

**ハードウェア脆弱性評価の最新技術動向  
に関するセミナー  
—CARTES/CARDIS 参加報告—**

2015年1月9日

独立行政法人 情報処理推進機構  
技術本部 セキュリティセンター

# 本日のセミナー 目次



<b>CARTES</b> (2014年11月4日-6日)	CARTES SECURE CONNEXIONS	スマートカードに関連した 展示会とそれに付随した conference
<b>CARDIS</b> (2014年11月5日-7日)	13 <sup>th</sup> Smart Card Research and Advanced Application Conference	スマートカードのセキュリ ティに関するconference

## CARTES 2014 参加報告

---

# 目次

- ◆ CARTES 2014の全体について
- ◆ Conferenceでの発表から、いくつかのトピックの紹介
  - Biometrics Applications
  - Security Documents & e-Governments
  - Towards Trusted Cloud Services
  - Instant Issuing and Personalization: What's new?

# 目次

- ◆ CARTES 2014の全体について
- ◆ Conferenceでの発表から、いくつかのトピックの紹介
  - Biometrics Applications
  - Security Documents & e-Governments
  - Towards Trusted Cloud Services
  - Instant Issuing and Personalization: What's new?

# CARTES概要

- ◆ CARTES Secure Connexions is the Global Event for Payment, Identification and Mobility [C0]
  - 毎年11月頃にパリで開かれる
  - 展示会とカンファレンスが同時開催される

# 展示会概要

- ◆ 国別の出展者数の上位3つは、フランス78、中国61、ドイツ60。<sup>\*1</sup>
- ◆ 日本は8、台湾は11、韓国は15
  - 日本からの出展者は、大日本印刷、電通、日本電産コパル(NIDEC)、QUADRAC、ソニー、TEAM NISCA & SWIFT COLOR、凸版印刷、東芝
- ◆ 出展者の分類
  - IC、テスト装置、電子部品・センサー、カード関連
  - SICソリューション、カード用OS、各種(モバイル、銀行、ID、M2Mなど)ソフトウェアとサービス

\*1 ブースの数をカウント

# CARTES Conference概要



- ◆ CARTES 2014のConference
  - 11月4日ー6日に開際
  - 160人の発表者
- ◆ 企業からの参加者が、自社のビジネスと直接関連した内容を発表する。



# Conference プログラム



Tuesday, Nov. 4	Wednesday, Nov. 5	Thursday, Nov. 6
mPOS & iBeacons: Always more Innovation for the Connected Commerce	Mobile Services, Enablers of our Mobile Future	NFC/HCE, a Successful Connected Commerce
Wallets, Bitcoins, New Means of Payments	Security Documents & e-Governments	Mobile Payment: Security First! (HCE, NFC, Apple Pay, SE, TEE)
Privacy in the Digital Society	EMV: Challenges & Benefits	Biometrics Applications
Instant Issuing and Personalization: What's new?	Connected Objects: Connectivity and Intelligence (M2M, Internet of Things)	Towards Trusted Cloud Services ----- Smart Mobility in Transport

- ◆ 3日間にわたって、4つのパラレルセッションが開かれる  
枠で囲ったセッションから、いくつかの発表を本日紹介する。

# 紹介するトピックと注目点

- ◆ **Biometrics Applications**
  - オリンピックとも関連し、日本国内での注目が高まっている。
- ◆ **Security Documents & e-Governments**
  - 認証機関という立場から、規格・標準の動向の注視が必要
  - 国の機関として、他国での電子政府の動向を確認する。
- ◆ **Towards Trusted Cloud Services**
  - カード以外へのセキュリティ技術の広がりの動向の調査
- ◆ **Instant Issuing and Personalization: What's new?**
  - 発行時のセキュアな手続きは決済カード以外でも重要

# (参考) 昨年のプログラム



Tuesday, Nov. 19	Wednesday, Nov. 20	Thursday, Nov. 21
Your Future is mobile, trust it!	Commerce Convergence, going Mobile!	Digital Wallet & eMoney
Cloud Security & Data Protection	Electronic Government Megatrends	Smart Cities: Embedded Connectivity & Intelligence
Innovation & Dematerialization in Prepaid	Best Practices for mPOS Acceptance	Biometrics: Privacy and Security Concerns
EMV 2.0, the Breakout Year!	NFC out of payment	Brazil: Building Trust in Mobile Life
		New Means of Payments for Financial Inclusion

# 今日紹介するトピック

- ◆ Biometrics Applications
  - Zwipe: 指紋認証の決済用カード
  - 行動学的特徴の使用
  - Fake Finger Detection
- ◆ Security Documents & e-Governments
  - eIDAS
  - PIVのアクセスコントロールへの使用
  - 携帯電話の公共サービスへの使用

# 今日紹介するトピック

- ◆ Towards Trusted Cloud Services
  - クラウドマーケットでセキュリティを確保する方法
- ◆ Instant Issuing and Personalization: What's new?
  - 銀行支店でのカード発行

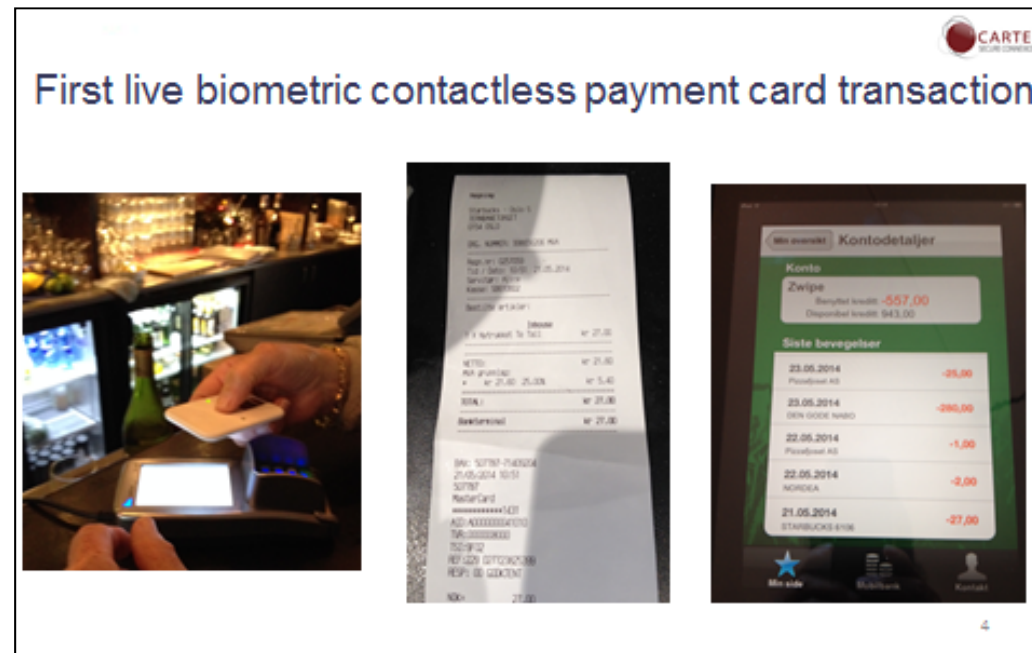
# 目次

- ◆ CARTES 2014の全体について
- ◆ Conferenceでの発表から、いくつかのトピックの紹介
  - Biometrics Applications
  - Security Documents & e-Governments
  - Towards Trusted Cloud Services
  - Instant Issuing and Personalization: What's new?

# Biometrics Applications

## Zwipe: 指紋認証の決済用カード[C1]

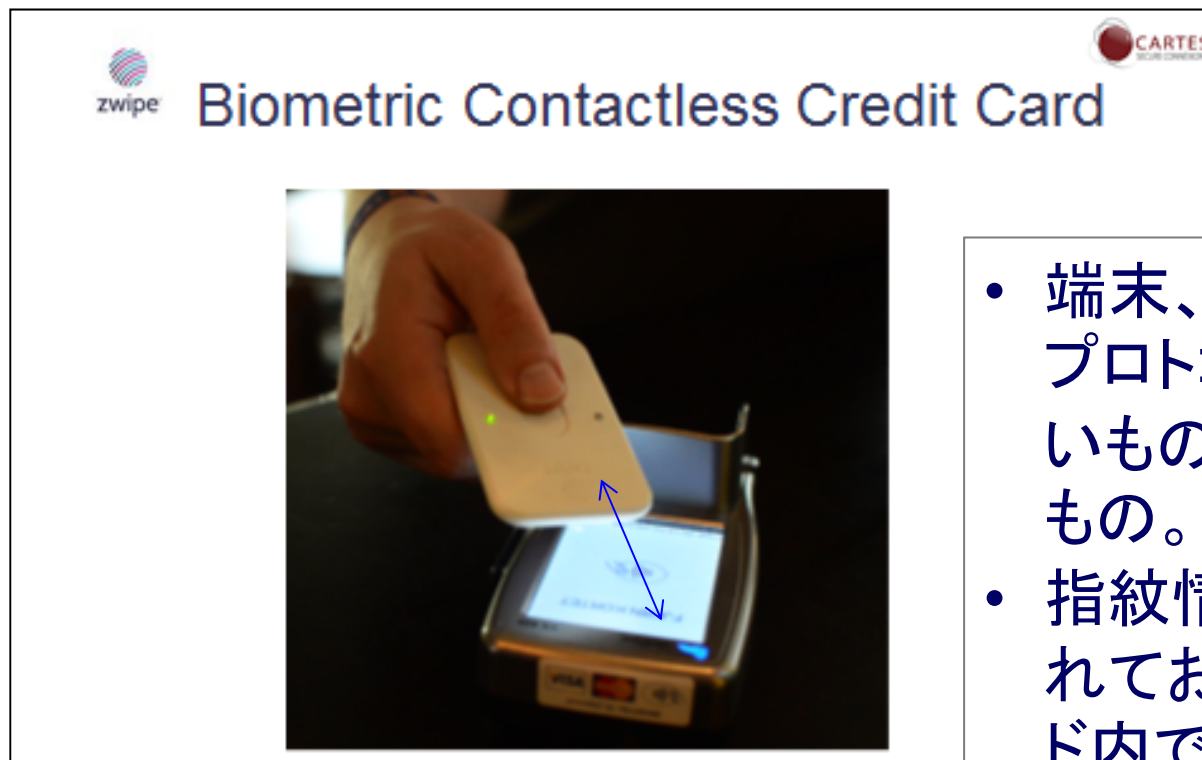
- ◆ 決済用カードのPINを指紋認証で置き換える
- ◆ 2014年5月に、Sparebanken DIN(ノルウェーの貯蓄銀行)とZwipe社が共同でノルウェーで200人規模の、最初の実証実験を実施した。



[C1] CARTES2014発表: Contactless Biometric Payment - Experience from Live Trial  
Susanne HANNESTAD, Executive Board Director - Zwipe, NORWAY

# Biometrics Applications

## Zwipe: 指紋認証の決済用カード



- 端末、カードと端末の通信プロトコルは(Zwipeではないものと同様の)一般的なものの。
- 指紋情報はカードに格納されており、指紋認証はカード内で実施される。



## Zwipe: 指紋認証の決済用カード

- ◆ 実証実験の結果、ユーザはPINよりあるいはPINと同程度、簡単で、速くて、セキュアであると感じたという結果が得られた。
- ◆ 今後、マスターカードと共同で、ISOに準拠した形の非接触カードの発行を予定している(2014年10月17日にプレスリリース)



[1]より引用

[1] <http://www.mastercard.co.jp/company/newsroom-141022.html>、"MasterCardとZwipe、世界初の指紋センサーを搭載した生体認証付き非接触決済カードを発表"、2014年11月27日閲覧  
[2] <http://zwipe.com/products/>、"Products | Zwipe"、2014年11月27日閲覧

## Zwipe: 指紋認証の決済用カード

- ◆ マスターカードに関する情報
  - 指紋データはカードに記録される
  - 決済端末の電力を使用
  - NFCで通信
  - ISO 7810 ID-1準拠
    - ISO 7810はIDカードの物理特性(形状を含む)を定めた国際規格。  
ID-1は85.60 x 53.98 x 0.76 mmと一般的なクレジットカードサイズ。

# Biometrics Applications

## 行動学的特徴の利用[C2]



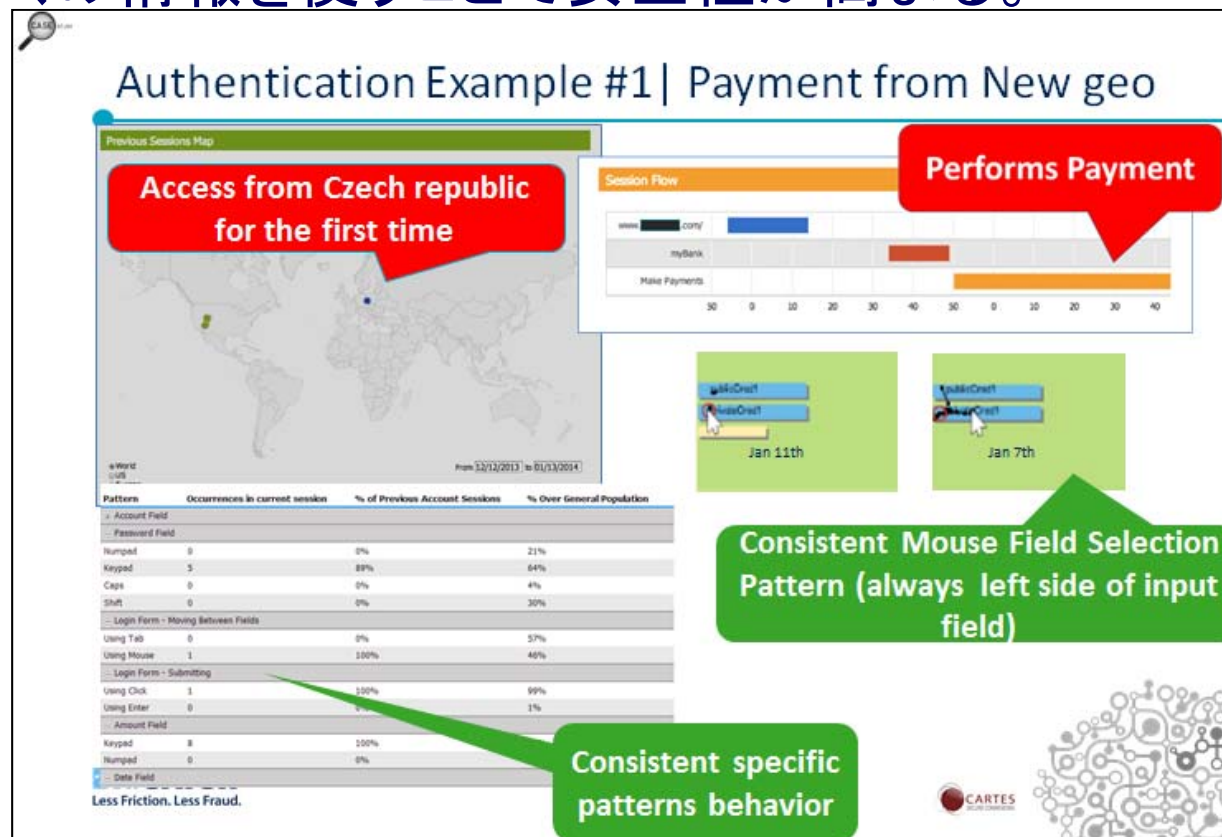
- ◆ 行動学的特徴の例
  - 歩き方
  - キーストローク
- ◆ マウスの動かしかたにはユーザごとに特徴がある。
- ◆ (インターネットバンキングなどの状況を想定したとき、) マウスの動きはJavaScript / SDK でサーバ側で取得し、解析・判断できる。
- ◆ 使用例の紹介

# Biometrics Applications

## 行動学的特徴の利用

例1:「いつもと同じようにパスワードウィンドウの左端をクリックしている」という情報を、アクセス時間、アクセス場所などと組み合わせ、正当な利用者であるかの判定に使う。

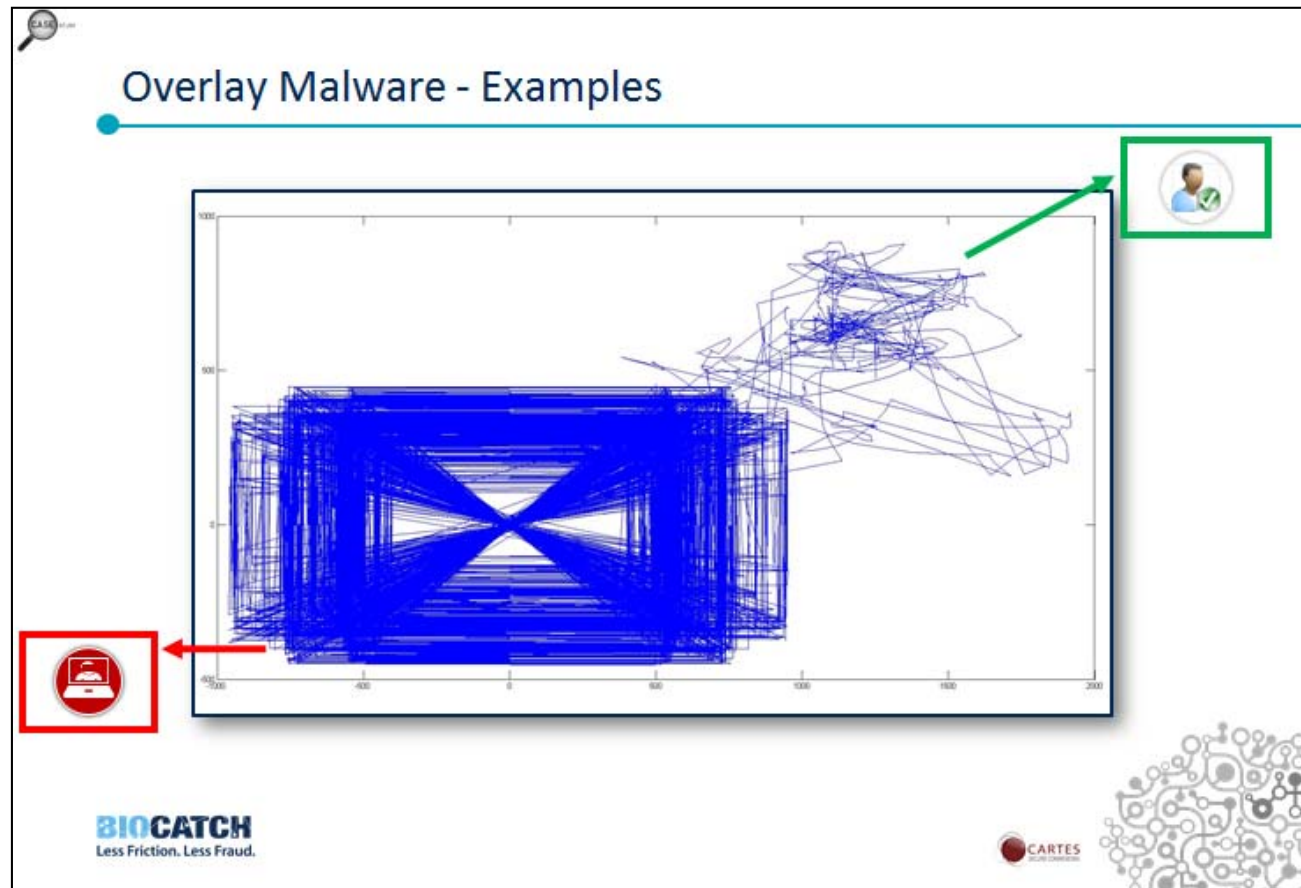
→より多くの情報を使うことで安全性が高まる。



# Biometrics Applications

## 行動学的特徴の利用

例2: マルウェアと人間を、マウスの動かし方で区別する。



## Fake Finger Detection [C3]


- ◆ 偽造指で指紋認証、指紋識別をだますことが現実になっている。
  - 2013年ブラジル: 病院で医師が、欠勤の同僚が出勤したこととするために、シリコン製の指を用いた。
  - 2008年日本: 入国管理での指紋読取りを、指にテープを張り付けて通過した。
- ◆ Fake Finger Detection (偽造指検知) の方法としては、ハードウェアベースのものとソフトウェアベースのものがあるが、それぞれ長所を組み合わせることによって、より優れた方法となるだろう。

# Biometrics Applications

## Fake Finger Detection

- ◆ ハードウェアベースのFFD  
偽指紋と生体指の組み合わせにだまされないような注意が必要



### FFD Solutions – Hardware



---

#### Hardware-based Biometrics

- Temperature
- Pulse
- Blood pressure
- Odor
- Electrocardiogram
- Multispectral imaging, spectroscopy



Should be integrated carefully so spoof cannot be combined with live finger to be accepted (e.g., translucent spoofing light-absorption-based pulse oximeter)

“Morpho, World’s First Company to Receive Common Criteria Certification for Fake Finger Detection”, July 2013

© NecID Biometrics 2014

7

# Biometrics Applications

## Fake Finger Detection

- ◆ MorphoSmart Optic 301
- ◆ 指のインピーダンスを測定し生体指であるかを判定
- ◆ 粘土、ゼラチン、芋などで作成した142種の偽指が、偽指として検知されることを開発者テストで確認した。

[3]より引用

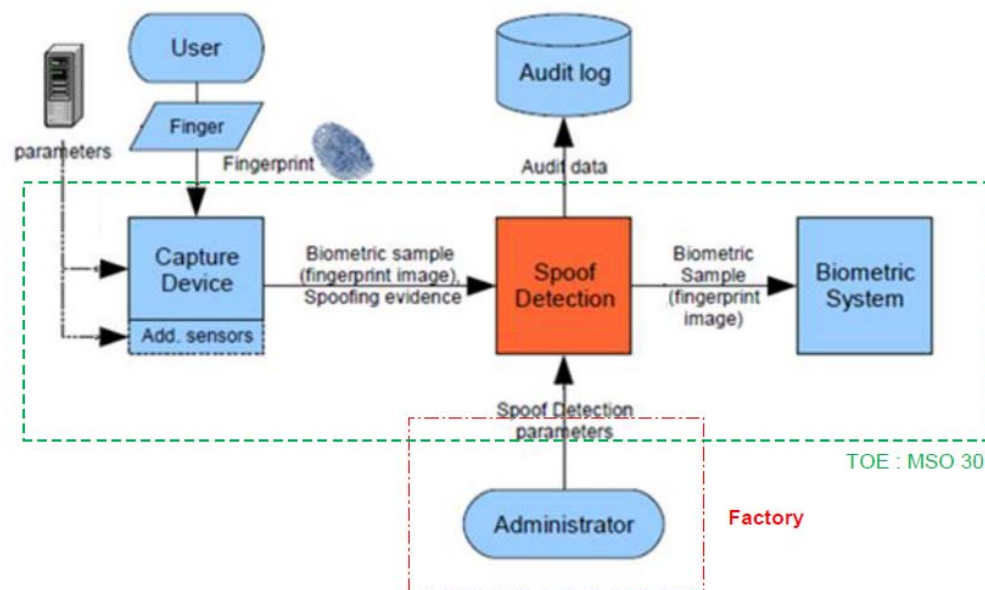


Figure 1: TOE Boundary

[3] MorphoSmart Optic 301 Public Security Target, SSE-0000096154-01, 2013-01-18  
[4] Certification Report, BSI-DSZ-CC-0790-2013



## 7.2 Functional Developer Testing

### Testing Approach

The developer used the following test tools and materials for different aspects of the testing activities. The following list gives an overview about the used tools and their purpose or field of application:

- MSO\_Demo: Tool for the testing of SDK functionality / implicit testing of TOE functionality
- ILV\_Scripter: Tool for testing the interface E.API
- Fake materials (Playdoh, latex, Window Color, white silicon, transparent silicon, candle wax, white glue, gelatine, foil, photocopy, wood glue, Micro Krystal Klear, potato): The materials were used to create fake fingers to test the spoof detection functionality of the TOE.

A test case conducted with the first two test tools thereby consists of several test steps which are executed sequentially and which results are compared to the expected results. Only if all checks of all test steps are successful, the corresponding test case passes.

The testing of the spoof detection functionality (according to FPT\_SPOD.1) was conducted by creating fake fingers from different materials (see list above). In total, the developer created 142 fakes and applied each fake 10 times to the TOE.

All in all, the developer tested the TOE systematically at the level of TSFI as given in the functional specification. The developer thereby followed the strategy to cover all TSFI.

# Biometrics Applications

## Fake Finger Detection

### ◆ ソフトウェアベースのFFD

人を識別、認証するための大局的な構造ではなく、ごく細かい構造に着目し、本物の人間であるかを判定する。

#### FFD Solutions – Software



#### Software-based Analysis of Image Characteristics

- Skin deformation / elasticity
- Pores / perspiration pattern
- Noise from spoof imperfections
- Combining multiple features

Image processing and statistical analysis of scanned images exploit inherent differences between images from live fingers versus severed and/or fake fingers. Feature extraction and machine learning most common approach.



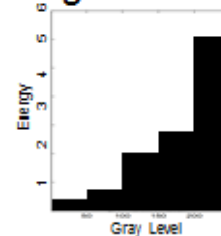
#### FFD Solutions – Software



Image features are extracted and statistically analyzed

- Example: Gray level distribution

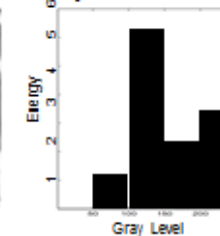
#### Live Finger



Features:

0.3 0.9 2.0 2.7 6.0

#### Gelatin Spoof



0.0 0.1 2.6 6.1 2.3 5

# 目次

- ◆ CARTES 2014の全体について
- ◆ Conferenceでの発表から、いくつかのトピックの紹介
  - Biometrics Applications
  - Security Documents & e-Governments
  - Towards Trusted Cloud Services
  - Instant Issuing and Personalization: What's new?

# Security Documents

## 規格の動向



- ◆ EU横断的なeIDASの動向
- ◆ PIVのアクセスコントロールへの適用

# Security Documents

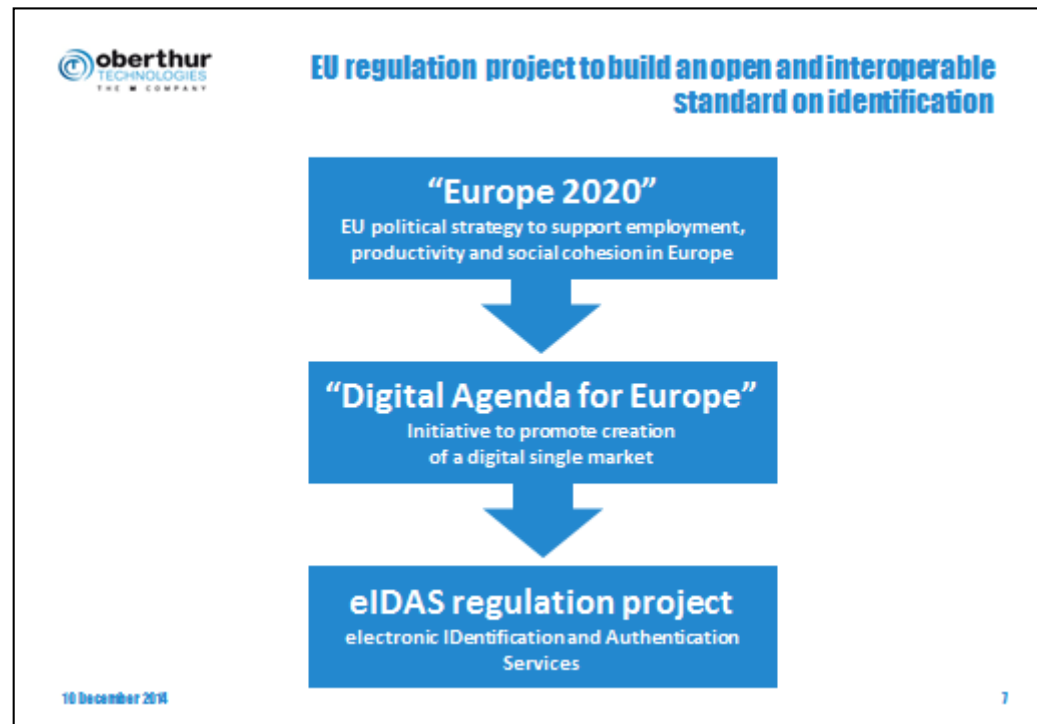
## 規格の動向



- ◆ 現在、3つのデジタルID Credentialsの主要な仕様がある。
  - フランスのIAS-ECC
  - ドイツのEAC
  - USのPIV
- ◆ EUにおいては新しいプロジェクトであるElectronic identification and trust services (eIDAS)が進んでいる。<sup>[5]</sup>
  - eIDASの普及によって、安全かつシームレスなクロスボーダー電子商取引の信頼と利便性を高めることを目的とする。

[5] <http://ec.europa.eu/dgs/connect/en/content/electronic-identification-and-trust-services-eidas-regulatory-environment-and-beyond>, "Electronic identification and trust services (eIDAS): regulatory environment and beyond", 2015年1月6日閲覧

- ◆ eIDASはEU横断的なIDの標準としてプロジェクトが進んでいる。



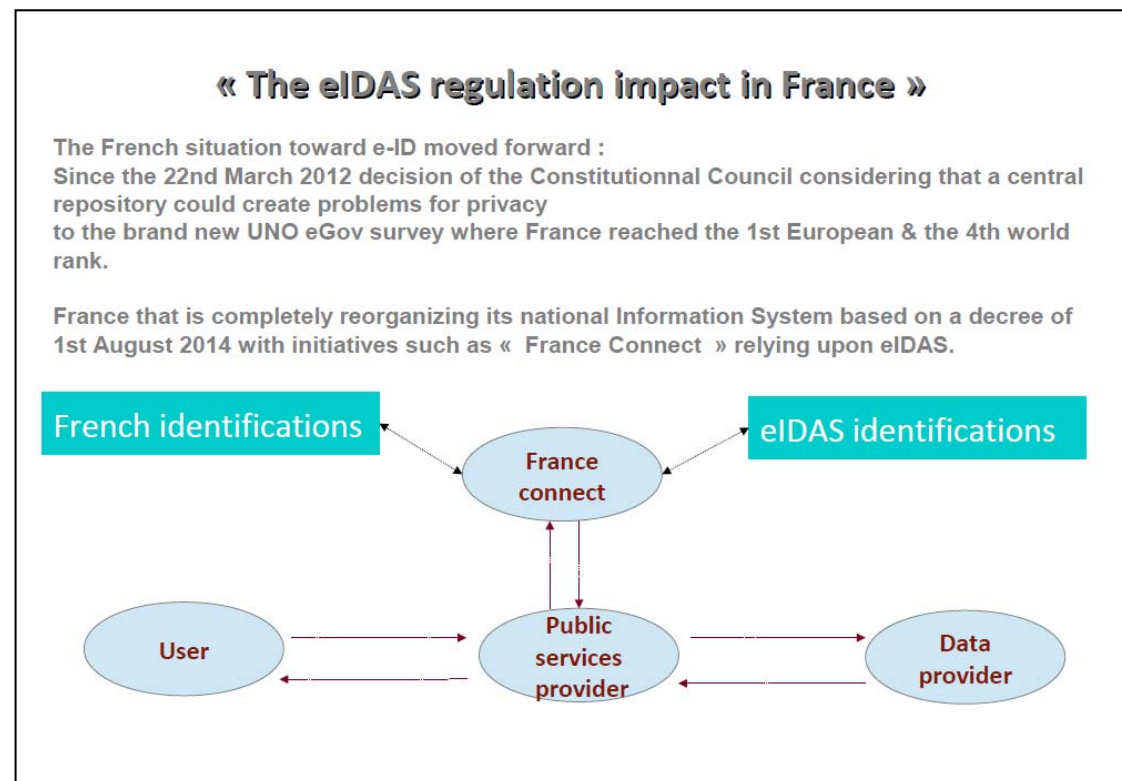
[C4] CARTES2014発表: Could PIV become a de facto standard for PAC/LAC convergence in Europe?

Hassan MAAD - Oberthur Technologies, FRANCE

# Security Documents

## eIDAS<sup>[C5]</sup>

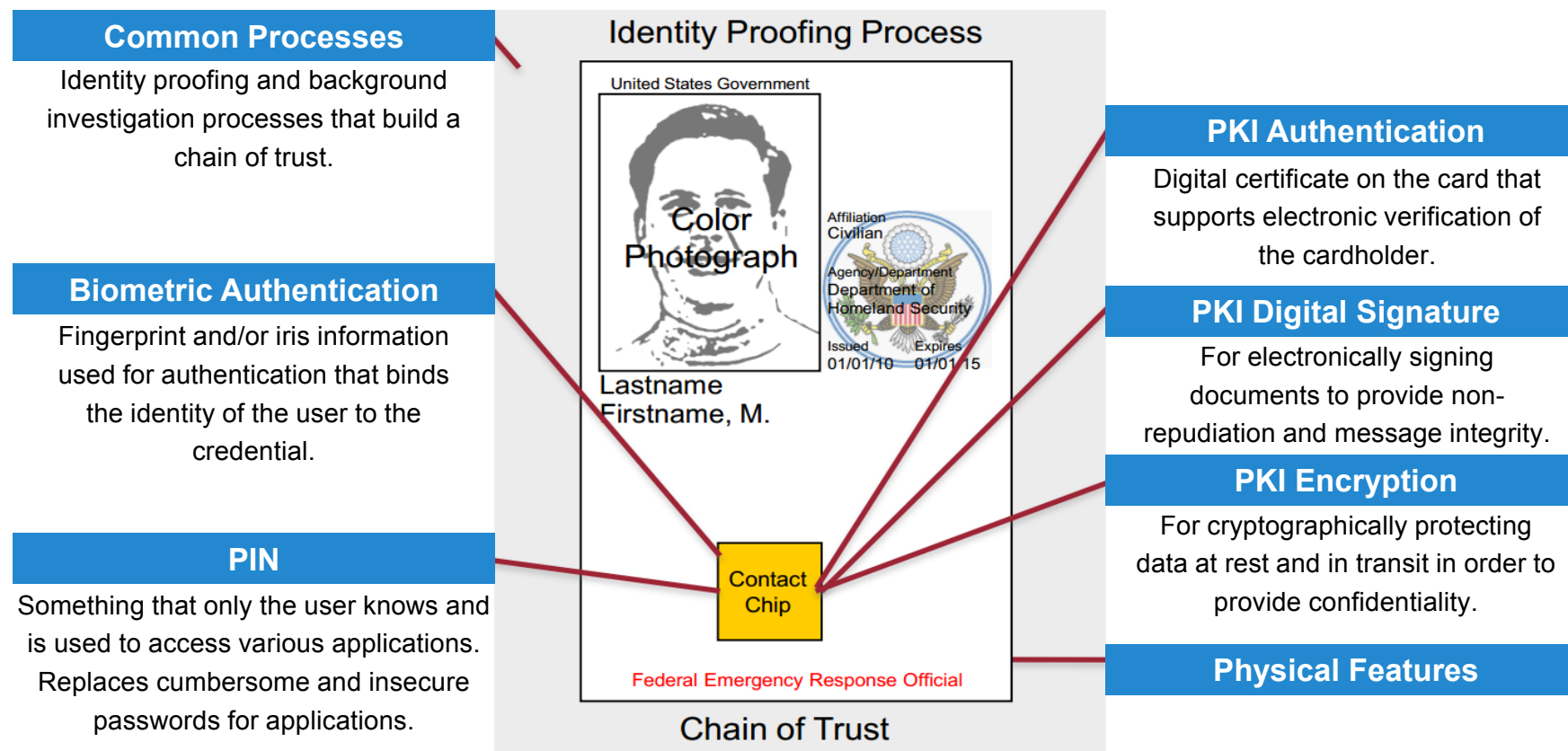
- ◆ フランス国内では、eIDASは国内市場用で電子識別と電子取引での認証サービスが2014年6月に始まった。
- ◆ 公共サービスでも使用していく。



# Security Documents

## PIVのアクセスコントロールへの使用[C4]

- ◆ PIV(Personal Identity Verification Card)はアメリカで、連邦職員と契約先で使われている。



[C4] CARTES2014発表: Could PIV become a de facto standard for PAC/LAC convergence in Europe?, Hassan MAAD - Oberthur Technologies, FRANCE

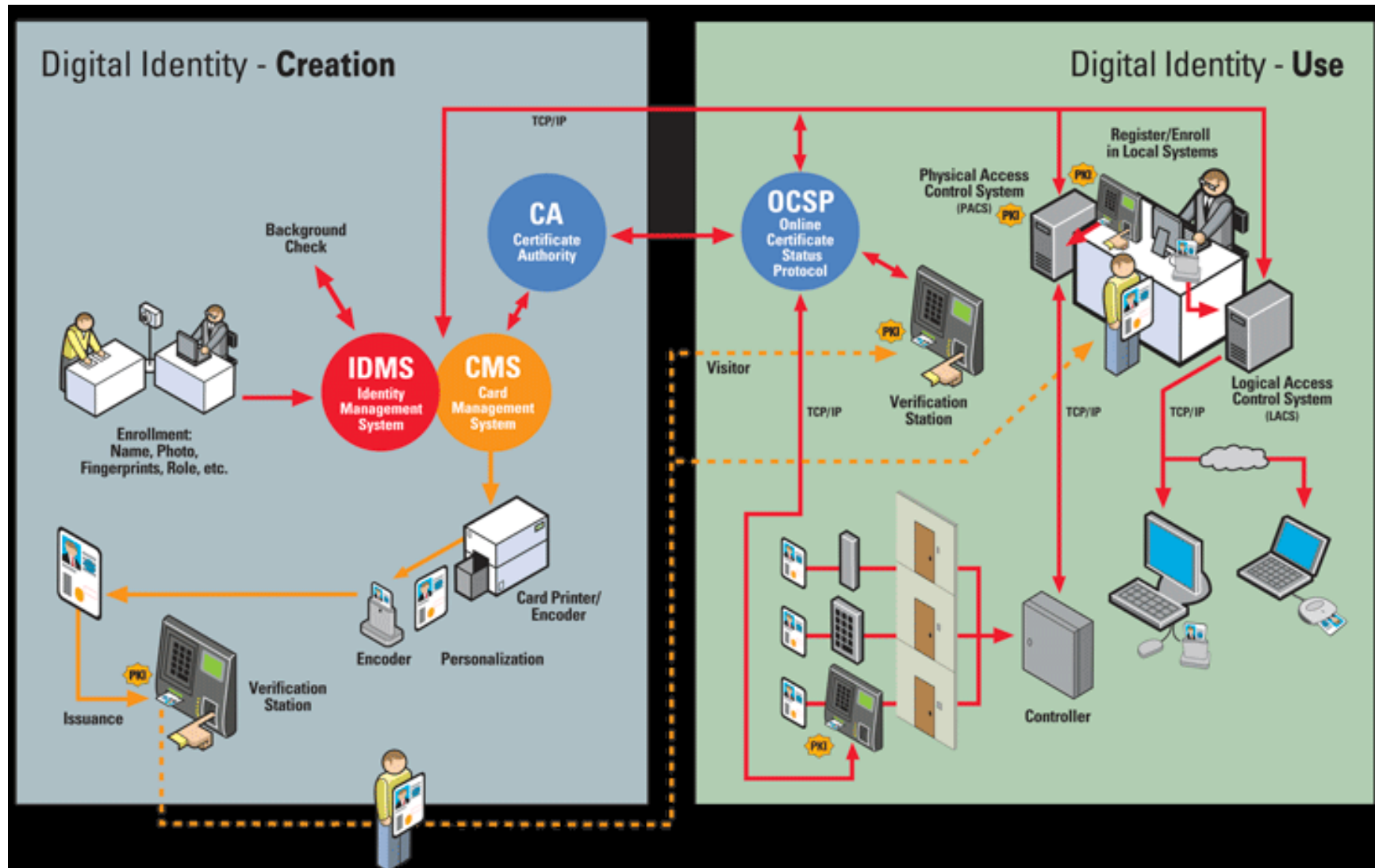


## PIVのアクセスコントロールへの使用

- ◆ PIVにはいろいろなセキュリティ機能があるので、物理・論理アクセスコントロールに使えるのではないか、という提案。
- ◆ PIVに含まれている機能
  - User vetting
  - High identity assurance
  - Interoperability
  - Accredited issuance processes
  - Cross-agency trust
  - Use for physical and logical access
  - Encryption
  - Digital Signature
  - Efficiencies
  - Biometric binding of identity

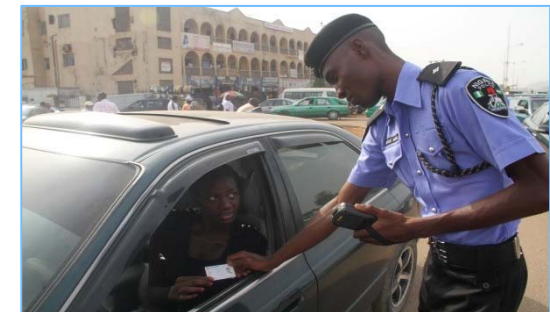
# Security Documents

## PIVのアクセスコントロールへの使用



## 携帯電話の公共サービスへの使用[C6]

- ◆ 携帯電話とRFIDを、交通の取り締まりに使う実験をナイジェリアで実施した。
  - 解決すべき課題：  
運転手と車の情報が十分でなく、警官がその場で使用できないため、取り締まりが効率的ではなかった。
  - 国土交通省は運転免許と車両文書を集めてはいたが、オンラインでは使用できなかった。



# 携帯電話の公共サービスへの使用

### ◆ ソリューション:

- 車はデータベースに登録される。
- 車のオーナーはRFID credentialを発行され、その中にオーナーの生体情報(指紋と写真)と、車の情報が登録される。
- 警官はリーダを所持し、credentialの情報にリアルタイムでアクセスできる。
- 警官は携帯電話も所持しており、携帯電話で事故や盗難事件の情報をリアルタイムで受信することができる。

### ◆ 結果

- リアルタイムで信頼できる情報に警官がアクセスできることで、取締りを強化することができた。
- 従来より低コストでシステムを構築できた。

# 目次

- ◆ CARTES 2014の全体について
- ◆ Conferenceでの発表から、いくつかのトピックの紹介
  - Biometrics Applications
  - Security Documents & e-Governments
  - Towards Trusted Cloud Services
  - Instant Issuing and Personalization: What's new?

# Towards Trusted Cloud Services

## クラウドでSecurityを確保する方法



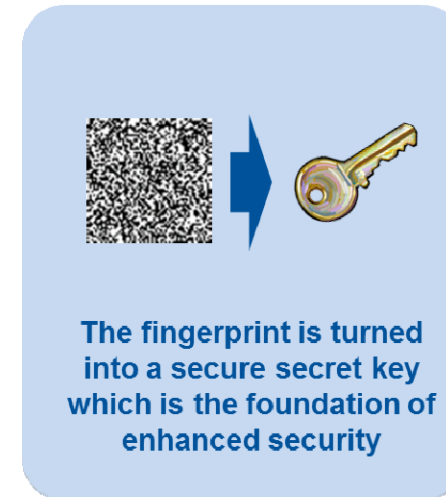
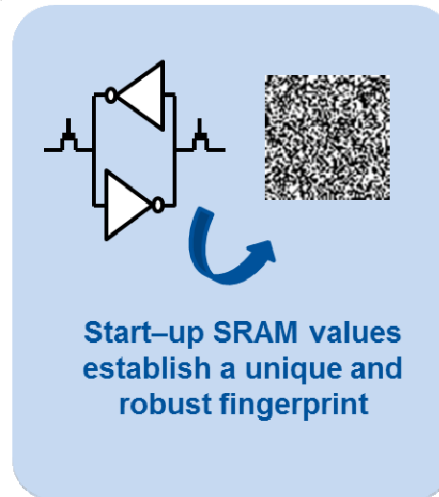
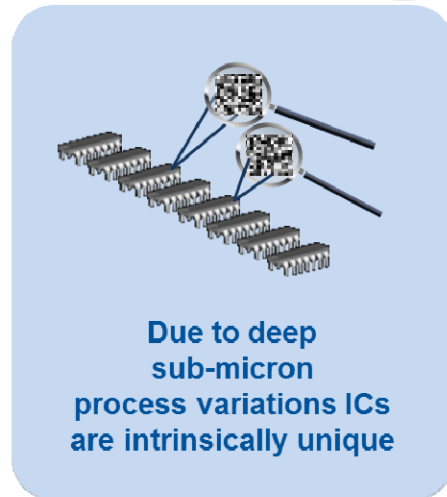
- ◆ クラウドのマーケット拡大に関連して、Securityを確保する方法の紹介があった。
- PUF (Physical Unclonable Function)
- HCE (Host Card Emulation)
- Tokenization

# Towards Trusted Cloud Services

## PUFの使用[C7]

PUFは、物理的に複製できない機器ごとに固有な特徴

- SRAMの電源投入時の値が一例



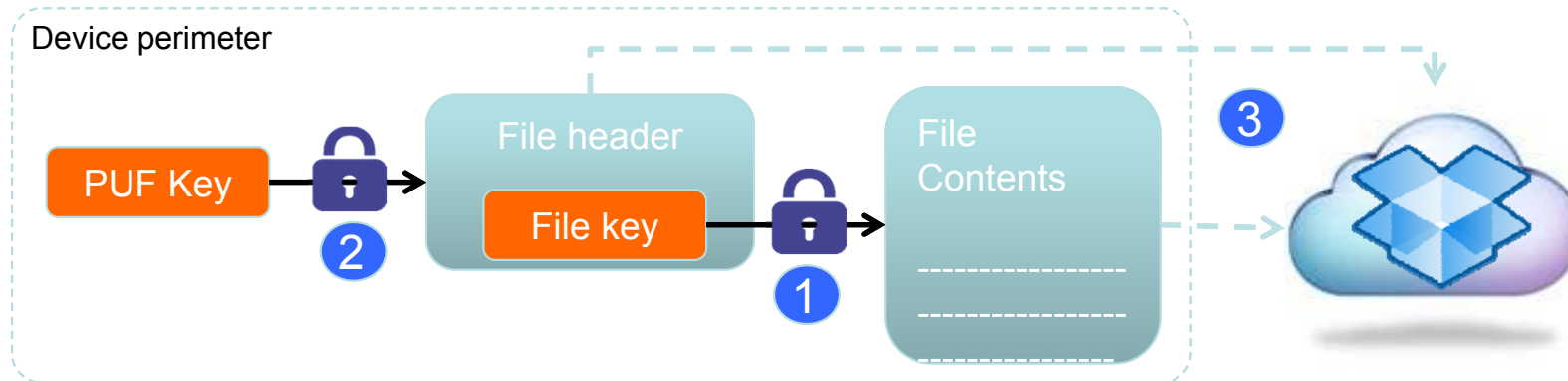
- PUF properties**
- Strong entropy, high randomness keys
  - Unclonable, tamper-proof
  - No keys at rest
  - Enables independent Root-of-Trust

- SRAM PUF benefits**
- SRAM available in every device
  - No custom design needed
  - Tested and vetted for defense markets
  - Proven, robust and scalable technology
  - Available in mobile phones, USB dongle

[C7] CARTES2014発表: Pim TUYLS, Founder & CEO - Intrinsic-ID, "NETHERLANDS Bringing Trust to the Cloud"

# Towards Trusted Cloud Services

## PUFの使用



### ◆ 使用法:

ファイルを暗号化するにあたって、暗号化鍵を保護するのに PUF Keyを使う

暗号化鍵をどう保護するかが課題

### ◆ PUFであることのメリット:

PUFは機器に結びついていて、複製できない

→PUF Keyが盗まれることがない。



# Towards Trusted Cloud Services

## HCEの使用[C8]

- ◆ HCEは、ソフトウェアでスマートカードの機能を実現する技術
- ◆ NFC技術と組み合わせて、携帯電話での決済に使われる
  - 長所: 安い、端末と通信は変更不要
  - セキュリティに関しては議論されている
- ◆ Google, Visa, Mastercardで採用され始めている



[C8] So why all this interest in HCE?, Douglas KINLOCH, VP Business Development, Metaforic - Inside Secure, UNITED KINGDOM

# Towards Trusted Cloud Services

## Tokenization<sup>[C9]</sup>



- ◆ 決済時の通信にPAN (Primary Account Number) の代わりに、機密データを含まないTokenを使う。
- ◆ HCEに組み合わせることで、HCE単独よりもセキュリティを向上できる。

# 目次

- ◆ CARTES 2014の全体について
- ◆ Conferenceでの発表から、いくつかのトピックの紹介
  - Biometrics Applications
  - Security Documents & e-Governments
  - Towards Trusted Cloud Services
  - Instant Issuing and Personalization: What's new?

# Instant Issuing and Personalization: What's new? 即時発行:銀行支店でのカード発行[C10]

- ◆ 銀行での即時発行はメリットが多い。
  - 支払い用カードの30%は発行日に使われる→使用量増加が見込まれる。
  - 配送の危険が減る。

**Why Offer Instant Issuance?**

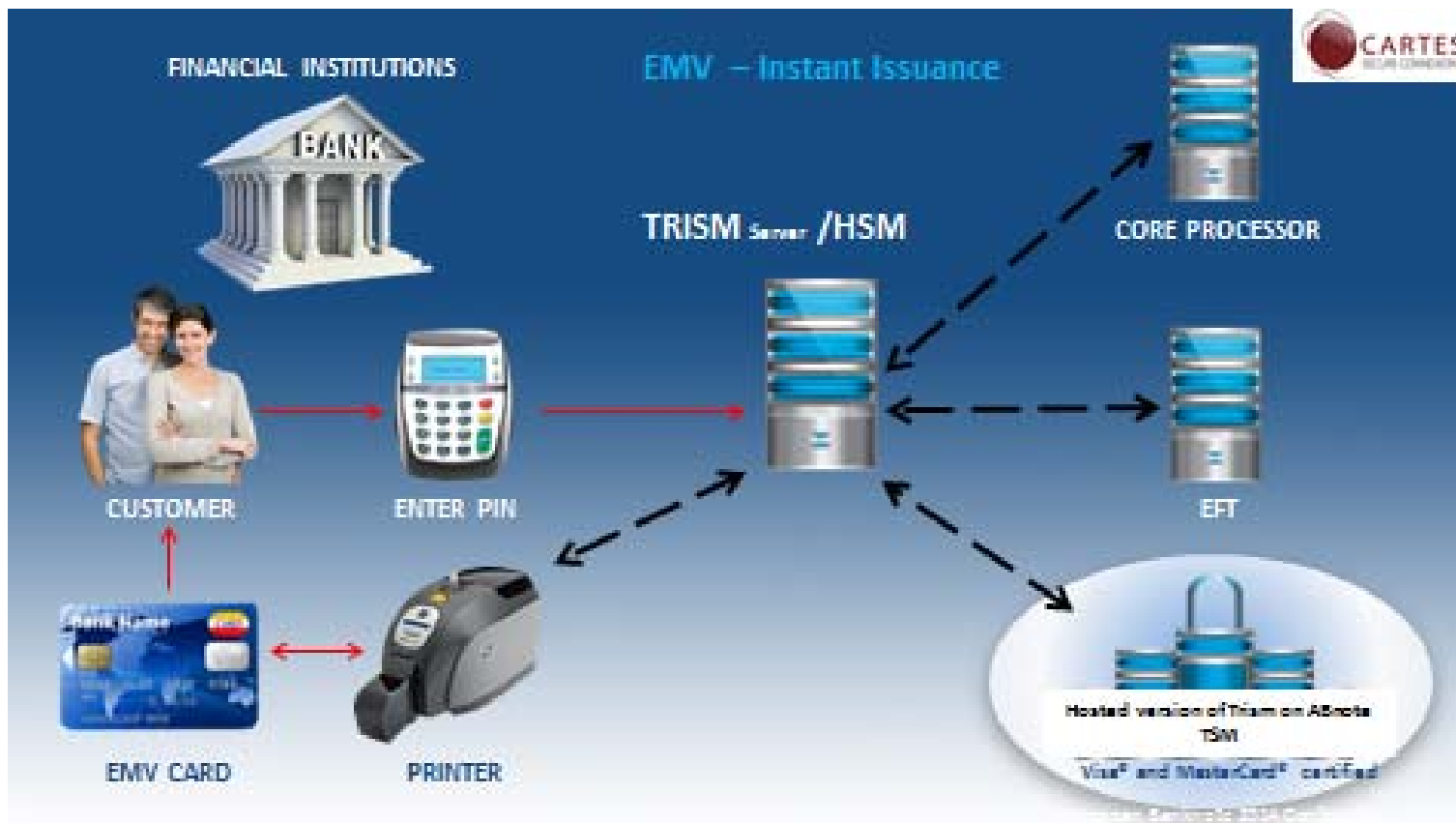
- Security**: Eliminate risk of card theft during shipping
- Cost Reduction**: Reduce paper waste from card and PIN mailers
- Transaction Increase**: No 7-14 day wait to make purchases with card
- Quality Assurance**: In-house control of card layouts ensures members receive a customized card meeting their specific demands

CARTES  
SCORE COMPANY

- ◆ 展示会では、小型カード発行機が多数展示されていた
- ◆ 即時発行を可能にする手法の提案

# Instant Issuing and Personalization: What's new? 即時発行:銀行支店でのカード発行[C10]

- ◆ ユーザデータは中央で用意される。
- ◆ 支店では鍵を扱う必要はない。
- ◆ 中央・支店の両方でHSMを使用したシステムとして実現される



## まとめと所感

- ◆ CARTESは「カード」を意味する語であるが、CARTES 2014ではカード以外の重要な発表も数多くあった。
  - バイオ、携帯端末、クラウド、、、
- ◆ セキュリティがより広い分野で求められている。
  - カードと同じセキュリティは現実的ではない。  
リーズナブルな妥協点は？？？
- ◆ IPAとしても情報収集し、共有していきたい。

**ハードウェア脆弱性評価の最新技術動向  
に関するセミナー  
— CARDIS参加報告 —**

2015年1月9日

独立行政法人 情報処理推進機構  
技術本部 セキュリティセンター

# 目次

---

- ◆ ハードウェアセキュリティピックの紹介
- ◆ CARDIS2014の発表の概要紹介
- ◆ IPAの取り組み



# ハードウェアセキュリティピックの 紹介

# サイドチャネル攻撃 (Side Channel Analysis)

- ◆ 暗号機能を実装したハードウェア(スマートカード等)の動作中に、そのハードウェアの状態を観測することで得られる情報を利用して、暗号鍵といった秘密情報の復元を試みる
  - 電力解析(Power Analysis)
    - ハードウェアの消費電力を測定し、その情報から解析する。
      - SPA (Simple Power Analysis): 1つの電力波形を直接調べる。IC内の処理のパターンを見る。
      - DPA (Differential Power Analysis): 多数の電力波形を統計処理して解析する。消費電力のデータ依存部分を抽出することができ、また、ノイズを軽減することができる。
    - CMOS半導体の特性上、トランジスタのスイッチング(0→1, 1→0)が起こる時に消費電力が大きくなることを利用。
  - 電磁波解析(Electromagnetic Analysis)
    - 動作中のハードウェアのからの漏洩電磁波から解析する。電力解析同様、1つの波形から解析するSEMA、多数の波形から解析するDEMAがある。
    - 局所的なアクティビティを検知することが可能。

# DPAの例1

## ◆ 初期のDPA: DoM (Difference of Mean)

鍵の先頭1バイト=00と仮定

平文(の先頭1バイト)	第1ラウンドのsboxの出力の先頭1バイト	MSB
7d	21	0
7c	10	0
6a	02	0
da	57	0
17	f0	1
...	...	...

鍵の先頭1バイト=01と仮定

平文(の先頭1バイト)	第1ラウンドのsboxの出力の先頭1バイト	MSB
7d	10	0
7c	21	0
6a	7f	0
da	b9	1
17	47	0
...	...	...

1. 平文をランダムに変化させて暗号化を行い、消費電力を測定する
2. 中間値のあるビットに注目し、それが0か1かによって電力波形を分類する。それを各鍵仮説(AES鍵の先頭1バイトの場合、256通り)に対して行う。
3. 2群に分けた電力波形について、それぞれ平均を取る
4. 誤った鍵仮説に対しては、平均値の差がゼロに近い値になるが、正しい鍵仮説に対しては、平均値の差が大きい値になると考えられるので、これによって正しい鍵の値が判明する

# DPAの例2

## ◆ CPA (Correlation Power Analysis: 相関係数を使用する)

鍵の先頭1バイト=00と仮定

平文(の先頭1バイト)	第1ラウンドのsboxの出力の先頭1バイト	HW
7d	21	2
7c	10	1
6a	02	1
da	57	5
17	f0	4
...	...	...

鍵の先頭1バイト=01と仮定

平文(の先頭1バイト)	第1ラウンドのsboxの出力の先頭1バイト	HW
7d	10	1
7c	21	2
6a	7f	7
da	b9	6
17	47	4
...	...	...

1. 平文をランダムに変化させて暗号化を行い、消費電力を測定する
2. 中間値のhamming weightを計算する。それを各鍵仮説(AES鍵の先頭1バイトの場合、256通り)に対して行う。
3. 消費電力と、hamming weightとの間の相関係数を計算する
4. 誤った鍵仮説に対しては、相関係数の値がゼロに近い値になるが、正しい鍵仮説に対しては、相関係数の値が大きい値になると考えられるので、これによって正しい鍵の値が判明する

## DPAの例3

### ◆ MIA (Mutual Information Analysis)

- ある中間値をターゲットにする (例:  $W=S(P\oplus k)$ )
- $O$ : 消費電力を測定し、その分布を求める。
- $L_k$ : leakageに現れるpower model。ただし、power modelが不明なら、 $L_k=Id$  (恒等関数) としてもよい。
- $H=L_k(W)$  を計算し、その分布を求める。
- 各鍵仮説に対して、Mutual Information  $I(O;H)$ を計算する。
- 最も高いMutual Informationを与える鍵仮説を鍵と推定する。
- 理論的には、正しい鍵仮説に対しては正のMutual Informationが得られ、誤った鍵仮説に対しては、 $O$ と $H$ は独立となり、 $I(O;H)=0$ となるはずである。

# サイドチャネル攻撃対策

## — Hiding —

- ◆ サイドチャネル攻撃は、暗号演算過程の中間値の情報が漏れることを利用する
  - → 消費電力と中間値との相関をなくそうとすることで対策する
- ◆ 例
  - Random Delay: 演算の間にランダムに遅延を挿入する
    - 電力波形の位置合わせを困難にする
  - ノイズ付加: 消費電力にノイズを付加して、データに依存する消費電力波形を見づらくする
  - Dual Rail Pre-Charge Logic
    - 普通のICでは1ビットを1本の信号線で表現する
    - Dual Rail では、1ビットを2本の信号線で表現する
      - 論理的なビットの値が0でも1でも消費電力が(理論的には)変わらない。

値	内部表現
0	01
1	10

# サイドチャネル攻撃対策

## — Masking —

- ◆ 中間値に、ランダムな値を「マスク」して、生の中間値の情報が漏れることを防ぐ。
- ◆ blinding とも言う。
- ◆ 秘密情報を2個(以上)の値に分散して持たせているとの観点から、Secret Sharingと言うこともある。

# サイドチャネル攻撃対策 — Masking —

## ◆ マスキングの種類

- Boolean Masking
  - 論理演算 (排他的論理和) によるmasking
- Arithmetic Masking
  - 算術演算 (加法や乗法) によるmasking



# サイドチャネル攻撃対策 — Masking —

## ◆ Boolean Maskingの例

AESの第1ラウンド

$a \leftarrow p_i \oplus k_i$  ( $p_i$ : 平文の第*i*バイト,  $k_i$ : 鍵の第*i*バイト)

$b \leftarrow \text{Sbox}(a)$

↑

この中間値が攻撃される

マスキング

$m_1, m_2$ : ランダムなマスク

$a' \leftarrow (p_i \oplus m_1) \oplus k_i$

$b' \leftarrow \text{Sbox}'(a)$  ( $\text{Sbox}'$ : マスクを計算に入れたSbox ( $=\text{Sbox}(x \oplus m_1) \oplus m_2$ ))

↑

この値は、鍵の値に依存しない (ランダムなマスクのため) ので、  
この値に対して攻撃されても鍵は復元できない

最終ラウンド終了後にマスクを外して暗号文を出力する

# サイドチャネル攻撃対策 — Masking —

## ◆ Arithmetic Maskingの例

RSA暗号での復号

$c^d \bmod n$  ( $c$ : 暗号文,  $d$ : 秘密鍵,  $n$ : 法)

↑

指数 $d$ が攻撃される可能性

exponent blinding

$r$ : 乱数

$d' = d + r\phi(n)$  ( $\phi$ : Eulerのトーシェント関数)

$c^{d'} \bmod n$  を計算する

↑

生の指数 $d$ を使用しないので、 $d$ そのものが攻撃対象になることはない

# サイドチャネル攻撃

## — Higher-Order Attack —

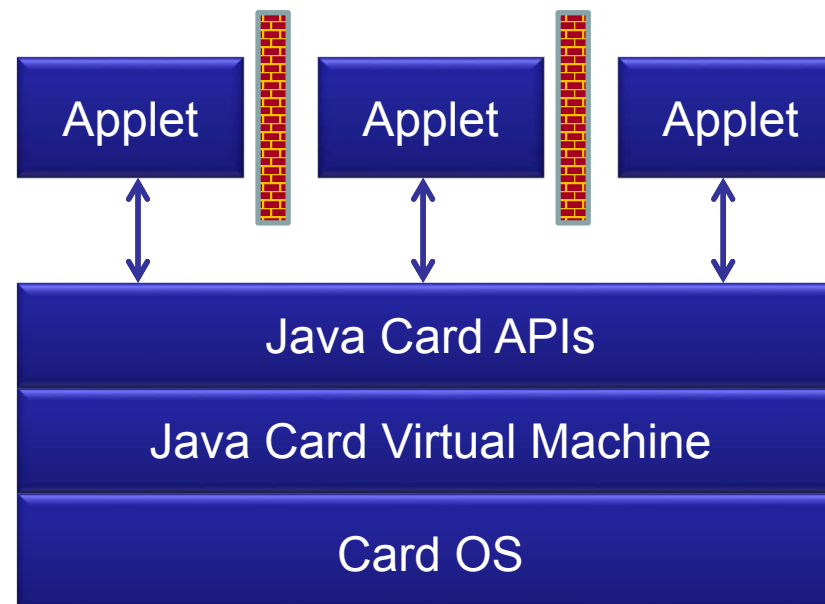
- ◆ Higher-Order Attack
  - Maskingを使った実装に対する攻撃
  - 2nd-order attackは、2個の中間値からのjoint leakageを悪用する攻撃
  - 例えば、maskingを使用したAES実装において、1個のマスク値を使い続けた場合、2nd-order attackが有効

# 故障利用攻撃 (Fault Injection Attack)

- ◆ 暗号機能を実装したハードウェアの動作中に故意に故障 (fault) を起こし、計算誤りを利用して解析を行う
  - クロックグリッチ
  - 電源グリッチ
  - レーザー照射
  - 電磁場印加
- ◆ 故障利用攻撃の例: RSA-CRTに対するBellCoRe Attack
  - $s = m^d \bmod n$  とする(正しい署名)
  - $s'_p = m^{dp} \bmod p$  ( $s_p$ の計算にfaultを入れる)
  - $s_q = m^{dq} \bmod q$
  - $s' = s_q + q(i_q(s'_p - s_q) \bmod p)$
  - このとき、 $\gcd(s - s', n) = q$ 。また、 $\gcd(m - s'^e, n) = q \rightarrow$  秘密の素因数が判明

# Java Card

- ◆ Javaテクノロジーに基づいている
- ◆ アプレットと呼ばれるJavaベースのアプリケーションを搭載できる
- ◆ 複数のアプレットをインストールできる
- ◆ 異なるアプレットからデータが保護される (ファイアウォール)



# Java Cardのセキュリティ機構



## ◆ Type Safety

- ある型の値を他の型の値として再解釈する (type confusion) ことは禁止されている

## ◆ Byte-code Verifier

- バイトコードを解析して、不正な形式のバイトコードを検出
- offcard あるいは oncard で実行される

## ◆ Defensive Virtual Machine

- 不正なバイトコードの実行が阻止される

## ◆ Firewall

- アプレットのデータへの、他のアプレットからの許可されないアクセスは禁止される

# Type Safety

- ◆ いかなるリファレンスも、元の型のリファレンスとしてのみでリファレンスができる
- ◆ もしbyte配列のリファレンスがshort配列のリファレンスとしてアクセスできると?

byte[4]としてリード

0	1	2	3
00	01	02	03

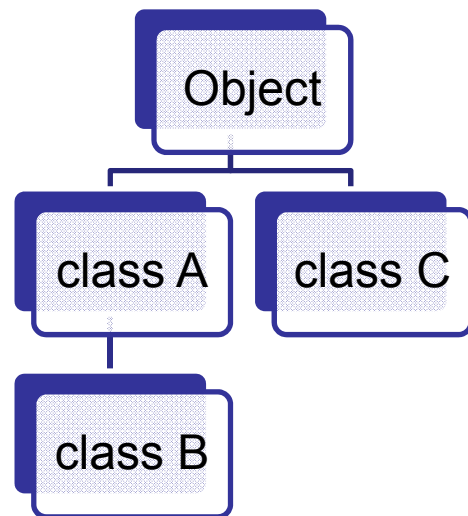
short[4]としてリード

0	2	4	6
0001	0203	XXXX	XXXX

- 配列境界を越えてアクセスできる!
- このような現象を”Type Confusion”と呼ぶ

# Type Safety

- 不正なクラスキャストは禁止されている。コンパイラ及び実行環境で規制される。



```
class A {};  
class B extends A {};  
class C {};  
A a;  
B b;  
C c;
```

キャストの試み	結果
(A)b	許可
(B)a	クラスBのオブジェクトでない場合、 ClassCastException 例外が投げられる
(A)c	コンパイルエラー



# Type Confusion

## ◆ Ill-formed applet

- 不正なバイトコードの並びを含むアプレット
- Javaコンパイラは決して生成することはない
  - CAPファイルを直接改変すると生成できることがある
- Ill-formed appletを防ぐ対策
  - Byte Code Verifierがコード解析で検出する
  - Defensive Virtual Machineが実行時に検出する

不正なバイトコードの並びの例

sload_1	1番目のローカル変数(short型)をスタックに積む
areturn	スタックトップの値(リファレンス型)としてメソッドからリターン

**short型の値をリファレンスとして再解釈!**

# Dangling Reference

- ◆ 不正な領域を指すリファレンス
- ◆ 実装に脆弱性がある場合、以下の方法で作成できることがある
  - type confusion (ill-formed appletで引き起こす)
  - トランザクション機構の欠陥
  - etc...

# CARDIS2014の発表内容の概要紹介

# Memory Forensics of a Java Card Dump

Jean-Louis Lanet, Guillaume Bouffard, Rokia Lamrani, Ranim Chakra,  
Afef Mestiri, Mohammed Monsif, and Abdellatif Fandi

Smart Secure Devices (SSD) Team, University of Limoges

# Memory Forensics of a Java Card Dump

- ◆ Java Card攻撃の目的
  - メモリダンプの取得
  - メモリダンプからのリバースエンジニアリング
- ◆ メモリダンプ取得を行う手段についての研究は多い
- ◆ メモリダンプからリバースエンジニアリングを行うのは容易ではない。それを助けるツールも今のところない
- ◆ メモリダンプに含まれるもの
  - 命令コード
  - データ
- ◆ Java Card Disassembler and Analyzer (JCDA)を開発
  - メモリダンプから、Javaコードあるいはネイティブコードを検出
  - 認識したJavaコードを逆アセンブル
  - CAPファイルを生成
  - CAPファイルが生成できれば、そこからclassファイル、さらにjavaファイル(ソース)を生成するツールは存在する

# Heap Hop! The Heap Is Also Vulnerable

Guillaume Bouffard<sup>1</sup>, Michael Lackner<sup>2</sup>, Jean-Louis Lanet<sup>1</sup>, and Johannes Loinig<sup>3</sup>

<sup>1</sup>University of Limoges

<sup>2</sup>Institute for Technical Informatics, Graz University of Technology

<sup>3</sup>NXP Semiconductors Austria GmbH

# Heap Hop! The Heap Is Also Vulnerable

- ◆ Java Cardへの主な攻撃
  - type confusion
- ◆ 対策
  - Typed Stack (タイプ付けされたスタック)
- ◆ Typed Stackの存在下で、スタックの攻撃は困難
- ◆ ヒープを攻撃
  - スタックはtypedでも、ヒープ上にあるオブジェクトのインスタンスフィールドはリソースの制限によりtypedでないことが多い

# Heap Hop! The Heap Is Also Vulnerable

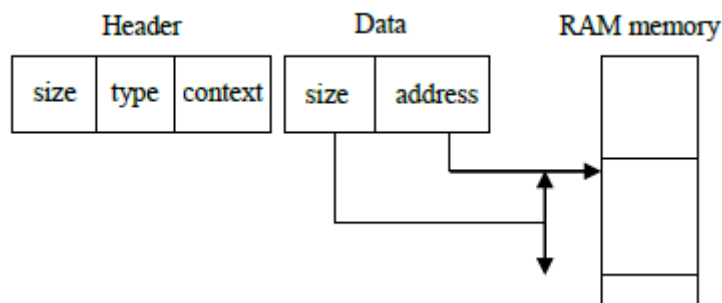
```
Short getObjectAddress(Object object){
    L0: aload_1 // object reference given in parameter
        putfield_a_this 0
        getfield_s_this 0
        sreturn
}
```

引数として与えられたobjectへのリファレンスがshortの値として返される



# Heap Hop! The Heap Is Also Vulnerable

Transient arrayの構造



transient arrayのサイズとデータアドレスが0x8E9Dから割り当てられていると仮定する

```
    sspush 0x00FF
    putstatic_s 0x8E9B // size: 0x00FF
    sspush 0x00FE
    putstatic_b 0x8E9D // address: start from 0x00FE
    sreturn
}
```

アドレスは、0から0xFFFF、すなわちメモリ全体をカバーできるので、このtransient arrayを通してメモリ全体のダンプを取得できる

# Study of a Novel Software Constant Weight Implementation

Victor Servant<sup>1</sup>, Nicolas Debande<sup>2</sup>, Housseem Maghrebi<sup>1</sup>, Julien Bringer<sup>1</sup>

<sup>1</sup>SAFRAN Morpho

<sup>2</sup>SERMA Technologies (ITSEF)

# Study of a Novel Software Constant Weight Implementation



- ◆ Hamming Weightが漏れるモデルを仮定
- ◆ Constant Weight Codes
  - すべての値が同じHamming Weightを持つコード
  - Hamming Weightが $x$ となる $y$ ビットの値で表現する場合、 $(x,y)$ -code という
  - Dual Rail Encodingは  $(1,2)$ -codeの例

0 → 01	1 → 10
--------	--------

- 例えば、 $(3,6)$ -code で4ビットをエンコードすることができる

0 → 000111	4 → 010011	8 → 011010	12 → 100110
1 → 001011	5 → 010101	9 → 011100	13 → 101001
2 → 001101	6 → 010110	10 → 100011	14 → 101010
3 → 001110	7 → 011001	11 → 100101	15 → 101100

# Study of a Novel Software Constant Weight Implementation

- ◆ (3,6)-code を使用してAESを実装
  - 内部表現において、1バイトを上位4ビットと下位4ビットに分割して、それぞれを(3,6)-codeでエンコードする
  - エンコードされた値でのSbox, XORのテーブルを作る
- ◆ 実装した結果
  - CPAには耐性あり
  - パフォーマンスは、マスキングによる実装より良い
  - ある程度のFault検出機能も備える

# Balanced Encoding to Mitigate Power Analysis: A Case Study

Cong Chen, Thomas Eisenbarth, Aria Shahverdi and Xin Ye

Worcester Polytechnic Institute

<http://users.wpi.edu/~teisenbarth/pdf/BalancedEncodingCARDIS2014.pdf>

# Balanced Encoding to Mitigate Power Analysis: A Case Study

## ◆ Balanced Encoding Countermeasure

- Hamming Weightが同じになるようなエンコーディング
- Dual rail encodingを基にしたエンコーディングを使用して、軽量暗号Princeを実装
- 1ニブル  $(b_3b_2b_1b_0)$  を、 $\bar{b}_3b_3\bar{b}_2b_2\bar{b}_1b_1\bar{b}_0b_0$  や  $b_0\bar{b}_2b_1b_3\bar{b}_1b_2\bar{b}_0\bar{b}_3$  のようにエンコードする

## ◆ Conclusion

- CPAに対してはかなりの効果はあるが、完璧ではない
- 追加のhiding countermeasureが必要となるケースにおいて、このcountermeasureは軽量暗号に対して有益と考える。

# On the Cost of Lazy Engineering for Masked Software Implementations

Josep Balasch<sup>1</sup>, Benedikt Gierlichs<sup>1</sup>, Vincent Grosso<sup>2</sup>,  
Oscar Reparaz<sup>1</sup>, François-Xavier Standaert<sup>2</sup>

<sup>1</sup>KU Leuven Dept. Electrical Engineering-ESAT/COSIC and iMinds

<sup>2</sup>ICTEAM/ELEN/Crypto Group, Université catholique de Louvain

<https://eprint.iacr.org/2014/413>

# On the Cost of Lazy Engineering for Masked Software Implementations



- ◆ d-th order masking
  - 1つの中間値を $d+1$ 個のshareに分ける
  - $d$ th-order attackに対して耐性がある
- ◆ Leakage
  - Value-based leakage
    - 中間値の値そのものからのleakage
    - Hamming Weight Modelが典型的
  - Transition-based leakage
    - 中間値の変化に対するleakage
    - Hamming Distance Modelが典型的
- ◆ Value-based leakageに対する $d$ th-order securityの証明は、Transition-based leakageに対する  $\lfloor d/2 \rfloor$ -order securityの証明につながる
- ◆ ATmega163にmaskingを使用したAESをソフトウェアで実装して検証 (Welch t-testを使用)
  - 1st-order maskingの場合、transition-based leakageでは1st-order leakageを検出
  - 2nd-order maskingの場合、transition-based leakageでも1st-order leakageは検出されない



# Kangaroos in Side-Channel Attacks

Tanja Lange<sup>1</sup>, Christine van Vredendaal<sup>1,2</sup>, and Marnix Wakker<sup>2</sup>

<sup>1</sup>Department of Mathematics and Computer Science  
Eindhoven University of Technology

<sup>2</sup>Brightsight B.V.

<https://eprint.iacr.org/2014/565>

- ◆ 楕円曲線暗号に対する攻撃
- ◆ Pollard's kangaroo algorithm
  - 楕円曲線上の離散対数問題を解くためのアルゴリズム
- ◆ サイドチャネル攻撃で、鍵のビットが部分的に復元でき、鍵空間が絞り込まれたと仮定
- ◆ Pollard's kangaroo algorithmを応用して、残りの鍵空間から正しい鍵の候補をランク付け

# On the Security of Fresh Re-keying to Counteract Side-Channel and Fault Attacks

Christoph Dobraunig, Maria Eichlseder, Stefan Mangard, and Florian Mendel

IAIK, Graz University of Technology

<https://eprint.iacr.org/2014/508>

## ◆ Fresh Re-keying: プロトコルレベルでのサイドチャネル/故障利用攻撃対策

- 暗号プリミティブそのものに対策を入れるのは、特に低コストのデバイスでは容易なことではない
- 同じ鍵で繰り返し暗号プリミティブが実行されることを防ぐことによって、サイドチャネル/故障利用攻撃への対策とする
- マスターキーからセッションキーを生成し、そのセッションキーを暗号鍵とする
- AfricaCrypt2010[1]及びCARDIS2011[2]でスキームを発表

## ◆ このFresh Re-keying schemeへの攻撃

- $n$ ビットの鍵に対し、 $2 \cdot 2^{n/2}$ の複雑さでの攻撃が可能であることを示す

1. Medwed, M., Standaert, F.X., Großschädl, J., Regazzoni, F.: Fresh Re-keying: Security against Side-Channel and Fault Attacks for Low-Cost Devices. In: Bernstein, D.J., Lange, T. (eds.) AFRICACRYPT. LNCS, vol. 6055, pp. 279-296. Springer(2010)  
<http://perso.uclouvain.be/fstandae/PUBLIS/78.pdf>
2. Medwed, M., Petit, C., Regazzoni, F., Renaud, M., Standaert, F.X.: Fresh Re-keying II: Securing Multiple Parties against Side-Channel and Fault Attacks. In: Prouff, E. (ed.) CARDIS. LNCS, vol. 7079, pp. 115-132. Springer (2011)

# Evidence of a larger EM-induced fault model

S. Ordas<sup>2</sup>, L. Guillaume-Sage<sup>2</sup>, K. Tobich<sup>2</sup>, J.-M. Dutertre<sup>1</sup>, P. Maurine<sup>1,2</sup>

<sup>1</sup>CEA-TECH and ENSMSE Centre microelectronique de Provence G. Charpak

<sup>2</sup>LIRMM-University of Montpellier

# Evidence of a larger EM-induced fault model

## ◆ Electromagnetic Fault Injection

- ICチップにコイルを接近させ、コイルに電流を流して電磁場を印加することによるfault injection攻撃
- faultが発生する仕組みは、回路におけるタイミング制約違反を起こすことと考えられてきた
- EM fault injectionは、タイミング違反だけでなく、Dフリップフロップのビットセット/リセットも引き起こしていることを示す
- ‘Crescent’ injector (三日月型のコイル)がより効果的

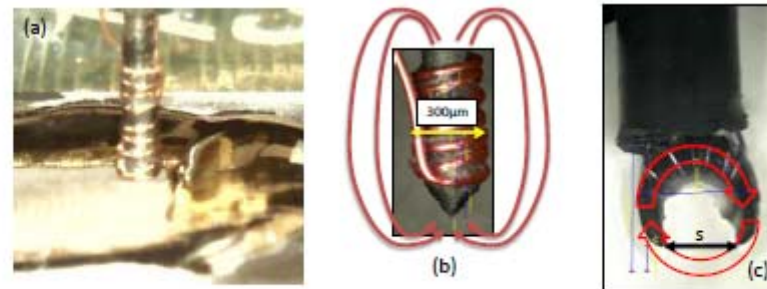


Fig. 2. EM-Injectors: (a) 'Flat' Injector (b) 'Sharp' Injector and (c) 'Crescent' Injector

- 極性 (コイルへの印加電圧の正負) が、ビットセット/リセットの振る舞いに影響
- EM Fault Injectionの可能性を広げる結果

# IPAの取り組み

## ◆ ハードウェア脆弱性評価に関する人材育成

- 新しい攻撃への耐性を評価する最先端のツールを整備して、日本の半導体ベンダ、ICカードベンダ、評価機関、大学などの研究機関が利用できる評価環境の整備を進めている。
  - 最先端の評価ツール及びテストビークル(評価対象のIC)を使用し、脆弱性を評価することで新しい攻撃手法を修得
    - TVCの開発が完了。希望者には貸与します。
  - ICカードの開発過程で利用し、対抗策を検証することで、高い攻撃耐性を持った製品開発が可能
  - 将来的な攻撃手法の研究活動に活用
  - 興味深い攻撃については、IPA所有の装置での再現実験の実施を検討
- 技術セミナーの開催
  - 2015年度から、ハードウェアセキュリティに関する初級者向けの技術セミナーの開催を検討中



ご清聴ありがとうございました。

当セミナーに関する質問は以下のメールアドレスまでどうぞ。

[jcmvp-info@ipa.go.jp](mailto:jcmvp-info@ipa.go.jp)