Table des matières

iMessage security overview

Apple iMessage is a messaging service for iOS and iPadOS devices, Apple Watch, and Mac computers. iMessage supports text and attachments such as photos, contacts, locations, links, and attachments directly on to a message, such as a thumbs up icon. Messages appear on all of a user's registered devices so that a conversation can be continued from any of the user's devices. iMessage makes extensive use of the Apple Push Notification service (APNs). Apple doesn't log the contents of messages or attachments, which are protected by end-to-end encryption so no one but the sender and receiver can access them. Apple can't decrypt the data.

When a user turns on iMessage on a device, the device generates encryption and signing pairs of keys for use with the service. For encryption, there is an encryption RSA 1280-bit key as well as an encryption EC 256-bit key on the NIST P-256 curve. For signatures, Elliptic Curve Digital Signature Algorithm (ECDSA) 256-bit signing keys are used. The private keys are saved in the device's keychain and only available after first unlock. The public keys are sent to Apple Identity Service (IDS), where they are associated with the user's phone number or email address, along with the device's APNs address.

As users enable additional devices for use with iMessage, their encryption and signing public keys, APNs addresses, and associated phone numbers are added to the directory service. Users can also add more email addresses, which are verified by sending a confirmation link. Phone numbers are verified by the carrier network and SIM. With some networks, this requires using SMS (the user is presented with a confirmation dialog if the SMS isn't zero rated). Phone number verification may be required for several system services in addition to iMessage, such as FaceTime and iCloud. All of the user's registered devices display an alert message when a new device, phone number, or email address is added.

Published Date: February 18, 2021

See also

iCloud security overview

iCloud Drive security

Security of iCloud Backup

Apple ID security overview

Avez-vous trouvé cet article utile ? Oui Non

Précédent
Adding transit and student ID cards to Wallet

Suivant
How iMessage sends and receives messages

Copyright © 2021 Apple Inc. Tous droits réservés.