

EXHIBIT I

EXHIBIT I

UNITED STATES PATENT NO. 6,463,534¹

Accused Apple Products: Apple Mac Pro, Apple iMac, new Apple iMac,² Apple Mac mini, new Apple Mac mini,³ Apple MacBook Pro, Apple MacBook, 15-inch Apple MacBook Pro with Retina Display, 13-inch Apple MacBook Pro with Retina Display,⁴ Apple MacBook Air, 3rd Generation Apple iPod Touch, 4th Generation Apple iPod Touch, 5th Generation Apple iPod Touch⁵, Apple iPhone 3GS, Apple iPhone 4, Apple iPhone 4S, Apple iPhone 6S⁷, Apple iPad, Apple iPad with 3G, Apple iPad 2, Apple iPad 2 with 3G, 3rd Generation Apple iPad, 3rd Generation Apple iPad + 4G, 4th Generation Apple iPad,⁸ 4th

¹ Motorola Mobility's investigation is ongoing and discovery is not yet complete. Apple has, thus far, not produced all of its documents and source code relevant to the accused methods and products. Motorola reserves the right to supplement or amend these contentions based on subsequent discovery or disclosures made pursuant to FRCP 26. Motorola further reserves the right to amend and supplement its contentions with respect to any products released by Apple subsequent to the service of these initial infringement contentions, in accordance with the schedule set forth in the Court's Order of October 25, 2012. Further, to the extent Apple releases any new products with the same functionality accused of infringement in the Accused Apple Products in these contentions, Motorola reserves the right to seek appropriate relief from the court in accordance with its order of October 25, 2012 and in accordance with the Federal Rules of Civil Procedure.

² The term "new Apple iMac" means Apple's new iMac computers announced by Apple on October 23, 2012. *See* <http://www.apple.com/pr/library/2012/10/23All-New-iMac-Features-Stunning-Design-Brilliant-Display-Faster-Performance.html>.

³ The term "new Apple Mac mini" means Apple's new Mac mini computers announced by Apple on October 23, 2012. *See* <http://www.apple.com/pr/library/2012/10/23All-New-iMac-Features-Stunning-Design-Brilliant-Display-Faster-Performance.html>.

⁴ The term "13-inch Apple MacBook Pro with Retina Display" means Apple's new 13-inch MacBook Pro computer announced by Apple on October 23, 2012. *See* <http://www.apple.com/pr/library/2012/10/23Apple-Introduces-13-inch-MacBook-Pro-with-Retina-Display.html>.

⁵ The term "5th Generation Apple iPod Touch" means Apple's new iPod Touch announced by Apple on September 12, 2012. *See* <http://www.apple.com/pr/library/2012/09/12Apple-Introduces-New-iPod-touch-iPod-nano.html>.

⁷ The term "Apple iPhone 5" means Apple's new iPhone announced by Apple on September 12, 2012. *See* <http://www.apple.com/pr/library/2012/09/12Apple-Introduces-iPhone-5.html>.

⁸ The terms "4th Generation Apple iPad" and "4th Generation Apple iPad [with cellular]" mean Apple's new iPad devices announced by Apple on October 23, 2012. *See* <http://www.apple.com/pr/library/2012/10/23Apple-Introduces-iPad-mini.html>.

Generation Apple iPad [with cellular], iPad Mini,⁹ iPad mini [with cellular], Apple TV 1st Gen, Apple TV 2nd Gen, Apple TV 3rd Gen

Apple directly infringes the '534 patent, either literally or through the doctrine of equivalents, pursuant to 35 U.S.C. § 271(a).


In addition to Apple's direct infringement of the '534 patent through its development, testing, use, distribution and sale of its products and services, Apple also indirectly infringes the '534 patent pursuant to 35 U.S.C. § 271(b) and (c). End-users and others in the distribution channel of the Accused Apple Products directly infringe this claim by using, selling, offering for sale, and/or importing these devices into the United States. Apple contributes to and induces the infringement of asserted claims 7 and 9 through its promotion and provision of marketing, sale and/or technical support of the Accused Apple Products and associated services in the United States, and through the design, marketing, manufacture, sale, and/or technical support of the Accused Apple Products. Apple supplies Accused Apple Products and actively encourages the use, sale, offer for sale, and importation of the same in the United States through the promotion and provision of marketing literature, promotion, and user guides, which induces and results in direct infringement. Apple has known or should have known that these actions would cause direct infringement of the '534 patent and did so with specific intent to encourage direct infringement, at least as of April 13, 2012, Motorola served Apple with Motorola's motion for leave to file Motorola's first amended complaint in this litigation, which attached the '534 patent as an exhibit. Despite knowing of the '534 patent, Apple continues to make, use, offer to sell, and sell its products and has continued to circulate marketing literature and user guides encouraging users of the Accused Apple Products to infringe. Additionally, the identified features of the Accused Apple Products are material parts of the inventions of the asserted claims and have no substantial non-infringing uses.

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
Claim 1	

⁹ The terms "Apple iPad mini" and "Apple iPad mini [with cellular]" mean Apple's new iPad mini devices announced by Apple on October 23, 2012. See <http://www.apple.com/pr/library/2012/10/23Apple-Introduces-iPad-mini.html>.

¹⁰ This chart provides Motorola's infringement analysis for the Accused Apple Products. Upon information and belief, the analysis set forth in this chart applies to all of the Accused Apple Products running versions of iOS 5, iOS 6, and OSX. iOS devices refers to the 3rd Generation Apple iPod Touch, 4th Generation Apple iPod Touch, 5th Generation Apple iPod Touch¹⁰, Apple iPhone 3GS, Apple iPhone 4, Apple iPhone 4S, Apple iPhone 5¹⁰, Apple iPad, Apple iPad with 3G, Apple iPad 2, Apple iPad 2 with 3G, 3rd Generation Apple iPad, 3rd Generation Apple iPad + 4G, 4th Generation Apple iPad, 4th Generation Apple iPad [with cellular], iPad Mini, and iPad mini [with cellular]. OSX devices refer to Apple Mac Pro, Apple iMac, new Apple iMac, Apple Mac mini, new Apple Mac mini, Apple MacBook Pro, Apple MacBook, 15-inch Apple MacBook Pro with Retina Display, 13-inch Apple MacBook Pro with Retina Display, Apple MacBook Air, Apple TV 1st Gen, Apple TV 2nd Gen, and Apple TV 3rd Gen.

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
<p>1. A method of conducting transactions in a wireless electronic commerce system</p>	<p>The accused devices, in conjunction with the Apple App Store and/or iTunes use a method of conducting transactions in a wireless electronic commerce system, as described below.</p> <p style="text-align: center;"><u>App Store</u></p> <p>Apple devices conduct transactions in a wireless commerce system with the App Store. For example, iOS devices can wirelessly purchase and download applications from the App Store:</p>

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="676 212 827 245">At a glance</p> <p data-bbox="676 250 1329 277">Use the App Store to browse, purchase, and download apps to iPhone.</p> <div data-bbox="676 298 1102 755">  <p data-bbox="940 318 1073 341">View a category.</p> <p data-bbox="940 683 1102 722">View updates and previous purchases.</p> <p data-bbox="747 735 867 755">Browse buttons</p> </div> <p data-bbox="676 792 877 818">Use the App Store to:</p> <ul data-bbox="676 834 1245 1000" style="list-style-type: none"> • Find new free or purchased apps by browsing or searching • Download previous purchases and updates • Redeem a gift card or download code • Recommend an app to a friend • Manage your App Store account <p data-bbox="676 1021 1396 1047">Note: You need an Internet connection and an Apple ID to use the App Store.</p> <p data-bbox="676 1062 1556 1146">Purchase an app: Tap the app's price (or tap Free), then tap Buy Now. If you already purchased the app, "install" appears instead of the price. You won't be charged to download it again. While an app is being downloaded, its icon appears on the Home screen with a progress indicator.</p>

¹¹ iPhone User Guide (iOS 6) at 96 (MOTO-SDFL-16228).

'534 Patent Claim **Exemplary Apple Product:** iOS and OSX devices¹⁰/Apple App Store and iTunes

About the App Store

You can search for, browse, review, purchase, and download apps from the App Store directly to iPad.

Note: The App Store may not be available in all countries or regions, and App Store content may vary by country or region. Features are subject to change.

To browse the App Store, iPad must be connected to the Internet. See "Network" on page 125. To purchase apps, you need an Apple ID. See "Store settings" on page 96.

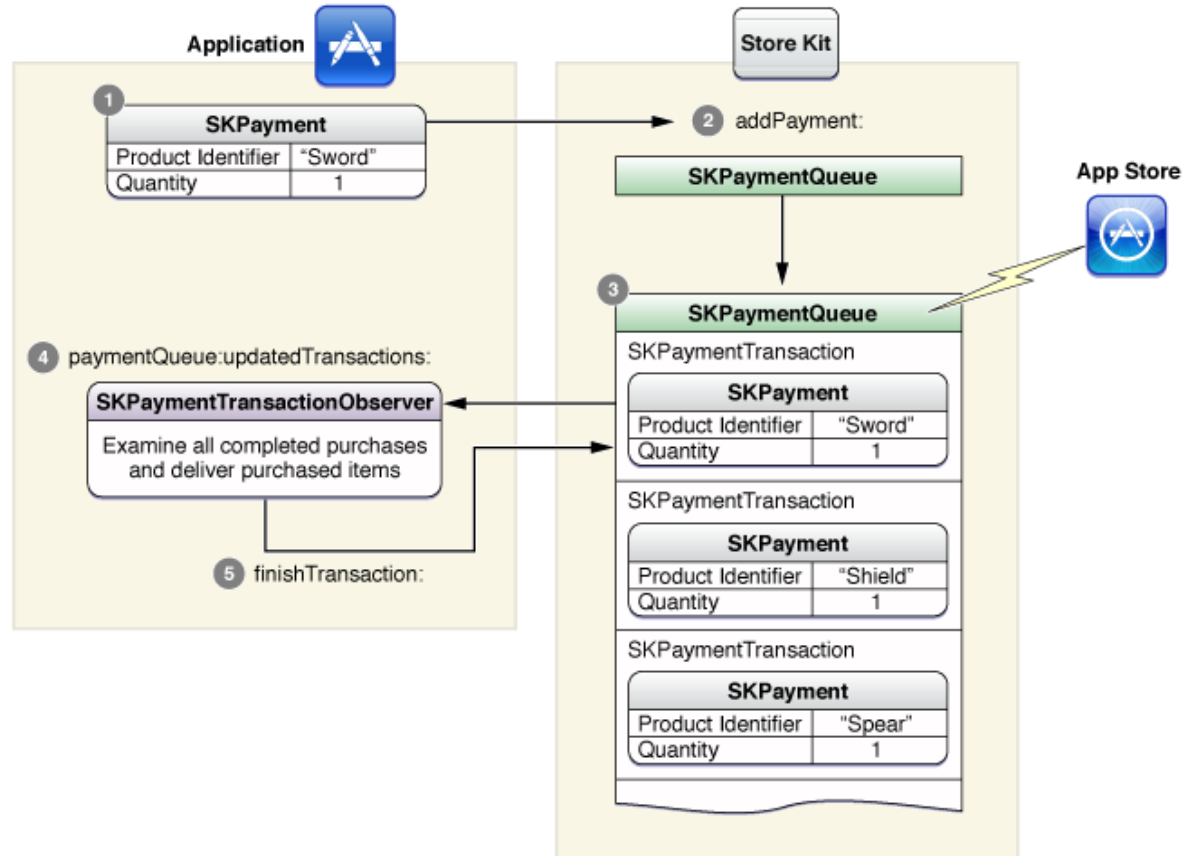


Check for app updates.

12

iOS devices can also download purchases from within apps themselves. The Apple App Store allows users to embed a store directly within an application. An in-app purchase feature is facilitated using the Store Kit framework. Store Kit prompts the user to authorize the payment, then notifies the application so that it can provide the items the user purchased.¹³ This process involves fine-grained access control.

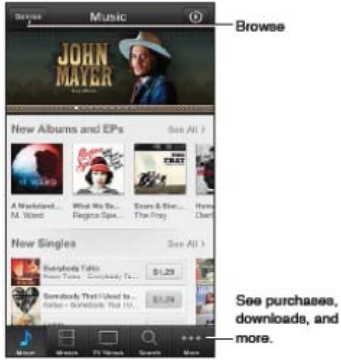
¹² iPad User Guide (iOS 5.1) at 94 (MOTO-SDFL-19948).
¹³ See generally Apple StoreKit Guide (MOTO-SDFL-18605-18640).



¹⁴ Apple StoreKit Guide at 17 (MOTO-SDFL-18621).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>And as a further example, OSX devices can wirelessly purchase and download applications from the App Store:</p> <p>Install any app with ease.</p> <p>The Mac App Store revolutionizes the way applications are installed on a computer — it happens in one step. Enter the same iTunes password you use to buy music and apps on your Mac, iPad, iPhone, or iPod touch. Within seconds, your new app flies to Launchpad, ready to go. So you can spend more time enjoying new apps and less time installing them.</p> <p>15</p>

¹⁵ <http://www.apple.com/osx/apps/app-store.html> (accessed November 7, 2012) (MOTO-SDFL-20441).


'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="520 212 636 248" style="text-align: center;"><u>iTunes</u></p> <p data-bbox="428 256 1738 326">Apple devices conduct transactions in a wireless commerce system with the iTunes. For example, iOS devices can wirelessly purchase and download content from iTunes.</p> <p data-bbox="428 350 1346 386">The iPhone can wirelessly purchase and download content from iTunes:</p> <div data-bbox="743 420 1383 852" style="border: 1px solid black; padding: 5px;"> <p data-bbox="743 420 873 451" style="color: blue;">At a glance</p> <p data-bbox="743 453 1383 475">Use the iTunes Store to add music and TV shows, music, and podcasts to iPhone.</p>  </div> <p data-bbox="743 873 905 896">Use iTunes Store to:</p> <ul data-bbox="743 909 1341 992" style="list-style-type: none"> • Find music, TV shows, movies, tones, and more, by browsing or searching • See your personal Genius recommendations • Download previous purchases <p data-bbox="743 1010 1379 1032"><i>Note:</i> You need an Internet connection and an Apple ID to use the iTunes Store.</p> <p data-bbox="743 1044 1446 1092">Browse content: Tap one of the categories. Tap Genres to refine the listings. To see more information about an item, tap it.</p> <p data-bbox="743 1104 1478 1153">Search for content: Tap Search, then tap the search field and enter one or more words, then tap Search.</p> <p data-bbox="743 1164 1184 1187">Preview an item: Tap a song or video to play a sample.</p> <p data-bbox="743 1198 1495 1247">Purchase an item: Tap the item's price (or tap Free), then tap again to buy it. If you already purchased the item, "Download" appears instead of the price and you won't be charged again..</p> <p data-bbox="743 1258 1444 1281">When items are being downloaded, tap More, then tap Downloads to see their progress.</p> <p data-bbox="743 1292 1488 1357">Rent a movie: In some areas, certain movies are available to rent. You have 30 days to begin viewing a rented movie. Once you've started playing it, you can watch it as many times as you want in 24 hours. After these time limits, the movie is deleted.</p>

¹⁶ iPhone User Guide (iOS 6) at 94; (MOTO-SDFL-16226).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>The iPad can wirelessly purchase and download content from iTunes:</p> <p>About the iTunes Store Use the iTunes Store to add content to iPad. You can browse and purchase music, TV shows, audiobooks, and alert tones. You can also buy and rent movies, or download and play podcasts or iTunes U collections. You need an Apple ID in order to purchase content. See "Store settings" on page 96.</p> <p><i>Note:</i> The iTunes Store may not be available in all regions, and iTunes Store content may vary across regions. Features are subject to change.</p> <p>To access the iTunes Store, iPad must have an Internet connection. See "Network" on page 125. 17</p> <p>As a further example, Apple TV can wirelessly purchase and download content from iTunes:</p> <p>Network</p> <ul style="list-style-type: none"> • An 802.11a, b, g, or n Wi-Fi wireless network (wireless video streaming requires 802.11a, g, or n), or 10/100Base-T Ethernet network • A broadband Internet connection (DSL, cable, or LAN) • Your wireless network name and password (if you use one) <p>Software and accounts</p> <p>To play content from a Mac or PC on Apple TV, you need:</p> <ul style="list-style-type: none"> • iTunes 10.5 or later • An Apple ID to rent movies or purchase TV shows from the iTunes store, and to use Home Sharing to stream content from a Mac or PC • A Netflix account to stream content. Other accounts may be required for full access to some Internet content. 18

¹⁷ iPad User Guide (iOS 5.1) at 90 (MOTO-SDFL-19864).

¹⁸ Apple TV 3rd Gen Setup Guide at 10 (MOTO-SDFL-19669).

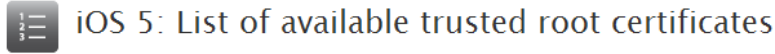
'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="598 228 1352 272">Renting movies and purchasing TV shows</p> <p data-bbox="598 282 1640 402">You can rent standard or high-definition movies and purchase TV shows directly on Apple TV (where available). Follow the onscreen instructions to find out when a rented movie expires. Purchased TV shows don't expire.</p> <p data-bbox="598 431 1598 509">When a rented movie expires, it's no longer available for playback. To watch it again, you can rent it again from iTunes. 19</p> <p data-bbox="428 566 1650 599">As a further example, OSX devices can wirelessly purchase and download content from iTunes:</p> <div data-bbox="726 634 1507 1312" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p data-bbox="739 654 1478 906">With iTunes in the Cloud, the music, apps, and books you purchase automatically appear on all your devices. Or you can download only the stuff you want — including movies and TV shows — to just the devices you want.* It's all part of iCloud and iTunes 10.7.</p> <div data-bbox="739 992 1339 1284" style="text-align: center;">  <p data-bbox="972 1040 1276 1133">iTunes 10.7 For Mac + PC</p> <p data-bbox="884 1214 1199 1252">Free Download </p> </div> <p data-bbox="1507 1279 1535 1300">20</p> </div>

¹⁹ *Id.* at 24 (MOTO-SDFL-19683).

²⁰ <http://www.apple.com/itunes/> (last accessed November 7, 2012) (MOTO-SDFL-20015).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
<p>comprising a wireless network operator certification authority having a root public key certificate</p>	<p style="text-align: center;"><u>App Store</u></p> <p>Apple is a wireless network operator and operates a certification authority (“CA”) available via a wireless network having a root public key certificate.</p> <p style="text-align: center;">2.1. Identification</p> <p>For the purposes of this CP, the term "Apple PKI" refers collectively to Apple PKI Service Providers and End Entities. Apple PKI Service Providers consist of (1) Apple Certification Authorities ("CAs"), including the Apple Root CA and Sub-CAs, and their related management teams that generate, issue, distribute, revoke and manage cryptographic keys and Certificates, (2) Apple Registration Authorities ("Apple RA"), and (3) the Apple CA Policy Authority ("Apple PA," or "PA"). End Entities consist of (1) Subscribers of Certificates and (2) Relying Parties who agree to be bound by the conditions set forth in this CP and any applicable CPS.</p> <p>For the purposes of this CP, the term "Apple CA" refers to any or all of the Apple Root CA and/or the Sub-CA's stated at CP §2.2. Details of policies and procedures that are unique to these Sub-CAs shall be documented in each Sub-CA's respective Certification Practice Statement ("CPS").</p> <p>In addition to the CAs described at CP §2.2, the Apple PKI may establish additional root certificates and subordinate certification authorities that are outside the scope of this CP. The Apple PKI may actively use and decommission these Certificates and certification authorities for the purpose of generating and using cryptographic keys, and issuing, distributing, revoking, administering, and managing digital Certificates. Actions taken by the Apple Root CA or other Apple root certificates with respect to these subordinate certification authorities, and the actions of these subordinate certification authorities themselves, will occur without public notice or consent, or inclusion in this or any other publicly available policy.</p> <p style="text-align: right;">21</p>

²¹ Apple Certificate Policy, Version 1.3 (February 28, 2012) at 9 (MOTO-SDFL-17988).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="716 212 947 240">Secure Boot Chain</p> <p data-bbox="716 261 1497 342">Each step of the boot-up process contains components that are cryptographically signed by Apple to ensure integrity, and proceeds only after verifying the chain of trust. This includes the bootloaders, kernel, kernel extensions, and baseband firmware.</p> <p data-bbox="716 363 1497 558">When an iOS device is turned on, its application processor immediately executes code from read-only memory known as the Boot ROM. This immutable code is laid down during chip fabrication, and is implicitly trusted. The Boot ROM code contains the Apple Root CA public key, which is used to verify that the Low-Level Bootloader (LLB) is signed by Apple before allowing it to load. This is the first step in the chain of trust where each step ensures that the next is signed by Apple. When the LLB finishes its tasks, it verifies and runs the next-stage bootloader, iBoot, which in turn verifies and runs the iOS kernel.</p> <p data-bbox="716 579 1472 631">This secure boot chain ensures that the lowest levels of software are not tampered with, and allows iOS to run only on validated Apple devices.</p> <p data-bbox="716 652 1497 821">If one step of this boot process is unable to load or verify the next, boot-up is stopped and the device displays the "Connect to iTunes" screen. This is called recovery mode. If the Boot ROM is not even able to load or verify LLB, it enters DFU (Device Firmware Upgrade) mode. In both cases, the device must be connected to iTunes via USB and restored to factory default settings. For more information on manually entering recovery mode, see http://support.apple.com/kb/HT1808. 22</p> <p data-bbox="422 873 1801 938">By way of example, Apple pre-installs various root certificates in iOS 5.x, and on information and belief, in iOS 6.x.</p> <div data-bbox="667 987 1436 1187" style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;">  <p data-bbox="667 1068 751 1089">Summary</p> <p data-bbox="667 1097 1079 1187">These trusted root certificates are preinstalled with iOS 5. When IT administrators create Configuration Profiles for iPhone, iPad, or iPod touch using the iPhone Configuration Utility, these certificates do not need to be included.</p> <p data-bbox="1104 1068 1255 1089">Products Affected</p> <p data-bbox="1104 1097 1272 1118">iPad, iPhone, iPod touch 23</p> </div>

²² iOS Security (May 12, 2012) at 4 (MOTO-SDFL-19817).

²³ <http://support.apple.com/kb/HT5012> (MOTO-SDFL-20032-20084). The Apple security hierarchy is described at http://images.apple.com/certificateauthority/pdf/Apple_WWDR_CPS_v1.7.pdf (MOTO-SDFL-19696-19721).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>These include certificates for the "Apple Root Certificate Authority":</p> <div data-bbox="674 277 1560 797" style="border: 1px solid gray; padding: 5px;"> <pre> Certificate: Data: Version: 3 (0x2) Serial Number: 2 (0x2) Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, O=Apple Inc., OU=Apple Certification Authority, CN=Apple Root CA Validity Not Before: Apr 25 21:40:36 2006 GMT Not After : Feb 9 21:40:36 2035 GMT Subject: C=US, O=Apple Inc., OU=Apple Certification Authority, CN=Apple Root CA </pre> <hr/> <pre> Certificate: Data: Version: 3 (0x2) Serial Number: 1 (0x1) Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, O=Apple Computer, Inc., OU=Apple Computer Certificate Authority, CN=Apple Root Certi Validity Not Before: Feb 10 00:18:14 2005 GMT Not After : Feb 10 00:18:14 2025 GMT Subject: C=US, O=Apple Computer, Inc., OU=Apple Computer Certificate Authority, CN=Apple Root Cert </pre> </div>


24

²⁴ <http://support.apple.com/kb/HT5012> (MOTO-SDFL-20032-20084).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>Consistent with the establishment of a certification authority, Apple may revoke certificates.</p> <p style="text-align: center;">APPLE-SA-2011-10-12-2 Apple TV Software Update 4.4</p> <hr/> <p>Subject: APPLE-SA-2011-10-12-2 Apple TV Software Update 4.4 From: Apple Product Security <email@hidden> Date: Wed, 12 Oct 2011 11:33:53 -0700 Delivered-to: email@hidden Delivered-to: email@hidden</p> <hr/> <p>-----BEGIN PGP SIGNED MESSAGE----- Hash: SHA1</p> <p>APPLE-SA-2011-10-12-2 Apple TV Software Update 4.4</p> <p>Apple TV Software Update 4.4 is now available and addresses the following:</p> <p>Apple TV Available for: Apple TV 4.0 through 4.3 Impact: An attacker with a privileged network position may intercept user credentials or other sensitive information Description: Fraudulent certificates were issued by multiple certificate authorities operated by DigiNotar. This issue is addressed by removing DigiNotar from the list of trusted root certificates, from the list of Extended Validation (EV) certificate authorities, and by configuring default system trust settings so that DigiNotar's certificates, including those issued by other authorities, are not trusted.</p> <p>Apple TV Available for: Apple TV 4.0 through 4.3 Impact: Support for X.509 certificates with MD5 hashes may expose users to spoofing and information disclosure as attacks improve Description: Certificates signed using the MD5 hash algorithm were accepted by iOS. This algorithm has known cryptographic weaknesses. Further research or a misconfigured certificate authority could have allowed the creation of X.509 certificates with attacker controlled values that would have been trusted by the system. This would have exposed X.509 based protocols to spoofing, man in the middle attacks, and information disclosure. This update disables support for an X.509 certificate with an MD5 hash for any use other than as a trusted root certificate. CVE-ID CVE-2011-3427</p>

25

²⁵ *Id.*

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>The Apple Root Certification Authority, being the domain's root certification authority, is the owner of the root certificate.</p> <div data-bbox="861 316 1375 357" style="text-align: center;"> <h3>Apple Root Certification Authority</h3> </div> <div data-bbox="861 381 1155 414" style="text-align: center;"> <h4>Apple Root Certificates</h4> </div> <div data-bbox="861 430 1365 722">  <p>Apple Inc. Root Certificate Root certificate authority Expires: Friday, February 9, 2035 1:40:36PM US/Pacific ✔ This certificate is valid Download certificate ▶ Download CRL ▶</p> <p>Apple Computer, Inc. Root Certificate Root certificate authority Expires: Sunday, February 9, 2025 4:18:14PM US/Pacific ✔ This certificate is valid Download certificate ▶ Download CRL ▶</p> </div> <div data-bbox="808 771 1092 803" style="text-align: center;"> <h4>Certificates, Keys, and Identities</h4> </div> <div data-bbox="861 820 1396 1088"> <p>A digital certificate is a collection of data used to verify the identity of the holder or sender of the certificate. For example, a certificate contains such information as:</p> <ul style="list-style-type: none"> ■ Certificate issuer ■ Certificate holder ■ Validity period (the certificate is not valid before or after this period) ■ Public key of the owner of the certificate ■ Certificate extensions, which contain additional information such as allowable uses for the private key associated with the certificate ■ Digital signature from the certification authority to ensure that the certificate has not been altered and to indicate the identity of the issuer <p>Each certificate is verified through the use of another certificate, creating a chain of certificates that ends with the root certificate. The issuer of a certificate is called a certification authority (CA). The owner of the root certificate is the root certification authority. See <i>Security Overview</i> for more details about the structure and contents of a certificate.</p> </div> <div data-bbox="1396 1047 1438 1079" style="text-align: right;"> <p>26</p> </div> <div data-bbox="504 1128 640 1185" style="text-align: center;"> <h2><u>iTunes</u></h2> </div> <p>Apple is a wireless network operator and operates a certification authority (“CA”) available via a wireless network having a root public key certificate.</p>

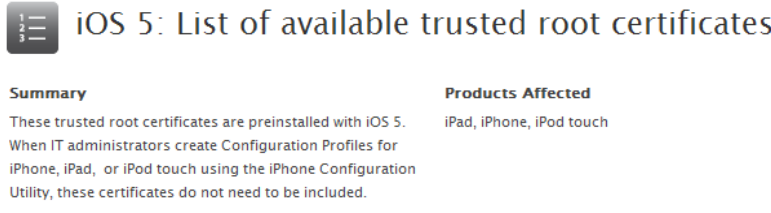
²⁶ Apple Certificate Policy v.1.3 (MOTO-SDFL-17980-18006).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="590 212 884 245">2.1. Identification</p> <p data-bbox="590 266 1635 456">For the purposes of this CP, the term "Apple PKI" refers collectively to Apple PKI Service Providers and End Entities. Apple PKI Service Providers consist of (1) Apple Certification Authorities ("CAs"), including the Apple Root CA and Sub-CAs, and their related management teams that generate, issue, distribute, revoke and manage cryptographic keys and Certificates, (2) Apple Registration Authorities ("Apple RA"), and (3) the Apple CA Policy Authority ("Apple PA," or "PA"). End Entities consist of (1) Subscribers of Certificates and (2) Relying Parties who agree to be bound by the conditions set forth in this CP and any applicable CPS.</p> <p data-bbox="590 472 1635 553">For the purposes of this CP, the term "Apple CA" refers to any or all of the Apple Root CA and/or the Sub-CA's stated at CP §2.2. Details of policies and procedures that are unique to these Sub-CAs shall be documented in each Sub-CA's respective Certification Practice Statement ("CPS").</p> <p data-bbox="590 570 1635 781">In addition to the CAs described at CP §2.2, the Apple PKI may establish additional root certificates and subordinate certification authorities that are outside the scope of this CP. The Apple PKI may actively use and decommission these Certificates and certification authorities for the purpose of generating and using cryptographic keys, and issuing, distributing, revoking, administering, and managing digital Certificates. Actions taken by the Apple Root CA or other Apple root certificates with respect to these subordinate certification authorities, and the actions of these subordinate certification authorities themselves, will occur without public notice or consent, or inclusion in this or any other publicly available policy.</p> <p data-bbox="1646 753 1671 773">27</p>

²⁷ Apple Certificate Policy Version 1.3 at 9 (MOTO-SDFL-17988).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p style="text-align: center;">Certificates, Keys, and Identities</p> <p>A digital certificate is a collection of data used to verify the identity of the holder or sender of the certificate. For example, a certificate contains such information as:</p> <ul style="list-style-type: none"> ■ Certificate issuer ■ Certificate holder ■ Validity period (the certificate is not valid before or after this period) ■ Public key of the owner of the certificate ■ Certificate extensions, which contain additional information such as allowable uses for the private key associated with the certificate ■ Digital signature from the certification authority to ensure that the certificate has not been altered and to indicate the identity of the issuer <p>Each certificate is verified through the use of another certificate, creating a chain of certificates that ends with the root certificate. The issuer of a certificate is called a certification authority (CA). The owner of the root certificate is the root certification authority. See <i>Security Overview</i> for more details about the structure and contents of a certificate.</p> <p>Every public key is half of a public-private key pair. As implied by the names, the public key can be obtained by anyone, but the private key is kept secret by the owner of the key. Data encrypted with the private key can be decrypted only with the public key, and vice versa. In order to both encrypt and decrypt data, therefore, a given user must have both a public key (normally embedded in a certificate) and a private key. The combination of a certificate and its associated private key is known as an identity. Certificate, Key, and Trust Services includes functions to find the certificate or key associated with an identity and to find an identity when given search criteria. The search criteria include the permitted uses for the key.</p> <p>In Mac OS X and iOS, keys and certificates are stored on a keychain, a database that provides secure (that is, encrypted) storage for private keys and other secrets as well as unencrypted storage for other security-related data. The Certificate, Key, and Trust Services functions that search for keys, certificates, and identities all use the keychain for this purpose. On a Mac OS X system, you can use the Keychain Access utility to see the contents of the keychain and to examine the contents of certificates.</p> <p style="text-align: right;">28</p>

²⁸ Certificate, Key, and Trust Services Programming Guide at 6-7 (MOTO-SDFL-19729-19730).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p style="text-align: center;">Secure Boot Chain</p> <p>Each step of the boot-up process contains components that are cryptographically signed by Apple to ensure integrity, and proceeds only after verifying the chain of trust. This includes the bootloaders, kernel, kernel extensions, and baseband firmware.</p> <p>When an iOS device is turned on, its application processor immediately executes code from read-only memory known as the Boot ROM. This immutable code is laid down during chip fabrication, and is implicitly trusted. The Boot ROM code contains the Apple Root CA public key, which is used to verify that the Low-Level Bootloader (LLB) is signed by Apple before allowing it to load. This is the first step in the chain of trust where each step ensures that the next is signed by Apple. When the LLB finishes its tasks, it verifies and runs the next-stage bootloader, iBoot, which in turn verifies and runs the iOS kernel.</p> <p>This secure boot chain ensures that the lowest levels of software are not tampered with, and allows iOS to run only on validated Apple devices.</p> <p>If one step of this boot process is unable to load or verify the next, boot-up is stopped and the device displays the "Connect to iTunes" screen. This is called recovery mode. If the Boot ROM is not even able to load or verify LLB, it enters DFU (Device Firmware Upgrade) mode. In both cases, the device must be connected to iTunes via USB and restored to factory default settings. For more information on manually entering recovery mode, see http://support.apple.com/kb/HT1808.²⁹</p> <p>By way of example, Apple pre-installs various root certificates in iOS 5.x.</p> <div style="text-align: center;">  <p>Summary These trusted root certificates are preinstalled with iOS 5. When IT administrators create Configuration Profiles for iPhone, iPad, or iPod touch using the iPhone Configuration Utility, these certificates do not need to be included.</p> <p>Products Affected iPad, iPhone, iPod touch</p> </div> <p style="text-align: right;">³⁰</p>

²⁹ iOS Security (May 12, 2012) at 4 (MOTO-SDFL-19817).

³⁰ <http://support.apple.com/kb/HT5012> (MOTO-SDFL-20032-20084). The Apple security hierarchy is described at http://images.apple.com/certificateauthority/pdf/Apple_WWDR_CPS_v1.7.pdf (MOTO-SDFL-19696-19721).



'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>These include certificates for the "Apple Root Certificate Authority":</p> <div data-bbox="674 277 1560 797" style="border: 1px solid gray; padding: 10px;"> <pre> Certificate: Data: Version: 3 (0x2) Serial Number: 2 (0x2) Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, O=Apple Inc., OU=Apple Certification Authority, CN=Apple Root CA Validity Not Before: Apr 25 21:40:36 2006 GMT Not After : Feb 9 21:40:36 2035 GMT Subject: C=US, O=Apple Inc., OU=Apple Certification Authority, CN=Apple Root CA Certificate: Data: Version: 3 (0x2) Serial Number: 1 (0x1) Signature Algorithm: sha1WithRSAEncryption Issuer: C=US, O=Apple Computer, Inc., OU=Apple Computer Certificate Authority, CN=Apple Root Certi Validity Not Before: Feb 10 00:18:14 2005 GMT Not After : Feb 10 00:18:14 2025 GMT Subject: C=US, O=Apple Computer, Inc., OU=Apple Computer Certificate Authority, CN=Apple Root Cert </pre> </div>

31

³¹ *Id.*

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>Consistent with the establishment of a certification authority, Apple may revoke certificates.</p> <p style="text-align: center;">APPLE-SA-2011-10-12-2 Apple TV Software Update 4.4</p> <hr/> <p>Subject: APPLE-SA-2011-10-12-2 Apple TV Software Update 4.4 From: Apple Product Security <email@hidden> Date: Wed, 12 Oct 2011 11:33:53 -0700 Delivered-to: email@hidden Delivered-to: email@hidden</p> <hr/> <p>-----BEGIN PGP SIGNED MESSAGE----- Hash: SHA1</p> <p>APPLE-SA-2011-10-12-2 Apple TV Software Update 4.4</p> <p>Apple TV Software Update 4.4 is now available and addresses the following:</p> <p>Apple TV Available for: Apple TV 4.0 through 4.3 Impact: An attacker with a privileged network position may intercept user credentials or other sensitive information Description: Fraudulent certificates were issued by multiple certificate authorities operated by DigiNotar. This issue is addressed by removing DigiNotar from the list of trusted root certificates, from the list of Extended Validation (EV) certificate authorities, and by configuring default system trust settings so that DigiNotar's certificates, including those issued by other authorities, are not trusted.</p> <p>Apple TV Available for: Apple TV 4.0 through 4.3 Impact: Support for X.509 certificates with MD5 hashes may expose users to spoofing and information disclosure as attacks improve Description: Certificates signed using the MD5 hash algorithm were accepted by iOS. This algorithm has known cryptographic weaknesses. Further research or a misconfigured certificate authority could have allowed the creation of X.509 certificates with attacker controlled values that would have been trusted by the system. This would have exposed X.509 based protocols to spoofing, man in the middle attacks, and information disclosure. This update disables support for an X.509 certificate with an MD5 hash for any use other than as a trusted root certificate. CVE-ID CVE-2011-3427</p> <p style="text-align: right;">32</p>

³² <http://lists.apple.com/archives/security-announce/2011/Oct/msg00002.html> (accessed November 7, 2012) (MOTO-SDFL-19606-19609).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>The Apple Root Certification Authority, being the domain's root certification authority, is the owner of the root certificate.³³</p> <div style="text-align: center;"> <h2>Apple Root Certification Authority</h2> <h3>Apple Root Certificates</h3> <div style="display: flex; justify-content: space-around;"> <div style="text-align: left;">  <p>Apple Inc. Root Certificate Root certificate authority Expires: Friday, February 9, 2035 1:40:36PM US/Pacific ✔ This certificate is valid Download certificate ▶ Download CRL ▶</p> </div> <div style="text-align: left;">  <p>Apple Computer, Inc. Root Certificate Root certificate authority Expires: Sunday, February 9, 2025 4:18:14PM US/Pacific ✔ This certificate is valid Download certificate ▶ Download CRL ▶</p> </div> </div> <h4>Certificates, Keys, and Identities</h4> <p>A digital certificate is a collection of data used to verify the identity of the holder or sender of the certificate. For example, a certificate contains such information as:</p> <ul style="list-style-type: none"> ■ Certificate issuer ■ Certificate holder ■ Validity period (the certificate is not valid before or after this period) ■ Public key of the owner of the certificate ■ Certificate extensions, which contain additional information such as allowable uses for the private key associated with the certificate ■ Digital signature from the certification authority to ensure that the certificate has not been altered and to indicate the identity of the issuer <p>Each certificate is verified through the use of another certificate, creating a chain of certificates that ends with the root certificate. The issuer of a certificate is called a certification authority (CA). The owner of the root certificate is the root certification authority. See <i>Security Overview</i> for more details about the structure and contents of a certificate.</p> </div>

³³ <http://www.apple.com/certificateauthority/>; Apple Certificate Policy v. 1.3 (MOTO-SDFL-17980-18006).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
<p>and at least one attribute authority having a digital certificate that is dependent from the root public key certificate,</p>	<p style="text-align: center;"><u>App Store</u></p> <p>See above. On information and belief, the App Store operates as an attribute authority that has a digital certificate that is dependent from the root public key certificate.</p> <p>As described below, Apple issues attribute certificates from the App Store that are dependent from the root public key certificate. Attributes distributed may provide fine-grained, role-based information and enable the use of privileges or attributes. For example, on information and belief, some applications downloaded from the App Store have attribute certificates that allow the application to store information on iCloud. As another example, some applications downloaded from the App Store have attribute certificates that allow the application to send push notifications. Apple refers to these attributes as "entitlements," and they are set by the developer during development of the software. As a further example, in-app purchases may enable more functionality or add features to existing applications, among other things. All Apple software developers are issued certificates by Apple that enable the developer to create and issue applications with these properties. Ultimately, such a certificate would be dependent on a root certificate owned by Apple.</p>

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>Entitlements confer specific capabilities or security permissions to your app.</p> <p>At a Glance</p> <p>Set entitlement values in order to enable iCloud, push notifications, and App Sandbox (only for OS X). Each entitlement has a default value, which in most cases disables the capability associated with the entitlement. When you set an entitlement, you are overriding the default by providing an appropriate key-value pair.</p> <ul style="list-style-type: none"> • iCloud entitlements let you enable the use of iCloud data storage for your iOS or OS X app. You set iCloud entitlement values on a target-by-target basis in your Xcode project. • Push notifications let your app alert the user even when your iOS or OS X app is not in the foreground. You set push notification entitlement values as part of configuring your development and distribution provisioning profiles. • App Sandbox entitlements let you enable the security feature called <i>sandboxing</i> for your OS X app. By carefully enabling only the resource access that you need, you minimize the potential for damage if malicious code successfully exploits your app. You set App Sandbox entitlement values on a target-by-target basis in your Xcode project. <p>You can set many entitlements using the Summary tab of the Xcode target editor. For other entitlements, you must employ a property list file.</p> <p>The sort of value to associate with an entitlement key depends on the key. Many entitlement keys take Boolean values. For entitlements defined in a property list in an Xcode project, a Boolean entitlement value is either <code><true/></code> or <code><false/></code>. Some entitlement keys take a string or an array of strings as a value. Refer to the chapters in this document for specifics on the values to apply to the various entitlement keys.</p> <p>To use any entitlement keys, you must code sign your app because an app's entitlements are built in to its code signature. 34</p> <p>In your OS X Xcode project, configure fine-grained security permissions by enabling settings in the Summary tab of the target editor. These settings, in turn, add Boolean values to entitlement keys in the target's <code>.entitlements</code> property list file. The values are then incorporated into the target's code signature when you build the project. 35</p>

³⁴ Entitlement Key Reference (September 19, 2012) at 5 (MOTO-SDFL-19773).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="690 207 1020 240">Runtime Process Security</p> <p data-bbox="690 256 1535 315">Once an app is verified to be from an approved source, iOS enforces security measures to ensure that it can't compromise other apps or the rest of the system.</p> <p data-bbox="690 334 1535 516">All third-party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device. This prevents apps from gathering or modifying information stored by other apps. Each app has a unique home directory for its files, which is randomly assigned when the app is installed. If a third-party app needs to access information other than its own, it does so only by using application programming interfaces (APIs) and services provided by iOS.</p> <p data-bbox="690 535 1520 688">System files and resources are also shielded from the user's apps. The majority of iOS runs as the non-privileged user "mobile," as do all third-party apps. The entire OS partition is mounted read-only. Unnecessary tools, such as remote login services, aren't included in the system software, and APIs do not allow apps to escalate their own privileges to modify other apps or iOS itself.</p> <p data-bbox="690 708 1528 925">Access by third-party apps to user information and features such as iCloud is controlled using declared entitlements. Entitlements are key/value pairs that are signed in to an app and allow authentication beyond runtime factors like unix user ID. Since entitlements are digitally signed, they cannot be changed. Entitlements are used extensively by system apps and daemons to perform specific privileged operations that would otherwise require the process to run as root. This greatly reduces the potential for privilege escalation by a compromised system application or daemon.</p>

36

³⁵ Entitlement Key Reference (September 19, 2012) at 11 (MOTO-SDFL-19779).

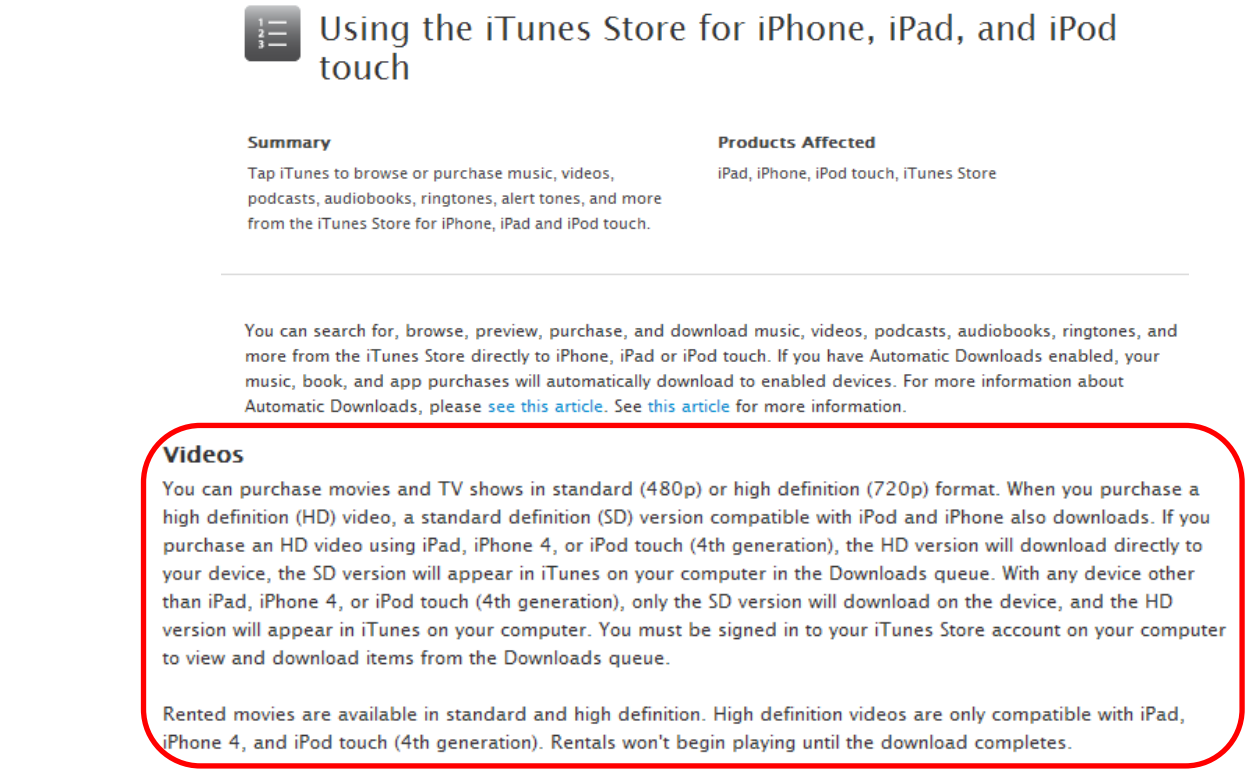
³⁶ iOS Security (May 12, 2012) at 6 (MOTO-SDFL-19819).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes																						
	<p>Examples of entitlements are shown below:</p> <table border="1" data-bbox="695 253 1535 1312"> <thead> <tr> <th data-bbox="695 253 1199 298">Entitlement key</th> <th data-bbox="1199 253 1535 298">Capability</th> </tr> </thead> <tbody> <tr> <td data-bbox="695 298 1199 386">com.apple.security.app-sandbox</td> <td data-bbox="1199 298 1535 386">Enables App Sandbox for a target in an Xcode project</td> </tr> <tr> <td data-bbox="695 386 1199 639">com.apple.security.application-groups</td> <td data-bbox="1199 386 1535 639">Allows access to group containers that are shared among multiple apps produced by a single development team, and allows certain additional interprocess communication between the apps. The format for this attribute is described in "Adding an App to an App Group" (page 18).</td> </tr> <tr> <td data-bbox="695 639 1199 727">com.apple.security.assets.movies.read-only</td> <td data-bbox="1199 639 1535 727">Read-only access to the user's Movies folder and iTunes movies</td> </tr> <tr> <td data-bbox="695 727 1199 815">com.apple.security.assets.movies.read-write</td> <td data-bbox="1199 727 1535 815">Read/write access to the user's Movies folder and iTunes movies</td> </tr> <tr> <td data-bbox="695 815 1199 902">com.apple.security.assets.music.read-only</td> <td data-bbox="1199 815 1535 902">Read-only access to the user's Music folder</td> </tr> <tr> <td data-bbox="695 902 1199 990">com.apple.security.assets.music.read-write</td> <td data-bbox="1199 902 1535 990">Read/write access to the user's Music folder</td> </tr> <tr> <td data-bbox="695 990 1199 1078">com.apple.security.assets.pictures.read-only</td> <td data-bbox="1199 990 1535 1078">Read-only access to the user's Pictures folder</td> </tr> <tr> <td data-bbox="695 1078 1199 1166">com.apple.security.assets.pictures.read-write</td> <td data-bbox="1199 1078 1535 1166">Read/write access to the user's Pictures folder</td> </tr> <tr> <td data-bbox="695 1166 1199 1224">com.apple.security.device.bluetooth</td> <td data-bbox="1199 1166 1535 1224">Interaction with Bluetooth devices</td> </tr> <tr> <td data-bbox="695 1224 1199 1312">com.apple.security.device.camera</td> <td data-bbox="1199 1224 1535 1312">Capture of movies and still images using the built-in camera, if available</td> </tr> </tbody> </table>	Entitlement key	Capability	com.apple.security.app-sandbox	Enables App Sandbox for a target in an Xcode project	com.apple.security.application-groups	Allows access to group containers that are shared among multiple apps produced by a single development team, and allows certain additional interprocess communication between the apps. The format for this attribute is described in "Adding an App to an App Group" (page 18).	com.apple.security.assets.movies.read-only	Read-only access to the user's Movies folder and iTunes movies	com.apple.security.assets.movies.read-write	Read/write access to the user's Movies folder and iTunes movies	com.apple.security.assets.music.read-only	Read-only access to the user's Music folder	com.apple.security.assets.music.read-write	Read/write access to the user's Music folder	com.apple.security.assets.pictures.read-only	Read-only access to the user's Pictures folder	com.apple.security.assets.pictures.read-write	Read/write access to the user's Pictures folder	com.apple.security.device.bluetooth	Interaction with Bluetooth devices	com.apple.security.device.camera	Capture of movies and still images using the built-in camera, if available
Entitlement key	Capability																						
com.apple.security.app-sandbox	Enables App Sandbox for a target in an Xcode project																						
com.apple.security.application-groups	Allows access to group containers that are shared among multiple apps produced by a single development team, and allows certain additional interprocess communication between the apps. The format for this attribute is described in "Adding an App to an App Group" (page 18).																						
com.apple.security.assets.movies.read-only	Read-only access to the user's Movies folder and iTunes movies																						
com.apple.security.assets.movies.read-write	Read/write access to the user's Movies folder and iTunes movies																						
com.apple.security.assets.music.read-only	Read-only access to the user's Music folder																						
com.apple.security.assets.music.read-write	Read/write access to the user's Music folder																						
com.apple.security.assets.pictures.read-only	Read-only access to the user's Pictures folder																						
com.apple.security.assets.pictures.read-write	Read/write access to the user's Pictures folder																						
com.apple.security.device.bluetooth	Interaction with Bluetooth devices																						
com.apple.security.device.camera	Capture of movies and still images using the built-in camera, if available																						

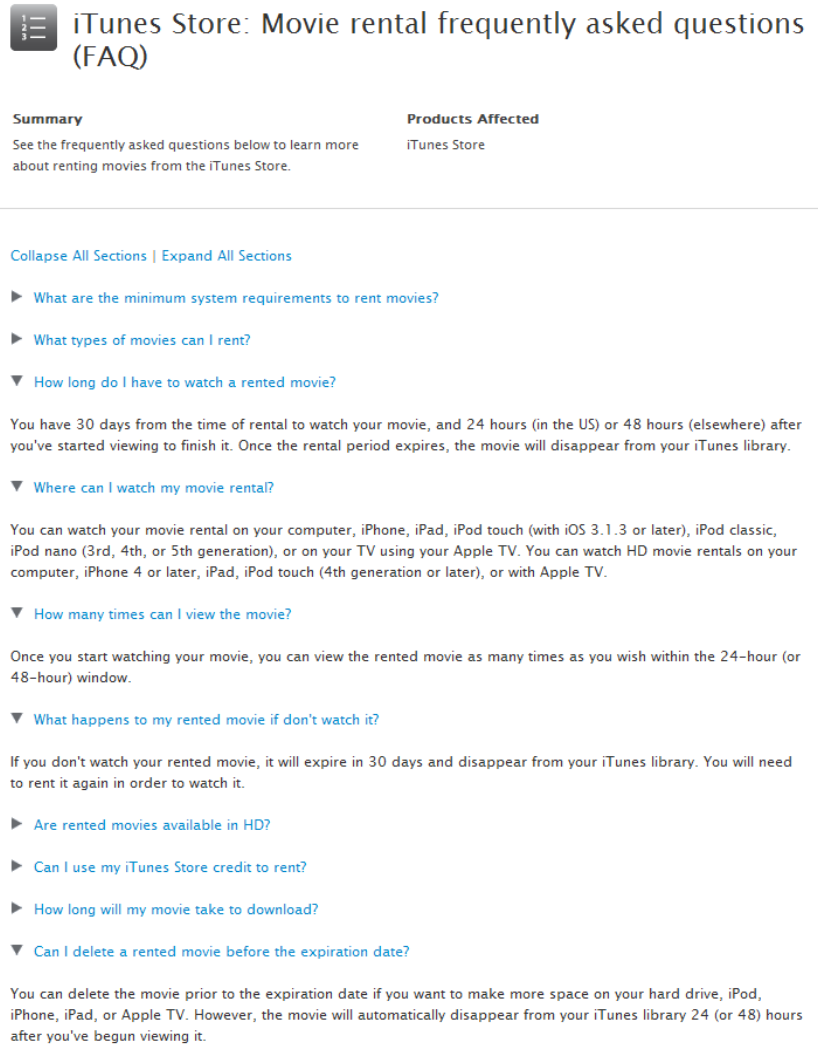
37

³⁷ Entitlement Key Reference (September 19, 2012) at 12 (MOTO-SDFL-19780).

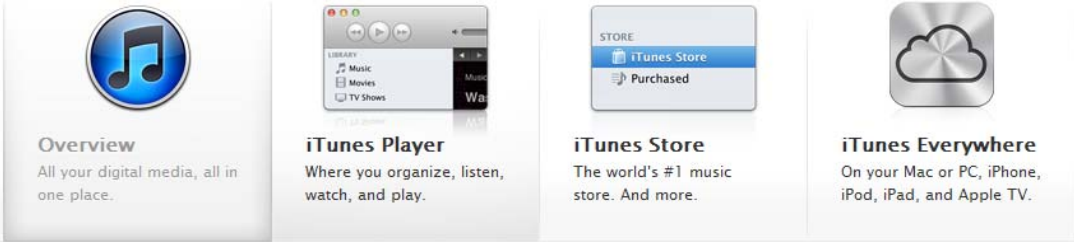
'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="520 212 638 250"><u>iTunes</u></p> <p data-bbox="424 293 1829 358">iTunes operates as an attribute authority that has a digital certificate that is dependent from the root public key certificate.</p> <p data-bbox="424 402 1829 618">Apple issues attribute certificates from iTunes. Attribute certificates enable devices to use certain software for a distinct period of time. For example, when a movie or television show is rented from iTunes, a user has a certain period of time (e.g., 30 days) to use that video, and once the user begins watching, the user has a certain period of time to watch the video (e.g., 24 hours). The user's device is given an attribute certificate that enables the user to access the video within those time periods. Ultimately, such a certificate would be dependent on a root certificate owned by Apple.</p>

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>By way of example, on iOS devices:</p>  <p>Using the iTunes Store for iPhone, iPad, and iPod touch</p> <p>Summary Tap iTunes to browse or purchase music, videos, podcasts, audiobooks, ringtones, alert tones, and more from the iTunes Store for iPhone, iPad and iPod touch.</p> <p>Products Affected iPad, iPhone, iPod touch, iTunes Store</p> <p>You can search for, browse, preview, purchase, and download music, videos, podcasts, audiobooks, ringtones, and more from the iTunes Store directly to iPhone, iPad or iPod touch. If you have Automatic Downloads enabled, your music, book, and app purchases will automatically download to enabled devices. For more information about Automatic Downloads, please see this article. See this article for more information.</p> <p>Videos You can purchase movies and TV shows in standard (480p) or high definition (720p) format. When you purchase a high definition (HD) video, a standard definition (SD) version compatible with iPod and iPhone also downloads. If you purchase an HD video using iPad, iPhone 4, or iPod touch (4th generation), the HD version will download directly to your device, the SD version will appear in iTunes on your computer in the Downloads queue. With any device other than iPad, iPhone 4, or iPod touch (4th generation), only the SD version will download on the device, and the HD version will appear in iTunes on your computer. You must be signed in to your iTunes Store account on your computer to view and download items from the Downloads queue.</p> <p>Rented movies are available in standard and high definition. High definition videos are only compatible with iPad, iPhone 4, and iPod touch (4th generation). Rentals won't begin playing until the download completes.</p> <p>TV shows, movies, and movie rentals are not available in some iTunes Store countries.</p>

³⁸ <http://support.apple.com/kb/HT1491> (MOTO-SDFL-20018-20023).


'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>By further example, other devices including OSX devices and Apple TV:</p>  <p>Summary See the frequently asked questions below to learn more about renting movies from the iTunes Store.</p> <p>Products Affected iTunes Store</p> <p>Collapse All Sections Expand All Sections</p> <ul style="list-style-type: none"> ▶ What are the minimum system requirements to rent movies? ▶ What types of movies can I rent? ▼ How long do I have to watch a rented movie? <p>You have 30 days from the time of rental to watch your movie, and 24 hours (in the US) or 48 hours (elsewhere) after you've started viewing to finish it. Once the rental period expires, the movie will disappear from your iTunes library.</p> <ul style="list-style-type: none"> ▼ Where can I watch my movie rental? <p>You can watch your movie rental on your computer, iPhone, iPad, iPod touch (with iOS 3.1.3 or later), iPod classic, iPod nano (3rd, 4th, or 5th generation), or on your TV using your Apple TV. You can watch HD movie rentals on your computer, iPhone 4 or later, iPad, iPod touch (4th generation or later), or with Apple TV.</p> <ul style="list-style-type: none"> ▼ How many times can I view the movie? <p>Once you start watching your movie, you can view the rented movie as many times as you wish within the 24-hour (or 48-hour) window.</p> <ul style="list-style-type: none"> ▼ What happens to my rented movie if don't watch it? <p>If you don't watch your rented movie, it will expire in 30 days and disappear from your iTunes library. You will need to rent it again in order to watch it.</p> <ul style="list-style-type: none"> ▶ Are rented movies available in HD? ▶ Can I use my iTunes Store credit to rent? ▶ How long will my movie take to download? ▼ Can I delete a rented movie before the expiration date? <p>You can delete the movie prior to the expiration date if you want to make more space on your hard drive, iPod, iPhone, iPad, or Apple TV. However, the movie will automatically disappear from your iTunes library 24 (or 48) hours after you've begun viewing it.</p>

³⁹ <http://support.apple.com/kb/HT1657> (MOTO-SDFL-20024-20027).


'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="611 224 1050 246">▼ Can I play my rental on more than one device?</p> <ul data-bbox="625 280 1640 500" style="list-style-type: none"> <li data-bbox="625 280 1640 435">▪ If you download a rented movie on your computer: You can transfer it to a device such as your Apple TV (1st generation), iPhone, iPad, or iPod if it's a standard-definition film (movies in HD can only be watched on your computer, iPad, iPhone 4 or later, iPod touch (4th generation or later), or Apple TV). Once you move the movie from your computer to a device, the movie will disappear from your computer's iTunes library. You can move the movie between devices as many times as you wish during the rental period, but the movie can only exist on one device at a time. <li data-bbox="625 451 1640 500">▪ If you download a rented movie on your iPhone 4 or later, iPad, iPod touch (4th generation or later), or Apple TV: It is not transferable to any other device or computer. <p data-bbox="1654 477 1680 500">40</p> <hr data-bbox="495 516 1738 519"/> <div data-bbox="495 573 1738 878"> <h3 data-bbox="989 573 1247 613">What is iTunes?</h3>  <p data-bbox="617 769 716 792">Overview All your digital media, all in one place.</p> <p data-bbox="884 769 1024 792">iTunes Player Where you organize, listen, watch, and play.</p> <p data-bbox="1150 769 1283 792">iTunes Store The world's #1 music store. And more.</p> <p data-bbox="1415 769 1612 792">iTunes Everywhere On your Mac or PC, iPhone, iPod, iPad, and Apple TV.</p> </div> <p data-bbox="695 948 1541 1045">Play, buy, and enjoy your music, movies, TV shows, apps, and more. Everywhere.</p> <p data-bbox="678 1060 1556 1157">iTunes is a free application for your Mac or PC. It lets you organize and play digital music and video on your computer. It can automatically download new music, app, and book purchases across all your devices and computers. And it's a store that has everything you need to be entertained. Anywhere. Anytime.</p> <p data-bbox="1738 1159 1764 1182">41</p>

⁴⁰ <http://support.apple.com/kb/HT1657> (accessed November 7, 2012) (MOTO-SDFL-20024-20027).

⁴¹ www.apple.com/itunes/what-is (accessed November 7, 2012) (MOTO-SDFL-20001-20007).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
<p>where the attribute authority is accessible by a wireless client device via a wireless network, the method comprising:</p>	<p style="text-align: center;"><u>App Store</u></p> <p>As discussed above, the App Store servers are accessible by a wireless client device via a wireless network.</p> <p>By way of example, the App Store servers are accessible by the iPhone via a wireless network.</p> <p style="color: blue; text-align: center;">At a glance</p> <p style="text-align: center;">Use the App Store to browse, purchase, and download apps to iPhone.</p> <div style="text-align: center;">  </div> <p>Use the App Store to:</p> <ul style="list-style-type: none"> • Find new free or purchased apps by browsing or searching • Download previous purchases and updates • Redeem a gift card or download code • Recommend an app to a friend • Manage your App Store account <p style="border: 1px solid red; padding: 2px;">Note: You need an Internet connection and an Apple ID to use the App Store.</p> <p>Purchase an app: Tap the app's price (or tap Free), then tap Buy Now. If you already purchased the app, "install" appears instead of the price. You won't be charged to download it again. While an app is being downloaded, its icon appears on the Home screen with a progress indicator.</p>


⁴² iPhone User Guide (iOS 6) at 96 (MOTO-SDFL-16228).

<p>'534 Patent Claim</p>	<p>Exemplary Apple Product: iOS and OSX devices¹⁰/Apple App Store and iTunes</p>
	<p>By way of example, the App Store servers are accessible by the iPad via a wireless network.</p> <p>About the App Store You can search for, browse, review, purchase, and download apps from the App Store directly to iPad.</p> <p><i>Note:</i> The App Store may not be available in all countries or regions, and App Store content may vary by country or region. Features are subject to change.</p> <p style="border: 2px solid red; padding: 5px;">To browse the App Store, iPad must be connected to the Internet. See "Network" on page 125. To purchase apps, you need an Apple ID. See "Store settings" on page 96.</p>  <p style="text-align: right;">Check for app updates.</p>

⁴³ iPad User Guide (iOS 5.1) at 94 (MOTO-SDFL-19948).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>And as a further example, the App Store servers are accessible by the OSX devices via a wireless network.</p> <p>Install any app with ease.</p> <p>The Mac App Store revolutionizes the way applications are installed on a computer — it happens in one step. Enter the same iTunes password you use to buy music and apps on your Mac, iPad, iPhone, or iPod touch. Within seconds, your new app flies to Launchpad, ready to go. So you can spend more time enjoying new apps and less time installing them.</p> <p>44</p>

⁴⁴ <http://www.apple.com/osx/apps/app-store.html> (accessed November 7, 2012) (MOTO-SDFL-20439-20445).

<p>'534 Patent Claim</p>	<p>Exemplary Apple Product: iOS and OSX devices¹⁰/Apple App Store and iTunes</p>
	<p style="text-align: center;"><u>iTunes</u></p> <p>As discussed above, iTunes is accessible by a wireless client device via a wireless network.</p> <p>The iPhone can wirelessly access iTunes via a wireless network:</p> <div style="text-align: center;"> <p>At a glance Use the iTunes Store to add music and TV shows, music, and podcasts to iPhone.</p>  </div> <p>Use iTunes Store to:</p> <ul style="list-style-type: none"> • Find music, TV shows, movies, tones, and more, by browsing or searching • See your personal Genius recommendations • Download previous purchases <p>Note: You need an Internet connection and an Apple ID to use the iTunes Store.</p> <p>Browse content: Tap one of the categories. Tap Genres to refine the listings. To see more information about an item, tap it.</p> <p>Search for content: Tap Search, then tap the search field and enter one or more words, then tap Search.</p> <p>Preview an item: Tap a song or video to play a sample.</p> <p>Purchase an item: Tap the item's price (or tap Free), then tap again to buy it. If you already purchased the item, "Download" appears instead of the price and you won't be charged again. When items are being downloaded, tap More, then tap Downloads to see their progress.</p> <p>Rent a movie: In some areas, certain movies are available to rent. You have 30 days to begin viewing a rented movie. Once you've started playing it, you can watch it as many times as you want in 24 hours. After these time limits, the movie is deleted.</p>

⁴⁵ iPhone User Guide (iOS 6) at 96 (MOTO-SDFL-16228).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>The iPad can wirelessly access iTunes via a wireless network:</p> <p>About the iTunes Store Use the iTunes Store to add content to iPad. You can browse and purchase music, TV shows, audiobooks, and alert tones. You can also buy and rent movies, or download and play podcasts or iTunes U collections. You need an Apple ID in order to purchase content. See "Store settings" on page 96.</p> <p><i>Note:</i> The iTunes Store may not be available in all regions, and iTunes Store content may vary across regions. Features are subject to change.</p> <p>To access the iTunes Store, iPad must have an Internet connection. See "Network" on page 125. 46</p> <p>As a further example, Apple TV can wirelessly access iTunes via a wireless network:</p> <p>Network</p> <ul style="list-style-type: none"> • An 802.11a, b, g, or n Wi-Fi wireless network (wireless video streaming requires 802.11a, g, or n), or 10/100Base-T Ethernet network • A broadband Internet connection (DSL, cable, or LAN) • Your wireless network name and password (if you use one) <p>Software and accounts</p> <p>To play content from a Mac or PC on Apple TV, you need:</p> <ul style="list-style-type: none"> • iTunes 10.5 or later • An Apple ID to rent movies or purchase TV shows from the iTunes store, and to use Home Sharing to stream content from a Mac or PC • A Netflix account to stream content. Other accounts may be required for full access to some Internet content. 47

⁴⁶ iPad User Guide (iOS 5.1) at 90 (MOTO-SDFL-19944).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p style="text-align: center;">Renting movies and purchasing TV shows</p> <p>You can rent standard or high-definition movies and purchase TV shows directly on Apple TV (where available). Follow the onscreen instructions to find out when a rented movie expires. Purchased TV shows don't expire.</p> <p>When a rented movie expires, it's no longer available for playback. To watch it again, you can rent it again from iTunes.</p> <p style="text-align: right;">48</p>
<p>establishing a wireless communication between the wireless client device and the attribute authority;</p>	<p>Apple devices can establish a wireless communication to an attribute authority, such as the App Store or iTunes.</p> <p style="text-align: center;"><u>App Store</u></p> <p>For example, iPhone and iPad can wirelessly connect to the App Store:</p> <p>Note: You need an Internet connection and an Apple ID to use the App Store.</p> <p>Purchase an app: Tap the app's price (or tap Free), then tap Buy Now. If you already purchased the app, "install" appears instead of the price. You won't be charged to download it again. While an app is being downloaded, its icon appears on the Home screen with a progress indicator.</p> <p style="text-align: right;">49</p>

⁴⁷ Apple TV 3rd Gen Setup Guide at 10 (MOTO-SDFL-19669).

⁴⁸ *Id.* at 24 (MOTO-SDFL-19683).

⁴⁹ iPhone User Guide (iOS 6) at 96 (MOTO-SDFL-16228).

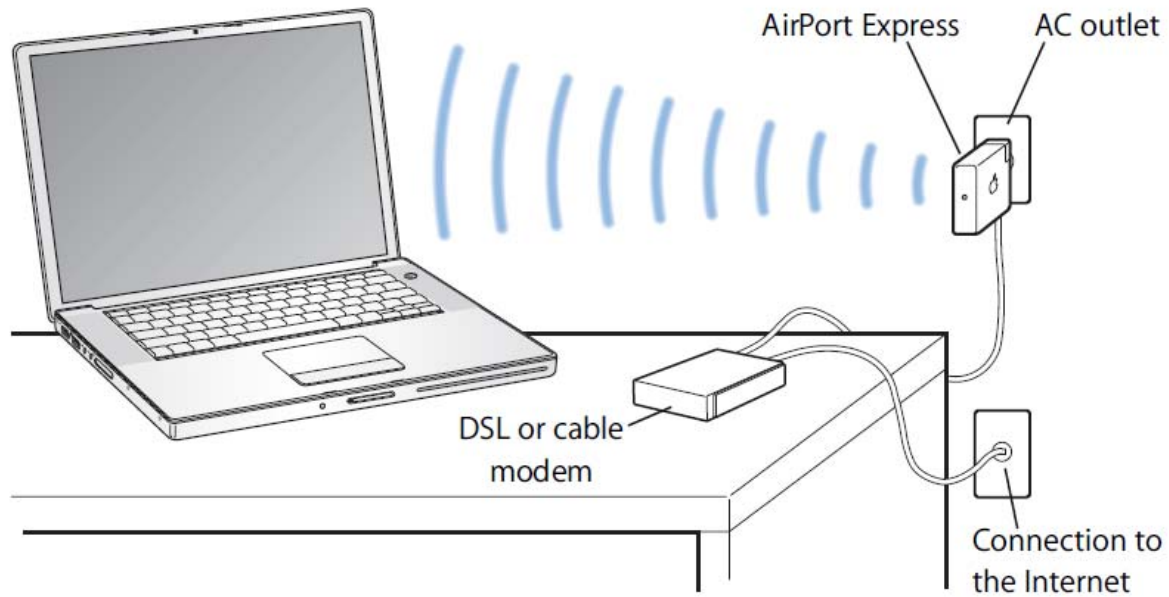
'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="520 245 638 285"><u>iTunes</u></p> <p data-bbox="426 329 1339 362">As an example, iOS and OSX devices can wirelessly connect to iTunes:</p> <p data-bbox="573 402 716 440">Network</p> <ul data-bbox="573 456 1682 646" style="list-style-type: none"> <li data-bbox="573 456 1682 537">• An 802.11a, b, g, or n Wi-Fi wireless network (wireless video streaming requires 802.11a, g, or n), or 10/100Base-T Ethernet network <li data-bbox="573 558 1346 591">• A broadband Internet connection (DSL, cable, or LAN) <li data-bbox="573 612 1419 646">• Your wireless network name and password (if you use one) <p data-bbox="573 683 953 721">Software and accounts</p> <p data-bbox="573 732 1360 764">To play content from a Mac or PC on Apple TV, you need:</p> <ul data-bbox="573 786 1661 1024" style="list-style-type: none"> <li data-bbox="573 786 863 818">• iTunes 10.5 or later <li data-bbox="573 839 1598 920">• An Apple ID to rent movies or purchase TV shows from the iTunes store, and to use Home Sharing to stream content from a Mac or PC <li data-bbox="573 941 1661 1024">• A Netflix account to stream content. Other accounts may be required for full access to some Internet content. <p data-bbox="1675 1003 1703 1024">50</p>

⁵⁰ Apple TV 3rd Gen Setup Guide at 10 (MOTO-SDFL-19669).

How AirPort Provides Wireless Internet Access

With AirPort Extreme technology, your MacBook Pro makes a wireless connection to an AirPort Express, Airport Extreme Base Station, or any 802.11a-, 802.11b-, or 802.11g-compliant product that is connected to the phone line, a DSL or cable modem, or a local-area network with Internet access.

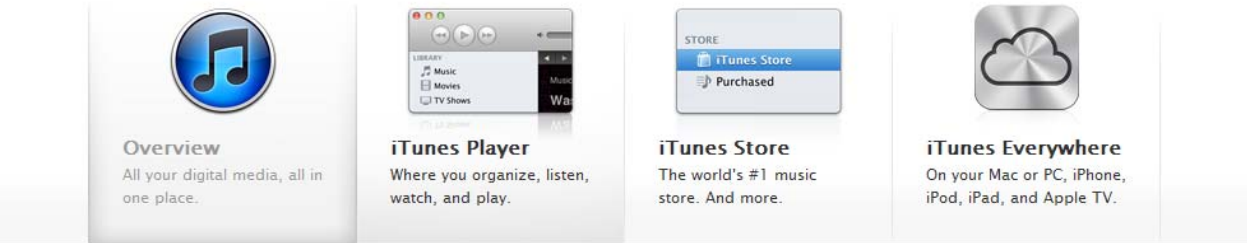
51



52

⁵¹ MacBook Pro User Guide at 62 (MOTO-SDFL-20146).

⁵² MacBook Pro User Guide at 63 (MOTO-SDFL-20147).

<p>'534 Patent Claim</p>	<p>Exemplary Apple Product: iOS and OSX devices¹⁰/Apple App Store and iTunes</p>
	<div style="text-align: center;"> <h3>What is iTunes?</h3>  <p>Overview All your digital media, all in one place.</p> <p>iTunes Player Where you organize, listen, watch, and play.</p> <p>iTunes Store The world's #1 music store. And more.</p> <p>iTunes Everywhere On your Mac or PC, iPhone, iPod, iPad, and Apple TV.</p> </div> <div style="text-align: center; margin-top: 20px;"> <h2>Play, buy, and enjoy your music, movies, TV shows, apps, and more. Everywhere.</h2> <p>iTunes is a free application for your Mac or PC. It lets you organize and play digital music and video on your computer. It can automatically download new music, app, and book purchases across all your devices and computers. And it's a store that has everything you need to be entertained. Anywhere. Anytime.</p> </div> <p style="text-align: right;">53</p>
<p>delivering an attribute certificate from the attribute authority to the wireless device;</p>	<p style="text-align: center;"><u>App Store</u></p> <p>When a purchase or other download is made from an Apple device via the App Store, an attribute certificate may be delivered from the associated attribute authority to the device. The attribute may provide fine-grained, role-based access control or enable the use of privileges or attributes. The App Store delivers an attribute certificate to a wireless device along with an application when the application or in-app purchase is downloaded to the device.</p>

⁵³ www.apple.com/itunes/what-is (accessed November 7, 2012) (MOTO-SDFL-20001-20007).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>At a Glance</p> <p>Set entitlement values in order to enable iCloud, push notifications, and App Sandbox (only for OS X). Each entitlement has a default value, which in most cases disables the capability associated with the entitlement. When you set an entitlement, you are overriding the default by providing an appropriate key-value pair.</p> <ul style="list-style-type: none"> • iCloud entitlements let you enable the use of iCloud data storage for your iOS or OS X app. You set iCloud entitlement values on a target-by-target basis in your Xcode project. • Push notifications let your app alert the user even when your iOS or OS X app is not in the foreground. You set push notification entitlement values as part of configuring your development and distribution provisioning profiles. • App Sandbox entitlements let you enable the security feature called <i>sandboxing</i> for your OS X app. By carefully enabling only the resource access that you need, you minimize the potential for damage if malicious code successfully exploits your app. You set App Sandbox entitlement values on a target-by-target basis in your Xcode project. <p>You can set many entitlements using the Summary tab of the Xcode target editor. For other entitlements, you must employ a property list file.</p> <p>The sort of value to associate with an entitlement key depends on the key. Many entitlement keys take Boolean values. For entitlements defined in a property list in an Xcode project, a Boolean entitlement value is either <code><true/></code> or <code><false/></code>. Some entitlement keys take a string or an array of strings as a value. Refer to the chapters in this document for specifics on the values to apply to the various entitlement keys.</p> <p>To use any entitlement keys, you must code sign your app because an app's entitlements are built in to its code signature.</p>

⁵⁴ Entitlement Key Reference (September 19, 2012) at 5 (MOTO-SDFL-19773).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="690 207 1020 240">Runtime Process Security</p> <p data-bbox="690 256 1535 315">Once an app is verified to be from an approved source, iOS enforces security measures to ensure that it can't compromise other apps or the rest of the system.</p> <p data-bbox="690 334 1535 516">All third-party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device. This prevents apps from gathering or modifying information stored by other apps. Each app has a unique home directory for its files, which is randomly assigned when the app is installed. If a third-party app needs to access information other than its own, it does so only by using application programming interfaces (APIs) and services provided by iOS.</p> <p data-bbox="690 535 1520 688">System files and resources are also shielded from the user's apps. The majority of iOS runs as the non-privileged user "mobile," as do all third-party apps. The entire OS partition is mounted read-only. Unnecessary tools, such as remote login services, aren't included in the system software, and APIs do not allow apps to escalate their own privileges to modify other apps or iOS itself.</p> <p data-bbox="690 708 1526 922">Access by third-party apps to user information and features such as iCloud is controlled using declared entitlements. Entitlements are key/value pairs that are signed in to an app and allow authentication beyond runtime factors like unix user ID. Since entitlements are digitally signed, they cannot be changed. Entitlements are used extensively by system apps and daemons to perform specific privileged operations that would otherwise require the process to run as root. This greatly reduces the potential for privilege escalation by a compromised system application or daemon. 55</p> <p data-bbox="630 964 1612 1084">In your OS X Xcode project, configure fine-grained security permissions by enabling settings in the Summary tab of the target editor. These settings, in turn, add Boolean values to entitlement keys in the target's .entitlements property list file. The values are then incorporated into the target's code signature when you build the project. 56</p>

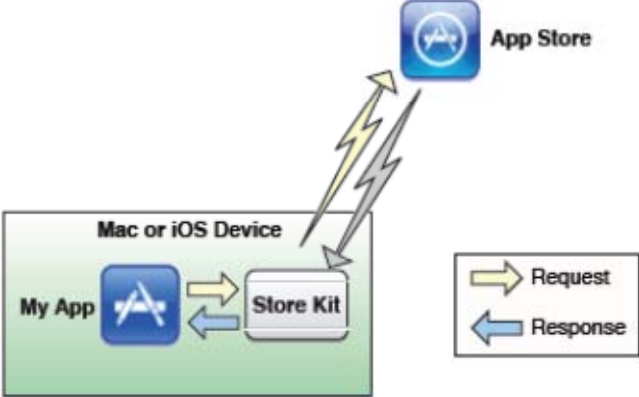
⁵⁵ iOS Security (May 12, 2012) at 6 (MOTO-SDFL-19819).

⁵⁶ *Id.* at 11 (MOTO-SDFL-19824).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes																						
	<table border="1"> <thead> <tr> <th data-bbox="667 215 1213 264">Entitlement key</th> <th data-bbox="1213 215 1560 264">Capability</th> </tr> </thead> <tbody> <tr> <td data-bbox="667 264 1213 358">com.apple.security.app-sandbox</td> <td data-bbox="1213 264 1560 358">Enables App Sandbox for a target in an Xcode project</td> </tr> <tr> <td data-bbox="667 358 1213 626">com.apple.security.application-groups</td> <td data-bbox="1213 358 1560 626">Allows access to group containers that are shared among multiple apps produced by a single development team, and allows certain additional interprocess communication between the apps. The format for this attribute is described in "Adding an App to an App Group" (page 18).</td> </tr> <tr> <td data-bbox="667 626 1213 721">com.apple.security.assets.movies.read-only</td> <td data-bbox="1213 626 1560 721">Read-only access to the user's Movies folder and iTunes movies</td> </tr> <tr> <td data-bbox="667 721 1213 815">com.apple.security.assets.movies.read-write</td> <td data-bbox="1213 721 1560 815">Read/write access to the user's Movies folder and iTunes movies</td> </tr> <tr> <td data-bbox="667 815 1213 909">com.apple.security.assets.music.read-only</td> <td data-bbox="1213 815 1560 909">Read-only access to the user's Music folder</td> </tr> <tr> <td data-bbox="667 909 1213 1003">com.apple.security.assets.music.read-write</td> <td data-bbox="1213 909 1560 1003">Read/write access to the user's Music folder</td> </tr> <tr> <td data-bbox="667 1003 1213 1097">com.apple.security.assets.pictures.read-only</td> <td data-bbox="1213 1003 1560 1097">Read-only access to the user's Pictures folder</td> </tr> <tr> <td data-bbox="667 1097 1213 1192">com.apple.security.assets.pictures.read-write</td> <td data-bbox="1213 1097 1560 1192">Read/write access to the user's Pictures folder</td> </tr> <tr> <td data-bbox="667 1192 1213 1252">com.apple.security.device.bluetooth</td> <td data-bbox="1213 1192 1560 1252">Interaction with Bluetooth devices</td> </tr> <tr> <td data-bbox="667 1252 1213 1346">com.apple.security.device.camera</td> <td data-bbox="1213 1252 1560 1346">Capture of movies and still images using the built-in camera, if available</td> </tr> </tbody> </table>	Entitlement key	Capability	com.apple.security.app-sandbox	Enables App Sandbox for a target in an Xcode project	com.apple.security.application-groups	Allows access to group containers that are shared among multiple apps produced by a single development team, and allows certain additional interprocess communication between the apps. The format for this attribute is described in "Adding an App to an App Group" (page 18).	com.apple.security.assets.movies.read-only	Read-only access to the user's Movies folder and iTunes movies	com.apple.security.assets.movies.read-write	Read/write access to the user's Movies folder and iTunes movies	com.apple.security.assets.music.read-only	Read-only access to the user's Music folder	com.apple.security.assets.music.read-write	Read/write access to the user's Music folder	com.apple.security.assets.pictures.read-only	Read-only access to the user's Pictures folder	com.apple.security.assets.pictures.read-write	Read/write access to the user's Pictures folder	com.apple.security.device.bluetooth	Interaction with Bluetooth devices	com.apple.security.device.camera	Capture of movies and still images using the built-in camera, if available
Entitlement key	Capability																						
com.apple.security.app-sandbox	Enables App Sandbox for a target in an Xcode project																						
com.apple.security.application-groups	Allows access to group containers that are shared among multiple apps produced by a single development team, and allows certain additional interprocess communication between the apps. The format for this attribute is described in "Adding an App to an App Group" (page 18).																						
com.apple.security.assets.movies.read-only	Read-only access to the user's Movies folder and iTunes movies																						
com.apple.security.assets.movies.read-write	Read/write access to the user's Movies folder and iTunes movies																						
com.apple.security.assets.music.read-only	Read-only access to the user's Music folder																						
com.apple.security.assets.music.read-write	Read/write access to the user's Music folder																						
com.apple.security.assets.pictures.read-only	Read-only access to the user's Pictures folder																						
com.apple.security.assets.pictures.read-write	Read/write access to the user's Pictures folder																						
com.apple.security.device.bluetooth	Interaction with Bluetooth devices																						
com.apple.security.device.camera	Capture of movies and still images using the built-in camera, if available																						

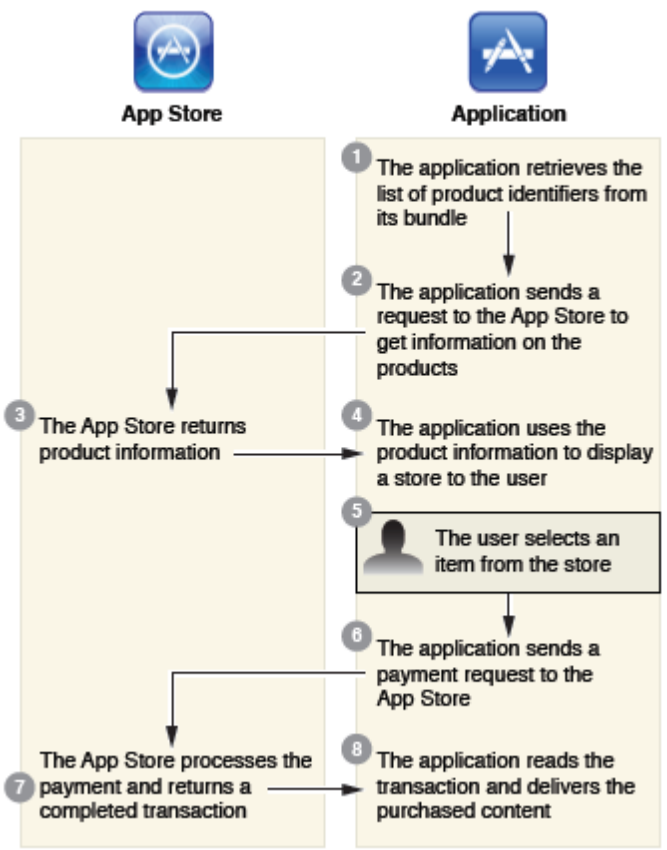
57

⁵⁷ *Id.* at 12 (MOTO-SDFL-19825).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>As another example, the App Store delivers an attribute certificate to a wireless device when an in-app purchase is made.</p> <p style="text-align: center;">Figure 1-1 In-App Store model</p>  <p>The diagram, titled 'Figure 1-1 In-App Store model', illustrates the interaction between a device and the App Store. A box labeled 'Mac or iOS Device' contains two components: 'My App' (represented by the App Store icon) and 'Store Kit' (represented by a white rounded rectangle). A yellow arrow points from 'My App' to 'Store Kit', and a blue arrow points from 'Store Kit' back to 'My App'. Outside the device box, the 'App Store' icon is shown. A yellow lightning bolt arrow points from the device towards the App Store, and a blue lightning bolt arrow points from the App Store back to the device. A legend to the right shows a yellow arrow labeled 'Request' and a blue arrow labeled 'Response'. The number '58' is located at the bottom right of the diagram area.</p>

⁵⁸ StoreKitGuide (February 16, 2012) at 7 (MOTO-SDFL-18611).

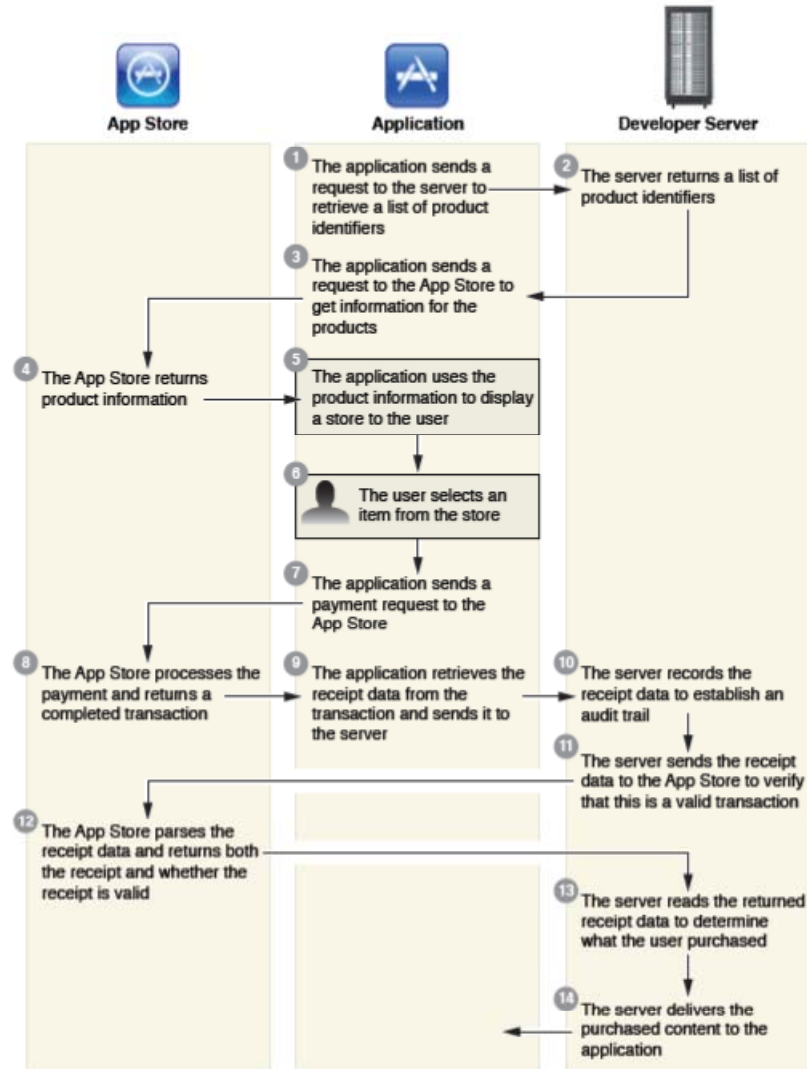
Figure 1-2 Built-in product delivery



59

⁵⁹ *Id.* at 10 (MOTO-SDFL-18614).

Figure 1-3 Server product delivery

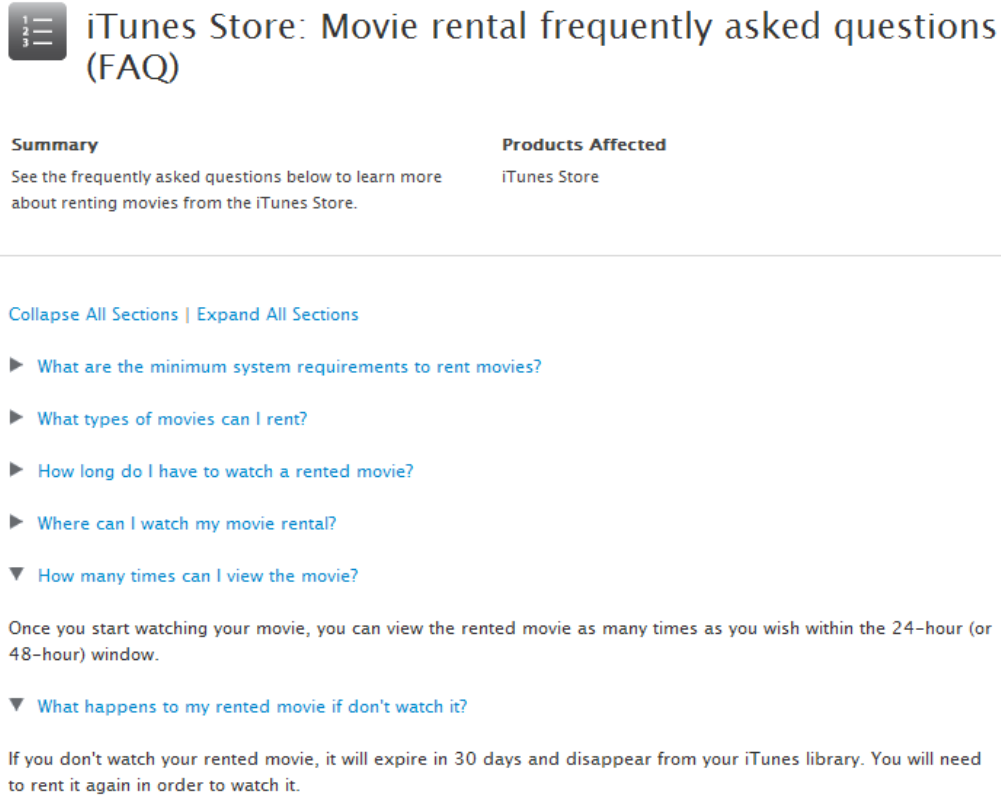


60

⁶⁰ *Id.* at 12 (MOTO-SDFL-18616).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="520 212 638 250"><u>iTunes</u></p> <p data-bbox="424 293 1801 358">iTunes delivers an attribute certificate to a wireless device along with a movie or TV show when a movie or TV show is rented and downloaded from iTunes.</p> <p data-bbox="674 415 1316 453">Renting movies and purchasing TV shows</p> <p data-bbox="674 461 1562 565">You can rent standard or high-definition movies and purchase TV shows directly on Apple TV (where available). Follow the onscreen instructions to find out when a rented movie expires. Purchased TV shows don't expire.</p> <p data-bbox="674 591 1524 656">When a rented movie expires, it's no longer available for playback. To watch it again, you can rent it again from iTunes.</p> <p data-bbox="1570 643 1596 659">61</p>

⁶¹ Apple TV 3rd Gen Setup Guide at 24 (MOTO-SDFL-19683).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	 <p>The screenshot shows the title "iTunes Store: Movie rental frequently asked questions (FAQ)" with a list of questions and answers. The questions include: "What are the minimum system requirements to rent movies?", "What types of movies can I rent?", "How long do I have to watch a rented movie?", "Where can I watch my movie rental?", "How many times can I view the movie?", and "What happens to my rented movie if don't watch it?". The answer to the last question states: "If you don't watch your rented movie, it will expire in 30 days and disappear from your iTunes library. You will need to rent it again in order to watch it."</p>

⁶² <http://support.apple.com/kb/ht1657> (accessed November 7, 2012) (MOTO-SDFL-20024-20027).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p style="text-align: center;">HD movies. Always the best seat in the house.</p> <p style="text-align: center;">With Apple TV, you get instant access to buy or rent the hottest HD movies — many in 1080p and often available the same day they come out on DVD.¹ That's perfect for spontaneous movie nights (or afternoons or mornings). Search by top movies, title, or genre. Can't decide? Read reviews, watch trailers, and check out Rotten Tomatoes ratings. Or let Genius make a recommendation based on movies you've watched before. Then pick a flick, press Play, and in seconds you're watching the opening credits in theater-like Dolby Digital 5.1 surround.²</p> <p style="text-align: right;">63</p>
<p>verifying the attribute authority to the wireless client device using the attribute certificate and the root public key certificate pre-loaded in the wireless client device under authority of the wireless network operator;</p>	<p>An attribute certificate and root public key certificates are used to verify the attribute authority. Apple pre-loads root public key certificates into devices for use in the verification process. For example:</p>

⁶³ <http://www.apple.com/appletv/whats-on/> (accessed November 7, 2012) (MOTO-SDFL-20246-20259).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="705 212 940 240">Secure Boot Chain</p> <p data-bbox="705 261 1514 345">Each step of the boot-up process contains components that are cryptographically signed by Apple to ensure integrity, and proceeds only after verifying the chain of trust. This includes the bootloaders, kernel, kernel extensions, and baseband firmware.</p> <p data-bbox="705 367 1514 573">When an iOS device is turned on, its application processor immediately executes code from read-only memory known as the Boot ROM. This immutable code is laid down during chip fabrication, and is implicitly trusted. The Boot ROM code contains the Apple Root CA public key, which is used to verify that the Low-Level Bootloader (LLB) is signed by Apple before allowing it to load. This is the first step in the chain of trust where each step ensures that the next is signed by Apple. When the LLB finishes its tasks, it verifies and runs the next-stage bootloader, iBoot, which in turn verifies and runs the iOS kernel.</p> <p data-bbox="705 594 1486 647">This secure boot chain ensures that the lowest levels of software are not tampered with, and allows iOS to run only on validated Apple devices.</p> <p data-bbox="705 669 1524 846">If one step of this boot process is unable to load or verify the next, boot-up is stopped and the device displays the "Connect to iTunes" screen. This is called recovery mode. If the Boot ROM is not even able to load or verify LLB, it enters DFU (Device Firmware Upgrade) mode. In both cases, the device must be connected to iTunes via USB and restored to factory default settings. For more information on manually entering recovery mode, see http://support.apple.com/kb/HT1808.</p> <p data-bbox="1528 829 1556 850">64</p> <p data-bbox="926 886 1083 909">Root certificates</p> <p data-bbox="926 919 1314 1284">Out of the box, iPhone includes a number of preinstalled root certificates. To view a list of the preinstalled system roots, see the Apple Support article at http://support.apple.com/kb/HT2185. If you are using a root certificate that is not preinstalled, such as a self-signed root certificate created by your company, you can distribute it to iPhone using one of the methods listed in the "Distributing and Installing Certificates" section of this document.</p> <p data-bbox="1318 1268 1346 1289">65</p>

⁶⁴ iOS Security (May 12, 2012) at 4 (MOTO-SDFL-19817).

⁶⁵ iPhone in Business – Digital Certificates at 1 (MOTO-SDFL-17555).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>Root certificates</p> <p>Out of the box, iPad includes a number of preinstalled root certificates. To view a list of the preinstalled system roots, see the Apple Support article at http://support.apple.com/kb/HT3580. If you are using a root certificate that is not preinstalled, such as a self-signed root certificate created by your company, you can distribute it to iPad using one of the methods listed in the "Distributing and Installing Certificates" section of this document. ⁶⁶</p> <h2 style="text-align: center;">Certificate, Key, and Trust Services Tasks for iOS</h2> <hr/> <p>This chapter describes and illustrates the use of Certificate, Key, and Trust Services functions to import an identity, evaluate the trust of a certificate, determine the cause of a trust failure, and recover from a trust failure.</p> <p>The sequence of operations illustrated in this chapter is:</p> <ol style="list-style-type: none"> 1. Import an identity. 2. Obtain a certificate from the imported data. 3. Obtain a policy object for the policy used in evaluation of the certificate. 4. Validate the certificate and evaluate whether it can be trusted as specified by the policy. 5. Test for a recoverable trust error. 6. Determine whether the trust error is due to an expired certificate. 7. Change the evaluation criteria to ignore expired certificates. 8. Reevaluate the certificate. <p style="text-align: right;">67</p>

⁶⁶ iPad in Business at 12 (MOTO-SDFL-17480).

⁶⁷ Certificate, Key, and Trust Services Programming Guide at 27 (MOTO-SDFL-19750).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="682 217 1388 250" style="text-align: center;">Extracting and Evaluating an Identity From a *.P12 File</p> <p data-bbox="772 293 1535 375">If you need a cryptographic identity (that is, a private key and its associated certificate) on an iOS-based device—for client-side authentication, for example—you can transfer it to the device securely as PKCS #12 data in a password-protected *.p12 file. This section shows how to extract the identity and trust objects from the PKCS #12 data and how to evaluate the trust.</p> <p data-bbox="772 394 1535 456">Listing 2-1 shows sample code for using the <code>SecPKCS12Import</code> function to extract identity and trust objects from a *.p12 file and how to evaluate the trust. Listing 2-2 (page 13) shows how to get the certificate from the identity and display certificate information. Explanations for numbered lines of code follow each listing. 68</p> <p data-bbox="682 524 1094 557" style="text-align: center;">Encrypting and Decrypting Data</p> <p data-bbox="772 602 1535 745">The Certificate, Key, and Trust API includes functions for generating asymmetric key pairs and using them to encrypt and decrypt data. You might want to use this feature to encrypt data that you do not want to be accessible in backup data, for example. Or, you can use a private-public key pair shared between your iOS application and a desktop application to send encrypted data over a network. The code in Listing 2-8 shows how to generate a public-private key pair for use on the mobile device. Listing 2-9 (page 20) shows how to use a public key to encrypt data using Certificate, Key, and Trust functions, and Listing 2-10 (page 22) shows how to use a private key to decrypt data. Notice that these samples use Cocoa objects (such as 69</p>

⁶⁸ Certificate, Key, and Trust Services Programming Guide at 6 (MOTO-SDFL-19729-19730).

⁶⁹ Certificate, Key, and Trust Services Programming Guide at 19 (MOTO-SDFL-19742).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>Attribute certificates may, for App Store downloads, be embedded in the developer signature.</p> <p>Runtime Process Security</p> <p>Once an app is verified to be from an approved source, iOS enforces security measures to ensure that it can't compromise other apps or the rest of the system.</p> <p>All third-party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device. This prevents apps from gathering or modifying information stored by other apps. Each app has a unique home directory for its files, which is randomly assigned when the app is installed. If a third-party app needs to access information other than its own, it does so only by using application programming interfaces (APIs) and services provided by iOS.</p> <p>System files and resources are also shielded from the user's apps. The majority of iOS runs as the non-privileged user "mobile," as do all third-party apps. The entire OS partition is mounted read-only. Unnecessary tools, such as remote login services, aren't included in the system software, and APIs do not allow apps to escalate their own privileges to modify other apps or iOS itself.</p> <p>Access by third-party apps to user information and features such as iCloud is controlled using declared entitlements. Entitlements are key/value pairs that are signed in to an app and allow authentication beyond runtime factors like unix user ID. Since entitlements are digitally signed, they cannot be changed. Entitlements are used extensively by system apps and daemons to perform specific privileged operations that would otherwise require the process to run as root. This greatly reduces the potential for privilege escalation by a compromised system application or daemon.</p>

70

⁷⁰ iOS Security (May 12, 2012) at 6 (MOTO-SDFL-19819).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="575 212 762 245">At a Glance</p> <p data-bbox="575 269 1644 363">Set entitlement values in order to enable iCloud, push notifications, and App Sandbox (only for OS X). Each entitlement has a default value, which in most cases disables the capability associated with the entitlement. When you set an entitlement, you are overriding the default by providing an appropriate key-value pair.</p> <ul data-bbox="583 386 1656 748" style="list-style-type: none"> <li data-bbox="583 386 1518 459">• iCloud entitlements let you enable the use of iCloud data storage for your iOS or OS X app. You set iCloud entitlement values on a target-by-target basis in your Xcode project. <li data-bbox="583 480 1633 586">• Push notifications let your app alert the user even when your iOS or OS X app is not in the foreground. You set push notification entitlement values as part of configuring your development and distribution provisioning profiles. <li data-bbox="583 607 1656 748">• App Sandbox entitlements let you enable the security feature called <i>sandboxing</i> for your OS X app. By carefully enabling only the resource access that you need, you minimize the potential for damage if malicious code successfully exploits your app. You set App Sandbox entitlement values on a target-by-target basis in your Xcode project. <p data-bbox="575 802 1656 862">You can set many entitlements using the Summary tab of the Xcode target editor. For other entitlements, you must employ a property list file.</p> <p data-bbox="575 894 1656 1024">The sort of value to associate with an entitlement key depends on the key. Many entitlement keys take Boolean values. For entitlements defined in a property list in an Xcode project, a Boolean entitlement value is either <code><true/></code> or <code><false/></code>. Some entitlement keys take a string or an array of strings as a value. Refer to the chapters in this document for specifics on the values to apply to the various entitlement keys.</p> <p data-bbox="575 1057 1625 1117">To use any entitlement keys, you must code sign your app because an app's entitlements are built in to its code signature.</p> <p data-bbox="1667 1089 1688 1109">71</p>

⁷¹ Entitlement Key Reference (September 19, 2012) at 5 (MOTO-SDFL-19773).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p>In Snow Leopard Server, several keychains can hold certificates:</p> <ul style="list-style-type: none"> • SystemRootCertificates: This keychain holds root certificates that ship with Mac OS X. The certificates already have trust given to them. • System: This keychain holds certificates that the computer administrator can add. All users on a given client can read from this keychain. The trust settings of a certificate in this keychain can override those of a certificate in SystemRootCertificates. • Any other keychain: This holds certificates for a given user and is only accessible to that user. The trust settings of a certificate in this keychain can override those of a certificate in SystemRootCertificates or System. <p>Trusted certificates can be in any of these locations, but to trust a certificate, trust settings must be given explicitly to a certificate.</p> <p style="text-align: right;">72</p>
delivering an attribute to the wireless client device over the wireless network; and enabling the attribute at the wireless client device.	<p>An attribute may be delivered to Apple devices over the wireless network and enabled.</p> <p style="text-align: center;"><u>App Store</u></p> <p>The App Store allows users to download applications having various attributes such as system operations permissions.</p>

⁷² Snow Leopard Server Security Configuration at 166 (MOTO-SDFL-18314).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p data-bbox="747 224 1031 248">Runtime Process Security</p> <p data-bbox="747 266 1486 315">Once an app is verified to be from an approved source, iOS enforces security measures to ensure that it can't compromise other apps or the rest of the system.</p> <p data-bbox="747 332 1486 493">All third-party apps are "sandboxed," so they are restricted from accessing files stored by other apps or from making changes to the device. This prevents apps from gathering or modifying information stored by other apps. Each app has a unique home directory for its files, which is randomly assigned when the app is installed. If a third-party app needs to access information other than its own, it does so only by using application programming interfaces (APIs) and services provided by iOS.</p> <p data-bbox="747 511 1486 646">System files and resources are also shielded from the user's apps. The majority of iOS runs as the non-privileged user "mobile," as do all third-party apps. The entire OS partition is mounted read-only. Unnecessary tools, such as remote login services, aren't included in the system software, and APIs do not allow apps to escalate their own privileges to modify other apps or iOS itself.</p> <p data-bbox="747 664 1486 850">Access by third-party apps to user information and features such as iCloud is controlled using declared entitlements. Entitlements are key/value pairs that are signed in to an app and allow authentication beyond runtime factors like unix user ID. Since entitlements are digitally signed, they cannot be changed. Entitlements are used extensively by system apps and daemons to perform specific privileged operations that would otherwise require the process to run as root. This greatly reduces the potential for privilege escalation by a compromised system application or daemon.</p> <p data-bbox="1493 821 1518 841">73</p> <p data-bbox="520 943 636 979"><u>iTunes</u></p> <p data-bbox="428 1024 1797 1089">As a further example, subscription-based purchases using iTunes or Apple TV also have attributes that may affect content access permissions.</p>

⁷³ iOS Security (May 12, 2012) at 6 (MOTO-SDFL-19819).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	<p style="text-align: center;">Renting movies and purchasing TV shows</p> <p>You can rent standard or high-definition movies and purchase TV shows directly on Apple TV (where available). Follow the onscreen instructions to find out when a rented movie expires. Purchased TV shows don't expire.</p> <p>When a rented movie expires, it's no longer available for playback. To watch it again, you can rent it again from iTunes.</p> <p style="text-align: right;">74</p>
Claim 2	
<p>2. The method of claim 1, further comprising the step of executing a transaction whereby the wireless client device authorizes payment for the attribute from the attribute authority.</p>	<p>Claim 1 is incorporated herein by reference.</p> <p>Apple devices, in conjunction with the Apple App Store and iTunes, use a method as described in claim one and further comprising the step of executing a transaction whereby the wireless client device authorizes payment for the attribute from the attribute authority.</p> <p>The Apple App store allows users to download and install verified software onto mobile devices. Users may pay for this software. Users may also pay to download applications from the App Store providing privileges or attributes or fine-grained, role-based access control. Further, users of Apple TV may download and play media content having certain access controls. Users of iTunes may download and play media content having certain access controls.</p>
Claim 7	
<p>7. The method of claim 1, wherein the attribute certificate represents at least one of (i) purchased service or product certificates and</p>	<p>Claim 1 is incorporated herein by reference.</p> <p>Apple devices, in conjunction with the Apple App Store and iTunes, use a method as described in claim one wherein the attribute represents (i) purchased service or product certificates.</p> <p>As described above in relation to claims 1 and 2, users may purchase service or product certificates from the</p>

⁷⁴ Apple TV 3rd Gen Setup Guide at 24 (MOTO-SDFL-19683).

'534 Patent Claim	Exemplary Apple Product: iOS and OSX devices ¹⁰ /Apple App Store and iTunes
	App Store and iTunes.
(ii) system operations permissions.	<p>The attribute may also represent (ii) system operations permissions.</p> <p>As discussed in relation to claim 1, the attribute described may relate to system operations permissions. By way of example, entitlements may be coupled to App Store content.</p>
Claim 8	
8. The method of claim 1, wherein the attribute is software code for execution by the wireless client device.	<p>Claim 1 is incorporated herein by reference.</p> <p>Apple devices, in conjunction with the Apple App Store and iTunes, use a method as described in claim one wherein the attribute is software code for execution by the wireless client device. As discussed above, content from the Apple App store may be software code for execution by the device.</p>