

公的個人認証サービス

利用者クライアントソフト API 仕様書

【Mac OS X C 言語 IF 編】

第 1.3 版

公的個人認証サービス 指定認証機関

財団法人 自治体衛星通信機構

変更履歴

版数	変更日付	変更内容
1.0 版	平成 18 年 11 月 1 日	新規作成
1.1 版	平成 19 年 4 月 10 日	表 3-1 動作環境 を変更
1.2 版	平成 19 年 10 月 4 日	表 3-1 動作環境 プラットフォームに Mac OS X 10.4.10, Mac OS X 10.4.9 を追加
1.3 版	平成 20 年 10 月 10 日	表 3-1 動作環境 プラットフォームに Mac OS X 10.5.4, Mac OS X 10.5.3, Mac OS X 10.5.2, , Mac OS X 10.5.1, Mac OS X 10.5 Mac OS X 10.4.11 を追加

— 目次 —

第 1 章 はじめに	1
第 2 章 ドキュメント体系	1
第 3 章 動作環境	2
第 4 章 機能仕様	3
第 1 節 ソフトウェア構成図	3
第 2 節 実現可能な機能の一覧	4
第 5 章 API 仕様	5
第 1 節 サポート API 一覧	5
第 2 節 サポート API 仕様詳細	6
1 Keychain Services/Manager	6
2 CSSM	6
第 3 節 コーリングシーケンス	7
1 IC カードへの接続	7
2 IC カードへのログイン	7
3 IC カードから切断	8
4 証明書取得（利用者証明書、都道府県知事の自己署名証明書）	8
5 署名生成（署名対象データを渡すパターン）	9
6 繰り返し署名生成（署名対象データを渡すパターン）	12
7 署名生成（ハッシュ値を渡すパターン）	12
8 繰り返し署名生成（ハッシュ値を渡すパターン）	13
9 署名検証（検証対象データを渡すパターン）	14
10 繰り返し署名検証（検証対象データを渡すパターン）	16
11 署名検証（ハッシュ値を渡すパターン）	17
12 繰り返し署名検証（ハッシュ値を渡すパターン）	19

第 1 章 はじめに

公的個人認証サービス 利用者クライアントソフト(以下、JPKI 利用者ソフト)における、以下の機能を実現するための Application Program Interface(以下、API)仕様について説明する。

- 証明書取得機能
- 電子署名生成機能
- 電子署名検証機能

第 2 章 ドキュメント体系

JPKI 利用者ソフトのドキュメント体系図を以下に示す。本書は以下の体系図の網掛け部分に該当する。

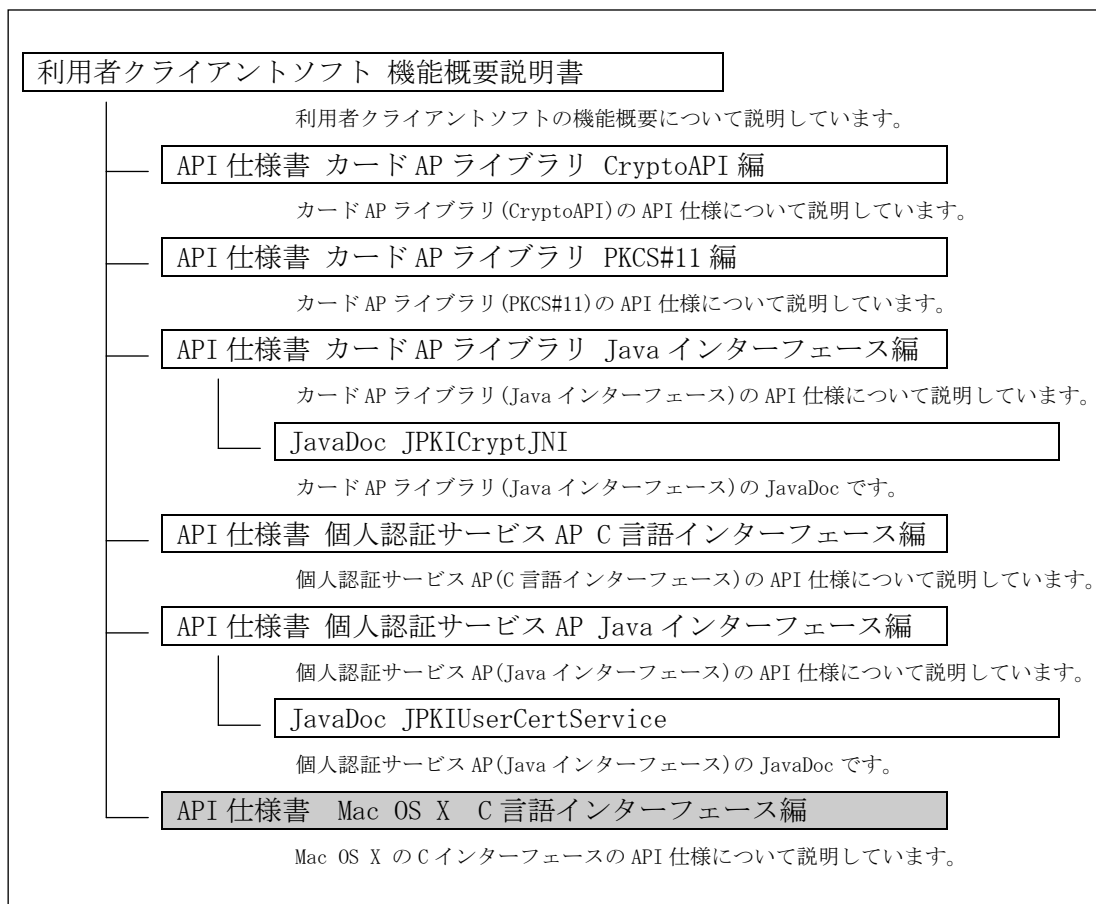


図 2-1 ドキュメント体系図

第3章 動作環境

Mac OS X の C 言語インターフェースの動作環境は以下の通りとする。

表 3-1 動作環境

項目	条件
プラットフォーム (※1)	Mac OS X 10.5.4 Mac OS X 10.5.3 Mac OS X 10.5.2 Mac OS X 10.5.1 Mac OS X 10.5 Mac OS X 10.4.11 Mac OS X 10.4.10 Mac OS X 10.4.9 Mac OS X 10.4.8 Mac OS X 10.4.5(※2)
IC カード	公的個人認証サービスカードアプリケーションを搭載し、公的個人認証サービスの電子証明書が格納された IC カードとする。
IC カードリーダー ライター	以下の条件を満たす IC カードリーダーライターとする。(「適合性検証済み IC カードリーダー一覧」を参照のこと。) <ul style="list-style-type: none"> ・ IC カードのインターフェース(非接触型、接触非接触両対応型)に対応していること ・ PC/SC 対応 IC カードリーダーライター(※3)であること ・ USB や RS-232C など、パソコンに接続するためのインターフェースを有すること ・ IC カードリーダーライターと通信するためのドライバソフトウェアが提供されていること ・ IC カードの搬送方式が手動挿入/手動排出タイプまたは自動挿入/自動排出タイプであること ・ IC カードを挿入するスロットの数は1つとし、1度に挿入できる IC カードは1枚であること

※1 最新情報については JPKI ポータルサイトを参照のこと。

※2 PowerPC ベースのみ。

※3 Personal Computer/Smart Card の略。Microsoft 社等のワーキンググループが推進する、Windows 環境における IC カード利用のための統一規格(PC/SC 規格)に対応した IC カードリーダーライターのこと。

第4章 機能仕様

第1節 ソフトウェア構成図

本仕様書では、JPKI 利用者ソフトのうち、下図の太枠に示す Keychain Services および CSSM(Common Security Services Manager)の仕様をまとめる。

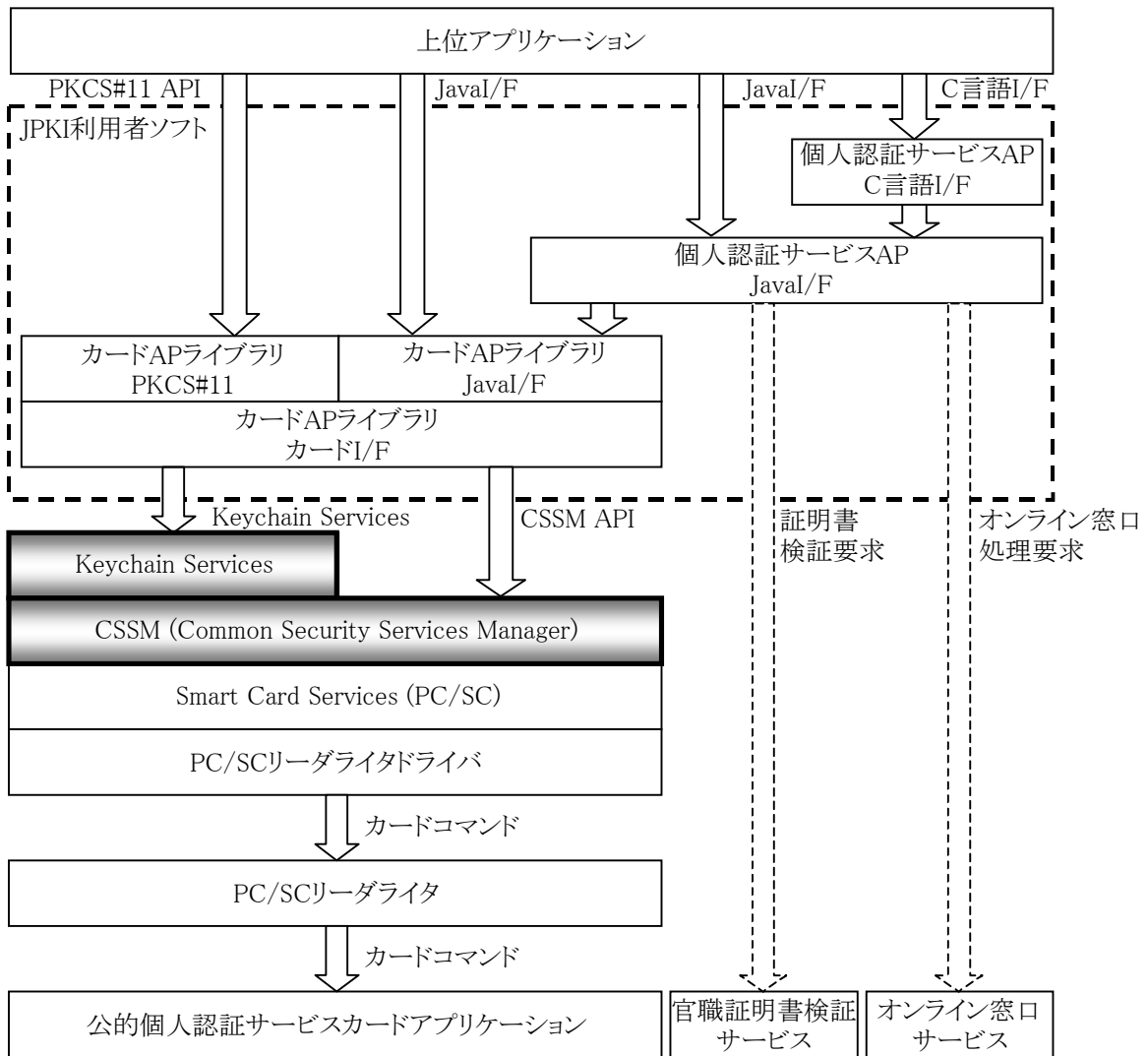


図 4-1 ソフトウェア構成図

第2節 実現可能な機能の一覧

Keychain Services および CSSM で実現可能な機能の一覧を表 4-1に示す。

表 4-1 実現可能な機能の一覧

NO	機能	概要
1	利用者証明書取得	IC カードに格納された利用者証明書を取得する。
2	都道府県知事の自己署名証明書取得	IC カードに格納された都道府県知事の自己署名証明書を取得する。
3	署名生成(署名対象データを渡すパターン)	署名対象データからハッシュ値を計算し、IC カードに格納された利用者秘密鍵を使用して電子署名を生成する。
4	繰り返し署名生成(署名対象データを渡すパターン)	N03 の処理を繰り返し実行し、複数の署名対象データに対する電子署名を生成する。
5	署名生成(ハッシュ値を渡すパターン)	ハッシュ値に対して、IC カードに格納された利用者秘密鍵を使用して電子署名を生成する。
6	繰り返し署名生成(ハッシュ値を渡すパターン)	N05 の処理を繰り返し実行し、複数のハッシュ値に対する電子署名を生成する。
7	署名検証(検証対象データを渡すパターン)	検証対象データからハッシュ値を計算し、ハッシュ値、電子署名、公開鍵を使用して電子署名を検証する。
8	繰り返し署名検証(検証対象データを渡すパターン)	N07 の処理を繰り返し実行し、複数の電子署名を検証する。
9	署名検証(ハッシュ値を渡すパターン)	ハッシュ値、電子署名、公開鍵を使用して電子署名を検証する。
10	繰り返し署名検証(ハッシュ値を渡すパターン)	N09 の処理を繰り返し実行し、複数の電子署名を検証する。

第 5 章 API 仕様

第 1 節 サポート API 一覧

Keychain Services および CSSM のサポート API の一覧を表 5-1 に示す。

表 5-1 サポート API 一覧

NO	API 名	概要
1	SecCertificateGetCLHandle	キーチェーンアイテムから CL ハンドルを取得する。
2	SecCertificateGetData	キーチェーンアイテムから証明書データを取得する。
3	SecKeychainCopyDomainSearchList	IC カードに対応するキーチェーンのリストを作成する。
4	SecKeychainGetCSPHandle	キーチェーンに対応する CSP ハンドルを取得する。
5	SecKeychainGetStatus	キーチェーンのステータスを取得する。
6	SecKeychainItemCopyAttributesAndData	キーチェーンアイテムからアイテムクラスを取得する。
7	SecKeychainLock	キーチェーンをロックする。
8	SecKeychainSearchCopyNext	サーチリストからキーチェーンアイテムを取得する。
9	SecKeychainSearchCreateFromAttributes	証明書のサーチリストを生成する。
10	SecKeychainUnlock	キーチェーンのロックを解除する。
11	SecKeyGetCredentials	キーチェーンアイテムから秘密鍵を利用する為の信用情報を取得する。
12	SecKeyGetCSSMKey	キーチェーンから CSSM のキー (秘密鍵) を取得する。
13	CSSM_CL_CertAbortQuery	証明書の検索を終了する。
14	CSSM_CL_CertGetFirstFieldValue	証明書から指定した OID に対応する属性を検索する。
15	CSSM_CSP_CreateDigestContext	CSSM で使用するダイジェストハンドルを取得する。
16	CSSM_CSP_CreateSignatureContext	CSSM で使用する署名生成ハンドルを取得する。
17	CSSM_DeleteContext	CSSM のハンドルを破棄する。
18	CSSM_DigestDataFinal	ダイジェストを取得・終了する。
19	CSSM_DigestDataInit	ダイジェストの初期化する。
20	CSSM_DigestDataUpdate	ダイジェスト値にデータをアップデートす

		る。
21	CSSM_GetSubserviceUIDFromHandle	CSP ハンドルから対応するサービス UID を取得する。
22	CSSM_Init	CSSM を初期化する。
23	CSSM_ModuleAttach	CSSM の CSP モジュールを CSSM にアタッチする。
24	CSSM_ModuleLoad	CSSM の CSP モジュールをロードする。
25	CSSM_SignData	署名を生成 (SHA1) する。
26	CSSM_VerifyData	署名を検証する。

第 2 節 サポート API 仕様詳細

1 Keychain Services

Keychain Services の詳細については、下記 URL 等の正式な資料を参照してください。

「<http://developer.apple.com/documentation/Security/Reference/SecurityFrameworkReference/index.html>」

Copyright © 2006 Apple Computer, Inc.

2 CSSM

CSSM の詳細については、下記 URL の正式な資料を参照してください。

「<http://www.opengroup.org/publications/catalog/c914.htm>」

Copyright © 1995-2005. The Open Group. All Rights Reserved.

第 3 節 コーリングシーケンス

「第 4 章 第 2 節 実現可能な機能の一覧」を実現するためのコーリングシーケンスを以下に示す。上位アプリケーションは、このコーリングシーケンスに沿って実装すること。

1 IC カードへの接続

IC カードへの接続のコーリングシーケンスを以下に示す (図 5-1)。

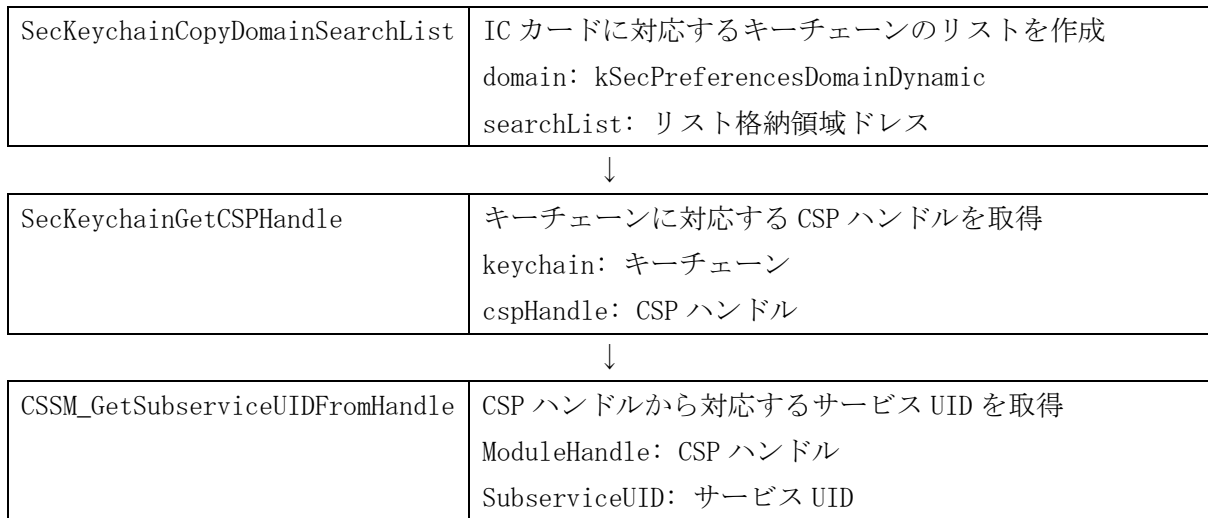


図 5-1 IC カードへの接続

2 IC カードへのログイン

IC カードへのログインのコーリングシーケンスを以下に示す (図 5-2)。

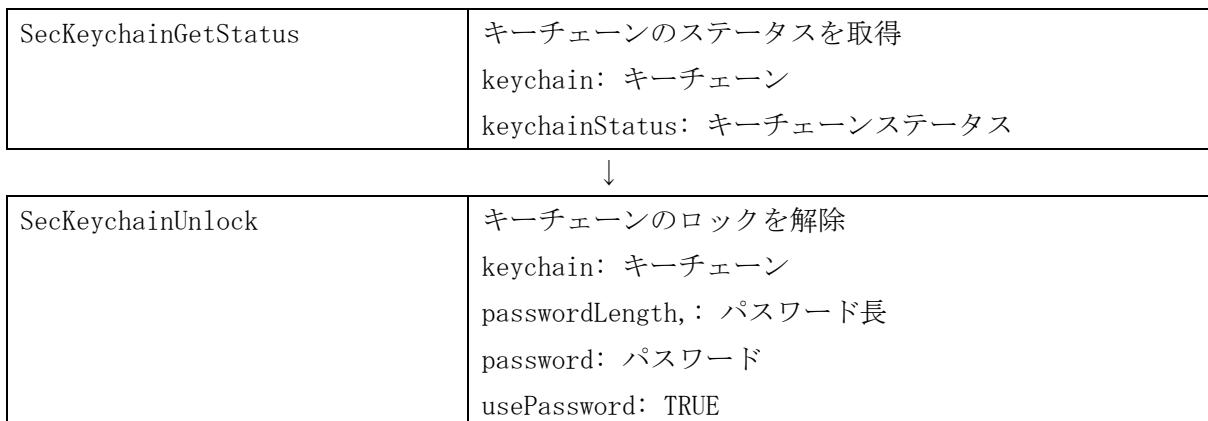


図 5-2 IC カードへのログイン

3 ICカードから切断

ICカードから切断のコーディングシーケンスを以下に示す（図 5-3）。

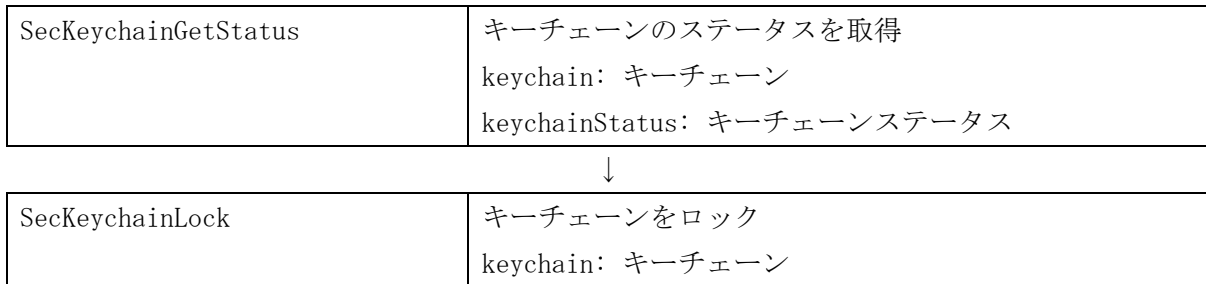
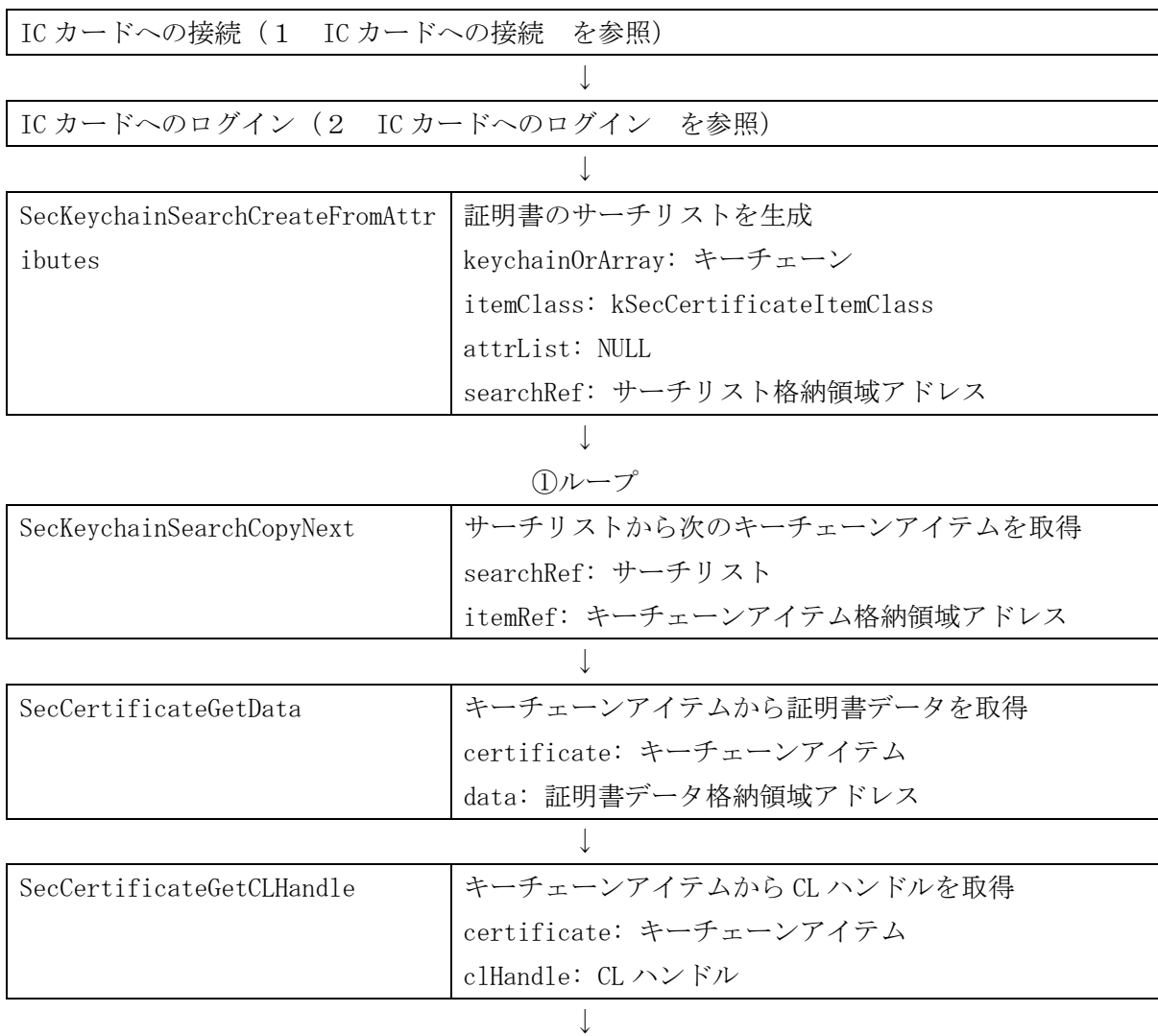


図 5-3 ICカードから切断

4 証明書取得（利用者証明書、都道府県知事の自己署名証明書）

証明書取得のコーディングシーケンスを以下に示す（図 5-4）。



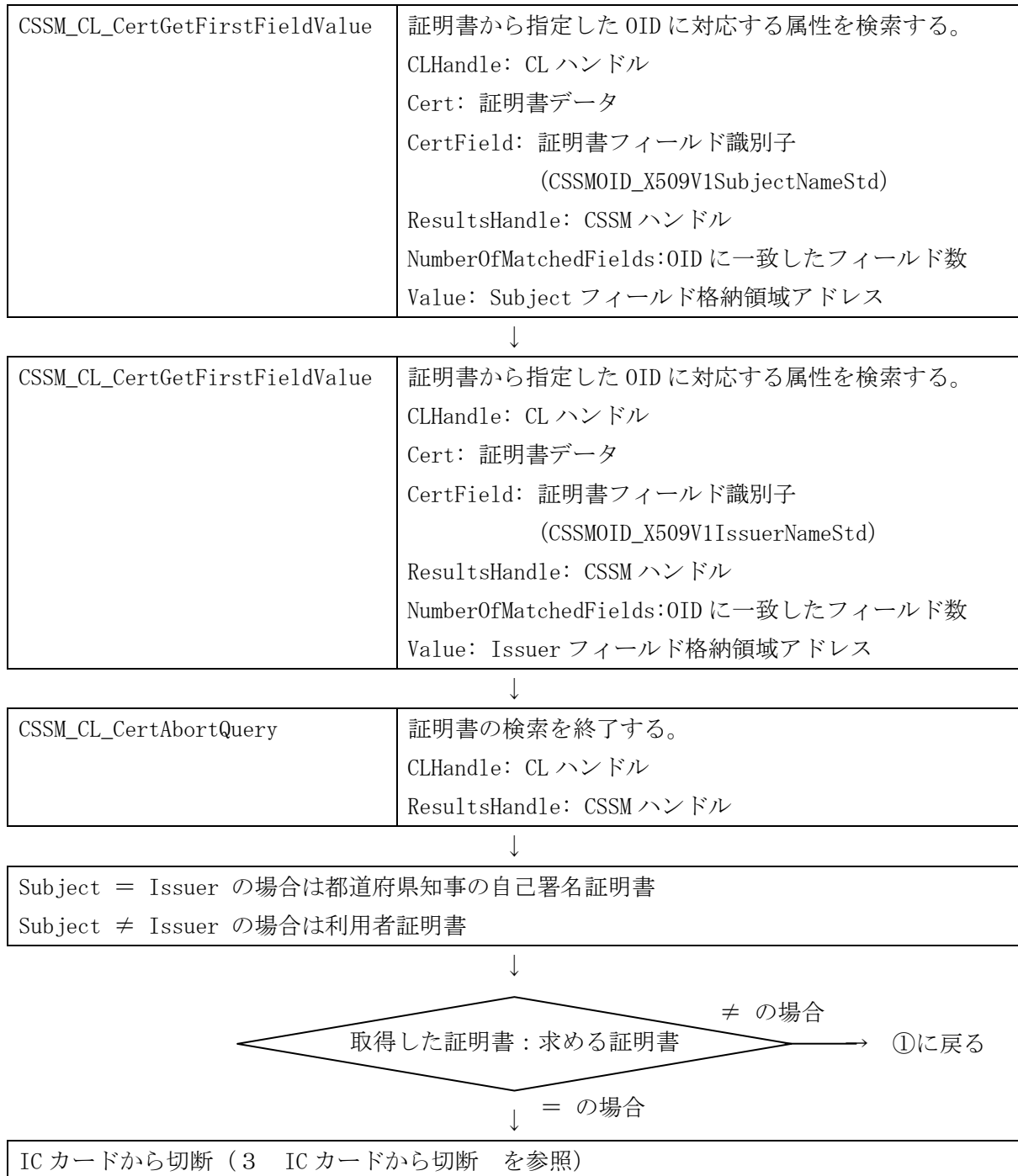


図 5-4 証明書取得

5 署名生成 (署名対象データを渡すパターン)

署名生成 (署名対象データを渡すパターン) のコーリングシーケンスを以下に示す (図 5-5)。

IC カードへの接続 (1 IC カードへの接続 を参照)



ICカードへのログイン (2 ICカードへのログイン を参照)



SecKeychainSearchCreateFromAttributes	証明書のサーチリストを生成 keychainOrArray: キーチェーン itemClass: CSSM_DL_DB_RECORD_ANY attrList: NULL searchRef: サーチリスト格納領域アドレス
---------------------------------------	---



SecKeychainSearchCopyNext	サーチリストから次のキーチェーンアイテムを取得 searchRef: サーチリスト itemRef: キーチェーンアイテム格納領域アドレス
---------------------------	---



SecKeychainItemCopyAttributesAndData	キーチェーンアイテムからアイテムクラスを取得 ItemRef: キーチェーンアイテム Info: NULL ItemClass: アイテムクラス *attrList: NULL length: NULL outData: NULL
--------------------------------------	---



SecKeychainGetCSPHandle	キーチェーンに対応する CSP ハンドルを取得 keychain, : キーチェーン cspHandle: CSP ハンドル
-------------------------	--



SecKeyGetCSSMKey	キーチェーンから CSSM のキー(秘密鍵)を取得 key: キーチェーンアイテム cssmKey: CSSM キー
------------------	--



SecKeyGetCredentials	キーチェーンアイテムから秘密鍵を利用する為の信用情報を取得 keyRef: キーチェーンアイテム operation: CSSM_ACL_AUTHORIZATION_SIGN credentialType: kSecCredentialTypeDefault outCredentials: 信用情報
----------------------	--



CSSM_CSP_CreateDigestContext	CSSM で使用するダイジェストハンドルを取得 CSPHandle: CSP ハンドル AlgorithmID: CSSM_ALGID_SHA1 NewContextHandle: ダイジェストハンドル
↓	
CSSM_DigestDataInit	ダイジェストの初期化 CCHandle: ダイジェストハンドル
↓	
CSSM_DigestDataUpdate	ダイジェスト値にデータをアップデート CCHandle: ダイジェストハンドル DataBufs: ハッシュ対象データ DataBufCount: 1
↓	
CSSM_DigestDataFinal	ダイジェストの取得・終了処理 CCHandle: ダイジェストハンドル Digest: ダイジェスト格納領域アドレス
↓	
CSSM_DeleteContext	CSSM のハンドルを破棄 CCHandle: ダイジェストハンドル
↓	
CSSM_CSP_CreateSignatureContext	CSSM で使用する署名生成ハンドルを取得 CSPHandle: CSP ハンドル AlgorithmID: CSSM_ALGID_RSA AccessCred: 信用情報 Key: CSSM キー NewContextHandle: 署名生成ハンドル
↓	
CSSM_SignData	署名生成 (SHA1) CCHandle: 署名生成ハンドル DataBufs: CSSM_DATA 型のハッシュ値 DataBufCount: 1 DigestAlgorithm: CSSM_ALGID_SHA1 Signature: 署名値
↓	
CSSM_DeleteContext	署名生成ハンドルを破棄 CCHandle: 署名生成ハンドル
↓	
IC カードから切断 (3 IC カードから切断 を参照)	

図 5-5 署名生成 (署名対象データを渡すパターン)

6 繰り返し署名生成 (署名対象データを渡すパターン)

「5 署名生成 (署名対象データを渡すパターン)」の網掛け部分を署名対象データの個数分だけ繰り返して呼び出す。

7 署名生成 (ハッシュ値を渡すパターン)

署名生成(ハッシュ値を渡すパターン)のコーリングシーケンスを以下に示す(図 5-6)。

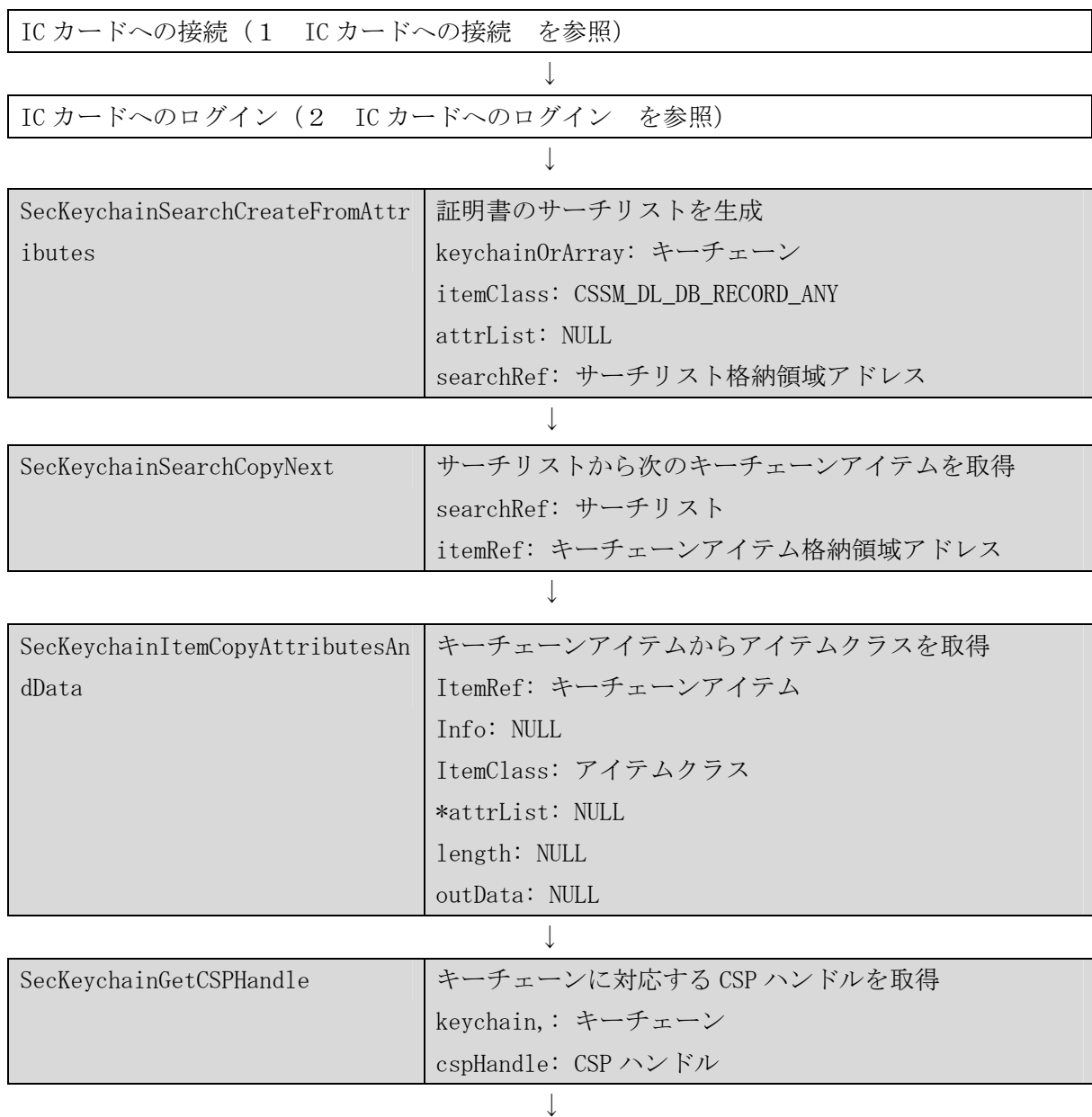




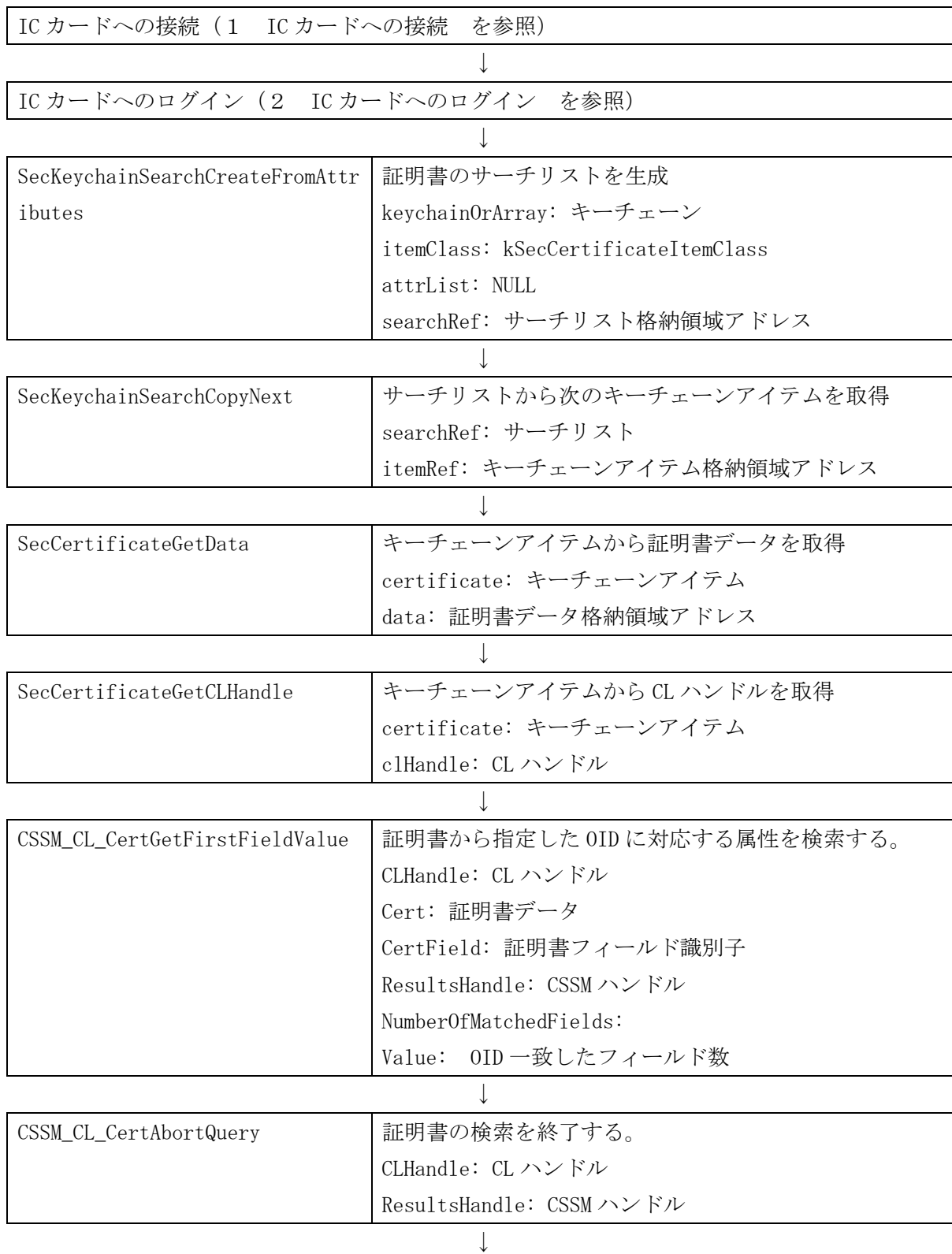
図 5-6 署名生成 (ハッシュ値を渡すパターン)

8 繰り返し署名生成 (ハッシュ値を渡すパターン)

「7 署名生成 (ハッシュ値を渡すパターン)」の網掛け部分を署名対象データの個数分だけ繰り返して呼び出す。

9 署名検証（検証対象データを渡すパターン）

署名検証（検証対象データを渡すパターン）のコーディングシーケンスを以下に示す（図5-7）。



SecKeychainGetCSPHandle	キーチェーンに対応するCSPハンドルを取得 keychain: キーチェーン cspHandle: CSPハンドル
↓	
CSSM_CSP_CreateDigestContext	CSSMで使用するダイジェストハンドルを取得 CSPHandle: CSPハンドル AlgorithmID: CSSM_ALGID_SHA1 NewContextHandle: ダイジェストハンドル
↓	
CSSM_DigestDataInit	ダイジェストの初期化 CCHandle: ダイジェストハンドル
↓	
CSSM_DigestDataUpdate	ダイジェスト値にデータをアップデート CCHandle: ダイジェストハンドル DataBufs: ハッシュ対象データ DataBufCount: 1
↓	
CSSM_DigestDataFinal	ダイジェストの取得・終了処理 CCHandle: ダイジェストハンドル Digest: ダイジェスト格納領域アドレス
↓	
CSSM_DeleteContext	CSSMのハンドルを破棄 CCHandle: ダイジェストハンドル
↓	
CSSM_Init	CSSMを初期化 Version: CSSMバージョン Scope: CSSM_PRIVILEGE_SCOPE_NONE CallerGuid: GID KeyHierarchy: CSSM_KEY_HIERARCHY_NONE PvcPolicy: CSSM_PVC_NONE Reserved: NULL
↓	
CSSM_ModuleLoad	CSSMのCSPモジュールをロード ModuleGuid: &gGuidAppleCSP KeyHierarchy: CSSM_KEY_HIERARCHY_NONE AppNotifyCallback: NULL AppNotifyCallbackCtx): NULL
↓	

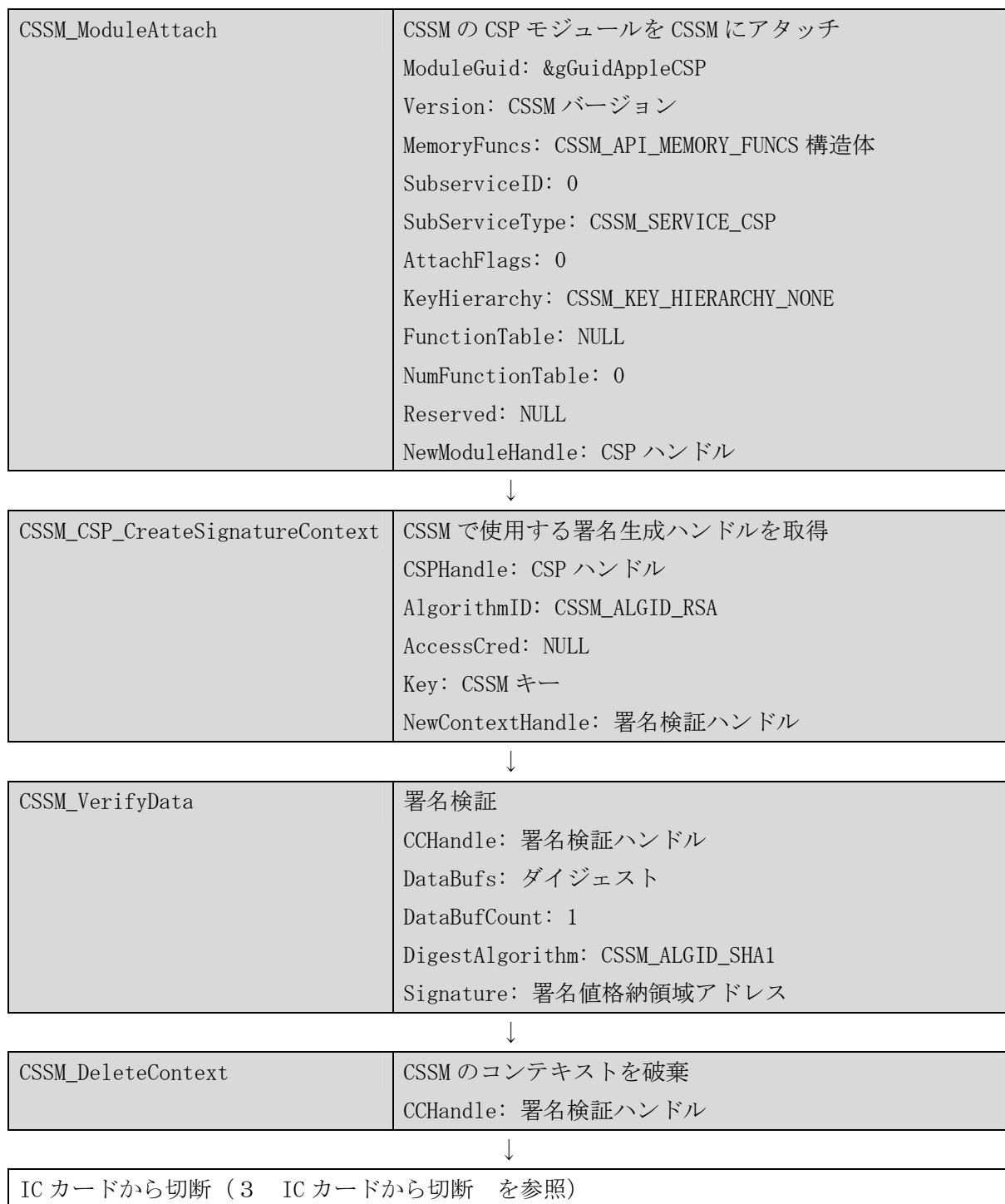


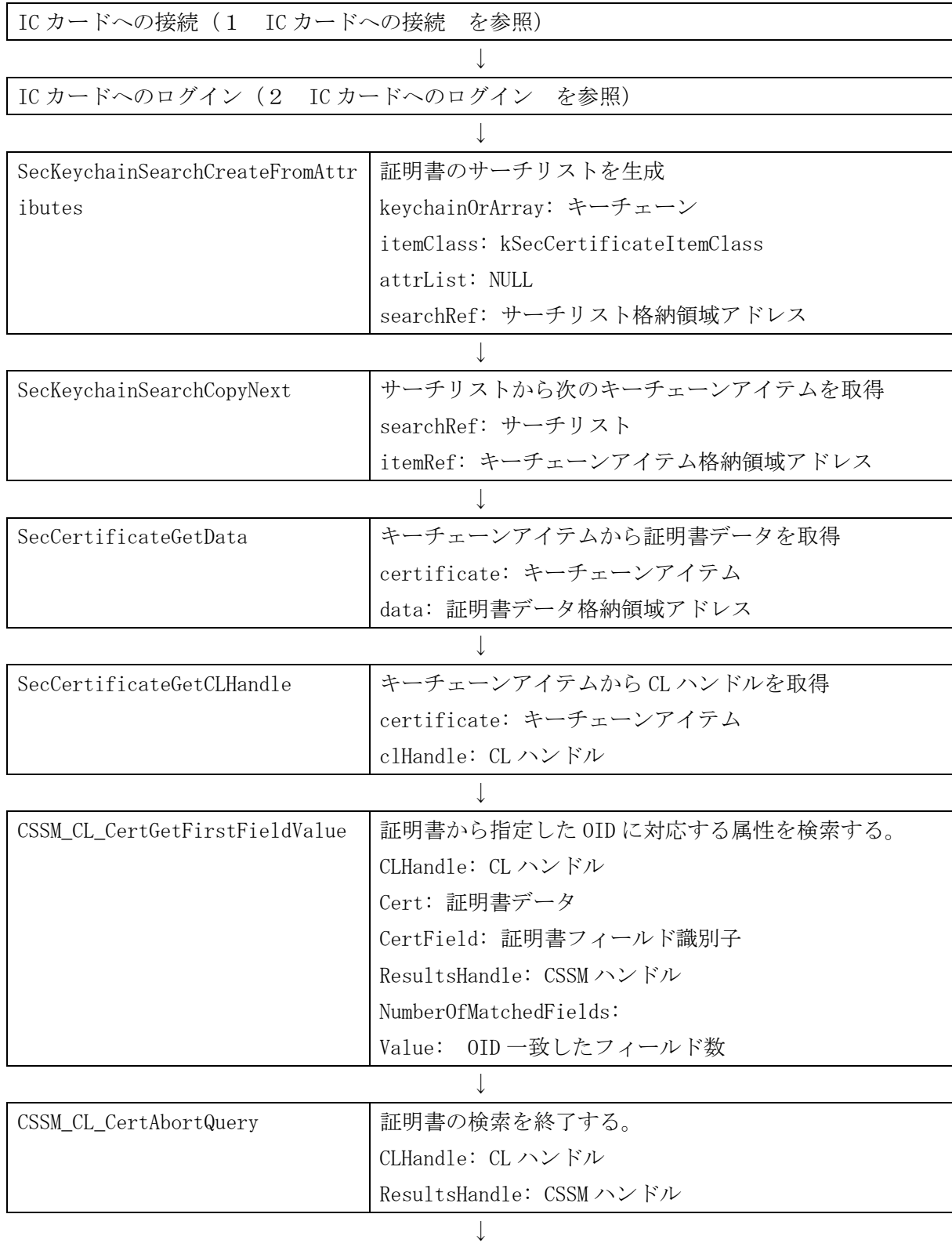
図 5-7 署名検証 (検証対象データを渡すパターン)

10 繰り返し署名検証 (検証対象データを渡すパターン)

「9 署名検証 (検証対象データを渡すパターン)」の網掛け部分を検証対象データの個数分だけ繰り返して呼び出す。

1.1 署名検証 (ハッシュ値を渡すパターン)

署名検証(ハッシュ値を渡すパターン)のコーリングシーケンスを以下に示す(図 5-8)。



SecKeychainGetCSPHandle	キーチェーンに対応するCSPハンドルを取得 keychain: キーチェーン cspHandle: CSPハンドル
↓	
CSSM_Init	CSSMを初期化 Version: CSSMバージョン Scope: CSSM_PRIVILEGE_SCOPE_NONE CallerGuid: GID KeyHierarchy: CSSM_KEY_HIERARCHY_NONE PvcPolicy: CSSM_PVC_NONE Reserved: NULL
↓	
CSSM_ModuleLoad	CSSMのCSPモジュールをロード ModuleGuid: &gGuidAppleCSP KeyHierarchy: CSSM_KEY_HIERARCHY_NONE AppNotifyCallback: NULL AppNotifyCallbackCtx): NULL
↓	
CSSM_ModuleAttach	CSSMのCSPモジュールをCSSMにアタッチ ModuleGuid: &gGuidAppleCSP Version: CSSMバージョン MemoryFuncs: CSSM_API_MEMORY_FUNCS 構造体 SubserviceID: 0 SubServiceType: CSSM_SERVICE_CSP AttachFlags: 0 KeyHierarchy: CSSM_KEY_HIERARCHY_NONE FunctionTable: NULL NumFunctionTable: 0 Reserved: NULL NewModuleHandle: CSPハンドル
↓	
CSSM_CSP_CreateSignatureContext	CSSMで使用する署名生成ハンドルを取得 CSPHandle: CSPハンドル AlgorithmID: CSSM_ALGID_RSA AccessCred: NULL Key: CSSMキー NewContextHandle: 署名検証ハンドル
↓	

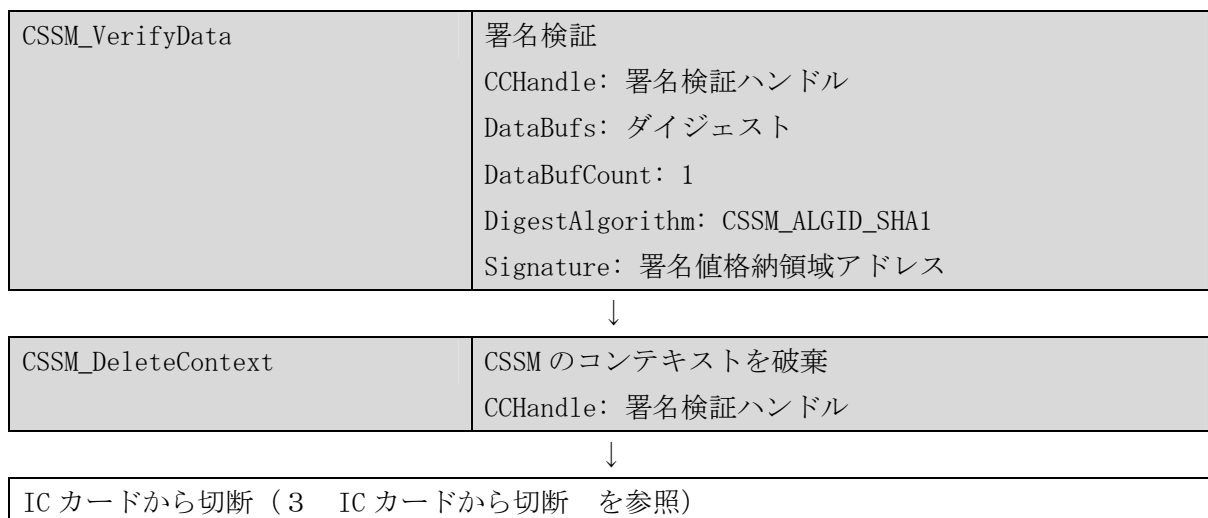


図 5-8 署名検証 (ハッシュ値を渡すパターン)

1.2 繰り返し署名検証 (ハッシュ値を渡すパターン)

「1.1 署名検証 (ハッシュ値を渡すパターン)」の網掛け部分を署名検証対象データの個数分だけ繰り返して呼び出す(すべての電子署名が同一の秘密鍵で生成された場合)。

禁・無断転載

公的個人認証サービス

利用者クライアントソフト API仕様書

【Mac OS X C言語IF編】

第1.3版

(注意事項)

※利用者クライアントソフトの著作権は、総務省、公的個人認証サービス都道府県協議会が保有しており、国際著作権条約及び日本国の著作権関連法令によって保護されています。

※JPKI利用者ソフトの利用に当たっては、次に掲げる行為を禁止します。

- (1) 利用者クライアントソフトを電子申請・届出等の行政手続等以外の目的で利用すること。
- (2) 利用者クライアントソフトに対し、総務省、公的個人認証サービス都道府県協議会に許可なく改造等を行うこと。

※総務省、公的個人認証サービス都道府県協議会、(財)自治体衛星通信機構は、利用者が利用者クライアントソフトを利用したことにより発生した利用者の損害及び利用者が第三者に与えた損害について、一切の責任を負いません。