

# Where Security Meets Privacy: OPACITY, the PKI protocol for private contactless transactions

Dom Fedronic, CTO ActivIdentity



**ActivIdentity**<sup>®</sup>

*The trusted choice for identity assurance*



# Introduction

- Privacy vs. Security
  - A system can be secure and not private
  - A insecure system cannot be private
  - Privacy requires NEW security protocols
- Privacy issues exist everywhere BUT Contactless interfaces bring them to light spectacularly
- The emergence of new protocols is required for the market to take up.
- The Open Protocol for Access Control Identification and Ticketing with privacY is an example of Privacy Enhanced Technology dedicated to contactless transactions.
- Centrelink Plaid is another one.

## Privacy: a problem wider over the contactless interface

Short term:

- Unprotected contactless transactions can be sniffed and spoofed at significant distances.
- BTW, Malware can have similar effect on contact transactions.

Longer term?

- More generally, in the same way that legitimate companies use our digital trail to “personalize” their offering, illegitimate players could also leverage our trail to “personalize their attacks”.

## Privacy vs Security

- Security protects systems in general
  - System's security insist on the importance of Identities
  - System's security require user to prove their identities over and over...
- Privacy protects Persons or Identities by enforcing Access Rules on information allowing identification
  - Privacy demands that identity information is only released on a need to know basis and in a governed way.
  - The ungoverned trail is a problem.
- Enforcement of Access Rules require
  - System Integrity
  - Authentication
  - Confidentiality of the information being transmitted

## Specifics of Privacy: the trail

- Protection of Personally Identifiable Information (PII)
  - The problem of de-identification
  - Format Preserving Encryption
- Protection of the Trail
  - All the transaction accomplished define your identities.
- IDs are sensitive data and must be protected for access, they are the first line of attack against the identities. They should be governed.
  - Inventoried
  - Organized in security domains
  - Rules to limit access
  - The problem is holistic: the whole interface must follow the rules

## Specifics of Privacy (2)

- Identifiers utilization in today's protocols
  - Card serial numbers
  - Certificates
  - Public keys
  - Contactless
  - CHUID
  - GUID
- The more the identifiers are global and unique , the more their usage and access should be restricted !

## Privacy meets security

- Unavoidable that weak systems will use the Global Unique Identifiers in databases along with biographic, demographic data and the binding becomes public when the systems get broken
- When specific users are located, specific aggressive actions might be triggered.
- Security depends on privacy!

## Current Authentication Protocols and Identity Leaks

- An "open" identification phase
  - certificates
  - serial numbers
  - diversification parameters
  - PKI, SKI, same problem
- System centric approach that requires the User to authenticate first, forcing him to reveal his identity, potentially to rogue systems.
- IDs should only be released to trusted systems (i.e., authenticated and authorized)

## Principles of Privacy Enhanced Protocols

- Establish secure session between the card and the terminal or host with ephemeral (only used for one session) keys pairs
- Card Authenticates Terminal or Host and validate that the terminal owns both the ephemeral private key and the authentication key.
- Authenticate the card to the terminal, protecting the identification data of the card with the session keys, and prove to the terminal that the card owns both the ephemeral private key and the Terminal authentication key.
- The channel is ready to transport any PII data back and forth with privacy and forward secrecy protection.

## Principles of Privacy Enhanced Protocols

- The protocol is asymmetrical:
  - One of the peers has to take a chance and identify him/herself even inside a P2P secure connection.
  - It should be the “authority” or the Terminal, not the user.
  - This shows the value of Group keys (what is important for the card is to know that the terminal or host is trusted, the identity of the terminal might only be relevant in an authorization context and can be represented by a Domain as opposed to an ID).
  - On the flip side, if the recipient was rogue the protocol will allow the terminal to know it.

## The Privacy Enhanced Protocols

- Step1: Key Agreement → Agree on a shared secret and derive sessions keys from it
  - **P2P un-authenticated key agreement** (shared secret establishment and Key Derivation Function), **not revealing card identity**
  - Optionally protect the Host authentication with the session keys
  - Authorization: what is the host authorized to see?
  - Card Authentication: **revealing identity data to authorized hosts only**
  - Optionally Repeat Key Agreement (optional KDF again)
- Step2: Secure Messaging → Use the session keys to encrypt and Mac the data

## Forward secrecy

- if the attacker has captured an exact transcript of the encrypted communication and stolen a Terminal or the Card or even the central Hardware Security Module and gained access to the static keys stored on those modules, he will not be able to decrypt the communications..
- The terminal generates an ephemeral key pair for each session, uses it to derive the shared secret and from their the session keys with the card, and deletes the ephemeral key pair, the shared secret and the sessions keys when the session ends

# The Privacy Enhanced Protocols

- Example of "modern protocols"
  - Protocol following NIST SP 800-56A (march 2007) guidance
  - NSA SuiteB recommendation (until 2030)
  - MXI
  - IPSEC-IKE
- Examples of PET protocols
  - En14890 - M-EAC2.0 (non 800-56A KDF)
  - PLAID (non 800-56A)
  - ISO24727-3 EC key agreement protocols (***Actividentity contribution***)
  - OPACITY

# In spite of huge Business Value Contactless Interfaces are under-utilized

- Current Usage
  - Physical Access
  - Transit
  - Payment
  - Dirty environments
- Current situation
  - VULNERABLE
  - OBSCURE
  - WEAK
  - VERTICAL
  - PROPRIETARY
- The Potential of ubiquity of contactless interfaces is not fulfilled.

Result: usage of contactless interfaces is limited by policy...

## Introduction to OPACITY

- Open Protocol for Access Control Identification and Ticketing with privacy – ( end of 2007 )
- State of the art PKI (SUITE B)
- No compromise on security and performance
- Optimized for contactless transactions
- One command/response for a Trusted Key Agreement and Authentication
- Robust to interruptions
- Standard
  - NIST SP 800-56A
  - ISO 7816-4
  - SuiteB

## Quick Protocol description

- We took the formal steps of a secure messaging protocol and “collapsed together some steps”
- A Baseline protocol version for speed
- An enhanced protocol version with Forward Secrecy for more sensitive needs.

# Terminal

SuNn/W/FhuW  
~FduFrp p dggv

VNhf/VNp df @  
NGI-HFGK +  
SxeNn|HF/SuNn|W,,

Ghfu|swp vj  
Fkhfn DxwFu|swF  
+Xvh IGF,

# OPACITY Baseline

FhuW/Fkdw

p vj<sub>VNhf/VNp df</sub> -IGF/DxwFu|swF, /  
SxeNn|HF

p vj<sub>VNhf/VNp df</sub> +FduFrp p dgg,

p vj<sub>VNhf/VNp df</sub> +FduUhsrqvh,

# Card

IGF/DxwNn/F

Fkhfn FhuW

DxwFu|swF @  
HQF<sub>DxwNn|F</sub> +Fkdw,

JhfHFNn|Sdu+22wdqvlnqwnh|v  
SxeNn|HF/SuNn|HF,

VNhf/VNp df @NGI-HFGK+  
SxeNn|W/SuNn|HF,,

Ghwh SuNn|HF

Surfhv FduFrp p dgg

# Terminal

Su<sub>y</sub>Nh|W/Fhuw  
~Fdu<sub>g</sub>F'rp p d<sub>g</sub>v<sub>t</sub>

Jhq<sub>F</sub>HNh|Sdlu+  
SxeNh|HW/  
Su<sub>y</sub>Nh|HW,

Rq<sub>d</sub> wk<sub>l</sub>bw<sub>h</sub>up l<sub>p</sub>dof<sub>d</sub>q gh<sub>f</sub>u|sw  
vh<sub>f</sub>r<sub>g</sub>g e<sub>a</sub>r<sub>e</sub> d<sub>g</sub>g j<sub>h</sub>wSxeNh|HF 1

VN<sub>h</sub>q<sub>f</sub>/VN<sub>p</sub> d<sub>f</sub> @  
NGI+HFGK +  
SxeNh|HF/Su<sub>y</sub>Nh|HW,

F'khfn DxwkFu|sw<sub>F</sub>

# Forward Secrecy

Fhu<sub>W</sub>/F'kd<sub>W</sub>/  
SxeNh|HW

p v<sub>j</sub> VN<sub>h</sub>q<sub>f</sub>/VN<sub>p</sub> d<sub>f</sub> -HGF/DxwkFu|sw<sub>F</sub> /  
Hq<sub>f</sub> SxeNh|w+SxeNh|HF , , /

p v<sub>j</sub> VN<sub>h</sub>q<sub>f</sub>/VN<sub>p</sub> d<sub>f</sub> -F'du<sub>g</sub>F'rp p d<sub>g</sub>g ,

p v<sub>j</sub> VN<sub>h</sub>q<sub>f</sub>/VN<sub>p</sub> d<sub>f</sub> -F'du<sub>g</sub>Uhvsr<sub>q</sub>vh ,

# Card

IGF/DxwkNh|F

F'khfn Fhu<sub>W</sub>

DxwkFu|sw<sub>F</sub> @  
HQ<sub>F</sub> DxwkNh|F +F'kd<sub>W</sub> ,

Jhq<sub>F</sub>HNh|Sdlu+  
SxeNh|HF/Su<sub>y</sub>Nh|HF ,

VN<sub>h</sub>q<sub>f</sub>/VN<sub>p</sub> d<sub>f</sub> @NGI+HFGK+  
SxeNh|HW/Su<sub>y</sub>Nh|HF , ,

Surfhw F'du<sub>g</sub>F'rp p d<sub>g</sub>g

## PLAID

- Crypto and Protocol
  - RSA + AES
- Standard
  - Proprietary ISO 7816-4 (0x80)
- Security
  - Same Group Private Key in Terminals of a Same group
  - No Forward secrecy
- Performance (Crypto Only)
  - 1x(RSA+AES)
- Usage
  - PKI multi domain
  - SKI mandatory
- Existing reference implementation

## OPACITY

- Crypto
  - ECC + AES
- Standard
  - Suite-B
  - Pure ISO 7816-4 (0x00)
  - NIST SP 800-56A C(1,1) or C(2,0) → FIPS 140-2 possible
- Security
  - Unique Private Key in each Terminal
  - Suite-B strength
- Performance (Crypto only)
  - 1x(ECKeyGen+ECDH+AES) (default)
  - 1xAES (optimal)
- Usage and Key Management
  - PKI open domain
  - PKI only mode

Thank You !

[Dfedronic@actvidentity.com](mailto:Dfedronic@actvidentity.com)

**Actvidentity**<sup>®</sup>

*The trusted choice for identity assurance*