

EXHIBIT D

CLAIM CHART – U.S. PATENT NO. 8,646,042
APPLE PASSKEYS

Assignee:	Proxense, LLC
Title:	Hybrid device having a personal digital key and receiver-decoder circuit and methods of use
Filing Date:	2012-04-12
Publication Date:	2014-02-04
Inventor:	Brown, David L.

042 Patent Claim ¹		Accused Instrumentality and Where Each Claim Element Is Found ²
1	A hybrid device comprising ³ :	This preamble is not limiting. Apple manufactures, imports, offers for sale, and sells in the United States mobile phones with the iOS 15+ operating system that include an integrated personal digital key and an integrated receiver decoder circuit. (“In macOS Monterey and iOS 15, we announced a developer preview of the solution -- passkeys -- and got so much great feedback. In macOS Ventura and iOS 16, we're excited to make passkeys available to everyone. Now is the time to adopt them.” Meet passkeys - WWDC22 - Videos - Apple Developer).
	an integrated personal digital key (PDK) for storing information and capable of communicating wirelessly with	<u>an integrated personal digital key (PDK)</u> Apple iPhones with iOS 15 and later operating systems enable the use of passkeys by utilizing an integrated personal digital key (PDK).

¹ All PICS set forth herein for any independent patent claims are hereby incorporated by reference into the PICS alleged for any dependent patent claims that depend on such independent claims, as if fully set forth therein.

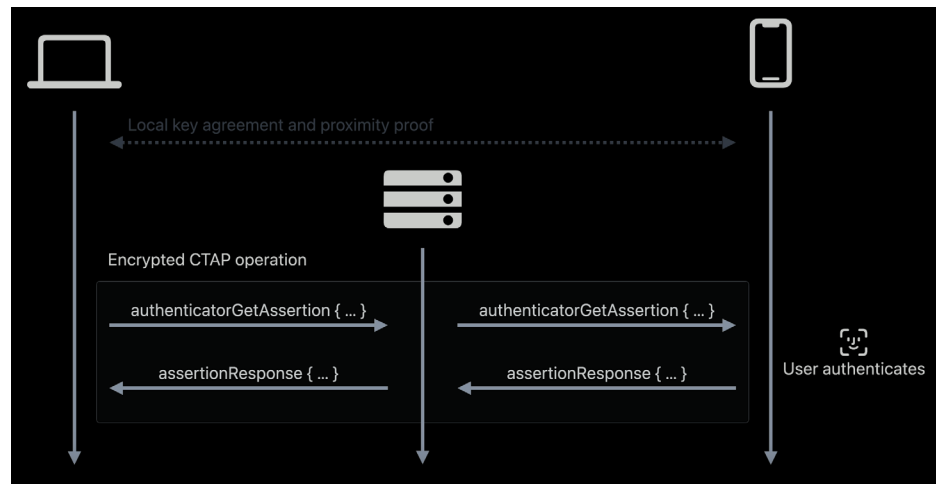
² The Accused Instrumentalities and associated exhibits discussed and/or cited for any claim herein are representative in all material respects of all other accused instrumentalities identified for that claim (e.g., a specified device or service may be used as a representative example in these charts since the other accused instrumentalities have immaterial differences in their hardware and/or software configuration, the cited references are believed to be illustrative of all such accused devices).

³ Plaintiff's inclusion of any claim preamble in this claim chart should not be interpreted as an admission that the preamble is limiting. Plaintiff reserves the right to take the position that the claim preambles are limiting or not limiting on a claim-by-claim basis.

at least one external receiver-decoder circuit (RDC); and	The 042 Patent defines a PDK as including “an antenna and a transceiver for communicating with an R[ecceiver] D[ecoder] C[ircuit] (not shown) and a controller and memory for storing information particular to a user.” 042 Patent, 13: 46-49. A component of the integrated PDK of the hybrid device, accordingly, is “a controller and memory for storing information particular to a user.” The 042 Patent defines the operation of the controller and memory for storing information particular to the user as entailing the receipt of an access key from an external application that is used to access a specific service block. 042 Patent, 6:23-27 (“Regardless of how created, once created, external applications (such as applications 120 in FIG. 1) can gain access to specific service block 112 by providing the corresponding access key 118. In FIG. 2., this is shown conceptually by control logic 250.”) The integrated PDK of the hybrid device, therefore, includes a controller placing within memory information that can only be accessed by a corresponding access key provided by an external application. Such memory is present in Apple iPhones with iOS 15, and later, because it is required by the standard. “Passkeys are built on the WebAuthentication -- or WebAuthn standard -- and use public-key cryptography.” Meet passkeys - WWDC22 - Videos - Apple Developer. Under the WebAuthn specification, “compliant authenticators protect public key credentials.” Web Authentication: An API for accessing Public Key Credentials - Level 2 (w3.org), § 1. A public key credential refers to a public key credential source, which includes a credential ID. Web Authentication: An API for accessing Public Key Credentials - Level 2 (w3.org), § 4 (Defining “public key credential” and “public key credential source.”). The credential ID uniquely identifies its public key credential source. Web Authentication: An API for accessing Public Key Credentials - Level 2 (w3.org), § 4 (Defining a credential ID as “A probabilistically-unique byte sequence identifying a public key credential source and its authentication assertions.”). In addition to the credential ID, each public key credential source contains a “credential private key.” Web Authentication: An API for accessing Public Key Credentials - Level 2 (w3.org), § 4, (Defining “public key credential source” as data structure including the credential private key and the credential ID.). “The credential private key is bound to a particular authenticator” and part of an asymmetric key pair containing a public key
--	---

		returned to a relying party. Web Authentication: An API for accessing Public Key Credentials - Level 2 (w3.org), § 4 (Defining a “credential key pair.”). Every Apple iPhone with iOS 15 and later, therefore, will store within memory a credential comprising a private key of an asymmetric key pair and a credential ID uniquely identifying the private/public key pair to which the private key belongs. The credentials stored within Apple iPhones with iOS 15 and later can only be accessed with the appropriate access key. “A public key credential can only be used for authentication with the same entity (as identified by the RP ID) it was registered with.” Web Authentication: An API for accessing Public Key Credentials - Level 2 (w3.org), § 4 (“A public key credential can only be used for authentication with the same entity (as identified by RP ID) it was registered with.”). When generating a response, therefore, the authenticator will only retrieve credentials corresponding to the RP ID provided to it by the external server. Client to Authenticator Protocol (CTAP) (fidoalliance.org), § 6.2.2 (“7.1 If the allowList parameter is present and is non-empty, locate all denoted credentials created by this authenticator and bound to the specified rpId. 7.2 If an allowList is not present, locate all discoverable credentials that are created by this authenticator and bound to the specified rpId.”). As only credentials corresponding to the RP ID will be retrieved, the RP ID is an access key. As Apple states it, “the system will take care of only letting me use it in the correct app or website, with strong built-in phishing resistance.” Meet passkeys - WWDC22 - Videos - Apple Developer. As Apple iPhones will only return credentials corresponding to the RP ID access key provided by the external relying party, Apple iPhones with iOS 15 and later have the controller and memory necessary for a minimal embodiment of a PDK. In addition to the controller and memory, a minimal embodiment of PDK is defined by the 042 Patent as including “an antenna and a transceiver for communication with an RDC.” 042 Patent, 13:46-48. With an Apple iPhone with iOS 15 or later, “Passkeys can also be used to sign in across devices in a secure, phishing-resistant manner. Here's how that works. There are two devices here. The client, which is the device or web browser where I'm signing in, and the authenticator, which is the device which has my passkey. First, the client shows a QR code, which the authenticator scans. This QR
--	--	---

code contains a URL that encodes a pair of single-use encryption keys. Then, the authenticator produces a Bluetooth advertisement containing routing information for a network relay server. Once the local exchange and key agreement have happened, the two devices connect to a relay server picked by the phone. From there, they perform a standard FIDO CTAP operation, which is encrypted using the keys from earlier, so the relay server can't see anything that's going on. This whole process is performed by the device and the web browser. The website is not involved at any point in the cross-device communication.” [Meet passkeys - WWDC22 - Videos - Apple Developer](#). The process is shown in the below figure.



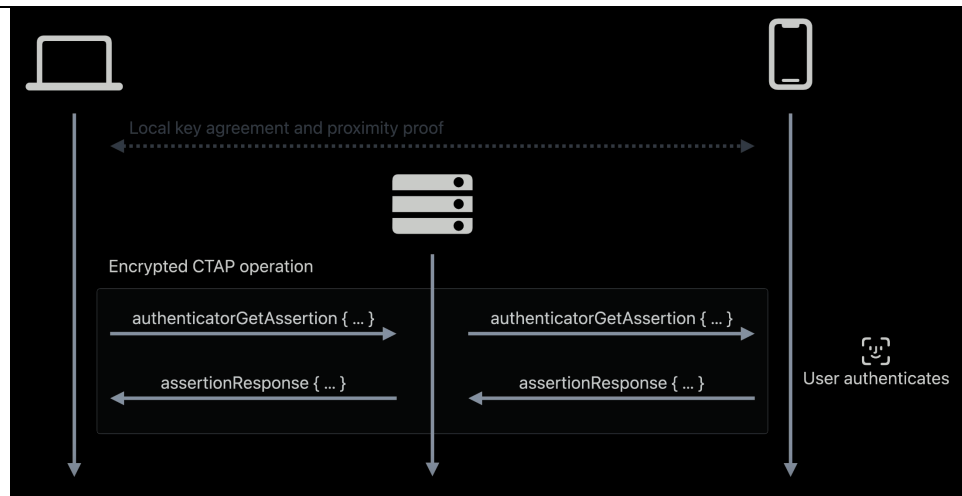
[Meet passkeys - WWDC22 - Videos - Apple Developer](#).

Establishing the connection over the internet requires utilizing either the device's Wi-Fi or cellular capabilities – both of which are wireless protocols. Accordingly, iPhones with iOS 15 and later have the antenna and transceiver necessary to implement the wireless protocols enabling transmission over the internet.

Having each of the elements of a minimal embodiment of a PDK, Apple iPhones with iOS 15 and later include an integrated PDK.

		<u>storing information</u> Apple iPhones with iOS 15 later store information for authenticating users. “Passkeys are a replacement for passwords. They are faster and easier to sign in. Just use Touch ID or Face ID to authenticate and you're done.” Deploy passkeys at work - WWDC23 - Videos - Apple Developer. “Apple platforms will always require UV for passkeys when biometrics are available, so you don't have to worry about that.” Meet passkeys - WWDC22 - Videos - Apple Developer. Accordingly, Apple iPhones with iOS 15 and later locally store biometric information for authenticating user. Apple iPhones utilize the Secure Enclave to securely store the biometric information for authentication. “During enrollment, the Secure Enclave processes, encrypts, and stores the corresponding Touch ID and Face ID template data.” Apple Platform Security, page 19. Apple has described the Secure Enclave thusly: “When you store a private key in the Secure Enclave, you never actually handle the key, making it difficult for the key to become compromised. Instead, you instruct the Secure Enclave to create the key, securely store it, and perform operations with it. You receive only the output of these operations, such as encrypted data or a cryptographic signature verification outcome.” Protecting Keys with the Secure Enclave, https://developer.apple.com/documentation/security/certificate_key_and_trust_services/keys/protecting_keys_with_the_secure_enclave “The Secure Enclave is a dedicated secure subsystem ... isolated from the main processor to provide an extra layer of security designed to keep sensitive data secure even when the Application Processor kernel becomes compromised.” Apple Platform Security, page 9. Protected even when a hack or malware comprises the Application Processor, the biometric data for Touch ID and Face ID are securely stored. <u>capable of communicating wirelessly with at least one external receiver-decoder circuit (RDC)</u>
--	--	--

		As detailed above, Apple iPhones with iOS 15 or later enable the use of passkeys to sign in across devices in a secure, phishing-resistant manner by utilizing either the device's Wi-Fi or cellular capabilities – both of which are wireless protocols. Consequently, Apple iPhones with iOS 15 and later are capable of communicating wirelessly with an external receiver decoder circuit.
	an integrated RDC for communicating wirelessly with at least one external PDK within a proximity zone, the integrated RDC coupled to the integrated PDK by a first signal line for communication, the integrated RDC coupled to at least one other component of the hybrid device by a second signal line, one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service on one or more of the hybrid device and a device associated with the external RDC.	<u>an integrated RDC for communicating wirelessly with at least one external PDK</u> As detailed above, Apple iPhones with iOS 15 and later communicate passkey signatures over an encrypted connection, through the internet, via Wi-Fi, and/or cellular protocols. Accordingly, Apple iPhones with iOS 15 and later include an RDC enabling wireless communications with at least one external device, such as a device running macOS Monterey or later requires. <u>the integrated RDC coupled to the integrated PDK by a first signal line for communication</u> Enabling the use of passkeys across devices with a QR code, Apple iPhones with iOS 15 or later include a signal line for communication that couples the integrated RDC to the integrated PDK. As noted above, using a passkey on Apple iPhone to sign into a website on external device begins by scanning a QR code. “First, the client shows a QR code, which the authenticator scans. This QR code contains a URL that encodes a pair of single-use encryption keys. Then, the authenticator produces a Bluetooth advertisement containing routing information for a network relay server. Once the local exchange and key agreement have happened, the two devices connect to a relay server picked by the phone. From there, they perform a standard FIDO CTAP operation, which is encrypted using the keys from earlier, so the relay server can't see anything that's going on. This whole process is performed by the device and the web browser. The website is not involved at any point in the cross-device communication.” Meet passkeys - WWDC22 - Videos - Apple Developer. The process is shown in the below figure.



[Meet passkeys - WWDC22 - Videos - Apple Developer.](#)

As shown in the above figure, an “authenticatorGetAssertion” is forward to the phone, which is request to provide cryptographic proof of user authentication. [Client to Authenticator Protocol \(CTAP\) \(fidoalliance.org\)](#), § 6.2 (Defining authenticatorGetAssertion as the method “used by a host to request cryptographic proof of user authentication as well as user consent to a given transaction, using a previously generated credential that is bound to the authenticator and relying party identifier.”). The authenticatorGetAssertion request contains a relying party identifier (RP ID) access key. [Client to Authenticator Protocol \(CTAP\) \(fidoalliance.org\)](#), § 6.2 (Defining the input parameters of the authenticatorGetAssertion as including a required relying party identifier.). A passkey, however, can only be used for authentication with the same entity (as identified by the RP ID) it was registered with.” [Web Authentication: An API for accessing Public Key Credentials - Level 2 \(w3.org\)](#), § 4 (“A public key credential can only be used for authentication with the same entity (as identified by RP ID) it was registered with.”). As such, the PDK on the phone must receive the RP ID access key, unlock the necessary passkey to generate cryptographic proof, and send the proof back to the external device via the relay server. The PDK within the iPhone, however, could only do so if the integrated RDC receiving the authenticatorGetAssertion and returning the cryptographic proof was communicatively

		coupled to the PDK. Apple iPhones, therefore, necessarily have the integrated RDC coupled to the integrated PDK by a first signal line for communication. <u>the integrated RDC coupled to at least one other component of the hybrid device by a second signal line</u> Apple iPhones with iOS 15 or later necessarily have a second signal line coupling the RDC to at least one other component. To function, the RDC must receive power from a battery and/or be coupled to at least one application processor or similar processing unit and/or one or more antenna. Accordingly, the 042 Patent states in Col. 14, ll. 12-14, “the cell phone components and a battery 2004 are coupled to the RDC 304a by signal line 1106.” <u>one or more of the integrated RDC and integrated PDK enabling one or more of an application, a function, and a service on one or more of the hybrid device and a device associated with the external RDC</u> When using passkeys to sign in across devices, the PDK of an iPhone with iOS 15 or later enables an authentication service. Authentication is a service provided by the relying party, and the credential ID is necessary for the relying party to perform the authentication function. Upon receiving the response, the relying party will use the credential ID to locate the appropriate public key to verify a signature generated with the private key held by the authenticator. Web Authentication: An API for accessing Public Key Credentials - Level 2 (w3.org), § 7.2 (“7. Using credential.id (or credential.rawId, if base64url encoding is inappropriate for your use case), look up the corresponding credential public key and let credentialPublicKey be that credential public key... 20. Using credentialPublicKey, verify that sig is a valid signature over the binary concatenation of authData and hash... 22. If all the above steps are successful, continue with the authentication ceremony as appropriate. Otherwise, fail the authentication ceremony.”) “[I]f an authenticator returns the wrong credential ID, or if an attacker intercepts and manipulates the credential ID, is that the WebAuthn Relying Party would not look up
--	--	--

		the correct credential public key with which to verify the returned signed authenticator data (a.k.a., assertion), and thus the interaction would end in an error.” Web Authentication: An API for accessing Public Key Credentials - Level 2 (w3.org), § 13.1. As the proper credential ID is needed for relying party to authenticate a user, and the credential ID held within the PDK of the iPhone is included within a response to the authenticatorGetAssertion request generated by the iPhone, the PDK of the iPhone is enabling authentication by relying party. The PDK of the iPhone, accordingly, enables one or more of an application, a function, and a service.
6	The hybrid device of claim 1, wherein the hybrid device is a cell phone and the hybrid device is enabled to provide cell phone service subsequent to the external PDK entering the proximity zone of the integrated RDC and based on the information stored by one or more of the external PDK and the integrated PDK.	Apple iPhones with iOS 15 or later are cell phones.