ユビキタスネットワーク時代のPKI
安全安心なネットワークへの技術的裏づけと応用
(基礎編)

セコム株式会社IS研究所
松本　泰
yas-matsumoto@secom.co.jp

ユビキタスネットワーク時代のPKI
安全安心なネットワークへの技術的裏づけと応用
(基礎編)

1. PKI技術の概要
2. サブスクライバー/署名者
3. リライングパーティ/検証者
4. 認証局の信頼
5. PKIの構成
6. 証明書発行
7. PKIの信頼性

ユビキタスネットワーク時代のPKI
PKI技術の概要

電子署名を中心としたPKIの基本的な仕組み

3

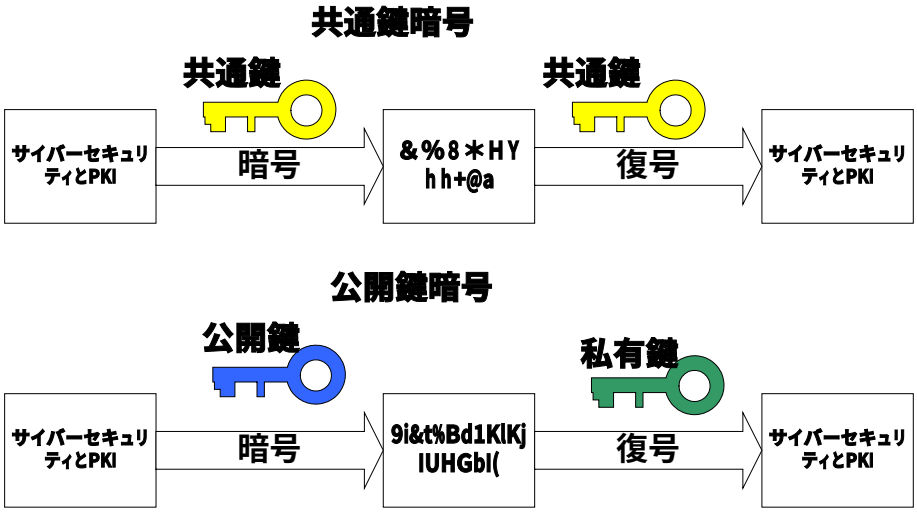
PKI技術の概要

基本的な用語の理解

- **Certification**と**Authentication**
  - 共に「認証」と訳されることが多いが。。違う概念
  - **Certification**
    - 証明書により何らかの権威者が何事かを証明する
      - 会社が社員を。自治体が市民を。。
  - **Authentication**
    - 真正性の確認（正当な本人であることを確認する）
- **署名**(Signature)と**認証**(Authentication)
  - 自然人による否認防止の署名
    - 自分の意志で文書に対して内容を確認した上で署名 － 自署名

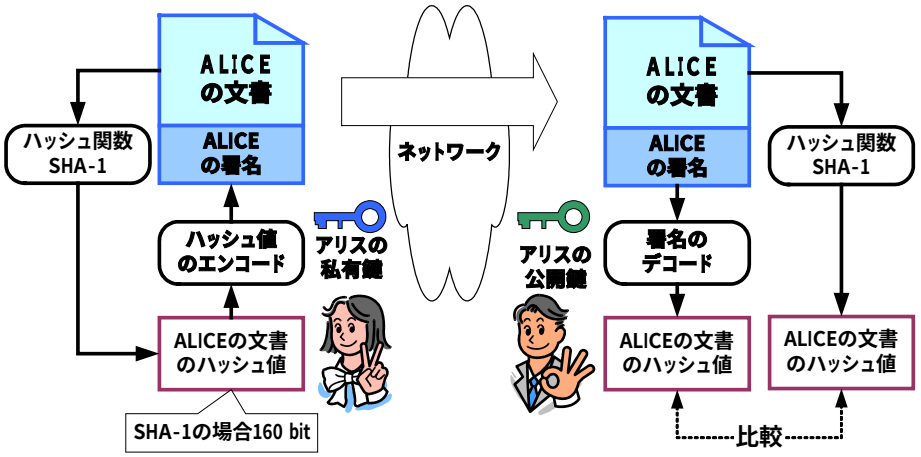
4

PKI技術の概要
共通鍵暗号と公開鍵暗号



5

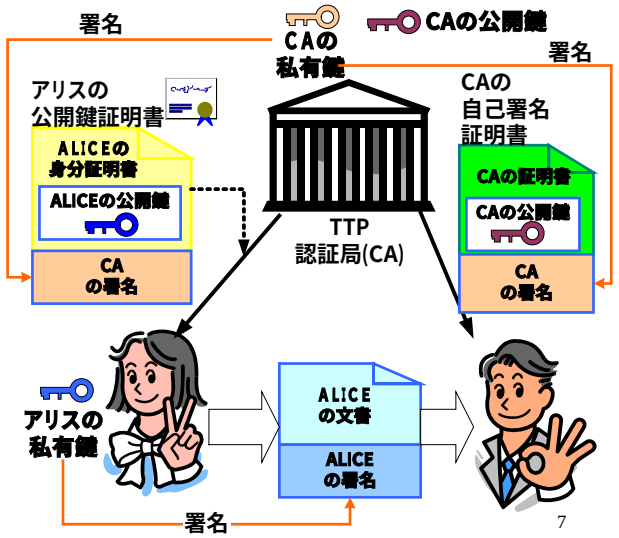
PKI技術の概要
署名の仕組み



6

PKI技術の概要
TTPよる署名（いかにアリスの公開鍵を信頼するか）

- TTP(Trusted Third Party)とは
  - 信頼できる第三者機関
  - TTPによって署名されたデータは信用できるものとする
  - 代表的な例はCA（Certificate Authority）
  - CAは印鑑証明を発行してくれる役所のイメージ
  - 公的個人認証サービスでは、都道府県CAが市民のための証明書を発行する。



7

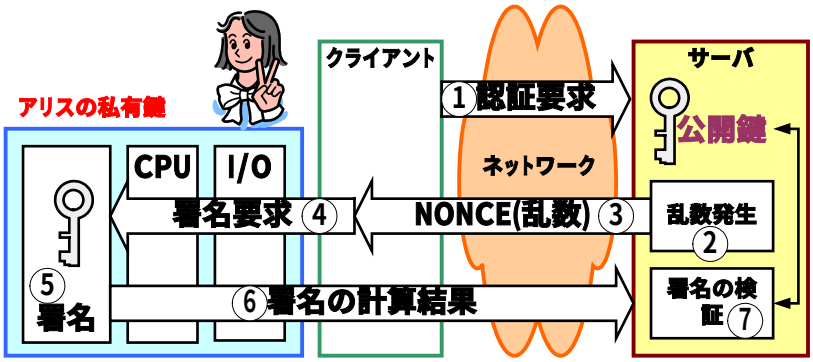
PKI技術の概要
リアル社会の証明書と電子証明書

- リアル社会の証明書
  - 例
    - パスポート
      - 「日本国外務大臣」が発行者
    - 運転免許証
    - 社員証、学生証、会員証
  - 発行者の何らかの「印鑑」が押されている。。
- 電子証明書
  - 公開鍵証明書
  - 属性証明書
    - 電子許可証など
  - 電子パスポート
  - 発行者により電子署名が施されている。

8

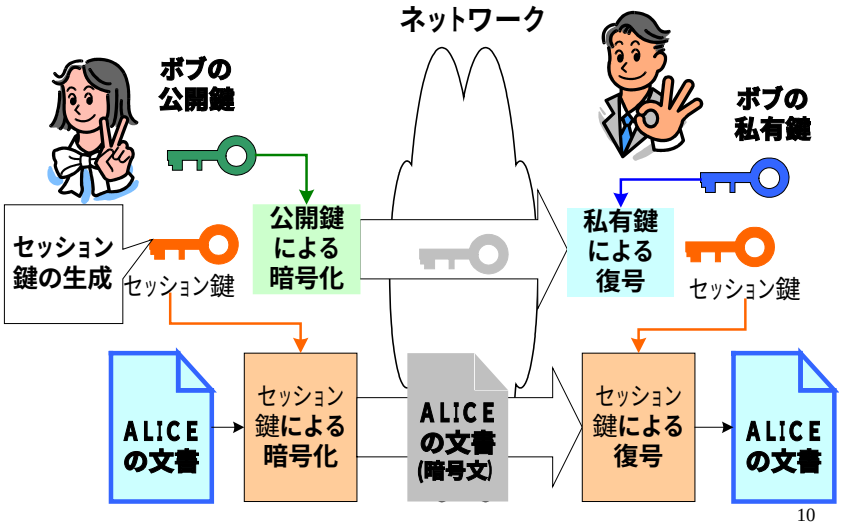
PKI技術の概要
PKIを用いた認証の例

- アリスの秘密情報（私有鍵）はハードウェアトークンから出ない
  - もちろんネットワークにも流れない
- アリスの秘密情報は、サーバには、格納されない
  - サーバは、アリスの秘密情報（例えばパスワード）を預かる必要がない
  - これは、アリスとっても、サーバの運用者にとってもメリット



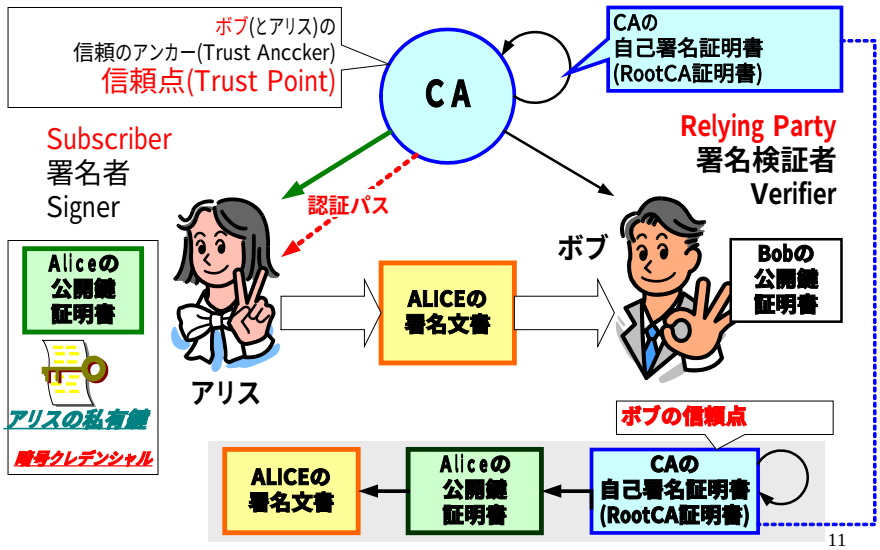
9

PKI技術の概要
PKIを用いた暗号の例（ハイブリッド暗号）



10

PKI技術の概要
PKIの基本的な信頼モデル



11

PKI技術の概要
X.509証明書

証明書バージョン番号 (V3)
証明書シリアル番号
デジタル署名アルゴリズム識別子
発行者名の識別名
有効期間
主体者 (ユーザ) の識別名
主体者の公開鍵
　アルゴリズム識別子
　公開鍵値
V3の拡張
拡張フィールド(タイプ、フラグ、値)
拡張フィールド(タイプ、フラグ、値)
CAのデジタル署名
　アルゴリズム識別子
　署名

- 代表的な公開鍵証明書
  - 主体者(アリス)と、主体者(アリス)の公開鍵や、その他の属性をCA鍵(アリスの証明書を発行したCAの署名鍵)の署名でバインドする。
  - この時、主体者(アリス)の公開鍵に対応した私有鍵は、主体者(アリス)しか使用できないことが理想。
- 1997年版 X.509 3rd Edition
  - X.509v3証明書フォーマット
    - X.509V3証明書拡張
  - 14の標準拡張フィールド

12

PKI技術の概要
X.509証明書の例

Version: v3

SerialNumber: 3a:1e:56:f9

SignatureAlgorithm: sha1WithRSAEncryption

Issuer: C=JP, O=ABC, OU=MedCA

Validity:Not Before: Dec 7 13:30:00 GMT 2003 Not After: Dec 6 13:05:00 GMT 2004

Subject: C=JP, O=ABC, OU=Person, CN=ALICE

Subject Public Key Info:

Public Key Algorithm: rsaEncryption

主体者の公開鍵値

Extensions:

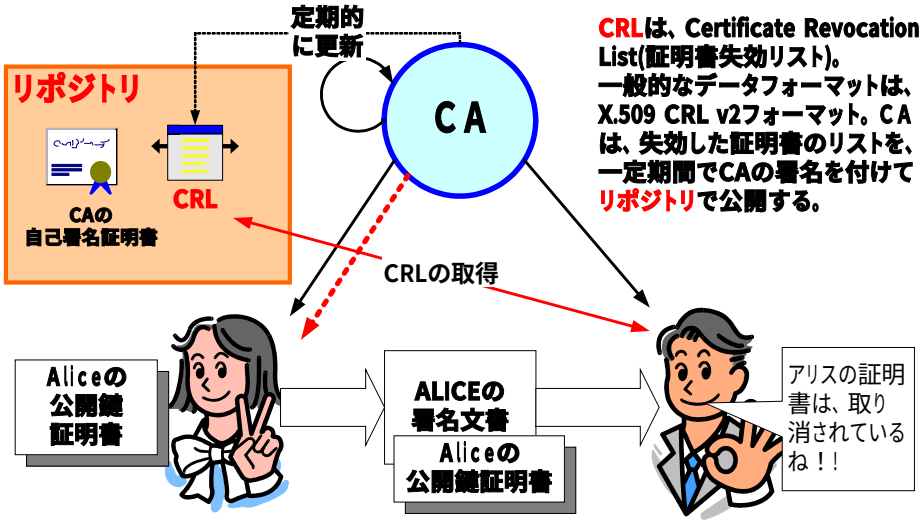
Certificate Policies: policyIdentifier: 1.2.3.4.3

Signature Algorithm: sha1WithRSAEncryption

Signature Data:

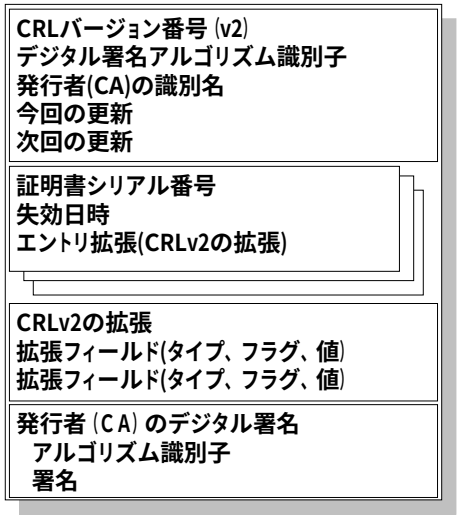
CA鍵による署名

PKI技術の概要
証明書の失効



CRLは、Certificate Revocation List(証明書失効リスト)。一般的なデータフォーマットは、X.509 CRL v2フォーマット。CAは、失効した証明書のリストを、一定期間でCAの署名を付けてリポジトリで公開する。

PKI技術の概要
ＣＲＬ（証明書失効リスト）



CRL

- あるCAが発行した証明書の有効期限内に証明書を失効したい場合、このCRLに、失効したい証明書のシリアル番号を入れて*リポジトリ（LDAPサーバなど）*で公開する。
- CRLは一定期間毎にCAの署名を付けて発行される。

1997年版 X.509 3rd Edition

- CRLv2フォーマット
- X.509v3証明書と同じく拡張がある

15

PKI技術の概要
PKIが安全であるための基本的な要件

- Subscriber側（アリス）の要件
  - セキュアな署名
    - なりすましをいかに防ぐか
    - 署名に使用する*私有鍵をいかに保護*するか??
    - セキュアなハードウェアトークンが有効
- Relying Party側（ボブ）の要件
  - 署名検証、証明書検証をいかに行うか
    - リポジトリ(LDAPサーバ)から必要な情報を取得
      - CRL、ARL、相互認証証明書ペアなど
    - ハードウェアトークン等に格納された*信頼点の公開鍵*からのリポジトリなどから読み出した情報を元に証明書チェーンを構築、そしてパス検証を行う
- 認証局の要件
  - 認証局の運用
  - 証明書やCRLを署名する鍵の管理
  - 本人の確認方法　　Etc…

16

サブスクライバー/署名者

PKIにおける署名者の要件
アリスは、いかに自分の「鍵」を守るか？

サブスクライバー/署名者
Subscriber側（アリス）の要件

- Subscriber側（アリス）の要件
  - セキュアな署名
    - なりすましをいかに防ぐか
    - 署名に使用する*私有鍵をいかに保護*するか??
    - セキュアな**ハードウェアトークン**などが有効
  - 私有鍵(Private Key)の保管場所
    - ハードウェアートークン
    - ローカルなハードディスク
    - 外部のサーバ
  - セキュアな署名装置のセキュリティ基準
    - 米国では、FIPS 140-2などの米国政府の調達基準
    - 欧州の電子署名では、SSCD （Secure signature creation device ）としてその要件を定義

サブスクライバー/署名者
私有鍵(Private Key)の保管場所

- **私有鍵の保管場所**
  - **ローカルなハードディスク**
  - **ハードウェアートークン**
  - **外部のサーバ**
- **ローカルなハードディスク**
  - **「鍵」をローカルなディスクに暗号化して保存**
- **ハードウェアートークン**
  - **耐タンパー性のあるハードウェアトークンに「鍵」を封じ込める**
- **外部のサーバ**
  - **外部のサーバに「鍵」を保管して使用時に取得する**
    - **ローミング鍵**

サブスクライバー/署名者
ハードウェアトークン（暗号トークン）とは??

- 主体者(アリス)の公開鍵に対応した私有鍵は、主体者(アリス)しか使用できないことが理想。
- そのためには、ハードウェアトークンの使用が有効になる。
  - ハードウェアトークンは、色々なPKIアプリケーションで使用できるべき
- ハードウェアトークン
  - 所有者を識別するための暗号クレデンシャル(Cryptographic Credential)を格納することが可能で、かつ携帯性のあるデバイス
- “暗号クレデンシャル(Cryptographic credentials)”ってなに?
  - 鍵と証明書（群）
- ハードウェアトークンの署名者認証
  - 通常はPIN
    - 所持による認証 + 記憶による認証
  - PINに代わる、バイオメトリクス情報
    - 生体情報をカード上にしか持たない方法でのバイオメトリクス認証が盛んに研究されている。
- 参考 -> PKI技術･補足編 PKIとハードウェアートークン他。

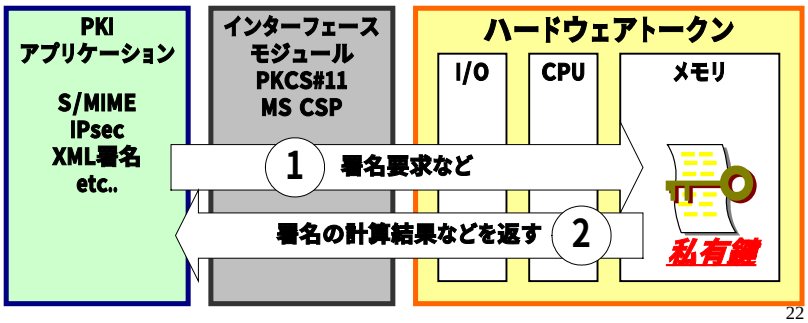
サブスクライバー/署名者
ハードウェアトークンの例

- スマートカード(ICカード)
- USB Token （Dongle）
- 生体認証と組み合わせたトークン
  - SonyのPuppy(FIU-810)など
    - http://www.sony.co.jp/Products/puppy/
- PCに内蔵されたセキュリティチップ
  - TCPA TPM (Trusted Platform Module)
  - 正確にはハードウェアトークンではないかもしれないが機能的には類似
- MOPASS（ Mobile Passport ）
  - フラッシュメモリカード用のモバイルコマース拡張規格
  - SDカードなど
  - http://www.mopass.info/
- 携帯電話
  - ドコモのFOMAの証明書サービスFirstPass。携帯電話に内蔵されたUIM（User Identity Module）をパソコンから利用することも可能

21

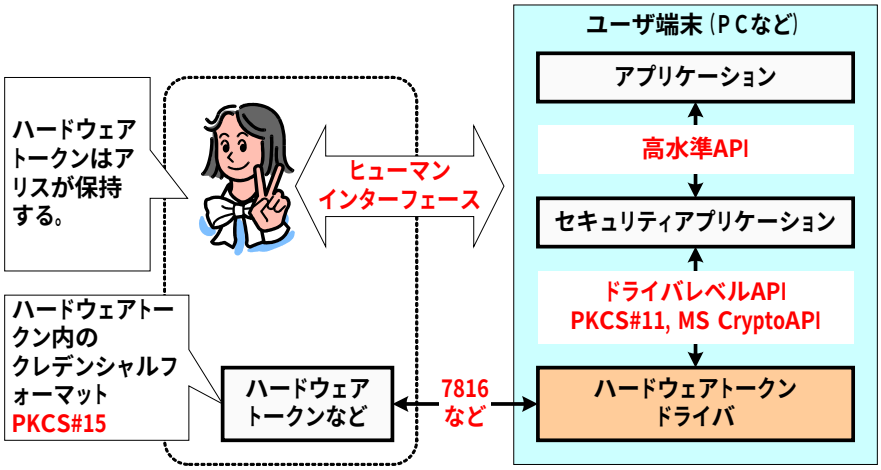
サブスクライバー/署名者
なぜハードウェアトークン

- **署名で使用する私有鍵（Private Key）を守る仕組みが可能**
- **私有鍵のコピーを防ぐ。私有鍵がハードウェアートークンから外に出ない**
- **私有鍵がハードウェアトークンのOSレベルで保護される**
- **ハードウェアトークンが盗難にあった場合を想定した耐タンパ性が重要**
- **PIN (Personal Identification Number)の入力や、指紋照合といった手段でハードウェアトークンにログインする。**

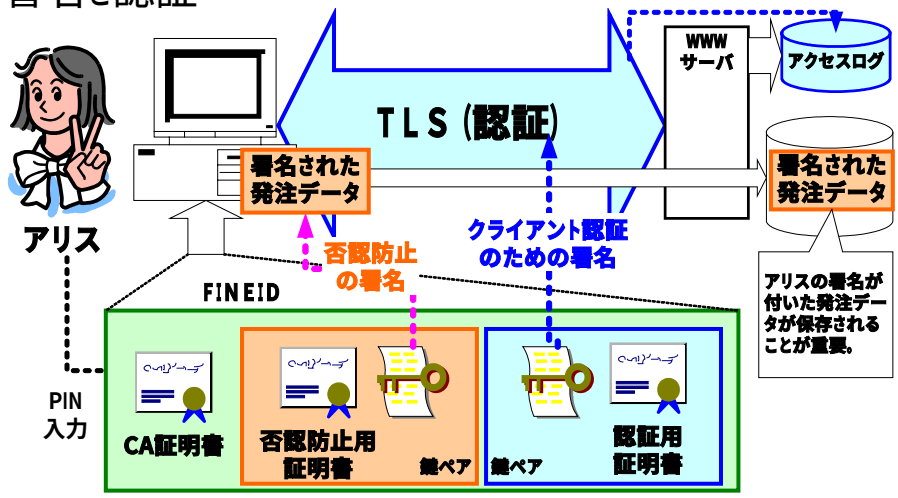


22

サブスクライバー/署名者
署名のAPI(I/F)



X.509証明書拡張
署名と認証



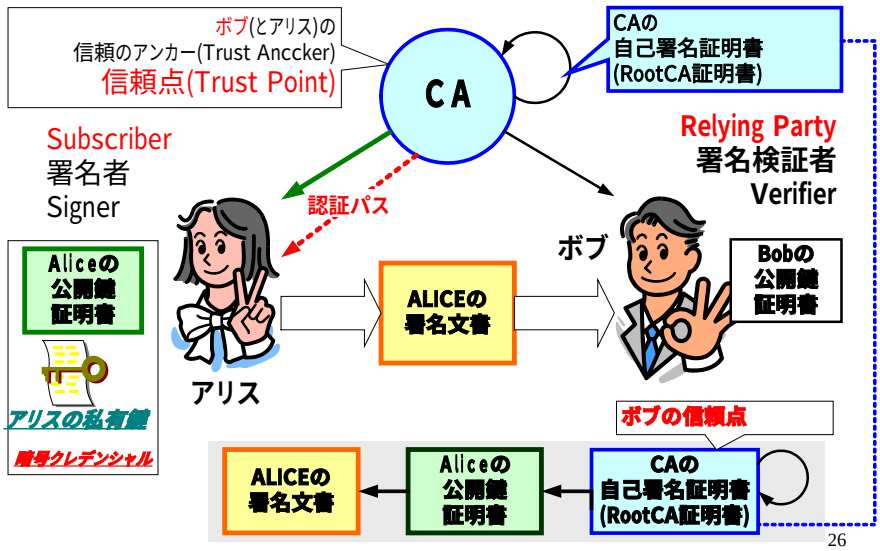
電子政府などでは、**文書に署名**され、**署名された文書が保存**されることが重要。欧州の市民カードは、**2種類の証明書**を使っている。

リライングパーティ/検証者

PIKの検証の考え方と、少し複雑なPKIの信頼モデルの説明

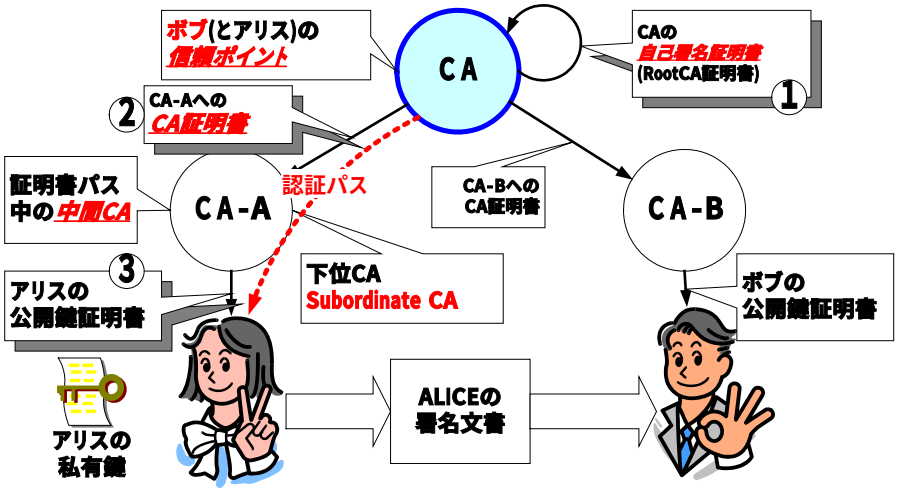
ボブは、いかにしてアリスの署名文書を信用することができるか？

リライングパーティ/検証者
PKIの基本的な信頼モデル



リライングパーティ/検証者
階層型CAモデル

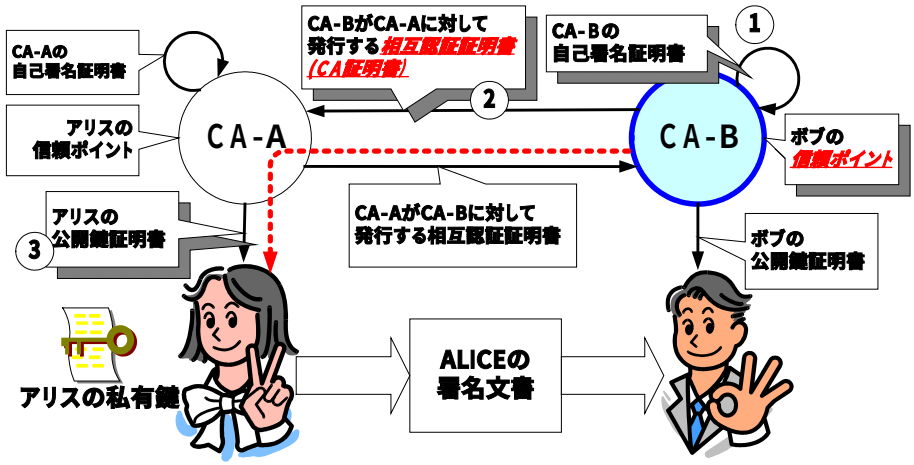
セコムIS研究所 Intelligent Systems Laboratory



27

リライングパーティ/検証者
相互認証モデル (Cross certificate)

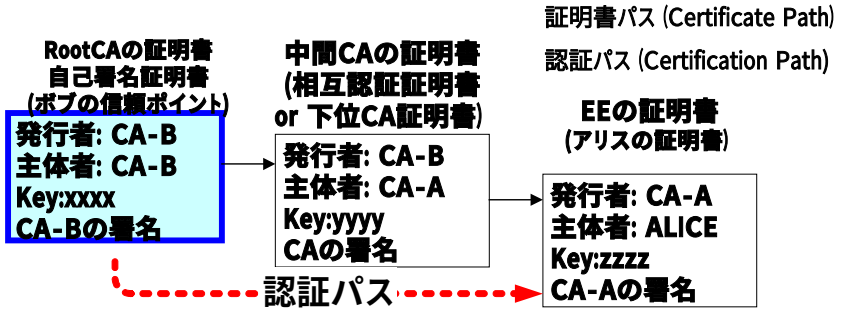
セコムIS研究所 Intelligent Systems Laboratory



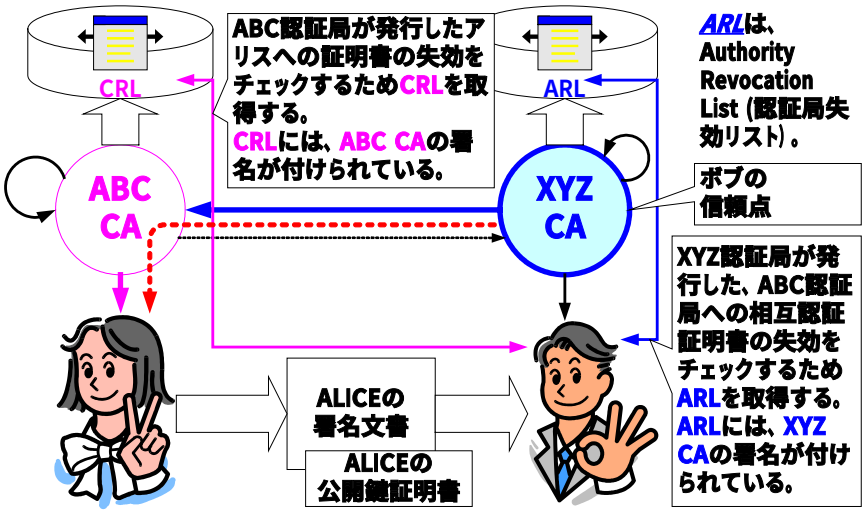
28

リライングパーティ/検証者
認証パスとは何か？

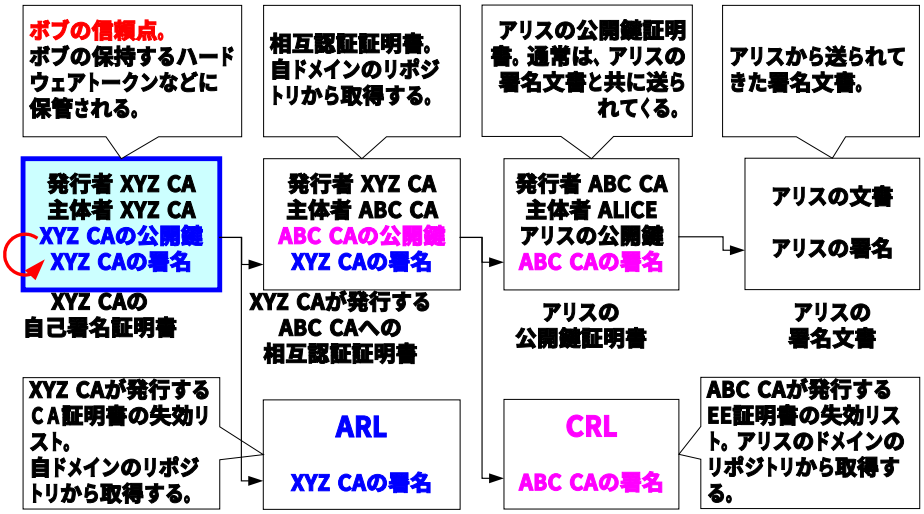
- ボブ(RP)はアリス(SC)からのメッセージを受け取った。
- ボブは、アリスからのメッセージの署名を検証したい
- 自分(ボブ)の“*信頼点*”(ボブのRootCA)からの*認証パス*を検証する
- 検証は署名のチェーンの検証だけでなく、各証明書の失効チェック、そしてX.509証明書拡張に関する検証が行われる。



リライングパーティ/検証者
相互認証モデルでのCRL/ARLによる失効情報の取得

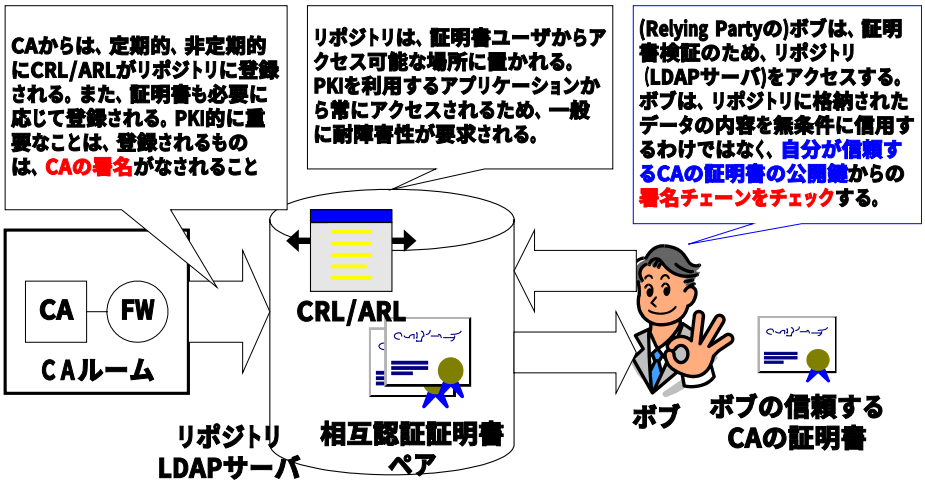


リライングパーティ/検証者
CRL/ARLと証明書検証



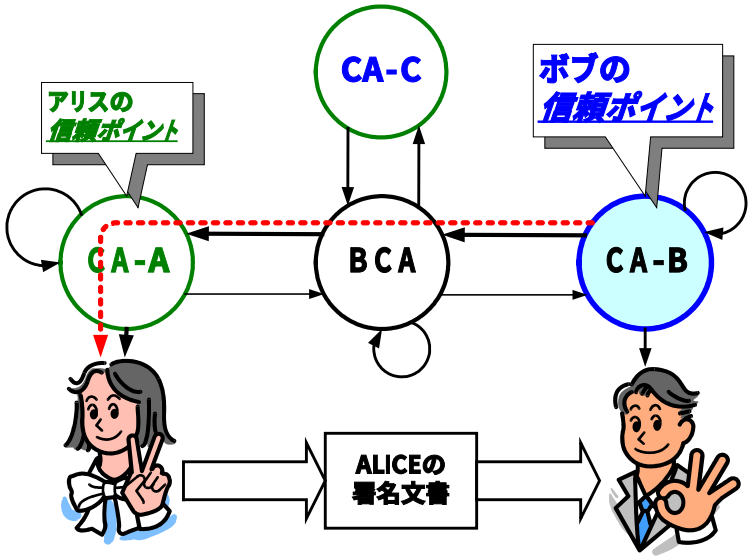
31

リライングパーティ/検証者
PKIにおけるリポジトリ



32

リライングパーティ/検証者
ブリッジモデル



33

認証局の信頼

アリスとボブの証明書を発行する認証局の信頼はどうやって確保されるのか？

34

認証局の信頼
ＣＰ／ＣＰＳの記述構成　**RFC 3647**
インターネット X.509 PKI：証明書ポリシーと認証実施フレームワーク

RFC 3647に準拠したCP/CPS

1. はじめに
2. 公開とリポジトリーの責任
3. **識別と認証**
4. 証明書のライフサイクルに対する運用上の要件
5. 設備上、運営上、運用上の管理
6. **技術的セキュリティ管理**
7. 証明書と、証明書失効リスト及びOCSPのプロファイル
8. 準拠性監査とその他の評価
9. 他の業務上の問題及び法的問題

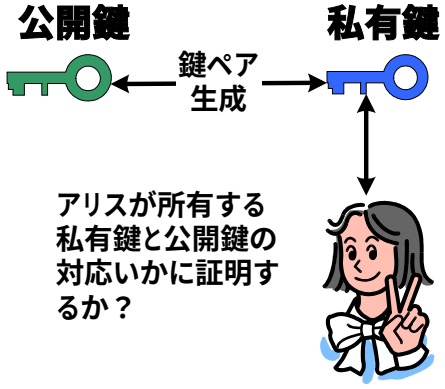
- RFC 3647
  - 2003年11月
  - http://www.ipa.go.jp/security/rfc/RFC3647JA.html
  - http://www.makino-law.jp/rfc2527-02/
    - 牧野弁護士事務所の若槻弁護士の翻訳。RFC 3647のドラフト時点の翻訳
  - 現時点ではRFC 3647の前バージョンであるRFC　2527に沿ったCP/CPSが多い。。

35

認証局の信頼
3章. 識別と認証 - IDENTIFICATION AND AUTHENTICATION

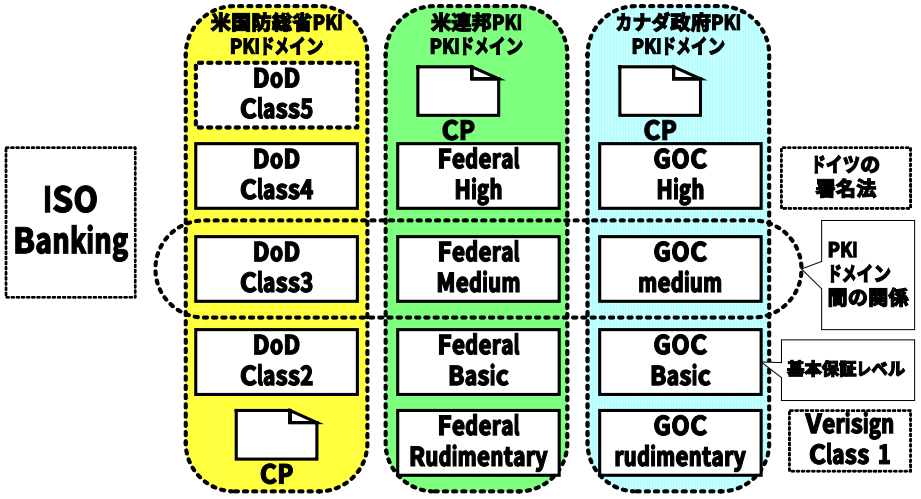
- ネーミングルール
  - 規約、解釈、ペンネームの可否. . .
  - ユニークであることの確保
- 識別、認証（個人、組織）
  - 本人又は組織の真偽の確認
  - 例：各種の公的証明書
- 初期登録／更新／失効後
  - 要求方法・手続
  - 認証方法・手続
- RFC 3647 4.3. I&A（識別と認証）
  - http://www.ipa.go.jp/security/rfc/RFC3647JA.html#043

POP: proof-of-possession
所有の証明



36

認証局の信頼
証明書ポリシと保証レベル



37

US Federal PKIのCPの例
3. IDENTIFICATION AND AUTHENTICATION
3.1.9 Authentication of individual identity

保証レベル	Identification Requirements
Rudimentary	身元確認のために要求はない。申込者は、電子メール・アドレスを送ることによって、証明書を受け取るかもしれない
Basic	Identity may be established by in-person proofing before a Registration Authority or Trusted Agent; or comparison with trusted information in a data base of user-supplied information (obtained and/or checked electronically, through other trusted means (such as the U.S. mail), or in-person); or by attestation of a supervisor, or administrative or information security officer, or a person certified by a state or Federal Entity as being authorized to confirm identities.
Medium	Identity shall be established by in-person proofing before the Registration Authority, Trusted Agent or an entity certified by a State or Federal Entity as being authorized to confirm identities; information provided shall be verified to ensure legitimacy. A trust relationship between the Trusted Agent and the applicant which is based on an in-person antecedent may suffice as meeting the in-person identity proofing requirement. Credentials required are either one Federal Government-issued Picture I.D., or two Non-Federal Government I.D.s, one of which shall be a photo I.D. (e.g., Drivers License)
High	申請者がR A に出向き、提出情報を法令に則って確認する。また、政府発行の写真付IDカード、または、ふたつの非政府発行のIDカード（ひとつは写真が必要、運転免許書など）で確認する。

38

認証局の信頼
6章　技術的セキュリティ管理

- 鍵ペア生成、鍵管理
  - CA、RA、リポジトリ、EEについて記載
  - 認証事業者側の鍵管理は最重要
  - 暗号モジュール、鍵長、Dual Control、鍵ライフサイクル管理. . .
  - CPとCPSを分けるなら. . .
    - EEの鍵管理→CP
- いわゆるコンピュータ／ネットワークセキュリティ
  - 認証業務システムの情報セキュリティ（C,I,A）
  - セキュリティ“管理”が実装されていること
- RFC 3647　4.6. 技術的セキュリティコントロール
  - http://www.ipa.go.jp/security/rfc/RFC3647JA.html#046

認証局の信頼
HSM(Hardware Security Modules)
セキュアなハードウェア鍵管理装置

- HSM　Hardware Security Modules
  - セキュアなハードウェア鍵管理装置
  - 鍵を守るための色々な仕組みを持つ
- FIPS 140-2
  - 米国標準技術院(NIST)によって1994年に策定された暗号モジュールの安全性に関する米国政府調達基準
  - FIPS 140-1と、見直された FIPS 140-2
  - 用途による複数のレベル　　Level 1　から　Level 4
  - FIPS 140-2 Level 2
    - 比較的簡易な認証局、サーバ、エンドユーザの鍵などの使用されている
  - FIPS 140-2 Level 3
    - 多くの商用の認証局で多く使用されている
- 電子署名法特定認証業務
  - FIPS 140 Level 3相当を要求

US Federal PKI のCPの例

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for cryptographic module

Assurance Level	Certification Authority	Subscriber	Registration Authority
Rudimentary	FIPS 140-2 Level 1 (HW or SW)	N/A	FIPS 140-2 Level 1 (HW or SW)
Basic	FIPS 140-2 Level 2 (HW or SW)	FIPS 140-2 Level 1 (HW or SW)	FIPS 140-2 Level 1 (HW or SW)
Medium	FIPS 140-2 Level 2 (HW)	FIPS 140-2 Level 1 (HW or SW)	FIPS 140-2 Level 2 (HW)
High	FIPS 140-2 Level 3 (HW)	FIPS 140-2 Level 2 (Hardware)	FIPS 140-2 Level 2 (HW)

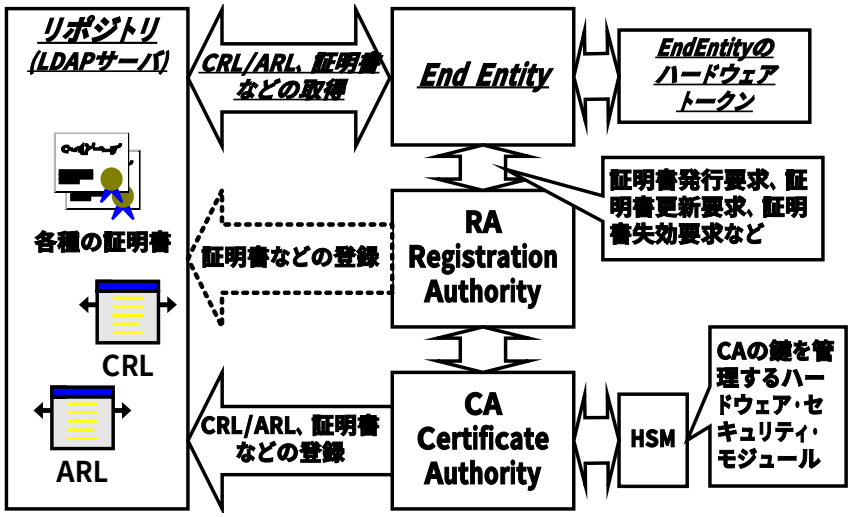
41

PKIの構成

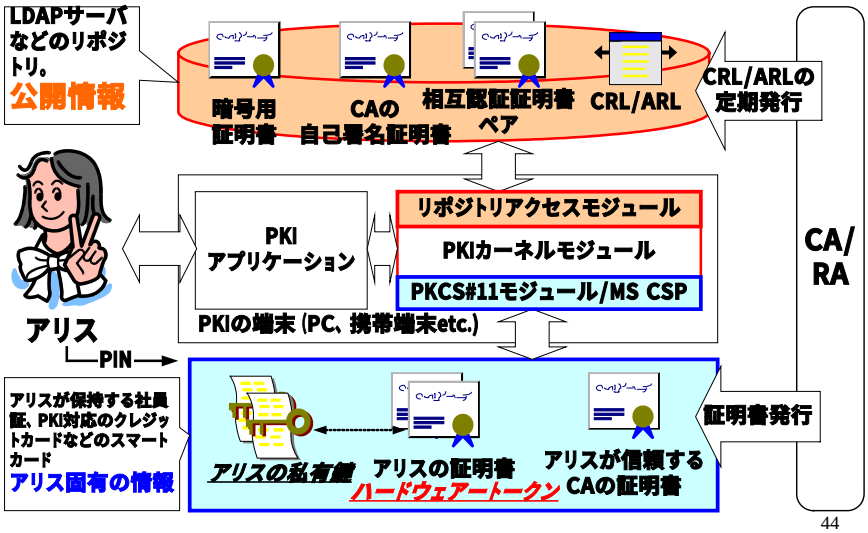
ここまで説明したことを踏まえ、PKIの構成を説明します

42

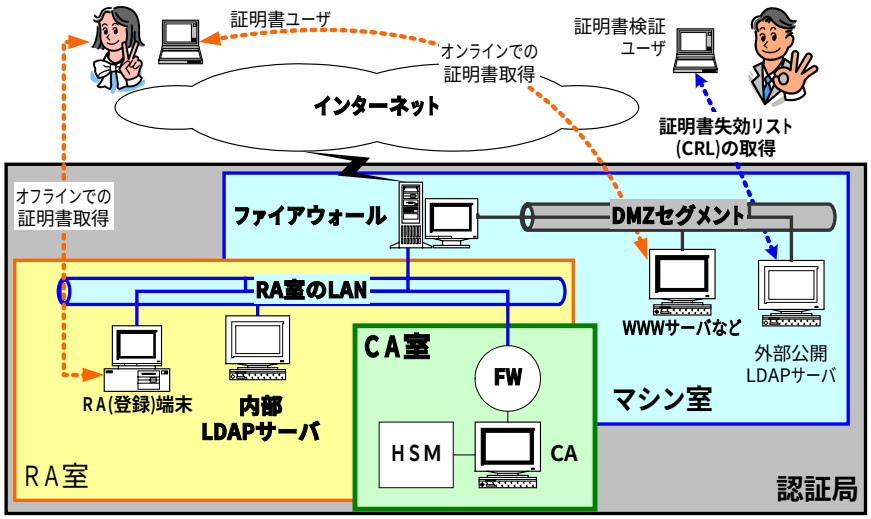
PKIの構成
PKIの基本コンポーネント



PKIの構成
PKIアプリケーションの構成例



認証局の信頼
認証局の構成例



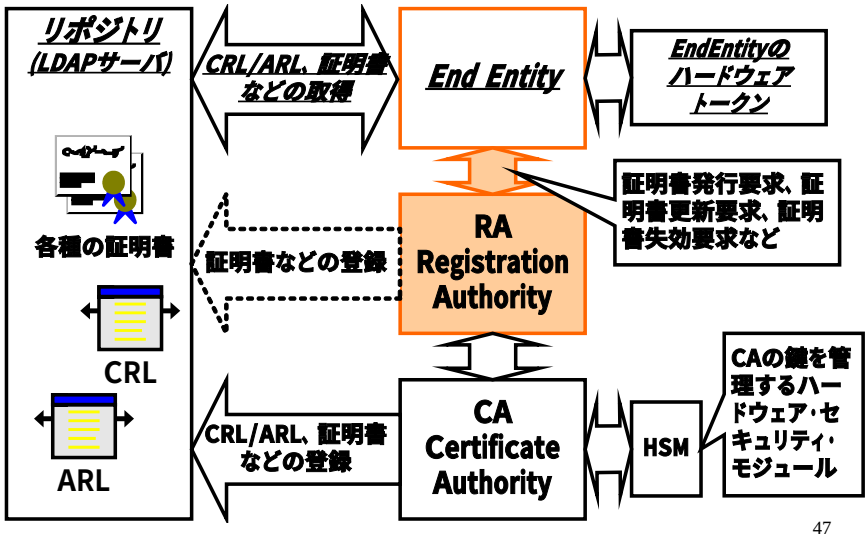
45

証明書発行

アリスの証明書はどのようにして発行されるのか?

46

証明書発行
PKIの基本コンポーネントと証明書発行



47

証明書発行
証明書発行と証明書の管理

- 鍵ペアの生成
  - EE(End Entity)での生成とCA/RA側での生成
- 証明書の要求
  - PKCS#10などの証明書要求のフォーマット
- 証明書の配布
  - オンラインでの配布
    - PKIX-CMP, SCEPなど
  - オフラインでの配布
    - FDやICカード等による配布
    - PKCS#12, PKCS#7
- その他(証明書管理)
  - 証明書の失効、証明書の更新、証明書の再発行とリカバリ

48

証明書発行
X.509証明書

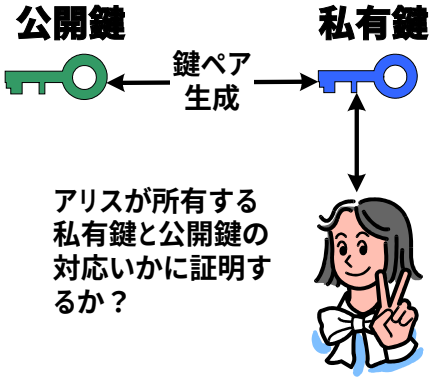
証明書バージョン番号 (V3)
証明書シリアル番号
デジタル署名アルゴリズム識別子
発行者名の識別名
有効期間
主体者 (ユーザ) の識別名
主体者の公開鍵
　アルゴリズム識別子
　公開鍵値
V3の拡張
拡張フィールド(タイプ、フラグ、値)
拡張フィールド(タイプ、フラグ、値)
CAのデジタル署名
　アルゴリズム識別子
　署名

- 代表的な公開鍵証明書
  - 主体者(アリス)と、主体者(アリス)の公開鍵や、その他の属性をCA鍵(アリスの証明書を発行したCAの署名鍵)の署名でバインドする。
  - この時、主体者(アリス)の公開鍵に対応した私有鍵は、主体者(アリス)しか使用できないことが理想。
- 1997年版 X.509 3rd Edition
  - X.509v3証明書フォーマット
    - X.509V3拡張
  - 14の標準拡張フィールド

証明書発行
CP/CPS　3章　識別と認証

- ネーミングルール
  - 規約、解釈、ペンネームの可否. . .
  - ユニークであることの確保
- 識別、認証 (個人、組織)
  - 本人又は組織の真偽の確認
  - 例:各種の公的証明書
- 初期登録／更新／失効後
  - 要求方法･手続
  - 認証方法･手続

POP: proof-of-possession
所有の証明

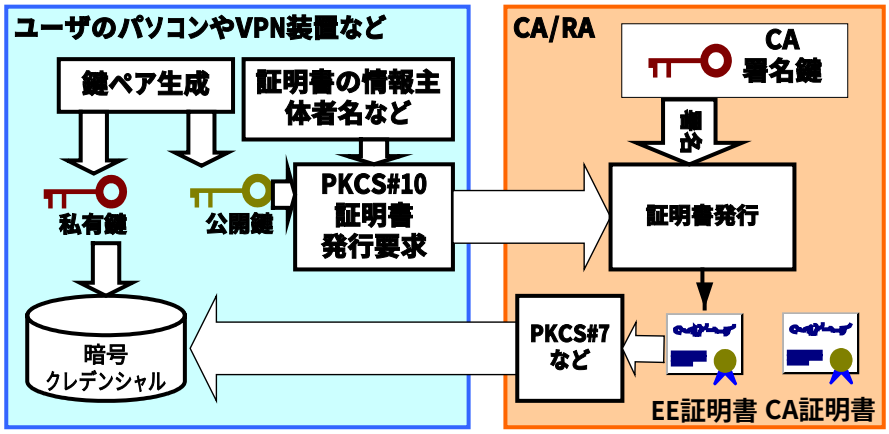


証明書発行
鍵ペアの生成と証明書発行

- EE側での鍵ペアの生成
  - 鍵とPC上で生成
    - ハードウェアートークン内部での生成が理想的
  - PKCS#10などで証明書要求を生成
  - CAで証明書を発行
  - CAからPKCS#7などで証明書を配布
- CA/RA側での鍵ペアの生成
  - CAで鍵ペアを生成
  - PKCS#12などで私有鍵、証明書を配布
    - PINなどを別途配布（別経路が望ましい）
  - ハードウェアートークンなどに格納して発行
- NTT DoCoMo **FirstPass**の例 – FOMAのPKIサービス
  - FOMAカード(UIM：User Identity Module) に鍵ペアが出荷時に格納されている。証明書要求はオンラインで行なっている。
  - http://www.nttdocomo.co.jp/p_s/firstpass/

51

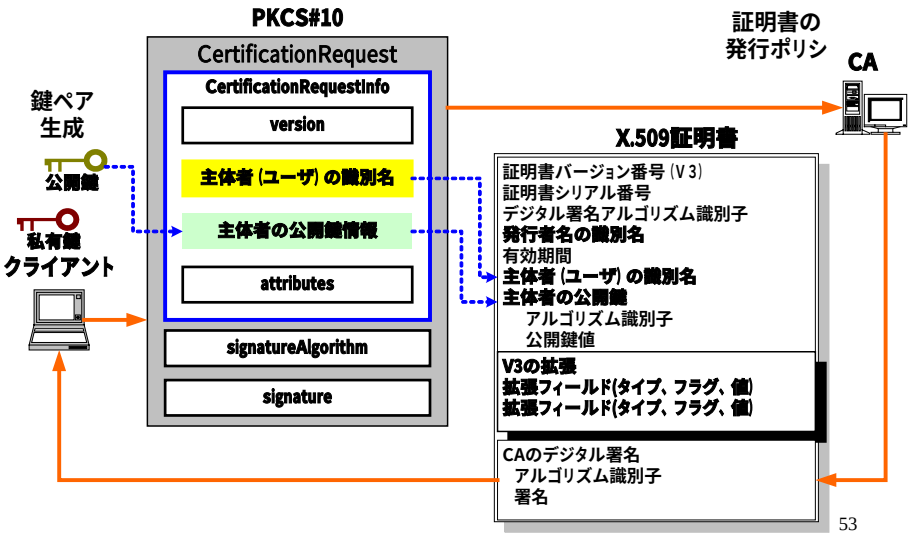
証明書発行
証明書発行（EE側での鍵ペア生成）



人に証明書発行を行なう場合、耐タンパー性のある「ハードウェアートークン内部での鍵ペア生成が理想的。またVPN装置などの場合は、装置自体が耐タンパー性を持っていることが理想的。

52

証明書発行
PKCS#10による証明書発行要求



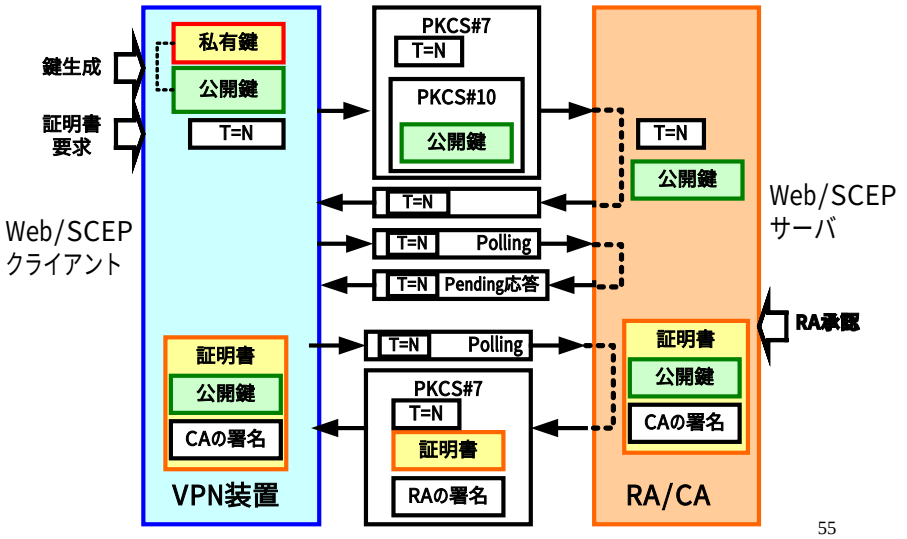
53

証明書発行
SCEP(SIMPLE Certificate Enrollment Protocol)

- SCEP
  - CISCOが仕様を作成。VPN装置などへの証明書発行が目的
  - http://www.cisco.com/warp/public/cc/pd/sqsw/tech/scep_wp.htm
- HTTPベース
  - SCEPデバイス側(VPN装置など)がHTTPのクライアトとして動作する
- メッセージに共通のデータ
  - メッセージには、トランザクションを一意に管理するためのTransaction IDが含まれる
- PKCS#10,PKCS#7などを使用した証明書要求
  - 通常の証明書要求であるPKCS#10をPKCS#7で暗号化して、他のメッセージも合わせて証明書要求メッセージを作っている
- 生成した証明書
  - PKCS#7でRAの署名がついてSCEPデバイスに返される

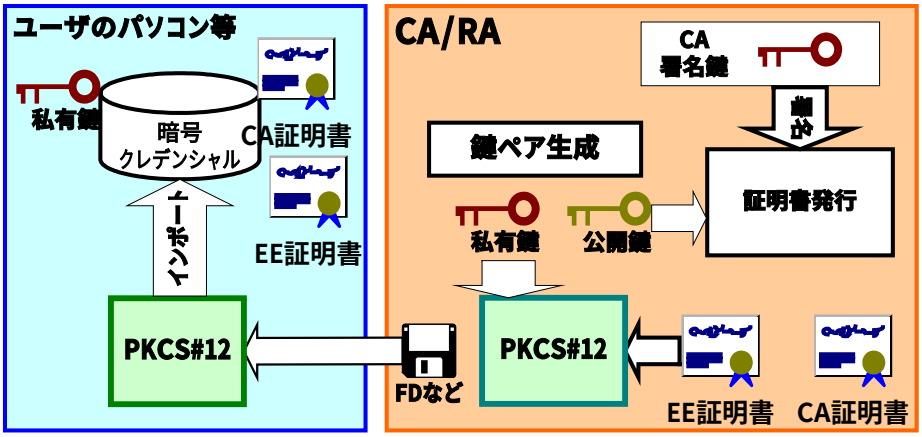
54

証明書発行
SCEPによるVPN装置への証明書発行



55

証明書発行
証明書発行（CA側の鍵ペア生成）



56

PKIの信頼性

ＰＫＩは、本当にセキュリティを提供できるのか？

セキュリティを提供するための基準は本当にあるのか？

PKIの信頼性

- 暗号アルゴリズムの信頼性
  - 暗号アルゴリズムは十分な強度を持っているか??
- 暗号モジュールの信頼性
  - 暗号に用いる鍵は、十分に保護されているか？
    - 耐タンパー性、その他 - 認証局の鍵、署名者の鍵
- 署名者の安全性
  - 署名者の鍵は、十分に保護されているか??
- 署名検証者
  - 信頼点は十分に信用が置けるものか??
  - 署名検証、証明書検証のモジュールは十分に信頼のおけるものか??
- 認証局
  - 証明書の本人確認のポリシーとのポリシーの運用
  - 鍵の運用

PKIの信頼性
関係する標準化、評価

項目	信頼性の要素	標準化、評価機関など
暗号アルゴリズムの信頼性	適切な暗号アルゴリズム、鍵長、耐用年数などの選択	CRYPTRECなど NIST、NESSIE
暗号モジュールの信頼性	評価基準	FIPS140-2
認証局	認証局のソフトウェア	ISO15408 PP
	CP/CPSのフレームワーク	RFC 3647
	認証局の認定制度	Webtrust for CA、 電子署名法特定認証業務認定
署名者の安全性	チップのセキュリティ評価	ISO15408 PP, FIPS140-2
	カードOSの評価	ISO15408 PP, FIPS140-2
	署名ソフトウェアの評価	ISO15408 PP, FIPS140-2
署名検証者	パス検証のアルゴリズム	RFC 3280
	パス検証ソフトウェアの評価	ISO 15408 PP (NIST PP draft)

59

参考
インターネット上のリソース

- PKI 関連技術解説
  - http://www.ipa.go.jp/security/pki/
  - IPAの報告書で比較的初心者向き
- セコムIS研究所　サイバーセキュリティ読本
  - http://www.secom.co.jp/isl/j/cs_reader/index.html
  - http://www.secom.co.jp/isl/j/cs_reader/pki/index.html

60