

## CACAnet証明書発行システム 基本仕様書

### 証明書の発行

SubjectがRAに対して証明書の発行を依頼。  
RAはその依頼を受け、本人確認を行って証明書の発行を行う。

対象: RA, Subject

アクセス制御などの権限管理は「個人証明書発行手続き」を参照。  
発行された証明書はリポジトリに登録。  
システムのディレクトリ構造は「ディレクトリ構造」を参照。  
証明書格納などのリポジトリ設計は「リポジトリ設計仕様書」を参照。  
発行の手続きは下記の「証明書発行機能仕様」と「個人証明書発行手続き」を参照。  
証明書発行機能仕様  
システム正常系

#### RA

- (1)証明書発行の要求を行ったSubjectの連絡先をデータベースに登録するページ  
セッションデータベースヘデータを登録する機能  
秘密情報を生成する機能  
手続きが開始された旨をRA、Subjectに通知するメールを配信できる機能  
RAには秘密情報、Subjectには作業を行うURLを記述すること
- (2)(1)に関しての登録内容の確認のページ
- (3)Subjectが登録した内容を確認するページ
- (4)Subjectへの証明書発行を承諾するページ
- (5)Subjectへの証明書発行が承諾されなかった場合に表示するページ
- (6)CAと通信をして鍵を生成する機能
- (7)証明書発行の完了を報告するページ  
Subjectに手続きが完了したメールを配信できる機能  
証明書が取得できるURLを記述する
- (8)RAの情報を管理する機能
- (9)エラーを表示するページ(エラー内容は下記のエラーの仕様に基づく)

#### Subject

- (1)Subject自身の情報を登録するページ  
秘密情報の正当性を確認できる機能  
セッションデータベースヘデータを登録する機能
- (2)(1)に関しての登録内容の確認のページ
- (3)鍵を生成する方法が選択できるページ  
Internet Explorerでの秘密鍵作成ができる機能  
Netscape Navigatorでの秘密鍵作成ができる機能  
RAに依頼して作成できる機能  
パスワードを入力するページ
- (4)証明書を取得できるページ
- (5)エラーを表示するページ(エラー内容は下記のエラー仕様に基づく)

#### システム異常系

- 1.RAの正当性が確認できなければエラーを返す機能  
  
クライアントのDNがRAデータベースになければエラーを返す機能  
RAの状態が正常でなければエラーを返す機能
- 2.セッションの正当性が確認できない場合はエラーを返す機能  
  
セッションIDが存在しなければエラーを返す機能  
無効なセッションであればエラーを返す機能  
時間超過であればエラーを返す機能  
遷移に異常があればエラーを返す機能
- 3.CAとの通信ができなければエラーを返す機能
- 4.入力値がなければエラーを返す機能(未確認)  
  
(# 定義されているが使用していないクラス)
- 5.以上の1～4のエラーが発生した場合、エラーページを表示させること

## 証明書の入手

Subjectがリポジトリより他のSubjectの証明書を入手することが出来る。

対象: Subject

CACAnetの証明書を持つSubjectがWebシステムより

Subject一覧や名前・メールアドレスなどからの検索により証明書取得が可能

(疑問点)

証明書の入手は既に個人証明書を持っている人のみとするか  
証明書を公開したくないなどの個人の制約を考慮に入れるか  
証明書格納などのリポジトリ設計は「リポジトリ設計仕様書」を参照。

## 証明書の廃棄

Subjectの証明書の廃棄を行う

対象: RA, Subject

Webベースのシステムとする

RAは自分が発行したSubjectの証明書のみ廃棄出来る。

CRL格納などのリポジトリ設計は「リポジトリ設計仕様書」を参照。

## CRLの発行

SubjectがリポジトリよりCRLを入手することが出来る。

対象: Subject

クライアントはCRLをリポジトリやWebシステムにて入手可能

Webシステムからは最新CRLのリポジトリへのリンクとする

CRL格納などのリポジトリ設計は「リポジトリ設計仕様書」を参照。

## システムの情報管理

システム上の情報管理を行う。

RAの管理

RAAがRAの登録や抹消を行うことが出来る。

対象: RAA, RA

- ・RAA専用アクセス制御であるWebベースのシステム
- ・特定のSubjectにRAの権限を登録が出来る。
- ・RAの権限を抹消することが出来る。

(疑問点)

- ・RAAはRAの発行している状態を監視できる必要があるか

セッションの管理

RAが発行処理中のセッションの管理を行うことが出来る。

対象: RA

- ・発行作業中のユーザ状況把握が可能
- ・RAが自身の発行したユーザのセッション状態を削除できる

## 推奨環境

推奨する環境は以下のとおり

Webブラウザ

Internet Explorer 5.5 6.0 (Windows推奨)

Netscape Navigator 4.7x 6.x

メールソフト

Outlook, Outlook Express

Netscape付属メーラー