KEYCHAIN

Keychain is **Apple's secure storage system** used to store sensitive information

by Shubam Gupta

Keychain is used to store sensitive information such as:

- **Passwords**
- **Tokens** (JWT, access tokens)
- **API keys**
- **Certificates**
- **Credentials**

It is encrypted, system-managed, and hardware-backed.

Why Prefer Keychain?

Because UserDefaults, plist, CoreData are NOT secure.

Keychain provides:

✅ Encryption at rest
✅ Protection via device passcode / biometrics
✅ **Secure Enclave** support
✅ Data isolation per app
✅ Persistence across app reinstalls (by default)

👉 **Best choice for sensitive data**

Alternatives to Keychain (and why they’re weaker)

Storage	Use Case	Security
UserDefaults	App settings	❌ Not secure
CoreData / SQLite	App data	❌ Not encrypted
File system	Caching	❌ Easy to extract
Keychain	Credentials	✅ Highly secure

👉 **Rule of thumb**:

If it’s sensitive → use Keychain

What Makes Keychain Special?

- Managed by iOS system
- Uses AES encryption
- Can be protected by Face ID / Touch ID
- Data can be tied to device-only
- Access controlled via Keychain Accessibility options

Keychain Accessibility Options

Examples:

- **kSecAttrAccessibleWhenUnlocked**
- **kSecAttrAccessibleAfterFirstUnlock**
- **kSecAttrAccessibleWhenPasscodeSetThisDeviceOnly**

👉 Controls when & where data is accessible

What Encryption Does Keychain Use?

- Uses AES (Advanced Encryption Standard)
- Keys are protected by:
    - Secure Enclave
    - Device passcode
    - Hardware UID (unique per device)

👉 Even Apple cannot read your Keychain data

Why Keychain?

*"Because it's **encrypted**, **system-managed**, and **secure** for **sensitive data**."*

Q1: If app is uninstalled, does Keychain data remain?

✅ Yes, by default

- Keychain data persists even after app uninstall
- Useful for:
    - Auto-login
    - Remembered credentials

⚠️ Unless explicitly deleted by the app

Q2: Is it safe to keep data after uninstall?

✅ Yes — but only when needed

- Tokens
- Login info
- Secure identifiers

❌ Do NOT store unnecessary or stale data

Q3. Does Keychain sync across devices?

✅ Yes — if iCloud Keychain is enabled

- User-controlled
- App-controlled using access groups

Q4: What if iPhone or iOS is corrupted?

- If Secure Enclave is intact → data is safe
- If device is factory reset / wiped → Keychain data is erased
- iTunes restore may or may not restore Keychain (depends on backup type)

Q5: How do we delete Keychain data?

You must explicitly delete it:

```
SecItemDelete(query as CFDictionary)
```

Best practice:

- Clear Keychain on **logout**
- Clear sensitive tokens on **account switch**

🎯 Final One-Line Summary

“Keychain is the safest place in iOS to store sensitive data - persistent, encrypted, and system-managed.”

👍 FOLLOW US

Thank you

by Shubam Gupta