PLAID
Authentication Protocol

Government Briefing

Will Kemp
CSIC Project Manager
Centrelink
Corporate IT Systems Division
Security and Information
Protection Branch
Phone: +612 6219 8807
Mobile: +614 27 625 515
will.kemp@centrelink.gov.au

Graeme Freedman
DotInDots
Centrelink Consultant
Mobile: +61(0403) 113624
Phone: +61 (02) 9983 9777
Fax: +61 (02) 9983 9778
graeme.freedman@dotindot.com

Agenda

- Threats
- Existing Technologies
- Changing Requirements
- What is PLAID?
- Technical skipped for high level presentations
- Centrelink Vision
- Transition Strategy

PACS Threats

- Security by obscurity no longer possible – the web and You Tube have changed that
- The attacks demonstrated in this video apply across most of the major PACS technologies including;
  - Spike of systems using weigand wire data protocols where ID leakage of weigand number is possible, including
  - 125 KHz, using various vendors proprietary protocols or
  - ISO/IEC 8000 RFID tags or most recently
  - Contactless smartcard using the CRYPTO-1 algorithm
- But not to well designed smartcard systems un-reliant on obscurity

Compendium from YouTube

Australian Government

Centrelink
giving you options

Why are PACS threats possible?

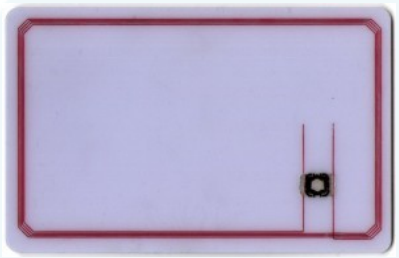
- Mostly because of technical compromises;
  - Need for speed <400ms, has meant that crypto algorithms are mostly not used, and where used;
  - Proprietary crypto has been weak, relied on obscurity, and is now totally exposed and;
  - Channel protection is slow, therefore vendors have used clear text over the air and;
  - Consequently authentication protocol data is freely readable from the communications channel and;
  - Obscuring the protocol is complex, so mostly every transaction is repeated and consequently it is easy for;
  - **Clone, Replay, Privacy, Identity Leakage and even (recently) Algorithmic attacks**

e.g: Information freely available over typical existing 125 KHz (ID tag) air interface

Site Number
"0180" is common to multiple buildings

User Number

Card sends "0180 56110"



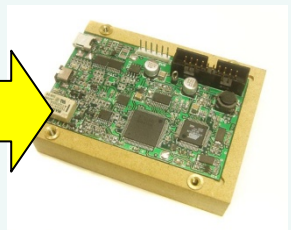
"0180 56110"

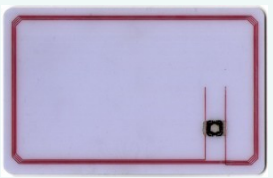
Existing door reader gets "0180 56110" and sends to access system – door opens

Reader can listen to interface at up to 10m or clone by close contact

No security or encryption on air interface – Full number meets Weigand specs

Purchase encoder from www.readx.com or build from design at www.cq.cx





Program card with "0180 56110"

Australian Government

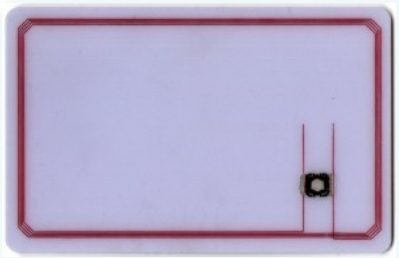
Centrelink
giving you options

e.g: Information freely available over PIV Card interfaces

CHUID, PIB
Card Holder Unique Identifier +Printed Info Buffer

Other Details

Card sends “0180 56110,Joe,Blogs”



“0180 56110,Joe,Blogs”

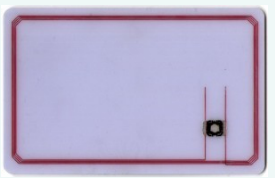
Existing door reader gets “0180 56110,Joe,Blogs” and sends “018056110 to access system – door opens

No security or encryption on air interface

Reader can listen to interface at up to 10m or clone by close contact or via Trojan on contact interface

Purchase reader/writer from almost anyone

Program card with “0180 56110,Joe ,Blogs”



Australian Government

Centrelink
giving you options

What about Logical Access Systems?

- Mostly contact based, not contactless, but changing
- Need for speed not such a big issue, users will accept 4 seconds over contactless, more over contact.
- Therefore not as problematic, since asymmetric crypto is viable for the speed requirement
  - RSA (1024/2048 bit) asymmetric crypto authentication protocols over contactless interfaces can reliably achieve 4-6 seconds
  - ECC could be used when faster smartcards are available that implement ECC in the mask/firmware (not now).
- Interface issues are actually the same for contact as contactless since a Trojan can read the interface more easily than a contactless scanner
- Having said the above, Centrelink actually needs tap-n-go on LACS over contactless

The Centrelink Problem

- Centrelink is a broad service delivery agency that deals with most Government to constituent business, particularly handing out benefits at 470+ locations across Australia
- 30,000 MS Windows/Novell desktops
- No counters, or barriers, open plan offices
- Identity card must not be removed, they must always be connected to a lanyard under a no de-badging policy. Contact cards are therefore not an option.
- Contactless needed for LACS, but COTS products initially not designed for tap-n-go
- Contactless needed for PACS, but COTS products at end of their fit-for-purpose life cycle
- Needed to develop a solution for both LACS & PACS

What is PLAID?

Protocol for Lightweight Authentication of IDentity (PLAID)

An authentication protocol which uses standards based symmetric and asymmetric cryptography in a unique way to protect the communications between smartcard and terminal devices such that strong authentication of the smartcard and data objects is possible in an extremely fast and highly secure fashion without the exposure of card or cardholder identifying information, or any other repeating information useful to an attacker.

Centrelink has an all-of-government interest and responsibility in this technology space and intends to make the intellectual property developed by Centrelink freely available to other agencies, Governments and commercial organisations on an open, free and non-discriminatory basis.

NIST and Centrelink are working on further evaluation of the protocol as well as how standardisation can be best implemented to the benefit of both countries, and Government broadly

PLAID 6 Protocol

- Uses existing off-the-shelf symmetric and asymmetric crypto algorithms (SHA1, AES 256, RSA 1024, RSA 1984) tied together via the PLAID protocol
  - Note - Neither SHA256 nor ECC are used at this time because production cards are either not obtainable from all vendors nor do they achieve the required performance, (in spite of theoretical advantage of ECC)
  - Note – RSA 1984 is a trade off between performance and security, and ensuring the transaction fits in one APDU command.
- Fast & simple - less than ½ second (400ms) and the Java Card - applet is extremely small (about 4 Kb)
- Not clone-able, re-playable or subject to privacy or identity leakage
- Same protocol can be used for PACS/LACS & contact/contactless
- PIN can be verified when card-not-present by comparing PIN hash
  - Saves user having to hold contactless card to reader during typical PKI session
- Mutual authentication Protocol
- Algorithms used are commercially available on virtually all modern smartcards including Java Card, MULTOS, most SIMs and many proprietary cards
- Algorithms and their selected key lengths have been tested on production cards and devices to ensure speeds are real, not theoretical

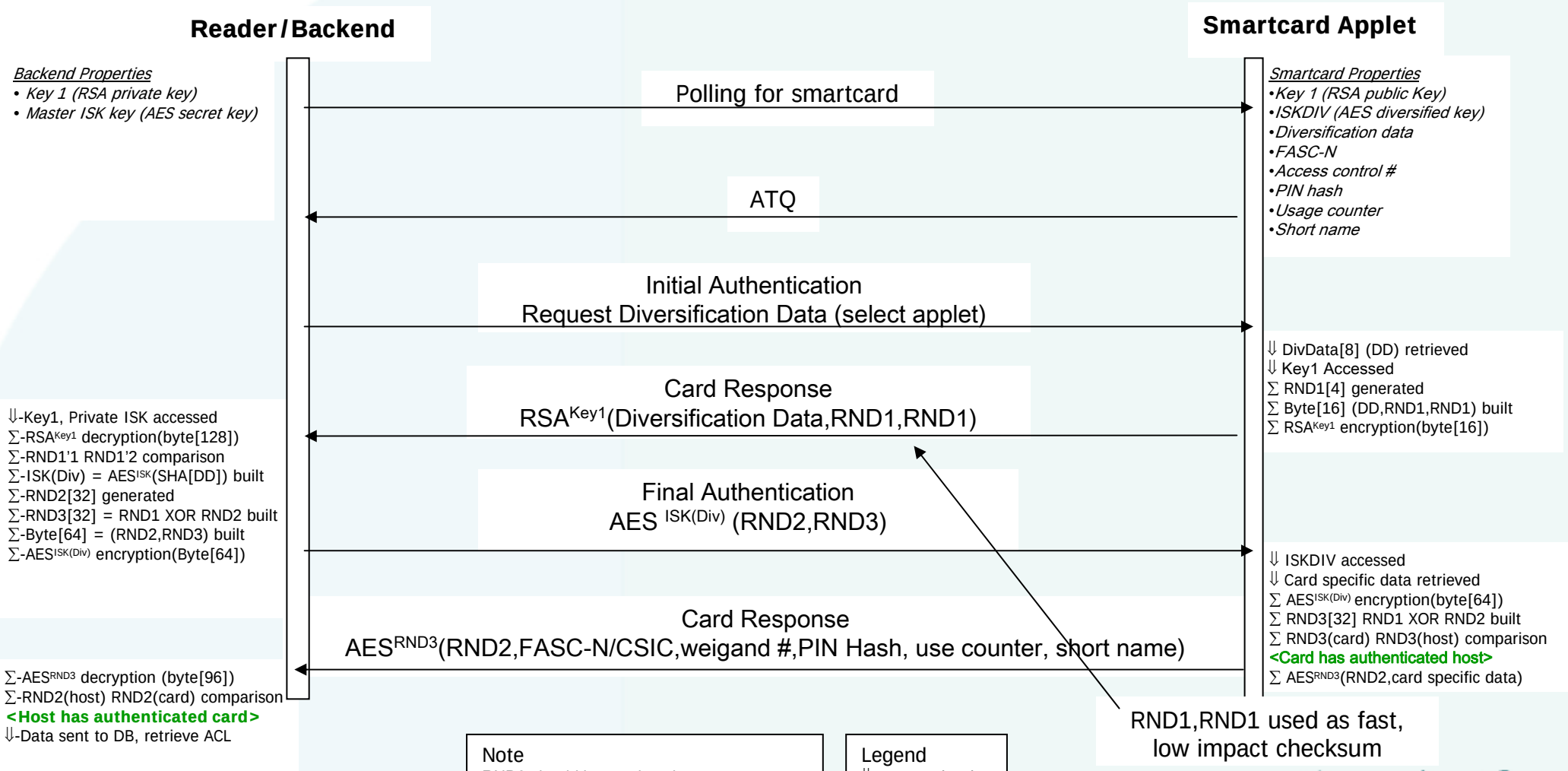
PLAID 6 Protocol

- No IP issues - IP was developed solely by the Australian Government by its agency, Centrelink, and will be openly and freely licensed
- Designed to be used either stand-alone or as a bootstrap into other specifications like Australian IMAGE, US PIV, ICAO Passports etc.
- Supports multiple concurrent specs dependant on device request to card
  - i.e. Card could supply Weigand number or CHUID or Centrelink CSIC or Passport MRZ etc etc dependant on use case
- Supports multiple (256) key sets dependant on device request to card
  - i.e. there might be a “perimeter key set” and a “high security key set” and a “LACS key set” and an “administrative key set” etc etc and the terminal device only requests the one it requires, reducing the possibility of compromise of the others.
  - The key sets can be rolled, by loading spare unused key sets (up to 255) in case of compromise (memory is the limitation)
- Optionally provides session keys for higher level specs
- Protocol can be registered and implemented under ISO/IEC 24727-3 and 6, and either used under ISO/IEC 24727or implemented separately

But

- Slightly slower than existing physical access Tag and proprietary solutions (by 0.2 to 0.3 seconds)
- Keys MUST be distributed & managed
  - Vendors need to build key management for PLAID into existing or new key management systems. (Centrelink vendor is doing this for LACS)
  - PACS using older Weigand technologies need secure SAM devices in the readers
  - Newer PACS can utilise back end HSM devices/SAMs on the network or in distribution frames

PLAID 6 Protocol



Australian Government

Centrelink
giving you options

Example of same information freely available over interface with PLAID

System Sends to Card Green represents APDU (CLA, INS, P1, P2, P3)	Card Response Session encrypted - Note no repeat of data
Transaction #1 00A4040006 A000676D6166	**Transaction #1** 9000
808A072080	53B6AAF8573D504686338DC43C1CAF72D10C3CC5B3EFA85AA95A1115B28 AD861B4CDC908F0EBC08467E413603B261EB5440F4F4495EEF6FE4BC2A0 D3C4687E97F7F367342024F76E2D2DD0E94BF072FD1625E874184DA680E 9882F8823E3752ED906F95BF9932B5A394C9E64540FE390171A93596424 A7D7DD7E7FA4A4C56F999000
808C082040 57D1BEB0CC1E087FEC2D9F917822E45E275D508A87C98F758067427640C7 5810A4641C1FFB36C4722928739DEA1C9882BE0ACBC0DEC8FE25B152DAF3 EA3171F0	126AABF3184BF4ECE565CAD9AE5FDD1E0CC95D2ED12DBCA037981B20 58B1154B81A75EBBAE0A6141232EEBA3D7F5ACF3DA984081380E3E193F6 81A910077B98986D7069B122E23C4B64A8678B0F90C011D9E323FE838D5 D5E9309A54C7CAABA59000
Identical Transaction #2 00A4040006 A000676D6166	**Identical Transaction #2** 9000
808A072080	C15DDF6DA63E1A22F436E2A62C1AA4578AD6764AFE39BD8CD84A1323380 07743EB3C0663EA19805390DF3299F2F8E5EAA97939D63E5997DF886FD4 7FE9A667766CA35F4083BEF1F47383A704CF8B8FA58CE0CF5B573D141ED 2B4D3D0C35E97C3CCA8A3B095B5FA170E36ACD3E33B920E3E82E7712584 C43B45378DC0CA73BB849000
808C082040 8EA6F3AFCD8CECB9E2087F9808C653F8481AD0BBDE040224B5BB880D6D19 C82BC6C64B98E9D99AF6F609E429A48A0225323826ADD9229F8C12688C8B B28FD1CE	6C9B05C10E2A41075D3C52A1C7CEB496A9A005AA3ECDF58D9972D7E8 56932256D1A71A6B39A5962DEC8C98B69A7BE45FD413EA3CCEDA11CFE8A 8E2A6323580E03495701E8BF13C0F512B4BE7350FF8FFB5C49268CA8E9C F4C3B299CD406C0C3A9000

Note "9000" at the end of each smartcard response is the ISO7816 response for a successfully handled operation (not ID leakage)

Australian Government

Centrelink
giving you options

PLAID 6 Definitions

Object	Description
Key 1	1024/1984 bit Public/Private RSA key pair to protect initial comms from ID leakage. Card holds Public Key, Device holds private key
ISK	AES 256 bit Issuer Secret Key – Primary authentication key (the diversified version of this key is denoted by ISKDIV)
Diversification Data	8 bytes of random fixed data written to card at issuance
Diversification algorithm (DIV)	Diversifies symmetric master key to a unique key per card by algorithm = AES ISK (SHA [Diversification Data])
FASC-N/CSIC/ISO 7812	Up to 19 bytes of unique per card identification data
Weigand/Access Control #	Up to 8 bytes for use during transition from Weigand physical access control systems to FASN-N/CSIC/ISO 7812 based systems
PIN hash	Returned hash for verification of on card PIN by Access control system (or back office)
Usage Counter	Sequential counter so back office can identify brute force attempts
Short Name	Used to confirm identity and to facilitate friendly interfaces

PLAID 6 Field Lengths

Object	Length Bytes
Diversification Data	8
RND1	4
RND2	32
FASC-N/CSIC (or ISO 7812 card number)	19
Access Control # (Weigand String)	8
PIN Hash	20 (when using SHA1)
Usage counter	2
Short name	15

Other PLAID Issues

- The ATR/ATQ command on any protocol will cause any existing smartcard to leak ID by responding with a string including the fixed Card Serial Number
  - If we are very serious on ID leakage, then we need to consider requiring random or null serial numbers in response to ATR/ATQ
  - This would be a change to the ISO 7816 standard
- Anti-Collision for contactless cards provides for random UID under ISO 14443-3 – This option should be specified
- How to put IP into Public domain? We need to discuss licensing and standards mechanisms with NIST/US agencies
- Multiple peer reviews underway for both strength and operational practicality including Defence Signals Directorate
- Reference Apps & Prototypes in place for both Physical & Logical access
- Centrelink in process of proving in live operations and incorporating into Australian IMAGE framework
- Centrelink Key Mgmt is being built to support – Collaboration might be useful in this area

Centrelink Vision

- Centrelink wishes;
  - To transition out insecure or inconvenient or slow PACS/LACS products in favor of PLAID (or its derivative)
  - To source forward solutions from COTS product in PACS/LACS markets
  - In the very long term to manage employees authentication from a single point of management for PACS/LACS
    - This does not mean that AUTHORISATION is to a single management point
  - For the overall benefit of the Australian Government
- To achieve this we must;
  - Encourage other governments, agencies and commercial organizations to implement PLAID to create a competitive COTS market
  - Demonstrate how it is possible to transition to PLAID

Transition Strategy

- Wires in walls and distribution frames are the most labor intensive (therefore expensive) things to change
- Most PACS systems use 2 wires for 12 volt power, and 2 wires for Weigand signaling
- Existing door readers can be replaced by a low cost unit as demonstrated which supports both PLAID and the existing protocol, but sends Weigand numbers up the existing two wires. No need to touch wiring or distribution frames, and you use a SAM for key management.
- Once the existing cards are transitioned out, the readers old protocol support is switched off and useful Weigand numbers are no longer available to attackers.
- As systems become more sophisticated, or the building re-wired, the CAT6 interface on this demo unit supports native IP protocol and flash programming.
- With IP protocol support out to the doors, key management and PACS could be moved to a back office with a HSM, which could also be the LACS system
- The record used could be changed (on the fly) from Weigand to “whatever”
- As cards improve in speed, and all systems are on line or cached on-line, the protocol could be further simplified to use ECC with longer key lengths (5 years)

End

Thank You

Australian Government | Centrelink giving you options

The Technical Problem

- Both contact and contactless smartcard interfaces can be recorded up to the point where a secure session is set up
  - i.e. at least whilst the card is being bootstrapped into a secure session
- Secure sessions cause a large performance hit (reduce bandwidth to the card by 1/3 to 1/2)
- Any private or ID related data, or supporting data transferred between card and device is potentially exposed
- We call this “ID leakage”
- ID leakage can be used to create copies of smartcards, to allow session replay, to initiate a cryptographic attack, to capture private data, or even to initiate a physical attack in military scenarios (pot plant threat)

The Technical Problem – More

- In the case of both contactless smartcards and tags the ID leakage can occur at a range of up to 10 metres or via a hand held device at short range
- In the case of contact smartcards, Trojans can do the same thing on an insecure PC
- Smartcard have a generic method for solving this problem. Secure messaging is defined under ISO 7816-4
- But whilst highly secure - secure messaging is a very slow way to deal with the card, and has very poor performance. This is a problem for contactless cards where the card may be out of range before the session is even set up.
- Due to the above, most existing “tap & go” contactless access systems do not secure the ID record AT ALL, making it freely available for reading, and consequently also totally open for copying or cloning the card

Interesting Video Links

- http://events.ccc.de/congress/2007/Fahrplan/events/2378.en.html
  - Chaos communications event page – Initial Mifare Classic Hack
- http://www.youtube.com/watch?v=oj3V0rAqBG0
  - RSA Conference – Cloning door cards
- http://www.youtube.com/watch?v=NW3RGbQTLhE
  - Radboud University - Mifare classic algebraic breach in action against a building system
- http://www.youtube.com/watch?v=k7JDVOl4mSM
  - RC08 Rump 10, Nicolas Courtois, mifare classic, algebraic attack (also see att paper)
- http://www.youtube.com/watch?v=z7oPn7V5mHg
  - Defcon Weigand wire splice hack with Gecko – by far the easiest against most existing buildings
- http://www.youtube.com/watch?v=n9E-zDgARpE
  - Speedpass clone example
- http://www.youtube.com/watch?v=Srzf2MSCO6Y
  - Mifare Classic key vault breach
- http://www.youtube.com/watch?v=vmajlKJlT3U
  - Skimming EMV Cards for use in on-line transactions
- http://www.youtube.com/watch?v=mrRCgd6wh5Y&
  - Dutch Mifare classic transit card breach – In triple Dutch - but somewhat understandable