RFI 5 Q 1.a.47.

the merged entity. […] though its standard features are similar to the one offered by SafeNet Java HSM.[307] It is also the only Payment HSM provider certified under the French cyber security agency, ANSSI.[308]

(459) In line with the above, many of respondents to the market investigation considered that the number of suppliers remaining on the Payment HSM market post-Transaction would be sufficient or did not express concerns.[309] This lack of concern about the decrease of the number of suppliers also matches the views on the position of Gemalto on this market, as discussed in Section 8.3.2 on closeness of competition between the Parties.

(460) The Commission therefore considers that competing Payment HSM manufacturers will have the ability and incentive to compete post-Transaction so as to compensate for the loss of competition.

8.3.2.4. Conclusion on non-coordinated horizontal effects on the EEA-wide market for Payment HSMs

(461) The Commission therefore considers that the Transaction would not give rise to non-coordinated horizontal effects on the on the EEA-wide or worldwide market for Payment HSMs.

8.3.2.5. Conclusion on non-coordinated horizontal effects on the worldwide market for Payment HSMs

(462) As explained in Section 7, the market for Payment HSMs is at least EEA-wide, if not global. The competitive assessment at a worldwide level would be the same as for the EEA level given the Parties' market shares, due to the fact that the same competitive conditions would apply at worldwide level. Thales remains by far the strongest player, whereas Gemalto's slightly higher market share is mainly due to its legacy presence in the Asia-Pacific region. As explained in recitals (432)-(449), the Parties' are not each other close competitor, and Gemalto does not exert a significant competitive constraint on Thales. In view of this, the Commission considers that the Transaction would not give rise to non-coordinated horizontal effects on the worldwide market for Payment HSMs.

8.3.3. Coordinated horizontal effects on the EEA-wide market for Payment HSMs

(463) A merger in a concentrated market may significantly impede effective competition due to horizontal coordinated effects if, through the creation or strengthening of a collective dominant position, it increases the likelihood that firms are able to coordinate their behaviour in this way and raise prices, even without entering into an agreement or resorting to a concerted practice within the meaning of Article 101 TFEU.[310] A merger may also make coordination easier, more stable or more effective for firms that were already coordinating before the merger, either by making the coordination more robust or by permitting firms to coordinate on even higher prices.[311]

---

307 [Reference to internal documents].
308 Article 6(1)(c) Response, para 71.
309 Replies to Questionnaire Q5 – customers of 7 September 2018, question 85.
310 Horizontal Merger Guidelines, para 39.
311 Horizontal Merger Guidelines, para 39.

8.3.3.1. Notifying Party's views

(464) The Notifying Party submits that the potential submarket for Payment HSMs is not conducive to coordinated conduct.[312] It considers that in a rather fragment, non-transparent, and innovative market with several competitors, there is no risk of tacit collusion. It submits that the number of competitors makes tacit coordination unlikely and also that it would be difficult to monitor deviations from coordination or to establish credible deterrent mechanisms in this non-transparent market. In addition, outsiders, including new entrants and customers, would jeopardise any possible coordination.[313]

8.3.3.2. Commission's assessment

(465) Based on the results of the market investigation, the Commission does not consider that the change brought about by the Transaction is likely to make coordination more likely in the industry.

(466) First, the affected market presents characteristics which make coordination difficult. In the market for Payment HSMs demand is highly fragmented. There is limited transparency on the market as these markets are characterised by infrequent, one-off orders rarely awarded through a bidding process. Rather, transactions are confidentially negotiated between buyers and sellers with prices and conditions agreed individually. The Transaction does not diminish these market characteristics which make coordination difficult.

(467) Second, the Transaction does not significantly increase symmetry in the market. Based on the market share figures presented in Table 8, the market will remain asymmetrical post-Transaction.

(468) Third, the market investigation has not indicated that either of the Parties is viewed as a maverick player, the removal of which as a competitive player would increase the likelihood or significance of coordinated effects in other ways.

(469) The Commission therefore considers that the Transaction would not give rise to significant coordinated horizontal effects on the on the EEA-wide or worldwide market for Payment HSMs.

8.4. Encryption software

8.4.1. Market shares

(470) Regarding ES solutions, the Transaction only gives rise to a horizontally affected market on the potential market for network encryptors for data in motion at Layer 2 (see recital (192)). Neither Thales nor Gemalto are active in offering network encryptor products. The limited revenues in this sub-segment are derived from reselling network encryption products manufactured by other companies ([…] in the case of Thales and […] in the case of Gemalto).

(471) Taking into account these revenues, and based on the narrowest potential market (network encryptors at Layer 2), the Parties' combined market share gives rise to a horizontally affected market: [30-40]% worldwide and [20-30]% at the EEA level.

312 Form CO, para 259.
313 Form CO, para 259.

Table 11: Worldwide and EEA market for network encryptors at Layer 2 (2017)

Company	WW	EEA
Thales	[0-5]%	[0-5]%
Gemalto	[20-30]%	[10-20]%
Combined	*[30-40]%*	*[20-30]%*

Source: Form CO

8.4.2. Non-coordinated horizontal effects on the EEA-wide market for network encryptors (for data in motion) at Layer 2

8.4.2.1. Notifying Party's views

(472) The Notifying Party submits that the Transaction would not give rise to any meaningful horizontal effect in the network encryptors market.

(473) First, the Notifying Party submits that the network encryption space is highly competitive and changing rapidly in line with the evolution of telecommunications network products generally. According to the Notifying Party, network encryptors integrated into equipment manufacturers' network devices continue to substantially constrain the Parties. The Notifying Party submits that from a customer's standpoint, stand-alone encryptors and encryptors integrated into network devices perform the same function (i.e. encrypting data in motion). In the Notifying Party's view, as network encryptors must be used in combination with a network device, customers can freely choose to either (i) buy a stand-alone encryptor from one vendor and a network device from another vendor; or (ii) buy a network device integrating an encryptor from a single vendor. As a result, to compete with equipment manufacturers' integrated network devices, vendors of stand-alone network encryptors need to offer encryptors at very competitive prices and/or encryptors with higher performance.

(474) Second, the Notifying Party explains that Thales and Gemalto both resell third-party equipment. According to the Notifying Party, Thales, in particular, […]. Certes, Rohde & Schwarz, and Viasat have their own technology platforms).

8.4.2.2. Commission's assessment

(475) The Commission contends that the Transaction would not significantly impede effective competition as a result of horizontal non-coordinated effects in the possible market for network encryptors for data in motion and the narrowest hypothetical market for Layer 2 network encryptors on the worldwide or EEA-wide market for the reasons set out in recitals (476)-(478).

(476) First, Thales' and Gemalto's activities on the market for network encryptors and the narrowest hypothetical market for Layer 2 network encryptors are very limited. As set out in recital (118), neither Thales nor Gemalto are active in offering network encryptor products and do not control the relevant technologies or production facilities. The […] revenues are derived from reselling network encryption products manufactured by other companies ([…] in the case of Thales and […] in the case of Gemalto). The increment to Thales' market share is limited to [0-5]% globally and [0-5]% in the EEA. Accordingly, the HHI delta is equally low.

(477) Second, based on the Notifying Party's submission, the network encryption space at Layer 2 represents a very small portion of the network encryption market which is

very competitive, including many players offering stand-alone network encryptor products such as Certes, Ciena, Cisco, Infogard, Juniper, Rohde&Schwartz, Secunet, Securosys, ST Electronics. The merged entity will also continue to face competitive constraints post-Transaction from equipment manufacturers offering network encryptors integrated in their network devices.

(478) Third, the market investigation strongly indicated that respondents are neutral as regards the impact on the market for ES, irrespective of the exact product and geographic market definition. The market is very fragmented and there are other strong players such that there will be a sufficient number of market players to ensure choice for consumers post-Transaction. The majority of competitors, customers and resellers which responded to the market investigation expressed the view that competition is not likely to decrease as a result of the Transaction.[314]

8.5. Non-horizontal overlaps

8.5.1. SIM cards, OTA SIM cards administration platforms and GSM-R integration

8.5.1.1. Market shares

(479) The Transaction would give rise to two vertical relationships related to the downstream market of GSM-R integration. In particular, (i) Gemalto's activities in the upstream market for manufacturing and supply of SIM cards and Thales' activities on the downstream market for GSM-R integration and (ii) Gemalto's activities in the upstream market for the supply of OTA SIM cards administration platforms and Thales' activities on the downstream market for GSM-R integration.

(480) Vertically affected markets arise as a result of the Transaction for the manufacturing and supply of SIM cards, where Gemalto's market share in 2017 was [30-40]% on the EEA-wide market and [20-30]% globally and for the supply of OTA SIM cards administration platforms where Gemalto's market share in 2017 was around [40-50]% on the EEA-wide market and around (or below) [40-50]% globally.

As indicated in recital (165), Thales does not purchase SIM cards and OTA SIM administration platforms for GSM-R in the EEA, whether from Gemalto or from anyone else. Thales has no GSM-R integration activities in the EEA and, outside the EEA, Thales is only active in […] countries – […] – with a share of well below [10-20]% in GSM-R integration globally. For projects in […], the SIM cards were provided with the GSM-R equipment by the GSM-R OEM ([…], respectively). [description of a project].

Table 12: Upstream supply of SIM cards and OTA SIM cards administration (2017)

Gemalto	WW	EEA
SIM card manufacturing and supply	[20-30]%	[30-40]%
OTA SIM cards administration platform	[40-50]%	[40-50]%

Source: Form CO

[314] Replies to Questionnaire Q1 – competitors of 19 June 2018, questions C.D.2 and C.D.3; replies to Questionnaire Q2 – customers of 19 June 2018, questions 73 and 76; replies to Questionnaire Q3 – resellers of 21 June 2018, questions 90 and 91.

8.5.1.2. Competitive assessment

A. Input foreclosure

Notifying Party's views

(481) The Notifying Party submits that the Transaction would not give the merged entity the ability and incentive to engage in input foreclosure with regard to the provision of SIM cards and OTA SIM card administration platforms for GSM-R equipment.

(482) The Notifying Party submits that Gemalto does not have market power in any relevant market. According to the Notifying Party, the SIM card sector is characterised by sophisticated and powerful buyers and intense competition, whereby post-Transaction the merged entity will continue to compete with strong competitors such as Idemia, G&D, Valid, INCARD and others. A number of SIM card providers also provide OTA SIM card administration platforms, including for GSM-R, in addition to specialised OTA SIM card administration providers such as ORGA Systems.

Commission's assessment

(483) The Commission considers that for the reasons set out in recitals (485)-(488), the Transaction would not significantly impede effective competition, regardless of any further segmentation.

(484) First, with regard to the ability to engage in input foreclosure, the merged entity does not appear to have a significant degree of market power on the upstream market for SIM cards and OTA SIM card administration platforms. Based on the Notifying Party's submission, Gemalto competes with other players such as IDEMIA (with a market share of 30-40% in the EEA), G&D (with a market share of around 10-20% in the EEA), Valid, INCARD, Eastcompeace and Watchdata which provide SIM cards for GSM-R. Gemalto's competitors have invested in expansion and/or acquisitions in recent years and strengthened their ability to compete within the SIM card sector.[315] Moreover, as regards OTA SIM card administration platforms, Gemalto competes with a number of SIM card providers such as Idemia and G&D but also with specialised OTA SIM card administration providers such as ORGA systems and network operators.

(485) Second, as discussed in recital (485), there are a number of competitors to Gemalto's SIM card and OTA SIM card administration platforms which could provide alternatives to the merged entity. Therefore, if Gemalto were to cease supplying SIM cards and OTA SIM card administration platforms for GSM-R or attempt to raise prices post-Transaction, Thales' rivals will continue to have access to alternative sources of supply.

(486) Third, based on the Notifying Party's submission, there are powerful buyers in the SIM card sector ensuring that the pricing remains competitive. Buyers engage in tenders and joint or multijurisdictional purchasing. In addition, due to the standardisation in SIM card technologies, customers can easily qualify multiple suppliers and shift their orders among them to increase competition.

---

315 Advent International – the controlling entity of Oberthur – acquired Morpho in 2017, increasing Oberthur's market share in SIM cards in the EEA by almost 20% (the Oberthur-Morpho group has become IDEMIA). Further, Valid entered the European commercial smart card sector in 2010 through the acquisition of Microelectronica Española, a Spanish SIM card provider. In 2015, Valid further expanded its European presence in SIM cards by acquiring a Danish smart card manufacturer, Fundamenture A/S.

(487) Fourth, with regard to the incentive to engage in any input foreclosure, the Commission considers that […] (see recital (481)) rule out any potential benefit for Gemalto by implementing an input foreclosure strategy.

(488) The Commission therefore concludes that the Transaction would not significantly impede effective competition as a result of input foreclosure in light of the vertical link between the upstream markets for the supply of SIM cards and OTA SIM card administration platforms and the downstream market for GSM-R integration.

B. Customer foreclosure

Notifying Party's views

(489) The Notifying Party submits that the Parties lack the ability and incentive to foreclose suppliers of SIM cards and OTA SIM card administration platforms to key customers.

(490) First, according to the Notifying Party, Thales is a small player in the market for GSM-R integration which does not have any GSM-R integration activities in the EEA and its activities outside the EEA are limited to […].

(491) Second, post-Transaction there will continue to be demand for SIM cards and OTA SIM card administration platforms from competing providers of GSM-R integration projects as well as from rolling stock operating companies.

Commission's assessment

(492) The Commission considers that for the reasons set out in recitals (494)-(495) the Transaction would not significantly impede effective competition as a result of potential customer foreclosure by which the merged entity would stop acquiring SIM cards and OTA SIM card administration platforms from other suppliers and would exclusively rely on Gemalto for the provision of these products.

(493) First, with regard to the ability to engage in any potential customer foreclosure strategy, the merged entity does not appear to be an important customer on the downstream market for GSM-R integration. This is evidenced by Thales' small role in the market (as demonstrated in recital (481), and the fact that Thales's activities in relation to GSM-R integration are limited to […]). Thales cannot be considered as an essential route to market for the providers of SIM cards and OTA SIM card administration platforms.

(494) Second, there are other GSM-R competing providers which will continue to exert competitive constraints on the merged entity post-Transaction. Based on the Notifying Party's submission, other competitors such as Siemens, Alstom, Ansaldo/Hitachi as well as the GSM-OEMs (Nokia, Huawei and Kapsch) are active globally and have a much stronger position than Thales.

(495) The Commission therefore concludes that the Transaction would not significantly impede effective competition in relation to customer foreclosure in light of the vertical link between the upstream market for the supply of SIM cards and OTA SIM card administration platforms and the downstream market for GSM-R integration.

8.5.2. Access control smart cards

8.5.2.1. Market shares

(496) The Transaction would give rise to a vertical relationship between Gemalto's activities in the upstream market for the provision of access control smart cards (including for use in remote administration of HSMs) and Thales' activities on the downstream markets for GP and Payment HSMs.

(497) Regarding the remote administration of HSMs, Gemalto offers the possibility to manage its HSMs remotely from a workstation as a standard feature in its GP and Payment HSMs without an additional charge. Thales offers remote HSM capabilities through […] – available to Thales' HSM customers as optional add-on licenses.

(498) Smart cards are only one way to allow for user authentication and access authorisation in a remote HSM administration solution. Both of Thales' […] support smart card authentication. Gemalto, on the other hand, despite being a smart card producer, does not use smart cards for remote administration of any of its HSMs.[316]

8.5.2.2. Competitive assessment

A. Input foreclosure

Notifying Party's views

(499) The Notifying Party submits that the Transaction would not give the merged entity the ability and incentive to engage in input foreclosure with regard to the provision of smart cards including for use in remote HSM administration for the reasons set out in recitals (501)-(504).

(500) First, in the Notifying Party's view, Gemalto only has a small market share on the market for access control smart cards, irrespective of the precise product and geographic market definition. In particular, Gemalto's market share is around [20-30]% on the EEA-wide market (Gemalto's market share globally is around [10-20]%). Considering the narrowest possible product market segmentation on the basis of a separate market for logical access control smart cards, Gemalto's market share is estimated to be below [30-40]% both globally and in the EEA.

(501) Furthermore, the Notifying Party submits that Gemalto competes with a large number of other companies selling access control smart cards (e.g. Assa Abloy/HID Global, Entrust Datacard, FEITIAN, G&D, NXP, Idemia, and Vasco).

(502) Second, according to the Notifying Party, smart cards are only one way to allow for user authentication and access authorisation in a remote HSM administration solution. Other options for remote HSM administration include PIN Entry Devices ("PEDs"), password programs, and virtual access control systems. In the Notifying Party's view, there is an emerging trend of replacing physical access control devices by virtual solutions (offered by a number of companies such as Centrify, Computer Associates, DUO Secuirty, Entrust Datacard, Forticode etc.).

(503) Third, in the Notifying Party's view, access control is not a key application of Gemalto's smart cards. According to the Notifying Party, out of […] smart cards sold by Gemalto in 2017, only […] were access control cards. The Notifying Party does not have precise information on the number of access control cards sold for use in remote HSM administration (as Gemalto does not always have information about customers' intended use of Gemalto's access control smart cards) but considers that such cards account for a de minimis percentage of the overall access control card sales.

316 Gemalto's ProtectServer HSMs support password authentication, while Gemalto's SafeNet Luna line of GP and Payment HSMs support both password and PED authentication.

Commission's assessment

(504) The Commission considers that for the reasons set out in recitals (506)-(508), the Transaction would not significantly impede effective competition, regardless of any further segmentation.

(505) First, with regard to the ability to engage in input foreclosure, the merged entity does not appear to have a significant degree of market power on the upstream market for access control smart cards given that Gemalto competes with many other suppliers of such products (see recital (502)) and its market share, irrespective of the precise product and geographic market definition, does not exceed 30% (see recital (501)).

(506) Second, as discussed in recitals (502)-(503), if Gemalto were to attempt any foreclosure strategy in relation to access control smart cards post-Transaction, the Parties' HSM competitors could easily shift demand to other smart card suppliers or choose to switch to a different technology altogether (e.g. PED or password).

(507) Third, with regard to the incentive to engage in any input foreclosure, the Commission considers that in view of the estimated limited sales of Gemalto for use on HSM remote administration (see recital (504)), Gemalto would not be incentivised to implement an input foreclosure strategy that would prevent other suppliers from selling access control smart cards to the market.

(508) The Commission therefore concludes that the Transaction would not significantly impede effective competition as a result of input foreclosure in light of the vertical link between the upstream markets for the supply of access control cards and the downstream market for GP and Payment HSMs.

B. Customer foreclosure

Notifying Party's views

(509) The Notifying Party submits that the Parties lack the ability and incentive to foreclose suppliers of access control smart cards from access to key customers.

(510) According to the Notifying Party, remote administration of HSMs is a niche use case for access control smart cards (as most such cards are used by undertakings for network access and remote PC access by their employees). In the Notifying Party's view, Thales' purchases of access control smart cards […] account for less than […] of Gemalto's total sales of access control smart cards. The Notifying Party submits that Thales similarly accounts for less than [0-5]% of the access control cards sold globally in 2017.

Commission's assessment

(511) The Commission considers that for the reasons set out in recitals (513)-(515) the Transaction would not significantly impede effective competition as a result of potential customer foreclosure by which the merged entity would stop acquiring access control smart cards for use in remote HSM administration from other suppliers and would exclusively rely on Gemalto for the provision of these products.

(512) First, with regard to the ability to engage in any potential customer foreclosure strategy, the Commission considers that in view of the limited demand for which Thales accounts on the downstream market, even if the merged entity were to purchase its access control smart cards exclusively from Gemalto, the impact on the sales of other suppliers would not be significant.

(513) Second, the Commission considers that other suppliers would still have ample alternative demand, including from other HSM providers, but also from a larger

number of other companies purchasing the access control smart cards for a variety of use cases other than remote HSM administration.

(514) Third, with regard to the incentive to engage in any potential customer foreclosure, the Commission considers that the merged entity would be impeded if it attempted a customer foreclosure strategy as it would significantly limit its market opportunities to reach a larger customer base, including selling access control smart cards to other HSM providers and other companies for different use cases.

(515) The Commission therefore concludes that the Transaction would not significantly impede effective competition in relation to customer foreclosure in light of the vertical link between the upstream market for the supply of access control smart cards and the downstream markets for GP and Payment HSMs.

8.5.3. Conglomerate effects

(516) Notifying Party's views

(517) The Notifying Party submits that the Transaction will not result in any negative conglomerate effects. The only related markets in which the Notifying Party sees a theoretical potential for conglomerate effects is in the link between GP and Payment HSMs, and ES. Nevertheless, the Notifying Party submits that the Parties will not have the ability to foreclose ES competitors or to foreclose companies who do not offer a combination of KMS, including HSMs (GP HSMs and/or Payment HSMs) and ES products for the reasons set out in recitals (519)-(523).

(518) First, the Parties do not offer unique or "must-have" products such that post-Transaction they would have a degree of market power on the GP or Payment HSM markets that could be leveraged into the ES market. In the Notifying Party's view, customers often do not buy GP or Payment HSMs for encryption use cases.[317] In particular, regarding Payment HSMs, the Notifying Party submits that customers rarely purchase ES in conjunction with Payment HSMs since ES and Payment HSMs address different use cases (i.e. ES is used for encryption purposes while Payment HSMs are used to secure payment transactions). The Notifying Party argues that any attempt to leverage market power in GP HSMs or Payment HSMs into ES would quickly be circumvented by the powerful ES competitors who would design new encryption software solutions to allow customers to work around any particular HSM product.

(519) Second, the Notifying Party submits that the merged entity would not have the ability post-Transaction to foreclose competitors who do not offer a combination of HSMs (GP HSMs and/or Payment HSMs) and enterprise encryption. Generally, customers do not purchase ES with their KMS (including HSMs), and even in such cases customers generally do not purchase both HSMs (GP or Payment) and ES from the same vendor but rather mix and match different solutions from different vendors. According to the Notifying Party, only very sophisticated customers may opt for integrated solutions, which are composed of one or several ES solutions and a centralised key management tool (e.g. relying on GP HSMs). Such customers

---

317 According to the Notifying Party, as regards GP HSMs, while customers sometimes purchase GP HSMs for encryption use cases, they can and do purchase GP HSMs for numerous other use cases, including for instance authentication and verification, code and document signing, PKI or credential management, SSL and TLS key protection – and for all of these use cases, customers would not need to buy encryption software in conjunction with their GP HSMs.

represent only marginal sales and address the needs of large undertakings which have countervailing buyer power.

(520) The Notifying Party submits that post-Transaction there will remain a number of competitors who offer both KMS (including GP and Payment HSMs) and ES solutions in competition with the Parties (e.g. IBM, Micro Focus and HSM aaS vendors offering ES in the cloud). In the Notifying Party's view, the Parties have not attempted in the last decade to foreclose competitors not able to offer both GP or Payment HSMs and ES and any such attempt would have been quickly quashed by the far larger ES players whose solutions drive customers' ES spend.

(521) Third, the Notifying Party submits that the Parties' customers are large multinational undertakings, with significant buying power and expertise of their own, which would move quickly to disrupt any attempted exclusionary strategy.

(522) Fourth, there is no past practice of bundling. The Notifying Party explains that numerous vendors supply integrated solutions including both encryption software and key management capabilities (e.g. Check Point Software Technologies, Eruces, Micro Focus, Oracle, Protegrity, PKWARE, Sophos, Symantec, and WinMagic). Each of these integrated solutions comes with a centralised key management tool. Keys are typically stored in a built-in software or hardware appliance, which may include a built-in HSM. In addition, many integrated solutions are designed so as to allow the customer to connect the integrated solution with his own HSMs in order to store keys in its separate HSMs. Thales and Gemalto also supply integrated solutions (i.e. Thales' Vormetric Data Security Platform and Gemalto's SafeNet KeySecure solutions.

B. Commission's assessment

(523) The Commission considers that the Transaction does not give rise to a significant impediment to effective competition as a result of any conglomerate effect.

(524) First, the Commission notes that the Parties do not have any GP or Payment HSMs products that other suppliers do not offer. The Parties are therefore not in a position to completely deny their customers any products in an effort to force customers to purchase other products such as ES from the Parties.

(525) Second, Thales and Gemalto both had a broad portfolio regarding GP and Payment HSMs and ES before the Transaction but the market investigation did not suggest that any of the Parties attempted to force bundling or tying.

(526) Third, the Commission notes that for a bundling strategy to effectively foreclose competitors, the merged entity must have a significant degree of market power. With regard to GP HSMs, the Commitments offered by the Notifying Party (see Section 9) will remove the overlap between the Parties. Therefore, the Transaction as modified by the Commitments will not lead to any change as regards the possibility to leverage market power from the GP HSM market into the market for ES.

(527) With regard to Payment HSMs, the Commission considers that the Transaction will not bring about significant change in market power on the market for Payment HSMs for the reasons set out in this Decision. As set out in Section 8.3.2.2., Gemalto's role is small in the Payment HSM market and there will be no merger-specific impact on the market position of the merged entity such that it will affect the Parties' ability to bundle and tie Payment HSM and ES products. In particular, the Transaction would not result in a change of the competitive landscape in the Payment HSM market and post-Transaction there will remain a sufficient number of competitors with the ability and incentive to constrain the merged entity if it were to attempt a bundling or tying

strategy. In addition, there are no indications based on the results of the market investigation that customers purchase Payment HSMs together with ES as Payment HSMs and ES address different use cases. As demonstrated in Section 7.2.1.3.D, Payment HSMs are used for specific use cases and need to comply with strict physical and logical security requirements in order to obtain PCI-HSM certification, which are not needed for ES products.

(528) Fourth, the Commission considers that any theoretical attempt to leverage market power from Payment HSMs into ES more generally would be circumvented by the numerous stronger players on the ES market such as Microsoft, IBM, Oracle, Symantec, Sophos, McAfee and others.

(529) The Commission therefore concludes that the Transaction does not give rise to a significant impediment to effective competition as a result of conglomerate effects.

9. COMMITMENTS

9.1. Introduction

(530) In order to remove the serious doubts arising from the Transaction described in Section 8.2 in relation to the market for GP HSM, the Notifying Party submitted commitments modifying the Transaction on 10 October 2018 (the "Initial Commitments").

(531) The Commission launched a market test of the Initial Commitments on 11 October 2018, seeking responses from actual and potential competitors, cloud service providers, customers as well as resellers. The Commission informed the Notifying Party of the results of the market test on 26 October 2018. Following the feedback received from market participants in the market test, the Notifying Party submitted a revised set of commitments on 7 November 2018 (the "Final Commitments").

(532) The Final Commitments are annexed to this decision and form an integral part thereof.

9.2. Initial Commitments

9.2.1. Description of the Initial Commitments

(533) The Initial Commitments consist of the divestment of Thales' global GP HSM business, marketed under the nShield brand (the "Divestment Business").

(534) The Divestment Business is integrated into Thales eSecurity, a business unit operating activities in data protection, including GP HSMs, Payment HSMs, Key Management, and Encryption Software. […] Thales proposes to carve-out the Divestment Business prior to transferring it to a suitable purchaser.

(535) The Divestment Business comprises all assets and most of the staff which contribute to the operation of Thales' GP HSM business, in particular: (i) all tangible and intangible assets (including intellectual property rights); (ii) all licences, permits, certifications and authorisations issued by any governmental organisation for the benefit of the Divestment Business; (iii) all contracts, leases, commitments and customer orders of the Divestment Business; (iv) all customer, credit and other records of the Divestment Business; and (v) the Personnel.

(536) At the option of the purchaser, the Divestment business could also include transitional services for a period to be agreed with the purchaser and pursuant to transition services agreements. At the purchaser's option, such services would cover […].

(537) The main tangible assets forming part of the transfer are: […] as well as all finished goods inventory, supplies tooling, test equipment, sales and promotional material, product documentation, and user manuals relating to the Divestment Business.

(538) As regards intangible assets, the Divestment Business will include a transfer, or license (as appropriate), of the following main intangible assets: (i) all registered nShield trademarks and patents; (ii) all additional unregistered intellectual property including know-how, testing procedures, manufacturing procedures, product design, trade secrets, source code, and associated utilities and libraries (including product specifications and quality control standards); (iii) all nShield product SKUs listed in the nShield price list; (iv) an assignment of the section of any and all inbound licenses that are necessary for the operation (or otherwise used by) the Divestment Business; (v) all documentation associated with R&D for products marketed (or intended to be marketed) under the nShield brand.

(539) In addition, the Initial Commitments provide that the purchaser of the Divestment Business shall be independent of and unconnected to the Parties; have the financial resources, proven expertise and incentive to maintain and develop the Divestment Business as a viable and active competitive force in competition with the Parties and other competitors, and that the acquisition of the Divestment Business by the purchaser must neither be likely to create, in light of the information available to the Commission, prima facie competition concerns nor give rise to a risk that the implementation of the Commitments will be delayed. In particular, the purchaser must reasonably be expected to obtain all necessary approvals from the relevant regulatory authorities for the acquisition of the Divestment Business.

(540) Finally, the Initial Commitments contain related commitments, including those regarding the separation of the Divestment Business from the businesses retained by Thales, the preservation of the viability, marketability and competitiveness of the Divestment Business, including the appointment of a monitoring trustee and, if necessary, a divestiture trustee.

9.2.2. Results of the market test

(541) The results of the market test were generally positive and several market participants expressed interest in acquiring the Divestment Business.

(542) The majority of the respondents to the market test did not express concerns about the viability of the Divestment Business or its suitability to address competition concerns identified by the Commission, subject to it being sold to a suitable purchaser.[318]

(543) The majority of the comments made by respondents to the market test were of a general nature and pointed to risks inherent in any asset divestiture. As for the more concrete replies to the market test, most of them concerned purchaser criteria and elements that should be included in the Divestment Business.[319] Most of these elements, however, were included in the Commitments as presented to the respondents such as, for example, sales personnel or R&D projects. In a few instances, the respondents indicated elements which do not form part of the GP HSM business, such as SafeSign or CipherTrust Monitor. A few respondents also commented on the non-inclusion of Payment HSM (in connection to that, one of the respondents to the market test raised an argument that the merged entity could leverage its position on the Payment HSM market to strengthen its position in the GP

318 Questionnaire Remedies market test v3 of 11 October 2018, replies to questions 6-8.

319 Questionnaire Remedies market test v3 of 11 October 2018.

HSM market by selling GP HSMs to customers who require both GP HSM and Payment HSM solutions)[320].

(544) For example, respondents to the market test considered it important for the Divestment Business to contain all the necessary elements to allow it to continue operating as a standalone business. To that end, some indicated in particular that the Divestment Business should include the existing R&D capability (technical/engineering staff; product roadmap), support and maintenance services and access to sales channels.[321]

(545) Respondents to the market test also indicated that the identity of the purchaser is important for their assessment of the viability of the Divestment Business. Previous expertise would be an essential condition for many of the respondents to the market test.[322] Many see it necessary for the purchaser to have an in-depth knowledge of the market segment. Reputation and trustworthiness of the purchaser is also important to the respondents to the market test. Customers responding to the market test see the ability to maintain security integrity as one of the necessary criteria for the purchaser of the Divestment Business in order to ensure its viability.[323] One of the customers responding to the market test considered that it should "be a trustworthy company regarding security in order to prevent backdoors from being implemented".[324]

(546) A few respondents to the market test considered the Commitments to be insufficient, since they are limited to GP HSMs and do not include Payment HSMs.[325] These respondents argue that the Transaction would also raise concerns on the Payment HSM market and that the Commitments do not address such concerns. They also consider that it might be difficult to carve-out GP HSM from Payment HSM, making the Divestment Business unviable, or that the continued use of the payShield trademark for Thales' Payment HSM products would have a negative impact on the Divestment Business A small minority of the respondents to the market test put into doubt the reliability and attractiveness of Thales' GP HSM business, indicating that Thales' nShield product line is dated and approaching end of life.

9.2.3. Commission's assessment of the Initial Commitments

9.2.3.1. Scope of the Divestment Business

(547) The Commission considers that the scope of the Divestment Business is sufficiently comprehensive as the Initial Commitments would remove the entire overlap between the Parties in relation to the worldwide market for GP HSM. In principle, they are therefore suitable to remove the competition concerns identified.

(548) The Commission considers that Payment HSM and GP HSM form two separate markets and identified competitive concerns only in relation to the latter market as set out in Section 8. The Commitments address the competitive concerns identified. In relation to the argument that the merged entity could leverage its position on the Payment HSM market to strengthen its position in the GP HSM market by selling GP HSMs to customers who require both GP HSM and Payment HSM solutions, the

320 Questionnaire Remedies market test v3 of 11 October 2018, reply to question 11.
321 Questionnaire Remedies market test v3 of 11 October 2018, replies to questions 2-5.
322 Questionnaire Remedies market test v3 of 11 October 2018, replies to question 7.
323 Questionnaire Remedies market test v3 of 11 October 2018, replies to questions 2, 7 and 8.
324 Questionnaire Remedies market test v3 of 11 October 2018, reply to question 7.
325 Questionnaire Remedies market test v3 of 11 October 2018, replies to question 2.

Commission notes that customers requiring both Payment HSM and GP HSM form only a small proportion of the market.[326]

(549) The Divestment Business comprises all assets and most of the staff that contribute to the operations of the GP HSM business, as detailed in Section 9.2, and so it is sufficiently comprehensive as it includes all the assets necessary for its viability and competitiveness. The question of viability of the Divestment Business is addressed further in Section 9.2.3.2.

9.2.3.2. Viability of the Divestment Business

(550) The Commission considers that the Divestment Business' viability will not be negatively affected by its separation from the Payment HSM business. A few respondents questioned the viability of the Divestment Business on the grounds that it might be difficult to carve-out GP HSM from Payment HSM, since they view them as strongly linked or even technologically dependent and not standalone. However, […].[327] […].[328] According to the Notifying Party, intangible assets […].[329] As a result, the Commission is satisfied that the assets can be separated and transferred into the Divestment Business without affecting the viability of the GP HSM business.

(551) The Commission also considers that the continued use of the payShield trademark by Thales in respect of its Payment HSM will not negatively affect the Divestment Business. Thales' HSM customers are sophisticated players.[330] The Commission therefore agrees with the Notifying Party's argument that customers will fully understand the difference between payShield and nShield HSMs.[331] In addition, the Divestment Business will also obtain the nCipher brand/trademark and so all "n' branded products will become part of the Divestment Business. Even if confusion were to arise as regards the use of the word "Shield", the Commission considers that it would not necessarily be to the prejudice of the Divestment Business as it could equally induce customers to purchase the Divestment Business products. The Commission also notes that the common word "shield" is a generic word generally associated with protection and security.

(552) Furthermore, the necessary personnel will be transferred to the Divestment Business to ensure its viability. The engineering team devoted to GP HSM will be transferred to the Divestment Business to ensure that all existing R&D projects can continue. Maintenance and support forming around […]% of the value of the business, the Initial Commitments also foresee […]. As explained in Annex 7 to the Commitments' Schedule, […].

(553) The Commission considers that the Initial Commitments contain sufficient provisions to ensure access to sales channels. They envisage the transfer of distribution and reseller agreements to the purchaser to the extent these relate to the products of the Divestment Business. […] Sales personnel handling most of the sales of the Divestment Business will transfer to the purchaser. Countries where

---

326 Article 6(1)(c) Response, para 32; replies to Questionnaire Q2 – customers of 19 June 2018, question 3; these would most likely be customers from the BFSI sector (Banking, Financial Services and Insurance).

327 Reply to RFI 22, question 3.

328 Form RM, para 12.

329 Form RM, para 12; reply to RFI 22, question 4.

330 Form CO, para 95.

331 Reply to RFI 22, question 7.

distribution is effected today via […]. Moreover, in each of those countries, the Divestment Business […].

(554) As to the concerns of individual respondents to the market test for the reliability and attractiveness of Thales' GP HSM business, the Commission notes that Thales is a leading player in the GP HSM space; Thales' significance as a competitive constraint is precisely the reason why commitments are considered necessary. While a large proportion of Thales' sales […], the Divestment Business is forecasted by the Notifying Party to grow in line with the overall market growth. In this regard, the Commission considers that these risks pointed out by individual respondents seem at least not to stem from the divestment but, if they exist at all, are inherent already to the business. The Commission further notes that the viability of the Divestment Business is to be maintained by the transfer of […].

(555) Thales [description of Thales' manufacturing process].

(556) Since the viability of the Divestment Business might hinge upon the assignment of the Supply Agreement with […] to the purchaser, the Commission considers that the Initial Commitments are insufficient to ensure viability of the Divestment Business.

9.2.3.3. Purchaser criteria

(557) For a divestment other than the divestment of a going concern to be an effective remedy, it is critical that the business is divested to a suitable purchaser. Taking into account the responses to the market test, the Commission considers that the purchaser criteria as taken from the standard model for divestiture commitments as contained in the Initial Commitments are not adequate to sufficiently ensure the suitability of the purchaser.

(558) In addition to these criteria, additional criteria should ensure that the purchaser has already experience in HSM or a closely related field and enjoys a high level of trust in these areas among EEA-based customers. Also, the purchaser should be able to show that it will be able to reliably provide GP HSM products and related services to EEA-based customers, that is will be able to receive all necessary certifications and that it will further invest into and develop the GP HSM product.

9.2.3.4. Conclusion

(559) The Commission therefore considers that the Initial Commitments would not be suitable to remove the serious doubts raised by the Transaction in a clear-cut manner.

9.3. Final Commitments

9.3.1. Description of the Final Commitments

(560) The Final Commitments consist of a revised version of the Initial Commitments. The modifications included in the Final Commitments with respect to the Initial Commitments are the following:

(a) the standard purchaser criteria are supplemented by an additional criterion that the "Purchaser shall be a player with significant experience in the HSM, or a closely related field, such as data security, enjoying a high level of trust and a good reputation in these areas among EEA-based customers. The Purchaser shall show by way of a business plan, at the Purchaser approval stage, that it has the ability and expertise, in using its own and the Divestment Business' assets, to reliably provide the relevant products and services to EEA customers, even for enterprise grade security applications and that it has sufficiently concrete plans to undertake (i) all necessary steps to achieve and continue achieving all certifications, and their updates, necessary to supply GP HSMs in

the EEA; and (ii) the required R&D for the further development of the Divestment Business."

(b) the Schedule to the Commitments now expressly refers to all registered nShield, nCipher, and CodeSafe trademarks and patents listed in Annex 1 along with all patents that are necessary for the operation of (or otherwise used by) the Divestment Business, and not just to nShield trademark.

(561) The Commission also received written assurances from […] that it would "permit Thales to assign the nShield related terms of the supply agreement to the buyer of the divested business subject to […] being comfortable with the credit risk of the Buyer, and the Buyer, […] and Thales entering into assignment and assumption agreements related to all rights and obligations in the supply agreement concerning nShield, so that the resulting commercial relationships will not disadvantage the buyer or […] vis-à-vis Thales compared to the current terms of the supply agreement."[332]

9.3.2. Commission's assessment of the Final Commitments

9.3.2.1. Viability of the Divestment Business

(562) As all issues with respect to the viability of the Divestment Business have been removed by a written assurance from […] that it would permit the assignment of the Supply Agreement to the Divestment Business purchaser, the Commission considers that the Final Commitments have the ability to effectively remove the serious doubts raised by the Transaction in a clear-cut manner.

9.3.2.2. Purchaser criteria

(563) The additional purchaser criteria ensure that the purchaser has the relevant expertise in the field and that it enjoys a high level of trust and reputation among the EEA customers so as to be able to reliably provide the relevant products. It also addresses concerns raised by the respondents to the market test about the ability of the purchaser to persist in the R&D efforts for the continuing development of the Divestment Business and to obtain the required certifications.

(564) Consequently, the Commission considers that the revised, stricter purchaser criteria offered by the Notifying Party in the Final Commitments are sufficient to address concerns expressed by the respondents to the market test and ensure that an appropriate purchaser can be selected so as to ensure the viability of the Divestment Business.

9.3.3. Conclusion

(565) The Commission therefore considers that the Final Commitments are capable of removing serious doubts as to the compatibility of the Transaction with the internal market in a clear-cut manner.

10. CONDITIONS AND OBLIGATIONS

(566) Pursuant to the second subparagraph of Article 8(2) of the Merger Regulation, the Commission may attach to its decision conditions and obligations intended to ensure that the undertakings concerned comply with the commitments they have entered into vis-à-vis the Commission with a view to rendering the concentration compatible with the internal market.

---

332 Email from […] dated 29 November 2018.

(567) The fulfilment of the measure that gives rise to the structural change of the market is a condition, whereas the implementing steps which are necessary to achieve this result are generally obligations on the Parties. Where a condition is not fulfilled, the Commission's decision declaring the concentration compatible with the internal market is no longer applicable. Where the undertakings concerned commit a breach of an obligation, the Commission may revoke the clearance decision in accordance with Article 8(6) of the Merger Regulation. The undertakings concerned may also be subject to fines and periodic penalty payments under Articles 14(2) and 15(1) of the Merger Regulation.

(568) In accordance with the basic distinction described in recital (566) as regards conditions and obligations, this Decision should be made conditional on the full compliance by the Notifying Party with Section B and recitals (1)-(5) of the Schedule of the Commitments submitted by the Notifying Party on 07 November 2018 and all other Sections (including recital 6 of the Schedule) should be obligations within the meaning of Article 8(2) of the Merger Regulation. The full text of the commitments is attached as an Annex to this Decision and forms an integral part thereof.

HAS ADOPTED THIS DECISION:

Article 1

The notified concentration whereby Thales S.A. acquires sole control of Gemalto N.V. within the meaning of Article 3(1)(b) of the Council Regulation (EC) No 139/2004 is hereby declared compatible with the internal market and the EEA Agreement.Article 2

Article 1 is subject to compliance with the conditions set out in Section B and recitals (1)-(5) of the Schedule of the Annex to the present Decision.

Article 3

Thales S.A. shall comply with the obligations set out in the sections of the Annex to the present Decision not referred to in Article 2.

Article 4

This Decision is addressed to:

THALES S.A.

Tour Carpe Diem

31, Place des Corolles

92098 Paris – La Defense

France

Done at Brussels,

For the Commission

(Signed)
Margrethe VESTAGER
Member of the Commission

Case M. 8797 – Thales/Gemalto

COMMITMENTS TO THE EUROPEAN COMMISSION

Pursuant to Articles 8(2) and 10(2), of Council Regulation (EC) No. 139/2004 (the "***Merger Regulation***"), Thales S.A. ("***Thales***") (the "***Notifying Party***") hereby enters into the following Commitments (the "***Commitments***") vis-à-vis the European Commission (the "***Commission***") with a view to rendering the acquisition of 100% of the issued and outstanding ordinary shares of Gemalto N.V. ("***Gemalto***") by Thales (the "***Concentration***") compatible with the internal market and the functioning of the EEA Agreement.

This text shall be interpreted in light of the Commission's decision pursuant to Article 8(2) of the Merger Regulation to declare the Concentration compatible with the internal market and the functioning of the EEA Agreement (the "***Decision***"), in the general framework of European Union law, in particular in light of the Merger Regulation, and by reference to the Commission Notice on remedies acceptable under Council Regulation (EC) No 139/2004 and under Commission Regulation (EC) No 802/2004 (the "***Remedies Notice***").

Section A. Definitions

1. For the purpose of the Commitments, the terms below shall have the following meaning:

   Affiliated Undertakings: undertakings controlled by the Parties and/or by the ultimate parents of the Parties, whereby the notion of control shall be interpreted pursuant to Article 3 of the Merger Regulation and in light of the Commission's Consolidated Jurisdictional Notice under Council Regulation (EC) No 139/2004 on the control of concentrations between undertakings (the "***Consolidated Jurisdictional Notice***").

   Assets: the assets that contribute to the current operation or are necessary to ensure the viability and competitiveness of the Divestment Business as indicated in Section B, paragraph 5 and described in more in detail in the Schedule.

   Closing: the transfer of the legal title to the Divestment Business to the Purchaser.

   Closing Period: the period of [Redacted] from the approval of the Purchaser and the terms of sale by the Commission.

   Confidential Information: any business secrets, know-how, commercial information, or any other information of a proprietary nature that is not in the public domain.

   Conflict of Interest: any conflict of interest that impairs the Trustee's objectivity and independence in discharging its duties under the Commitments.

   Divestment Business: the business or businesses as defined in Section B and in the Schedule which the Notifying Party commits to divest.

   Divestiture Trustee: one or more natural or legal person(s) who is/are approved by the Commission and appointed by Thales and who has/have received from Thales the exclusive Trustee Mandate to sell the Divestment Business to a Purchaser at no minimum price.

Effective Date: the date of adoption of the Decision.

First Divestiture Period: the period of [Redacted] from the Effective Date.

Hold Separate Manager: the person appointed by Thales for the Divestment Business to manage the day-to-day business under the supervision of the Monitoring Trustee.

Key Personnel: all Personnel necessary to maintain the viability and competitiveness of the Divestment Business, as listed in **Annex 6** to the Schedule, including the Hold Separate Manager.

Monitoring Trustee: one or more natural or legal person(s) who is/are approved by the Commission and appointed by Thales, and who has/have the duty to monitor Thales' compliance with the conditions and obligations attached to the Decision.

Parties: Thales and Gemalto.

Personnel: all staff of the Divestment Business as outlined in **Annex 7** and **Annex 8** to the Schedule.

Purchaser: the entity approved by the Commission as acquirer of the Divestment Business in accordance with the criteria set out in Section D.

Purchaser Criteria: the criteria laid down in paragraph 14 of these Commitments that the Purchaser must fulfil in order to be approved by the Commission.

Schedule: the schedule to these Commitments describing more in detail the Divestment Business.

Trustee(s): the Monitoring Trustee and/or the Divestiture Trustee as the case may be.

Trustee Divestiture Period: the period of [Redacted] from the end of the First Divestiture Period.

Section B. The Commitment to Divest and the Divestment Business

Commitment to Divest

2. In order to maintain effective competition in General Purpose Hardware Security Modules ("GP HSMs"), Thales commits to divest, or procure the divestiture of the Divestment Business by the end of the Trustee Divestiture Period as a going concern to a Purchaser and on terms of sale approved by the Commission in accordance with the procedure described in paragraph 15 of these Commitments. To carry out the divestiture, Thales commits to find a Purchaser and to enter into a final binding sale and purchase agreement for the sale of the Divestment Business within the First Divestiture Period. If Thales has not entered into such an agreement at the end of the First Divestiture Period, Thales shall grant the Divestiture Trustee an exclusive mandate to sell the Divestment Business in accordance with the procedure described in paragraph 27 during the Trustee Divestiture Period.

3. Thales shall be deemed to have complied with this commitment if:

   a) by the end of the Trustee Divestiture Period, Thales or the Divestiture Trustee has entered into a final binding sale and purchase agreement and the

Commission approves the proposed purchaser and the terms of sale as being consistent with the Commitments in accordance with the procedure described in paragraph 15; and

b) the Closing of the sale of the Divestment Business to the Purchaser takes place within the Closing Period.

4. [Redacted].

Structure and Definition of the Divestment Business

5. The Divestment Business consists of Thales' global GP HSM business, marketed under the nShield brand. The legal and functional structure of the Divestment Business as operated to date is described in the Schedule. The Divestment Business, as described in the Schedule, includes all assets and staff that contribute to the current operation or are necessary to ensure the viability and competitiveness of the Divestment Business, in particular:

a) all tangible and intangible assets (including intellectual property rights);

b) all licences, permits, certifications and authorisations issued by any governmental organisation for the benefit of the Divestment Business;

c) all contracts, leases, commitments and customer orders of the Divestment Business; all customer, credit and other records of the Divestment Business; and

d) the Personnel.

Section C. Related Commitments

Preservation of Viability, Marketability and Competitiveness

6. From the Effective Date until Closing, Thales shall preserve or procure the preservation of the economic viability, marketability and competitiveness of the Divestment Business, in accordance with good business practice, and shall minimise as far as possible any risk of loss of competitive potential of the Divestment Business. In particular Thales undertakes:

a) not to carry out any action that might have a significant adverse impact on the value, management or competitiveness of the Divestment Business or that might alter the nature and scope of activity, or the industrial or commercial strategy or the investment policy of the Divestment Business;

b) to make available, or procure to make available, sufficient resources for the development of the Divestment Business, on the basis and continuation of the existing business plans; and

c) to take all reasonable steps, or procure that all reasonable steps are being taken, including appropriate incentive schemes (based on industry practice), to encourage all Key Personnel to remain with the Divestment Business, and not to solicit or move any Personnel to Thales' remaining business. Where, nevertheless, individual members of the Key Personnel exceptionally leave the Divestment Business, Thales shall provide a reasoned proposal to replace the person or persons concerned to the Commission and the Monitoring Trustee. Thales must be able to demonstrate to the Commission that the replacement is well suited to carry out the functions exercised by those individual members of

the Key Personnel. The replacement shall take place under the supervision of the Monitoring Trustee, who shall report to the Commission.

Hold-Separate Obligations

7. Thales commits, from the Effective Date until Closing, to keep the Divestment Business separate from the businesses it is retaining and to ensure that unless explicitly permitted under these Commitments: (i) management and staff of the businesses retained by Thales have no involvement in the Divestment Business; and (ii) the Key Personnel and Personnel of the Divestment Business have no involvement in any business retained by Thales and do not report to any individual outside the Divestment Business.

8. Until Closing, Thales shall assist the Monitoring Trustee in ensuring that the Divestment Business is managed as a distinct and saleable entity separate from the businesses which Thales is retaining. Immediately after the adoption of the Decision, Thales shall appoint a Hold Separate Manager. The Hold Separate Manager, who shall be part of the Key Personnel, shall manage the Divestment Business independently and in the best interest of the business with a view to ensuring its continued economic viability, marketability and competitiveness and its independence from the businesses retained by Thales. The Hold Separate Manager shall closely cooperate with and report to the Monitoring Trustee and, if applicable, the Divestiture Trustee. Any replacement of the Hold Separate Manager shall be subject to the procedure laid down in paragraph 6(c) of these Commitments. The Commission may, after having heard Thales, require Thales to replace the Hold Separate Manager.

Ring-Fencing

9. Thales shall implement, or procure to implement, all necessary measures to ensure that it does not, after the Effective Date, obtain any Confidential Information relating to the Divestment Business and that any such Confidential Information obtained by Thales before the Effective Date will be eliminated and not be used by Thales. This includes measures vis-à-vis Thales' appointees on the management team of the Divestment Business. In particular, the participation of the Divestment Business in any central information technology network shall be severed to the extent possible, without compromising the viability of the Divestment Business. Thales may obtain or keep information relating to the Divestment Business which is reasonably necessary for the divestiture of the Divestment Business or the disclosure of which to Thales is required by law.

Non-Solicitation Clause

10. The Parties undertake, subject to customary limitations, not to solicit, and to procure that Affiliated Undertakings do not solicit, the Key Personnel transferred with the Divestment Business for a period of [Redacted] after Closing.

Due Diligence

11. In order to enable potential purchasers to carry out a reasonable due diligence of the Divestment Business, Thales shall, subject to customary confidentiality assurances and dependent on the stage of the divestiture process:

    a) provide to potential purchasers sufficient information as regards the Divestment Business; and

b) provide to potential purchasers sufficient information relating to the Personnel and allow them reasonable access to the Personnel.

Reporting

12. Thales shall submit written reports in English on potential purchasers of the Divestment Business and developments in the negotiations with such potential purchasers to the Commission and the Monitoring Trustee no later than [Redacted] after the end of every [Redacted] following the Effective Date (or otherwise at the Commission's request). Thales shall submit a list of all potential purchasers having expressed interest in acquiring the Divestment Business to the Commission at each and every stage of the divestiture process, as well as a copy of all the offers made by potential purchasers within [Redacted] of their receipt.

13. Thales shall inform the Commission and the Monitoring Trustee on the preparation of the data room documentation and the due diligence procedure and shall submit a copy of any information memorandum to the Commission and the Monitoring Trustee before sending the memorandum out to potential purchasers.

Section D. The Purchaser

14. In order to be approved by the Commission, the Purchaser must fulfil the following criteria:

a) The Purchaser shall be independent of and unconnected to the Parties (this being assessed having regard to the situation following the divestiture);

b) The Purchaser shall have the financial resources, proven expertise and incentive to maintain and develop the Divestment Business as a viable and active competitive force in competition with the Parties and other competitors;

c) The Purchaser shall be a player with significant experience in the HSM, or a closely related field, such as data security, enjoying a high level of trust and a good reputation in these areas among EEA-based customers. The Purchaser shall show by way of a business plan, at the Purchaser approval stage, that it has the ability and expertise, in using its own and the Divestment Business' assets, to reliably provide the relevant products and services to EEA customers, even for enterprise grade security applications and that it has sufficiently concrete plans to undertake (i) all necessary steps to achieve and continue achieving all certifications, and their updates, necessary to supply GP HSMs in the EEA; and (ii) the required R&D for the further development of the Divestment Business.

d) The acquisition of the Divestment Business by the Purchaser must neither be likely to create, in light of the information available to the Commission, *prima facie* competition concerns nor give rise to a risk that the implementation of the Commitments will be delayed. In particular, the Purchaser must reasonably be expected to obtain all necessary approvals from the relevant regulatory authorities for the acquisition of the Divestment Business.

15. The final binding sale and purchase agreement (as well as ancillary agreements) relating to the divestment of the Divestment Business shall be conditional on the Commission's approval. When Thales has reached an agreement with a proposed purchaser, it shall submit a fully documented and reasoned proposal, including a copy

of the final agreement(s), within [Redacted] to the Commission and the Monitoring Trustee. Thales must be able to demonstrate to the Commission that the proposed purchaser fulfils the Purchaser Criteria and that the Divestment Business is being sold in a manner consistent with the Commission's Decision and the Commitments. For the approval, the Commission shall verify that the proposed purchaser fulfils the Purchaser Criteria and that the Divestment Business is being sold in a manner consistent with the Commitments including their objective to bring about a lasting structural change in the market. The Commission may approve the sale of the Divestment Business without one or more Assets or parts of the Personnel, or by substituting one or more Assets or parts of the Personnel with one or more different assets or different personnel, if this does not affect the viability and competitiveness of the Divestment Business after the sale, taking account of the proposed purchaser.

Section E. Trustee

I. Appointment Procedure

16. Thales shall appoint a Monitoring Trustee to carry out the functions specified in these Commitments for a Monitoring Trustee. Thales commits not to close the Concentration before the appointment of a Monitoring Trustee.

17. If Thales has not entered into a binding sale and purchase agreement regarding the Divestment Business [Redacted] before the end of the First Divestiture Period or if the Commission has rejected a purchaser proposed by Thales at that time or thereafter, Thales shall appoint a Divestiture Trustee. The appointment of the Divestiture Trustee shall take effect upon the commencement of the Trustee Divestiture Period.

18. The Trustee shall:

a) at the time of appointment, be independent of Thales and Gemalto and their Affiliated Undertakings; and

b) possess the necessary qualifications to carry out its mandate, for example have sufficient relevant experience as an investment banker or consultant or auditor; and neither have nor become exposed to a Conflict of Interest.

19. The Trustee shall be remunerated by the Notifying Party in a way that does not impede the independent and effective fulfilment of its mandate. In particular, where the remuneration package of a Divestiture Trustee includes a success premium linked to the final sale value of the Divestment Business, such success premium may only be earned if the divestiture takes place within the Trustee Divestiture Period.

Proposal by Thales

20. No later than two weeks after the Effective Date, Thales shall submit the name or names of one or more natural or legal persons whom Thales proposes to appoint as the Monitoring Trustee to the Commission for approval. No later than one month before the end of the First Divestiture Period or on request by the Commission, Thales shall submit a list of one or more persons whom Thales proposes to appoint as Divestiture Trustee to the Commission for approval. The proposal shall contain sufficient information for the Commission to verify that the person or persons proposed as Trustee fulfil the requirements set out in paragraph 18 and shall include:

a) the full terms of the proposed mandate, which shall include all provisions necessary to enable the Trustee to fulfil its duties under these Commitments;

b) the outline of a work plan which describes how the Trustee intends to carry out its assigned tasks; and

c) an indication whether the proposed Trustee is to act as both Monitoring Trustee and Divestiture Trustee or whether different trustees are proposed for the two functions.

Approval or Rejection by the Commission

21. The Commission shall have the discretion to approve or reject the proposed Trustee(s) and to approve the proposed mandate subject to any modifications it deems necessary for the Trustee to fulfil its obligations. If only one name is approved, Thales shall appoint or cause to be appointed the person or persons concerned as Trustee, in accordance with the mandate approved by the Commission. If more than one name is approved, Thales shall be free to choose the Trustee to be appointed from among the names approved. The Trustee shall be appointed within one week of the Commission's approval, in accordance with the mandate approved by the Commission.

New Proposal by Thales

22. If all the proposed Trustees are rejected, Thales shall submit the names of at least two more natural or legal persons within one week of being informed of the rejection, in accordance with paragraphs 16 and 21 of these Commitments.

Trustee Nominated by the Commission

23. If all further proposed Trustees are rejected by the Commission, the Commission shall nominate a Trustee, whom Thales shall appoint, or cause to be appointed, in accordance with a trustee mandate approved by the Commission.

II. Functions of the Trustee

24. The Trustee shall assume its specified duties and obligations in order to ensure compliance with the Commitments. The Commission may, on its own initiative or at the request of the Trustee or Thales, give any orders or instructions to the Trustee in order to ensure compliance with the conditions and obligations attached to the Decision.

Duties and Obligations of the Monitoring Trustee

25. The Monitoring Trustee shall:

a) propose in its first report to the Commission a detailed work plan describing how it intends to monitor compliance with the obligations and conditions attached to the Decision.

b) oversee, in close co-operation with the Hold Separate Manager, the on-going management of the Divestment Business with a view to ensuring its continued economic viability, marketability and competitiveness and monitor compliance by Thales with the conditions and obligations attached to the Decision. To that end the Monitoring Trustee shall:

(i) monitor the preservation of the economic viability, marketability and competitiveness of the Divestment Business, and the keeping separate of the Divestment Business from the business retained by the Parties, in accordance with paragraphs 6 and 7 of these Commitments;

(ii) supervise the management of the Divestment Business as a distinct and saleable entity, in accordance with paragraph 8 of these Commitments;

(iii) with respect to Confidential Information:

— determine all necessary measures to ensure that Thales does not after the Effective Date obtain any Confidential Information relating to the Divestment Business,

— in particular strive for the severing of the Divestment Business' participation in a central information technology network to the extent possible, without compromising the viability of the Divestment Business,

— make sure that any Confidential Information relating to the Divestment Business obtained by Thales before the Effective Date is eliminated and will not be used by Thales and

— decide whether such information may be disclosed to or kept by Thales as the disclosure is reasonably necessary to allow Thales to carry out the divestiture or as the disclosure is required by law;

(iv) monitor the splitting of Assets and the allocation of Personnel between the Divestment Business and Thales or Affiliated Undertakings; propose to Thales such measures as the Monitoring Trustee considers necessary to ensure Thales's compliance with the conditions and obligations attached to the Decision, in particular the maintenance of the full economic viability, marketability or competitiveness of the Divestment Business, the holding separate of the Divestment Business and the nondisclosure of competitively sensitive information;

c) review and assess potential purchasers as well as the progress of the divestiture process and verify that, dependent on the stage of the divestiture process:

(i) potential purchasers receive sufficient and correct information relating to the Divestment Business and the Personnel in particular by reviewing, if available, the data room documentation, the information memorandum and the due diligence process, and

(ii) potential purchasers are granted reasonable access to the Personnel;

d) act as a contact point for any requests by third parties, in particular potential purchasers, in relation to the Commitments;

e) provide to the Commission, sending Thales a non-confidential copy at the same time, a written report within 15 days after the end of every month that shall

cover the operation and management of the Divestment Business as well as the splitting of assets and the allocation of Personnel so that the Commission can assess whether the business is held in a manner consistent with the Commitments and the progress of the divestiture process as well as potential purchasers;

f) promptly report in writing to the Commission, sending Thales a non-confidential copy at the same time, if it concludes on reasonable grounds that Thales is failing to comply with these Commitments;

g) within one week after receipt of the documented proposal referred to in paragraph 15 of these Commitments, submit to the Commission, sending Thales a non-confidential copy at the same time, a reasoned opinion as to the suitability and independence of the proposed purchaser and the viability of the Divestment Business after the Sale and as to whether the Divestment Business is sold in a manner consistent with the conditions and obligations attached to the Decision, in particular, if relevant, whether the Sale of the Divestment Business without one or more Assets or not all of the Personnel affects the viability of the Divestment Business after the sale, taking account of the proposed purchaser;

h) assume the other functions assigned to the Monitoring Trustee under the conditions and obligations attached to the Decision.

26. If the Monitoring and Divestiture Trustee are not the same legal or natural persons, the Monitoring Trustee and the Divestiture Trustee shall cooperate closely with each other during and for the purpose of the preparation of the Trustee Divestiture Period in order to facilitate each other's tasks.

Duties and Obligations of the Divestiture Trustee

27. Within the Trustee Divestiture Period, the Divestiture Trustee shall sell at no minimum price the Divestment Business to a Purchaser, provided that the Commission has approved both the Purchaser and the final binding sale and purchase agreement (and ancillary agreements) as in line with the Commission's Decision and the Commitments in accordance with paragraphs 14 and 15 of these Commitments. The Divestiture Trustee shall include in the sale and purchase agreement (as well as in any ancillary agreements) such terms and conditions as it considers appropriate for an expedient sale in the Trustee Divestiture Period. In particular, the Divestiture Trustee may include in the sale and purchase agreement such customary representations and warranties and indemnities as are reasonably required to effect the sale. The Divestiture Trustee shall protect the legitimate financial interests of Thales, subject to the Notifying Party's unconditional obligation to divest at no minimum price in the Trustee Divestiture Period.

28. In the Trustee Divestiture Period (or otherwise at the Commission's request), the Divestiture Trustee shall provide the Commission with a comprehensive monthly report written in English on the progress of the divestiture process. Such reports shall be submitted within 15 days after the end of every month with a simultaneous copy to the Monitoring Trustee and a non-confidential copy to the Notifying Party.

III. <u>Duties and Obligations of the Parties</u>

29. Thales shall provide and shall cause its advisors to provide the Trustee with all such co-operation, assistance and information as the Trustee may reasonably require to perform its tasks. The Trustee shall have full and complete access to any of Thales' or the Divestment Business' books, records, documents, management or other personnel, facilities, sites and technical information necessary for fulfilling its duties under the Commitments and Thales and the Divestment Business shall provide the Trustee upon request with copies of any document. Thales and the Divestment Business shall make available to the Trustee one or more offices on their premises and shall be available for meetings in order to provide the Trustee with all information necessary for the performance of its tasks.

30. Thales shall provide the Monitoring Trustee with all managerial and administrative support that it may reasonably request on behalf of the management of the Divestment Business. This shall include all administrative support functions relating to the Divestment Business which are currently carried out at headquarters level. Thales shall provide and shall cause its advisors to provide the Monitoring Trustee, on request, with the information submitted to potential purchasers, in particular give the Monitoring Trustee access to the data room documentation and all other information granted to potential purchasers in the due diligence procedure. Thales shall inform the Monitoring Trustee on possible purchasers, submit lists of potential purchasers at each stage of the selection process, including the offers made by potential purchasers at those stages, and keep the Monitoring Trustee informed of all developments in the divestiture process.

31. Thales shall grant or procure Affiliated Undertakings to grant comprehensive powers of attorney, duly executed, to the Divestiture Trustee to effect the sale (including ancillary agreements), the Closing and all actions and declarations which the Divestiture Trustee considers necessary or appropriate to achieve the sale and the Closing, including the appointment of advisors to assist with the sale process. Upon request of the Divestiture Trustee, Thales shall cause the documents required for effecting the sale and the Closing to be duly executed.

32. Thales shall indemnify the Trustee and its employees and agents (each an "***Indemnified Party***") and hold each Indemnified Party harmless against, and hereby agrees that an Indemnified Party shall have no liability to Thales for, any liabilities arising out of the performance of the Trustee's duties under the Commitments, except to the extent that such liabilities result from the wilful default, recklessness, gross negligence or bad faith of the Trustee, its employees, agents or advisors.

33. At the expense of Thales, the Trustee may appoint advisors (in particular for corporate finance or legal advice), subject to Thales' approval (this approval not to be unreasonably withheld or delayed) if the Trustee considers the appointment of such advisors necessary or appropriate for the performance of its duties and obligations under the Mandate, provided that any fees and other expenses incurred by the Trustee are reasonable. Should Thales refuse to approve the advisors proposed by the Trustee the Commission may approve the appointment of such advisors instead, after having heard Thales. Only the Trustee shall be entitled to issue instructions to the advisors. Paragraph 32 of these Commitments shall apply *mutatis mutandis*. In the Trustee Divestiture Period, the Divestiture Trustee may use advisors who served Thales during the Divestiture Period if the Divestiture Trustee considers this in the best interest of an expedient sale.

34. Thales agrees that the Commission may share Confidential Information proprietary to Thales with the Trustee. The Trustee shall not disclose such information and the principles contained in Article 17 (1) and (2) of the Merger Regulation apply *mutatis mutandis*.

35. Thales agrees that the contact details of the Monitoring Trustee are published on the website of the Commission's Directorate-General for Competition and they shall inform interested third parties, in particular any potential purchasers, of the identity and the tasks of the Monitoring Trustee.

36. For a period of 10 years from the Effective Date the Commission may request all information from the Parties that is reasonably necessary to monitor the effective implementation of these Commitments.

IV. Replacement, Discharge and Reappointment of the Trustee

37. If the Trustee ceases to perform its functions under the Commitments or for any other good cause, including the exposure of the Trustee to a Conflict of Interest:

a) the Commission may, after hearing the Trustee and Thales, require Thales to replace the Trustee; or

b) Thales may, with the prior approval of the Commission, replace the Trustee.

38. If the Trustee is removed according to paragraph 37 of these Commitments, the Trustee may be required to continue in its function until a new Trustee is in place to whom the Trustee has effected a full hand over of all relevant information. The new Trustee shall be appointed in accordance with the procedure referred to in paragraphs 16-23 of these Commitments.

39. Unless removed according to paragraph 37 of these Commitments, the Trustee shall cease to act as Trustee only after the Commission has discharged it from its duties after all the Commitments with which the Trustee has been entrusted have been implemented. However, the Commission may at any time require the reappointment of the Monitoring Trustee if it subsequently appears that the relevant remedies might not have been fully and properly implemented.

Section F. The Review Clause

40. The Commission may extend the time periods foreseen in the Commitments in response to a request from Thales or, in appropriate cases, on its own initiative. Where Thales requests an extension of a time period, it shall submit a reasoned request to the Commission no later than one month before the expiry of that period, showing good cause**.** This request shall be accompanied by a report from the Monitoring Trustee, who shall, at the same time send a non-confidential copy of the report to the Notifying Party. Only in exceptional circumstances shall Thales be entitled to request an extension within the last month of any period.

41. The Commission may further, in response to a reasoned request from the Notifying Party showing good cause waive, modify or substitute, in exceptional circumstances, one or more of the undertakings in these Commitments. This request shall be accompanied by a report from the Monitoring Trustee, who shall, at the same time send a non-confidential copy of the report to the Notifying Party. The request shall not have the effect of suspending the application of the undertaking and, in particular, of

suspending the expiry of any time period in which the undertaking has to be complied with.

Section G. Entry Into Force

42. The Commitments shall take effect upon the date of adoption of the Decision.

duly authorised for and on behalf of Thales

SCHEDULE

1. The Divestment Business currently is operated by Thales and sits within the Thales eSecurity business unit. This business unit encompasses three legal entities globally that are active in various areas including but not limited to GP HSMs, namely: [Redacted].

2. In order to implement the Divestment, Thales will [Redacted].

3. In accordance with paragraph 5 of these Commitments, the Divestment Business includes, but is not limited to:

   a) A transfer of the following main tangible assets: [Redacted] sites (in the form of lease assignments), as well as all finished goods inventory, supplies, tooling, test equipment, sales and promotional material, product documentation, and user manuals relating to the Divestment Business held at the date of Closing;

   b) A transfer, or license (as appropriate), of the following main intangible assets:

      (i) All registered nShield, nCipher, and CodeSafe trademarks listed in **Annex 1** along with all patents that are necessary for the operation of (or otherwise used by) the Divestment Business;

      (ii) All additional unregistered intellectual property including know-how, testing procedures, manufacturing procedures, product design, trade secrets, source code, and associated utilities and libraries (including product specifications and quality control standards);

      (iii) All nShield product SKUs listed in the nShield price list attached as **Annex 2**;

      (iv) An assignment of the section of any and all inbound licenses that are necessary for the operation of (or otherwise used by) the Divestment Business. These include the licenses listed in **Annex 3**;

      (v) All documentation associated with research and development for products currently marketed (or intended to be marketed) under the nShield brand.

      For the avoidance of doubt, for those intangible assets that do not exclusively relate to the Divestment Business (*e.g.*, existing R&D or intellectual property rights relating to Payment HSMs, key management products, or encryption software products), Thales will, for each intangible asset, either (i) where the intangible asset relates primarily to products outside the Divestment Business, retain ownership of the intangible asset and provide the Purchaser with access to and use of this intangible asset as is reasonably necessary for the Purchaser to maintain the viability of the Divestment Business; or (ii) where the intangible asset relates primarily to products that are part of the Divestment Business, transfer the intangible asset and obtain from the Purchaser access to and use of this intangible asset as is reasonably necessary for Thales to operate its retained businesses. To the extent the Purchaser notifies Thales that they require additional intangible Thales assets which relate primarily to products

outside the Divestment Business and which are not reasonably necessary for the Purchaser to maintain the viability of the Divestment Business, Thales shall provide access to such assets if the assets are used by the Divestment Business and reasonably needed for the operation of the Divestment Business. The Monitoring Trustee shall supervise Thales' performance in this regard, in accordance with Section E of the Commitments.

c) A transfer of, or access to, as appropriate, all licenses, permits, certifications (as listed in **Annex 4**), and authorisations issued by any governmental or other regulatory organization that are necessary to manufacture and/or sell the products belonging to the Divestment Business, including any dossiers relating to current or pending authorisations available to Thales and, where necessary, assistance related to the transfer to the Purchaser in transferring such licences, permits, certifications, and authorisations concerning the Divestment Business.

d) A transfer of any additional contracts, agreements, leases, commitments, and understandings that relate exclusively to the Divestment Business (including the active nShield Master Agreements listed in **Annex 5**). To the extent certain contracts, agreements, leases, commitments, and understandings relevant to the Divestment Business are not exclusively related to the Divestment Business, Thales shall use its best efforts to sub-divide these contracts and transfer the portions relating to the Divestment Business to the Purchaser or otherwise ensure that the Purchaser is able to enter into comparable new contracts, agreements, leases, commitments, and understandings in relation to the products belonging to the Divestment Business.

e) A transfer of the following customer, credit and other records to the extent exclusively related to the Divestment Business: Thales' existing contracts with customers globally relating to the products of the Divestment Business, Thales' customer lists, and customer records as they relate to the Divestment Business. To the extent that any such records relate partially to the Divestment Business, the portion of the records relevant to the Divestment Business shall be transferred to the Purchaser to the extent the Purchaser requires them.

f) All Key Personnel, as listed in **Annex 6**;

g) All Personnel related to the products belonging to the Divestment Business, as outlined in **Annex 7** and **Annex 8**. Thales estimates that this will include a total of [Redacted] employees (depending on the number of employees required by the Purchaser).

Thales is also prepared to provide transitional services to the Purchaser for a period to be agreed with the Purchase and pursuant to transition services agreements. At the Purchaser's option, such services would cover [Redacted].

4. The Divestment Business shall not include:

a) tangible and intangible assets (including intellectual property rights) which do not contribute to the current operation of the Divestment Business;

b) the Thales company name, mark, or logo in any form;

c) any personnel other than the Key Personnel and the Personnel;

d) books and records required to be retained pursuant to any statute, rule, regulation or ordinance, provided that copies of such documents necessary for the Divestment Business shall be provided to the Purchaser, upon request; and

e) general books of account and books of original entry that comprise Thales' or an Affiliated Undertaking's permanent accounting or tax records provided that copies of such documents necessary for the Divestment Business shall be provided to the Purchaser, upon request.

5. To the extent that any assets or personnel are identified at a later point in time that are not covered by paragraph 3 of this Schedule but which are used (exclusively or not) by the Divestment Business and necessary for the continued viability and competitiveness of the Divestment Business, any such assets or adequate substitutes will be offered to the Purchaser.

6. The Monitoring Trustee shall supervise Thales' implementation of this Schedule, in accordance with Section E of the Commitments.

List of Annexes

Annex 1	List of registered nShield, nCipher, and CodeSafe trademarks
Annex 2	List of nShield product SKUs
Annex 3	List of main inbound licenses related to the products of the Divestment Business
Annex 4	List of certifications related to the products of the Divestment Business
Annex 5	List of active nShield Master Agreements
Annex 6	List of Key Personnel
Annex 7	Overview of Personnel
Annex 8	List of Personnel