EN

Case No COMP/M.6564 - ARM/ GIESECKE & DEVRIENT/ GEMALTO/ JV

Only the English text is available and authentic.

REGULATION (EC) No 139/2004
MERGER PROCEDURE

Article 6(1)(b) in conjunction with Art 6(2)
Date: 06/11/2012

In electronic form on the EUR-Lex website under document number 32012M6564

Office for Publications of the European Union
L-2985 Luxembourg

EUROPEAN COMMISSION

Brussels, 6.11.2012
C(2012) 8106 final

In the published version of this decision, some information has been omitted pursuant to Article 17(2) of Council Regulation (EC) No 139/2004 concerning non-disclosure of business secrets and other confidential information. The omissions are shown thus […]. Where possible the information omitted has been replaced by ranges of figures or a general description.

PUBLIC VERSION

MERGER PROCEDURE
ARTICLE 6(1)(b) IN CONJUNCTION WITH ARTICLE 6(2) DECISION

To the notifying parties:

Dear Sir/Madam,

Subject: Case No COMP/M.6564 – ARM/ GIESECKE & DEVRIENT/ GEMALTO/ JV
Commission decision pursuant to Article 6(1)(b) in conjunction with Article 6(2) of Council Regulation No 139/2004[1]

1. On 15 June 2012, the European Commission received a notification of a proposed concentration pursuant to Article 4 of Council Regulation (EC) No 139/2004[2] by which the undertakings ARM Limited ("ARM", UK), Giesecke & Devrient GmbH ("G&D", Germany) and Gemalto N.V. ("Gemalto", Netherlands and, together with ARM and G&D, the "notifying parties") will create a new joint venture (the "JV").

2. This notification was, however, withdrawn by the notifying parties on 3 July 2012.

3. On 14 September 2012, the Commission received a re-notification of the proposed concentration pursuant to Article 4 of Council Regulation (EC) No 139/2004.

I. THE PARTIES AND THE JV

4. **ARM**. ARM is a semiconductor intellectual property ("IP") supplier. In particular, ARM licenses IP for application processors ("APs"). ARM's IP for AP is licensed with an integrated security feature called "TrustZone". TrustZone consists of a

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 will be used throughout this decision.

2 OJ L 24, 29.1.2004, p. 1 (the "Merger Regulation").

hardware extension integrated into AP's core design that provides the means to implement a Trusted Execution Environment ("TEE") by being able to create two separate spaces (one considered "non-secure" and the other "secure") within a single AP and enforcing a strict separation between the two spaces. A TEE is a security solution that provides a separate execution environment for use by trusted applications (that is to say applications which offer enhanced security for more personalized and, therefore, more valued, services to users)[3] on consumer electronic ("CE") devices, which include an AP.[4] A TEE creates a secure operating system ("OS") running alongside the main OS, but isolated through hardware-enforced separation.

5. **G&D**. G&D is active in security solutions for the production and processing of banknotes and in the provision of secure elements ("SEs"). G&D has also developed a TEE software solution, MobiCore. MobiCore is designed to work with TrustZone-enabled APs. It is based on G&D's proprietary Application Programming Interface ("API") set and does not comply with the standards published so far by the independent industry standards organization GlobalPlatform.[5] MobiCore was commercially released in May 2012. However […].[6]

6. **Gemalto**. Gemalto is a digital security company that provides secure personal devices, such as SEs and tokens, and Near Field Communication ("NFC") solutions.[7] In 2009, Gemalto acquired the company Trusted Logic S.A. ("Trusted Logic"), which had developed a TEE software solution, Trusted Foundations. Gemalto's solution was the first TEE solution for TrustZone-enabled APs to become commercially available. Trusted Foundations complies with the industry standards so far adopted by GlobalPlatform. Gemalto's revenues from Trusted Foundations have so far been limited (around EUR […] in 2011).[8]

7. **JV**. The JV will develop and market a TEE solution. The JV aims at responding to the increasing customer demand for security solutions for CE devices by combining

---

3 Trusted applications typically entail accessing or processing sensitive information and, as a result, require an enhanced level of security. Examples of potential trusted applications include mobile payment and banking applications, content management applications and corporate access applications.

4 A wide variety of CE devices contain APs, including smartphones, tablets, eReaders, netbooks, automotive navigation devices, gaming consoles, digital TVs, and in-car-entertainment systems.

5 Founded in 1999, GlobalPlatform is a cross-industry, not-for-profit membership association with currently over 80 company members including semiconductor IP providers and chip manufacturers, software developers, OEMs, MNOs, and service providers. It identifies, develops and publishes specifications facilitating the secure and interoperable deployment and management of multiple embedded applications on secure chip technology. It is active, among other things, in developing standards for TEE solutions. More information on GlobalPlatform is available on GlobalPlatform's website, at http://www.globalplatform.org/.

6 G&D has entered into contracts […].

7 Gemalto was formed in 2006 by the combination of two companies, Axalto Holding N.V. and Gemplus International S.A. This transaction was authorized by the Commission on 19 May 2006 (Case COMP/M.3998 - *Axalto/Gemplus*).

8 2012 revenues are estimated at around EUR […]and 2013-2015 revenues are estimated at around EUR […]. As of today, Gemalto has entered into contracts with […].

Gemalto's and G&D's activity in the development and marketing of TEE solutions for use with APs embodying ARM's TrustZone technology.

II. THE CONCENTRATION

8. ***Joint control.*** The agreement bringing about the JV (the "JV Agreement") attributes to each shareholder […] veto rights over strategic decisions […]. Further, the JV Agreement establishes that ARM will hold 40% of the JV's equity and each of G&D and Gemalto will own 30% of the JV's equity. Hence, each of the notifying parties to the JV will have veto rights over the JV's strategic decisions.

9. For these reasons, it can be concluded that ARM, G&D, and Gemalto will exercise joint control over the JV.

10. ***Full function joint venture***. The JV qualifies as a full-function joint venture as it will operate on the market autonomously from its parent companies, performing all the functions of undertakings normally active on the same market. In more detail:

    a) The JV will sell TEE solutions primarily to third parties, such as Original Equipment Manufacturers ("OEMs") of CE devices and semiconductor manufacturers. It will also sell the cryptographic keys to its TEE solution primarily to third parties, including OEMs, Mobile Network Operators ("MNOs") and Trusted Service Managers ("TSMs"). While Gemalto and G&D may become resellers of TEE solutions for the JV, the JV will likely not depend on sales to its parent companies.

    b) The JV will have its own management. A board of directors will be appointed which will have all powers required to control and manage the JV's business and the JV will have a management team, including a chief executive officer, which will be responsible for the implementation of the strategy and day-to-day management.

    c) The JV will have a dedicated team of employees. ARM will provide […] employees, G&D will provide […] employees, and Gemalto will provide […] employees. The employees include research and development ("R&D") and software engineers, security architects, project managers, product managers, business developers, market engineers, and directors of marketing.

    d) The JV will have adequate funding to perform its activities. It will be financed initially out of the proceeds of the share subscriptions until it starts generating its own revenues from commercialising its products.

    e) The JV will have access to sufficient assets and infrastructure to allow it to operate on a lasting basis. G&D will transfer assets and rights relating to its TEE technology, including: (1) certain hardware and development software; (2) all know how, trade secrets, techniques, information expertise and proprietary knowledge; (3) business records; (4) claims; and (5) certain IP rights, including business trademarks, and patents. G&D will also transfer to the JV certain contracts related to its TEE business. Gemalto will sell to the JV all its shares in Trusted Logic, the Gemalto subsidiary active in the development and marketing of TEE solutions. Trusted Logic is also the owner of certain IP rights, including business trademarks and patents.

    f) The JV will be formed for an indefinite period.

11. For the above reasons, the proposed transaction leads to the creation of a joint venture performing on a lasting basis all the functions of an autonomous economic entity within the meaning of Article 3(4) of the Merger Regulation.

12. The transaction constitutes a concentration within the meaning of Article 3(1)(b) of the Merger Regulation.

III. UNION DIMENSION

13. The undertakings concerned have a combined aggregate worldwide turnover for the year 2011 of more than EUR 2 500 million[9] (ARM: EUR 567 million, G&D: EUR 1 635 million, Gemalto: EUR 2 015 million). In the same year, the combined aggregate turnover of the parties was more than EUR 100 million in each of at least three Member States (France - ARM: EUR […], G&D: EUR […], Gemalto: EUR […]; Germany - ARM: EUR […], G&D: EUR […], Gemalto: EUR […]; the United Kingdom - ARM: EUR […], G&D: EUR […], Gemalto: EUR […]). In each of these three Member States, the aggregate turnover of at least two of the Parties (that is to say […]) was more than EUR 25 million (France – […]: EUR […]; Germany – […]; the United Kingdom – […]). The aggregate Union-wide turnover of each of at least two of the parties (that is to say […]) was more than EUR 100 million, and none of the parties achieve more than two-thirds of their aggregate Union-wide turnover within one and the same Member State.

14. The notified operation therefore has a Union dimension within the meaning of Article 1(3) of the Merger Regulation.

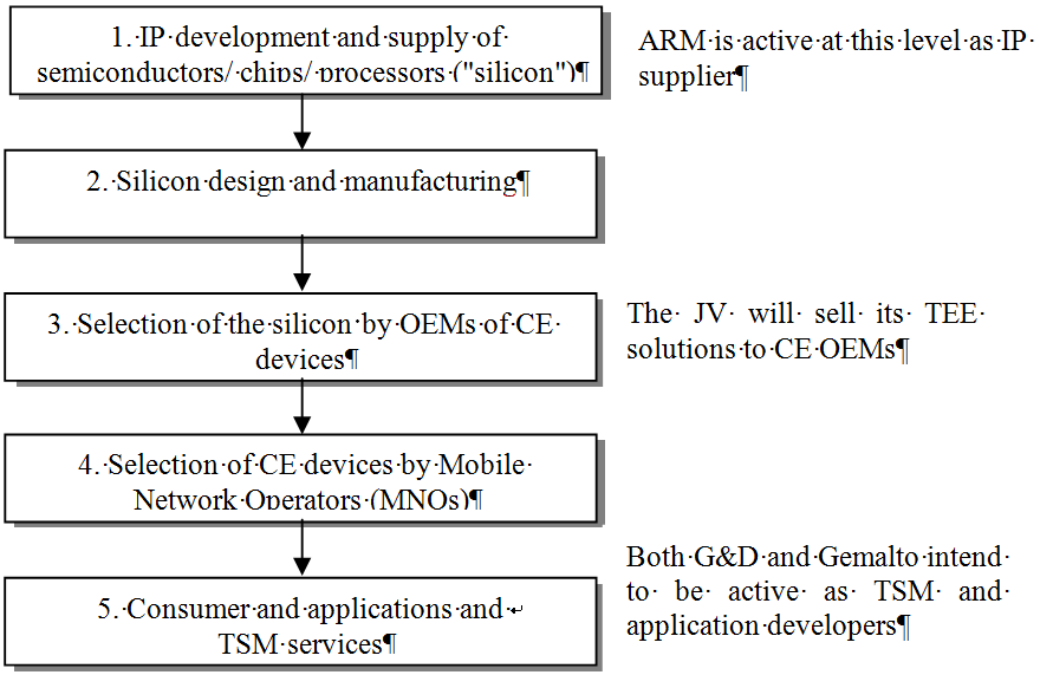
IV. RELEVANT MARKETS

1. INTRODUCTION

1.1. Industry value chain

15. The main stages of the value chain for a CE device can be summarised as follows. This description uses smartphones as an example.

9 Turnover calculated in accordance with Article 5(1) of the Merger Regulation and the Commission Consolidated Jurisdictional Notice (OJ C 95, 16.4.2008, p. 1).



16. ***Developers and suppliers of IP for semiconductors***. Semiconductor manufacturers increasingly tend to outsource the IP from third-party IP developers instead of developing their own proprietary technology. Semiconductor IP suppliers, such as ARM, MIPS, and Rambus research and develop technology for semiconductors. The IP is generally licensed to semiconductor manufacturers or foundries that use it in the development and manufacture of their chipsets and processors.

17. ***Semiconductor manufacturers.*** Semiconductor manufacturers design and manufacture chipsets and their components, including APs. The AP is the device's primary chipset. At the outset of the design process, semiconductor manufacturers choose the technology most suitable for the proposed final use of the product. In addition to the AP architecture, the design of a chipset requires the selection of other technologies or components to be embedded in the processor. At this stage, semiconductor manufacturers are free to adopt all or some of the functionalities (including security) that a given IP offers.

18. ***OEMs select the silicon, security solutions, and pre-issuance trusted applications.*** OEMs purchase from semiconductor manufacturers processors that correspond to their CE devices' needs in terms of performance, functionality, and software requirements. Semiconductor manufacturers generally design their chipsets to support many different software products (mainly OSs), so OEMs are free to select which OS and software to install on the chipsets. At this stage, OEMs also select which security solution(s) to install on their CE devices. Which technology or combination of technologies is the most appropriate will depend on the level of security required. At this level of the value chain, OEMs may also decide to pre-install certain applications, including trusted applications, (developed by the OEM itself or licensed from a third party) on their CE devices ("pre-issuance" trusted applications). For technical reasons, pre-issuance applications cannot, in principle, be uninstalled.

19. ***MNOs select the CE device/ smartphone.*** MNOs stock CE devices according to their price, capabilities, and several other factors. During the negotiations with OEMs, MNOs may request OEMs to add software, services, and pre-issuance

applications or to remove software (including security software, such as TEE) and/or pre-issuance applications previously installed by the OEM.

20. ***Service providers (for example, credit card companies) mandate application developers to develop post-issuance trusted applications (for example, payment applications), which are managed by TSMs.*** Trusted applications can be downloaded from online application stores (for example, Apple App Store, Google Play, BlackBerry App World, Windows Phone 7 Marketplace) by the end user after the device has been shipped ("post-issuance" trusted applications). Installing post-issuance trusted applications requires the intervention of a TSM provider who, on behalf of the service provider, installs, personalizes, and provides lifecycle management of the trusted side of a post-issuance application. End users are free to uninstall any post-issuance application.

1.2. The JV's and the notifying parties' activities

21. ARM is active in the development and supply of IP for APs for CE devices, including the design of the necessary hardware extension (TrustZone) to incorporate the JV's TEE into these APs.

22. The JV will be principally active at the level of the value chain where the marketing of security solutions takes place, that is, at the level of semiconductor manufacturers and OEMs who incorporate security solutions into their chipsets/ CE devices. The JV will develop and market a TEE designed to work on AP chipsets containing ARM’s TrustZone technology.

23. The JV’s business model will be two-fold. First, the JV will license TEEs to OEMs and, to a lesser extent, semiconductor manufacturers, for use on chips with TrustZone. The JV also plans to supply and market (mainly to OEMs and MNOs) pre-issuance trusted applications (the "pre-issuance" business model).

24. Second, the JV will sell cryptographic keys to its TEE solution so that trusted applications can be installed when demanded by consumers (the "post-issuance" business model). For a trusted application to execute in a device equipped with the JV’s TEE, the JV will need to create a secure space, or container, into which the trusted application can be installed within the TEE of a given CE device and where the trusted application will safely execute. The container is created through the JV generating a cryptographic key that is specific to the CE device.

25. With respect to the post-issuance business model, the notifying parties submit that OEMs/MNOs, which are the principal decision-makers in relation to the security options on CE devices, will insist to control the keys to access the JV's TEE. Therefore, they are likely to be the JV’s (direct) customers with respect to such keys. The OEMs/MNOs would then make the keys available to application providers (either directly or via TSMs mandated by these application providers) so that trusted applications can be installed on devices supporting the JV's TEE solutions. The notifying parties submit that application providers will pay the TSM to deploy and manage trusted applications on a per-application, per-device, or per-transaction basis, depending on the application and the CE device concerned. The TSM will request a security domain for applications from the OEM/MNO and pay the OEM/MNO an activation fee for each security domain that the TSM will manage. Application providers who perform the role of TSM themselves will simply pay the OEM/MNO an activation fee, as if they were third-party TSMs.

26. The JV does not plan to be active in the development of post-issuance trusted applications or TSM services.

27. Each of Gemalto and G&D will engage in the development of post-issuance trusted applications running on top of the JV's TEE solution, as well as in the provision of TSM services for, amongst others, the JV's TEE solution. In addition, each of Gemalto and G&D will continue to be active, among other things, in the provision of SEs, such as smart cards.

2. PRODUCT MARKET DEFINITIONS

2.1. AP-based security solutions for CE devices

View of the notifying parties

28. The JV will be active in TEEs, which is a type of AP-based security solution for CE devices. The notifying parties submit that other AP-based security solutions include:

a) Virtualization software. This technology isolates two or more software environments from each other to enhance security and reliability of the overall system. Virtualization creates parallel "worlds" in which an OS, applications and data reside. These parallel "worlds" exist side-by-side on the AP. They are separated from each other by the hypervisor - a layer of software - which is the heart of virtualization technology. Virtualization software includes Type 1 virtualization solutions where the hypervisor runs directly on the hardware and Type 2 virtualization solutions where the hypervisor runs inside the main operating system.

b) Custom integrated hardware/software modules. They provide specialized functionality in hardware alongside the rest of the AP system.

c) OS-based security solutions. They consist of security features built into the OS installed on a given device, such as Android, iOS or Windows Phone, including process and file access controls, permission-based protections, data protection frameworks or isolation mechanisms and/or the removal of non-essential tools and applications that might provide potential back-door access to threats.

d) Application software security solutions. These solutions include software obfuscation, white box cryptography and application wrapping, as well as endpoint software security solutions such as anti-virus or anti-malware solutions.

29. The notifying parties submit that the relevant product market includes all the above listed AP-based security solutions for CE devices or, at least, TEE and virtualization solutions.

30. The notifying parties further submit that: (1) mobile media content delivery; (2) mobile banking, mobile payment and e-commerce solutions; and (3) enterprise data solutions are the type of (trusted) applications, which will likely require additional security in the CE devices. Based on the notifying parties' submissions,[10] it appears that virtualization can be a full substitute for all three types of applications. While

10 Replies to the Commission's request for information sent on 29 August 2012, question 5.

not allowing for post-issuance download, custom integrated hardware/software modules can be a substitute for mobile media content delivery applications and mobile banking/ payment solutions. Conversely, OS-based solutions as well as application software security solutions, do not appear to be a substitute for mobile media content delivery, and would require complementary solutions for mobile banking/ payment applications and enterprise data solutions.

31. In any event, the notifying parties submit that it is not necessary to take a view as to the exact scope of the relevant product market as the proposed transaction would not give rise to competition concerns even on the narrowest possible product market definition, that is, TEE solutions for AP for CE devices. Furthermore, in their presentation to the Commission of 4 October 2012, the notifying parties submitted that they "*do not contest the Commission's analysis of the transaction (for Phase I purposes) on a narrow market for TEEs.*"[11] They submit, however, that the non-confidential versions of the key responses to the second market investigation made available to the notifying parties on 1 October 2012 confirm that TEEs compete - depending on application/use case - with other AP-based security solutions, that will "exert competitive constraints on TEE providers."

Commission's assessment

32. In light of the market investigation on the whole, the Commission has not been able to confirm the notifying parties' claim that TEE solutions are substitutable with other AP-based security solutions for CE devices, such as virtualization, custom integrated hardware/software modules, OS-based security, and application software security solutions. The investigation carried out by the Commission when the proposed transaction was first notified (the “first market investigation”) produced mixed results with respect to the question whether the relevant product market is wider than just TEE solutions.[12] The market investigation carried out by the Commission when the proposed transaction was re-notified (the “second market investigation”) contained more focused questions with respect to the definition of the relevant product market. Moreover, the number of respondents to the second market investigation was higher than the number of respondents to the first market investigation. The majority of the respondents to the second market investigation indicated that TEE solutions may not be, or may be only partially, substitutable with other AP-based security solutions.[13] In the words of one respondent: "[n]*on-TEE solutions are not direct substitutes for TEE solutions of the type proposed by the planned Joint Venture.*"[14]

---

11 Cleary Gottlieb Steen & Hamilton LLP, presentation entitled "State of Play Meeting", 4 October 2012, slide 3.

12 Customers' replies to the Commission's request for information sent on 21 June 2012, question 12; Competitors' replies to the Commission's request for information sent on 21 June 2012, question 17 and TSM's replies to the Commission's request for information sent on 21 June 2012, question 9.

13 Replies to question 3 of each following: Competitors' replies to the Commission's request for information sent on 17 September 2012; Customers' replies to the Commission's request for information sent on 7 September 2012; TSM's replies to the Commission's request for information sent on 17 September 2012; and MNO's replies to the Commission's request for information sent on 13 September 2012

14 Customers' replies to the Commission's request for information sent on 17 September 2012, response by Apple Inc. to question 3.

33. Several respondents to the second market investigation indicated that whether TEE solutions are substitutable with other AP-based security solutions depends on a number of factors, including their security level, cost, processing speed capability and accessible memory space required by different types of trusted applications.[15]. They indicated that, at least for some types of trusted applications, TEE solutions are likely to be (or to become in the near future) the only or, in any event, the most attractive, security solution on CE devices.[16]

34. The second market investigation was very clear in that OS-based security solutions, as well as application software security solutions, do not achieve the level of security necessary for any of the trusted applications expected to drive the market adoption of TEE solutions. As one respondent pointed out, these solutions "*are not appropriate for* [mobile banking/ payment, eCommerce, media content delivery, or enterprise data solutions applications] *because SW* [software] *only solutions are relatively breakable compared to HW* [hardware] *assisted solutions, and therefore service providers do not prefer OS-based security solutions.*"[17]

35. While custom integrated, separate hardware/software modules may achieve comparable levels of security, they tend to be less flexible and typically run at lower speed than an AP, which results in these modules not having the same level of performance as TEE solutions.[18] Moreover, developers of TEE solutions pointed out that a TEE solution is considerably cheaper than such custom developments.[19]

36. As regards virtualization solutions, the second market investigation indicated that such solutions, in particular those using a Type I hypervisor,[20] are closer to TEE solutions than other AP-based security solutions, at least with respect to certain types of applications such as trusted enterprise applications. However, when asked to compare TEE solutions with Type I virtualization solutions, which are considered to be more secure than Type II virtualization solutions, the majority of the respondents to the market investigations indicated that they do not believe that these solutions can achieve the same level of security, which is the primary purpose for implementing an AP-based security solution:[21] "*Google's understanding is that type*

---

15 Competitors' and Customers' replies to the Commission's request for information sent on 17 September 2012, question 3.

16 Customers' replies to the Commission's request for information sent on 17 September 2012 to questions 3.1.

17 Customers' replies to the Commission's request for information sent on 17 September 2012, response by Samsung Electronics Co. Ltd. to questions 3.4 and 3.5.

18 Customers' replies to the Commission's request for information sent on 17 September 2012, response by Texas Instruments France S.A. to question 3.3.

19 Competitors' replies to the Commission's request for information sent on 17 September 2012, responses by Solacia and Sierraware LLC. to question 3.3.

20 Please see paragraph 28.a) above for a definition of "hypervisor" and a short explanation of type I and type II virtualization software.

21 Replies to question 6.2 of each of the following: Competitors' replies to the Commission's request for information sent on 17 September 2012; Customers' replies to the Commission's request for information sent on 17 September 2012; TSM's replies to the Commission's request for information sent on 7

1 [and type 2] *virtualization solutions do not provide a security functionality comparable with TEE solutions, when they are used on their own without a TEE solution.*"[22]. Apple stated that: "[a]*lthough hypervisor solutions are the closest substitutes for TEE solutions, any security solution that relies on a single execution environment that shares resources (such as physical memory) is susceptible to serious security breaches. A physically separate execution environment is ideal, which makes TEE solutions ideal from a security standpoint*."[23] Semiconductor manufacturer Texas Instruments pointed out that "[v]*irtualization provides an isolation solution between several OSs but does not bring anywhere near the same level of security as a TEE. Virtualization does not provide the level of security and does not provide hardware based security required by trusted applications* […]."[24] Moreover, the majority of respondents, which expressed an opinion on this issue, do not believe that TEE and virtualisation solutions have a similar cost, with costs associated to virtualization likely to be higher than those associated with a TEE solution.[25]

37. In light of the above and on the basis of the facts available in the first phase of the investigation, the Commission considers that the existence of a narrow product market limited to TEE solutions cannot be excluded. At the same time, since the TEE business is at a nascent stage, it is likely that certain AP-based security solutions, including notably Type I virtualization solutions, may exercise, particularly in the short term during which TEE solutions need to gain market adoption, a competitive constraint upon TEE solutions, at least with respect to types of trusted applications currently using such AP-based security solution (an example being enterprise data solutions using Type I virtualization software).

38. For the purposes of this decision, it can therefore be concluded that the provision of TEE solutions may constitute a separate market from other AP-based security solutions. As a result, the Commission will conduct its competitive assessment also on a possible product market comprising the supply of TEE services only.

September 2012 and MNO's replies to the Commission's request for information sent on 13 September 2012.

22 Customers' replies to the Commission's request for information sent on 17 September 2012, response by Google Inc. to question 3.

23 Customers' replies to the Commission's request for information sent on 17 September 2012, response by Apple Inc. to questions 3.1 and 3.2.

24 Customers' replies to the Commission's request for information sent on 17 September 2012, response by Texas Instruments France S.A. to questions 3.1 and 3.2.

25 Replies to question 6.4 of each of the following: Competitors' replies to the Commission's request for information sent on 17 September 2012; Customers' replies to the Commission's request for information sent on 17 September 2012; TSM's replies to the Commission's request for information sent on 7 September 2012 and MNO's replies to the Commission's request for information sent on 13 September 2012.

2.2. SEs

View of the notifying parties

39. The notifying parties submit that, consistent with the Commission's findings in the *Axalto/Gemplus* decision,[26] AP-based security solutions for CE devices should be distinguished from SEs where the Commission identified a separate product segment for secure smart cards, which may be further sub-divided based on the technology used in the chip (memory or microprocessor) and the application of the card.

40. An SE can be defined as a secure processing element running sensitive code on a chip different from the main AP. Unlike AP-based security solutions, SEs therefore have very limited interaction with the AP and the OS of the device, as they normally have their own microprocessor and OS. SEs can be built into small removable memory cards, so-called “smart cards” (i.e., removable SEs), or embedded into CE devices (i.e., embedded SEs). The most common types of smart cards found in mobile devices include removable UICC/SIM cards and removable secure Micro SD cards.

41. The notifying parties submit that while there is some degree of supply-side substitutability, there is no demand-side substitutability between SEs and AP-based security solutions such as TEEs. SEs and AP-based security solutions are more complementary security solutions than substitutes.

Commission's assessment

42. The Commission broadly confirms, on the basis of the market investigation, the notifying parties' view, in particular that SEs are not a substitute, but rather a complement, to TEE solutions. A clear majority of respondents to the first market investigation considered that TEEs and SEs do not share sufficiently similar characteristics, functionalities and performance, as well as that the cost of the solutions is significantly different (with SEs being significantly more expensive than TEE solutions).[27] A majority of the respondents confirmed this view also in the second market investigation.[28]

43. Moreover, several respondents pointed out the complementarity of both solutions for a number of trusted applications: Telefonica stated that the "*Secure Element is an optional complementary asset to the TEE solution - it cannot run the applications that the TEE can run due to extreme CPU/memory/API constraints*."[29] Google stated

---

26 Commission decision of 19 May 2006 in Case M.3998 - *AXALTO / GEMPLUS*, paragraphs 11-24.

27 Customers' replies to the Commission's request for information sent on 21 June 2012, question 13; Competitors' replies to the Commission's request for information sent on 21 June 2012, question 18 and TSM's replies to the Commission's request for information sent on 21 June 2012, question 10.

28 Replies to question 3.6 of each of the following: Competitors' replies to the Commission's request for information sent on 17 September 2012; Customers' replies to the Commission's request for information sent on 17 September 2012; TSM's replies to the Commission's request for information sent on 17 September 2012 and MNO's replies to the Commission's request for information sent on 13 September 2012.

29 MNO's replies to the Commission's request for information sent on 17 September 2012, response by Telefonica S.A. to question 3.6.

that "[i]*n practice, SE and TEE solutions will often be combined*."[30] Sierraware, which provides an open-source TEE solution, pointed out that "*SEs and TEE work in conjunction to provide unique identification and security. SEs by itself is not enough to provide comprehensive security* […]."[31]

44. In the Commission's decision in the case *Axalto/Gemplus*, the Commission distinguished, within the provision of secure plastic cards, at least between a relevant product market for SIM cards and payment cards.[32] Moreover, it considered that the provision of Over-The-Air ("OTA") SIM card administration and services platforms was a distinct product market.[33]

45. In addition, the market investigation supports the notifying parties' views that SEs are separate from AP-based security solutions for CE devices.

46. For the purposes of this decision, it can therefore be concluded that SEs are not part of the same relevant product market as TEE solutions.

2.3. Other relevant product markets

47. There are a number of other possible relevant markets for the purposes of the assessment of the proposed transaction, which are either vertically related, or closely neighbouring, to the market for TEE solutions where the JV will operate.

IP licensing for semiconductors

48. ARM develops IP solutions for chipsets and APs used in CE devices. ARM does not supply processors itself, but only designs the architecture, which is used by semiconductor manufacturers in the development and manufacture of their products.

49. The notifying parties submit that the relevant market should include all AP architectures used in CE devices and that no distinction should be made based on the type of CE device (including smartphones, tablets, digital TV/STB, game consoles, netbooks, notebooks, and desktops), in which the AP is ultimately incorporated.[34] This is because smartphones and other CE devices use the same or similar APs or families of APs (and therefore the same or similar IP). In any event, the notifying parties consider that the Commission may leave open the question whether there is a narrower product market limited to the licensing of IP for AP for specific types of

---

30 Customers' replies to the Commission's request for information sent on 17 September 2012, response by Google Inc. to question 3.6.

31 Competitors' replies to the Commission's request for information sent on 17 September 2012, response by Sierraware LLC to question 3.6.

32 Commission decision of 19 May 2006 in Case M.3998 - *AXALTO / GEMPLUS*, paragraph 24.

33 Commission decision of 19 May 2006 in Case M.3998 - *AXALTO / GEMPLUS*, paragraph 29.

34 The notifying parties submit that CE devices encompass in this context smartphones, tablets, DVD/STBs, game consoles, netbooks, notebooks, and desktops. This classification is likely not entirely accurate on the ground that enterprises (as opposed to consumers) are also significant purchasers of notebooks and desktops, but this question may also be left open as it does not materially affect the competitive assessment.

CE devices/ platforms, since the proposed transaction raises no competition concerns regardless of how the market is defined.

50. In a prior decision concerning the licensing of microprocessor core architectures,[35] the Commission considered that a distinction may exist between various core architectures but left open the precise definition of the relevant product market. In its decision in *Intel/McAfee*,[36] the Commission concluded that the relevant product market was based on the architecture – in that case the market for x86 Central Processing Units ("CPUs" – also called microprocessors when incorporated into personal computers). The decision further stated that this market could potentially be segmented according to the type of platform (such as servers, desktops and notebooks).

51. In light of these precedents, the Commission will consider in its competitive assessment a possible segmentation of the relevant market for the licensing of IP for APs for CE devices based on the type of architecture (namely ARM, x86, MIPS and Power PC) and/or based on the type of platform including, in particular, smartphones and tablets. In any event, for the purposes of this decision, the exact product market definition can be left open as the result of the competitive assessment would not be materially different.

Trusted applications

52. As explained in more detail in paragraph 7 above, trusted applications are applications which offer enhanced security for more personalized and, therefore, more valued, services to users on CE devices. As further described in paragraph 18 above, the JV will have the ability to develop pre-issuance trusted applications. Further, it is anticipated that each of G&D and Gemalto may develop post-issuance trusted applications in the future.

53. In the view of the notifying parties, all applications for CE devices (regardless of whether they are "trusted" or not) belong to the same market as any application, regardless of its final use, can be categorized as “trusted” if it requires a certain level of security. The notifying parties also submit that pre-issuance and post-issuance applications do not belong to separate product markets.

54. The Commission considers that for the purposes of the present decision, the exact product market definition can be left open, as the proposed transaction raises no competition concerns regardless of how the market is defined.

TSM services

55. Each of Gemalto and G&D will be active in the provision of TSM services. TSM providers install, personalize, and provide lifecycle management of the trusted side of an application. The notifying parties submit that TSM services is a nascent business and most of today’s TSM activity derives from secure management and OTA application download and personalization to NFC-enabled SEs, such as SIM

35 Commission decision of 3 July 2001 in Case M. 2439 *Hitachi/STmicroelectronic/Superh JV*, paragraph 16.

36 Commission decision of 26 January 2011 in Case M. 5984, *Intel/ McAfee*, paragraphs 23-30.

cards. In the future, they expect that TSMs will also manage the post-issuance implementation of applications for other security solutions, including AP-based security solutions such as TEEs. However, such offering does not currently exist for TEEs or other AP-based security solutions and is unlikely to develop before 2013-2014.

56. The notifying parties submit that all TSM services belong to the same relevant product market due to a considerable degree of supply side substitutability among TSM services for NFC-enabled SEs and other security solutions, including TEEs and other AP-based security solutions, should such services successfully develop. In any case, the exact product market definition can be left open, since the proposed transaction raises no competition concerns regardless of how the market is defined.

57. TSM or service providers responding to the first market investigation mostly confirmed that TSM services for CE devices containing TEE solutions are likely to be substitutable to TSM services for NFC-enabled SEs.[37]

58. The Commission considers that for the purposes of the present decision, the exact product market definition can be left open, as the proposed transaction raises no competition concerns regardless of how the market is defined.

3. GEOGRAPHIC MARKET DEFINITIONS

View of the notifying parties

59. The notifying parties submit that the relevant geographic market for AP-based security solutions and its segments, as well as for SEs, IP licensing for semiconductors, trusted applications and TSM services are worldwide or, at least, EEA-wide since all relevant products are generally offered globally, in standard versions, purchased by customers who are active worldwide, and not affected by transportation and similar costs. The notifying parties submit that in any event, the geographic market definition can be left open for the purposes of the assessment of the proposed transaction.

Commission's assessment

60. The vast majority of respondents to the first market investigation considered that the relevant geographic markets for AP-based security solutions and its possible sub-markets are global.[38]

61. In light of the above and on the basis of the facts available at the first phase of the investigation, the Commission considers that the geographic market for the supply of TEEs and more generally of AP-based security solutions for CE devices are likely to be at least EEA-wide, if not global. In light of the notifying parties' arguments, the relevant geographic market for SEs, IP licensing for semiconductors, trusted applications and TSM services also appear to be global or at least EEA-wide. For the

---

37 TSM's replies to the Commission's request for information sent on 21 June 2012, question 7.1.

38 Customers' replies to the Commission's request for information sent on 21 June 2012 question 18; Competitors' replies to the Commission's request for information sent on 21 June 2012, question 22 and TSM's replies to the Commission's request for information sent on 21 June 2012, question 15.

purposes of the present decision, the precise definition can be left open as the result of the competitive assessment would not be materially different.

V. COMPETITIVE ASSESSMENT

1. INTRODUCTION

62. The notifying parties submit that the security solutions' industry is at a critical point. In their view, unless a standard-based solution achieves widespread acceptance during this early stage of market growth, security solutions promoted or owned by large IT firms such as Apple, Google, Microsoft and Intel, are likely to dominate the landscape in the near future.

63. According to the notifying parties, the JV would be a specific attempt to help the industry move away from the fragmented proprietary solutions that are in use today and to counter the threats posed by vertically integrated firms. The JV's offer - an open standard TEE solution - would, if it is developed, be state-of-the-art and create a catalyst for the development of an open ecosystem of trusted applications.

2. HORIZONTAL ASSESSMENT

2.1. Elimination of competition in the provision of TEE services

Introduction

64. If the relevant market were to be defined more broadly than the provision of TEE solutions for APs for CE devices, the proposed transaction would likely not give rise to horizontal competition concerns. This reflects the fact that if virtualisation solutions alone were to be considered part of the same market as TEE solutions, the JV's market share would be below [0-5]%.[39]

65. However, if the relevant market were to be defined as limited to the provision of TEE solutions for APs for CE devices (whether or not based on ARM's TrustZone technology),[40] the JV would combine the two most advanced TEE technologies currently available on the (merchant) market. Based on the notifying parties' own estimates, under this product market definition, Gemalto alone would today account for a share of around [70-80]% (in volume), with G&D controlling the second most developed TEE technology.

66. By way of background, it should also nonetheless be noted that, as of today, the market for TEE solutions would be a very small market with a total size of around

---

39 For completeness, it is also noted that if SEs, where each of Gemalto and G&D have rather strong positions (respectively, around [30-40]% and [20-30]% in the EEA) were to be included in the same relevant product market as TEE solutions (with or without other security solutions), the proposed transaction would also likely not give rise to competition concerns since the JV's position on such broader product market would be very limited (less than [0-5]%) and the impact of the proposed transaction would therefore be negligible, particularly in light of the fact that, as explained in paragraph 184, the proposed transaction would likely not give rise to any risk of coordination between the retained activities of each of Gemalto and G&D in the provision of SEs.

40 At present, there are no commercialised TEE solutions for APs for CE devices based on other architecture than ARM's TrustZone.

EUR […] in 2011 and a similar size in 2012. This market is, however, poised to grow significantly in the coming years, particularly due to the increased uptake of CE devices, including smartphones and tablets. As a result, absent high barriers to entry, such growing market is likely to attract entry from different players, including in particular, both companies active at different level of the CE value chain and companies active in neighbouring markets (for instance software companies). The market investigation confirmed the likelihood of such entry (see paragraphs 78 to 93 below).

Views of the notifying parties

67. The notifying parties put forward several arguments supporting the view that, even on a market defined as the provision of TEE solutions for APs for CE devices, the proposed transaction would not give rise to competition concerns.

68. First, the notifying parties claim that G&D […]. Therefore, according to them, G&D should be considered as a potential, and not an actual, competitor on this market. Moreover, the JV would create a product with new features (including, in particular, being based on open standards and supporting the download of post-issuance applications) compared to those currently offered by each of Gemalto and G&D.

69. Second, the notifying parties submit that there are a number of competitors, which either already provide TEE solutions for APs for CE devices for the merchant market (for example Sierraware, Solacia) or for their captive use (for example Qualcomm, ST-Ericsson and Intel), or which are likely to start developing similar solutions in the short term (for example GHS, which already provides virtualisation solutions). Furthermore, they submit that barriers to entry are very low, particularly for companies which are already active in the IT sector, and that the market is growing very fast.

70. Third, the notifying parties explain that, immediately after its launch, the JV would have every incentive to license its TEE solution as cheaply and as widely as possible to ensure its adoption by OEMs and MNOs (against competing non-TEE security solutions or any proprietary TEE solution developed by integrated players, such as Intel and Apple, or by silicon vendors) and incentivise the creation of an ecosystem of trusted applications based on the JV's TEE solution. Moreover, they submit that the JV's direct and indirect customers would be large and sophisticated market players, which will exercise significant countervailing buyer power.

71. Fourth, the notifying parties claim that, even if the JV were to develop the most successful TEE solution available on the market and create an ecosystem of trusted applications running on top of its TEE, since both such solution and the trusted applications would be based on open industry standards defined by GlobalPlatform, competitors would have the ability to develop alternative TEE solutions which, provided they are GlobalPlatform compliant, will interoperate with such ecosystem of trusted applications. Moreover, the JV would not have any incentive to depart from open industry standards since the whole ecosystem, including trusted applications, would be based on the standards defined by GlobalPlatform. As a result, the JV's customers would not be "locked-in" the JV's TEE solutions and, if the JV were to raise prices, they could easily switch to another TEE solution provider or

develop in-house their own GlobalPlatform-compliant TEE solution,[41] without losing the benefit of a TEE solution that is compatible with the existing ecosystem of trusted applications.

Commission's assessment

72. The market investigation conducted by the Commission for the purpose of the assessment of the proposed transaction primarily aimed at testing the validity of the arguments put forward by the notifying parties in support of the contention that, even if the relevant product market were to be limited to TEE solutions, the proposed concentration would not give rise to horizontal competition concerns.

Competition between Gemalto and G&D

73. The Commission could not fully confirm, in light of the market investigation, the claim of the notifying parties that G&D is a potential rather than actual competitor of Gemalto on the provision of TEE solutions. While a respondent explained that "[…] *bringing G&D to the level of completeness, readiness and maturity of Gemalto would be a significant effort*"[42], a number of respondents to the market investigation indicated that, as of today, Gemalto's Trusted Foundations and G&D's MobiCore are the most advanced and mature TEE technologies and the only two TEE solutions which, as of today, have been implemented to a meaningful extent in the CE space.[43]

74. A number of respondents, however, also confirmed that Gemalto's and G&D's products currently have different features, including, in particular, the fact that Gemalto's Trusted Foundations solution is GlobalPlatform compliant and G&D's MobiCore solution is able to support the download of post-issuance applications. Therefore these products are not necessarily particularly close substitutes. Indeed, one of the stated aims of the creation of the JV, also confirmed by the market investigation, is to develop a product that would combine into one the key features of Gemalto's and of G&D's TEE solutions.[44]

75. Moreover, for all practical purposes, G&D's TEE solution has not yet been commercially deployed. […]. By the same token, as explained, Gemalto's TEE solution, which is the most advanced TEE solution to date, only generated around EUR […] in revenues in 2011 and is expected to generate a similar level of revenues in 2012. Gemalto only has licensing agreements in place with […] semiconductor manufacturers (namely […]) for the licensing of its TEE solution.

---

41 The notifying parties submit that developing a new TEE for the merchant market from scratch requires an investment of approximately USD 10 million and around two years and the time and cost to develop similar solutions in-house would likely be smaller (since the TEE solution would have to developed for a single type of chipsets). This has been broadly confirmed by the results of the market investigation; see replies to the Commission's request for information sent on 17 September 2012, question 17.

42 Customers' replies to the Commission's request for information sent on 17 September 2012, response by Texas Instrument to question 12.2.

43 Competitors', Customers', TSM's and MNO's replies to the Commission's request for information sent on 17 September 2012, questions 8.

44 Competitors', Customers', TSM's and MNO's replies to the Commission's request for information sent on 17 September 2012, question 12.1.

76. It therefore does not appear to be the case that Gemalto and G&D currently enjoy a huge installed base of smartphones including their respective TEE solutions. To the contrary, in the Commission's view, the above elements confirm the limited uptake of each of Gemalto's and G&D's TEE solutions as of today and, more generally, nascent nature of the TEE market.

77. The Commission therefore concludes that, while Gemalto's Trusted Foundations and G&D's MobiCore appear to be the most advanced and mature TEE technologies and are therefore actual, more than potential, competitors, the TEE solutions that are currently offered by each of Gemalto and G&D also have different characteristics, which will be combined into the TEE solution that will be offered by the JV. Moreover, as of today, the size of the TEE market where these companies operate and the commercial uptake of TEE solutions (including those offered by Gemalto and G&D) is very limited.

Actual and/or potential TEE competitors

78. On the basis of its market investigation, the Commission broadly confirms the notifying parties' claim that there are a number of competitors, which either are already providing competing TEE solutions for the merchant market or for their captive use, or which are likely to start developing similar solutions in the short term.

79. The Commission, however, also notes from the outset that most of the actual and/or potential competitors identified in this section are likely to develop a TEE solution, which will be based on ARM's TrustZone. As explained in more detail in Section 3.3 below, in order to be able to develop any such solution and compete with the JV's TEE solution, these competitors will likely require not only to have access to the relevant technical specifications concerning ARM's TrustZone, but also to be granted access to such information at the same time as the JV. Furthermore, ARM should not seek to degrade the interoperability of alternative TEEs with the TrustZone technology.

80. Subject to the above, and on the basis of the market investigation, the Commission confirmed that, by the time that the JV expects to commercially release the first version of its TEE (namely the first quarter of 2014 at the earliest)[45] other TEE solutions will likely have already been launched or will likely be about to be launched on the market.

81. First, there are a number of large IT companies, which are already active in vertically-related or neighbouring markets, which plan to enter the TEE space in the near future.

82. […] In other words, the Commission understands that Apple and its silicon providers will likely be self-sufficient in terms of TEE solutions and will not use the JV's or any other TEE solution.[46] Furthermore, the Commission considers that, given the current importance of its App Store in the provision of applications, Apple could

---

45 Reply from the Notifying Parties to question 1 of the Request for Information of the Commission of 10 October 2012.

46 Non-confidential version of the minutes of the conference call with Apple Inc., 04 October 2012.

persuade application developers/service providers to develop trusted applications for its TEE solution regardless of the JV.

83. Microsoft explained that it has a "*TEE-like*" solution for some of its operating systems and plans to build TEE solutions for other offerings.[47] Microsoft stated that it "*might develop a competing TEE solution in the near future. Microsoft's strategy is generally not to rely on software development by third companies. Hence, it is unlikely that Microsoft will rely on the JV's TEE*". Furthermore, if "*Microsoft decides to enter the TEE market, the company should be able to surpass entry barriers and notably catch up with the development of trusted applications depending on the successful development of its TEE*".[48]

84. Intel confirmed that it has *"a portfolio of technologies that offer AP-based security solutions and include trusted executive environments*".[49] While Intel's presence today in the CE space, where the JV will operate, is rather limited, Intel itself explained that it's *"goal is to gain a significant presence in such devices* [smartphones and tablets] *by the end of that period* [2-3 years]".[50]

85. Second, other companies confirmed that they are likely to develop TEE solutions or solutions, including in the relatively short term. One of them confirmed that *"it is in the process of developing a TEE solution, which will likely compete with products developed by the JV.* […]. *The developer of the solution is currently planning to enter into partnerships for the use of its TEE solution. Moreover, the developer of the solution considers that trusted applications running on top its TEE solution are likely to be developed after the commercial release of the solution*". [51]

86. In addition, two market participants indicated that they believed that Oracle is in the process of developing a TEE solution, which would likely compete directly with that of the JV. One of these two market participant explained that because its solution would likely be a Java-based TEE, it would be "*very limited in scope and capabilities*"[52]. The Commission nonetheless notes that Oracle, which claims that its Java Card is "*the World's Leading Open Platform for Embedded Secure Elements, SIMs, and Smart Cards*"[53] may be able to use its experience / expertise in Secure Elements to attract certain Application developers (notably for mobile payments) which may want to have a security solution based on Secure Element, plus a TEE (a

---

47 Competitors' replies to the Commission's request for information sent on 17 September 2012, question 2.

48 Non-confidential version of the minutes of the conference call with Microsoft Inc., 08 October 2012.

49 Customers' replies to the Commission's request for information sent on 17 September 2012, question 3.

50 Competitors' replies to the Commission's request for information sent on 17 September 2012, response by Intel to question 16.

51 Email referenced in Commission file as ID NUMBER 2012/116137

52 Customers' replies to the Commission's request for information sent on 17 September 2012, question 15.

53 See: http://www.oracle.com/us/technologies/java/embedded/card/overview/index.html .

combination that a number of market participants have suggested may be the way forward for future mobile payment security solutions).[54]

87. The likelihood that there is potential entry of significant competitors such as […] and […] is also supported by […] internal documents, according to which "[…]".[55]

88. Moreover, there is a number of software companies, which are also likely future entrants in the TEE space.

89. Oberthur – a leading competitor in the smart card space - confirmed that it is "*working today on TEE solutions at operating system level and for TSM services*"[56].

90. Solacia confirmed that, although its TEE solution is not yet commercially deployed, it has already been trialled with some silicon vendors and prototypes are being tested with silicon vendors and OEMs,[57] which indicates that the company is likely close to deploy commercially its TEE solution. A number of respondents to the market investigation identified Solacia as an actual competitor with its "SecuriTEE" solution".[58] One respondent, however, noted that Solacia is a new entrant which "*would require a good deal of investment and time to get a commercial TEE implementation up and running*".[59]

91. Sierraware confirmed that its software competes "*with the Trusted Logic TEE part of the joint venture*" and is currently available under commercial as well as open source licenses[60]. One market participant, however, explained that "*although SierraWare's "Open TrustZone" stack aims to compete with that of the JV, […] this stack is in its infancy […] so we wouldn't consider it a main competitor of the JV's stack*"[61].

92. Third, certain semiconductor manufacturers, such as Qualcomm and ST-Ericsson, have also developed their own TEE solution for captive use only. While these solutions today may not necessarily have the same functionalities as the JV's TEE solution, these market players would likely be able to develop competing solutions to the JV's TEE in the future if they were to find it profitable.

93. Based on the above, including the level of investment required to develop a TEE solution, the Commission concludes that, by the time the JV will commercialise its

---

54 Competitors' and Customers' replies to the Commission's request for information sent on 17 September 2012, question 27.

55 […].

56 TSM's replies to the Commission's request for information sent on 17 September 2012, response by Oberthur to question 2.

57 Competitors' replies to the Commission's request for information sent on 17 September 2012, question 2.

58 Competitors' replies to the Commission's request for information sent on 17 September 2012, question 9.4.

59 Customers' replies to the Commission's request for information sent on 17 September 2012, response by Texas Instrument to question 15.

60 Customers' replies to the Commission's request for information sent on 17 September 2012, question 9.4.

61 Customers' replies to the Commission's request for information sent on 17 September 2012, response by NVIDIA Corporation to question 9.3.

TEE solution (namely the first quarter of 2014), there will likely be a number of market participants other than Gemalto and G&D, which already have a commercial presence or will likely enter the TEE market. In the interim period, that is to say between the closing of the proposed transaction and the launch of the JV's TEE solution, the notifying parties expressly confirmed that legacy products (Trusted Foundations and MobiCore) will no longer be developed and/or marketed to new customers, although some customers may continue to use these products during a transitional period before migrating to the JV TEE (or to a competitor's TEE or alternative solution). The latter point was confirmed by the assumptions underlying the revenues projections in the business plan of the JV, as explained by the notifying parties.[62]

94. Furthermore, as outlined in paragraph 37, the Commission notes that a number of existing or future market participants may also develop security solutions such as for instance virtualisation solutions which are not TEEs, but which may have similar features and characteristics as the TEE developed by the JV, and as such may exert a competitive constraint on the JV's TEE offering at least in the short term with respect to certain trusted applications.

95. Given the above, the Commission also considers that the argument put forward by one of the respondents to the market investigation, according to which, since, post transaction, the JV will be dominant in the provision of TEE solutions and will be vertically integrated with ARM, which will be dominant in the upstream supply of IP for AP for CE devices, any new entrant would need to enter at both levels of the value chain in order to meaningfully compete with the JV, is not founded. Indeed, the JV will likely face competition from a number of strong players in the provision of TEE solutions. Therefore the premise on which the above argument is based, that is to say, the JV being dominant in the provision of TEE solutions, is not founded.

96. The Commission, however, also notes that the above outlined conclusions concerning the likelihood of entry of competitors in the provision of TEE solutions is premised on these competitors' ability to develop solutions, which would run on ARM's TrustZone technology. In particular, as explained in more detail in paragraphs 139 and forward, in order to compete with the JV's TEE, these competitors would need to be provided with the necessary information to be able to develop a TEE solution based on ARM's hardware architecture.

JV's incentives post transaction

97. The market investigation provided mixed results as regards the notifying parties' claims that the JV would have every incentive to license its TEE solution as cheaply and as widely as possible and to comply with GlobalPlatform's open standards to ensure its adoption by OEMs and MNOs and incentivise the creation of an ecosystem of trusted applications based on the JV's TEE solution.

98. On one hand, according to some respondents, the proposed transaction could potentially lead to the creation of a monopolistic situation, with the JV's TEE solution becoming the *de facto* industry standard.

---

62 Reply from the notifying parties to the Commission's Request for Information of 16 October 2012.

99. If this was the case and the JV's TEE solution was to become the *de facto* proprietary industry standard, future TEE competitors may have to depend on the JV to receive the necessary information to develop TEE solutions which are fully interoperable with the ecosystem of trusted applications which may develop around the JV's TEE. In this scenario, the JV would therefore be able to prevent the development of competing TEE solutions.[63]

100. As a result, a number of market participants indicated that the JV's compliance with GlobalPlatform current and future open standards[64] would be a necessary pre-condition for these competitors to be able to develop alternative TEE solutions.

101. On the other hand, a number of respondents confirmed the notifying parties' claims that the JV's open standard TEE solution may help the industry move away from the fragmented proprietary solutions that are in use today and create a catalyst for the development of an open ecosystem of trusted applications.

102. Notably, one respondent explained that the JV may help *"to create a more standard and more open ecosystem for secure applications using the* TrustZone *TEE, and hence to attract more developers and applications users*"[65], while another considered that *"the formation of the JV, if handled properly, helps control the fragmentation and therefore a broader adoption of the TEE technology*"[66] and a third considered that *"if the JV does not intentionally raise barriers to entry or to interrupt other parties, it may provide better solutions to silicon vendors and OEMs*".[67]

103. Furthermore, a majority of respondents to the market investigation conducted for the purpose of assessing the remedies proposed by the notifying parties also stated that the notifying parties have an incentive to comply with GlobalPlatform's open industry standards to achieve the widest market adoption of its TEE solution by customers. For instance, Ericsson underlines that "*today, the hurdle to gain market adoption is to be endorsed by either Apple or Google. An open industry standard is maybe more likely to be adopted by those two (at least Google) as they do not seem to have any proprietary work in this field*".[68]

104. In addition, a majority of respondents to the market investigation conducted for the purpose of assessing the remedies proposed by the notifying parties submitted that the JV is likely to have the incentive to comply with GlobalPlatform’s open industry standards if credible competing TEE solutions are likely to enter market for TEE

---

63 Customers' replies to the Commission's request for information sent on 17 September 2012, question 28.

64 These standards would include, in particular, GlobalPlatform’s TEE Client API, TEE Internal API and TEE Administration Framework, as well as the relevant compliance program.

65 MNO's replies to the Commission's request for information sent on 17 September 2012, response by Vodafone to question 31.

66 Customers' replies to the Commission's request for information sent on 17 September 2012, response by NVIDIA Corporation to question 28.

67 Customers' replies to the Commission's request for information sent on 17 September 2012, response by Samsung question 28.

68 Replies to remedies market test questionnaire sent on 12 October 2012, response by Telefonaktiebolaget LM Ericsson to question 15.

solutions in a timely fashion. This reflects the fact that the JV TEE's compliance with open industry standards could be a competitive advantage over future competing TEE solutions and thereby would help the JV to achieve market adoption.[69]

105. Also, according to the respondents to the market test, it would probably take the JV 18 to 24 months, and in any event 1 to 3 years, to develop a significant and attractive eco-system of trusted applications around its TEE solution.[70]

106. Based on the above, the Commission concludes that, since the JV will likely face competition from alternative providers of TEE solutions, its TEE solution is unlikely to become the *de facto* industry standard. For the same reasons, the Commission takes the view that the JV will likely have the incentive to comply with open standards (including, in particular, GlobalPlatform's open standards). Similarly, the Commission considers it unlikely that the JV would be able to develop an ecosystem of trusted applications, which would not comply with open standards and which would result in the exclusion of competing TEE providers from the TEE market.

Switching costs

107. The results of the market investigation were mixed as regards switching costs for TEE's customers. On one hand, a number of respondents to the market investigation highlighted the high costs for customers in switching between different TEE solutions.

108. On the other hand, a majority of market participants also replied that standardisation should make the switch easier between different TEE solutions.[71]

Conclusion

109. All in all the Commission considers, in light of the investigation that the proposed concentration would not give rise to horizontal competition concerns. In particular, the Commission confirms that, post transaction, the JV will likely face competition from a number of strong market players, which will develop and launch TEE or TEE-like solutions even prior to the launch of the JV's TEE solution. Moreover, even if the JV's TEE solution were to be first-to-market and able to start developing an ecosystem of trusted applications running on top of its TEE solution, these new entrants will likely enter the market prior to the development of any such ecosystem (which would likely take 1 to 3 years). In addition, even if the JV were able to develop this ecosystem, these new entrants would likely be able to counter any possible network effects and persuade service providers / application developers to develop trusted applications, which would also run on their TEE solutions.

110. The Commission therefore considers that, faced with the actual and/or potential competition by these market players, the JV will likely have the incentive to comply

---

69 Replies to remedies market test questionnaire sent on 12 October 2012, question 16.

70 Replies to the remedies market test questionnaire sent on 12 October 2012, question 17.

71 Competitors', Customers', TSM's and MNO's replies to the Commission's request for information sent on 17 September 2012, question 20.

with open industry standards defined by Global Platform to attract as many application developers/service providers as possible and to license its TEE solution as widely and as cheaply as possible to gain market acceptance.

Overall conclusion

111. Based on the results of the investigation and the analysis above, the Commission considers that the proposed transaction would not give rise to serious doubts as to its compatibility with the internal market as a result of horizontal effects in the market for the provision of TEE services.

3. NON-HORIZONTAL ASSESSMENT

112. According to the Non-Horizontal Merger Guidelines, a merger is likely to result in foreclosure where actual or potential rivals' access to supplies or markets is hampered or eliminated as a result of the merger, thereby reducing these companies' ability and incentive to compete.[72] Such foreclosure is regarded as anticompetitive where, as a result of the merger, the merged entity, and possibly also some of its competitors, are able to profitably increase the price charged to consumers.

113. When assessing the likelihood of such an anticompetitive foreclosure scenario, it needs to be examined "*first, whether the merged entity would have, post-merger, the ability to substantially* foreclose *access to inputs, second, whether it would have the incentive to do so, and third, whether a foreclosure strategy would have a significant detrimental effect in the competition downstream*".[73]

114. In this case, also based on the results of the market investigation, the non-horizontal assessment focuses on the following possible foreclosure concerns: (1) the JV's ability and incentive to favour Gemalto and G&D and to foreclose third party developers of trusted applications and of TSM services; and (2) ARM's ability and incentive to foreclose the JV's competitors in the provision of TEE solutions.

3.1. Possible foreclosure of third party providers of trusted applications

115. As explained in paragraph 4, a TEE solution provides a secure environment for trusted applications. As also explained in paragraph 4, trusted applications are applications which process sensitive information and offer an enhanced, more personalized and therefore more valued service to end users.

116. The JV aims at developing a TEE that supports both pre-issuance and post-issuance trusted applications. The JV will also be active in the development of pre-issuance applications.

117. Post transaction, G&D and Gemalto will be active in the development of post-issuance applications.[74]

---

72 OJ C265, 5.2.2008, p.6, paragraph 31.

73 OJ C265, 5.2.2008, p.6, paragraph 32.

74 Paragraph 50 of the Form CO.

118. Post transaction, there will therefore be a vertical relationship between the activities of the JV in the provision of TEE solutions and the activities of the JV in the provision of pre-issuance applications and of each of Gemalto and G&D in the provision of post-issuance applications, which will run on top of the JV's TEE solution.

Views of the notifying parties

119. The notifying parties submit that, post transaction, every application developer or service provider could develop applications for the JV's open standard TEE solutions.

120. The notifying parties also submit that the applications sector is highly competitive and fragmented. The JV, as well as each of G&D and Gemalto, would compete with hundreds of service providers / application developers, many of which are well-established software companies. In any event, according to the notifying parties, the JV and, in particular, ARM, which would not be active in the provision of trusted applications, would have every incentive to have as many applications as possible developed for its TEE solutions to gain wide market acceptance.[75]

Commission's assessment

121. In light of the market investigation, the Commission confirmed the notifying parties' claim that the proposed transaction will likely not give rise to competition concerns as a result of the non-horizontal relationship between the JV's activities in the provision of TEE solutions and the JV's and each of Gemalto's and G&D's activities in the provision of trusted applications.

122. First, provided the JV's TEE solution will be compliant with GlobalPlatform standards, the JV (and/or the notifying parties) will likely not have the ability to foreclose third party application developers / service providers. Indeed, these third parties will likely have the ability to develop trusted applications, which will run on top of the JV's TEE solution.

123. Second, the JV will likely have the incentive to have as many service providers and trusted application developers as possible, and not only itself and/or two of its parent companies, to write applications running on top of the JV's TEE solution.[76]

124. Indeed, the Commission considers that the attractiveness of any TEE solution and its future market acceptance is conditional upon the availability of a wide range of diverse and attractive trusted applications. Hence, the development of an eco-system open to third parties trusted application developers is essential to the notifying parties and to the JV. The Commission considers that the notifying parties and/or the JV will likely have no incentive to foreclose third parties application developers in order to favour its parent companies.

---

75 Paragraph 63 of the Form CO.

76 Customers' replies to the Commission's request for information sent on 17 September 2012, question 14.1. MNO's replies to the Commission's request for information sent on 17 September 2012, questions 14 and 31.

125. Third, even if (which the Commission considers highly unlikely) the JV, as well as each of Gemalto and G&D, were to be able to prevent third party service providers / application developers from developing applications running on top of the JV's TEE solution, since there will likely be other TEE solution providers competing with the JV's TEE, no customer foreclosure would arise since third party service providers / application developers would likely develop applications for the JV's competitors.

126. Accordingly, the Commission considers that the proposed transaction will not give rise to serious doubts as to its compatibility with the internal market as a result to the vertical relationship between the activities of the JV in the provision of TEE solutions and of the JV and of each of Gemalto and G&D in the provision of trusted applications.

3.2. TSMs

127. As explained in paragraph 20, the installation of post-issuance trusted applications requires the intervention of a Trusted Service Managers ("TSM"), which installs, personalizes, and provides lifecycle management of the trusted side of a post-issuance application.

128. The role of a TSM is already well defined in the framework of NFC technology. The TSM acts as a neutral broker, which sets up business agreements and technical connections with mobile network operators, phone manufacturers or other entities controlling the secure element (or the TEE in the present case). A TSM enables service providers to distribute and manage their trusted applications remotely by allowing access to the secure element (or the TEE).

129. Post transaction, each of G&D and Gemalto will be active as TSMs.

Views of the notifying parties

130. The notifying parties submit that, since the JV will be based on GlobalPlatform open standards, post transaction, competitors of each of Gemalto and G&D would be able to develop TSMs, which will interoperate with the JV's TEE solutions.

131. The notifying parties also submit that the information needed by TSM providers to interoperate with the JV's TEE solutions would be defined in the "TEE Administration framework", currently being discussed within GlobalPlatform and expected to be publicly released at the end of 2012.

132. The notifying parties further submit that G&D and Gemalto would face competition from other TSMs, including those TSMs, which currently provide TSM services for NFC.[77] The notifying parties expect that G&D and Gemalto's share of TSM for AP-based security solutions would not exceed [10-20]% in the medium term.

Commission's assessment

133. In light of the market investigation, the Commission confirmed that the proposed transaction would not give rise to non-horizontal competition concerns as a result of

77 These include G&D, Gemalto, Atos (France), Cassis International (Singapore), Ericsson (Sweden), FDR (U.S.A.), IBM (U.S.A.), MasterCard (U.S.A.), Oberthur (France) and Orange (UK).

the non-horizontal relationship between the JV's activities in the provision of TEE solutions and Gemalto's and G&D's activities in the provision of TSM services.

134. The Commission reached this conclusion despite the fact that certain respondents to the market investigation indicated that, if the JV's solution were to emerge as the dominant TEE solution and if the necessary interfaces allowing for interoperability between the JV's TEE solution and the TSM were not to be open, the JV would have the ability and likely the incentive to reserve to its parent companies the growing TSM market/segment. Indeed, according to these respondents, only G&D and Gemalto would have access to the necessary information to develop TSMs which would be compatible with the JV's TEE solution.

135. The Commission, however, takes the view that the above outlined concerns arising from the market investigation are not founded. This reflects, in particular, the fact that the JV will likely not have the incentive to favour Gemalto and G&D over third party TSM providers. In particular, ARM, will likely have the incentive to make sure that the JV's TEE solution works with as many TSM providers as possible, including, but not limited to, Gemalto's and G&D's TSMs, as this would likely increase the attractiveness of the JV's TEE solution to its customers.

136. In any event, and even if (which the Commission considers it highly unlikely to happen) the JV were to have the ability and incentive to prevent third party TSM providers from being able to interoperate with its TEE solution, the Commission considers that this conduct would likely not give rise to the foreclosure of competing TSM providers. Indeed, since, as explained in paragraph 93, the JV will likely face competition from several strong market players, even if TSM providers other than Gemalto and G&D were unable to interoperate with the JV's TEE solution, they could still continue to successfully provide TSM services to competing providers of TEE solutions, to the customers of these TEE solutions and/or to service providers / application developers for these TEE solutions.

137. Accordingly, the Commission considers that the proposed transaction will not give rise to serious doubts as to its compatibility with the internal market as a result to the non-horizontal relationship between the activities of the JV in the provision of TEE solutions and of each of Gemalto and G&D in the provision of TSM services.

138. For the sake of completeness, the Commission also notes that few respondents to the market investigation raised the concern that, following the proposed transaction, the JV could potentially leverage its dominant position in the market for TEE solutions to enter in the neighbouring market for SEs and foreclose Gemalto's and G&D's competitors in this space. However, as explained in paragraphs 78, the JV will likely face competition in the provision of TEE solutions from several strong market players. Hence, the Commission concludes the factual premise on which the above outlined concern is based is flawed and the concern should be dismissed.

3.3. IP licensing for APs for CE devices

139. As explained in paragraph 4, ARM's IP architectures for APs for CE devices are licensed with an integrated security feature called TrustZone. TrustZone consists of a hardware extension integrated into the microprocessor core design that provides the means to implement a TEE.

140. TrustZone allows the AP system to run in two states, one supporting the main OS and the other one supporting a secure execution environment.

141. With respect to the possible effects of the proposed transaction resulting from the vertical relationship between the activities of ARM in the licensing of IP for APs for CE devices, including TrustZone, and the activities of the JV in the provision of TEE solutions, several respondents to the market investigation indicated that the proposed concentration would give rise to competition concerns. These respondents indicated that, post transaction, ARM would have the ability and incentive to eliminate and/or degrade the interoperability between TrustZone and the TEE solutions developed by the JV's competitors. This, in turn, would lead to the foreclosure or, at least, the marginalisation of these competitors from the market for the provision of TEE solutions.

142. ARM currently commercialises two families of IP architectures for AP for CE devices (the so-called V6 and V7 families) and is to commercially release its V8 family of IP architectures in the coming months. Any foreclosure would, according to the Commission's understanding, be related to future shipments of CE devices, which would use APs based on the V6, V7, or V8 architectures of ARM (and/or possible evolutions thereof)[78]. The installed base of already commercialised CE devices whose APs run on ARM's architecture IP would presumably not be affected by any such foreclosure. However, CE device penetration rates, including based on current and future ARM architectures, are predicted by industry analysts, such as Gartner, to grow significantly in the short to medium term. Smartphone penetration rates, for example, are forecast to increase by a factor of four by 2015 and the demand for tablets is predicted to grow by a factor of 15 over the same period[79].

143. According to the Non-Horizontal Merger Guidelines, the Commission analysed: (1) ARM's ability to foreclose the JV's competitors, (2) ARM's incentive to do so and (3) the overall likely impact of this practice on competition and consumers.

ARM's ability to foreclose the JV's competitors

Views of the notifying parties

144. The notifying parties submit that, post transaction, ARM would not have the ability to foreclose the JV's competitors from access to TrustZone for the following reasons:

a) Many of ARM’s customers are large semiconductor manufacturers, which are sophisticated buyers with a significant degree of bargaining power and expert knowledge. While these companies have in effect decided to outsource a portion of their R&D by licensing ARM IP, they could to readily switch to in-house production at low cost and within a short time frame. They can also switch to numerous other licensors;

---

78 The Commission understands that new CE devices or CE devices that are in the process of being launched commercially could still use APs that are based on ARM's V6 or V7 architecture, even though ARM's new V8 architecture is about to be launched commercially.

79 Form CO, paragraph 141, based on Gartner report of 2010 and 2011.

b) The TrustZone IP is provided to all of ARM's customers as a standard feature of its AP architecture. Technically removing TrustZone from the IP design of ARM's AP (so that the technology would only be available to the JV) would very impractical. Moreover, customers could choose to support another TEE solution (also GlobalPlatform compliant) without relying on TrustZone; and

c) Granting to the JV better licensing terms and conditions for TrustZone than to the JV's competitors is unlikely as ARM has always licensed this technology as part of its AP architecture at no extra cost. Moreover, ARM does not plan to release a new architecture requiring a new license before five years.

Commission's assessment

145. As regards ARM's position upstream, that is to say in the provision of IP for APs for CE devices, the majority of the respondents to the market investigation clearly indicates that ARM currently holds a very strong market position, which is particularly strong with respect to certain CE devices, such as smartphones and tablets, where ARM holds a share of close to [90-100]%.[80]

146. Several respondents to the market investigation do not consider that Intel will have the ability to significantly challenge ARM's market position within the next few years, particularly as regards smartphones, but also in relation to other CE devices[81]. The market investigation indicated that Intel's APs do not currently reach the same level of performance and low consumption as ARM-based APs.

147. Accordingly, Texas Instruments states that: "*TI believes that in this time frame* [one or two years] *Intel's Atom may get a small market share on smartphones and a more considerable market share on tablets. ARM's chip would make up the remainder of those markets.*"".[82] Similarly, Sierraware notes that "[t]*oday, ARM is the leader in the CE device market. While Intel is formidable, we believe ARM has a market advantage over Intel in this space and will continue to dominate*".[83]

148. A majority of respondents to the market investigation also indicate that, following the transaction, ARM would be in a position to unilaterally standardize the hardware interface with TrustZone. For instance, Oberthur underlines that "*ARM has a very dominant position in the market and could de facto standardise the hardware interface*".[84] Deutsche Telekom adds that "*the planned Joint Venture would be positioned as dominant player from the start creating a de facto standard available*

80 Customers' replies to the Commission's request for information sent on 17 September 2012, question 16.

81 Competitors' and Customers' replies to the Commission's request for information sent on 17 September 2012, question 16.

82 Customers' replies to the Commission's request for information sent on 17 September 2012, question 16.

83 Competitors' replies to the Commission's request for information sent on 17 September 2012, question 16.

84 TSM's replies to the Commission's request for information sent on 17 September 2012, response by Oberthur to question 7.1.

on any mobile device. ARM has already created a de-facto standard (supplier) regarding CPUs for mobile devices. The market share is almost 100%".[85]

149. Based on that ability to define the hardware interface, a majority of respondents to the market investigation indicate that ARM would likely have the ability to modify the TrustZone technology and/or interface in order to degrade the interoperability between TrustZone and the TEE solutions that may be developed by the JV's competitors. In particular, these respondents claim that ARM could easily deny these competitors (full and timely) access to current and future versions of TrustZone.

150. For instance, Solacia underlines that "[h]*aving ARM also incorporated in the proposed JV causes more complexity as it goes beyond a horizontal joint venture to a horizontal JV in which Gemalto and G&D would be given a great advantage in the TEE industry. It would be inevitable that they would have first insight to new architecture and updates in a market where time-to-market is critical*".[86]

151. Sierraware underlines that "*ARM has the ability to raise barriers that would prevent alternative TSM providers to develop TEE and TSM solutions for ARM processors.* […]"[87] Sierraware adds that "*If ARM changes the TrustZone hardware extensions in future versions of its architectures, ARM should document all changes and make this information public to other TEE vendors"*.[88] As regards the impact on competitors, Sierraware notes that they "*have seen in one sales opportunity that the customer was concerned that ARM may only support the JV in the future and prevent other TEE solutions from working with future generations of ARM architectures*".[89]

152. Similarly, Apple explains that "[t]*here are two ways this proposed JV could raise barriers* […]*: 1) If the proposed TEE solution resulting from the JV becomes a part of the ARM specification such that it MUST be implemented in order to boot ARM* […]"[90].

153. In the same vein, France Télécom-Orange submits that: "*device OEM Suppliers should be free to use ARM based chipset without being forced to implement the JV Licence. In other term, it could be possible for a Devices supplier to implement the TEE of its choice over ARM based chipset*".[91]

154. Another respondent to the market investigation underlines that the vertical

---

85 MNO's replies to the Commission's request for information sent on 17 September 2012, response by Deutsche Telekom to question 31.

86 Competitors' replies to the Commission's request for information sent on 17 September 2012, question 28.

87 Competitors' replies to the Commission's request for information sent on 17 September 2012, question 25.

88 Competitors' replies to the Commission's request for information sent on 17 September 2012, response by Sierraware to question 18.1.

89 Competitors' replies to the Commission's request for information sent on 17 September 2012, response by Sierraware to question 28.

90 Customers' replies to the Commission's request for information sent on 17 September 2012, response by Apple to question 25.

91 Replies to the remedies market test questionnaire sent on 12 October 2012, response by France Télécom to question 4.

integration of the parties' dominant positions will enable ARM to degrade the interoperability with alternative TEEs to the one developed by the JV. Software developers need access to specific tools and information to develop and optimize their software for a given processor. This is particularly true for security solutions, which operate closer to the processor than other software and interacts closely with hardware components. ARM would likely utilise its control of the TrustZone hardware architecture to positively discriminate in favour of the JV's products and thus degrade interoperability of other TEEs, or at the very least delay disclosure of significant interface and functionality information to the JV's competitors.

155. As a starting point, the Commission considers that ARM currently holds a significant degree of market power in the licensing for IP for AP devices as whole, as well as, at least, in its possible segments based on the type of platform such as smartphones and tablets.

156. The above conclusion is supported not only by the results of the market investigation, but also from the information provided by the notifying parties in the Form CO,[92] according to which ARM currently holds a very high share of any possible market definition.[93]

a) [50-60]% of all CE devices, including personal computers, and [70-80]%, excluding personal computers, shipped in 2011 worldwide; and

b) [90-100]% of all smartphones and tablets shipped in 2011 worldwide;

157. The Commission also considers, based on the results of the market investigation, that, at least for the next few years, Intel is unlikely to make sufficient inroads in the CE device space, including, in particular, in the smartphone and tablet segments, to challenge ARM's current pre-eminent position and significant degree of market power.

158. The Commission further considers that, at least today, ARM's TrustZone hardware extension constitutes an essential input for any provider of TEE solutions willing to develop any such solution for one or more categories of CE devices. This reflects the fact that, as explained, the vast majority of the APs included in CE devices are based on ARM's architecture and include TrustZone as the only hardware extension, which is able to support security software, such as a TEE. Due to the lack of likely entrants able to challenge ARM's market position, the Commission is also of the view that this situation is likely to remain the same in the near future.

159. Accordingly, a foreclosure strategy could be implemented by ARM by degrading the interoperability between TrustZone and the TEE solutions that may be developed by the JV's competitors.

160. As of today, ARM has provided TrustZone's API to GlobalPlatform and this API is therefore available to any TEE provider. Moreover, ARM makes available on its website or otherwise certain additional information that is required or, in any event, important to ensure interoperability between TrustZone and TrustZone-based TEE

92 Paragraph 420 of the Form CO.

93 See Section 2.3.1. of the present decision on the market definition of IP for AP in CE devices.

solutions. This information includes, for example, (i) processor architecture specific information, (ii) ARM's implementation of the ARM architectures, (iii) system-wide hardware IP, (iv) training courses and (v) non-essential guidance on how to implement secure systems using the TrustZone security extensions as a component of an overall solution.

161. Post transaction, however, since ARM controls TrustZone, including its API and source codes, there is a risk that ARM could modify TrustZone's API and/or other technical aspects and stop providing the relevant information to the JV's TEE competitors. Similarly, ARM could also stop providing to the JV's TEE competitors the above outlined information and/or similar information which these competitors would likely need to develop their solutions (which it is under no obligation to provide to third parties).

162. Short of not providing the above outlined APIs and/or additional information to the JV's competitors, ARM would equally have the ability to provide these elements selectively (i.e., not in full) and/or at a different point in time compared to when they are provided to the JV, which would place these competitors at a disadvantage in terms of development work and time to market for their TEE solutions.

163. Alternatively, the market investigation indicates that ARM would also have the technical ability to degrade TrustZone's interoperability with alternative TEE solutions, for instance by modifying certain technical aspects of TrustZone in order to discriminate TEEs developed by competitors of the JV. The Commission considers that a technical degrade of interoperability would have a similar effect as blocking / limiting / delaying the access of competitors to the relevant APIs, codes and/or other information. It would constitute just an alternative means to implement a foreclosure strategy of the JV's competitors.

ARM's incentive to foreclose the JV's competitors

Views of the notifying parties

164. The notifying parties submit that, post transaction, ARM would not have any incentive to create any technical, legal or other barrier to the development of TrustZone, as its primary business is and will remain the licensing of its IP. ARM will therefore have an economic interest in favouring the adoption of as many TEE solutions based on its AP design as possible.

Commission's assessment

165. Contrary to the notifying parties' claim, the evidence collected through the market investigation indicates that the risk of monopoly on the TEE market/segment resulting from the transaction is high because of the presence of ARM in the JV and that ARM is likely to have an incentive to favour the JV over competing TEE providers.

166. Accordingly, for instance, ZTE notes that "*the transaction may cause monopoly,*

especially if ARM is in".[94]

167. NVIDIA adds that "*the fact that JV's participating entities (that is to say. ARM, G&D, and Gemalto) have significant market power and leverage within the ecosystem, could pose a potential risk to the rest of ecosystem as they would be capable of monopolizing this technology and business*".[95].

168. For Solacia, "[h]*aving ARM also incorporated in the proposed JV causes more complexity as it goes beyond a horizontal joint venture to a horizontal JV in which Gemalto and G&D would be given a great advantage in the TEE industry. It would be inevitable that they would have first insight to new architecture and updates in a market where time-to-market is critical*"[96].

169. Sierraware also explained that it "*is concerned about the impact of the transaction. We have seen in one sales opportunity that the customer was concerned that ARM may only support the JV in the future and prevent other TEE solutions from working with future generations of ARM architectures.*"[97].

170. Based on the information available to it (including the results of the market investigation), the Commission considers that there is a serious risk that ARM would have an incentive to favour the JV over competing TEE providers with a view to leveraging its market power in the provision of IP for APs for CE devices in the nascent market for the provision of TEE solutions for a number of reasons.

a) First, as explained, the likely competitors of the JV in the provision of TEE solutions will be different from ARM's direct customers for the licensing of IP for APs for CE devices (which are silicon vendors), which is, and will likely continue to be post transaction, ARM's core business. In other words, there will likely be no direct customer relationship between ARM and the market players, which would be impacted by the relevant foreclosure strategy. As a result, the cost that ARM could potentially face in terms of possible disruption of customer relationships and revenue loss may be limited and could be offset by the gain stemming from (ARM's share of) the increased JV's revenues in the TEE market following the foreclosure / marginalisation of the JV's competitors. Moreover, given the limited uptake of TEE solutions, at least as of today, the availability of the TrustZone feature and/or of TEE solution is not a determining factor in ARM' customer choice of a given hardware architecture.

b) Second, with specific respect to the cost for ARM of any such foreclosure strategy in terms of foregone revenues, the Commission notes that today ARM

---

94 Customers' replies to the Commission's request for information sent on 17 September 2012, response by ZTE to question 28.

95 Customers' replies to the Commission's request for information sent on 17 September 2012, response by NVIDIA Corporation to question 28.

96 Competitors' replies to the Commission's request for information sent on 17 September 2012, response by Solacia to question 28.

97 Competitors' replies to the Commission's request for information sent on 17 September 2012, response by Sierraware to question 28.

derives no revenues from the licensing of TrustZone to its customers. TrustZone is a feature of ARM AP architectures that silicon vendors that license ARM's IP can freely chose to use or ignore. As ARM provides the TrustZone feature at no additional cost, ARM does not generate revenue from the licensing of TrustZone. More than […] semiconductor vendors have licensed TrustZone-enabled APs from ARM but only a few of them have implemented chipsets that contain a system able to support a software TEE running on top of the TrustZone architecture. In other words, the vast majority of ARM customers who could use TrustZone-based security solutions have chosen not to do so even though there is no extra charge. ARM even donated the TrustZone APIs to GlobalPlatform and thus, these APIs are available to all third parties free of charge. Moreover, at least as far as the existing licenses for ARM's v6 and v7 architecture, ARM will likely not be able to amend the existing license terms and conditions and start charging for TrustZone. As a result, since ARM does not make any profit (and is not likely to make any profit) from the licensing of TrustZone in the near future, a foreclosure strategy aimed at favouring the JV's TEE solution over competing TEE solutions may be profitable for ARM, at least in the short-run. Whilst the cost of foreclosure could increase over time (as TEE solutions gain broader market acceptance, and ARM can start charging its customers for TrustZone), the transaction may still induce ARM to favour the JV's TEE solution in order to increase its downstream revenues, at least in the short-run.

171. In other words, in the Commission's view, as of today, there appears to be limited correlation between ARM's sales of IP and the offer of TEE solutions. Hence, a foreclosure strategy by ARM is not likely to have any negative effect on ARM's core IP revenues at least in the short run. Accordingly, the Commission considers that there is a serious concern that ARM may face an incentive to foreclose the JV's competitors.

Overall likely impact on competition and consumers

Views of the notifying parties

172. The notifying parties submit that the proposed transaction will not have any foreclosure effect on the JV's TEE competitors, which will continue to be able to operate on the market by providing Trustzone and non-Trustzone-based TEE solutions.

Commission's assessment

173. The Commission observes that a significant number of respondents to the market investigation, including large MNOs and OEMs, consider that the foreclosure of competing TEE providers would negatively affect them by imposing on them a unique TEE solution and a *de facto* standard. This unique solution would not necessarily be adapted to their specific needs and this could in turn impact the retail market of trusted applications and restrict end customers' choice.

174. With respect of the impact on OEMs, Sony underlines that "*If TEE solutions of the proposed JV, G&D and/or Gemalto, which are designed to work with ARM's TrustZone, hold a monopoly position in the field of the TEE solutions in the future,*

user/customer of a TEE solution would not be able to have any other alternatives of the TEE solutions other than the TEE solution offered by the proposed JV, G&D and/or Gemalto".[98]

175. As regards the effect on end customers, FT-Orange added that: "*Pour Orange-FT il est primordial à ce stade du développement des technologies et des usages, que le consommateur puisse librement choisir les services sans que ce choix ne soit entravé artificiellement par des solutions techniques liées aux couches basses des composants/logiciels présents dans le terminal qu'il utilise : ne connaissant pas ces solutions techniques, le client ne peut pas choisir son terminal en ayant connaissance des implications que cela entrainera quant à l'usage des services et applications qui lui seront proposés par des acteurs autres que les équipementiers ou fournisseurs de solutions de sécurité.* […] *Un fournisseur de service non « choisi » par la JV ne pourra pas bénéficier de la sécurisation native de cette TEE, qui est une solution fermée. Ce fournisseur n'aura aucun choix : s'il veut accéder à des services de sécurisation d'interfaces, il devra passer par la JV, sans possibilité pour lui de bénéficier de solutions alternatives*".[99]

176. Another respondent to the market investigation adds that the removal of third party TEE providers would not only remove consumer choice but also affect innovation on the TEE market.

177. The Commission considers that the foreclosure strategy described above is likely to effectively hamper third party developers from launching competing TEEs that are interoperable with the TrustZone technology. As a result customers of the JV, that is to say OEMs, are likely to be adversely affected by it, to the extent that it would restrict their choice and possibly lead to less innovation and higher prices.

178. In turn, less innovation on the TEE market/segment is likely to have a negative impact on the downstream development of pre-issuance and post-issuance of trusted applications. Trusted applications take advantage of the possibilities offered by the secure operating system, that is to say the TEE, in order to provide a value added service to end-customers. Hence, less choice on the TEE market/segment could lead to hamper the development of certain innovative trusted applications. This would in turn restrict consumer choice for MNOs (in the case of pre-issuance trusted applications) and for end-customers (in the case of post-issuance trusted applications).

Overall conclusion

179. In light of the above, the Commission considers that, post transaction, ARM would likely have the ability and the incentive, due to its strong position upstream in the supply of IP for AP for CE devices, to foreclose and/or marginalise the JV's competitors in the market for the provision of TEE services and that therefore the proposed transaction raises serious doubts as to its compatibility with the internal market.

---

98 Customers' replies to the Commission's request for information sent on 17 September 2012, response by Sony to question 28.

99 MNO's replies to the Commission's request for information sent on 17 September 2012, response by France Télécom to question 31.

Contractual tying between ARM's IP and the JV's TEE

180. A few respondents to the market investigation also indicated that, following the proposed transaction, ARM could potentially leverage its position in IP for APs for CE devices by contractually tying its IP offering with the JV's TEE solution.

181. The Commission considers that this concern is unlikely to materialize for a number of reasons, including the fact that ARM's customers are mainly silicon vendors, while the customers of the JV's TEE solutions will likely also be OEMs. It would therefore be very difficult for ARM to engage in any contractual tying vis-à-vis these OEM customers, which will not have a direct contractual relationship with ARM.

182. Moreover, with specific respect to ARM's direct customers, the Commission considers that ARM would likely not have the incentive in engaging in any such conduct. Indeed, contrary to the type of foreclosure strategy outlined in paragraphs 145 to 163 above which would not affect ARM's relationship with its direct customers, a contractual tying strategy would likely harm ARM's sales of its core IP architecture, which would likely be negatively impacted if customers were to be forced to also license the JV's TEE solution and were not to like this conduct.

183. Based on the above, the Commission therefore concludes that the concern according to which, following the proposed transaction, ARM could potentially leverage its position in IP for APs for CE devices by contractually tying its IP offering with the JV's TEE solution should be dismissed.

4. COOPERATIVE EFFECTS OF THE JV

184. Both Gemalto and G&D have a significant presence in the provision of SEs, including, in particular, smart cards (see footnote 39). As explained, each of Gemalto and G&D will also be active in the provision of (post-issuance) trusted applications and TSMs. The Commission takes the view that the creation of the JV will not give rise to the coordination of the behaviour of Gemalto and G&D in each of these markets / segments for the following reasons:

a) Concerning the smart card activity, any coordination in this sector is not likely to be related to the present Transaction. First, the supply of smart cards is not vertically related to the JV's activity. Second, the difference in customers also excludes any conglomerate links between them. AP-based security solutions are purchased by OEMs and semiconductor manufacturers. Smart cards are instead purchased by MNOs (UICC/SIM cards) and service providers (Micro SD cards). Third, smart cards and TEEs are technically different and have different end uses. While the primary end use of smart cards is the identification and authentication of users in the network, TEEs aim at protecting services and applications against various threats and software attacks. Hence, there is no risk of meaningful anti-competitive coordination, related to the present Transaction, between G&D and Gemalto in the smart cards industry.

b) With respect of the development of post-issuance trusted applications, it is a highly fragmented sector; G&D and Gemalto will compete with hundreds of thousands of application developers, many of which are well-established software companies. In contrast, software development is not G&D's and Gemalto's core business. Their combined market share in the medium term is expected to be lower than [10-20]%. Accordingly, there is no risk of meaningful

anti-competitive coordination between G&D and Gemalto regarding post-issuance applications.

c) As regards TSM activities, current NFC-enabled TSM customers include issuing banks, public transportation operators, and MNOs. The customer base for TEE TSMs is expected to be comparable, with potentially new players such as vendors of enterprise security, e-commerce loyalty programs, and video-on-demand services. Given the dynamic and structure of the TSM business, the shares of G&D and Gemalto is not likely to exceed [10-20]% in the medium term. Accordingly, there is no risk of meaningful coordination between G&D and Gemalto.

Overall conclusion of the competitive assessment

185. Given the above, the Commission has serious doubts as to the compatibility of the transaction with the internal market. In particular, the Commission considers that, due to its very strong position in the upstream market for the licensing of IPs for APs for CE devices, post transaction, ARM would likely have the ability and incentive to favour the JV over competing providers of TEE solutions in the provision of the necessary information for the JV's competitors to be able to develop a TEE solution based on ARM's hardware architecture. This, in turn, would likely lead to a reduction of competition in the market for the provision of TEE solutions since these competitors will likely be unable to develop TEE solutions which interoperate with ARM's hardware architecture, which is almost omnipresent in smartphones and tablets, and which is included in the vast majority of CE devices currently existing on the market.

VI. COMMITMENTS

186. At the State of Play meeting of 4 October 2012, the Commission related to the notifying parties the following concerns based on the preliminary results of the market investigation:

a) The proposed transaction raises serious doubts as to its compatibility with the internal market as a result of ARM's ability and incentive to foreclose the JV's competitors in the provision of TEE solutions , by refusing to (fully and timely) disclose to these competitors the necessary information for competing TEE solutions to work on ARM's TrustZone hardware ("foreclosure concern").

b) Some respondents to the market investigation consider that ARM may seek to tie the grant of licence to use ARM IP to a requirement for the customer also to licence the JV's TEE solution ("tying concern", together with the foreclosure concern referred to in the following as "non-horizontal concerns").

c) A number of respondents to the market investigation consider that the proposed transaction would bring together the two most advanced TEE solutions, which could result in the creation or strengthening of a dominant position of the JV's TEE absent the timely and credible entry of competitors in the growing market/ segment of TEE solutions, and that the development of a "closed" ecosystem of trusted applications (which could not be interoperable with alternative TEEs) could raise barriers to entry for actual or potential competitors ("horizontal concern").

187. In order to address these concerns, the notifying parties submitted, on 12 October 2012, commitments (the "First Commitments"). The Commission launched a market test of the First Commitments on the same day in order to gather the views of relevant market participants on their effectiveness and their ability to restore effective competition in the markets where competition concerns were identified (the "market test").

188. Following the launch of the market test, the Commission continued its market investigation, notably by conducting a number of interviews with actual or potential competitors of the JV. In light of the responses to the market test, as well as the results of the supplementary market investigation, the Commission was able to exclude the horizontal concern and the tying concern for the reasons fully developed in sections V.2.1 and V.3.3.5 above, respectively.

189. On 22 October 2012, the Commission communicated the results of the supplementary market investigation and of the market test to the notifying parties. In accordance with the Remedies Notice,[100] the Commission informed them that its final assessment shows that there are no competition concerns with respect to the horizontal and tying concerns and that the notifying parties may withdraw the unnecessary commitments that had purported to address these issues. The Commission, however, also informed the notifying parties that, based on the results of the market test, certain aspects of the commitments offered to address the foreclosure concerns should be improved. In light thereof, the notifying parties submitted a revised set of commitments on 26 October 2012 (the "Final Commitments").

190. The Commission assessed the Final Commitments, and their ability to eliminate the serious doubts raised by the proposed transaction, in line with its Notice on remedies acceptable under Council Regulation (EC) No 139/2004 and under Commission Regulation (EC) No 802/2004 (the "Remedies Notice").[101]

1. DESCRIPTION OF THE FIRST COMMITMENTS

191. To address possible non-horizontal concerns related to ARM's position in the provision of IP for APs for CE devices, ARM commits, for a period of eight years after the adoption of the decision, to:

a) Continue to make the "TrustZone Secure Monitor Code"[102] needed for a TEE solution to run on ARM's architecture V6 and V7 processors available free of charge on the ARM website. ARM will also make other information, if any,

---

100 Paragraph 84 of the Remedies Notice.

101 OJ C 267, 22.10.2008, p.1.

102 According to the notifying parties, the TrustZone Secure Monitor Code manages the state of the AP, transitioning it between Non-secure and Secure modes. ARM currently makes available such example secure monitor code available as source code. There is no standardised secure monitor code yet. At the most basic level, the TrustZone Secure Monitor Code stores register level information, or context onto the stack, and enables the registers to hold secure data. This level is implementation independent and is the same for all ARM V6 and ARM V7 processors. Chipset manufacturers can significantly increase the TrustZone Secure Monitor Code's complexity depending on the system-level hardware and the device being manufactured.

needed for a TEE solution to run on ARM architecture V6 and V7 processors available to developers of TEE solutions no later than and on no worse terms as it makes the same available to the JV or any of the other JV parent companies;

b) Make any new version of the TrustZone Secure Monitor Code and other information, if any, needed for a TEE to run on future ARM-designed processors containing TrustZone available upon request to developers of TEEs no later than and on no worse terms as it makes this information available to the JV or any of the other JV parent companies;

c) Not require or incentivize its customers to use the JV's TEE solution by way of tying the grant of a license to use ARM intellectual property to a requirement for the customer also to license the JV TEE solution.

192. The Parties also submitted some commitments related to other preliminary concerns raised by the Commission related to the JV's market position in the provision of TEE and TSM services. Once it was able to dismiss these concerns, the Commission asked the Parties to take back the remedies aimed at addressing them.

193. Finally, to ensure the effective implementation of the First Commitments, the notifying parties committed to appoint a Monitoring Trustee approved by the Commission to carry out the functions specified in the commitments. The notifying parties also committed to provide for a fast-track dispute resolution procedure in the event that any dispute arises out of their implementation.

2. ANALYTICAL FRAMEWORK

194. Where a concentration would likely raise serious doubts as to its compatibility with the internal market, the parties may seek to modify the proposed concentration in order to resolve the competition concerns.

195. Under the Merger Regulation, it is the responsibility of the Commission to show that a concentration would be likely to raise serious doubts as to its compatibility with the internal market. By contrast, it is for the parties to the concentration to put forward appropriate commitments. The Commission only has the power to accept commitments that are deemed capable of rendering the concentration compatible with the internal market so that they will prevent any significant impediment to effective competition in all relevant markets where competition concerns were identified. To this aim, the commitments have to eliminate the competition concerns entirely and have to be comprehensive and effective from all points of view.[103]

3. ASSESSMENT OF THE FIRST COMMITMENTS

196. In this section, the Commission assesses the First Commitments addressing the foreclosure concerns related to ARM's position in the upstream market of IP licensing for APs for CE devices. For the reasons set out in paragraph 188 above, the Commission does not assess the First Commitments addressing the potential horizontal concerns or the tying concern.

---

[103] Paragraph 9 of the Remedies Notice.

3.1. Sufficiency of interoperability information

197. The market test provided mixed results with respect to the question whether the scope of the information proposed to be provided by ARM in its commitment to make available to third party TEE developers current and new versions of the TrustZone Secure Monitor Code, as well as other information needed for a TEE to run on ARM architecture, is sufficient.[104] According to a number of respondents, the scope of the information is insufficient and/or unclear and the commitments should contain a more detailed list of the technical information that third parties would require from ARM.

198. In particular, one OEM expressly listed certain technical information that should be included into the commitments including, amongst others, the ARM architecture reference manual and other technical reference manuals, ARM's hardware library (i.e., required hardware IP blocks/ components), software architecture (description of the interfaces of the system), its reference design (including design brief, example use cases and reference system specification). It further referred to the TrustZone Security Whitepaper as a necessary source of documentation.[105]

199. According to one TSM provider, beside the technical documentation, the "security guidelines for implementation" should also be provided to ensure competing companies can develop and deploy similar solutions.[106]

200. According to one MNO, ARM should provide the source code (or at least a very precise description of the API) of its TrustZone Secure Monitor Code to enable alternative TEEs to be compatible with ARM.[107]

201. The Commission considers that it is crucial to define a more detailed list of "other information" that would be necessary or useful for third party TEE providers to develop and optimize their TEE solution making use of ARM's TrustZone (or similar future ARM technology). The Commission finds that suggestions in paragraphs 198 above and 199 above provide useful guidance.

202. With respect to the suggestion in paragraph 200 above, the Commission understands from ARM that the TrustZone Secure Monitor Code that ARM currently makes available is provided as source code as it is typically modified for a given AP implementation by semiconductor manufacturers. Furthermore, the First Commitments define TrustZone Secure Monitor Code as "*small piece of low-level example software that executed within the Secure Monitor Mode of TrustZone-enable ARM processors*", and therefore ensures that the TrustZone Secure Monitor Code will continue to be provided as source code.

203. The market test also sought respondents' views as to the point in time at which ARM typically makes available technical specifications to semiconductor manufacturers and, specifically, users of its TrustZone hardware extension. One semiconductor

---

[104] Replies to the remedies market test questionnaire sent on 12 October 2012, question 2.

[105] Replies to the remedies market test questionnaire sent on 12 October 2012, question 3.

[106] Replies to the remedies market test questionnaire sent on 12 October 2012, questions 2 and 3.

[107] Replies to the remedies market test questionnaire sent on 12 October 2012, question 3.

manufacturer pointed out that specifications are provided at the time the ARM IP license is executed with semiconductor vendors.[108] The Commission understands from ARM that this is typically the case when the architecture is officially launched or publicly released, although, before that, there may be limited releases covered by Non-Disclosure Agreements to specific semiconductor partners of non-finalised versions, for purposes of testing and receiving feedback.[109] Once launched or publicly released, the Commission understand that it usually takes between 12 and 18 months before the APs based on the new architecture (potentially incorporating TrustZone) are released and shipped to the market.[110] During this period, TEE solution providers can adapt their TEE solution to the new architecture and integrate it with the new ARM-based chipsets provided by various semiconductor manufacturers.

204. The provisions relating to the timing at which ARM commits to make available future versions of ARM architecture and TrustZone included in the First Commitments stipulate that relevant information should be released no later than the point in time when ARM makes these information available to the JV. While these provisions implementing the principle of non-discrimination are appropriate, the Commission considers that the monitoring of the timing provisions would be improved by adding a clear point in time by which, at the latest, ARM would need to make new versions of the TrustZone Secure Monitor Code – which is at the heart of the interoperability commitment - available to both the JV and its competitors.

3.2. Additional commitments and clarifications regarding interoperability

205. When asked whether the commitments would be sufficient to remove the foreclosure concern, the market test yielded mixed results and a number of clarifications were proposed by respondents:[111]

a) The First Commitments explicitly mention only versions V6 and V7 of ARM's AP architecture, which were released in 2002 and 2007, respectively. A number of respondents pointed out that the commitments should contain an express reference at least to the forthcoming version (V8), which was announced by ARM in 2011 and will be commercially released, according to ARM, before the end of 2012.

b) Moreover, a number of respondents suggested that, with respect to future releases of its architecture, ARM publishes a summary or a reference to the key terms of the license under which the relevant technical information would be made available to third parties.[112]

c) A number of respondents are concerned about the licensing terms of the IP related to ARM's TrustZone technology, such as the TrustZone Secure Monitor

---

[108] Replies to the remedies market test questionnaire sent on 12 October 2012, question 5.

[109] Replies of the notifying parties of 18 October 2012 to the Commission's request for information dated 16 October 2012, question 2a.

[110] Replies to the remedies market test questionnaire sent on 12 October 2012, question 5.

[111] Replies to the remedies market test questionnaire sent on 12 October 2012, question 1.

[112] Replies to the remedies market test questionnaire sent on 12 October 2012, question 4.

Code in particular, with respect to future architectures (V8 and beyond). Some respondents suggest that terms should be royalty-free, while others consider that it should at least be a license based on a fair, reasonable and non-discriminatory ("FRAND") requirement.[113]

d) One actual or potential competitor submitted that the First Commitments do not prevent ARM from using its patents (or other IP) for litigating against TEE providers competing with the JV. Customers would also be reluctant to rely on a competing TEE provider because of the risk of litigation.[114]

e) One OEM suggests that the First Commitments do not cover the scenario where ARM would integrate the JV's TEE solution as part of ARM's specifications (for instance by requiring the use of the JV's TEE to boot an ARM-based AP).[115] Therefore, ARM should commit to not integrating the JV's TEE as part of the ARM's specification, as licenses granted by ARM may provide for limited flexibility to alter the architecture they license.

f) One semiconductor manufacturer submitted that the JV should support all potential ARM-based system-on-chip ("SOC") implementations by providing a hardware abstraction layer for TrustZone.[116] The respondent refers to a scenario in which ARM would release new IP related to other security components of the SOC hardware that ARM would technically tie to the TrustZone technology, thereby potentially foreclosing other TEEs. The development and publication of a hardware abstraction layer would allow other providers to develop a TEE solution that would still interoperate with ARM's IP related to both TrustZone technology and other security components.

206. The Commission considers that the suggestion submitted under point a) in paragraph 205 above is appropriate and relevant given the imminent launch of ARM's V8 architecture. With respect to points b) and c), the Commission considers that ARM should be prevented from discriminating between the JV and competing providers of TEE solutions and that the publication of standard terms and conditions for the licensing of the relevant IP would help monitoring ARM's compliance with any such non-discrimination commitment. As regards point d), the Commission considers that the commitments should provide for the unrestricted use of ARM's TrustZone-related software and information by TEE providers competing with the JV.

207. With respect to point e) above, the Commission considers that a commitment not to integrate the JV's TEE with ARM specifications would be excessive, as it is not excluded that there could be technical benefits in proposing such solution to the market. However, the Commission agrees that the competition concerns identified in section V.3.3.4 include a situation in which ARM would intentionally design its AP architecture to degrade the performance of TEE solutions other than the one

---

[113] Replies to the remedies market test questionnaire sent on 12 October 2012, question 4.

[114] Replies to the remedies market test questionnaire sent on 12 October 2012, question 1 and 13.

[115] Replies to the remedies market test questionnaire sent on 12 October 2012, question 6 and 7.

[116] Replies to the remedies market test questionnaire sent on 12 October 2012, question 1.

provided by the JV. The commitments therefore should be complemented by a provision addressing this concern.

208. With respect to point f) above, the Commission considers the concern to be expressed by the respondent to be highly speculative at this stage. This conclusion essentially reflects the fact that, as the Commission understands it, as of today ARM is not yet active in the provision of the new IP related to other security components of the SOC hardware that ARM would allegedly tie to TrustZone. It is therefore unclear if and when ARM would develop any such IP.

3.3 Duration of the interoperability commitments

209. Finally, the vast majority of respondents to the relevant question consider that a period of eight years is adequate for the commitments addressing the foreclosure concerns.[117] The Commission considers that an eight year duration is appropriate to ensure the effectiveness of the commitments.

4. FINAL COMMITMENTS

210. Following the communication to the notifying parties of the Commission's assessment of the First Commitments including the market test, the notifying parties submitted a revised and final set of commitments on 26 October 2012.

211. The Final Commitments now define as "TrustZone Information" all information that is necessary or useful to developers of TEE solutions that utilize ARM's TrustZone functionality, being in respect of ARM architecture V6, V7 and the forthcoming architecture V8. It lists as such a number of technical information and tools that are listed and described in paragraph 221 below.

212. To address the foreclosure concern, ARM commits, for a period of eight years after the adoption of the decision, to:

a) Continue to make the TrustZone Secure Monitor Code needed for a TEE solution to run on ARM's architecture V6 and V7 processors available free of charge on the ARM website. ARM now commits to also immediately make TrustZone Information in respect of ARM architectures V6 and V7 available via the ARM website on no worse terms as it makes the same available to the JV or any of the other JV parent companies.

b) Make the TrustZone Secure Monitor Code needed for a TEE to run on ARM's (forthcoming) architecture V8 available free of charge on the ARM website, along with the TrustZone Information on no worse terms than it makes the same available to the JV or any of the other Parents, no later than as provided to the JV or other Parents, and in any case, within six months of the launch date of ARM architecture V8.

c) Make any new version of the TrustZone Secure Monitor Code or any other equivalent software as well as any other TrustZone Information for future ARM Achitectures available upon request on terms that are no worse than those on

[117] Replies to the remedies market test questionnaire sent on 12 October 2012, question 8.

which such information is made available to the JV or any other JV parent companies and no later than the earlier of the (i) date they are made available to the JV or any other Parents; or (ii) the date of the release of the new version of the TrustZone Secure Monitor Code.

d) Publish on its website the standard terms and conditions of any license required to obtain access to the TrustZone Secure Monitor Code and TrustZone Information for existing and future ARM architectures, no later than the relevant information is made available under the Commitments.

e) Not design its intellectual property intentionally to degrade performance of third-party TEEs.

213. Finally, the Final Commitments provide for a Monitoring Trustee approved by the Commission to carry out the functions specified in the commitments to ensure their effective implementation. The Final Commitments also foresee a dispute settlement procedure including fast-track arbitration in the event that any dispute arises out of their implementation.

5. COMMISSION'S ASSESSMENT OF THE FINAL COMMITMENTS

214. According to the Remedies Notice, commitments have to eliminate the competition concerns entirely and have to be comprehensive and effective from all points of view. Furthermore, commitments must be capable of being implemented effectively within a short period of time as the conditions of competition on the market will not be maintained until the commitments have been fulfilled.[118]

215. Furthermore, the Remedies Notice specifies that commitments in phase I can only be accepted where the competition problem is readily identifiable and can easily be remedied. The competition problem therefore needs to so straightforward and the remedies so clear-cut that it is not necessary to enter into an in-depth investigation and that the commitments are sufficient to clearly rule out 'serious doubts' raised by the transaction.[119]

216. Accordingly, the Commission assesses in the following whether the Final Commitments are:

a) Compatible with the remedies policy principles;

b) Sufficient to clearly rule out serious doubts raised by the transaction; and

c) Capable of being implemented effectively within a short period of time.

5.1 The Final Commitments are compatible with the remedies policy principles

217. The Remedies Notice provide that, whilst being preferred remedy, divestitures or the removal of links with competitors are not the only remedy possible to eliminate certain competition concerns. The Commission may accept other types of commitments, but

---

[118] Paragraph 9 of the Remedies Notice.

[119] Paragraph 81 of the Remedies Notice.

only in circumstances where the other remedy proposed is at least equivalent to a divestiture with respect to its effects.[120]

218. In a number of cases, the Commission has accepted remedies foreseeing the granting of access to key technology, including patents, know-how or other IP rights, and essential inputs. Normally, the parties grant such access to third parties on a non-discriminatory and transparent basis.[121] The control of key technology may lead to concerns of foreclosure of competitors which depend on the technology as essential input for the activities in a downstream market. This, for example, concerns cases where competition problems arise as the parties may withhold information necessary for the interoperability of different equipment. In such circumstances, commitments to grant competitors access to the necessary information may eliminate the competition concerns.[122]

219. According to the Remedies Notice, commitments should then foresee the disclosure of information on a non-exclusive basis to all third parties which depend on the information for their activities. It has to be ensured that the terms and conditions for the granting of information do not impede the effective implementation of such a license remedy. If no clearly determined terms and conditions for the granting of licenses exist in the market at stake, the terms and conditions, including the pricing, should be clearly apparent from the commitments. Generally, the Commission will only accept such commitments if it can be concluded that they will be effective and competitors will likely use them.

220. Access remedies are also adequate in the present case and compatible with the Remedies Notice. In the vertical case at stake, remedies other than divestiture remedies appear best suited to directly address the concerns raised. The serious doubts raised by the proposed transaction are related to the timely access to comprehensive information necessary or useful for TEE providers to develop a TEE solution using ARM's TrustZone technology. The investigation in this case revealed that TrustZone is a key input for competing TEE providers and that the notifying parties could potentially withhold that information and possibly impede the capacity of the JV's competitors to develop a TEE solution based on ARM's TrustZone technology. In these circumstances, commitments to grant competitors of the JV access to the necessary information would eliminate the competition concerns.[123]

5.2 The Final Commitments are sufficient to clearly rule out serious doubts raised by the proposed transaction

Sufficiency of interoperability information

221. With respect to the scope of TrustZone-related information necessary or useful for TEE providers, the Commission requested the notifying parties to provide a list of, and describe, all information and/or tools, relevant for any semiconductor manufacturer to

---

120 Paragraph 61 of the Remedies Notice.

121 Paragraph 62 of the Remedies Notice.

122 Paragraph 65 of the Remedies Notice.

123 Cases: M.5984 *Intel/McAfee* of 26 January 2011, M.3083 *GE/Instrumentarium* of 2 September 2003 and M.2861 *Siemens/Draegerwerk* of 30 April 2003.

fully and effectively implement ARM TrustZone in a processor/ chipset, and relevant for any TEE provider to be able to full rely on ARM TrustZone for implementing their TEE solution, including information/ tools that are currently available, after registration, on ARM's website, that ARM typically provides to licensees of ARM's intellectual property or that ARM typically provides with respect to updates, optimization measures, bug fixes. The notifying parties responded with a list of information and tools including:[124]

a) ARM architecture reference manual defining the TrustZone security extensions to the ARM architecture;

b) Technical reference manuals for the ARM Cortex A class processors, which implement the security extensions;

c) System-wide hardware IP, described as a number of additional components of intellectual property, which ARM produces and licenses under an implementation license, that could be used as part of a secure system (based around TrustZone or otherwise). These include bus fabric IP, interrupt controllers, memory controllers, and address space controllers.

d) TrustZone white paper entitled "Building a Secure System using TrustZone Technology" described as non-essential guidance.

e) Platform design documents offering sample designs and helping hardware and software system architects who require more guidance.

f) ARM TrustZone training courses in respect of ARM architecture

g) Updates such as the ARM manual errata list

222. The Final Commitments explicitly reference and define as "TrustZone Information" all of the information listed in paragraph 222 above, as well as "equivalent information" with respect to any future ARM architectures. This TrustZone Information (or equivalent information related to future ARM architectures) needs to be made available to developers of TEE in respect of current and future ARM architectures. The scope of the interoperability information now covers the information that respondents to the market test identified as relevant for actual or potential TEE providers. Therefore, the Commission considers that the Final Commitments appropriately cover all interoperability information necessary of useful for competing TEE providers that rely on ARM's TrustZone technology.

223. Another improvement of the Final Commitments regards the addition of a clear point in time by which ARM would need to make new versions of the TrustZone Secure Monitor Code and the relevant TrustZone Information available to both the JV and its competitors at the latest. For the avoidance of doubt, the Final Commitments continue to stipulate that this information, as well as any TrustZone Information, needs to be made available to third parties no later than it is made available to the JV or its other parent companies.

---

[124] Replies of the notifying parties of 21 October 2012 to the Commission's request for information dated 18 October 2012.

224. As for ARM architecture V8 (now expressly mentioned in the text of the commitments, see paragraph 225 below), the Final Commitments provide that in any event the TrustZone Secure Monitor Code is made available no later than within six months of the launch date of ARM architecture V8. The Commission understands from ARM that the latter may need this time to be able to test and finalise the software code following the launch of the architecture V8. The Commission finds this provision acceptable given that the Final Commitments prevent ARM from sharing the software code with the JV or its other parent companies earlier than with competing TEE providers. As for versions following architecture V8, the Final Commitments provide that the new version of the TrustZone Secure Monitor Code will be provided, upon request, to any third party no later than it is released.

Additional commitments and clarifications regarding interoperability

225. The Final Commitments now contain an express reference to ARM's forthcoming architecture V8. ARM commits to make the TrustZone Secure Monitor Code needed for a TEE to run on ARM Architecture V8 available free of charge on its website.

226. Furthermore, ARM now commits to publish on its website the standard terms and conditions of any license required to obtain access to TrustZone Information for existing and future ARM architectures. The Commission considers that, in line with suggestions by respondents to the market test, this will enable sufficient transparency of the terms and conditions. Moreover, the Final Commitments prevent ARM from granting the JV or its other parent companies more favourable conditions than the JV's competitors.

227. Moreover, the Final Commitments now also specify that ARM makes the TrustZone Secure Monitor Code (or equivalent software) as well as TrustZone Information available in order to enable developers of TEEs "to develop, market, sell or otherwise commercially exploit competing TEEs". This clarification allows the unrestricted use of this software and information by TEE providers competing with the JV. This should address, amongst others, the concern submitted by a respondent to the market test that ARM could use its patents (or other IP) for litigating against competing TEE providers.

228. Finally, ARM now commits to not design its IP intentionally to degrade the performance of third-party TEEs. This provision will cover the scenario raised in the market test in which ARM would integrate the JV's TEE as part of the ARM specification in a way that degrades – or makes impossible - the operation of an alternative TEE solution.

Duration of the interoperability commitments

229. In the light of the market test's results confirming the sufficiency of the commitments' duration, the Commission considers that the eight-year period is appropriate to address the serious doubts raised by the proposed transaction. ARM will shortly launch a new AP design (V8). Considering that ARM's product life cycle is five to eight years, the period is likely to provide sufficient assurances to current and prospective ARM licensees, including TEE providers competing with the JV, which may be making product development decisions several years after the Effective Date[125], that when their

[125] The effective date (as defined on the first page of the commitments annexed to the present decision), is the date of adoption of the present decision

TEE products are ready for launch they will be protected against any risk of discriminatory treatment by ARM.

Enforcement provisions of the commitments

230. The Final Commitments include both a section on a Monitoring Trustee and a section on a dispute settlement procedure including a fast-track arbitration procedure.

231. The Final Commitments provide for the appointment of a Monitoring Trustee to be approved by the Commission and to carry out obligations consistent with the Commission's precedents[126] in this area. The function, mandate and related provisions provided for in the Final Commitments are in line with the Commission standard requirements for commitments, according to which the monitoring trustee must be in a position to act as the Commission's 'eyes and ears' to ensure the compliance of the parties with the commitments. The Monitoring Trustee is also involved in the initial bilateral dispute resolution before triggering arbitration.

232. The Final Commitments also provide for a dispute settlement mechanism, including a fast track arbitration procedure. Given that the arbitration court may make a preliminary ruling within one month and the final ruling shall be rendered within six months, the procedure should allow third-party TEE providers to enforce any breach of the commitments quickly. Furthermore, the Commission has the possibility to get involved in the arbitration procedure.

233. It can be concluded that the enforcement provisions enable an effective and efficient implementation of the commitments.

Conclusion on the sufficiency of the Final Commitments

234. For the above reasons, the Commission concludes that the Final Commitments are sufficient to clearly eliminate serious doubts that the formation of the JV might give ARM the incentive and ability to favour the JV in its IP licensing activities.

5.3. The Final Commitments are capable of being implemented effectively within a short period of time

235. The Final Commitments will enter into force as of the Effective Date. The Monitoring Trustee will be appointed normally within two weeks after the Effective Date. Accordingly, the Commitments are capable of being implemented effectively within a short period of time.

5.4 Conclusion

236. For the reasons outlined above, the Final Commitments entered into by the notifying parties are adequate and sufficient to eliminate the serious doubts as to the compatibility of the transaction with the internal market.

237. The Final Commitments annexed to the present decision constitute obligations attached to this decision, as only through full compliance therewith can the structural changes in the relevant markets be achieved.

---

[126] See for example Case M.5984 *Intel/McAfee* of 26 January 2011.

VII. CONCLUSION

238. For the above reasons, the Commission has decided not to oppose the notified operation as modified by the commitments and to declare it compatible with the internal market and with the functioning of the EEA Agreement, subject to full compliance with the obligations in the commitments annexed to the present decision. This decision is adopted in application of Article 6(1)(b) in conjunction with Article 6(2) of the Merger Regulation.

For the Commission
(signed)

Joaquín ALMUNIA
Vice-President

October 26, 2012

By hand and by fax: 00 32 2 296 4301
European Commission – DG Competition Rue Joseph II 70 Jozef-II straat B-1000 BRUSSELS

Case M. 6564 - ARM/G&D/Gemalto/JV

COMMITMENTS TO THE EUROPEAN COMMISSION

Pursuant to Article 6(2) of Council Regulation (EC) No. 139/2004 as amended (the "***Merger Regulation***"), ARM, G&D, Gemalto and the JV (each as defined below) (together the "***Parties***" and each a "***Party"***) hereby provide the following Commitments (the "***Commitments***") in order to enable the European Commission (the "***Commission***") to declare the creation of the JV compatible with the internal market and the EEA Agreement by its decision pursuant to Article 6(1)(b) of the Merger Regulation (the "***Decision***").

The Commitments shall take effect upon the date of adoption of the Decision.

This text shall be interpreted in the light of the Decision to the extent that the Commitments are attached as conditions and obligations, in the general framework of EU law, in particular in the 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.

Definitions

For the purpose of the Commitments, the following terms shall have the following meaning:

Arbitral Tribunal: has the meaning given in paragraph 28

ARM: ARM Limited

ARM Architecture Reference Manual: the manual that defines the ARM Architecture including the security extensions to the ARM Architecture

ARM Architecture V6: is the sixth version of a Reduced Instruction Set Computer (RISC) architecture developed by ARM

ARM Architecture V7: is the seventh version of a Reduced Instruction Set Computer (RISC) architecture developed by ARM

ARM Architecture V8: when released will be the eighth version of a Reduced Instruction Set Computer (RISC) architecture developed by ARM

Effective Date: the date of adoption of the Decision

Gemalto: Gemalto N.V.

G&D: Giesecke & Devrient GmbH

ICC: has the meaning given in paragraph 28

Indemnified Party: has the meaning given in paragraph 19

JV: the full-function joint venture, named NEWINCCO 1150 Limited, between ARM, G&D and Gemalto

JV TEE: the new GlobalPlatform-compliant TEE to be developed and marketed by the JV

Monitoring Trustee: a person appointed in accordance with part I of Section C

Parents: ARM, Gemalto and G&D

PDD: platform design documents offering sample designs

Relevant Party: has the meaning given in paragraph 24

Rules: has the meaning given in paragraph 29

System-wide Hardware IP: a number of additional components of intellectual property, which ARM produces and licenses under an implementation license, that could be used as part of a secure system (based around TrustZone or otherwise). These include bus fabric IP, interrupt controllers, memory controllers, and address space controllers

Technical Reference Manuals for the ARM Cortex A class processors: a technical reference manual that is used to implement hardware and develop software including by developers of a TEE

TEE: trusted execution environment

TrustZone Secure Monitor Code: an extremely small piece of low-level example software that executes within the Secure Monitor Mode of TrustZone-enabled ARM processors, that switches the processor between secure and normal state

TrustZone Information: information that is necessary or useful to developers of TEE solutions that utilize ARM's TrustZone functionality, being in respect of ARM Architecture V6, V7 and V8: ARM Architecture Reference Manuals; Technical Reference Manuals for the ARM Cortex A class processors; System-wide Hardware IP; TrustZone White Paper; PDDs and ARM TrustZone training courses, as applicable, and equivalent information with respect to any future ARM Architecture, together with any updates thereto

TrustZone White Paper: ARM's white paper called "Building a Secure System using TrustZone Technology"

Section A. Purpose

1. The Parties understand that the Commission is concerned that ARM may withhold from third-party TEE suppliers information necessary for tees to run on ARM-designed processors containing trustzone when the processor manufacturer decides to implement trustzone into its chip and/or chipset.

2. Pursuant to the commitments in Section B below, ARM intends that, following the creation of the JV, it will make available to third-party TEE suppliers information which is necessary for TEEs to run on TrustZone no later than and on no worse terms than it makes the same available to the JV or any of the other Parents. ARM also intends to design its intellectual property in a way that will not intentionally degrade performance of third-party TEEs.

3. ARM therefore makes the following commitments to address the Commission's concerns.

Section B. TrustZone

4. ARM has made and will continue to make the TrustZone Secure Monitor Code needed for a TEE to run on ARM Architecture V6 and V7 processors available free of charge on the ARM website to developers of TEEs to enable them to develop, market, sell or otherwise commercially exploit competing TEEs. ARM will also make TrustZone Information in respect of ARM Architectures V6 and V7 available via the ARM website to developers of TEEs to enable them to develop, market, sell or otherwise commercially exploit competing TEEs, no later than the Effective Date and on no worse terms than it makes the same available to the JV or any of the other Parents.

5. ARM will make TrustZone Secure Monitor Code needed for a TEE to run on ARM Architecture V8 available free of charge on the ARM website and will make TrustZone Information for ARM Architecture V8 processors available via the ARM website to developers of TEEs to enable them to develop, market, sell or otherwise commercially exploit competing TEEs, on no worse terms than it makes the same available to the JV or any of the other Parents, no later than as provided to the JV or the other Parents, and in any case, within six months of the launch date of ARM Architecture V8.

6. ARM will make any new version of the TrustZone Secure Monitor Code, or any other equivalent software that supports future JV TEE solutions, and, upon request, other TrustZone Information for future ARM Architectures, available to developers of TEEs to enable them to develop, market, sell or otherwise commercially exploit competing TEEs, on terms that are no worse than those on which such information is made available to the JV or any other Parents and no later than the earlier of the (i) date they are made available to the JV or any other Parents; or (ii) date of the release of the new version of the TrustZone Secure Monitor Code, or any other equivalent software that supports future JV TEE solutions.

7. ARM will publish on its website the standard terms and conditions of any license required to obtain access to the TrustZone Secure Monitor Code and TrustZone Information for existing and future ARM architectures, no later than the relevant information is made available under the Commitments.

8. ARM will not design its intellectual property intentionally to degrade performance of third-party TEEs.

Section C. Monitoring Trustee

I. Appointment Procedure

9. The Parties shall appoint a Monitoring Trustee to carry out the functions specified in part II of this Section. The Monitoring Trustee shall be independent of the Parties, possess the necessary qualifications to carry out its mandate, and shall neither have nor become exposed to a conflict of interest. The Monitoring Trustee shall be remunerated by the Parties in a way that does not impede the independent and effective fulfilment of its mandate.

Proposal by the Parties

10. No later than two weeks after the Effective Date, the Parties shall submit a list of one or more persons whom the Parties propose to appoint as the Monitoring Trustee to the Commission for approval. The proposal shall contain sufficient information for the Commission to verify that the proposed Monitoring Trustee fulfils the requirements set out in paragraph 17 and shall include:

(a) the full terms of the proposed mandate, which shall include all provisions necessary to enable the Monitoring Trustee to fulfil its duties under these Commitments;

(b) the outline of a work plan which describes how the Monitoring Trustee intends to carry out its assigned tasks.

Approval or rejection by the Commission

11. The Commission shall have the discretion to approve or reject the proposed Monitoring Trustee(s) and to approve the proposed mandate subject to any modifications it deems necessary for the Monitoring Trustee to fulfil its obligations. If only one name is approved, the Parties shall appoint or cause to be appointed, the individual or institution concerned as Monitoring Trustee, in accordance with the mandate approved by the Commission. If more than one name is approved, the Parties shall be free to choose the Monitoring Trustee to be appointed from among the names approved. The Monitoring Trustee shall be appointed within one week of the Commission's approval, in accordance with the mandate approved by the Commission.

New proposal by the Parties

12. If all the proposed Monitoring Trustees are rejected, the Parties shall submit the names of at least two more candidates within two weeks of being informed of the rejection, in accordance with the requirements and the procedure set out in paragraphs 10 and 11.

Monitoring Trustee nominated by the Commission

13. If all further proposed Monitoring Trustees are rejected by the Commission, the Commission shall nominate a Monitoring Trustee, whom the Parties shall appoint, or cause to be appointed, in accordance with a trustee mandate approved by the Commission.

II. Functions of the Monitoring Trustee

14. The Monitoring Trustee shall act on behalf of the Commission to ensure ARM's compliance with the Commitments. The Commission may, on its own initiative or at the request of the Monitoring Trustee or the Parties, give any orders or instructions to the Monitoring Trustee in order to ensure compliance with the conditions and obligations. The Parties are not entitled to give instructions to the Monitoring Trustee. The Monitoring Trustee will act on behalf of the Commission as a trusted expert in the fast track dispute settlement procedure described in Section D.

15. The Monitoring Trustee shall propose to the Parties such measures as the Monitoring Trustee considers necessary to ensure ARM's compliance with the Commitments, and the Monitoring Trustee shall propose necessary measures to the Commission in the event that ARM do not comply with the Monitoring Trustee's proposals within the timeframe set by the Monitoring Trustee.

Mandate of the Monitoring Trustee

16. The Monitoring Trustee shall:

(i) broker a resolution of any dispute that arises between a third party and ARM regarding compliance with these Commitments;

(ii) advise and, if need be, make written recommendations to the Commission when any dispute between a third party and ARM regarding compliance with these Commitments is brought before the Arbitral Tribunal referred to in paragraph 28;

(iii) provide to the Commission, sending ARM a non-confidential copy at the same time, a report bi-annually during the first year that the Commitments are in effect and annually every year during the rest of the term of the Commitments as indicated in paragraph 45, regarding the status and outcome of any dispute between a third party and ARM in which the Monitoring Trustee has participated;

(iv) propose to ARM such measures as the Monitoring Trustee considers necessary to ensure compliance with these Commitments;

(v) promptly report in writing to the Commission, sending ARM a non-confidential copy at the same time, if it concludes on reasonable grounds that ARM is failing to comply with these Commitments.

17. The Monitoring Trustee shall provide a detailed work plan to the Commission within one month of its appointment, sending a copy to the Parties at the same time, describing how it intends to carry out its mandate.

III. Duties and obligations of the Parties in relation to the Monitoring Trustee

18. The Parties shall provide and shall cause their advisors to provide the Monitoring Trustee with all such cooperation, assistance and information, including copies of all relevant documents and access to relevant staff, as the Monitoring Trustee may reasonably require to perform its tasks in relation to these Commitments.

19. The Parties shall indemnify the Monitoring 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 the Parties for any liabilities arising out of the performance of its duties under the Commitments, except to the extent that such liabilities result from the wilful default, recklessness, gross negligence or bad faith of the Monitoring Trustee, its employees, agents or advisors.

20. At the expense of the Parties, the Monitoring Trustee may appoint advisors (in particular for technical or legal advice), subject to the Parties' approval (this approval not to be unreasonably withheld or delayed) if the Monitoring 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 Monitoring Trustee are reasonable. Should the Parties refuse to approve the advisors proposed by the Monitoring Trustee, the Commission may, after having heard the Parties, approve the appointment of such advisors instead. Only the Monitoring Trustee shall be entitled to issue instructions to the advisors. Paragraph 15 shall apply to the advisors mutatis mutandis.

IV. Replacement, discharge and re-appointment of the Monitoring Trustee

21. If the Monitoring Trustee ceases to perform its functions under the Commitments or for any other good cause, including its exposure to a conflict of interest:

(a) the Commission may, after hearing the Monitoring Trustee, require the Parties to replace the Monitoring Trustee; or

(b) the Parties, with the prior approval of the Commission, may replace the Monitoring Trustee.

22. If the Monitoring Trustee is removed according to paragraph 11, the Monitoring Trustee may be required to continue in its function until a new Monitoring Trustee is in place to whom the Monitoring Trustee has effected a full hand over of all relevant information. The new Monitoring Trustee shall be appointed in accordance with the procedure referred to part I of this Section.

23. Besides the removal according to paragraph 12 the Monitoring Trustee shall cease to act as Monitoring Trustee only after the Commission has discharged it from its duties after all the Commitments with which the Monitoring Trustee has been entrusted have lapsed.

Section D. Fast-track dispute resolution

24. In the event that a third party, showing a sufficient legitimate interest, claims that ARM (the "***Relevant Party***") is failing to comply with its obligations arising from these Commitments, such third party may invoke the dispute settlement procedure described in this Section.

25. The third party who seeks to initiate the procedure shall notify the Relevant Party and the Monitoring Trustee of its request and specify the reasons why it believes that the Relevant Party is failing to comply with the Commitments. The Relevant Party shall use its best efforts to resolve all differences of opinion and to settle all disputes of which it has been notified through co-operation and consultation within a reasonable period of time not to exceed fifteen working days after receipt of the request.

26. The Monitoring Trustee shall present its own proposal to the Commission, the JV and the relevant third party, for resolving the dispute within eight working days, specifying in writing the action, if any, to be taken by the Relevant Party in order to ensure compliance with the Commitments vis-à-vis the third party, and be prepared, if requested, to facilitate the settlement of the dispute.

27. Should the Relevant Party and the third party fail to resolve their differences of opinion through cooperation and consultation, the third party may initiate the arbitration process described below. The arbitration process shall be used only to resolve disputes regarding compliance with the Commitments.

28. To initiate the arbitration process, the third party shall give written notice to the Relevant Party nominating an arbitrator and stating the specific nature of the claim, the factual basis of its position and the relief requested. The Relevant Party shall appoint another arbitrator within fourteen calendar days after receipt of the written notice. The arbitrators so appointed shall appoint a third arbitrator to be president of the arbitral tribunal within seven calendar days after both arbitrators have been nominated. Should the Relevant Party fail to nominate an arbitrator, or if the two arbitrators fail to agree on the president, the default appointment(s) shall be made by the International Chamber of Commerce ("***ICC***"). All three arbitrators shall have experience and expertise in the area of embedded security software technology. The three-person arbitral tribunal shall herein be referred to as the "***Arbitral Tribunal***".

29. The dispute shall be finally resolved by arbitration under the ICC Rules of Arbitration, with such modifications or adaptations as foreseen herein or necessary under the circumstances (the "***Rules***"). The arbitration shall be conducted in London, England, in the English language.

30. The procedure shall be a fast-track procedure. For this purpose, the Arbitral Tribunal shall shorten all applicable procedural time-limits under the Rules as far as appropriate in the circumstances.

31. The Arbitral Tribunal shall, as soon as practical after the confirmation of the Arbitral Tribunal, hold an organisational conference to discuss any procedural issues with the parties to the arbitration. Terms of Reference shall be drawn up and signed by the parties to the arbitration and the Arbitral Tribunal at the organisational meeting or thereafter and a procedural time-table shall be established by the Arbitral Tribunal. An oral hearing shall, as a rule, be established within two months of the confirmation of the Arbitral Tribunal.

32. In order to enable the Arbitral Tribunal to reach a decision, it shall be entitled to request any relevant information from the Relevant Party or the third party, to appoint experts and to examine them at the hearing, and to establish the facts by all appropriate means. The Arbitral Tribunal is also entitled to ask for assistance by the Monitoring Trustee in all stages of the procedure.

33. The arbitrators shall agree in writing to keep any confidential information and business secrets disclosed to them in confidence. The Arbitral Tribunal may take the measures necessary for protecting confidential information in particular by restricting access to confidential information to the Arbitral Tribunal, the Monitoring Trustee and outside counsel and experts of the opposing party.

34. The burden of proof in any dispute governed under the Rules shall be borne as follows:

(i) the party who has requested the arbitration must produce evidence of a prima facie case;

(ii) if that party does so, the Arbitral Tribunal must find in favour of the requesting party unless the Relevant Party can produce evidence to the contrary.

35. The Commission shall be allowed and enabled to participate in all stages of the procedure by:

(a) receiving all written submissions (including documents and reports, etc.) made by the parties to the arbitration;

(b) receiving all orders, interim and final awards and other documents exchanged by the Arbitral Tribunal with the parties to the arbitration (including Terms of Reference and procedural time-table);

(c) filing any Commission amicus curiae briefs; and

(d) being present at the hearing(s) and being allowed to ask questions to parties, witnesses and experts.

The Arbitral Tribunal shall forward, or shall order the parties to the arbitration to forward, the documents mentioned to the Commission without delay.

36. In the event of disagreement between the parties to the arbitration regarding the interpretation of the Commitments, the Arbitral Tribunal shall inform the Commission and may seek the Commission's interpretation of the Commitments before finding in favour of any party to the arbitration and shall be bound by the interpretation.

37. The Arbitral Tribunal shall decide the dispute on the basis of the Commitments and the Decision. The Commitments shall be construed in accordance with the Merger Regulation, EU law and general principles of law common to the legal orders of the Member States without a requirement to apply a particular national system. The Arbitral Tribunal shall take all decisions by majority vote.

38. Upon request of the third party, the Arbitral Tribunal may make a preliminary ruling on the Dispute. The preliminary ruling shall be rendered within one month after the confirmation of the Arbitral Tribunal, shall be applicable immediately and, as a rule, remain in force until a final decision is rendered.

39. The Arbitral Tribunal shall, in the preliminary ruling as well as in the final award, specify the action, if any, to be taken by the Relevant Party in order to comply with the Commitments vis-à-vis the third party (e.g. specify a contract including all relevant terms and conditions). The final award shall be final and binding on the parties to the arbitration and shall resolve the dispute and determine any and all claims, motions or requests submitted to the Arbitral Tribunal. The arbitral award shall also determine the reimbursement of the costs of the successful party and the allocation of the arbitration costs. In case of granting a preliminary ruling or if otherwise appropriate, the Arbitral Tribunal shall specify that terms and conditions determined in the final award apply retroactively.

40. The final award shall, as a rule, be rendered within six months after the confirmation of the Arbitral Tribunal. The time-frame shall, in any case, be extended by the time the Commission takes to submit an interpretation of the Commitments if asked by the Arbitral Tribunal.

41. The parties to the arbitration shall prepare a non-confidential version of the final award, without business secrets. The Commission may publish the non-confidential version of the award.

42. Nothing in the above-described arbitration procedure shall affect the powers of the Commission to take decisions in relation to the Commitments in accordance with its powers under the Merger Regulation and the Treaty on the Functioning of the European Union.

Section E. General Provisions

43. If the JV is abandoned, unwound or otherwise terminated, these Commitments shall automatically cease to apply.

44. If the approval of the JV by another Governmental authority is made subject to requirements that are potentially inconsistent with these Commitments, ARM may request a review and adjustment of these Commitments in order to avoid such inconsistencies.

45. These Commitments shall be effective worldwide and shall remain in effect for 8 years from the Effective Date.

Section F. Review

46. The Commission may, where appropriate, in response to a request from ARM showing good cause and accompanied by a report from the Monitoring Trustee, waive, modify or substitute, in exceptional circumstances, one or more of the undertakings in these Commitments.

(signed)

duly authorised for and on behalf of
ARM Limited

……

duly authorised for and on behalf of
Gemalto N.V.

(signed)

duly authorised for and on behalf of
Giesecke & Devrient GmbH

(signed)

duly authorised for and on behalf of
NEWINCCO 1150 Limited