# Appendix A



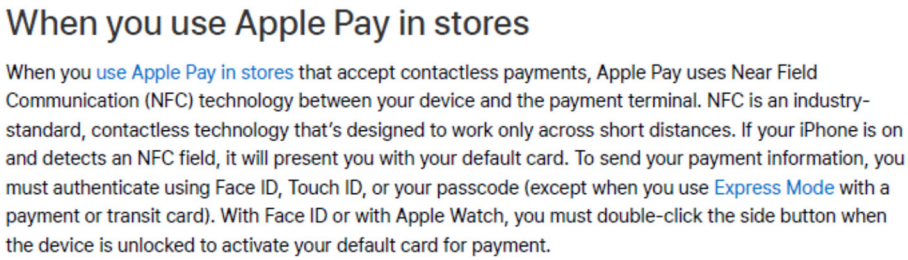
APPLE 1052

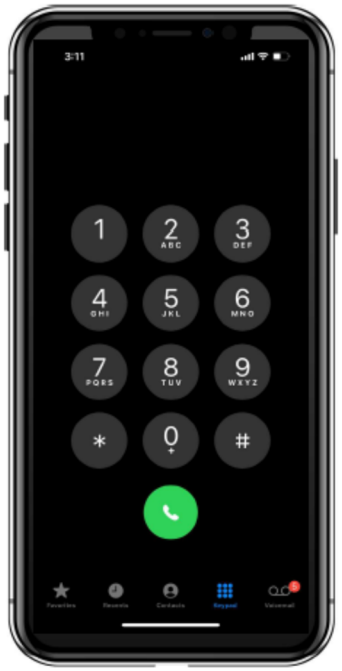
## Appendix A: Claim Chart for U.S. Patent No. 8,127,984

| Claim No. | Claim Language | Accused Products[1],[2],[3] |
|---|---|---|
| 1[a] | A method for providing a radio frequency identification (RFID) from a switchable mobile communications device capable of RFID communication and voice call communication, the method comprising: | To the extent that the claim's preamble is determined to be a limitation or otherwise limiting, the Accused Products perform a method for providing RFID from a switchable mobile communications device capable of RFID communication and voice call communication, comprising the steps in the subsequent limitations.<br><br>For example, as reflected in Apple's product literature, the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (*e.g.*, via LTE, CDMA, UMTS, and/or GSM), and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling), as well as RFID communication (*e.g.*, via RFID/NFC, including via Apple Pay, which uses NFC technology between the device and the payment terminal).<br><br>**Audio Calling**[5]<br>▪ FaceTime audio<br>▪ Voice over LTE (VoLTE)[6]<br>▪ Wi-Fi calling[6] |

[1] Accused Products, as used herein, are defined in the cover document to Varia's Preliminary Infringement Contentions. As set forth in the cover document to Varia's Preliminary Infringement Contentions, this is based on Varia's present understanding without the benefit of discovery.
[2] The citations in this Claim Chart are exemplary and illustrative. Varia reserves the right to amend and/or supplement these Contentions, including this Claim Chart, in any manner and for any of the reasons set forth in the cover document to Varia's Preliminary Infringement Contentions, including this Claim Chart, including after a complete production of the relevant source code and other non-public technical information and claim construction.
[3] This Claim Chart incorporates Appendix D by reference in its entirety. Appendix D is based on publicly available information without the benefit of discovery. Varia reserves the right to amend and/or supplement Appendix D, in any manner and for any of the reasons set forth in the cover document to Varia's Preliminary Infringement Contentions, including this Claim Chart, including after a complete production of the relevant source code and other non-public technical information and claim construction.

| | | |
|---|---|---|
| | | **Cellular and Wireless**<br>■ **Model A1660**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>TD-SCDMA 1900 (F), 2000 (A)<br>CDMA EV-DO Rev. A (800, 1900, 2100 MHz)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **Model A1778**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **All models**<br>802.11ac Wi-Fi with MIMO<br>Bluetooth 4.2 wireless technology<br>NFC with reader mode<br>Express Cards<br>(VAR0000849-855).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (*e.g.*, Via LTE, LTE, CDMA, UMTS, GSM, and/or 5G) and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling), as well as RFID communication (*e.g.*, via RFID/NFC, including via Apple Pay, which uses NFC technology between the device and the payment terminal). (VAR0000639-1074). |

| | | |
|---|---|---|
| | |  <br>(VAR0000010-14).<br><br>NFC is a subset within the family of RFID technology. (VAR0000026-42) ("RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology."); (VAR0000043-53) ("Hierarchically, NFC is a subset of RFID.")).<br><br>For example, the iPhone as a whole is capable of entering two different modes, including a telephony mode and an RFID/NFC mode. A user can affirmatively launch the telephony and/or RFID/NFC modes, and/or the iPhone enters the telephony and/or RFID/NFC mode when its received the relevant signal (e.g., an incoming call or detecting an RFID reader), as shown below. |

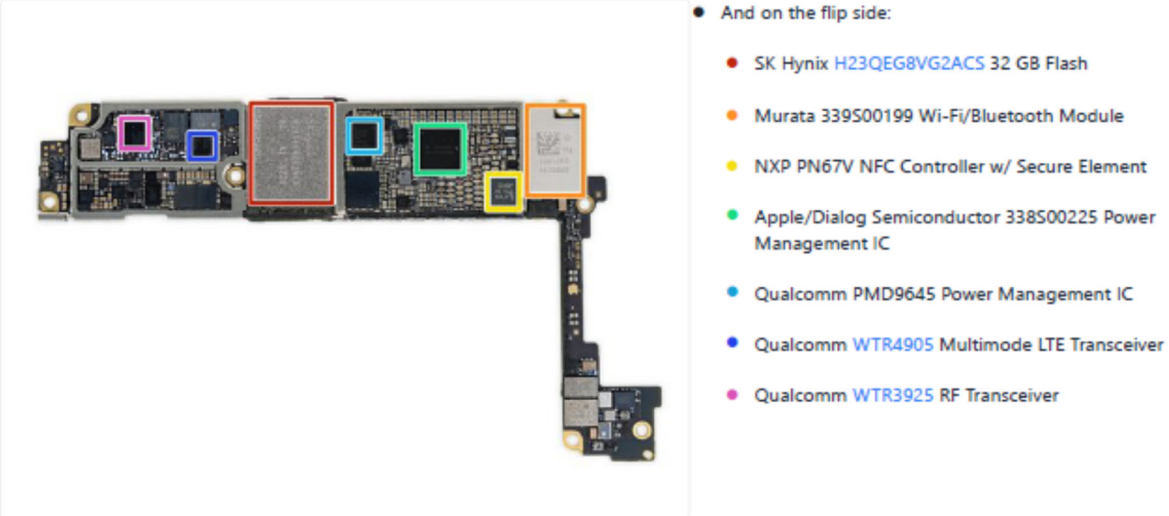
| | | | |
|---|---|---|---|
| | |  3:11 1 2 ABC 3 DEF 4 GHI 5 JKL 6 MNO 7 PQRS 8 TUV 9 WXYZ * 0 + #  3:11 citi PREMIER •••• 4222 Hold Near Reader Starbucks Card BALANCE $0.00 | |

| | | |
|---|---|---|
| | |  <br>  <br>When an RFID reader signal is detected by the mobile communications device, the user must first address how to respond to that signal telephony controls, and vice versa.<br><br>To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (*e.g.,* emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (*e.g.,* mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions). |

| | | |
|---|---|---|
| 1[b] | receiving, by the mobile communications device, from an RFID reader external to the mobile device, an instruction to transmit first RFID transponder data in a format compatible with said RFID reader; | The Accused Products receive, by the mobile communications device, from an RFID reader external to the mobile device, an instruction to transmit first RFID transponder data in a format compatible with said RFID reader.<br><br>The Accused RFID/NFC features (e.g., Apple Pay) conform to the EMV Contactless standard, which incorporates the ISO/IEC 14443 standard for proximity cards.<br><br>**What does EMV mean for Apple Pay?**<br><br>Apple Pay conforms to the latest EMV standards for tokenizing transactions, which leads to a more secure payment experience. With the EMV shift, merchants should update their terminals to support the latest software, which should also include NFC (near field communication), so you can accept Apple Pay and other contactless transactions. Learn what to do before you update your terminals.<br><br>(VAR0000001-02).<br><br>The Accused Products implementing Apple Pay act as a proximity card (PICC) as defined by the ISO/IEC 14443 standard. The Accused Products use signals and commands according to ISO/IEC 1443 and/or ISO/IEC 7816-4.[4] In accordance with ISO/IEC 14443, the Accused Products receive an RFID probing signal (*e.g.*, Request (REQA) and Wake Up (WUPA) commands) from an RFID reader external to the mobile communication device (*e.g.*, a coupling device/RFID reader/contactless point of sale terminal). The Accused Products transmit RFID transponder data in a format compatible with said RFID reader (*e.g.*, Answer to Request or ATQA) in response to receipt of the RFID probing signal.<br><br>**3.5**<br>**PICC**<br>*contactless integrated circuit card* (3.3) or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device<br><br>Note 1 to entry: Commonly called a proximity card. |

[4] https://developer.apple.com/documentation/corenfc/cardsession/

| | | |
|---|---|---|
| | | (VAR0000054-71).<br><br>**5.2.1 Polling**<br><br>In order to detect PICCs which are in the operating field, the PCD shall send repeated request commands. The PCD shall send REQA (or WUPA) and REQB (or WUPB) in any sequence using an equal or configurable duty cycle when polling Type A and Type B. In addition, the PCD may send other commands as described in Annex C.<br><br>**6.4.1 REQA and WUPA commands**<br><br>The REQA and WUPA commands are sent by the PCD to probe the field for PICCs of Type A. They are transmitted within a short frame. See Figure 7 to check in which cases PICCs actually have to answer to these respective commands.<br><br>Particularly, the WUPA command is sent by the PCD to put PICCs which have entered HALT state back into READY* state. They shall then participate in further anticollision and selection procedures.<br><br>(VAR0000126-189).<br><br>**6.3.2 IDLE state**<br><br>**Description:**<br><br>In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands.<br><br>**State exit conditions and transitions:**<br><br>The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA.<br><br>(VAR0000126-189). |
| 1[c] | switching a transceiver of the mobile communications device from a first state to a second state upon reception of said instruction, the | The Accused Products switch a transceiver of the mobile communications from a first state to a second state upon reception of said instruction, the transceiver configured to output voice call signals in the first state and to output RFID transponder signals in the second state.<br>For example, the iPhone 7 has internal circuitry and components, including: NXP 67V04 NFC Controller, Qualcomm WTR4905 Multimode LTE Transceiver, Qualcomm WTR3925 RF |

| | | |
|---|---|---|
| | transceiver configured to output voice call signals in the first state and to output RFID transponder signals in the second state; and | Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module (collectively, "transceiver"), that is configured to output voice call signals in the first state (*e.g.*, via LTE, CDMA, UMTS, GSM and/or audio calling services that use a Wi-Fi connection), and to output RFID transponder signals (*e.g.*, via RFID/NFC) in the second state.<br><br>  <br><br><br>(VAR0000504-518). |

| | | |
|---|---|---|
| | | **Cellular and Wireless**<br>■ **Model A1660**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>TD-SCDMA 1900 (F), 2000 (A)<br>CDMA EV-DO Rev. A (800, 1900, 2100 MHz)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **Model A1778**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **All models**<br>802.11ac Wi-Fi with MIMO<br>Bluetooth 4.2 wireless technology<br>NFC with reader mode<br>Express Cards<br><br>(VAR0000849-855).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Column D of Appendix D (collectively, "transceiver"), that is configured to output voice call signals in the first state (*e.g.*, via LTE, CDMA, UMTS, GSM, 5G and/or audio calling services that use a Wi-Fi connection), and to output RFID transponder signals (*e.g.*, via RFID/NFC) in the |

| | | |
|---|---|---|
| | | second state. The "transceiver" for each Accused Product specified in Column D of Appendix D is incorporated here by reference. (Appendix D; VAR0000639-1074).<br><br>• For example, as specified in Column D of Appendix D, the iPhone 6 has internal circuitry and components including: Qualcomm WTR1625L RF Transceiver, NXP 65V10 NFC module, and Murata 339S0228 Wi-Fi Module (collectively, "transceiver") that is configured to output voice call signals in the first state (*e.g.*, via LTE, CDMA, UMTS, GSM and/or audio calling services that use a Wi-Fi connection), and to output RFID transponder signals (*e.g.*, via RFID/NFC) in the second state.<br><br>To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (*e.g.,* emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (*e.g.,* mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions). |
| 1[d] | outputting the first data by the transceiver in the second state, the transceiver outputting the first data as an RFID transponder signal in the format compatible with said RFID reader.% | The Accused Products output the first data by the transceiver in the second state, the transceiver outputting the first data as an RFID transponder signal in the format compatible with said RFID reader.<br><br>The Accused RFID/NFC Features (e.g., Apple Pay) conforms to the EMV Contactless standard, which incorporates the ISO/IEC 14443 standard for proximity cards. |

## What does EMV mean for Apple Pay?

Apple Pay conforms to the latest EMV standards for tokenizing transactions, which leads to a more secure payment experience. With the EMV shift, merchants should update their terminals to support the latest software, which should also include NFC (near field communication), so you can accept Apple Pay and other contactless transactions. Learn what to do before you update your terminals.

(VAR0000001-02).

The Accused Products implementing Apple Pay act as a proximity card (PICC) as defined by the ISO/IEC 14443 standard. The Accused Products use signals and commands according to ISO/IEC 1443 and/or ISO/IEC 7816-4.[5] In accordance with ISO/IEC 14443, the Accused Products receive an RFID probing signal (*e.g.*, Request (REQA) and Wake Up (WUPA) commands) from an RFID reader external to the mobile communication device (*e.g.*, a coupling device/RFID reader/contactless point of sale terminal). The Accused Products transmit RFID transponder data in a format compatible with said RFID reader (*e.g.*, Answer to Request or ATQA) in response to receipt of the RFID probing signal.

**3.5**
**PICC**
*contactless integrated circuit card* (3.3) or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device

Note 1 to entry: Commonly called a proximity card.

(VAR0000054-71)

[5] https://developer.apple.com/documentation/corenfc/cardsession/

| | | |
|---|---|---|
| | | **5.2.1 Polling**<br><br>In order to detect PICCs which are in the operating field, the PCD shall send repeated request commands. The PCD shall send REQA (or WUPA) and REQB (or WUPB) in any sequence using an equal or configurable duty cycle when polling Type A and Type B. In addition, the PCD may send other commands as described in Annex C.<br><br>**6.4.1 REQA and WUPA commands**<br><br>The REQA and WUPA commands are sent by the PCD to probe the field for PICCs of Type A. They are transmitted within a short frame. See Figure 7 to check in which cases PICCs actually have to answer to these respective commands.<br><br>Particularly, the WUPA command is sent by the PCD to put PICCs which have entered HALT state back into READY* state. They shall then participate in further anticollision and selection procedures.<br><br>(VAR0000126-189).<br><br>**6.3.2 IDLE state**<br><br>**Description:**<br><br>In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands.<br><br>**State exit conditions and transitions:**<br><br>The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA.<br><br>(VAR0000126-189).<br><br>The Accused Products output the first data, including e.g., data from applets within the Secure Element. |

## Secure Element

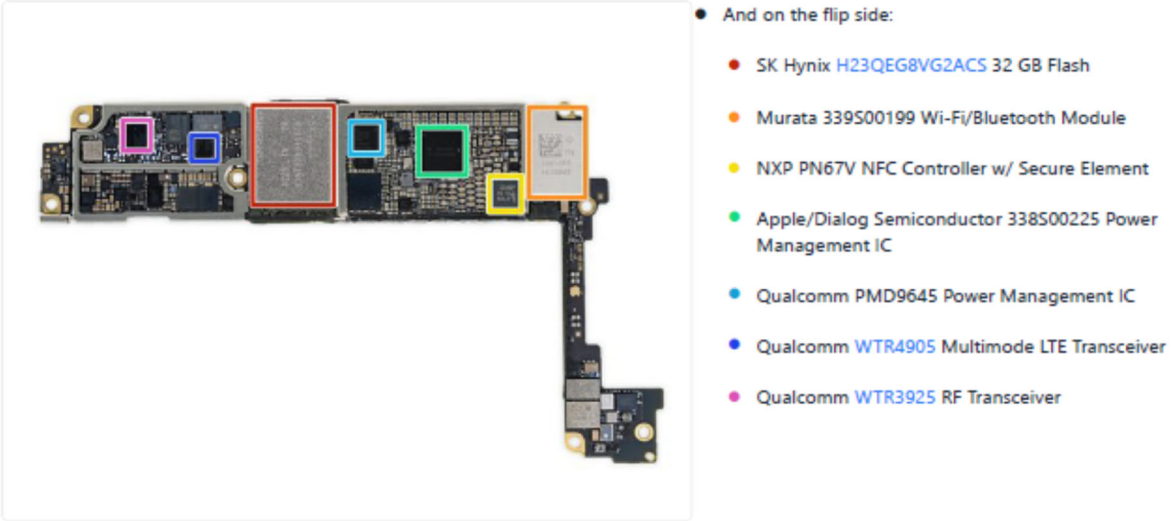
The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus.

## NFC controller

As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.

After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.

(VAR0001075 at 1209).

| | | |
|---|---|---|
| 2 | The method of claim 1, wherein said transceiver comprises a first signal processing unit configured to process voice call signals and a second signal processing unit configured to process RFID signals, said switching comprising coupling the second signal processing unit to a transmission path of the transceiver. | The Accused Products perform the method of claim 1, wherein said transceiver comprises a first signal processing unit configured to process voice call signals and a second signal processing unit configured to process RFID signals, said switching comprising coupling the second signal processing unit to a transmission path of the transceiver.<br><br>For example, the iPhone 7 has internal circuitry and components, including: NXP 67V04 NFC Controller, Qualcomm WTR4905 Multimode LTE Transceiver, Qualcomm WTR3925 RF Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module (collectively, "transceiver"), wherein said transceiver comprises a first signal processing unit (*e.g.*, Qualcomm WTR4905 Multimode LTE Transceiver, Qualcomm WTR3925 RF Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module) configured to process voice call signals (*e.g.*, via LTE, CDMA, UMTS, GSM and/or audio calling services that use a Wi-Fi connection) and a second signal processing unit (*e.g.*, NXP 67V04 NFC) configured to process RFID signals (*e.g.*, via RFID/NFC), said switching comprising coupling the second signal processing unit to a transmission path of the transceiver.<br><br>  <br><br><br>(VAR0000504-518). |

| | | |
|---|---|---|
| | | As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Column D of Appendix D (collectively, "transceiver"), wherein said transceiver comprises a first signal processing unit specified in Column E of Appendix D configured to process voice call signals (*e.g.*, via LTE, CDMA, UMTS, GSM, 5G and/or audio calling services that use a Wi-Fi connection) and a second signal processing unit specified in Column F of Appendix D configured to process RFID signals (*e.g.*, via RFID/NFC), said switching comprising coupling the second signal processing unit to a transmission path of the transceiver. The "transceiver" for each Accused Product specified in Column D of Appendix D is incorporated here by reference.<br><br>• For example, as specified in Column D of Appendix D, the iPhone 6 has internal circuitry and components including: Qualcomm WTR1625L RF Transceiver, NXP 65V10 NFC module, and Murata 339S0228 Wi-Fi Module (collectively, "transceiver"), wherein said transceiver comprises a first signal processing unit specified in Column E of Appendix D (*e.g.*, Qualcomm WTR1625L RF Transceiver and Murata 339S0228 Wi-Fi Module) configured to process voice call signals (*e.g.*, via LTE, CDMA, UMTS, GSM and/or audio calling services that use a Wi-Fi connection) and a second signal processing unit specified in Column F of Appendix D (*e.g.*, NXP 65V10 NFC) configured to process RFID signals (*e.g.*, via RFID/NFC), said switching comprising coupling the second signal processing unit to a transmission path of the transceiver.<br><br>To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (*e.g.,* emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (*e.g.,* mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions). |

| | | |
|---|---|---|
| 3 | The method of claim 1, wherein said first RFID transponder data comprises a selected one of a security key and an identifier. | The Accused Products perform the method of claim 1, wherein said first RFID transponder data comprises a selected one of a security key and an identifier. For example, credit cards can be added to Apple Pay, and the Accused Products may then be used to make contactless payments using those credit cards. In addition, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Products may then be used to unlock the hotel room and/or car. (VAR0000003-09; VAR0000020-22; VAR0001075-1293).<br><br>The data includes, e.g., data from applets within the Secure Element.<br><br>**Secure Element**<br>The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.<br><br>(VAR0001075 at 1209). |

| | | |
|---|---|---|
| | | **Privacy and security**<br>Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted.<br><br>(VAR VAR0001075 at 12222). |
| 4 | The method of claim 3, wherein said security key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key. | The Accused Products perform the method of claim 3, wherein said security key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Products may then be used to unlock the hotel room and/or car. (VAR0000003-09).<br><br>The keys include, e.g., keys stored on applets in the Secure Element.<br><br>**Privacy and security**<br>Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted.<br><br>(VAR VAR0001075 at 12222). |

| | | |
|---|---|---|
| 5 | The method of claim 1, wherein said first RFID transponder data comprises an identifier, and said identifier comprises a selected one of a social security number, a driver's license number, an affinity program account number, and a credit card number. | The Accused Products perform the method of claim 5, wherein said first RFID transponder data comprises an identifier, and said identifier comprises a selected one of a social security number, a driver's license number, an affinity program account number, and a credit card number. For example, credit cards can be added to Apple Pay, and the Accused Products may then be used to make contactless payments using those credit cards. (VAR0000020-22; VAR0001075-1293).<br><br>The data includes, e.g., data from applets within the Secure Element.<br><br>**Secure Element**<br>The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.<br><br>(VAR0001075 at 1209). |
| 6 | The method of claim 1, wherein the method further comprises facilitating the | The Accused Products perform the method of claim 1, wherein the method further comprises facilitating the user in selecting the first RFID transponder data from a plurality of RFID transponder data using the mobile communication device. For example, multiple payment cards can be added to |

| | | |
|---|---|---|
| | user in selecting the first RFID transponder data from a plurality of RFID transponder data using the mobile communication device. | Apple Pay, and the Accused Products may then be used to select a card to make a contactless payment. (VAR0000020-22).<br><br>The data includes, e.g., data from applets within the Secure Element.<br><br>**Secure Element**<br>The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.<br><br>(VAR0001075 at 1209). |
| 7 | The method of claim 1, wherein the method further comprises facilitating provision of the first RFID transponder data to the mobile communication device. | The Accused Products perform the method of claim 1, wherein the method further comprises facilitating provision of the first RFID transponder data to the mobile communication device. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless |

| | | |
|---|---|---|
| | | payments with Apple Pay using the Accused Products. (VAR0001075-1293 at 1210-11). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09).<br><br>**Credit, debit, and prepaid cards**<br><br>**Card provisioning security overview**<br><br>When a user adds a credit, debit, or prepaid card (including store cards) to Apple Wallet, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer determines whether to approve adding the card to Apple Wallet. As part of the card provisioning process, Apple Pay uses three server-side calls to send and receive communication with the card issuer or network:<br><br>• Required Fields<br>• Check Card<br>• Link and Provision<br><br>The card issuer or network uses these calls to verify, approve, and add cards to Apple Wallet. These client-server sessions use TLS 1.2 to transfer the data.<br><br>Full card numbers aren't stored on the device or on Apple Pay servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from most credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is never stored on Apple Pay servers or backed up to iCloud, and it is isolated from iOS, iPadOS, and watchOS devices and from Mac computers with Touch ID.<br><br>Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone, or within a card issuer's iPhone app. Adding a card to Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch. |

**Adding credit or debit cards manually**

To add a card manually, the name, card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, Apple Wallet, or the Apple Watch app, users can enter that information either by typing or by using the device's camera. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are then encrypted and sent to the Apple Pay server.

If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network. This includes information about (a) the user's iTunes and App Store account activity (for example, whether the user has a long history of transactions within iTunes), (b) the user's device (for example, the phone number, name, and model of the user's device plus any companion Apple device necessary to set up Apple Pay), and (c) the user's approximate location at the time the user adds their card (if the user has Location Services enabled). Using this information, the card issuer determines whether to approve adding the card to Apple Pay.

As the result of the Link and Provision process, two things occur:

- The device begins to download the Apple Wallet pass file representing the credit or debit card.
- The device begins to bind the card to the Secure Element.

The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card can make payments with Apple Pay.

| | | |
|---|---|---|
| | | The data includes, e.g., data from applets within the Secure Element.<br><br>**Secure Element**<br>The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.<br><br>(VAR0001075 at 1209). |
| 8 | The method of claim 7, wherein said facilitating of the provisioning of the RFID transponder data to the mobile communication device includes facilitating provision of at least a signaling attribute | The Accused Products perform the method of claim 7, wherein said facilitating of the provisioning of the RFID transponder data to the mobile communication device includes facilitating provision of at least a signaling attribute associated with the outputting of the RFID transponder data in the format compatible with said RFID reader. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Devices, and Apple further directs, controls, and specifies the communication and security protocols associated with making |

| | | |
|---|---|---|
| | associated with the outputting of the RFID transponder data in the format compatible with said RFID reader. | contactless payments via Apple Pay. The data includes, e.g., data from applets within the Secure Element.(VAR0001075-1293 at 1208-209). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09).<br><br>**NFC controller**<br>The NFC controller handles Near Field Communication protocols and routes communication between the Application Processor and the Secure Element, and between the Secure Element and the point-of-sale terminal.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server. |

| | | |
|---|---|---|
| 9[a] | The method of claim 1, wherein the method further comprises: | The Accused Products perform the method of claim 1, wherein the method further comprises the steps below. |
| 9[b] | monitoring for proximal presence of the RFID reader by the mobile communication device; and | The Accused Products monitor for proximal presence of the RFID reader by the mobile communication device.<br><br>The Accused RFID/NFC features conform to the EMV Contactless standard, which incorporates the ISO/IEC 14443 standard for proximity cards.<br><br>**What does EMV mean for Apple Pay?**<br><br>Apple Pay conforms to the latest EMV standards for tokenizing transactions, which leads to a more secure payment experience. With the EMV shift, merchants should update their terminals to support the latest software, which should also include NFC (near field communication), so you can accept Apple Pay and other contactless transactions. Learn what to do before you update your terminals.<br><br>(VAR0000001-02).<br><br>The Accused Products act as a proximity card (PICC) as defined by the ISO/IEC 14443 standard. The Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.[6] In accordance with ISO/IEC 14443, the Accused Products monitor for the proximal presence of an external l RFID reader (*e.g.*, a coupling device) by listening for commands and recognizing Request (REQA) and Wake Up (WUPA) commands from the RFID reader.<br><br>**3.5**<br>**PICC**<br>*contactless integrated circuit card* (3.3) or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device<br><br>Note 1 to entry: Commonly called a proximity card. |

[6] https://developer.apple.com/documentation/corenfc/cardsession/

| | | |
|---|---|---|
| | | (VAR0000054-71). |
| 9[c] | on detection of the RFID reader by the mobile communication device, outputting by the transceiver second RFID transponder data as a second radio frequency signal, the outputting emulating output of the second RFID transponder data by an RFID transponder of a passive type. | On detection of the RFID reader by the mobile communication device, the Accused Products output by the transceiver second RFID transponder data as a second radio frequency signal, the outputting emulating output of the second RFID transponder data by an RFID transponder of a passive type.<br><br>For example, the Accused Products, acting in accordance with the format employed by the RFID reader (*e.g.*, ISO/IEC 14443) and on detection of the RFID reader (*e.g.*, IDLE state exit), output RFID transponder data (*e.g.*, Answer to Request or ATQA), the outputting emulating output of the RFID transponder data by an RFID transponder of a passive type.<br><br>**6.3.2 IDLE state**<br><br>**Description:**<br><br>In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands.<br><br>**State exit conditions and transitions:**<br><br>The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA.<br><br>(VAR0000126-189).<br><br>The data includes, e.g., data from applets within the Secure Element. |

| | | |
|---|---|---|
| | | **Secure Element**<br>The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.<br><br>(VAR0001075 at 1209). |
| 10 | The method of claim 9, wherein said monitoring comprises sensing for a probing radio frequency signal of the RFID reader by the mobile communication device. | The Accused Products perform the method of claim 9, wherein said monitoring comprises sensing for a probing radio frequency signal of the RFID reader by the mobile communication device.<br><br>For example, the Accused Products, in accordance with ISO/IEC 14443, listen for and recognize Request (REQA) and Wake Up (WUPA) commands from the RFID reader.<br><br>**3.5**<br>**PICC**<br>*contactless integrated circuit card* (3.3) or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device<br><br>Note 1 to entry: Commonly called a proximity card. |

| | | |
|---|---|---|
| | | (VAR0000054-71).<br><br>**6.3.2 IDLE state**<br><br>**Description:**<br><br>In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands.<br><br>**State exit conditions and transitions:**<br><br>The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA.<br><br>(VAR0000126-189). |
| 11 | The method of claim 9, wherein said first RFID transponder data and second RFID transponder data are the same data. | The Accused Products perform the method of claim 9, wherein said first RFID transponder data and second RFID transponder data are the same data.<br><br>For example, the Accused Products, acting in accordance with the format employed by the RFID reader (*e.g.*, ISO/IEC 14443) and on detection of the RFID reader (*e.g.*, IDLE state exit), output RFID transponder data (*e.g.*, Answer to Request or ATQA), the outputting emulating output of the RFID transponder data by an RFID transponder of a passive type.<br><br>**6.3.2 IDLE state**<br><br>**Description:**<br><br>In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands.<br><br>**State exit conditions and transitions:**<br><br>The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA.<br><br>(VAR0000126-189). |

| | | |
|---|---|---|
| | | The data includes, e.g., data from applets within the Secure Element.<br><br>**Secure Element**<br>The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.<br><br>(VAR0001075 at 1209). |
| 12 | The method of claim 1, wherein the mobile communication device is a selected one of a wireless mobile phone and a personal digital assistant equipped with communication capability. | The Accused Products perform the method of claim 1, wherein the mobile communication device is a selected one of a wireless mobile phone and a personal digital assistant equipped with communication capability. For example the Accused Products are wireless mobile phones and/or personal digital assistants equipped with communication capability. For example the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (*e.g.*, via LTE, CDMA, UMTS, and/or GSM), and/o audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling). |

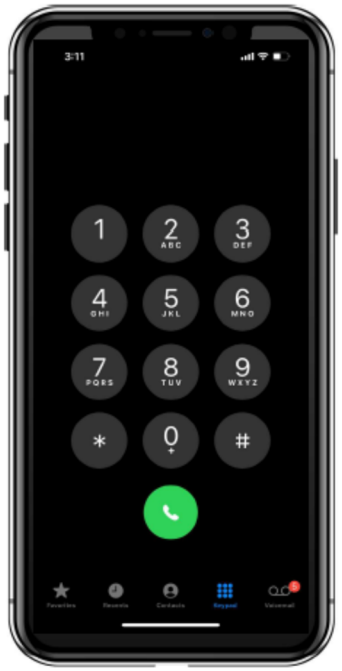
| | | |
|---|---|---|
| | | **Audio Calling**[5]<br>■ FaceTime audio<br>■ Voice over LTE (VoLTE)[6]<br>■ Wi-Fi calling[6]<br><br>**Cellular and Wireless**<br>■ **Model A1660**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>TD-SCDMA 1900 (F), 2000 (A)<br>CDMA EV-DO Rev. A (800, 1900, 2100 MHz)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **Model A1778**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30) |

30

| | | |
|---|---|---|
| | | TD-LTE (Bands 38, 39, 40, 41)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>▪ **All models**<br>802.11ac Wi-Fi with MIMO<br>Bluetooth 4.2 wireless technology<br>NFC with reader mode<br>Express Cards<br>(VAR0000849-855).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (*e.g.*, Via LTE via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling). (VAR0000639-1074). |
| 13[a] | A method for providing a radio frequency identifier (RFID), from a switchable mobile communications device capable of RFID communication and voice call communication, the method comprising: | To the extent that the claim's preamble is determined to be a limitation or otherwise limiting, the Accused Products perform a method for providing RFID from a switchable mobile communications device capable of RFID communication and voice call communication, comprising the steps in the subsequent limitations.<br><br>For example, as reflected in Apple's product literature, the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (*e.g.*, via LTE, CDMA, UMTS, and/or GSM), and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling), as well as RFID communication (*e.g.*, via RFID/NFC, including via Apple Pay, which uses NFC technology between the device and the payment terminal). |

| | | |
|---|---|---|
| | | **Audio Calling**[5]<br>■ FaceTime audio<br>■ Voice over LTE (VoLTE)[6]<br>■ Wi-Fi calling[6]<br><br>**Cellular and Wireless**<br>■ **Model A1660**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>TD-SCDMA 1900 (F), 2000 (A)<br>CDMA EV-DO Rev. A (800, 1900, 2100 MHz)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **Model A1778**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **All models**<br>802.11ac Wi-Fi with MIMO<br>Bluetooth 4.2 wireless technology<br>NFC with reader mode<br>Express Cards<br>(VAR0000849-855). |

| | | |
|---|---|---|
| | | As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (*e.g.*, via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling), as well as RFID communication (*e.g.*, via RFID/NFC, including via Apple Pay, which uses NFC technology between the device and the payment terminal). (VAR0000639-1074).<br><br>**When you use Apple Pay in stores**<br><br>When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that's designed to work only across short distances. If your iPhone is on and detects an NFC field, it will present you with your default card. To send your payment information, you must authenticate using Face ID, Touch ID, or your passcode (except when you use Express Mode with a payment or transit card). With Face ID or with Apple Watch, you must double-click the side button when the device is unlocked to activate your default card for payment.<br><br>(VAR0000010-14).<br><br>NFC is a subset within the family of RFID technology. (VAR0000026-42) ("RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology."); (VAR0000043-53) ("Hierarchically, NFC is a subset of RFID.")).<br><br>For example, the iPhone as a whole is capable of entering two different modes, including a telephony mode and an RFID/NFC mode. A user can affirmatively launch the telephony and/or RFID/NFC modes, and/or the iPhone enters the telephony and/or RFID/NFC mode when its received the relevant signal (e.g., an incoming call or detecting an RFID reader), as shown below. |

| | | | |
|---|---|---|---|
| | |   | |

| | | |
|---|---|---|
| | |   <br><br>When an RFID reader signal is detected by the mobile communications device, the user must first address how to respond to that signal telephony controls, and vice versa.<br><br>To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (*e.g.,* emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (*e.g.,* mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions). |

| | | |
|---|---|---|
| 13[b] | monitoring for proximal presence of a proximal RFID reader external to said mobile communication device by said mobile communication device | The Accused Products monitor for the proximal presence of a proximal RFID reader (*e.g.*, a contactless point-of-sale terminal/reader) external to said mobile communication device.<br><br>The Accused RFID/NFC features conform to the EMV Contactless standard, which incorporates the ISO/IEC 14443 standard for proximity cards.<br><br>**What does EMV mean for Apple Pay?**<br><br>Apple Pay conforms to the latest EMV standards for tokenizing transactions, which leads to a more secure payment experience. With the EMV shift, merchants should update their terminals to support the latest software, which should also include NFC (near field communication), so you can accept Apple Pay and other contactless transactions. Learn what to do before you update your terminals.<br><br>(VAR0000001-02).<br><br>The Accused Products act as a proximity card (PICC) as defined by the ISO/IEC 14443 standard. The Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.[7] In accordance with ISO/IEC 14443, the Accused Products monitor for the proximal presence of a proximal, external RFID reader (*e.g.*, a coupling device) by listening for commands and recognizing Request (REQA) and Wake Up (WUPA) commands from the RFID reader.<br><br>**3.5**<br>**PICC**<br>*contactless integrated circuit card* (3.3) or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device<br><br>Note 1 to entry: Commonly called a proximity card.<br><br>(VAR0000054-71). |

[7] https://developer.apple.com/documentation/corenfc/cardsession/

| | | |
|---|---|---|
| | | **6.3.2 IDLE state**<br><br>**Description:**<br><br>In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands.<br><br>**State exit conditions and transitions:**<br><br>The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA.<br><br>(VAR0000126-189). |

## How to pay using Apple Pay in stores and other places

With your iPhone or Apple Watch, you can use Apple Pay in stores, restaurants, gas stations, taxis, or wherever else you see one of these symbols[1].

### Pay with your iPhone

1. To use your default card:
   - If your iPhone has Face ID, double-click the side button. If prompted, authenticate with Face ID or enter your passcode to open Apple Wallet.
   - If your iPhone has Touch ID, double-click the Home button.
2. To use a different card, tap your default card to see your other cards. Tap a new card and authenticate.
3. Hold the top of your iPhone near the contactless reader until Done and a checkmark appear on the display.

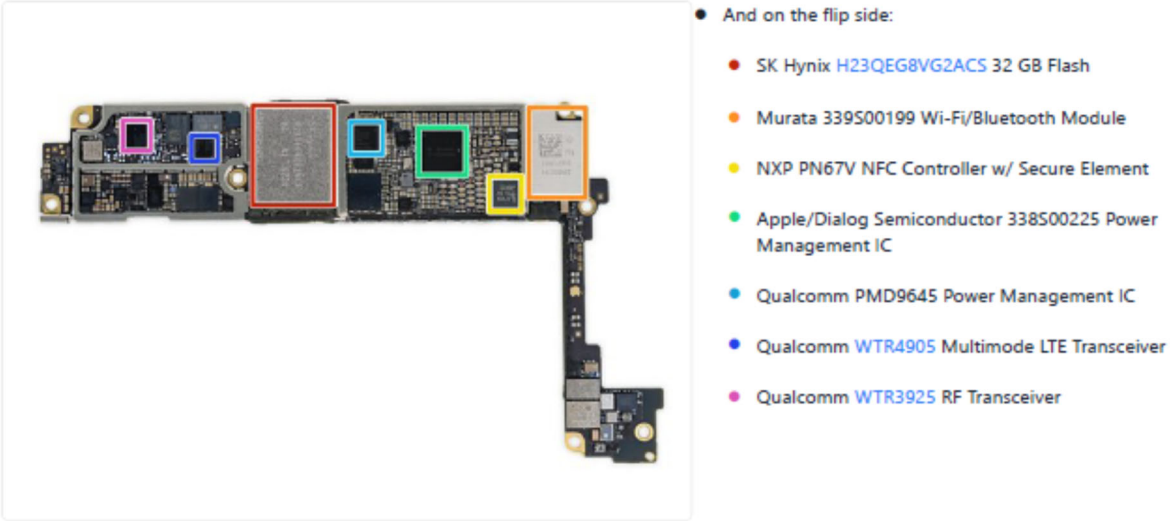



### Pay with your Apple Watch

1. Double-click the side button.
2. Your default card opens automatically. Scroll down to choose another card.
3. Hold the display of your Apple Watch near the contactless reader until you feel a gentle tap and hear a beep.

Want to see your recent purchases? Learn how to check your Apple Pay transaction history.

(VAR0000020-22).

| | | |
|---|---|---|
| 13[c] | the mobile device having a transceiver configured, to output, in a first state, RFID transponder data in a format compatible with said RFID reader upon the mobile communications device determining proximal presence of one or more RFID readers, the transceiver being also configured to output, in a second state, a voice call signal for transmission at least in part over a wireless network; and | The Accused Products' transceiver is configured to output, in a first state, RFID transponder data in a format compatible with said RFID reader upon the mobile communications device determining proximal presence of one or more RFID readers, the Accused Products' transceiver being also configured to output, in a second state, a voice call signal for transmission at least in part over a wireless network.<br><br>For example, the iPhone 7 has internal circuitry and components, including an NXP 67V04 NFC Controller, Qualcomm WTR4905 Multimode LTE Transceiver, Qualcomm WTR3925 RF Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module (collectively, "transceiver"), that outputs, in a first state, RFID transponder data in a format compatible with said RFID reader (*e.g.*, a contactless point-of-sale terminal) upon the mobile communications device determining proximal presence of one or more RFID readers, and in a second state, outputs a voice call signal for transmission at least in part over a wireless network (*e.g.*, via LTE, CDMA, UMTS, GSM, Wi-Fi).<br><br>  <br><br><br>(VAR0000504-518). |

| | | |
|---|---|---|
| | | **Cellular and Wireless**<br>■ **Model A1660**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>TD-SCDMA 1900 (F), 2000 (A)<br>CDMA EV-DO Rev. A (800, 1900, 2100 MHz)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **Model A1778**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **All models**<br>802.11ac Wi-Fi with MIMO<br>Bluetooth 4.2 wireless technology<br>NFC with reader mode<br>Express Cards<br><br>(VAR0000849-855). |

40

| | | |
|---|---|---|
| | | As further examples, Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Column D of Appendix D (collectively, "transceiver"), that outputs, in a first state, RFID transponder data in a format compatible with said RFID reader (*e.g.*, a contactless point-of-sale terminal) upon the mobile communications device determining proximal presence of one or more RFID readers, and in a second state, outputs a voice call signal for transmission at least in part over a wireless network (*e.g.*, via LTE, CDMA, UMTS, GSM, 5G and/or Wi-Fi). The "transceiver" for each Accused Product specified in Column D of Appendix D is incorporated here by reference. (VAR0001075-1293; VAR0000639-1074).<br><br>• For example, as specified in Column D of Appendix D, the iPhone 6 has internal circuitry including: Qualcomm WTR1625L RF Transceiver, NXP 65V10 NFC module, and Murata 339S0228 Wi-Fi Module (collectively, "transceiver"), that outputs, in a first state, RFID transponder data in a format compatible with said RFID reader (*e.g.*, a contactless point-of-sale terminal) upon the mobile communications device determining proximal presence of one or more RFID readers, and in a second state, outputs a voice call signal for transmission at least in part over a wireless network (*e.g.*, via LTE, CDMA, UMTS, GSM, and/or Wi-Fi).<br><br>To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder data through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (*e.g.,* emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (*e.g.,* mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions). |
| 13[d] | on detection of the RFID reader, outputting, by the transceiver, the RFID transponder data as a radio frequency signal, said data | On detection of the RFID reader, the Accused Products output, by the transceiver, the RFID transponder data as a radio frequency signal, said data being output in said format employed by the RFID reader. |

| | | |
|---|---|---|
| | being output in said format employed by the RFID reader. | For example, the Accused Products, acting in accordance with the format employed by the RFID reader (*e.g.*, ISO/IEC 14443) and on detection of the RFID reader (*e.g.*, IDLE state exit), transmit RFID transponder data (*e.g.*, Answer to Request or ATQA) as a radio frequency signal (*e.g.*, 13.56 MHz frequency).<br><br>**6.3.2 IDLE state**<br><br>**Description:**<br><br>In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands.<br><br>**State exit conditions and transitions:**<br><br>The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA.<br><br>(VAR0000126-189).<br><br>**6.2 Frequency**<br><br>The frequency, $f_c$, of the RF operating field shall be 13,56 MHz ± 7 kHz.<br><br>(VAR0000072-125). |

| | | |
|---|---|---|
| | | The data includes, e.g., data from applets within the Secure Element.<br><br>**Secure Element**<br>The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.<br><br>(VAR0001075 at 1209). |
| 14 | The method of claim 13, wherein the monitoring comprises sensing for one or more probing radio frequency signals of the one or more RFID readers by the mobile communications device. | The Accused Products perform the method of claim 13 wherein the monitoring comprises sensing for one or more probing radio frequency signals of the one or more RFID readers by the mobile communications device. For example, the Accused Products, in accordance with ISO/IEC 14443, listen for and recognize Request (REQA) and Wake Up (WUPA) commands from the RFID reader. |

| | | |
|---|---|---|
| | | **3.5**<br>**PICC**<br>*contactless integrated circuit card* (3.3) or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device<br><br>Note 1 to entry: Commonly called a proximity card.<br><br>(VAR0000054-71).<br><br>**6.3.2 IDLE state**<br><br>**Description:**<br><br>In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands.<br><br>**State exit conditions and transitions:**<br><br>The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA.<br><br>(VAR0000126-189). |
| 15 | The method of claim 13, wherein said data comprises a security key. | The Accused Products perform the method of claim 13 wherein said data comprises a security key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Product may then be used to unlock the hotel room and/or car. (VAR0000003-09). |

| | | |
|---|---|---|
| | | The keys include, e.g., keys stored on applets in the Secure Element.<br><br>**Privacy and security**<br>Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted.<br><br>(VAR VAR0001075 at 12222). |
| 16 | The method of claim 15, wherein said security key comprises a door key. | The Accused Products perform the method of claim 15 wherein said data comprises a security key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Product may then be used to unlock the hotel room and/or car.<br><br>(VAR0000003-09). |
| 17 | The method of claim 16, wherein said door key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key. | The Accused Products perform the method of claim 16, wherein said door key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key.<br><br>For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Product may then be used to unlock the hotel room and/or car.<br><br>(VAR0000003-09). |
| 18 | The method of claim 13, wherein the method further comprises facilitating provision of the RFID transponder data to the | The Accused Products perform the method of claim 13, wherein the method further comprises facilitating provision of the RFID transponder data to the mobile communication device. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments |

| | | |
|---|---|---|
| | mobile communication device. | with Apple Pay using the Accused Products. (VAR0001075-1293 at 1210-211). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09). |

46

## Credit, debit, and prepaid cards

### Card provisioning security overview

When a user adds a credit, debit, or prepaid card (including store cards) to Apple Wallet, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer determines whether to approve adding the card to Apple Wallet. As part of the card provisioning process, Apple Pay uses three server-side calls to send and receive communication with the card issuer or network:

- Required Fields
- Check Card
- Link and Provision

The card issuer or network uses these calls to verify, approve, and add cards to Apple Wallet. These client-server sessions use TLS 1.2 to transfer the data.

Full card numbers aren't stored on the device or on Apple Pay servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from most credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is never stored on Apple Pay servers or backed up to iCloud, and it is isolated from iOS, iPadOS, and watchOS devices and from Mac computers with Touch ID.

Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone, or within a card issuer's iPhone app. Adding a card to Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

**Adding credit or debit cards manually**

To add a card manually, the name, card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, Apple Wallet, or the Apple Watch app, users can enter that information either by typing or by using the device's camera. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are then encrypted and sent to the Apple Pay server.

If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network. This includes information about (a) the user's iTunes and App Store account activity (for example, whether the user has a long history of transactions within iTunes), (b) the user's device (for example, the phone number, name, and model of the user's device plus any companion Apple device necessary to set up Apple Pay), and (c) the user's approximate location at the time the user adds their card (if the user has Location Services enabled). Using this information, the card issuer determines whether to approve adding the card to Apple Pay.

As the result of the Link and Provision process, two things occur:

- The device begins to download the Apple Wallet pass file representing the credit or debit card.
- The device begins to bind the card to the Secure Element.

The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card can make payments with Apple Pay.

| | | |
|---|---|---|
| | | The data includes, e.g., data from applets within the Secure Element.<br><br>**Secure Element**<br>The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.<br><br>(VAR0001075 at 1209). |
| 19 | The method of claim 18, wherein said facilitating of the provisioning of the RFID transponder data to the mobile communication device includes facilitating provision of at least a signaling attribute associated with the outputting of the RFID | The Accused Products perform the method of claim 18, wherein said facilitating of the provisioning of the RFID transponder data to the mobile communication device includes facilitating provision of at least a signaling attribute associated with the outputting of the RFID transponder data in the format employed by the RFID reader. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Devices, and Apple further directs, controls, and specifies the communication and security protocols associated with making contactless |

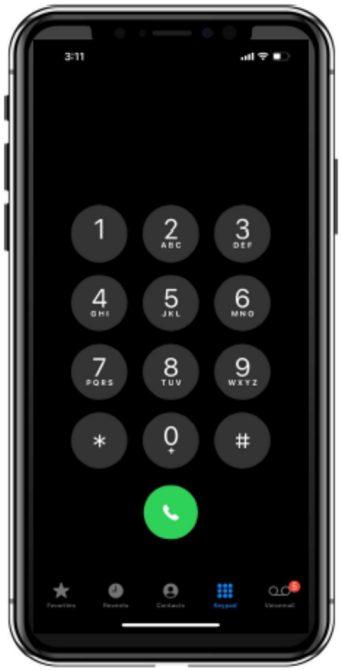
| | | |
|---|---|---|
| | transponder data in the format employed by the RFID reader. | payments via Apple Pay. (VAR0001075-1293 at 1208-09). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09).<br><br>**NFC controller**<br>The NFC controller handles Near Field Communication protocols and routes communication between the Application Processor and the Secure Element, and between the Secure Element and the point-of-sale terminal.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server. |
| 20 | The method of claim 13, wherein the mobile communication device is a selected of a wireless mobile phone and a personal digital assistant | The Accused Products perform the method of claim 13, wherein the mobile communication device is a selected of a wireless mobile phone and a personal digital assistant equipped with communication capability. For example the Accused Products are wireless mobile phones and/or personal digital assistants equipped with communication capability. |

| | | |
|---|---|---|
| | equipped with communication capability. | For example the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (*e.g.*, via LTE, CDMA, UMTS, and/or GSM), and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling).<br><br>**Audio Calling**[5]<br>▪ FaceTime audio<br>▪ Voice over LTE (VoLTE)[6]<br>▪ Wi-Fi calling[6]<br><br>**Cellular and Wireless**<br>▪ **Model A1660**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>TD-SCDMA 1900 (F), 2000 (A)<br>CDMA EV-DO Rev. A (800, 1900, 2100 MHz)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>▪ **Model A1778**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>▪ **All models**<br>802.11ac Wi-Fi with MIMO<br>Bluetooth 4.2 wireless technology<br>NFC with reader mode<br>Express Cards |

| | | |
|---|---|---|
| | | (VAR0000849-855).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (*e.g.*, Via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling). (VAR0000639-1074). |
| 21[a] | A switchable mobile communication device capable of RFID communication and voice call communication, the mobile communication device comprising: | To the extent that the claim's preamble is determined to be a limitation or otherwise limiting, the Accused Products are switchable mobile communication device[s] capable of RFID communication and voice call communication.<br><br>For example, as reflected in Apple's product literature, the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (*e.g.*, via LTE, CDMA, UMTS, and/or GSM), and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling), as well as RFID communication (*e.g.*, via RFID/NFC, including via Apple Pay, which uses NFC technology between the device and the payment terminal).<br><br>**Audio Calling**[5]<br>▪ FaceTime audio<br>▪ Voice over LTE (VoLTE)[6]<br>▪ Wi-Fi calling[6] |

| | | |
|---|---|---|
| | | **Cellular and Wireless**<br>■ **Model A1660**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>TD-SCDMA 1900 (F), 2000 (A)<br>CDMA EV-DO Rev. A (800, 1900, 2100 MHz)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **Model A1778**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **All models**<br>802.11ac Wi-Fi with MIMO<br>Bluetooth 4.2 wireless technology<br>NFC with reader mode<br>Express Cards<br>(VAR0000849-855).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (*e.g.*, via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling), as well as RFID communication (*e.g.*, via RFID/NFC, including via Apple Pay, which uses NFC technology between the device and the payment terminal). (VAR0000639-1074). |

| | | |
|---|---|---|
| | | **When you use Apple Pay in stores**<br><br>When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that's designed to work only across short distances. If your iPhone is on and detects an NFC field, it will present you with your default card. To send your payment information, you must authenticate using Face ID, Touch ID, or your passcode (except when you use Express Mode with a payment or transit card). With Face ID or with Apple Watch, you must double-click the side button when the device is unlocked to activate your default card for payment.<br><br>(VAR0000010-14).<br><br>NFC is a subset within the family of RFID technology. (VAR0000026-42) ("RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology."); (VAR0000043-53) ("Hierarchically, NFC is a subset of RFID.")).<br><br>For example, the iPhone as a whole is capable of entering two different modes, including a telephony mode and an RFID/NFC mode. A user can affirmatively launch the telephony and/or RFID/NFC modes, and/or the iPhone enters the telephony and/or RFID/NFC mode when its received the relevant signal (e.g., an incoming call or detecting an RFID reader), as shown below. |

| | | | |
|---|---|---|---|
| | |   | |

| | | |
|---|---|---|
| | |   <br><br>When an RFID reader signal is detected by the mobile communications device, the user must first address how to respond to that signal telephony controls, and vice versa.<br><br>To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (*e.g.,* emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (*e.g.,* mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions). |

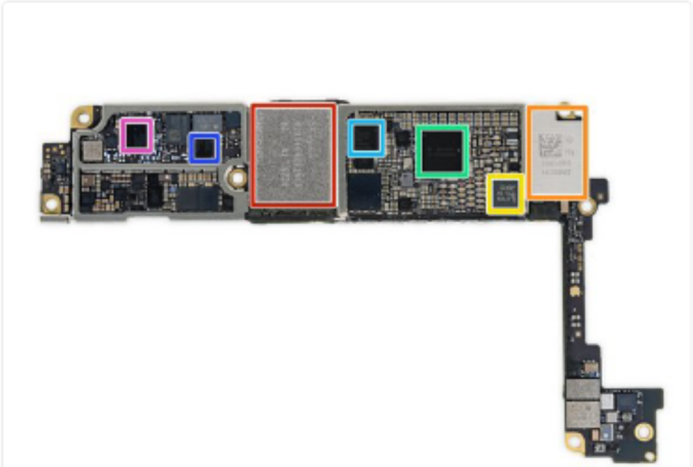
| | | |
|---|---|---|
| 21[b] | a transmitter configured to transmit a radio frequency signal, the transmitter comprising a first signal processing section and a second signal processing section, the first signal processing section configured to output voice call signals in a first radio frequency range and the second signal processing section configured to output RFID transponder signals in a second radio frequency range; | The Accused Products have a transmitter configured to transmit a radio frequency signal, the transmitter comprising a first signal processing section and a second signal processing section, the first signal processing section configured to output voice call signals in a first radio frequency range and the second signal processing section configured to output RFID transponder signals in a second radio frequency range.<br><br>For example, the iPhone 7 has internal circuitry and components, including an NXP 67V04 NFC Controller, Qualcomm WTR4905 Multimode LTE Transceiver, Qualcomm WTR3925 RF Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module (collectively, "transmitter"), comprising a first signal processing section specified in Column E of Appendix D (*e.g.*, Qualcomm WTR4905 Multimode LTE Transceiver, Qualcomm WTR3925 RF Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module) and a second signal processing section specified in Column F of Appendix D (*e.g.*, NXP 67V04 NFC Controller), the first signal processing section configured to output voice call signals in a first radio frequency range (*e.g.,* 850 MHz, 1900 MHz, 2100 MHz, 4G LTE and LTE advanced in bands 2, 3, 4, 5, 7, 8, 13, and/or Wi-Fi in 2.4 GHz and 5 GHz ) and the second signal processing section configured to output RFID transponder signals in a second radio frequency range (*e.g.*, 13.56 MHz). (VAR0000504-518; VAR0000849-855).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Column D of Appendix D (collectively, "transmitter"), comprising a first signal processing section specified in Column E of Appendix D and a second signal processing section specified in Column F of Appendix D, the first signal processing section configured to output voice call signals in a first radio frequency range and the second signal processing section configured to output RFID transponder signals in a second radio frequency range. The "transmitter" for each Accused Product specified in Column D of Appendix D is incorporated here by reference. (Appendix D; VAR0000639-1074).<br><br>• For example, as specified in Column D of Appendix D, the iPhone 6 has internal circuitry and components including: Qualcomm WTR1625L RF Transceiver, NXP 65V10 NFC module, and Murata 339S0228 Wi-Fi Module (collectively, "transmitter") comprising a first signal processing section specified in Column E of Appendix D (*e.g.*, Qualcomm WTR1625L RF Transceiver, Murata 339S0228 Wi-Fi Module) and a second signal processing section specified in Column F of Appendix D (*e.g.*, NXP 65V10 NFC module), the first signal |

| | | |
|---|---|---|
| | | processing section configured to output voice call signals in a first radio frequency range (*e.g.,* 850 MHz, 1900 MHz, 2100 MHz, 4G LTE and LTE advanced in bands 2, 3, 4, 5, 7, 8, 13, and/or Wi-Fi in 2.4 GHz and 5 GHz ) and the second signal processing section configured to output RFID transponder signals in a second radio frequency range (*e.g.*, 13.56 MHz). (VAR0000821-27).<br><br>To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (*e.g.,* emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (*e.g.,* mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions). |
| 21[c] | a storage medium to store a first data and instructions to: | The Accused Products have a storage medium to store a first data and instructions to perform the instructions below.<br><br>For example, the iPhone 7 has a storage medium (*e.g.*, SK Hynix 32 GB flash memory, NXP 67V04 NFC Controller, Secure Element) to store RFID transponder data that includes instructions (e.g., iOS operating system, RFID/NFC protocols, Secure element applets), to perform the instructions below. (VAR0000504-518).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Column C of Appendix D (collectively, "storage medium") to store RFID transponder data that includes instructions (e.g., iOS operating system or watchOS operating system, and RFID/NFC protocols), to perform the instructions below. The "storage medium" for each Accused Product specified in Column C of Appendix D, as well as the "instructions" specified in Appendix D, is incorporated here by reference. |

| | | |
|---|---|---|
| | | • For example, as specified in Column C of Appendix D, the iPhone 6 has a storage medium (*e.g.,* SanDisk SDMFLBCB2 128GB (16GB) NAND flash, NXP 65V10 NFC module, Secure Element) to store RFID transponder data that includes instructions (e.g., iOS operating system, RFID/NFC protocols, secure element applets), to perform the instructions below. (VAR0000432-448). |
| 21[d] | monitor for proximal presence of one or more RFID readers external to the mobile communication device; and | The Accused Products monitor for proximal presence of one or more RFID readers external to the mobile communication device.<br><br>The Accused RFID/NFC features conform to the EMV Contactless standard, which incorporates the ISO/IEC 14443 standard for proximity cards.<br><br>**What does EMV mean for Apple Pay?**<br><br>Apple Pay conforms to the latest EMV standards for tokenizing transactions, which leads to a more secure payment experience. With the EMV shift, merchants should update their terminals to support the latest software, which should also include NFC (near field communication), so you can accept Apple Pay and other contactless transactions. Learn what to do before you update your terminals.<br><br>(VAR0000001-02).<br><br>The Accused Products act as a proximity card (PICC) as defined by the ISO/IEC 14443 standard. The Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.[8] In accordance with ISO/IEC 14443, the Accused Products monitor for the proximal presence of an external l RFID reader (*e.g.*, a coupling device) by listening for commands and recognizing Request (REQA) and Wake Up (WUPA) commands from the RFID reader. |

[8] https://developer.apple.com/documentation/corenfc/cardsession/

| | | |
|---|---|---|
| | | **3.5**<br>**PICC**<br>*contactless integrated circuit card* (3.3) or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device<br><br>Note 1 to entry: Commonly called a proximity card.<br><br>(VAR0000054-71). |
| 21[e] | operate the transmitter to switch between the first and second signal processing sections to selectively: (a) output first RFID transponder data as said RFID transponder signals in a format employed by a proximal RFID reader, in response to detection by the mobile communication device of the proximal RFID reader, and (b) output a voice call signal for transmission over a wireless network; and | The Accused Products operate the transmitter to switch between the first and second signal processing sections to selectively: (a) output first RFID transponder data as said RFID transponder signals in a format employed by a proximal RFID reader, in response to detection by the mobile communication device of the proximal RFID reader, and (b) output a voice call signal for transmission over a wireless network.<br><br>For example, the iPhone 7 has internal circuitry and components, including: NXP 67V04 NFC Controller, Qualcomm WTR4905 Multimode LTE Transceiver, Qualcomm WTR3925 RF Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module (collectively, "transmitter") including the first and second signal processing sections, that is configured to output first RFID transponder data as said RFID transponder signals in a format employed by a proximal RFID reader, in response to detection by the mobile communication device of the proximal RFID reader (e.g., via RFID/NFC), and configured to output a voice call signal for transmission over a wireless network (e.g., via LTE, CDMA, UMTS, GSM and/or audio calling services that use a Wi-Fi connection). |



- And on the flip side:
  - SK Hynix H23QEG8VG2ACS 32 GB Flash
  - Murata 339S00199 Wi-Fi/Bluetooth Module
  - NXP PN67V NFC Controller w/ Secure Element
  - Apple/Dialog Semiconductor 338S00225 Power Management IC
  - Qualcomm PMD9645 Power Management IC
  - Qualcomm WTR4905 Multimode LTE Transceiver
  - Qualcomm WTR3925 RF Transceiver

(VAR0000504-518).

**Cellular and Wireless**

- **Model A1660**

  FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)
  TD-LTE (Bands 38, 39, 40, 41)
  TD-SCDMA 1900 (F), 2000 (A)
  CDMA EV-DO Rev. A (800, 1900, 2100 MHz)
  UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)
  GSM/EDGE (850, 900, 1800, 1900 MHz)

- **Model A1778**

  FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)

| | | |
|---|---|---|
| | | TD-LTE (Bands 38, 39, 40, 41)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>▪ **All models**<br>802.11ac Wi-Fi with MIMO<br>Bluetooth 4.2 wireless technology<br>NFC with reader mode<br>Express Cards<br>(VAR0000849-855).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Column D of Appendix D (collectively, "transmitter"), including the first and second signal processing sections, that is configured to output first RFID transponder data as said RFID transponder signals in a format employed by a proximal RFID reader, in response to detection by the mobile communication device of the proximal RFID reader (e.g., via RFID/NFC), and configured to output a voice call signal for transmission over a wireless network (e.g., via LTE, CDMA, UMTS, GSM, 5G and/or audio calling services that use a Wi-Fi connection). The "transmitter" for each Accused Product specified in Column D of Appendix D is incorporated here by reference. (Appendix D; VAR0001075-1293; VAR0000639-1074).<br><br>• For example, as specified in Column D of Appendix D, the iPhone 6 has internal circuitry and components including: Qualcomm WTR1625L RF Transceiver, NXP 65V10 NFC module, and Murata 339S0228 Wi-Fi Module (collectively, "transmitter") "), including the first and second signal processing sections, that is configured to output first RFID transponder data as said RFID transponder signals in a format employed by a proximal RFID reader, in response to detection by the mobile communication device of the proximal RFID reader (e.g., via RFID/NFC), and configured to output a voice call signal for transmission over a wireless network (e.g., via LTE, CDMA, UMTS, GSM and/or audio calling services that use a Wi-Fi connection). (VAR0000821-827). |

| | | |
|---|---|---|
| | | On detection by the mobile communication device of the proximal RFID reader, the Accused Products output first RFID transponder data as said RFID transponder signals in a format employed by a proximal RFID reader.<br><br>For example, the Accused Products, acting in accordance with the format employed by the RFID reader (*e.g.*, ISO/IEC 14443) and on detection of the RFID reader (*e.g.*, IDLE state exit), transmit RFID transponder data (*e.g.*, Answer to Request or ATQA) as a radio frequency signal (*e.g.*, 13.56 MHz frequency).<br><br>**6.3.2 IDLE state**<br><br>**Description:**<br><br>In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands.<br><br>**State exit conditions and transitions:**<br><br>The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA.<br><br>(VAR0000126-189).<br><br>**6.2 Frequency**<br><br>The frequency, $f_c$, of the RF operating field shall be 13,56 MHz ± 7 kHz.<br><br>(VAR0000072-125).<br><br>The data includes, e.g., data from applets within the Secure Element. |

| | | |
|---|---|---|
| | | **Secure Element**<br>The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.<br><br>(VAR0001075 at 1209).<br><br>To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (*e.g.,* emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (*e.g.,* mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions). |

| | | |
|---|---|---|
| 21[f] | a processor coupled to the transmitter and the storage to execute the instructions. | The Accused Products have a processor coupled to the transmitter and the storage to execute the instructions.<br><br>For example, the iPhone 7 has a processor (e.g., A10 Fusion chip, NXP 67V04 NF Controller, Secure Element) coupled to the transmitter (*e.g.*, NXP 67V04 NFC Controller, Qualcomm WTR4905 Multimode LTE Transceiver, Qualcomm WTR3925 RF Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module) and the storage (e.g., SK Hynix 32 GB flash memory, NXP 67V04 NFC controller, Secure Element) to execute the instructions (e.g., iOS operating system, RFID/NFC protocols, Secure Element applets). (VAR0000504-518).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Column B of Appendix D (collectively, "processor") coupled to the transmitter (specified in Column D of Appendix D) and the storage (specified in column C of Appendix D) to execute the instructions (specified in Column G of Appendix D) – these components are incorporated here by reference.<br><br>For example, as specified in Appendix D, the iPhone 6 has a processor (*e.g.,* A8 chip, NXP 65V10 NFC module, Secure Element) coupled to the transmitter (Qualcomm WTR1625L RF Transceiver and NXP 65V10 NFC module, Murata 339S0228 Wi-Fi Module ) and the storage (e.g., SanDisk SDMFLBCB2 128GB (16GB) NAND flash, NXP 65V10 NFC module, Secure Element) to execute the instructions (e.g., iOS operating system, RFID/NFC protocols, Secure Element applets). (VAR0000432-448). |
| 22 | The device of claim 21, wherein said first RFID transponder data comprises a selected one of a security key and an identifier. | The Accused Products embody the device of claim 21, wherein said first RFID transponder data comprises a selected one of a security key and an identifier. For example, credit cards can be added to Apple Pay, and the Accused Products may then be used to make contactless payments using those credit cards. In addition, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Products may then be used to unlock the hotel room and/or car. (VAR0000003-09; VAR0000020-22; VAR0001075-1293). |

| | | |
|---|---|---|
| | | The keys include, e.g., keys stored on applets in the Secure Element.<br><br>**Privacy and security**<br>Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted.<br><br>(VAR VAR0001075 at 1222). |
| 23 | The device of claim 22, wherein said first RFID transponder data comprises a security key, and said security key comprises a door key. | The Accused Products embody the device of claim 22, wherein said first RFID transponder data comprises a security key, and said security key comprises a door key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Products may then be used to unlock the hotel room and/or car.<br>(VAR0000003-09; VAR0000020-22; VAR0001075-1293). |
| 24 | The device of claim 23, wherein said door key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key. | The Accused Products embody the device of claim 23, wherein said door key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Products may then be used to unlock the hotel room and/or car.<br>(VAR0000003-09). |
| 25 | The device of claim 22, wherein said first RFID transponder data comprises an identifier, and said | The Accused Products embody the device of claim 22, wherein said first RFID transponder data comprises an identifier, and said identifier comprises a selected one of a social security number, a driver's license number, an affinity program account number, and a credit card number. For example, |

| | | |
|---|---|---|
| | identifier comprises a selected one of a social security number, a driver's license number, an affinity program account number, and a credit card number. | credit cards can be added to Apple Pay, and the Accused Products may then be used to make contactless payments using those credit cards. (VAR0000020-22, VAR0001075-1293).<br><br>The data includes, e.g., data from applets within the Secure Element.<br><br>**Secure Element**<br>The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.<br><br>(VAR0001075 at 1209). |
| 26 | The device of claim 21, wherein the instructions are further designed to facilitate the user in selecting the first RFID | The Accused Products embody the device of claim 21, wherein the instructions are further designed to facilitate the user in selecting the first RFID transponder data from a plurality of RFID transponder data, and instructing said output. For example, multiple payment cards can be added to Apple Pay, and the Accused Products may then be used to select a card to make a contactless payment. (VAR0000020-22). |

| | | |
|---|---|---|
| | transponder data from a plurality of RFID transponder data, and instructing said output. | |
| 27 | The device of claim 21, wherein the instructions are further designed to facilitate provision of the first RFID transponder data to the mobile communication device. | The Accused Products embody the device of claim 21, wherein the instructions are further designed to facilitate provision of the first RFID transponder data to the mobile communication device. For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Products. (VAR0001075-1293 at 1210-211). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09). |

68

| | | |
|---|---|---|
| | | **Credit, debit, and prepaid cards**<br><br>**Card provisioning security overview**<br><br>When a user adds a credit, debit, or prepaid card (including store cards) to Apple Wallet, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer determines whether to approve adding the card to Apple Wallet. As part of the card provisioning process, Apple Pay uses three server-side calls to send and receive communication with the card issuer or network:<br><br>• Required Fields<br>• Check Card<br>• Link and Provision<br><br>The card issuer or network uses these calls to verify, approve, and add cards to Apple Wallet. These client-server sessions use TLS 1.2 to transfer the data.<br><br>Full card numbers aren't stored on the device or on Apple Pay servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from most credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is never stored on Apple Pay servers or backed up to iCloud, and it is isolated from iOS, iPadOS, and watchOS devices and from Mac computers with Touch ID.<br><br>Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone, or within a card issuer's iPhone app. Adding a card to Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch. |
| 28 | The device of claim 27, wherein the instructions are further designed to include with said facilitating, provisioning of at least a signaling attribute associated with the outputting of the first RFID transponder data in the form of a radio frequency signal. | The Accused Products embody the device of claim 27, wherein the instructions are further designed to include with said facilitating, provisioning of at least a signaling attribute associated with the outputting of the first RFID transponder data in the form of a radio frequency signal.<br><br>For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Devices (e.g., via RFID/NFC), and Apple further directs, controls, and specifies the communication and security protocols associated with making contactless payments via Apple Pay. (VAR0001075-1293 at 1208-209). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09). |

| | | |
|---|---|---|
| | | **NFC controller**<br>The NFC controller handles Near Field Communication protocols and routes communication between the Application Processor and the Secure Element, and between the Secure Element and the point-of-sale terminal.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server. |

70

| | | |
|---|---|---|
| 29 | The device of claim 21, wherein the instructions are further designed to sense for a probing radio frequency signal of the RFID reader. | The Accused Products embody the device of claim 21, wherein the instructions are further designed to sense for a probing radio frequency signal of the RFID reader. For example, the Accused Products, in accordance with ISO/IEC 14443, listen for and recognize Request (REQA) and Wake Up (WUPA) commands from the RFID reader.<br><br>**3.5**<br>**PICC**<br>*contactless integrated circuit card* (3.3) or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device<br><br>Note 1 to entry: Commonly called a proximity card.<br><br>(VAR0000054-71).<br><br>**6.3.2 IDLE state**<br><br>**Description:**<br><br>In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands.<br><br>**State exit conditions and transitions:**<br><br>The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA.<br><br>(VAR0000126-189). |
| 31 | The device of claim 21, wherein the mobile communication device is a selected one of a wireless mobile phone and a personal digital assistant equipped with communication capability. | The Accused Products embody the device of Claim 21, wherein the mobile communication device is a selected one of a wireless mobile phone and a personal digital assistant equipped with communication capability. For example the Accused Products are wireless mobile phones and/or personal digital assistants equipped with communication capability. For example the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (*e.g.*, via LTE, CDMA, UMTS, and/or GSM), and/o audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling). |

| | | |
|---|---|---|
| | | **Audio Calling**[5]<br>■ FaceTime audio<br>■ Voice over LTE (VoLTE)[6]<br>■ Wi-Fi calling[6]<br><br>**Cellular and Wireless**<br>■ **Model A1660**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>TD-SCDMA 1900 (F), 2000 (A)<br>CDMA EV-DO Rev. A (800, 1900, 2100 MHz)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **Model A1778**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30) |

| | | |
|---|---|---|
| | | TD-LTE (Bands 38, 39, 40, 41)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>▪ **All models**<br>802.11ac Wi-Fi with MIMO<br>Bluetooth 4.2 wireless technology<br>NFC with reader mode<br>Express Cards<br>(VAR0000849-855).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (*e.g.*, Via LTE via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling). (VAR0000639-1074). |
| 32[a] | A switchable mobile communication device capable of radio frequency identifier RFID communication and voice call communication, the mobile communication device comprising: | To the extent that the claim's preamble is determined to be a limitation or otherwise limiting, the Accused Products are switchable mobile communication device[s] capable of RFID communication and voice call communication.<br><br>For example, as reflected in Apple's product literature, the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (*e.g.*, via LTE, CDMA, UMTS, and/or GSM), and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling), as well as RFID communication (*e.g.*, via RFID/NFC, including via Apple Pay, which uses NFC technology between the device and the payment terminal).<br><br>**Audio Calling**[5]<br>▪ FaceTime audio<br>▪ Voice over LTE (VoLTE)[6]<br>▪ Wi-Fi calling[6] |

| | | |
|---|---|---|
| | | **Cellular and Wireless**<br>■ **Model A1660**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>TD-SCDMA 1900 (F), 2000 (A)<br>CDMA EV-DO Rev. A (800, 1900, 2100 MHz)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **Model A1778**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>■ **All models**<br>802.11ac Wi-Fi with MIMO<br>Bluetooth 4.2 wireless technology<br>NFC with reader mode<br>Express Cards<br>(VAR0000849-855).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (*e.g.*, via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling), as well as RFID communication (*e.g.*, via RFID/NFC, including via Apple Pay, which uses NFC technology between the device and the payment terminal). (VAR0000639-1074). |

| | | |
|---|---|---|
| | | When you use Apple Pay in stores<br><br>When you use Apple Pay in stores that accept contactless payments, Apple Pay uses Near Field Communication (NFC) technology between your device and the payment terminal. NFC is an industry-standard, contactless technology that's designed to work only across short distances. If your iPhone is on and detects an NFC field, it will present you with your default card. To send your payment information, you must authenticate using Face ID, Touch ID, or your passcode (except when you use Express Mode with a payment or transit card). With Face ID or with Apple Watch, you must double-click the side button when the device is unlocked to activate your default card for payment.<br><br>(VAR0000010-140).<br><br>NFC is a subset within the family of RFID technology. (VAR0000026-42) ("RFID is the process by which items are uniquely identified using radio waves, and NFC is a specialized subset within the family of RFID technology."); (VAR0000043-53) ("Hierarchically, NFC is a subset of RFID.")).<br><br>For example, the iPhone as a whole is capable of entering two different modes, including a telephony mode and an RFID/NFC mode. A user can affirmatively launch the telephony and/or RFID/NFC modes, and/or the iPhone enters the telephony and/or RFID/NFC mode when its received the relevant signal (e.g., an incoming call or detecting an RFID reader), as shown below. |

75

75

76







When an RFID reader signal is detected by the mobile communications device, the user must first address how to respond to that signal telephony controls, and vice versa.

To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (*e.g.,* emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (*e.g.,* mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions).

| | | |
|---|---|---|
| 32[b] | a transmitter configured to transmit a voice call signal in a first operational state and a RFID transponder signal in a second operational state; | The Accused Products have a transmitter configured to transmit a voice call signal in a first operational state and a RFID transponder signal in a second operational state.<br><br>For example, the iPhone 7 has internal circuitry and components, including an NXP 67V04 NFC Controller, Qualcomm WTR4905 Multimode LTE Transceiver, Qualcomm WTR3925 RF Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module (collectively, "transmitter"), configured to transmit a voice call signal (*e.g.*, 850 MHz, 1900 MHz, 2100 MHz, 4G LTE and LTE advanced in bands 2, 3, 4, 5, 7, 8, 13, and/or Wi-Fi in 2.4 GHz and 5 GHz) in a first operational state and a RFID transponder signal (*e.g.*, 13.56 MHz) in a second operational state.<br><br>(VAR0000504-518; VAR0000849-855).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Column D of Appendix D (collectively, "transmitter"), configured to transmit a voice call signal (*e.g.*, 850 MHz, 1900 MHz, 2100 MHz, 4G LTE and LTE advanced in bands 2, 3, 4, 5, 7, 8, 13, and/or Wi-Fi in 2.4 GHz and 5 GHz) in a first operational state and a RFID transponder signal (*e.g.*, 13.56 MHz) in a second operational state. The "transmitter" for each Accused Product specified in Column D of Appendix D is incorporated here by reference. (Appendix D; VAR0000639-1074).<br><br>• For example, as specified in Column D of Appendix D, the iPhone 6 has internal circuitry and components including: Qualcomm WTR1625L RF Transceiver, NXP 65V10 NFC module, and Murata 339S0228 Wi-Fi Module (collectively, "transmitter") configured to transmit a voice call signal (*e.g.*, 850 MHz, 1900 MHz, 2100 MHz, 4G LTE and LTE advanced in bands 2, 3, 4, 5, 7, 8, 13, and/or Wi-Fi in 2.4 GHz and 5 GHz) in a first operational state and a RFID transponder signal (*e.g.*, 13.56 MHz) in a second operational state. (VAR0000432-438; VAR0000821-827).<br><br>To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (*e.g.,* emulating an RFID tag and performing voice call communication in a single device |

| | | |
|---|---|---|
| | | using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (*e.g.,* mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions). |
| 32[c] | a storage medium to store a first data and instructions to switch the transmitter between the first and second operational states to selectively (a) monitor for proximal presence of a proximal RFID reader, and on detection of the proximal RFID reader, output RFID transponder data as an RFID signal in a format employed by the RFID reader, and (b) transmit a voice call signal to another user of another communication device at least in part over a wireless network; and | The Accused Products have a storage medium to store a first data and instructions to switch the transmitter between the first and second operational states to selectively (a) monitor for proximal presence of a proximal RFID reader, and on detection of the proximal RFID reader, output RFID transponder data as an RFID signal in a format employed by the RFID reader, and (b) transmit a voice call signal to another user of another communication device at least in part over a wireless network.<br><br>For example, the iPhone 7 has a storage medium (*e.g.*, SK Hynix 32 GB flash memory, NXP 67V04 NFC Controller, Secure Element) to store a first data and instructions (*e.g.*, iOS operating system, RFID/NFC protocols, Secure Element applets) to switch the transmitter (*e.g.*, NXP 67V04 NFC Controller, Qualcomm WTR4905 Multimode LTE Transceiver, Qualcomm WTR3925 RF Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module) between the first and second operational states to selectively (a) monitor for proximal presence of a proximal RFID reader, and on detection of the proximal RFID reader, output RFID transponder data as an RFID signal in a format employed by the RFID reader (e.g., via RFID/NFC), and (b) transmit a voice call signal to another user of another communication device at least in part over a wireless network (*e.g.*, via LTE, CDMA, UMTS, GSM and/or audio calling services that use a Wi-Fi connection). (VAR0000504-518).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Column C of Appendix D (collectively, "storage medium") to store a first data and instructions to switch the transmitter between the first and second operational states to selectively (a) monitor for proximal presence of a proximal RFID reader, and on detection of the proximal RFID reader, output RFID transponder data as an RFID signal in a format employed by the RFID reader, and (b) transmit a voice call signal to another user of another communication device at least in part over a wireless network. The "storage medium," for each Accused Product specified in Column C of |

| | | |
|---|---|---|
| | | Appendix D, as well as the "instructions" and "transmitter," specified in Appendix D are incorporated here by reference.<br><br>• For example, as specified in Column C of Appendix D, the iPhone 6 has a storage medium (*e.g.,* SanDisk SDMFLBCB2 128GB (16GB) NAND flash, NXP 65V10 NFC module, Secure Element) to store a first data and instructions (*e.g.*, iOS operating system, RFID/NFC protocols, Secure Element applets) to switch the transmitter (*e.g.*, Qualcomm WTR1625L RF Transceiver, NXP 65V10 NFC module, Murata 339S0228 Wi-Fi Module) between the first and second operational states to selectively (a) monitor for proximal presence of a proximal RFID reader, and on detection of the proximal RFID reader, output RFID transponder data as an RFID signal in a format employed by the RFID reader (e.g., via RFID/NFC), and (b) transmit a voice call signal to another user of another communication device at least in part over a wireless network (*e.g.*, via LTE, CDMA, UMTS, GSM and/or audio calling services that use a Wi-Fi connection). (VAR0000432-448).<br><br>The Accused Products monitor for proximal presence of a proximal RFID reader (*e.g.* a contactless point-of-sale terminal/reader), and on detection of the proximal RFID reader, output RFID transponder data as an RFID signal in a format employed by the RFID reader (via RFID/NFC).<br><br>The Accused RFID/NFC features conform to the EMV Contactless standard, which incorporates the ISO/IEC 14443 standard for proximity cards.<br><br>**What does EMV mean for Apple Pay?**<br><br>Apple Pay conforms to the latest EMV standards for tokenizing transactions, which leads to a more secure payment experience. With the EMV shift, merchants should update their terminals to support the latest software, which should also include NFC (near field communication), so you can accept Apple Pay and other contactless transactions. Learn what to do before you update your terminals. |

80

| | | |
|---|---|---|
| | | (VAR0000001-02).<br><br>The Accused Products act as a proximity card (PICC) as defined by the ISO/IEC 14443 standard. The Accused Products use signals and commands according to ISO/IEC 14443 and/or ISO/IEC 7816-4.[9] In accordance with ISO/IEC 14443, the Accused Products monitor for the proximal presence of a proximal, external RFID reader (*e.g.*, a coupling device) by listening for commands and recognizing Request (REQA) and Wake Up (WUPA) commands from the RFID reader. On detection of the reader, the Accused Products, acting in accordance with ISO/IEC 14443, output RFID transponder data as an RFID signal in a format employed by the RFID reader (*e.g.*, Answer to Request or ATQA) in response.<br><br>**3.5**<br>**PICC**<br>*contactless integrated circuit card* (3.3) or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device<br><br>Note 1 to entry: Commonly called a proximity card.<br><br>(VAR0000054-71).<br><br>**6.3.2 IDLE state**<br><br>**Description:**<br><br>In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands.<br><br>**State exit conditions and transitions:**<br><br>The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA.<br><br>(VAR0000072-125).<br><br>The data includes, e.g., data from applets within the Secure Element. |

[9] https://developer.apple.com/documentation/corenfc/cardsession/

| | | |
|---|---|---|
| | | **Secure Element**<br>The Secure Element hosts a specially designed applet to manage Apple Pay. It also includes applets certified by payment networks or card issuers. Credit, debit, or prepaid card data is sent from the payment network or card issuer encrypted to these applets using keys that are known only to the payment network or card issuer and the applets' security domain. This data is stored within these applets and protected using the Secure Element's security features. During a transaction, the terminal communicates directly with the Secure Element through the near-field-communication (NFC) controller over a dedicated hardware bus.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br><br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server.<br><br>(VAR0001075 at 1209).<br><br>To the extent this limitation is not literally met by the Accused Products because the Accused Products do not output voice call signals and RFID transponder signals through mutually exclusive single-mode states or via a singular chip, the Accused Products are insubstantially different from, and equivalent to, this limitation. For example, the Accused Products performs substantially the same function (*e.g.,* emulating an RFID tag and performing voice call communication in a single device using partially overlapping components), in substantially the same way (e.g., through a switchable mobile communications device that can perform either function separately based on user input or detected signals) to achieve substantially the same result (*e.g.,* mobile communications device capable of both RFID emulation and voice call communication that leverages some shared components in a single housing and lets the user toggle between the two functions). |

| | | |
|---|---|---|
| 32[d] | a processor coupled to the transmitter and the storage to execute the instructions. | The Accused Products have a processor coupled to the transmitter and the storage to execute the instructions.<br><br>For example, the iPhone 7 has a processor (e.g., A10 Fusion chip, NXP 67V04 NF Controller, Secure Element) coupled to the transmitter (*e.g.*, NXP 67V04 NFC Controller, Qualcomm WTR4905 Multimode LTE Transceiver, Qualcomm WTR3925 RF Transceiver, and Murata 339S00199 Wi-Fi/Bluetooth Module) and the storage (e.g., SK Hynix 32 GB flash memory, NXP 67V04 NFC controller, Secure Element) to execute the instructions (e.g., iOS operating system, RFID/NFC protocols, Secure Element applets). (VAR0000504-518).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, each have internal circuitry and components, including, for each Accused Product, the components specified in Column B of Appendix D (collectively, "processor") coupled to the transmitter (specified in Column D of Appendix D) and the storage (specified in column C of Appendix D) to execute the instructions (specified in Column G of Appendix D) – these components are incorporated here by reference.<br><br>For example, as specified in Appendix D, the iPhone 6 has a processor (*e.g.,* A8 chip, NXP 65V10 NFC module, Secure Element) coupled to the transmitter (Qualcomm WTR1625L RF Transceiver and NXP 65V10 NFC module, Murata 339S0228 Wi-Fi Module ) and the storage (e.g., SanDisk SDMFLBCB2 128GB (16GB) NAND flash, NXP 65V10 NFC module, Secure Element) to execute the instructions (e.g., iOS operating system, RFID/NFC protocols, Secure Element applets). (VAR0000432-438). |
| 33 | The device of claim 32, wherein said instructions are further designed to sense for a probing radio frequency signal of the RFID reader. | The Accused Products embody a device of claim 32, wherein said instructions are further designed to sense for a probing radio frequency signal of the RFID reader.<br><br>For example, the Accused Products, in accordance with ISO/IEC 14443, listen for and recognize Request (REQA) and Wake Up (WUPA) commands from the RFID reader. |

| | | |
|---|---|---|
| | | **3.5**<br>**PICC**<br>*contactless integrated circuit card* (3.3) or other object with which communication and power transfer are done by inductive coupling in proximity of a coupling device<br><br>Note 1 to entry: Commonly called a proximity card.<br><br>(VAR0000054-71).<br><br>**6.3.2 IDLE state**<br><br>**Description:**<br><br>In IDLE state, the PICC is powered. It listens for commands and shall recognize REQA and WUPA commands.<br><br>**State exit conditions and transitions:**<br><br>The PICC enters READY state after it has received a valid REQA or WUPA command and transmitted its ATQA.<br><br>(VAR0000126-189). |
| 34 | The device of claim 32, wherein said RFID transponder data comprises a security key. | The Accused Products embody the device of claim 32, wherein said RFID transponder data comprises a security key. For example, credit cards can be added to Apple Pay, and the Accused Products may then be used to make contactless payments using those credit cards. In addition, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Products may then be used to unlock the hotel room and/or car.<br>(VAR0000003-09; VAR0000020-22; VAR0001075-1293). |

| | | |
|---|---|---|
| | | The keys include, e.g., keys stored on applets in the Secure Element.<br><br>**Privacy and security**<br>Keys in Apple Wallet take full advantage of the privacy and security built into iPhone and Apple Watch. When or where a person uses their keys in Apple Wallet is never shared with Apple or stored on Apple servers, and credentials are securely stored inside the Secure Element (SE) of supported devices. The SE hosts specially designed applets to securely manage and store access keys, ensuring that keys can't be extracted.<br><br>(VAR VAR0001075 at 12222). |
| 35 | The device of claim 34, wherein said security key comprises a door key. | The Accused Products embody the device of claim 34, wherein said security key comprises a door key. For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Product may then be used to unlock the hotel room and/or car.<br><br>(VAR0000003-09). |
| 36 | The device of claim 35, wherein said door key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key. | The Accused Products embody the device of claim 35, wherein said door key comprises a selected one of a garage door key, an exterior door key, an interior door key, and a motor vehicle door key.<br><br>For example, hotel room keys and/or car keys can be added to the Apple Wallet app, and the Accused Product may then be used to unlock the hotel room and/or car.<br><br>(VAR0000003-09). |
| 37 | The device of claim 32, wherein the instructions are further designed to facilitate provision of the RFID transponder data to | The Accused Products embody the device of claim 32, wherein the instructions are further designed to facilitate provision of the RFID transponder data to the mobile communication device.<br>For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless |

| | | |
|---|---|---|
| | the mobile communication device. | payments with Apple Pay using the Accused Products. (VAR0001075-1293 at 1210, 1211). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09). |

86

87

# Credit, debit, and prepaid cards

## Card provisioning security overview

When a user adds a credit, debit, or prepaid card (including store cards) to Apple Wallet, Apple securely sends the card information, along with other information about user's account and device, to the card issuer or card issuer's authorized service provider. Using this information, the card issuer determines whether to approve adding the card to Apple Wallet. As part of the card provisioning process, Apple Pay uses three server-side calls to send and receive communication with the card issuer or network:

- Required Fields
- Check Card
- Link and Provision

The card issuer or network uses these calls to verify, approve, and add cards to Apple Wallet. These client-server sessions use TLS 1.2 to transfer the data.

Full card numbers aren't stored on the device or on Apple Pay servers. Instead, a unique Device Account Number is created, encrypted, and then stored in the Secure Element. This unique Device Account Number is encrypted in such a way that Apple can't access it. The Device Account Number is unique and different from most credit or debit card numbers; the card issuer or payment network can prevent its use on a magnetic stripe card, over the phone, or on websites. The Device Account Number in the Secure Element is never stored on Apple Pay servers or backed up to iCloud, and it is isolated from iOS, iPadOS, and watchOS devices and from Mac computers with Touch ID.

Cards for use with Apple Watch are provisioned for Apple Pay using the Apple Watch app on iPhone, or within a card issuer's iPhone app. Adding a card to Apple Watch requires that the watch be within Bluetooth communications range. Cards are specifically enrolled for use with Apple Watch and have their own Device Account Numbers, which are stored within the Secure Element on the Apple Watch.

| | | |
|---|---|---|
| | | **Adding credit or debit cards manually**<br>To add a card manually, the name, card number, expiration date, and CVV are used to facilitate the provisioning process. From within Settings, Apple Wallet, or the Apple Watch app, users can enter that information either by typing or by using the device's camera. When the camera captures the card information, Apple attempts to populate the name, card number, and expiration date. The photo is never saved to the device or stored in the photo library. After all the fields are filled in, the Check Card process verifies the fields other than the CVV. They are then encrypted and sent to the Apple Pay server.<br>If a terms and conditions ID is returned with the Check Card process, Apple downloads and displays the terms and conditions of the card issuer to the user. If the user accepts the terms and conditions, Apple sends the ID of the terms that were accepted as well as the CVV to the Link and Provision process. Additionally, as part of the Link and Provision process, Apple shares information from the device with the card issuer or network. This includes information about (a) the user's iTunes and App Store account activity (for example, whether the user has a long history of transactions within iTunes), (b) the user's device (for example, the phone number, name, and model of the user's device plus any companion Apple device necessary to set up Apple Pay), and (c) the user's approximate location at the time the user adds their card (if the user has Location Services enabled). Using this information, the card issuer determines whether to approve adding the card to Apple Pay.<br>As the result of the Link and Provision process, two things occur:<br>• The device begins to download the Apple Wallet pass file representing the credit or debit card.<br>• The device begins to bind the card to the Secure Element.<br>The pass file contains URLs to download card art, metadata about the card such as contact information, the related issuer's app, and supported features. It also contains the pass state, which includes information such as whether the personalizing of the Secure Element has completed, whether the card is currently suspended by the card issuer, or whether additional verification is required before the card can make payments with Apple Pay. |
| 38 | The device of claim 37, wherein the instructions are further designed to include | The Accused Products embody the device of claim 37, wherein the instructions are further designed to include with said facilitating, provisioning of at least a signaling attribute associated with the outputting of the RFID transponder data in the form of a radio frequency signal. |

88

| | | |
|---|---|---|
| | with said facilitating, provisioning of at least a signaling attribute associated with the outputting of the RFID transponder data in the form of a radio frequency signal. | For example, Apple directs and controls the provisioning process for the Accused RFID/NFC Features. For example, Apple directs and controls the provisioning process by which a user can add credit, debit, or prepaid card (including store cards) to Apple Wallet before making contactless payments with Apple Pay using the Accused Devices, and Apple further directs, controls, and specifies the communication and security protocols associated with making contactless payments via Apple Pay. (VAR0001075-1293 at 1208, 1209). Apple also directs and controls the provisioning of keys and passes. (VAR0000003-09).<br><br>**NFC controller**<br>The NFC controller handles Near Field Communication protocols and routes communication between the Application Processor and the Secure Element, and between the Secure Element and the point-of-sale terminal.<br><br>**NFC controller**<br>As the gateway to the Secure Element, the NFC controller helps ensure that all contactless payment transactions are conducted using a point-of-sale terminal that's in close proximity to the device. Only payment requests arriving from an in-field terminal are marked by the NFC controller as contactless transactions.<br>After a credit, debit, or prepaid card (including store cards) payment is authorized by the cardholder using Face ID, Touch ID, or a passcode, or on an unlocked Apple Watch by double-clicking the side button, contactless responses prepared by the payment applets within the Secure Element are exclusively routed by the controller to the NFC field. Consequently, payment authorization details for contactless payment transactions are contained to the local NFC field and are never exposed to the Application Processor. In contrast, payment authorization details for payments within apps and on the web are routed to the Application Processor, but only after encryption by the Secure Element to the Apple Pay server. |
| 39 | The device of claim 32, wherein the mobile communication device is a selected of a wireless | The Accused Products embody the device of claim 32, wherein the mobile communication device is a selected of a wireless mobile phone and a personal digital assistant equipped with communication capability. |

| | | |
|---|---|---|
| | mobile phone and a personal digital assistant equipped with communication capability. | For example the Accused Products are wireless mobile phones and/or personal digital assistants equipped with communication capability. For example the iPhone 7 is capable of voice call communication, such as traditional cellular telephone service (*e.g.*, via LTE, CDMA, UMTS, and/or GSM), and/o audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling).<br><br>**Audio Calling**[5]<br>▪ FaceTime audio<br>▪ Voice over LTE (VoLTE)[6]<br>▪ Wi-Fi calling[6]<br><br>**Cellular and Wireless**<br>▪ **Model A1660**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30)<br>TD-LTE (Bands 38, 39, 40, 41)<br>TD-SCDMA 1900 (F), 2000 (A)<br>CDMA EV-DO Rev. A (800, 1900, 2100 MHz)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>▪ **Model A1778**<br>FDD-LTE (Bands 1, 2, 3, 4, 5, 7, 8, 12, 13, 17, 18, 19, 20, 25, 26, 27, 28, 29, 30) |

| | | |
|---|---|---|
| | | TD-LTE (Bands 38, 39, 40, 41)<br>UMTS/HSPA+/DC-HSDPA (850, 900, 1700/2100, 1900, 2100 MHz)<br>GSM/EDGE (850, 900, 1800, 1900 MHz)<br>▪ **All models**<br>802.11ac Wi-Fi with MIMO<br>Bluetooth 4.2 wireless technology<br>NFC with reader mode<br>Express Cards<br>(VAR0000849-855).<br><br>As further examples, the Accused Products, including iPhone models and Apple Watch models, are also capable of voice call communication, such as traditional cellular telephone service (*e.g.*, Via LTE via LTE, CDMA, UMTS, GSM and/or 5G) and/or audio calling services that use a Wi-Fi connection (*e.g.*, via FaceTime audio and Wi-Fi calling). (VAR0000639-1074). |