セコムIS研究所
Intelligent Systems Laboratory

IC・ID カードの相互運用可能性向上に係る基礎調査
シーズ編

2007年3月28日

セコム㈱ IS研究所
PKI相互運用技術WGリーダー
松本　泰

シーズ調査の概要
シーズ調査のコンセプト

セコム IS 研究所
Intelligent Systems Laboratory

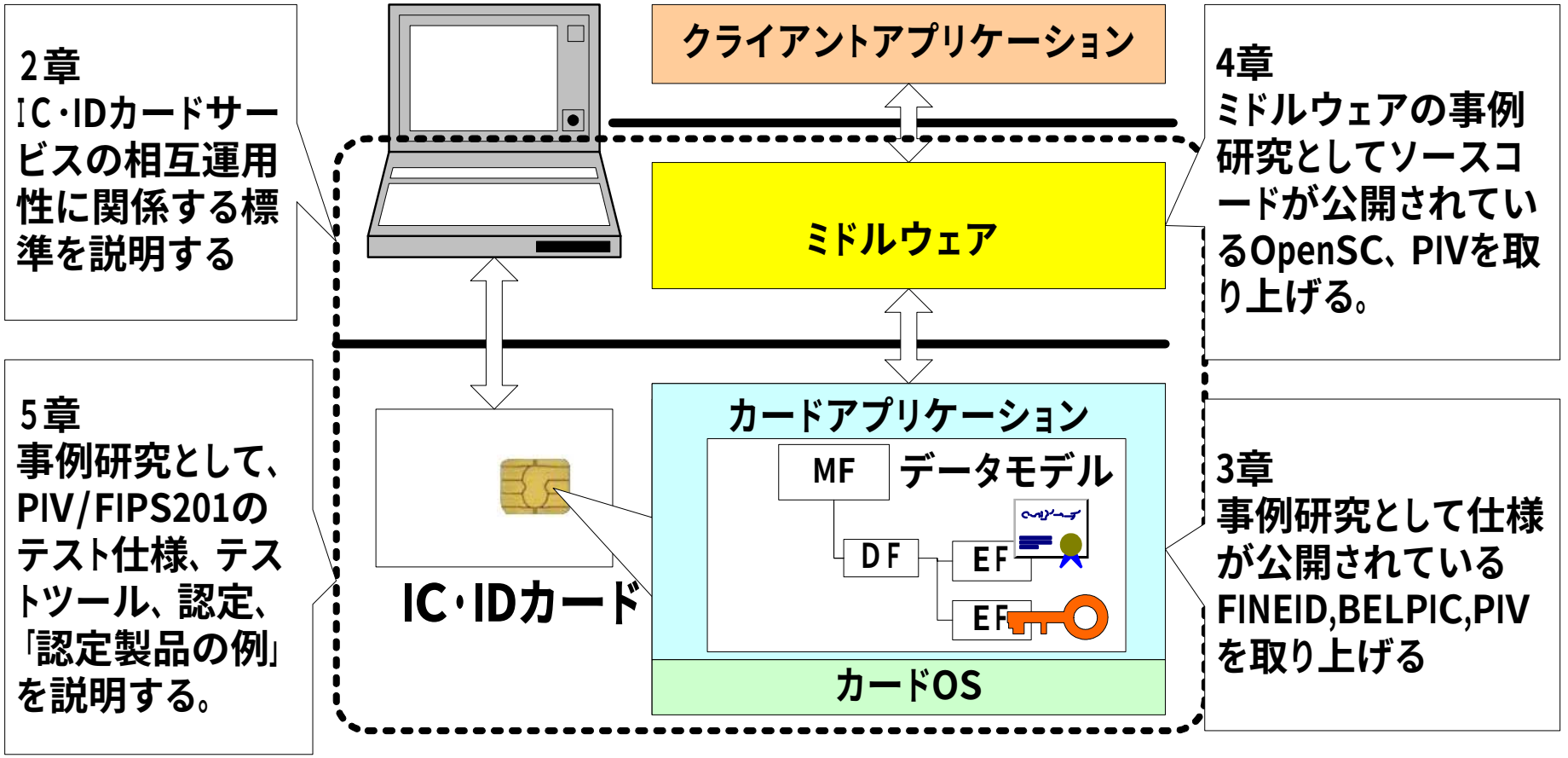
- (1) IC・IDカード（サービス）の全体像を簡潔に記述し相互運用可能性の問題を分かり易く説明
  - PKIを扱ったICカードと、このICカードに対応したミドルウェア、PKIアプリケーションの関係を簡潔に説明する。相互運用可能性の問題は、技術上の問題だと思われている。現実的には、相互運用可能性の問題の解決には、様々なステークホルダー間の調整が必要であり、共通認識としての全体のアーキテクチャと相互運用可能性の問題をステークホルダー間で共有する必要がある。
- (2) ミドルウェアの重要性の説明
  - 一般にICカードと言えば、ICカードとカード上のアプリケーションに焦点が当てられている。しかし、PKIを扱うICカードの場合、カードアプリケーションよりも、PC側のミドルウェアの扱いが難しい。こうしたことと説明する。
- (3) 調達者、認証システムの設計者、開発者等の視点を重視し、標準、仕様、実装をバランスよく説明
  - 公開されているIC・IDカードの仕様やミドルウェアのソースコードを説明することで、複雑なミドルウェアなどの相互運用可能性の問題を標準、仕様、実装のそれぞれの面から説明する。
- (4) 今後の方向性の示唆

シーズ調査の概要
調査報告書(シーズ編) の構成

セコム IS 研究所
Intelligent Systems Laboratory

章	大項目	中項目	コンセプト＆内容
1	概要 28 Page	ICカードの概要 相互運用可能性の概要	IC・IDカードのサービス、アーキテクチャをバランスよく記述し、その上で、相互運用可能性の課題の概要を説明する
2	相互運用可能性に関連した標準 33 Page	ISO/IEC 7816-4,8,9 ISO/IEC 7816-15、 ISO/IEC 24727	相互運用可能性に関連したIC・IDカードの標準を簡潔に説明する。特に3章、4章を説明する上で理解が欠かせない部分について説明する。
3	IC・IDカードの実装例 28 Page	FINEID (フィンランド) BELPIC(ベルギー) PIV(米国)	事例研究として、相互運用可能性を配慮して発行されているIC・IDカードの実際の仕様を説明する。
4	ミドルウェアの実装例 45 Page	OpenSC PIV(米国)	事例研究として、ミドルウェア実装を説明する。実際の実装が相互運用可能性の問題にどの様に対処しているかに焦点を当てる。
5	PIVのテストと認定 18 Page	PIV(米国)	事例研究として、テスト仕様、テストツール、認定制度、認定製品の例としてPIV/FIPS201を説明する。

シーズ調査の概要
調査報告書(シーズ編) の構成　(続き)



3章、4章、5章は、事例研究

シーズ調査の概要
IC・IDカード（サービス）の事例研究

セコムIS研究所
Intelligent Systems Laboratory

IC・IDカード	説明	報告書の意図
FINEID フィンランド	FINEIDは、フィンランド国民ICカードであり、1999年末から発行されている。ISO/IEC 7816-15に準拠している。	PKCS#15に準拠したカードの事例 IC・IDカードのとしてオープンで簡潔な仕様を提示している。ミドルウェアとしてOpenSCが利用できる。
BELPIC ベルギー	BELPIC(Belgian Personal Identity Card)は、ベルギー国民ICカード 全面的導入は 2004 年にスタートしている。2006年10月現在400万枚以上のカードが発行されている。	PKCS#15に準拠したカードの事例 OpenSCを中心にミドルウェアを構成しており、多くのBELPICをサポートするソフトウェア(ミドルウェアとアプリケーション)のソースコードが公開されている。
PIV 米国	米国政府全体を対象とするセキュアで信頼性のある身分証標準を規定する大統領指令（HSPD-12）に基づき発行されるICカード。 各政府機関は、NISTが策定したFIPS-201に準拠するカードを2006年10月27日までに、発行開始	大量のドキュメントが公開されている。 ミドルウェア(PIVミドルウェア)のレファレンス実装のソースコードが公開されている。 PIVカードアプリケーション、PIVミドルウェアの認定制度(NPIVP)がある。

セコムIS研究所
Intelligent Systems Laboratory

事例研究
ベルギーのＢＥＬＰＩＣ

Q.

なぜ、身近に使えない海外の事例なの？

A.

それはね、国内で技術仕様が公開されたよい事例がないからなんだよ。。。。。

BELPIC (Belgian Electronic Identity Card)

- BELPIC
  - 12歳以上の全国民に配布されるカード
    - 否認防止の署名用証明書は18歳以上
- カード保有者のふたつの証明書と、それぞれに対応したRSAプライベート鍵
- カードエッジI/F
  - ISO/IEC 7816-4,8準拠
- データモデル
  - PKCS#15に準じたファイルレイアウト
- ミドルウェア
  - ベルギー政府によって提供されるオフィシャル・ミドルウェアは、OpenSCをベースにした、オープンなソース・ライセンスの下で利用できる。

課題

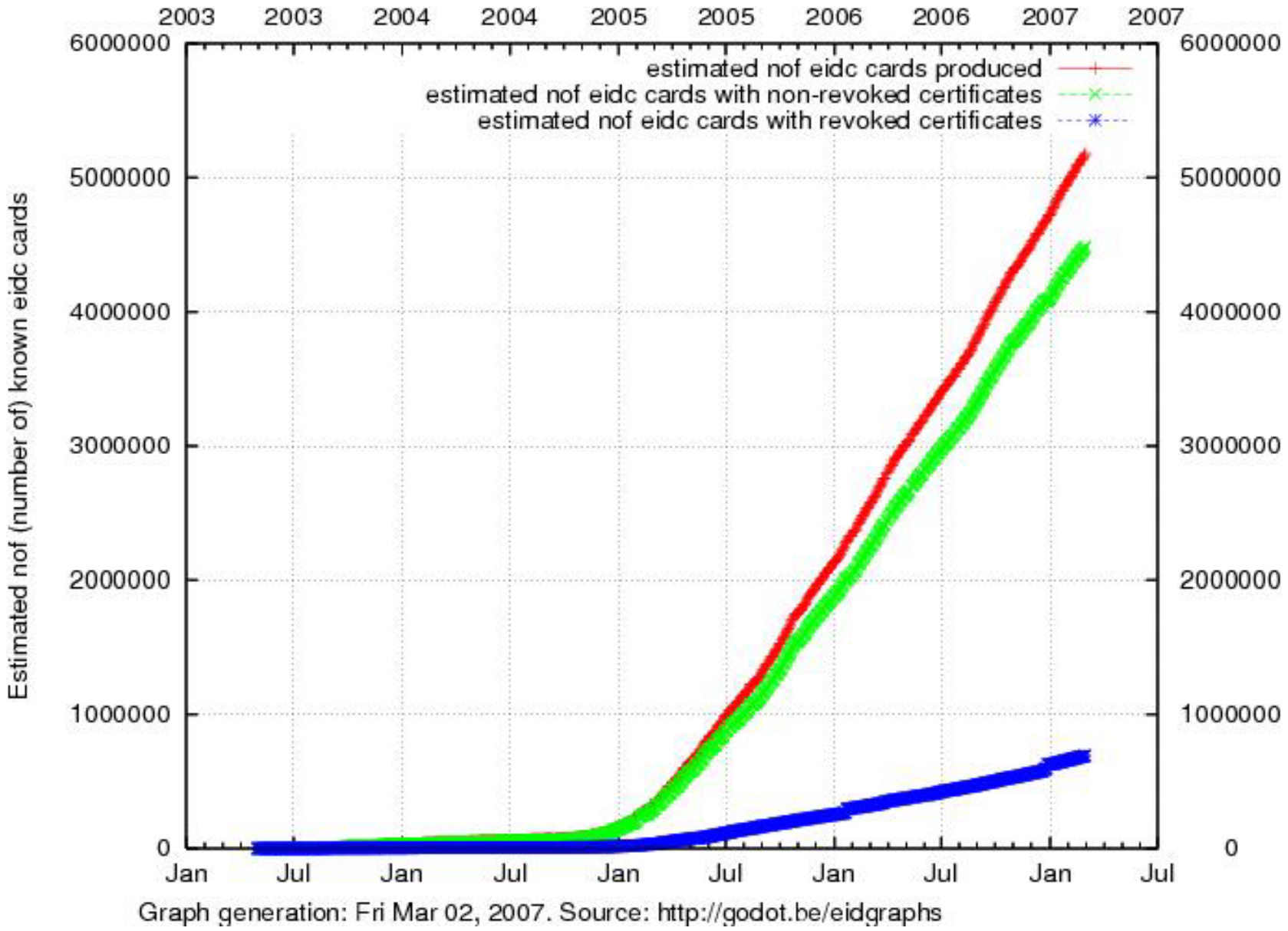
ベルギーの最近の調査（2006年）では、ベルギーのインターネット利用者の43%はeIDカードを現在所有しているものの、電子カード・リーダーを所有しているのはわずか8%であることが明らかになった。

http://www.ecom.jp/report/Study_on_PKI_2006_in_EUROPE-FINAL.pdf

BELPICに関するお薦めサイト
http://homes.esat.kuleuven.be/~decockd/wiki/bin/view.cgi/Eid/EidForum

BELPICの発行枚数

セコムIS研究所
Intelligent Systems Laboratory



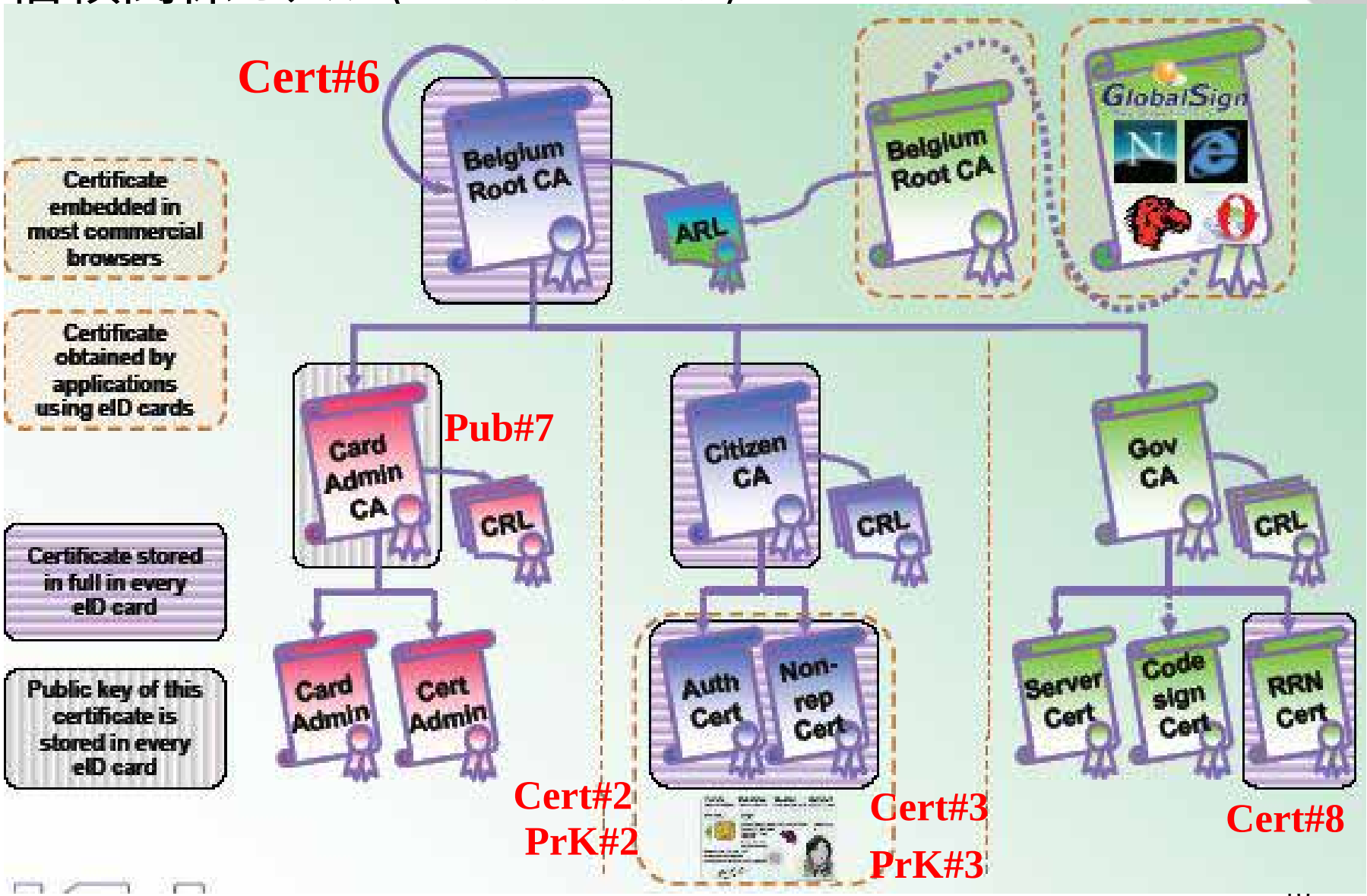
ベルギーのBELPICと公的個人認証サービスの比較

セコムIS研究所 Intelligent Systems Laboratory

比較項目	BELPIC	公的個人認証サービス
配布対象	12歳以上の全国民	15歳以上の希望者
配布枚数	450万枚(2007年3月現在)	18.3万枚 (2006年10月末現在)
プラットフォーム対応	Windows,Mac,Linuxに対応	Windowsのみ。Macの対応が一部なされている。
ミドルウェアとユーティリティ	オープンソースが多く利用されており、専用ソフトのソースコードも数多く公開されている	バイナリコードを無償で配布
カードエッジI/F	カードエッジI/F　公開 7816-4,8に準拠	非公開
カード内のデータモデル	公開 PKCS#15に基づく	非公開
格納されるEE証明書	否認防止用の証明書 認証用の証明書	否認防止用の証明書のみ

BELPIC (ベルギー)
信頼関係モデル (Trust Model)

セコムIS研究所
Intelligent Systems Laboratory



http://homes.esat.kuleuven.be/~decockd/site/EidCards/belpic/mySlides/belgian.eid.card.technical.overview.pdf

BELPIC (ベルギー)
カードに格納されるクレデンシャル

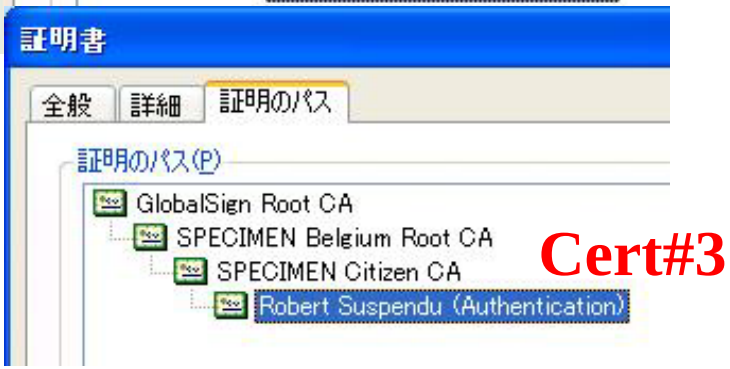
セコム IS 研究所
Intelligent Systems Laboratory

#	Private Key	証明書	備考
1	PrK#1	-	カード認証用(内部認証用)
2	PrK#2	Cert#2	認証用　PIN(認証)
3	PrK#3	Cert#3	否認防止用　PIN(署名) 署名毎にPINが必要
4	PrK#4	Cert#4	Citizen's CA certificate
6	PrK#6	Cert#6	Root CA 信頼点となる自己署名証明書
7	PrK#7	Cert#7	Pub#7 外部認証用　Role証明書
8	PrK#8	Cert#8	RRN証明書

BELPIC (ベルギー)
証明書パス (Certificate Path)

セコム IS 研究所
Intelligent Systems Laboratory

テスト用証明書



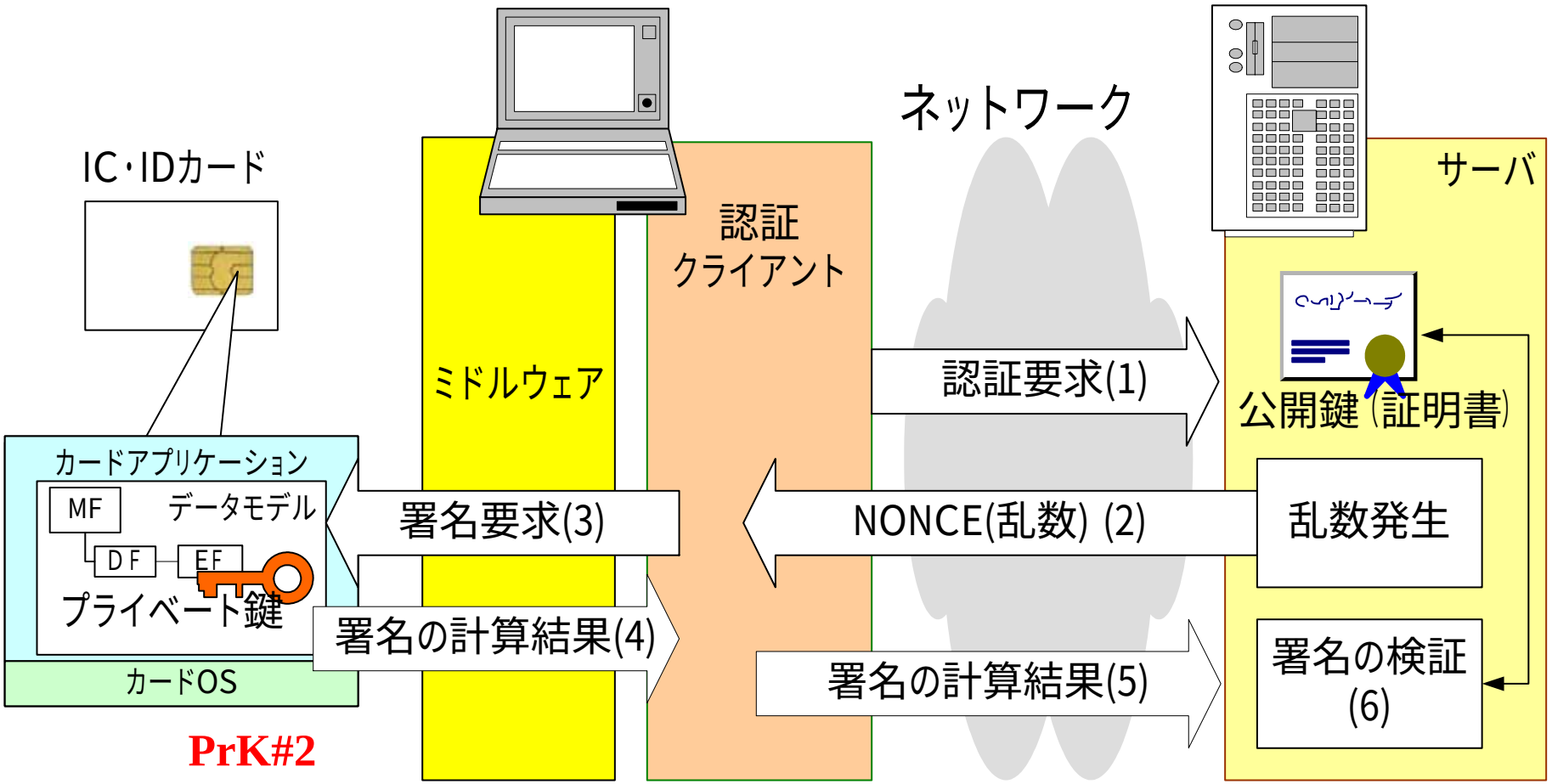
多分。。属性認証局向け

多分。。外国人向け認証局

- IC・IDカードの仕様を理解する上で、信頼関係モデルの理解は欠かせない。どこで暗号化や署名で行なわれ、どこで検証が行われるか、そのために、どこに耐タンパー性が必要なのか。システム全体のセキュリティとしては、こうしたことの理解なしにIC・IDカードの仕様は作れない。

IC・IDカードに要求される機能
認証(Authentication)

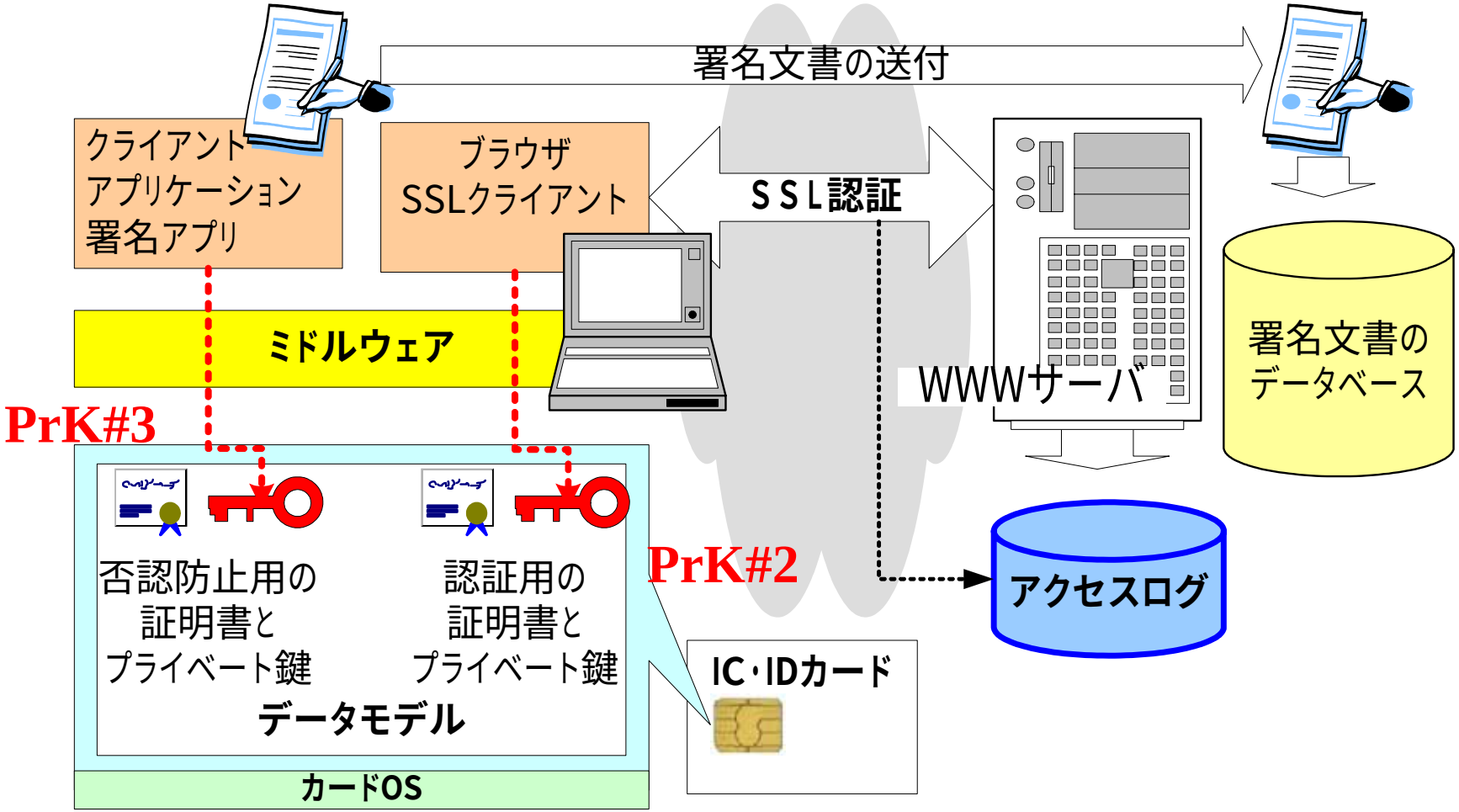
セコムIS研究所
Intelligent Systems Laboratory



- カード上で署名操作が行われる
- 鍵はカードから外部に出ない

IC・IDカードに要求される機能
(否認防止の) 署名と認証(Authentication)

セコムIS研究所
Intelligent Systems Laboratory



- 目的に応じたプライベート鍵と証明書が格納される
- 目的によりプライベート鍵に対するアクセス制御ルールも異なる

プライベート鍵と証明書の扱いの比較

セコムIS研究所
Intelligent Systems Laboratory

IC・ID カード	カード保有者の証明書	証明書に対応した「プライベート鍵」の利用に関する説明
BELPIC ベルギー	認証用の証明書 Cert#2	認証（のための署名）に使用する。復号には使用できない（暗号には利用できない）。PrK#2
	否認防止の署名用証明書（18歳以上のみ） Cert#3	署名操作のみ。署名操作毎にPINによるカード保有者の認証が必要。 PrK#3
PIV 米国	認証用の証明書	認証（のための署名）に使用する。
	否認防止の署名用証明書 (オプション)	署名操作のみ。署名操作毎にPINによるカード保有者の認証が必要。
	暗号用の証明書 （オプション）	発行者により「鍵」のバックアップがなされる。
公的個人認証サービス	否認防止の署名用証明書	署名操作のみ。 否認防止用の証明書のみ発行される。

データに対する操作

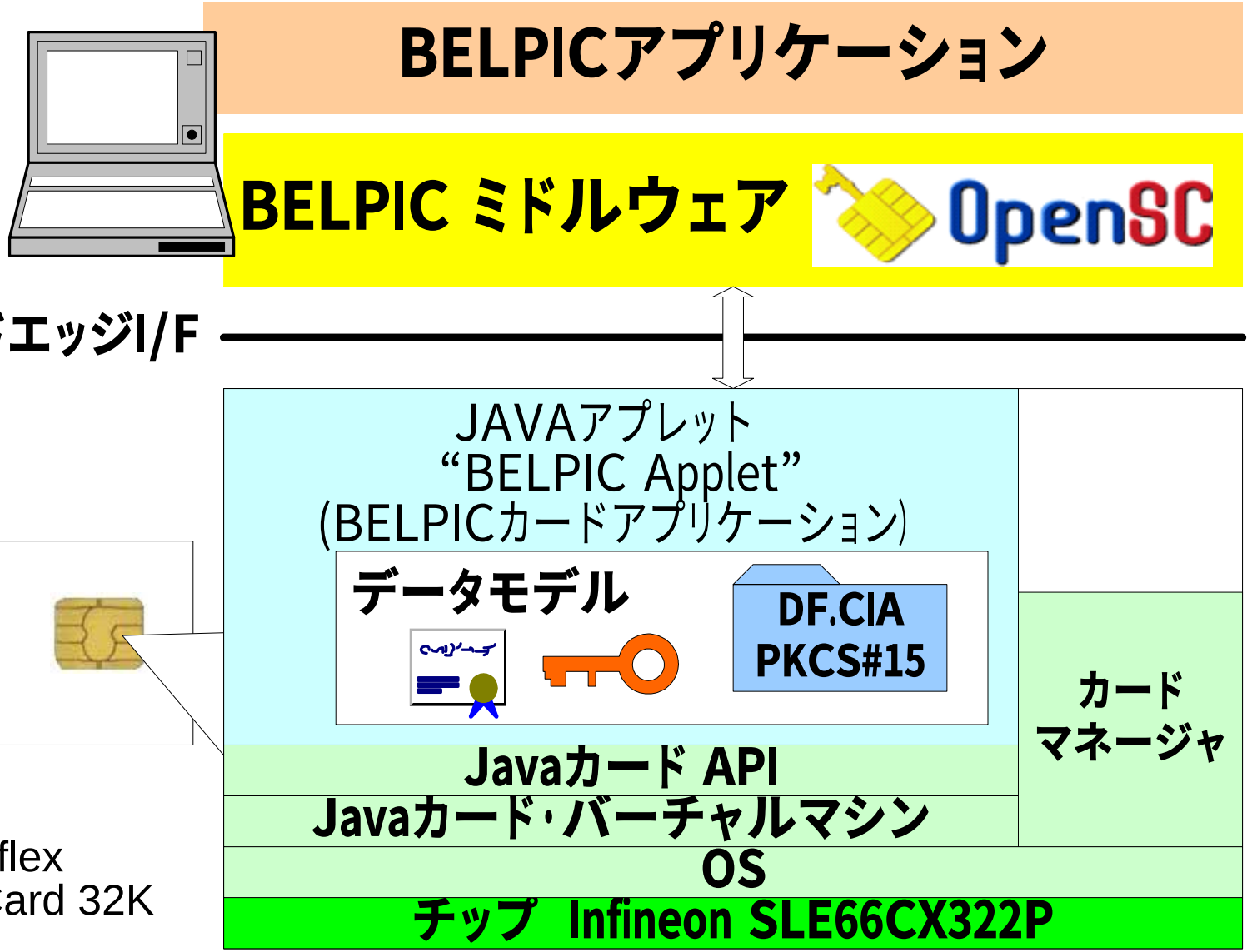
セコムIS研究所
Intelligent Systems Laboratory

データ	データに対する操作 カードエッジインターフェース	説明
プライベート鍵 Private Key	署名操作 (PSO: COMPUTE DIGITAL SIGNATURE) 復号 (PSO: DECIPHER)	認証(Authentication)に使う鍵(PrK#2) 否認防止の署名に使う鍵(PrK#3) 復号 (BELPICでは使用せず)
公開鍵 Public Key	署名検証 (PSO: VERIFY DIGITAL SIGNATURE) 暗号 (PSO: ENCIPHER)	署名 (認証も含む) 目的の場合IC・IDカード上で公開鍵の演算 (暗号化) を行なう必要はない。 IC・IDカード自体が外部を認証する (外部認証) の場合、カード上での署名検証が要求される。 BELPICのPub#7
証明書	READ BINARY GET DATA	カード保有者が、署名検証を行う場合、カードに格納された信頼点の証明書(Cert#6)の公開鍵を利用する。また、暗号化を行なう場合、カード保有者の証明書の公開鍵を利用する。
認証情報	VERIFY RESET RETRY COUNTER	カード保有者をIC・IDカードが認証する PINやバイオメトリクステンプレートなど

** PSO :Perform Security Operation

BELPIC (ベルギー)
IC・IDカードの実装

セコム IS 研究所
Intelligent Systems Laboratory



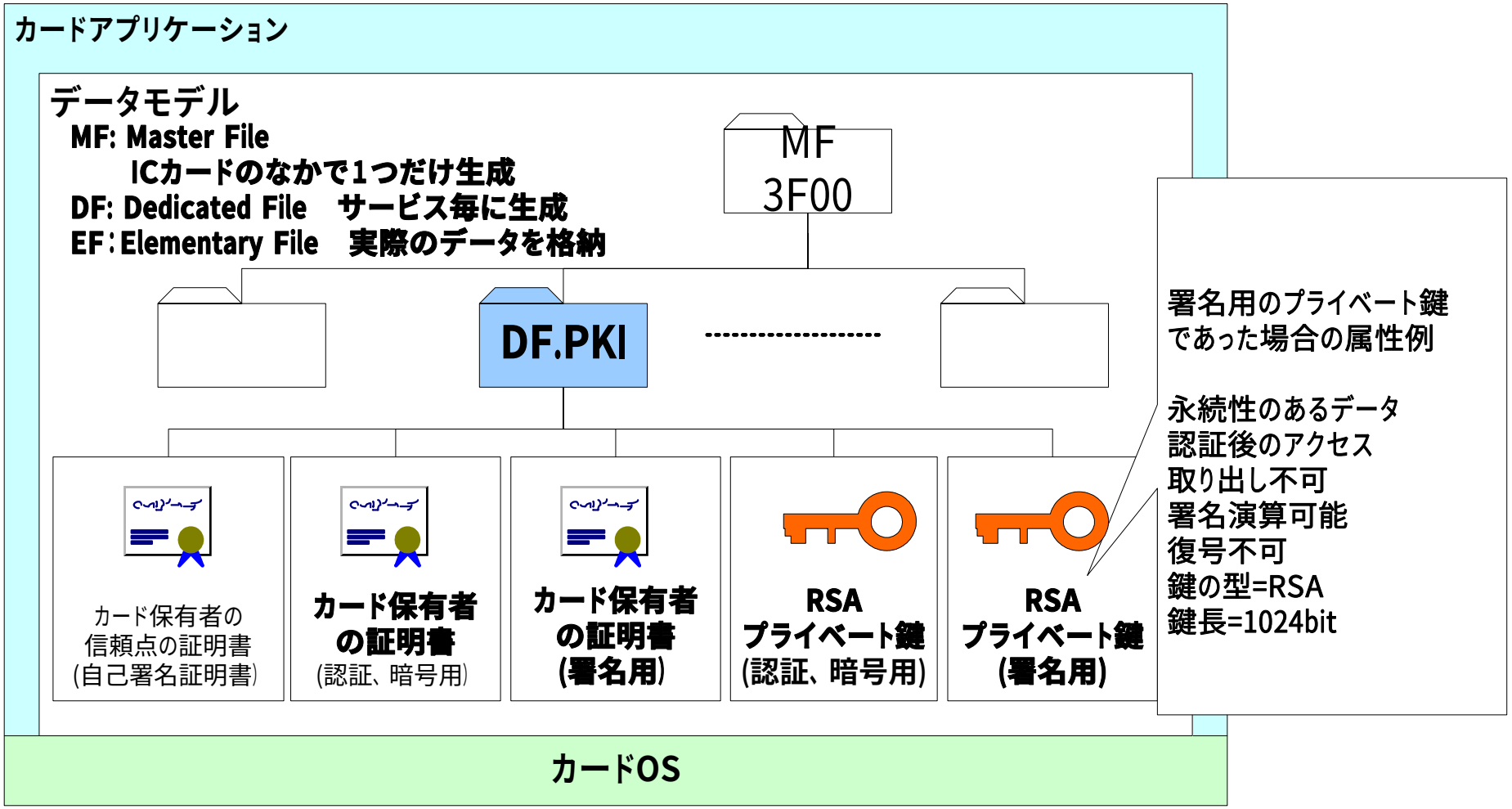
OpenSC http://www.opensc-project.org/

IC・IDカードに格納されるデータ

セコム IS 研究所
Intelligent Systems Laboratory

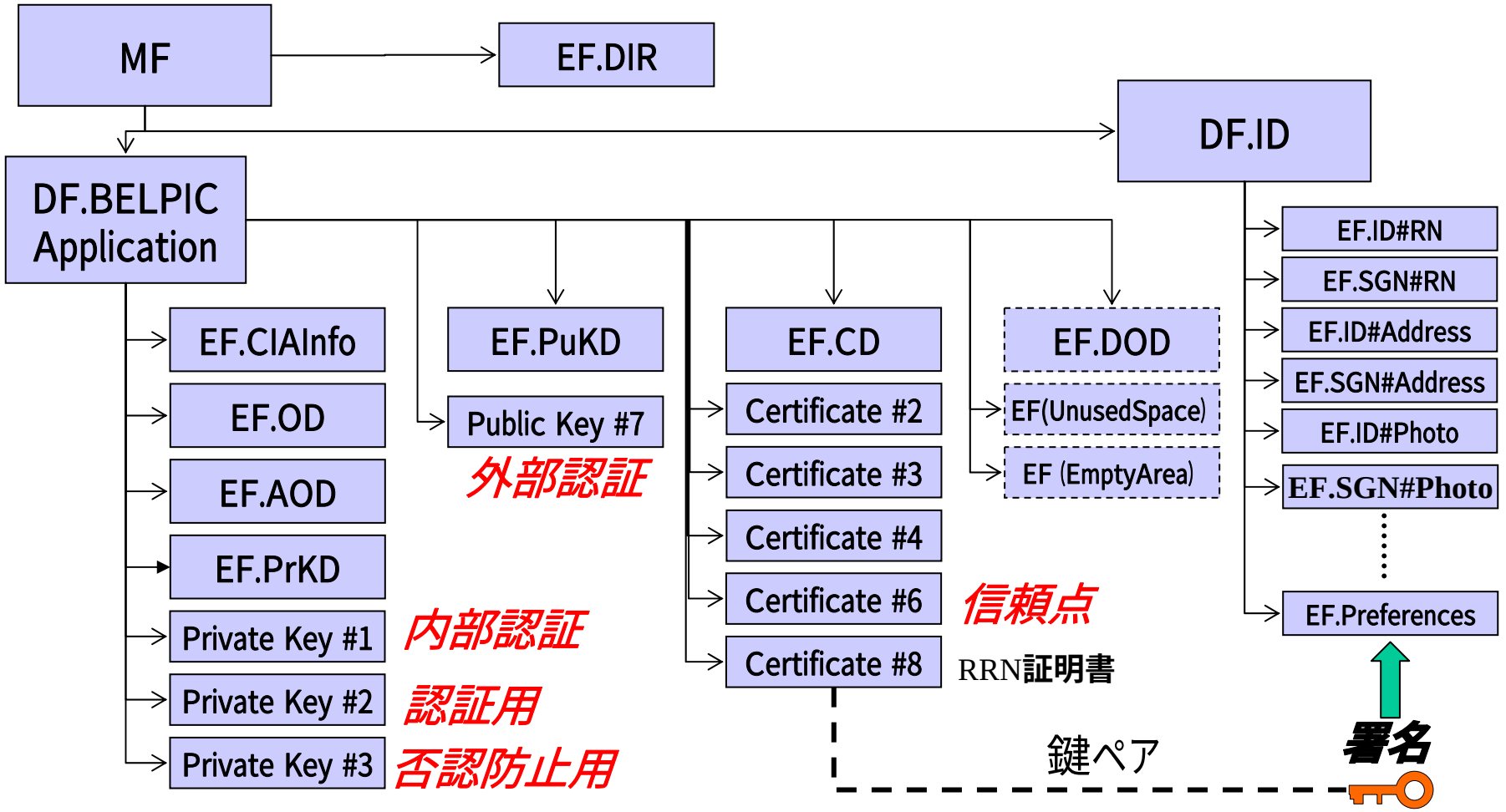
- ICカードのファイルの種類
  - MF(Master File) ,DF(Dedicated File) ,EF(Elementary File)
- EFのデータの形式
  - レコード、ファイル(データユニット)、オブジェクト
- 主な格納されるデータの種類
  - プライベート鍵(Private Key)
  - 公開鍵(Public Key)
  - 秘密鍵(Secret Key)
  - 証明書 (公開鍵証明書、属性証明書など)
  - 認証オブジェクト (Authentication objects : PINやバイオメトリクステンプレートなど)

IC・IDカードに格納されるデータの例

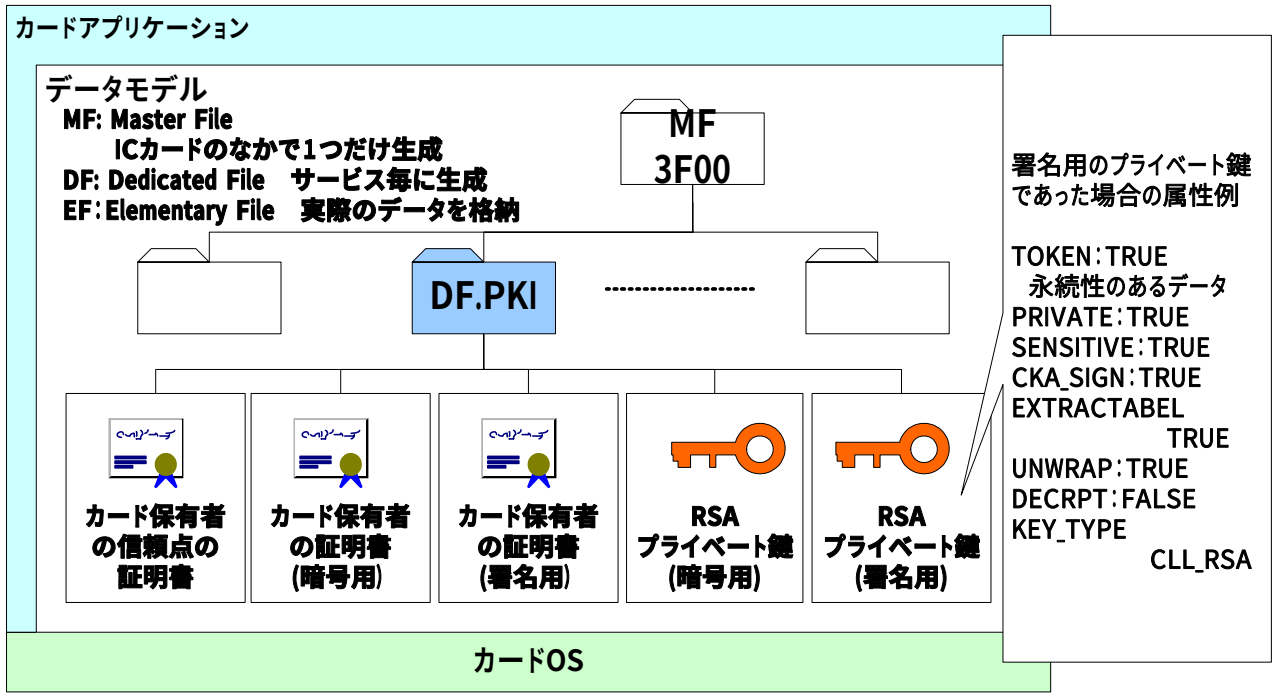


BELPIC (ベルギー)
データモデル　ファイル構成

セコム IS 研究所
Intelligent Systems Laboratory



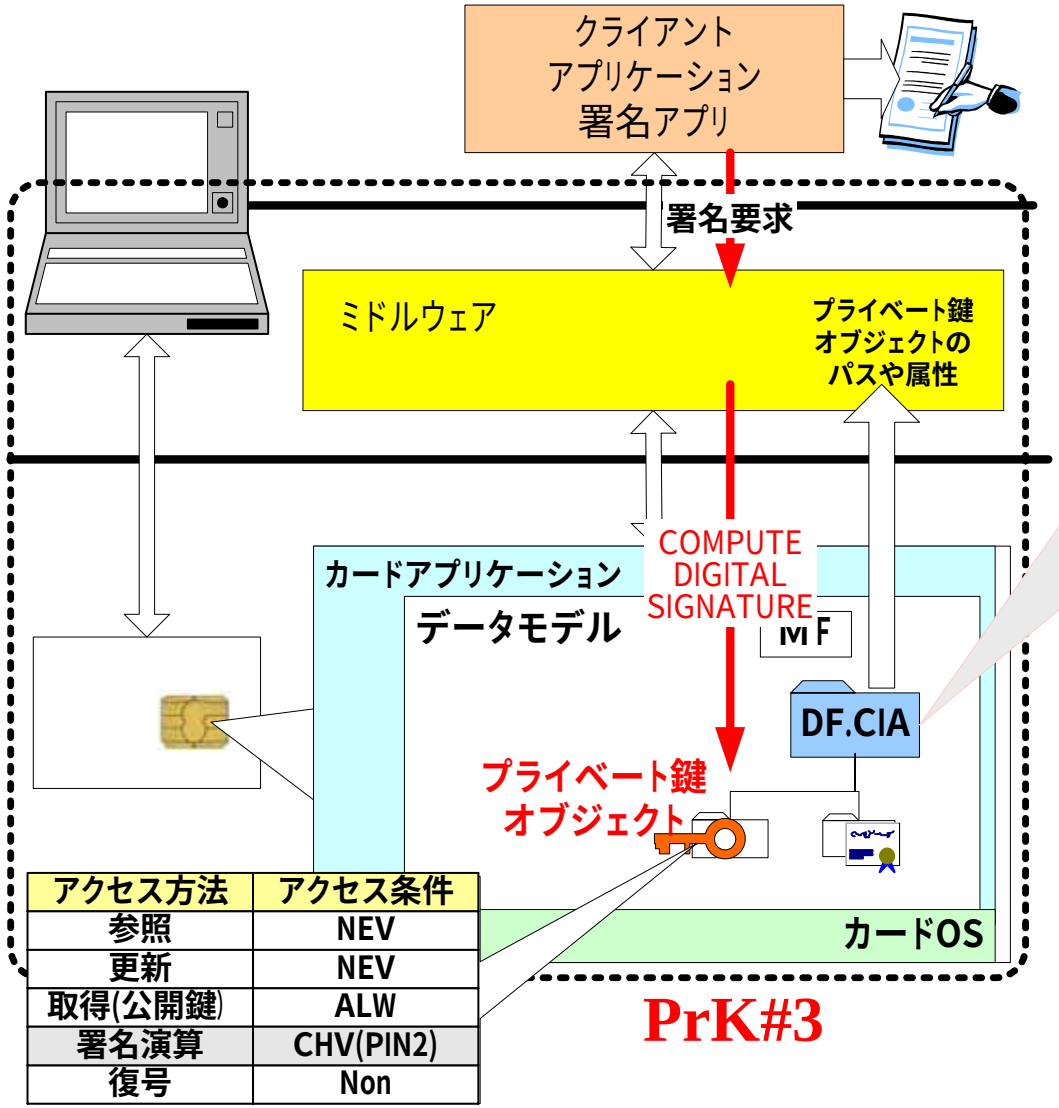
データモデル



- IC・IDカードでは、生のICカードをフォーマットして、クレデンシャル（鍵や証明書）を配置する。このカードを扱うためには、これらのクレデンシャルのレイアウトや属性を知っている必要がある。
- 一般的な考えは、「だからドライバーが必要」。
  - 調査報告書の観点は、「ドライバーではダメでミドルウェアが必要」

PKCS#15 or ISO/IEC 7816-15

セコムIS研究所
Intelligent Systems Laboratory

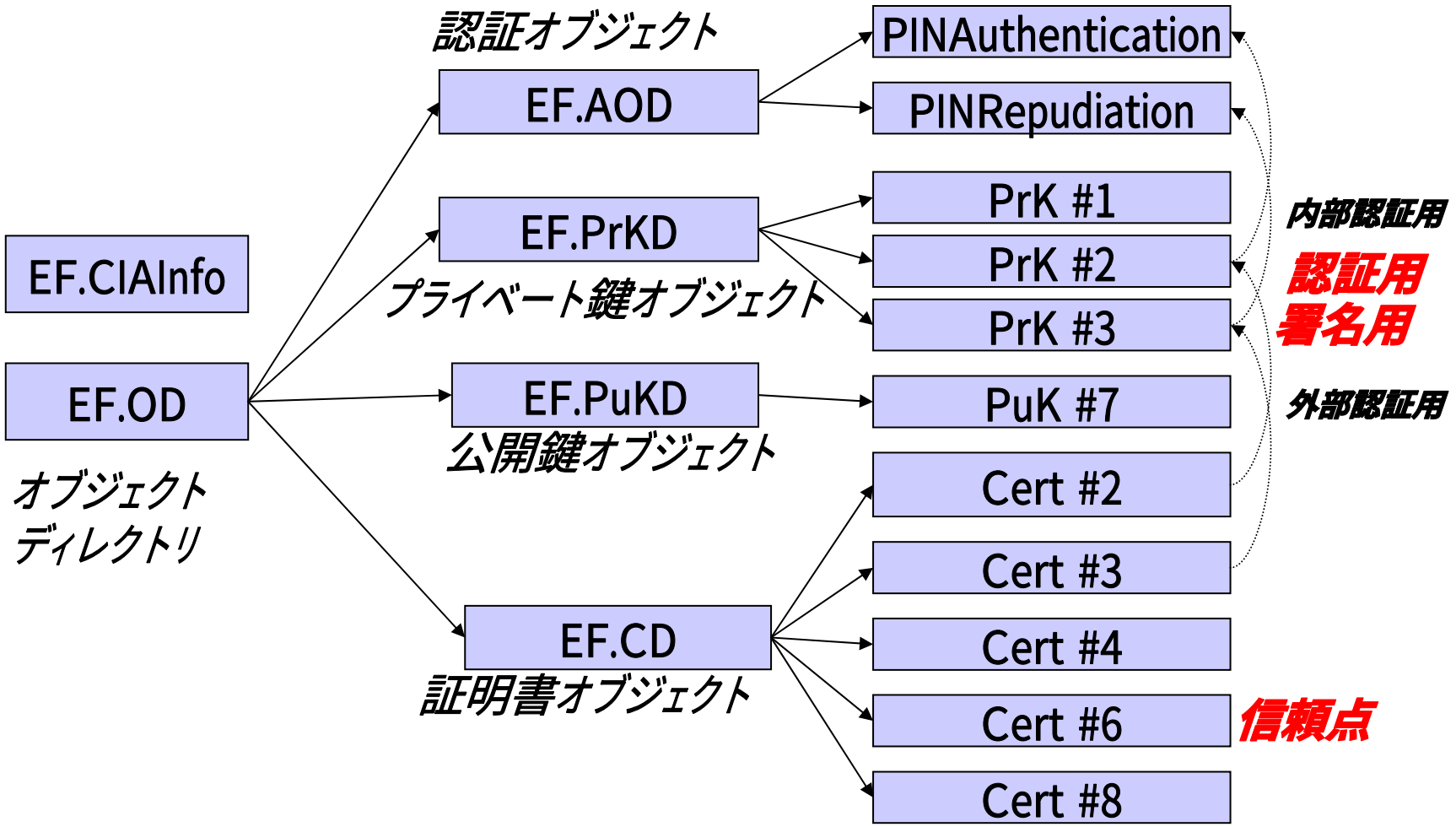


アクセス方法	アクセス条件
参照	NEV
更新	NEV
取得(公開鍵)	ALW
署名演算	CHV(PIN2)
復号	Non

```
privateRSAKey : {
  commonObjectAttributes { -- CommonObjectAttributes
    label “signature key”,
    flags {private},
    authID ‘02’H,
    userConsent ‘01’H -- user consent required for each
    private key operation !!!
    accessControlRules: { -- SEQUENCE OF AccessControlRule
      { --- AccessControlRule
        accessMode { execute }
        authId ‘02’H
      }
    }
  },
  classAttributes { -- CommonKeyAttributes
    iD ‘46’H,
    usage {nonRepudiation},
    -- native by default true (HW RSA)
    accessFlags {sensitive, alwaysSensitive, neverExtractable,
    cardGenerated},
    keyRef
    erence ‘00’H
  },
  subClassAttributes { -- CommonPrivateKeyAttributes
    keyIdentifiers { -- SEQUENCE OF PKCS15KeyIdentifier
      {
        idType 4, -- Subject public key hash
        idValue OCTET STRING :
        ‘11223344556677889900112233445566778899 00’H
        -- Faked value of SHA-1 hash
      }
    }
  },
  typeAttributes { -- PrivateRSAKeyAttributes
    value indirect : path : {
      path ‘3F0050164B02’H
    },
    modulusLength 1024,
  }
}
```

BELPIC (ベルギー)
データモデル　オブジェクト関連図(PKCS#15)

セコム IS 研究所
Intelligent Systems Laboratory



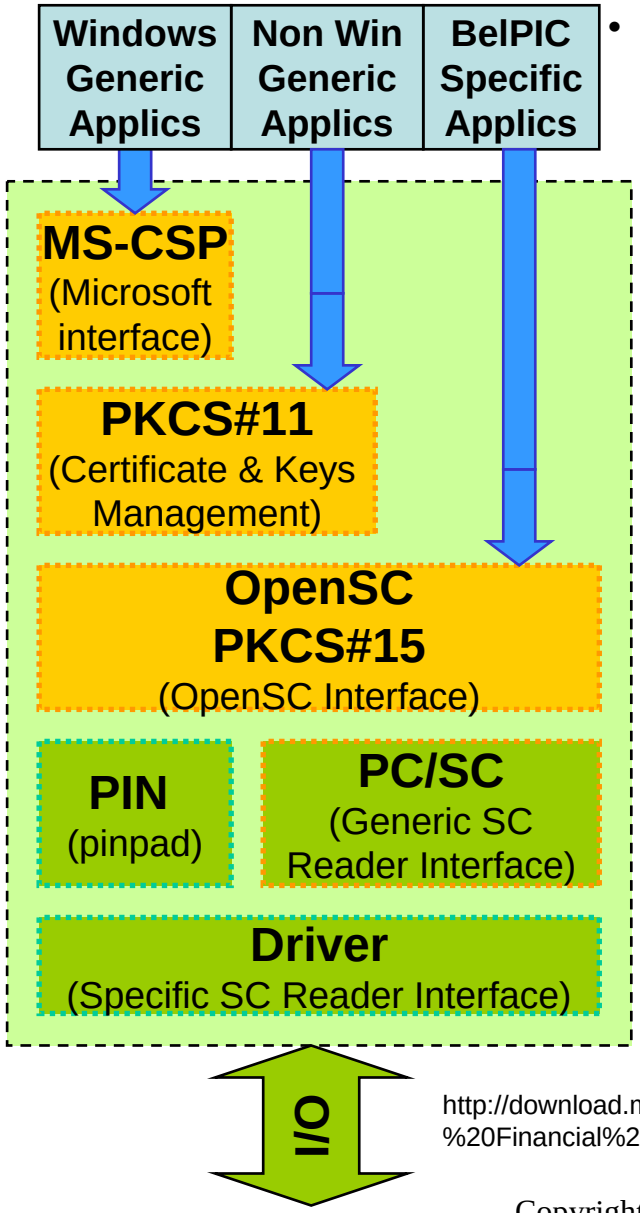
BELPIC (ベルギー)
カードエッジI/F

セコムIS研究所
Intelligent Systems Laboratory

コマンド種別、コマンド名		参照標準
選択コマンド		
	SELECT FILE	ISO/IEC 7816-4
データ操作コマンド		
	READ BINARY	ISO/IEC 7816-4
	UPDATE BINARY	
	ERASE BINARY	
認証関連コマンド		
	VERIFY	ISO/IEC 7816-4
	CHANGE REFERENCE DATA	
	RESET RETRY COUNTER	

コマンド種別、コマンド名		参照標準
伝送処理関数		
	GET RESPONSE	ISO/IEC 7816-4
MANAGE SECURITY ENVIRONMENT		
	SET	ISO/IEC 7816-4
	RESTORE	
PERFORM SECURITY OPERATION		
	COMPUTE DIGITAL SIGNATURE	ISO/IEC 7816-8
	VERIFY DIGITAL SIGNATURE	
	VERIFY CERTIFICATE	
GENERATE PUBLIC KEY PAIR		
ACTIVATE FILE		ISO/IEC 7816-9
DEACTIVATE FILE		

BELPIC (ベルギー)　ミドルウェアの構成



- Card & Reader Software
  - Card MiddleWare
    - **PKCS#15** ⇔ ID specific applications
      - Card is accessed as a simple file system
      - No key management possible (no PIN)
      - for belgian police, post, banks, etc
    - **PKCS#11** ⇔ Generic applications
      - Only keys & Certs available via PKCS#11 API
      - allows authentication (& signature)
      - for Netscape, Linux, Unix, etc
    - **MS-CSP** ⇔ Windows applications
      - Only keys & certs available via MSCrypto API
      - allows authentication (& signature)
      - for Microsoft Explorer, Outlook, etc
  - Reader Driver/Firmware
    - most part is generic (orange part)
    - small part is specific (green part)

http://download.microsoft.com/download/4/f/d/4fd49a94-8772-4bd0-88ca-bf46e2d029fc/15_DECEMBER_2004/3%20-%20Financial%20Services%20eID%20Technical%2015%20Dec%202004%20-%20FedICT%20Olivier%20Libon.ppt

セコムIS研究所
Intelligent Systems Laboratory

相互運用可能性の課題

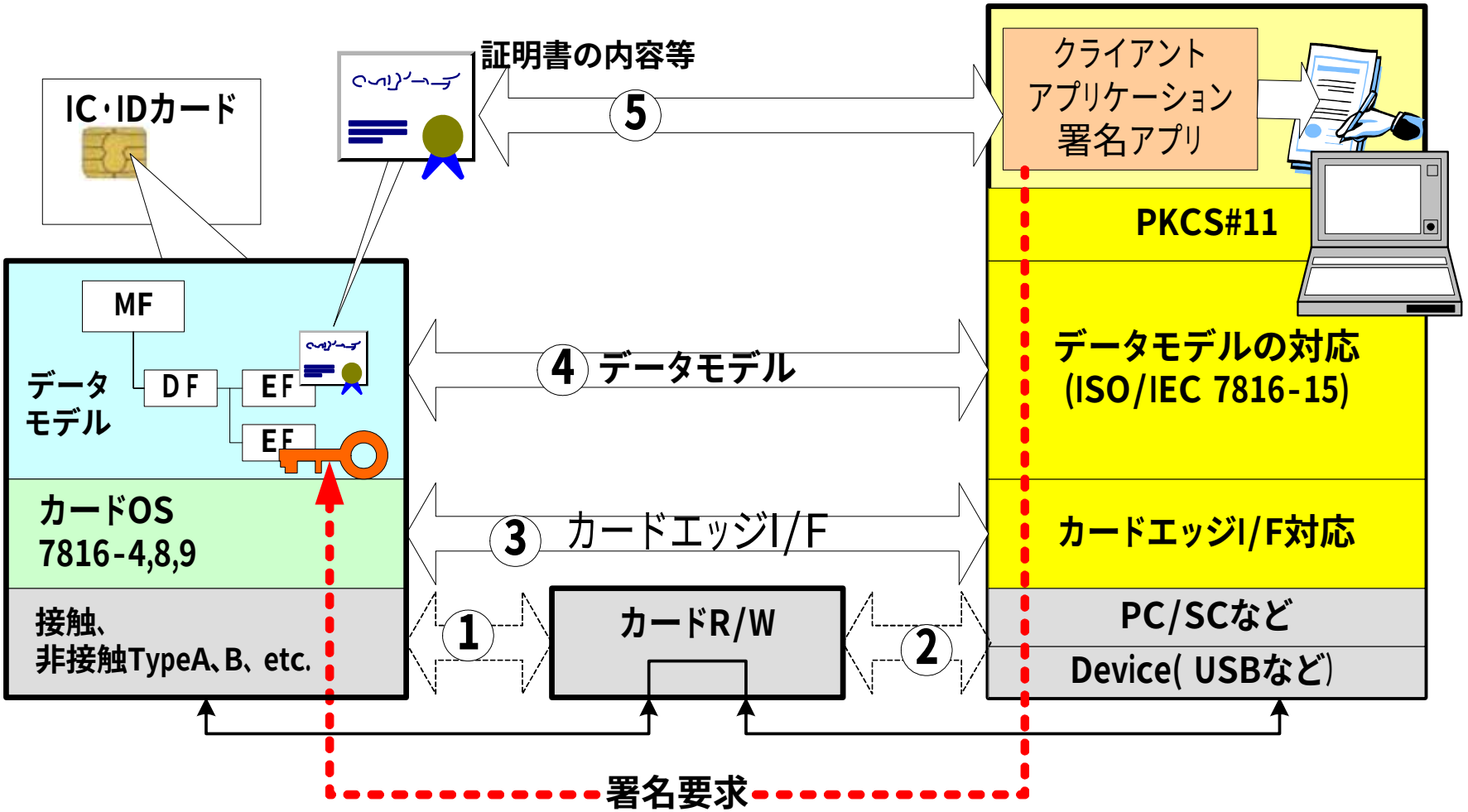
Q.　相互運用可能性の確保は？

A.　世界標準のISO/IEC 14443 TypeB、ISO/IEC7816準拠ですから大丈夫

Q.　データモデルは？？？

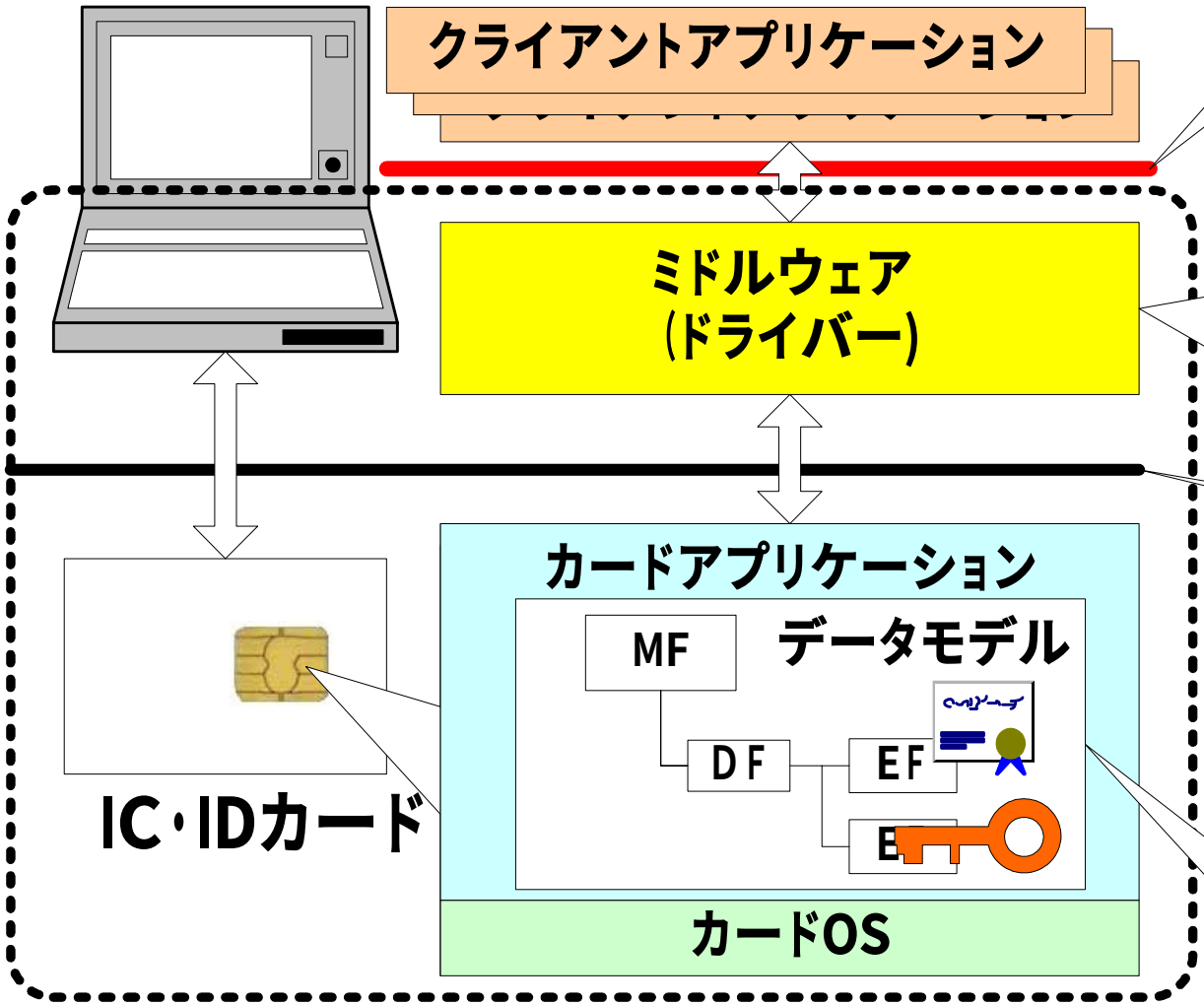
A.　（え？？）決まっていません。だけど、ポストイシューでどんなアプリケーションでも入れられるので大丈夫です。

相互運用可能性の課題
相互運用可能性の分類



相互運用可能性が問題になる部分は、5つに分類し、主に（3）、（4）をこの調査報告書で取り上げた。

相互運用可能性の課題
IC・IDカード(サービス) の提供形態



PKCS#11などのデファクトスタンダードなAPI

ベンダー独自のデータモデルのカードエッジI/Fをサポートするためのミドルウェア (IC・IDカードに依存したドライバー)

ベンダー等に依存したカードエッジI/F。非公開の場合もある。

ベンダー等に依存したデータモデル。多くの場合、非公開。

相互運用可能性の課題
現状のIC・IDカードの提供形態での課題

セコム IS 研究所
Intelligent Systems Laboratory

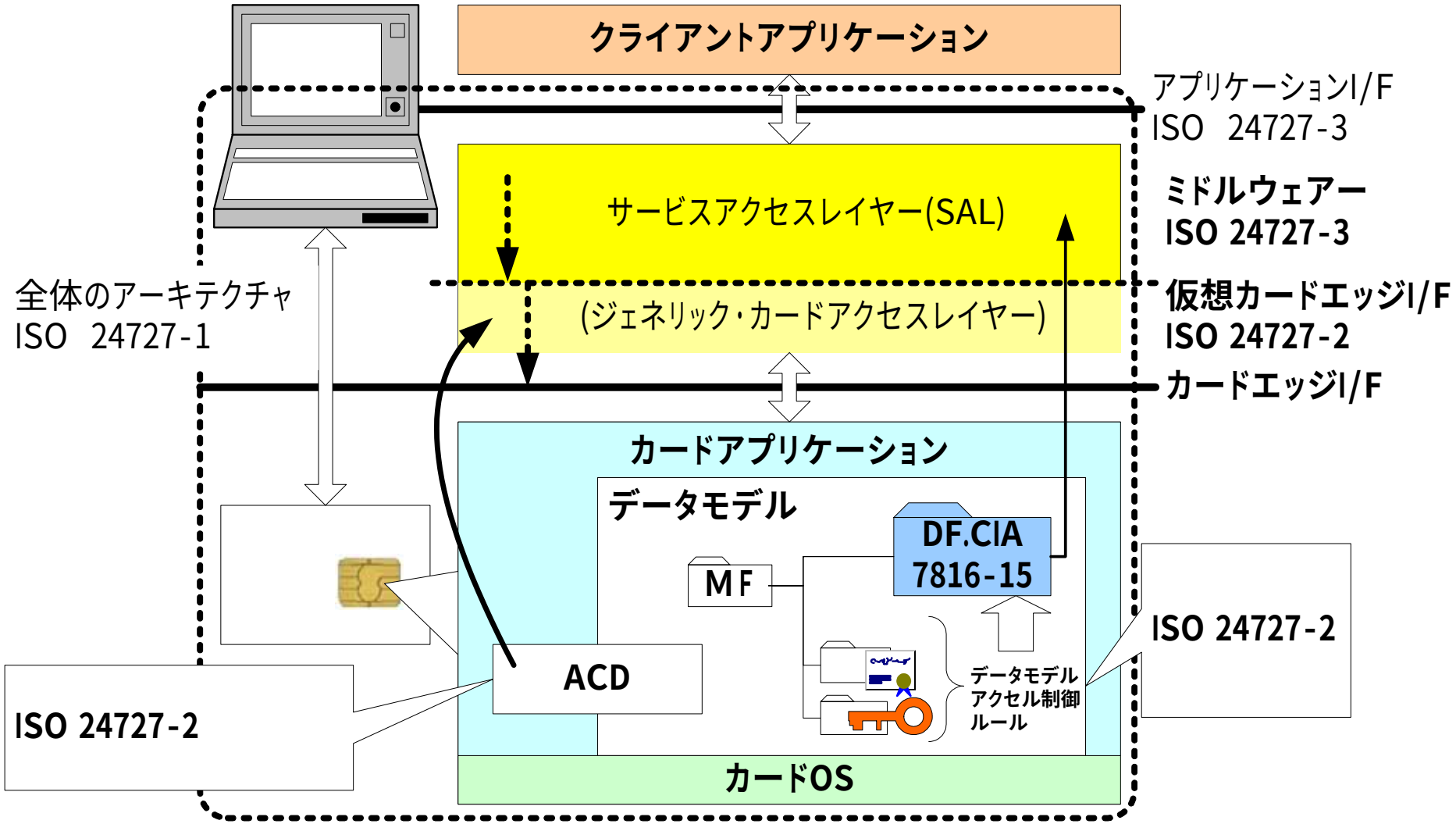
- PKCS#11等のデファクトスタンダードなAPI
  - PKCS#11と言っても実装のレベルは様々であり、サブセットの実装
  - 準拠性テスト仕様（＆テストツール）の不在などの理由から、多くの問題が内在する。これらは、「相性の問題」で片付けられてしまっている。
  - こうした問題は、少数のアプリケーションしが動作していない初期の導入時には気が付かない場合もある。
- ベンダー独自のデータモデルとカードエッジI/Fをサポートするためのミドルウェア（IC・IDカードに依存したドライバー）
  - IC・IDカードとミドルウェアが一体化されて提供されている。そのため、IC・IDカードとミドルウェアそれぞれの独立性がない。IC・IDカード毎のドライバーが必要になり、ドライバーのコンフリクト等のトラブルの元になっている。
- ベンダー等に依存したカードエッジI/F、ベンダー等に依存したデータモデル
  - IC・IDカードとしての独立性、ポータビリティーがない。使う環境が限定される。
- 結果としてマルチプラットフォームで動作するIC・IDカードが少ない
  - IC・IDカード自体がベンダー依存のため、ミドルウェアの提供も限定されてしまう。結果として、マルチプラットフォームで動作するIC・IDカードも少ない。

相互運用可能性の課題　標準化動向

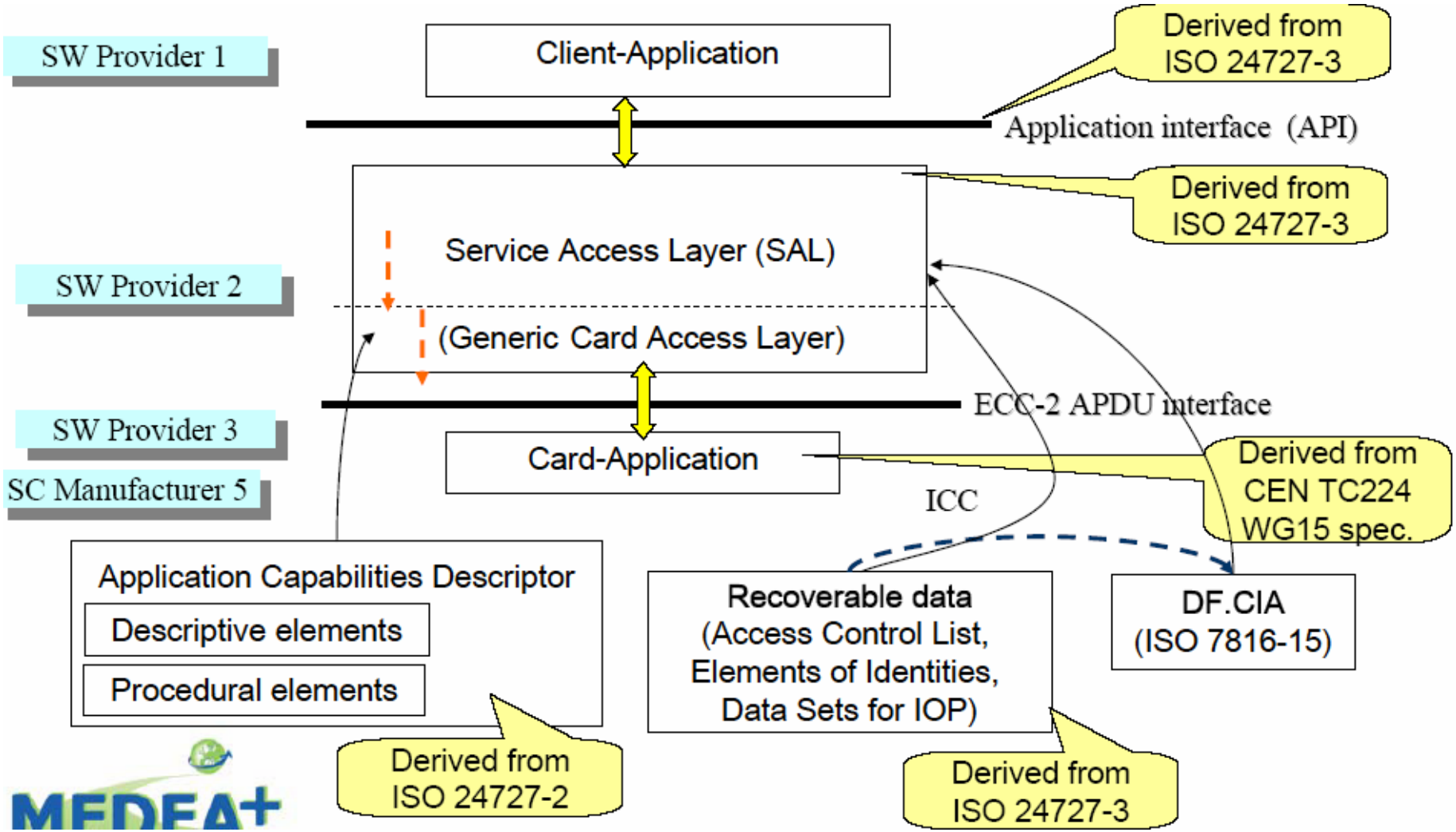
セコム IS 研究所
Intelligent Systems Laboratory

- カードエッジインターフェース
  - ISO/IEC 7816-4,8,9
  - Identification cards― Integrated circuit cards with contacts
- データモデル
  - ISO/IEC 7816-15
    - Part 15: Cryptographic information application (CIA)
  - PKCS#15　7816-15の前身
  - JIS X 6320-15：2006　7816-15をJIS化
    - 第15 部：暗号情報アプリケーション　(CIA)
- アプリケーションAPI
  - ISO/IEC 24727 - ミドルウェアも含めたIC・IDカードサービスの標準化
    - Identification cards -- Integrated circuit card programming interfaces
    - ISO/IEC FDIS 24727-1　アーキテクチャ
    - ISO/IEC FCD 24727-2　汎用カードインターフェース
    - ISO/IEC CD 24727-3　アプリケーションインターフェース
    - ISO/IEC NP 24727-4　API管理
    - ISO/IEC NP 24727-5　テスト

相互運用可能性の課題　標準化動向
ISO/IEC 24727、ISO/IEC 7816-15などの関係



相互運用可能性の課題　標準化動向
欧州での動向　CEN TC 224 WG 15　/　CEN/TS 15480



http://porvoo9.gov.si/pdf/FRI_15_1000_MFaher_AXALTO_Porvoo9.pdf

相互運用可能性の課題

セコム IS 研究所
Intelligent Systems Laboratory

- なぜ仕様が十分に開示されないか？
  - 実力以上にICカードのセキュリティの高さが喧伝されている？
  - 実際には、様々なリスクがある。仕様が開示される（理解される）と、その「様々なリスク」が浮上する？
  - セキュリティに完全は無いにも係わらず、完全で無いことを脆弱性があるとか、プライバシー上の問題があるとか呼ばれることのリスク??
- 「情報セキュリティ vs. 相互運用可能性の確保」なのか??
  - BELPIC、米国のPIV
    - 「仕様をオープンにすることで、安全・安心なIC・IDカードの普及を図る」
  - 公的個人認証サービス、国家公務員身分証ICカード
    - 「仕様をオープンにしないことで、安全・安心なIC・IDカードを実現する」（と考えている??）
- IC・IDカードの仕様の閉鎖性は、相互運用可能性の問題解決を阻害し、それが、安全、安心を提供するとされているIC・IDカードの普及の阻害要因となっている??
- また、技術の不透明さは、セキュリティ上の不毛な議論を助長する。

セコムIS研究所
Intelligent Systems Laboratory

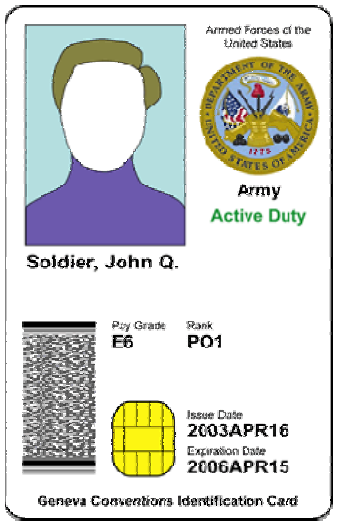
その他　おまけ

(1) IPAの報告書で詳細を説明している米国のPIV
(2)世界初のネット投票もこれでやっているエストニアのeID
(3) フランス版「健康ITカード??」　SESAM-Vitale2

PIV (米国)

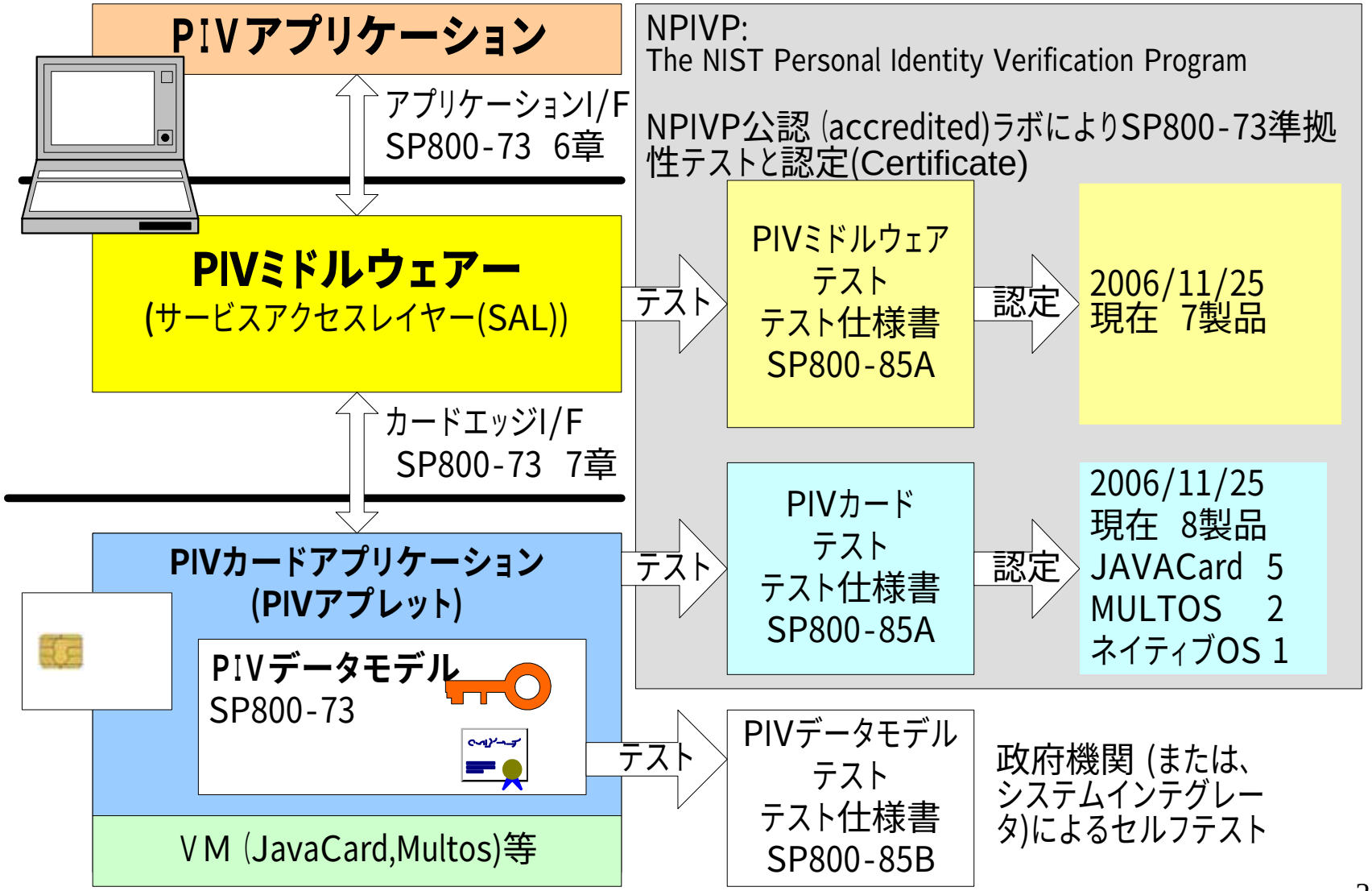
セコム IS 研究所
Intelligent Systems Laboratory

- Homeland Security Presidential Directive/Hspd-12
  - http://csrc.nist.gov/policies/Presidential-Directive-Hspd-12.html
  - 主題：連邦政府職員と契約業者の共通識別基準のための方針
  - 2004年8月27日に発行
- PIV
  - 連邦機関が職員、契約業者へ発行するIC・IDカード
- フィジカル＆ロジカル
  - 接触、非接触のふたつのインターフェースを持つ。仕様上は、デュアルインターフェースカードでもハイブリッドカードでもよい仕様になっている
- PIVカードエッジインターフェース
  - SP800-73
- PIVデータモデル
  - SP800-73
- ミドルウェア
  - PIVミドルウェア



http://csrc.nist.gov/piv-program/index.html

PIV　－　PIVのテスト方法論と仕様



米国PIVと国家公務員身分証明書ICカードの比較

セコム IS 研究所 Intelligent Systems Laboratory

比較項目	PIV	国家公務員身分証明書 ICカード
配布対象	連邦政府職員と契約業者	国家公務員
配布枚数	2000万枚が予定されている	不明
プラットフォーム対応	規定なし	規定なし
IC・IDカードをサポートするミドルウェア	仕様、テスト仕様が公開されており認定制度(NPIVP)がある。 ミドルウェアのレファレンス実装のソースコードなども公開されている	不明
カードエッジI/F	NIST SP800-73	非公開
カード内のデータモデル	NIST SP800-73	非公開
格納されるEE(End Entity)証明書	認証用の証明書 署名用の証明書(Option) 暗号用の証明書(Option)	規定なし

エストニアのeID

セコムIS研究所
Intelligent Systems Laboratory

- エストニア
  - 人口：１３５万人
  - IT国家を目指している　Skypeの開発拠点としても知られている
- エストニアのeIDの概要
  - 15歳以上の全国民に配布されるカードで約100万枚が発行済み
  - カード保有者のふたつの証明書(否認防止の署名と認証)
  - ミドルウェアは、OpenSCが使用可能
  - 16KBのEEPROM　->　PKIのカードアプリケーション　+ 券面情報のみ（多分。。）
- eIDの利用
  - 様々な用途に利用されている（　しかし単一カードアプリケーション？　）
    - 主な利用用途は、「否認防止の署名」ではなく、「認証(Authentication)」
    - 自分の情報へのアクセス記録が参照できる（そのための認証）
    - 世界初の全国ネット選挙　2005/10 1%、2007/3　3%が、インターネットから
- 日本の住基カードの普及策の考え??　マルチカードアプリケーション
  - 多目的利用＝マルチカードアプリケーション(　本当にこれが正しいのか？)
  - #「ICカードありき」の考え方が強すぎる。ICカードはフロントンドツールでしかない。
  - BELPICもエストニアのeIDも、カードアプリケーション(データモデルとクレデンシャル)を明確にして、仕様を広く公開することにより利用を拡大しようとしている。

フランスのSESAM-Vitale2　健康保険証カード
#「健康ITカード」（仮称）のモデル??

セコムIS研究所
Intelligent Systems Laboratory

- 以前(2000年)からICカード化されていた健康保険証カード(SESAM-Vitale)
  - １６歳以上全国民
- SESAM-Vitale2
  - フランス版EHR(Electronic Health Record)に対応させるためのPKI対応
  - フランス版HER　->2006年秋から開始
  - ３年で全てリプレース(年2000万枚??)
- NXP「SmartMX」、フランスの健康保険カード“Sesam-Vitale2”に採用
  - http://japan.internet.com/webtech/20061110/4.html
    - 保持者は請求書にサインできるだけでなく、セキュアな電子環境で自分の個人医療ファイルへアクセスすることが可能となる
    - 36K EEPROM PKI（公開鍵基盤）コンタクトマイクロコントローラ

上がSESAM-Vitale2

下が医師のカード

「健康ITカード」が、ちゃんと利用できるためには、医師カードとの連携が重要なのだが、医師カードが標準化できるかが鍵になる。

http://www.sesam-vitale.fr/index.asp

http://www.sesam-vitale.fr/programme/programme_eng.asp

参考

セコム IS 研究所
Intelligent Systems Laboratory

- IC・ID カードの相互運用可能性の向上に係る基礎調査
  - http://www.ipa.go.jp/security/fy18/reports/ICID/index.html
  - シーズ編
    - http://www.ipa.go.jp/security/fy18/reports/ICID/seeds_rep.pdf
- BELPIC仕様
  - http://www.rijksregister.fgov.be/cie_fr/cie/archives_diverses/cahiers_charge/eik_bestek_bijlage5.doc
- BELPICお薦めプレゼン
  - http://homes.esat.kuleuven.be/~decockd/site/EidCards/belpic/mySlides/belgian.eid.card.technical.overview.pdf
- BELPICのドキュメント類
  - http://www.snelbalie.be/content/content/record.php?ID=131
- PIV
  - http://csrc.nist.gov/piv-program/index.html
- エストニアIDカードの利用状況
  - http://www.soumu.go.jp/menu_03/shingi_kenkyu/kenkyu/kojin_ninsho/pdf/070201_si4.pdf