

**UNITED STATES PATENT NO. 6,008,737**

**SUPPLEMENTAL INFRINGEMENT CONTENTIONS<sup>1</sup>**


**Accused Apple Products:**<sup>2</sup> Apple iPhone 3G, Apple iPhone 3GS, Apple iPhone 4, and Apple iPhone 4S, Apple iPad, Apple iPad with 3G, Apple iPad 2, Apple iPad 2 with 3G, Apple iPod Touch (collectively, "Apple Phones"), Apple MacBook, Apple MacBook Pro, Apple MacBook Air, Apple iMac, Apple Mac Mini, and Apple Mac Pro (collectively, "Apple Computers").

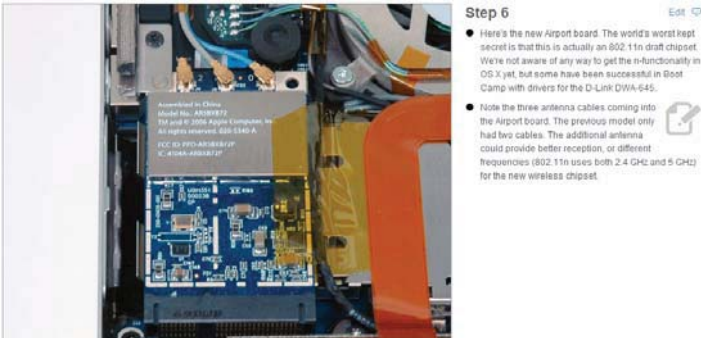
<b>'737 Patent Claim</b>	<b>Accused Apple Products<sup>3</sup></b>
<p>9. A portable communication device in a communication system having a fixed portion, the portable communication device comprising:</p>	<p>Upon information and belief, Apple imports, manufactures, sells, offers to sell, and uses the Accused Apple Products, which are portable communication devices. Moreover, the Accused Apple Products operate in the normal course of use in a communication system having a fixed portion, which is the authentication system used in one or more of Apple's iTunes, Apple's App Store, and Apple's enterprise application system.</p> <p><i>See, e.g.,</i> iPhone 4 Technical Specifications, (<a href="http://www.apple.com/iphone/specs.html">http://www.apple.com/iphone/specs.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126659:</p>

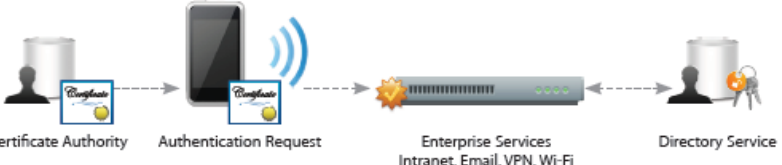
<sup>1</sup> Motorola Mobility's investigation is ongoing and discovery and claim construction are not yet complete. Apple has, thus far, produced neither all documents relevant to the accused methods and products, nor the requested Rule 30(b)(6) witnesses. Mobility reserves the right to supplement or amend these contentions with contentions arising under the doctrine of equivalents in response to any proposed or ordered claim construction, subsequent discovery response or production, or subsequent disclosure made pursuant to FRCP 26.

<sup>2</sup> Motorola Mobility reserves the right to supplement this list of Accused Apple Products.

<sup>3</sup> This chart provides Motorola's infringement analysis for the Accused Apple Products. Upon information and belief, the analysis set forth in this chart for applies equally to all of the Accused Apple Products.


'737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p><b>Size and weight<sup>1</sup></b></p> <p>Height: <b>4.5 inches (115.2 mm)</b></p> <p>Width: <b>2.31 inches (58.6 mm)</b></p> <p>Depth: <b>0.37 inch (9.3 mm)</b></p> <p>Weight: <b>4.8 ounces (137 grams)</b></p>  <p><b>Cellular and wireless</b></p> <ul style="list-style-type: none"> <li>■ UMTS/HSDPA/HSUPA (850, 900, 1900, 2100 MHz)</li> <li>■ GSM/EDGE (850, 900, 1800, 1900 MHz)</li> <li>■ 802.11b/g/n Wi-Fi (802.11n 2.4GHz only)</li> <li>■ Bluetooth 2.1 + EDR wireless technology</li> </ul> <p><i>See also e.g., Apple iPad Technical Specifications, (<a href="http://www.apple.com/ipad/specs">www.apple.com/ipad/specs</a>), accessed on April 12, 2011, MOTO-APPLE-0005383110_35376:</i></p>

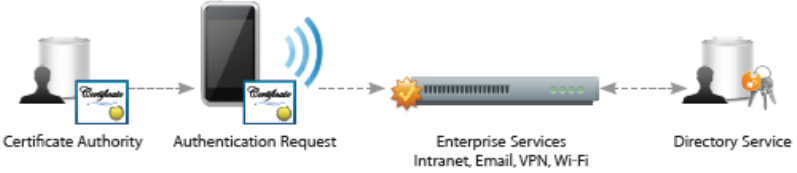
'737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p data-bbox="594 277 716 321">Wireless and Cellular</p> <ul data-bbox="825 293 1026 329" style="list-style-type: none"> <li>■ Wi-Fi (802.11a/b/g/n)</li> <li>■ Bluetooth 2.1 + EDR technology</li> </ul> <ul data-bbox="1142 293 1415 436" style="list-style-type: none"> <li>■ Wi-Fi + 3G model: UMTS/HSDPA/HSUPA (850, 900, 1900, 2100 MHz), GSM/EDGE (850, 900, 1800, 1900 MHz)</li> <li>■ Wi-Fi + 3G for Verizon model: CDMA EV-DO Rev. A (800, 1900 MHz)</li> <li>■ Data only<sup>s</sup></li> <li>■ Wi-Fi (802.11 a/b/g/n)</li> <li>■ Bluetooth 2.1 + EDR technology</li> </ul> <p data-bbox="1150 453 1329 469"><a href="#">Learn more about Wi-Fi + 3G</a></p> <p data-bbox="594 524 1919 630"><i>See also, e.g., MacBook Pro 15" Core 2 Duo Model A1211 Teardown, (<a href="http://www.ifixit.com/Teardown/MacBook-Pro-15-Inch-Core-2-Duo-Model-A1211-Teardown/593/1">http://www.ifixit.com/Teardown/MacBook-Pro-15-Inch-Core-2-Duo-Model-A1211-Teardown/593/1</a>), accessed on May 14, 2011, MOTO-APPLE-0006037953_127250:</i></p> <div data-bbox="600 667 1297 1003">  <p data-bbox="1058 670 1108 686"><b>Step 6</b></p> <ul data-bbox="1058 695 1297 849" style="list-style-type: none"> <li>● Here's the new Airport board. The world's worst kept secret is that this is actually an 602.11 in draft chipset. We're not aware of any way to get the n-functionality in OS X yet, but some have been successful in Boot Camp with drivers for the D-Link DWA-545.</li> <li>● Note the three antenna cables coming into the Airport board. The previous model only had two cables. The additional antenna could provide better reception, or different frequencies (802.11n uses both 2.4 GHz and 5 GHz) for the new wireless chipset.</li> </ul> </div> <p data-bbox="594 1049 1919 1409">In addition, Apple has performed each and every step of this claim, and, through its design of the Accused Apple Products, Apple also contributes to the infringement of the '737 patent by users of the device. Apple and Motorola have been in talks since 2007 regarding the licensing of Motorola's patent portfolio, and, on information and belief, in accordance with those negotiations, Apple has reviewed said portfolio, including Motorola's '737 Patent. Thus, at least as early as 2007, Apple knew that offering to sell or selling the Accused Apple Products would contribute to direct infringement of the '737 Patent. Apple knew that the Accused Apple Products contain two specific components for sending and receiving authorization requests and responses. Apple knew that these components could be combined and had no substantial non-infringing use, and that the combination, for which the two components were especially made, was both patented and infringing. Moreover, Accused Apple</p>

‘737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p>Products users have, in fact, combined these components into an infringing device. Apple further contributes to the direct infringement of the users of the Accused Apple Products, including but not limited to by describing infringing combinations in its advertisements, promotional materials, and user manuals. <i>See e.g.</i>, iPhone in Business: Security Overview, MOTO-APPLE-0006037953_126666.</p> <p><b>Mandatory Code Signing</b>  All iPhone applications must be signed. The applications provided with the device are signed by Apple. Third-party applications are signed by the developer using an Apple-issued certificate. This ensures that applications haven't been tampered with or altered. Additionally, runtime checks are made to ensure that an application hasn't become untrusted since it was last used.</p> <p><i>See also</i> iPhone in Business: Digital Certificates, MOTO-APPLE-0006037953_126669:</p> <p><b>Digital certificates</b>  Digital certificates can be used to securely authenticate users to corporate services without the need for user names, passwords or soft tokens. On iPhone, certificate-based authentication is supported for access to Microsoft Exchange ActiveSync, VPN, and Wi-Fi networks.</p>  <p><i>See also id.:</i></p>

‘737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p>iPhone supports digital certificates, giving business users secure, streamlined access to corporate services. A digital certificate is composed of a public key, information about the user, and the certificate authority that issued the certificate. Digital certificates are a form of identification that enables streamlined authentication, data integrity, and encryption.</p> <p>On iPhone, certificates can be used in a variety of ways. Signing data with a digital certificate helps to ensure that information cannot be altered. Certificates can also be used to guarantee the identity of the author or “signer.” Additionally, they can be used to encrypt configuration profiles and network communications to further protect confidential or private information.</p> <p><i>See also</i> Distributing Enterprise Apps for iOS 4 Devices, (<a href="http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html">http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598:</p> <p><b>"Certificate Validation.</b> The first time an application is opened on a device, the distribution certificate is validated by contacting Apple's OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a response from the OCSP server is not interpreted as a revocation. To verify the status, the device must be able to reach ocsf.apple.com. See 'Network Configuration Requirements.'</p> <p>The OCSP response is cached on the device for the period of time specified by the OCSP server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a revocation is received at that time, the app will be prevented from running. Note that revoking a distribution certificate will invalidate all of the applications you have distributed.</p> <p>An app will not run if the distribution certificate has expired. Currently, distribution certificates are valid for one year. A few weeks before your certificate expires request a new distribution certificate from the Dev Center, use it create new distribution provisioning profiles, then recompile and distribute the updated apps to your users. See 'Providing Updated Apps.'"</p>
a processor;	Upon information and belief, the Apple Phones contain a variety of different processors, such as an Apple A4 processor, and Apple Computers contain a variety of different processors, such as the

'737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p>2.4GHz Intel Core 2 Duo processor.</p> <p>See, e.g., (<a href="http://www.apple.com/channel/iphone/iphone-4/best-buy/design.html">http://www.apple.com/channel/iphone/iphone-4/best-buy/design.html</a>), accessed May 12, 2011, MOTO-APPLE-0006037953_127201:</p> <div data-bbox="590 444 1421 786" data-label="Image"> </div> <p>See also e.g., Apple iPad Technical Specifications, (<a href="http://www.apple.com/ipad/specs">www.apple.com/ipad/specs</a>), accessed on April 12, 2011, MOTO-APPLE-0005383110_35376:</p> <div data-bbox="590 948 1312 1094" data-label="Image"> </div> <p>See also, e.g., MacBook Pro 15" Core 2 Duo Model A1211 Teardown, (<a href="http://www.ifixit.com/Teardown/MacBook-Pro-15-Inch-Core-2-Duo-Model-A1211-Teardown/593/1">http://www.ifixit.com/Teardown/MacBook-Pro-15-Inch-Core-2-Duo-Model-A1211-Teardown/593/1</a>), accessed on May 14, 2011, MOTO-APPLE-0006037953_127248:</p>

‘737 Patent Claim	Accused Apple Products <sup>3</sup>
	 <p data-bbox="611 711 1073 781"><b>MacBook Pro 15" Core 2 Duo Model A1211</b></p> <p data-bbox="611 800 982 821">2.16 or 2.33 GHz Core 2 Duo processor</p>
<p data-bbox="191 914 583 1125">an authorization element coupled to the processor for obtaining usage authorization for utilizing software in the portable communication device,</p>	<p data-bbox="583 914 1919 979">Upon information and belief, the Accused Apple Products contain an authorization element coupled to the processor for obtaining usage authorization for utilizing software:</p> <p data-bbox="604 1027 852 1052"><b>Mandatory Code Signing</b></p> <p data-bbox="604 1057 1430 1203">All iPhone applications must be signed. The applications provided with the device are signed by Apple. Third-party applications are signed by the developer using an Apple-issued certificate. This ensures that applications haven't been tampered with or altered. Additionally, runtime checks are made to ensure that an application hasn't become untrusted since it was last used.</p> <p data-bbox="583 1252 1598 1284">iPhone in Business: Security Overview, MOTO-APPLE-0006037953_126666.</p> <p data-bbox="583 1325 1713 1357"><i>See also</i> iPhone in Business: Digital Certificates, MOTO-APPLE-0006037953_126669:</p>

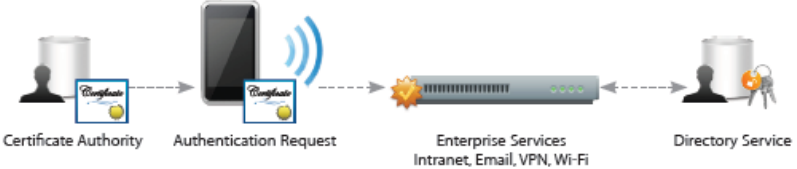
'737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p><b>Digital certificates</b>                      Digital certificates can be used to securely authenticate users to corporate services without the need for user names, passwords or soft tokens. On iPhone, certificate-based authentication is supported for access to Microsoft Exchange ActiveSync, VPN, and Wi-Fi networks.</p>  <p><i>See also id.:</i></p> <p>iPhone supports digital certificates, giving business users secure, streamlined access to corporate services. A digital certificate is composed of a public key, information about the user, and the certificate authority that issued the certificate. Digital certificates are a form of identification that enables streamlined authentication, data integrity, and encryption.</p> <p>On iPhone, certificates can be used in a variety of ways. Signing data with a digital certificate helps to ensure that information cannot be altered. Certificates can also be used to guarantee the identity of the author or "signer." Additionally, they can be used to encrypt configuration profiles and network communications to further protect confidential or private information.</p> <p><i>See also</i> Distributing Enterprise Apps for iOS 4 Devices, (<a href="http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html">http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598:</p> <p><b>"Certificate Validation.</b> The first time an application is opened on a device, the distribution certificate is validated by contacting Apple's OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a response from the OCSP server is not interpreted as a revocation. To verify the status, the device must be able to reach ocsf.apple.com. See 'Network Configuration Requirements.'</p>

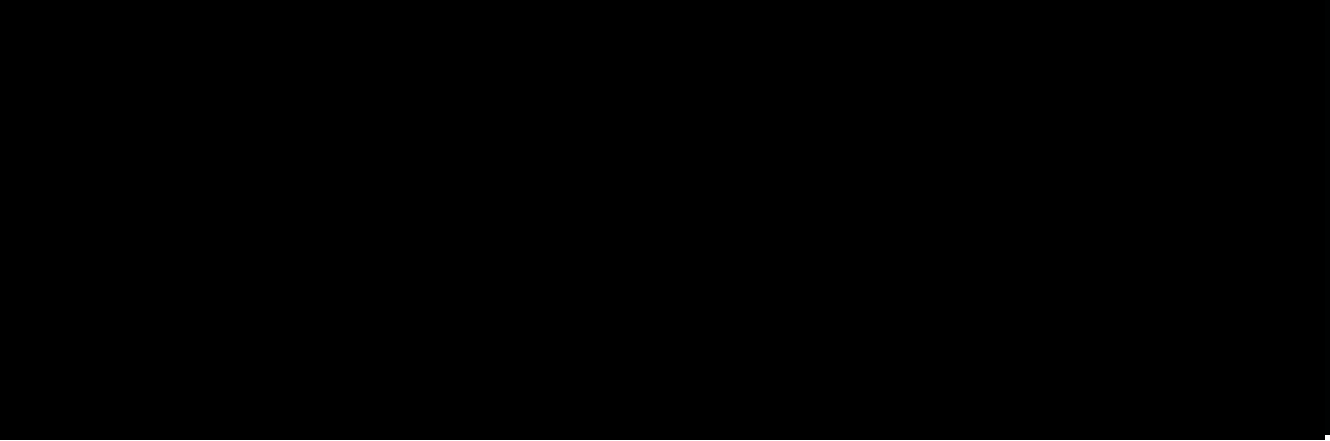


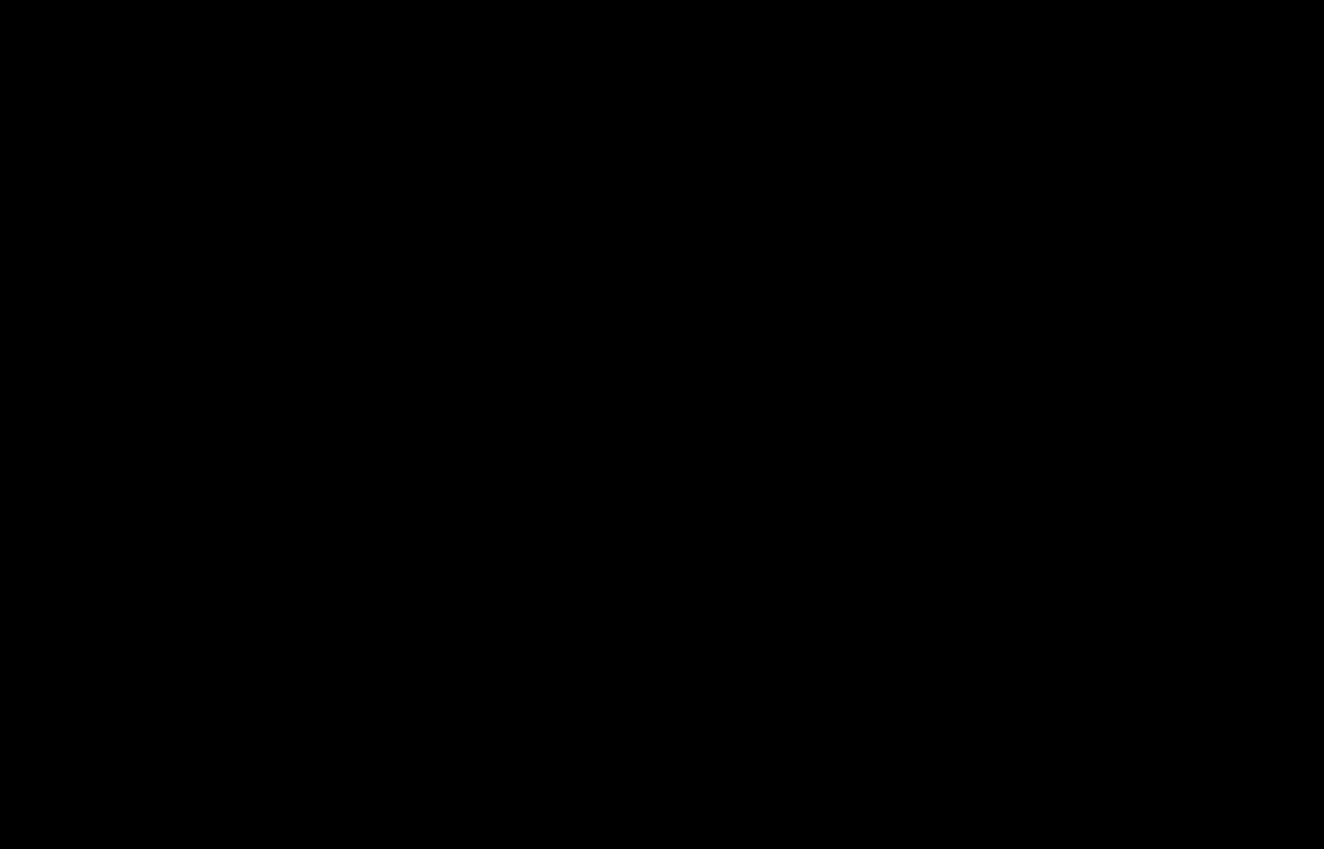
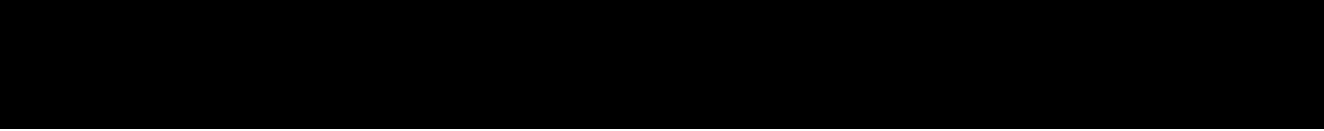
<b>'737 Patent Claim</b>	<b>Accused Apple Products<sup>3</sup></b>
	<p>The OCSP response is cached on the device for the period of time specified by the OCSP server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a revocation is received at that time, the app will be prevented from running. Note that revoking a distribution certificate will invalidate all of the applications you have distributed.</p> <p>An app will not run if the distribution certificate has expired. Currently, distribution certificates are valid for one year. A few weeks before your certificate expires request a new distribution certificate from the Dev Center, use it create new distribution provisioning profiles, then recompile and distribute the updated apps to your users. See 'Providing Updated Apps.'</p> <p><u>Communications with the Apple App store.</u> In connection with a request to use or download software onto an Accused Apple Product, an authorization element coupled to the processor of that Accused Apple Product requests usage authorization for utilizing that software in the Accused Apple Product.</p> <p><i>See also e.g.,</i> Email from Dallas De Atley, dated December 14, 2010, 745-Apple10360097-98:</p> <div data-bbox="598 906 1913 1365" style="background-color: black; width: 100%; height: 283px; margin: 10px 0;"></div> <p><i>See also e.g.,</i> iTunes Authentication Use Case Chart, 745-Apple5374978-81:</p>

'737 Patent Claim	Accused Apple Products <sup>3</sup>
	 <p data-bbox="598 1182 1806 1221"><i>See also e.g.,</i> Email from Henri Lamiraux, dated December 13, 2010, 745-Apple10362501-32:</p> 

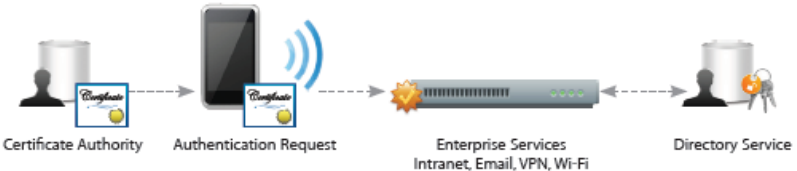
‘737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p><i>See also</i> e.g. iPhone SDK, dated October 4, 2007, 745-Apple8563808-27;  <a href="http://support.apple.com/kb/HT1420">http://support.apple.com/kb/HT1420</a>; <a href="http://support.apple.com/kb/HT2204?viewlocale=en_US">http://support.apple.com/kb/HT2204?viewlocale=en_US</a>;  <a href="http://support.apple.com/kb/HE37">http://support.apple.com/kb/HE37</a></p>
<p>in which the authorization element generates an external authorization request, and</p>	<p>Upon information and belief, the authorization element in the Accused Apple Products generates an external authorization request sent to Apple's iTunes, Apple's App Store authentication servers and / or Apple's enterprise application system. For example, the digital certificate (authorization element) is validated by contacting an external OCSP server (external authorization request) upon initial opening, and by a runtime check (external authorization request) at each time of use.</p> <p><i>See</i> Distributing Enterprise Apps for iOS 4 Devices, (<a href="http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html">http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598:</p> <p><b>"Certificate Validation.</b> The first time an application is opened on a device, the distribution certificate is validated by contacting Apple's OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a response from the OCSP server is not interpreted as a revocation. To verify the status, the device must be able to reach ocspp.apple.com. See 'Network Configuration Requirements.'</p> <p>The OCSP response is cached on the device for the period of time specified by the OCSP server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a revocation is received at that time, the app will be prevented from running. Note that revoking a distribution certificate will invalidate all of the applications you have distributed.</p> <p>An app will not run if the distribution certificate has expired. Currently, distribution certificates are valid for one year. A few weeks before your certificate expires request a new distribution certificate from the Dev Center, use it create new distribution provisioning profiles, then recompile and distribute the updated apps to your users. See 'Providing Updated Apps.'"</p> <p><i>See also</i> iPhone in Business: Security Overview, MOTO-APPLE-0006037953_126666:</p>

‘737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p><b>Mandatory Code Signing</b>                      All iPhone applications must be signed. The applications provided with the device are signed by Apple. Third-party applications are signed by the developer using an Apple-issued certificate. This ensures that applications haven't been tampered with or altered. Additionally, runtime checks are made to ensure that an application hasn't become untrusted since it was last used.</p> <p><i>See also iPhone in Business: Digital Certificates, MOTO-APPLE-0006037953_126669:</i></p> <p><b>Digital certificates</b>                      Digital certificates can be used to securely authenticate users to corporate services without the need for user names, passwords or soft tokens. On iPhone, certificate-based authentication is supported for access to Microsoft Exchange ActiveSync, VPN, and Wi-Fi networks.</p>  <p>The diagram illustrates a secure authentication process. On the left, a 'Certificate Authority' (represented by a server icon) issues a certificate to an iPhone. The iPhone then sends an 'Authentication Request' (indicated by a dashed arrow) to 'Enterprise Services' (represented by a server rack icon), which includes 'Intranet, Email, VPN, Wi-Fi'. Finally, the Enterprise Services connect to a 'Directory Service' (represented by a server icon with a key icon).</p> <p><u>Communications with the Apple App store.</u> In connection with a request to use software on or download software onto an Accused Apple Product, an authorization element coupled to the processor of that Accused Apple Product requests usage authorization for utilizing that software in the Accused Apple Product. The authorization element within the Accused Apple Product generates an external authorization request in order to secure this authorization.</p> <p><i>See also e.g., Email from Dallas De Atley, dated December 14, 2010, 745-Apple10360097-98:</i></p>

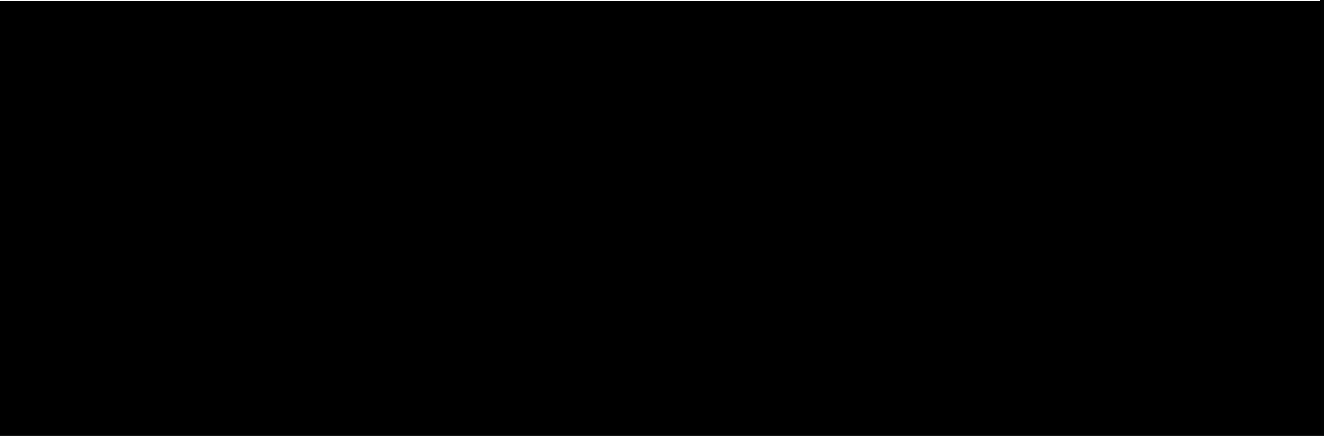
'737 Patent Claim	Accused Apple Products <sup>3</sup>
	 <p data-bbox="590 737 1577 773"><i>See also e.g., iTunes Authentication Use Case Chart, 745-Apple5374978-81:</i></p>

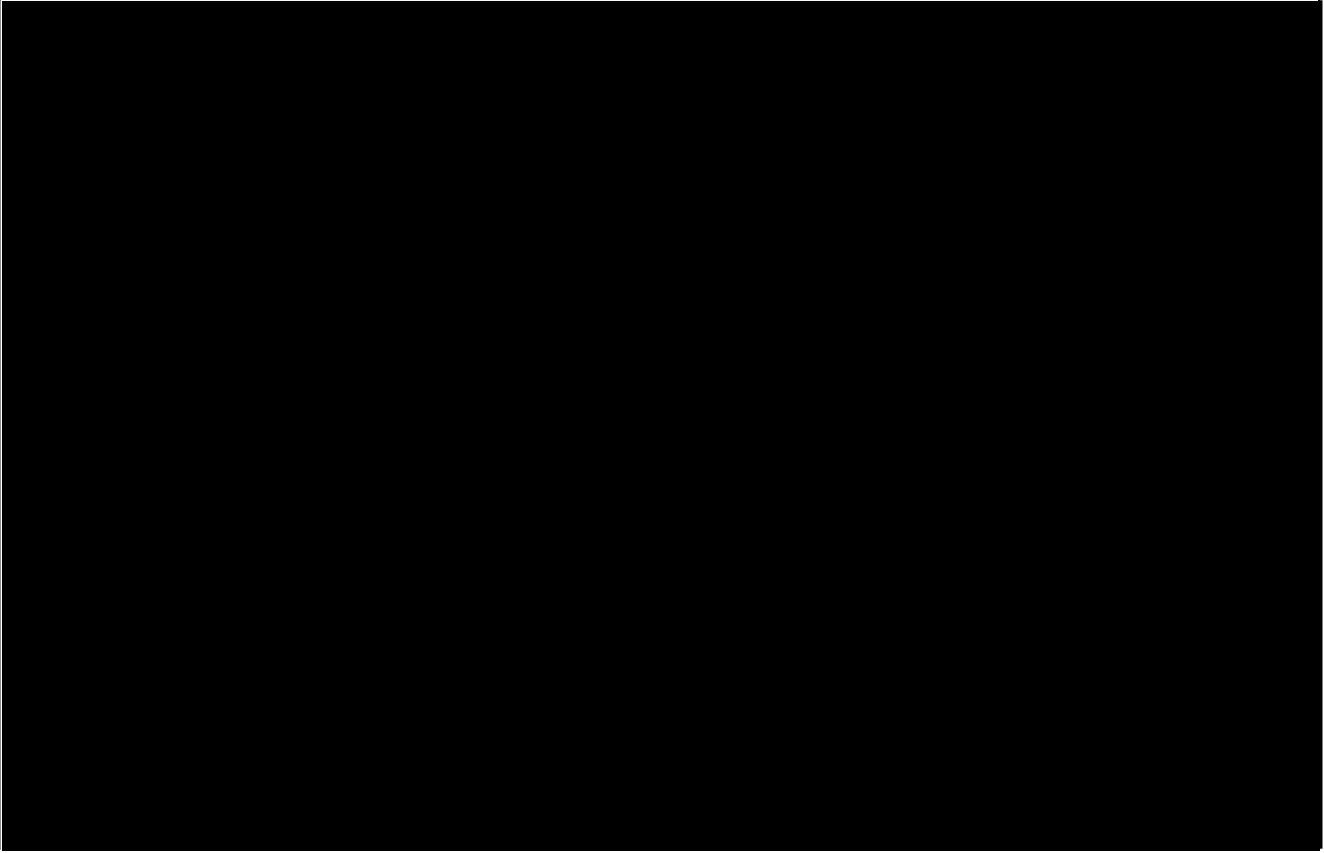
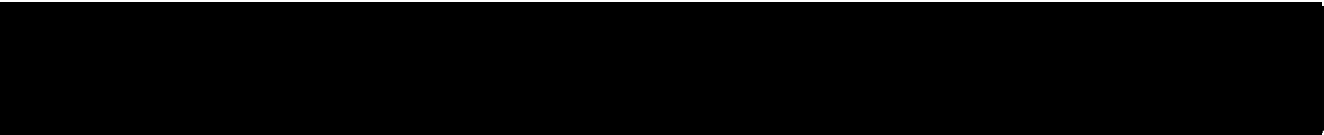
'737 Patent Claim	Accused Apple Products <sup>3</sup>
	 <p data-bbox="598 1144 1806 1185"><i>See also e.g.</i>, Email from Henri Lamiraux, dated December 13, 2010, 745-Apple10362501-32:</p>  <p data-bbox="598 1380 1543 1421"><i>See also e.g.</i> iPhone SDK, dated October 4, 2007, 745-Apple8563808-27;</p>

‘737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p><a href="http://support.apple.com/kb/HT1420">http://support.apple.com/kb/HT1420</a>; <a href="http://support.apple.com/kb/HT2204?viewlocale=en_US">http://support.apple.com/kb/HT2204?viewlocale=en_US</a>; <a href="http://support.apple.com/kb/HE37">http://support.apple.com/kb/HE37</a>; 745-Apple5375102-04</p>
<p>in which the authorization element communicates with the fixed portion to obtain the usage authorization in response to the external authorization request, and</p>	<p>Upon information and belief, the authorization element in the Accused Apple Products communicates with the fixed portion (<i>i.e.</i>, the authentication server for Apple's iTunes, Apple's App Store and / or Apple's enterprise application system) to obtain the usage authorization in response to the external authorization request. For example, the digital certificate (authorization element) is validated by contacting an external OCSP server (communication to fixed portion to obtain usage authorization) upon initial opening, and by a runtime check (external authorization request) at each time of use.</p> <p><i>See, e.g.</i>, Distributing Enterprise Apps for iOS 4 Devices, (<a href="http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html">http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598:</p> <p><b>"Certificate Validation.</b> The first time an application is opened on a device, the distribution certificate is validated by contacting Apple's OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a response from the OCSP server is not interpreted as a revocation. To verify the status, the device must be able to reach ocspl.apple.com. See 'Network Configuration Requirements.'</p> <p>The OCSP response is cached on the device for the period of time specified by the OCSP server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a revocation is received at that time, the app will be prevented from running. Note that revoking a distribution certificate will invalidate all of the applications you have distributed.</p> <p>An app will not run if the distribution certificate has expired. Currently, distribution certificates are valid for one year. A few weeks before your certificate expires request a new distribution certificate from the Dev Center, use it create new distribution provisioning profiles, then recompile and distribute the updated apps to your users. See 'Providing Updated Apps.'"</p>

‘737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p><i>See also</i> iPhone in Business: Security Overview, MOTO-APPLE-0006037953_126666:</p> <p><b>Mandatory Code Signing</b>                      All iPhone applications must be signed. The applications provided with the device are signed by Apple. Third-party applications are signed by the developer using an Apple-issued certificate. This ensures that applications haven't been tampered with or altered. Additionally, runtime checks are made to ensure that an application hasn't become untrusted since it was last used.</p> <p><i>See also</i> iPhone in Business: Digital Certificates, MOTO-APPLE-0006037953_126669:</p> <p><b>Digital certificates</b>                      Digital certificates can be used to securely authenticate users to corporate services without the need for user names, passwords or soft tokens. On iPhone, certificate-based authentication is supported for access to Microsoft Exchange ActiveSync, VPN, and Wi-Fi networks.</p>  <p>The diagram illustrates the authentication process. On the left, a 'Certificate Authority' icon is shown with a dashed arrow pointing to an iPhone icon labeled 'Authentication Request'. The iPhone is emitting wireless signals. A dashed arrow then points from the iPhone to a server rack icon labeled 'Enterprise Services Intranet, Email, VPN, Wi-Fi'. Finally, a dashed arrow points from the server rack to a 'Directory Service' icon on the right, which includes a person icon and a key icon.</p> <p><u>Communications with the Apple App store.</u> In connection with a request to use software on or download software onto an Accused Apple Product, an authorization element coupled to the processor of that Accused Apple Product requests usage authorization for utilizing that software in the Accused Apple Product. The authorization element within the Accused Apple Product generates an external authorization request in order to secure this authorization. The authorization element communicates with Apple servers to obtain the usage authorization in response to the external authorization request.</p> <p><i>See also e.g.</i>, Email from Dallas De Atley, dated December 14, 2010, 745-Apple10360097-98:</p>

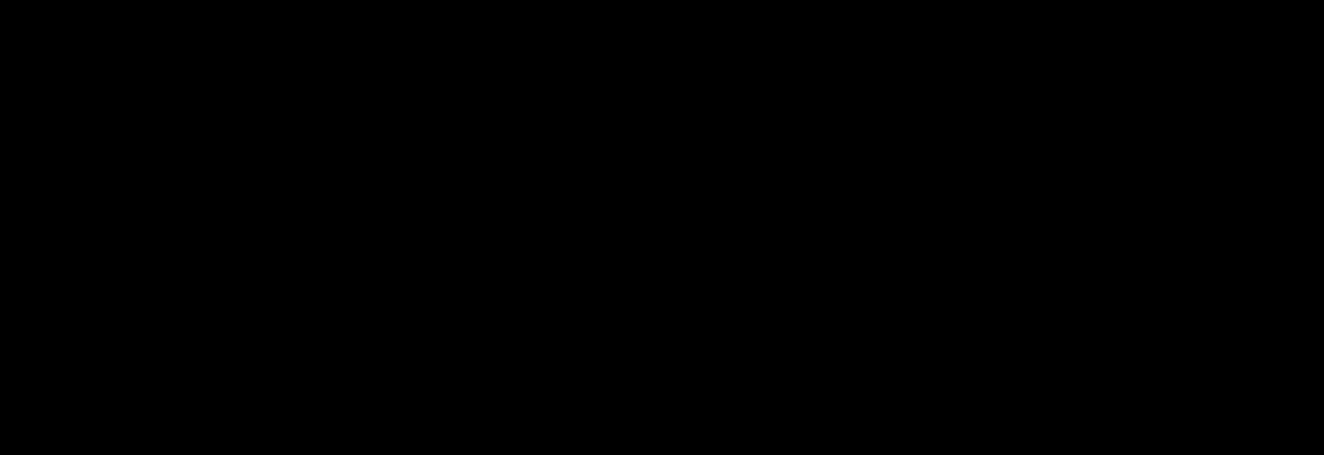


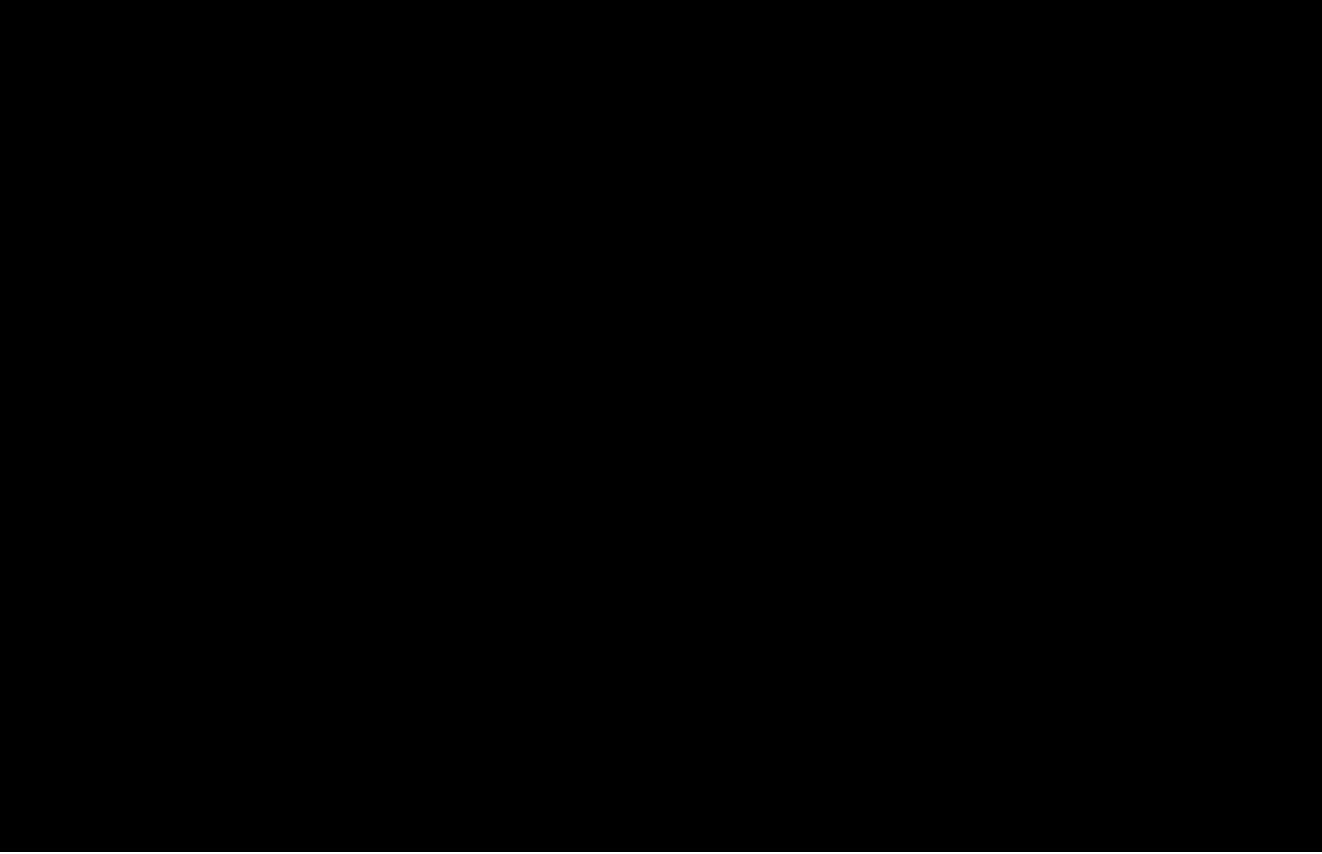

'737 Patent Claim	Accused Apple Products <sup>3</sup>
	 <p data-bbox="596 737 1864 876"><i>See also e.g., iTunes Authentication Use Case Chart, 745-Apple5374978-81</i><a href="http://support.apple.com/kb/HT1420">http://support.apple.com/kb/HT1420</a><a href="http://support.apple.com/kb/HT1420">http://support.apple.com/kb/HT1420</a><a href="http://support.apple.com/kb/HT2204?viewlocale=en_US">http://support.apple.com/kb/HT2204?viewlocale=en_US</a><a href="http://support.apple.com/kb/HT2204?viewlocale=en_US">http://support.apple.com/kb/HT2204?viewlocale=en_US</a><a href="http://support.apple.com/kb/HE37">http://support.apple.com/kb/HE37</a><a href="http://support.apple.com/kb/HE37">http://support.apple.com/kb/HE37</a>:</p>

'737 Patent Claim	Accused Apple Products <sup>3</sup>
	 <p data-bbox="598 1149 1795 1182"><i>See also e.g.</i>, Email from Henri Lamiraux, dated December 13, 2010, 745-Apple10362501-32</p>  <p data-bbox="598 1385 1537 1417"><i>See also e.g.</i> iPhone SDK, dated October 4, 2007, 745-Apple8563808-27;</p>


‘737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p><a href="http://support.apple.com/kb/HT1420">http://support.apple.com/kb/HT1420</a>; <a href="http://support.apple.com/kb/HT2204?viewlocale=en_US">http://support.apple.com/kb/HT2204?viewlocale=en_US</a>; <a href="http://support.apple.com/kb/HE37">http://support.apple.com/kb/HE37</a>; 745-Apple5375102-04.</p>
<p>in which the external authorization request includes at least one of: an address identifying the portable communication device, a software name and a size of the software; and</p>	<p>Upon information and belief, the external authorization request includes at least one of: an address identifying the portable communication device, a software name and a size of the software.</p> <p>For example, an X.509 digital certificate for an iPhone 4 “enforces a trust policy referred to as the S/MIME policy, which specifies that in order to be trusted to verify a digitally signed email, a certificate must contain an email address that matches the address of the sender of the email.” Security Concepts, (<a href="http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/Concepts/Concepts.html">http://developer.apple.com/library/ios/#documentation/Security/Conceptual/Security_Overview/Concepts/Concepts.html</a>), accessed on May 13, 2011, MOTO-APPLE-0006037953_126611.</p> <p><i>See id.</i> at MOTO-APPLE-0006037953_126608:</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, an X.509 certificate contains such information as:</p> <ul style="list-style-type: none"> <li>• Version</li> <li>• Serial number</li> <li>• Certificate issuer</li> <li>• Certificate holder</li> <li>• Validity period (the certificate is not valid before or after this period)</li> <li>• Attributes, known as certificate extension, that contain additional information such as allowable uses for this certificate</li> <li>• Digital signature from the certification authority to ensure that the certificate has not been altered and to indicate the identity of the issuer</li> <li>• Public key of the owner of the certificate</li> <li>• Message digest algorithm used to create the signature."</li> </ul> <p><i>See also</i> Distributing Enterprise Apps for iOS 4 Devices, (<a href="http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Int">http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Int</a></p>

‘737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p><a href="#">roduction/Introduction.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598:</p> <p><b>"Certificate Validation.</b> The first time an application is opened on a device, the distribution certificate is validated by contacting Apple's OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a response from the OCSP server is not interpreted as a revocation. To verify the status, the device must be able to reach ocsf.apple.com. See 'Network Configuration Requirements.'</p> <p>The OCSP response is cached on the device for the period of time specified by the OCSP server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a revocation is received at that time, the app will be prevented from running. Note that revoking a distribution certificate will invalidate all of the applications you have distributed.</p> <p>An app will not run if the distribution certificate has expired. Currently, distribution certificates are valid for one year. A few weeks before your certificate expires request a new distribution certificate from the Dev Center, use it create new distribution provisioning profiles, then recompile and distribute the updated apps to your users. See 'Providing Updated Apps.'"</p> <p><u>Communications with the Apple App store.</u> In connection with a request to use software on or download software onto an Accused Apple Product, an authorization element coupled to the processor of that Accused Apple Product requests usage authorization for utilizing that software in the Accused Apple Product. The authorization element within the Accused Apple Product generates an external authorization request in order to secure this authorization. The external authorization request includes at least one of: an address identifying the portable communication device, a software name and a size of the software.</p> <p><i>See also e.g.,</i> Email from Dallas De Atley, dated December 14, 2010, 745-Apple10360097-98:</p>


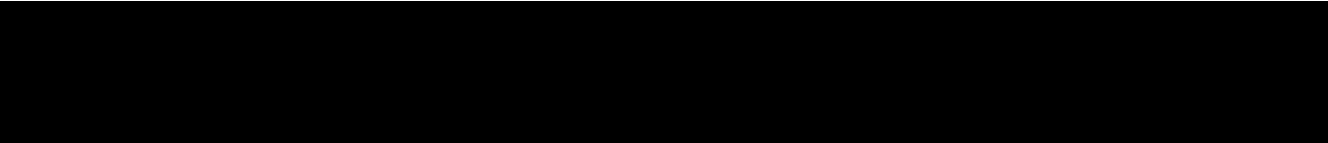
'737 Patent Claim	Accused Apple Products <sup>3</sup>
	 <p data-bbox="596 737 1577 773"><i>See also e.g., iTunes Authentication Use Case Chart, 745-Apple5374978-81:</i></p>

'737 Patent Claim	Accused Apple Products <sup>3</sup>
	 <p data-bbox="598 1149 1801 1182"><i>See also e.g.</i>, Email from Henri Lamiraux, dated December 13, 2010, 745-Apple10362501-32:</p>  <p data-bbox="598 1385 1535 1417"><i>See also e.g.</i> iPhone SDK, dated October 4, 2007, 745-Apple8563808-27;</p>

‘737 Patent Claim	Accused Apple Products <sup>3</sup>
	<p><a href="http://support.apple.com/kb/HT1420">http://support.apple.com/kb/HT1420</a>; <a href="http://support.apple.com/kb/HT2204?viewlocale=en_US">http://support.apple.com/kb/HT2204?viewlocale=en_US</a>; <a href="http://support.apple.com/kb/HE37">http://support.apple.com/kb/HE37</a>; 745-Apple5375102-04.</p>
<p>second authorization element coupled to the processor for allowing utilization of the software, in response to usage authorization being obtained from the fixed portion.</p>	<p>Upon information and belief, the Accused Apple Products contain a second authorization element coupled to the processor for allowing utilization of the software, in response to an authorization being obtained from the fixed portion.</p> <p>For example, the iPhone 4 software application is allowed to run (second authorization element) once the digital certificate is authorized (usage authorization obtained from fixed portion).</p> <p><i>See, e.g.,</i> Distributing Enterprise Apps for iOS 4 Devices, (<a href="http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html">http://developer.apple.com/library/ios/#featuredarticles/FA_Wireless_Enterprise_App_Distribution/Introduction/Introduction.html</a>), accessed on May 12, 2011, MOTO-APPLE-0006037953_126598:</p> <p><b>"Certificate Validation.</b> The first time an application is opened on a device, the distribution certificate is validated by contacting Apple's OCSP server. Unless the certificate has been revoked, the app is allowed to run. Inability to contact or get a response from the OCSP server is not interpreted as a revocation. To verify the status, the device must be able to reach <a href="http://ocsp.apple.com">ocsp.apple.com</a>. See 'Network Configuration Requirements.'</p> <p>The OCSP response is cached on the device for the period of time specified by the OCSP server; currently between 3 and 7 days. The validity of the certificate will not be checked again until the device has restarted and the cached response has expired. If a revocation is received at that time, the app will be prevented from running. Note that revoking a distribution certificate will invalidate all of the applications you have distributed.</p> <p>An app will not run if the distribution certificate has expired. Currently, distribution certificates are valid for one year. A few weeks before your certificate expires request a new distribution certificate from the Dev Center, use it create new distribution provisioning profiles, then recompile and distribute the updated apps to your users. See 'Providing Updated Apps.'"</p> <p><u>Communications with the Apple App store.</u> In connection with a request to use software on or download software onto an Accused Apple Product, an authorization element coupled to the</p>

<b>'737 Patent Claim</b>	<b>Accused Apple Products<sup>3</sup></b>
	<p>processor of that Accused Apple Product requests usage authorization for utilizing that software in the Accused Apple Product. The authorization element within the Accused Apple Product generates an external authorization request in order to secure this authorization. The Accused Apple Products contain a second authorization element coupled to the processor for allowing utilization of the software, in response to usage authorization being obtained from Apple's servers.</p> <p><i>See also e.g.,</i> Email from Dallas De Atley, dated December 14, 2010, 745-Apple10360097-98:</p>  <p><i>See also e.g.,</i> iTunes Authentication Use Case Chart, 745-Apple5374978-81:</p>



'737 Patent Claim	Accused Apple Products <sup>3</sup>
	 <p data-bbox="594 1149 1806 1182"><i>See also e.g.</i>, Email from Henri Lamiraux, dated December 13, 2010, 745-Apple10362501-32:</p>  <p data-bbox="594 1385 1537 1417"><i>See also e.g.</i> iPhone SDK, dated October 4, 2007, 745-Apple8563808-27;</p>

<b>'737 Patent Claim</b>	<b>Accused Apple Products<sup>3</sup></b>
	<a href="http://support.apple.com/kb/HT1420">http://support.apple.com/kb/HT1420</a> ; <a href="http://support.apple.com/kb/HT2204?viewlocale=en_US">http://support.apple.com/kb/HT2204?viewlocale=en_US</a> ; <a href="http://support.apple.com/kb/HE37">http://support.apple.com/kb/HE37</a> ; 745-Apple5375102-04.