Authentication Services / Public-Private Key Authentication

API Collection

Public-Private Key Authentication

Register and authenticate users with passkeys and security keys, without using passwords.

Overview

Eliminating passwords simplifies account creation and authentication for apps and websites. Additionally, it reduces risks that arise from the reuse of one password across multiple services, brute force attacks, and social engineering that bad actors use to obtain credential information. By implementing public-private authentication according to the W3C Web Authentication specification, your users no longer need to remember complicated passwords or rely on password managers.

Instead of using a password, your macOS, iOS, or iPadOS device, known as the *authenticator*, generates a public-private key pair at account creation time, and sends the public key to the server. The server, known as the *relying party*, holds the public key for subsequent authentication, and uses *assertion* to challenge the authenticator to prove its identity is valid.

There are two forms of public-private key authentication: *passkeys* and *security keys*. With passkeys, the device stores its public-private key pair in the user's iCloud Keychain and syncs the keys across the user's devices. Security keys store the public-private key pair on a physical medium, such as a security card or a USB key.

Topics

Fundamentals

{} Connecting to a service with passkeys

Allow users to sign in to a service without typing a password.

Supporting passkeys

Eliminate passwords for your users when they sign in to apps and websites.

Supporting Security Key Authentication Using Physical Keys

Allow users to authenticate using NFC, USB, and Lightning security keys in your app or service.

Account registration

`protocol ASAuthorizationPublicKeyCredentialRegistration`

An interface that credential registration requests adhere to.

`class ASAuthorizationPlatformPublicKeyCredentialRegistration`

A newly created platform credential that results from a credential registration request.

`class ASAuthorizationSecurityKeyPublicKeyCredentialRegistration`

A newly created security key credential that results from a credential registration request.

`protocol ASAuthorizationPublicKeyCredentialRegistrationRequest`

An interface that defines properties for a credential registration request.

`class ASAuthorizationPlatformPublicKeyCredentialRegistrationRequest`

The object for registering a new platform public key credential.

`class ASAuthorizationSecurityKeyPublicKeyCredentialRegistrationRequest`

The object for registering a new security key credential.

Account authentication

`protocol ASAuthorizationPublicKeyCredentialAssertion`

An interface for establishing a public key-based assertion.

`class ASAuthorizationPlatformPublicKeyCredentialAssertion`

A class that represents the platform credential assertion type.

`class ASAuthorizationSecurityKeyPublicKeyCredentialAssertion`

A class that represents the security key credential assertion type.

`protocol ASAuthorizationPublicKeyCredentialAssertionRequest`

An interface for requesting a public key-based credential assertion.

`class ASAuthorizationPlatformPublicKeyCredentialAssertionRequest`

The concrete assertion request type for platform credentials.

`class ASAuthorizationSecurityKeyPublicKeyCredentialAssertionRequest`

A class that defines the assertion request type for security key credentials.

Credential providers

`class ASAuthorizationPlatformPublicKeyCredentialProvider`

A mechanism for providing public key credential requests to an app or service with iCloud Keychain.

`class ASAuthorizationSecurityKeyPublicKeyCredentialProvider`

A mechanism for providing public key credential requests to an app or service with a physical security key.

Request configuration

`protocol ASPublicKeyCredential`

An interface that defines the properties of the public key.

`class ASAuthorizationPublicKeyCredentialParameters`

An object that provides required parameters for the credential during registration.

`struct ASCOSEAlgorithmIdentifier`

An identifier for the algorithm that a credential’s key pair uses.

`struct ASCOSEEllipticCurveIdentifier`

A structure that contains the elliptic curve identifier.

`struct ASAuthorizationPublicKeyCredentialAttestationKind`

A structure that defines the types of attestations a developer can request.

`struct ASAuthorizationPublicKeyCredentialResidentKeyPreference`

A structure that specifies the relying party’s preference for resident key storage.

`struct ASAuthorizationPublicKeyCredentialUserVerificationPreference`

A structure that defines the relying party’s user verification preference.

`protocol ASAuthorizationPublicKeyCredentialDescriptor`

An interface that defines the credential identifier.

`class ASAuthorizationPlatformPublicKeyCredentialDescriptor`

An object that holds the credential.

`class ASAuthorizationSecurityKeyPublicKeyCredentialDescriptor`

An object that holds public key credential transport information.

`struct Transport`

A structure that defines the security key credential transport type.

`static var allSupported: [ASAuthorizationSecurityKeyPublicKeyCredentialDescriptor.Transport]`

An array of currently supported transport types.

See Also

Passkeys

Passkey use in web browsers

Register and authenticate website users by using passkeys.

Performing fast account creation with passkeys

Allow people to quickly create an account with passkeys and associated domains.

Connecting to a service with passkeys

Allow users to sign in to a service without typing a password.