

# IAB Agenda

- **Opening Remarks** (*Tim Baldrige, NASA and Randy Vanderhoof, SCA*)
- **Insight on HSPD-12** (*Carol Bales, OMB*)
- **Identity Management Task Force Report** (*Duane Blackman, OSTP EOC*)
- **Federal Emergency Response Officials Linkage to HSPD-12** (*Craig Wilson Don Grant/Chris Geldart, FEMA*)
- **Electronic Submission of Fingerprints to OPM from GSA SSA Enrollment Infrastructure** (*Steve Duncan/David Temoshok, GSA*)
- **Briefing on PLAID (Protocol for Lightweight Authentication of Identity)** (*Terry Schwarzhoff/Graeme Freedman*)
- **HSPD-12 Select Agency Implementation Overview**
  - **GSA SSP Serving 70 Agencies** (*Mike Butler, GSA*)
  - **NASA** (*Tim Baldrige, NASA*)
- **Closing Remarks** (*Tim Baldrige, NASA*)

# PLAID

## Authentication Protocol

### Short 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

# 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 strict no de-badging policy. Contact cards are therefore not an option.
- Contactless needed for LACS, but COTS products not designed for tap-n-go
- Contactless needed for PACS, but COTS products beyond the end of their fit-for-purpose life cycle or not tap-n-go
- Needed to develop a solution for both LACS & PACS

# What is PLAID?

Protocol for Lightweight Authentication of IDentity (PLAID)

An authentication protocol suitable for PACS & LACS which uses **standards based** symmetric and asymmetric cryptography in a unique way to protect the communications between smartcard and terminal devices such that **strong mutual 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.

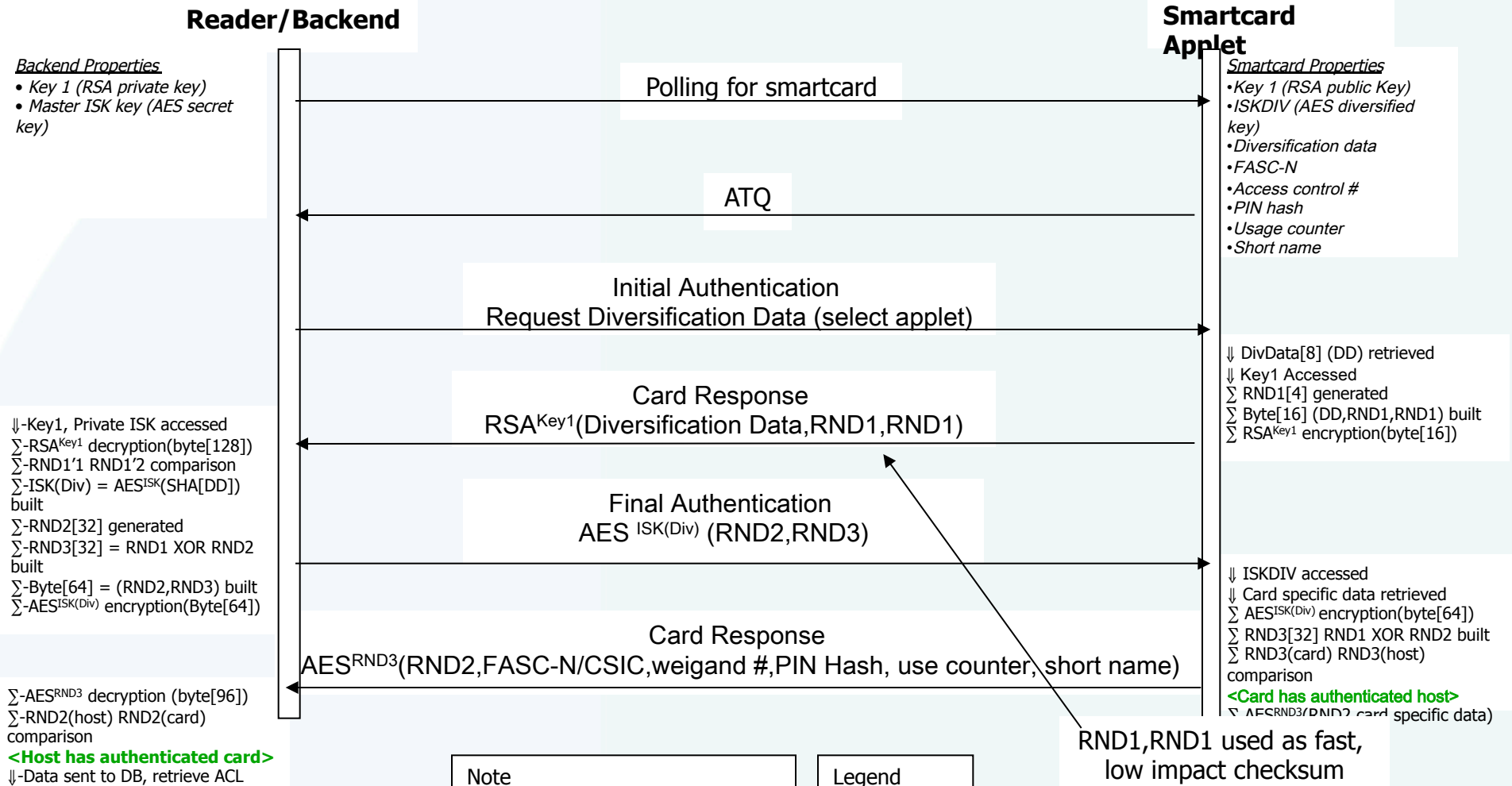
Centrelink has an all-of-government interest and responsibility in this technology space and intends to make the intellectual property developed by Centrelink freely available to other agencies, Governments and commercial organisations on an open, free and non-discriminatory basis.

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



# 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 24727 or 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

End

Thank You