セコムIS研究所
Intelligent Systems Laboratory

サブスクライバー/署名者

サブスクライバー/署名者

セコム IS 研究所
Intelligent Systems Laboratory

- 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
  - セキュアな装置のセキュリティ基準
    - 欧州の電子署名では、SSCD （Secure signature creation device)としてその要件を定義
    - 米国では、FIPS 140-2レベル2などの調達基準
  - 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、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

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。また、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)

サブスクライバー/署名者
ハードウェアトークンの例

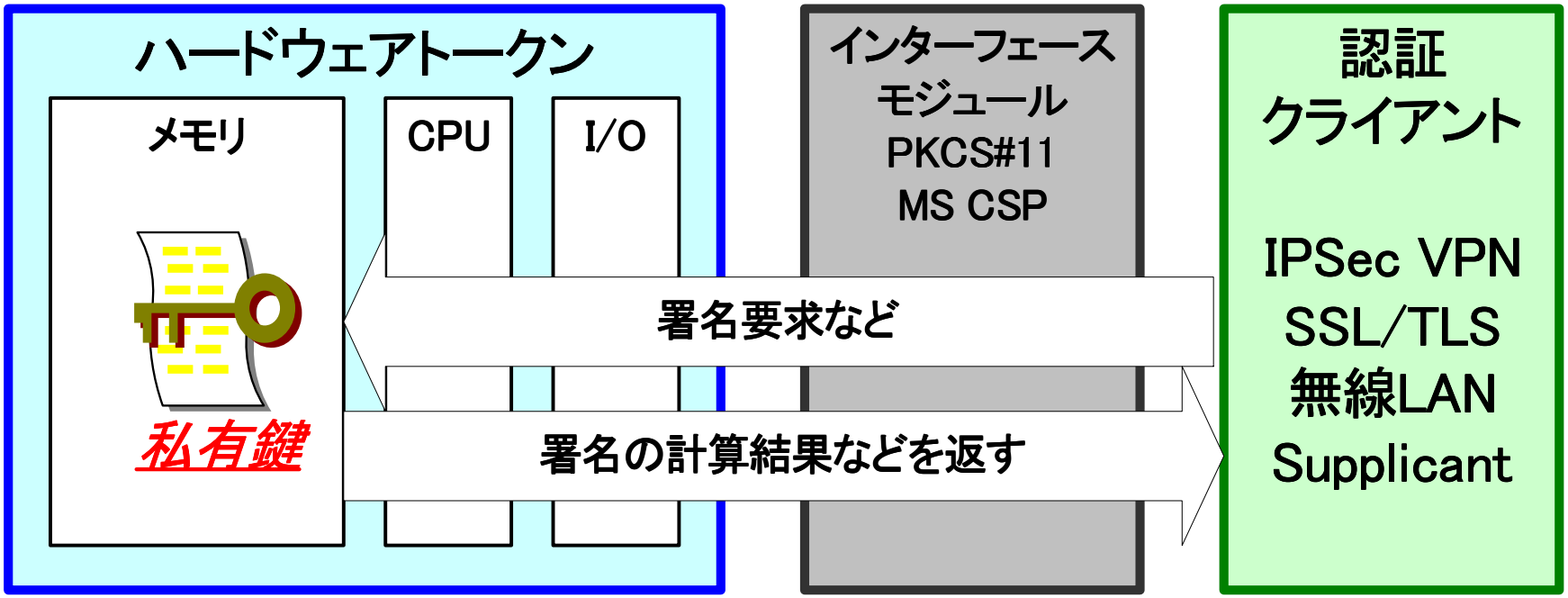
セコムIS研究所
Intelligent Systems Laboratory

- 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-710)など
- PCに内蔵されたセキュリティチップ
  - TCG 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同じ
- 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

サブスクライバー/署名者
なぜハードウェアトークン

セコム IS 研究所
Intelligent Systems Laboratory

- 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。



サブスクライバー/署名者
ハードウェアトークンとのI/F

- スマートカードリーダとのI/F
  - PC/SC
    - スマートカードリーダを仮想化する
      - USB、RS232C、PCMCIA、etc..
    - 主にWin32環境
- トークンとのAPI（PKCS#11、MS CryptoAPI）
  - PKIアプリケーションとハードウェアトークンとのAPI
  - 私有鍵などのトークンオブジェクトを保護するメカニズムを持っている
  - スマートカード以外のUSB Token などでも同じ

サブスクライバー/署名者
PKIクライアントとCryptoAPI

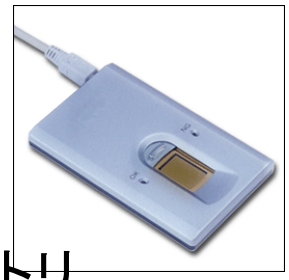
セコムIS研究所
Intelligent Systems Laboratory

PKIによる認証クライアントのレパートリ

Webクライアント SSL-VPN (MS IE)	無線LAN クライアント (MS Supplicant)	IPSec VPN Client CISCO　VPNクライアント

CryptoAPI

Microsoft Base CPS	ICカード (Activcard) のCSP	USBトークン (Aladin) のCSP	指紋認証 (Sony Puppy) のCSP	TCPA/TPM (IBM ThinkPad)の CSP

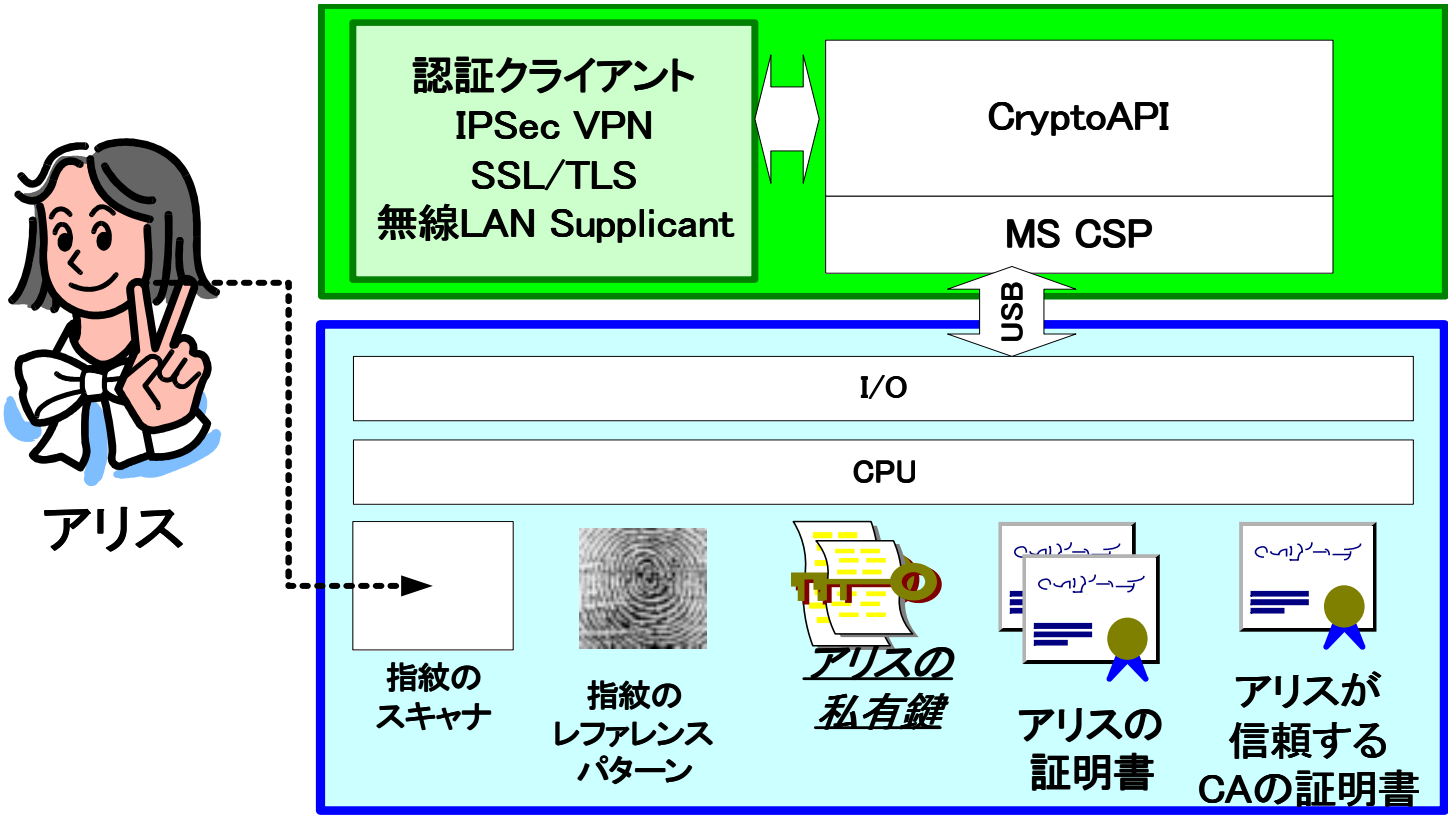



組み込みセキュリティー・チップ

PKIによる暗号クレデンシャルのレパートリ

CSP : Cryptographic Service Provider

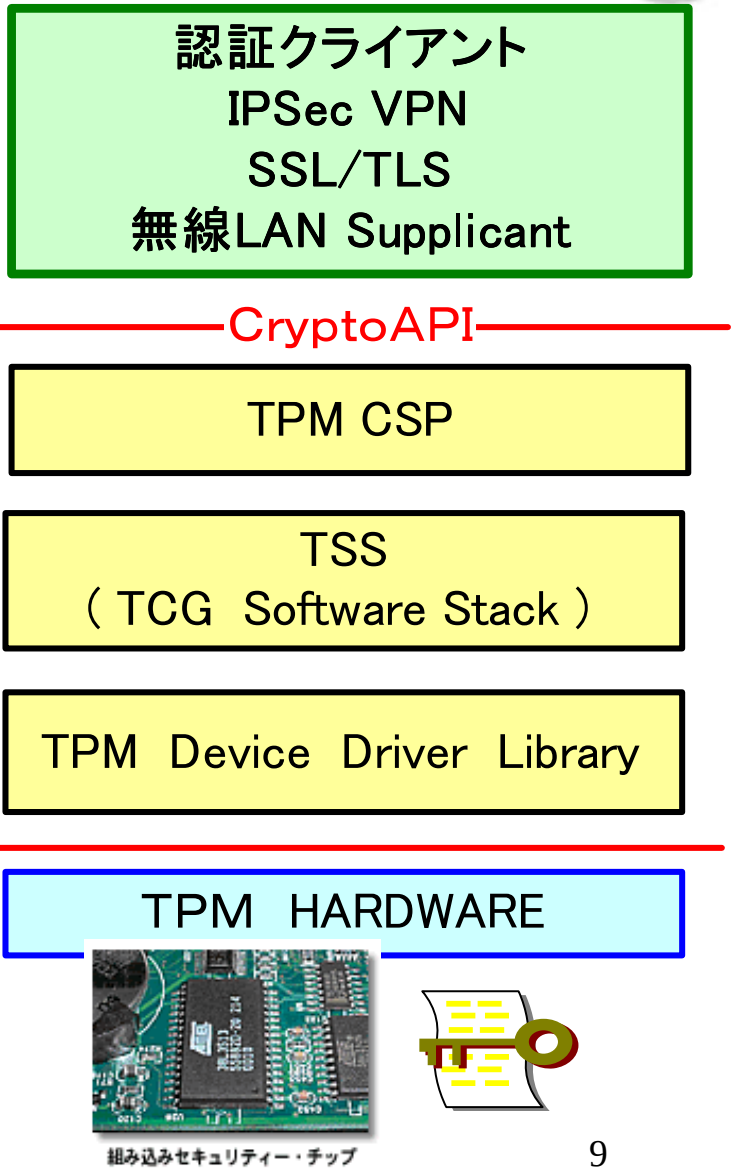
サブスクライバー/署名者
バイオメトリクス認証とPKI



•装置の中に私有鍵、指紋のレファレンスパターンなどが格納される。これらがこの装置から外部へ出ない。*私有鍵、指紋といった個人の情報がネットワークに流れないことが重要*

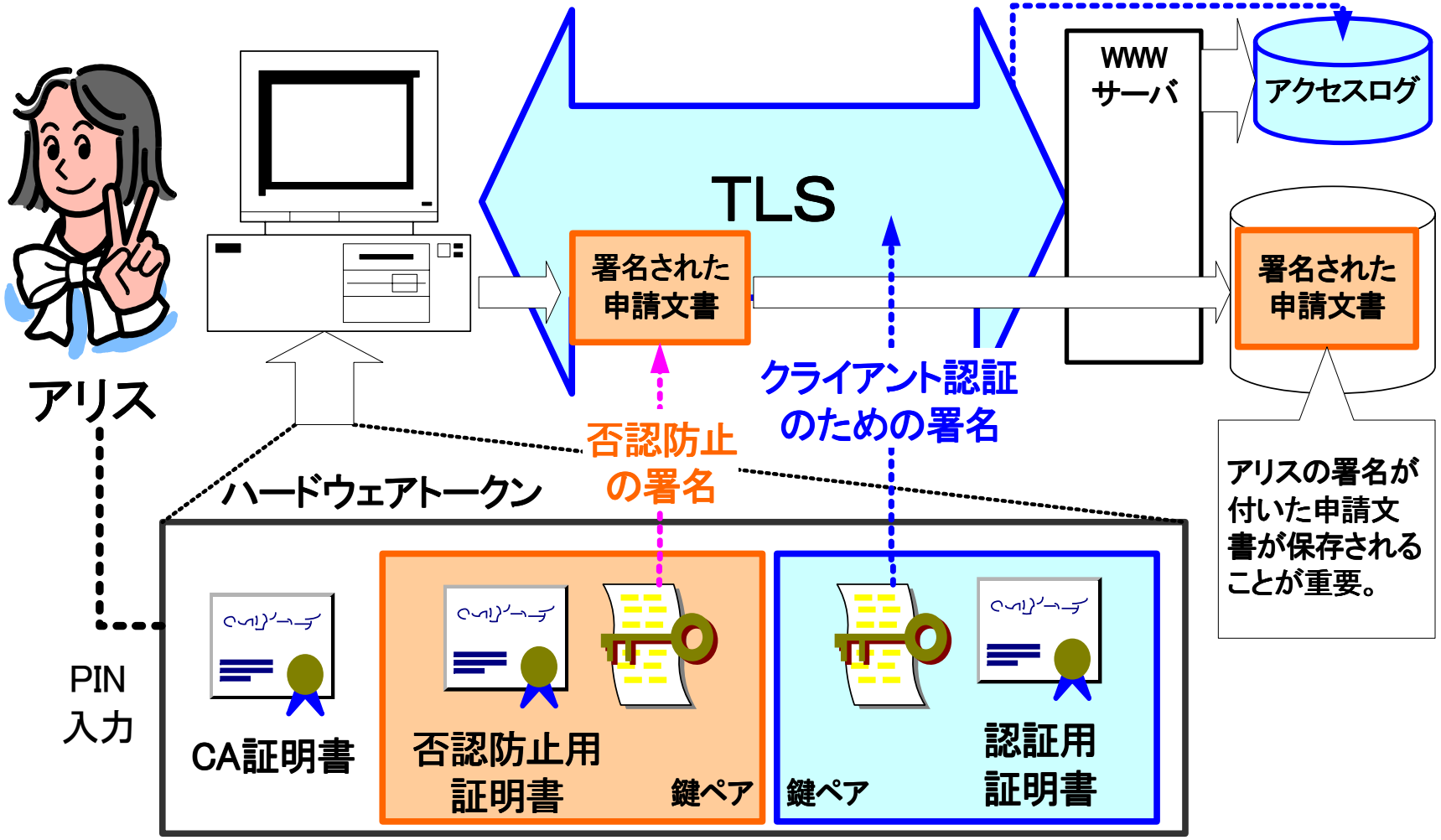
サブスクライバー/署名者
TCGのTPM

- TCG(Trusted Computing Group)
  - 1999年に結成されたTCPA(Trusted Computing Platform Alliance)がTCGとして発展的に再構成
  - Compaq, HP, IBM, Intel, Microsoft により設立
  - コンピュータデータのセキュリティを高めるための仕様を策定
- TCPAのセキュリティチップ
  - トラステッド・プラットフォーム・モジュール(TPM)
  - マザーボードに組み込まれたPKI対応スマートカードのようなもの
- IBMのセキュリティチップ搭載パソコン
  - ATMEL (AT90SP0801) を採用
  - ISO15408 EAL3 Augmented
  - Crypto API、PKCS#11に対応



サブスクライバー/署名者
PKIにおける認証と署名の違い

セコムIS研究所
Intelligent Systems Laboratory



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。

サブスクライバー/署名者
署名のAPI(I/F)