

---

## **Fundamentals of Hardware Security Devices including the Queensland Smartcard Licence**

Tim Hudson – [tjh@cryptsoft.com](mailto:tjh@cryptsoft.com)  
Technical Director, Cryptsoft Pty Ltd

---

1

## Abstract

---

- ▶ The range of hardware based security devices just ready to solve every security problem you have and some you didn't even know you had is amazing.
  - ▶ There are open source security devices (both software and hardware), standalone battery powered personal security devices, directly host connected devices (USB, PCMCIA, PCI, SCSI), wireless security solutions, and a plethora of network attached security modules.
  - ▶ This presentation provides an overview the pros and cons of each general type of security device and the challenges you will face when integrating them into your existing environments.
- 

2

## Disclaimer

---

Any opinions expressed in this presentation represent the opinions of the presenter only.

No authorisation, endorsement or approval by any other party is implied unless explicitly stated.

The presenter does not speak on behalf of the Queensland Government Department of Transport and Main Roads or any other part of Queensland Government.

---

## Topics

---

- ▶ Authentication Options
  - ▶ Authentication Form Factors
  - ▶ Local Deployment Examples
  - ▶ Authentication Standards
  - ▶ Application Program Interfaces
  - ▶ Architectural Integration Options
  - ▶ Queensland Smartcard Licence
-

## Security Focus

---



---

5

## Authentication Options

---

- ▶ Implicit
  - ▶ Username + Password
  - ▶ Hardware Token
  - ▶ One-factor
  - ▶ Two-factor
  - ▶ Biometrics
  
  - ▶ One-way / Challenge-Response
  - ▶ Connected / disconnected
  - ▶ Contact / contactless
- 

6

# Authentication Options

## One-time Password Authentication

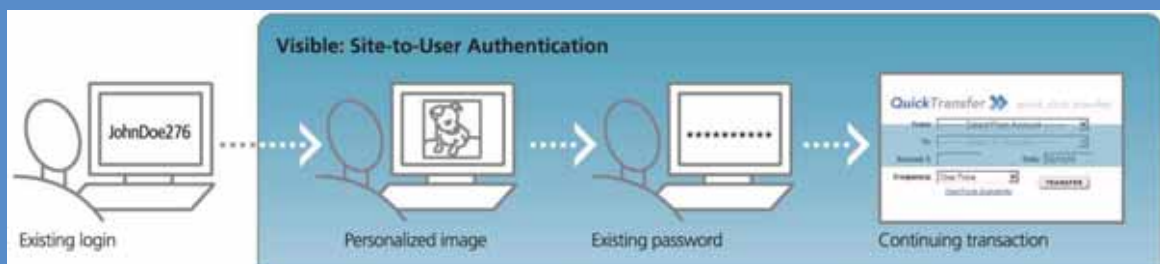


Source: [www.rsasecurity.com](http://www.rsasecurity.com)

7

# Authentication Options

## Site-to-User Authentication

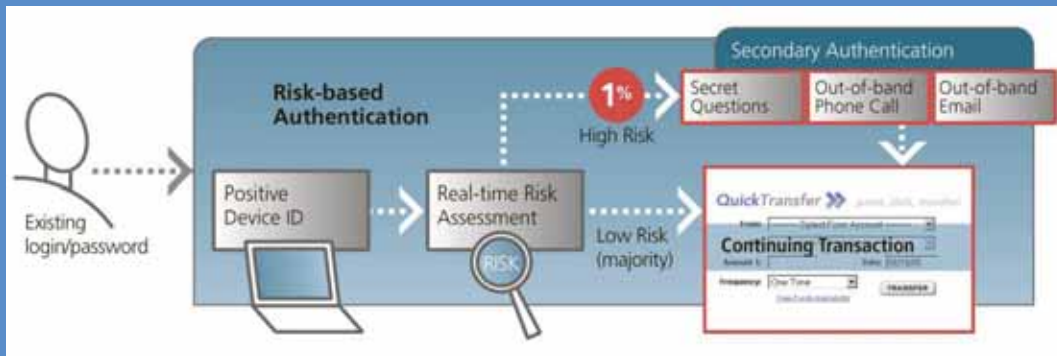


Source: [www.rsasecurity.com](http://www.rsasecurity.com)

8

# Authentication Options

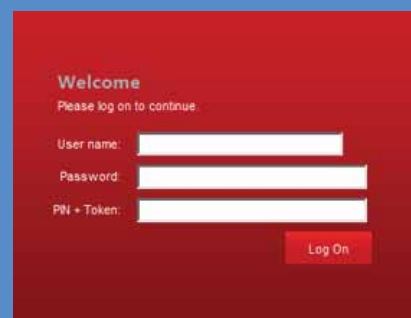
## Risk Based Authentication



Source: [www.rsasecurity.com](http://www.rsasecurity.com)

# Authentication Options

## One-time Password Authentication



Source: various including [www.mi-token.com](http://www.mi-token.com) and [www.rohos.com](http://www.rohos.com)

# Authentication Form Factors

- ▶ Personal non-connected Token
- ▶ Personal connected portable Token (USB, PCMCIA, smartcard)
- ▶ Non-portable Token (SCSI, PCI)
- ▶ Network attached Hardware Security Modules

11

# Authentication Form Factors

RSA, the Security Division of EMC



RSA SecurID DS1000



RSA SecurID DS2000



RSA SecurID DS6000



RSA SecurID DS7000



RSA SecurID DS8000  
RSA SecurID DS9000 token



Source: [www.rsasecurity.com](http://www.rsasecurity.com)

12

# Authentication Form Factors

## Mi-Token



Android



Blackberry



iPhone



Java



Windows Mobile



# Authentication Form Factors

## Vasco



# Authentication Form Factors

## CRYPTOCARD

### SecureHQ CRYPTOCard Token Overview



KT-1



KT-2



KT-3



RB-1



SC-1



SC-3

## PINPAD Devices



# PCI and PCMCIA Authentication Devices



IBM4764-XCP



IBM4758



IBM4758



IBM4765-PCle



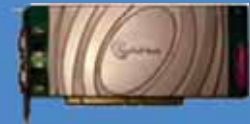
SafeNet Luna-PCI



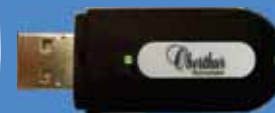
Thales / nCipher



Sun-CA-6000



# USB Authentication Devices





## Readers – RFID and NFC

---



---

21

## USB HSMs

---



---

22

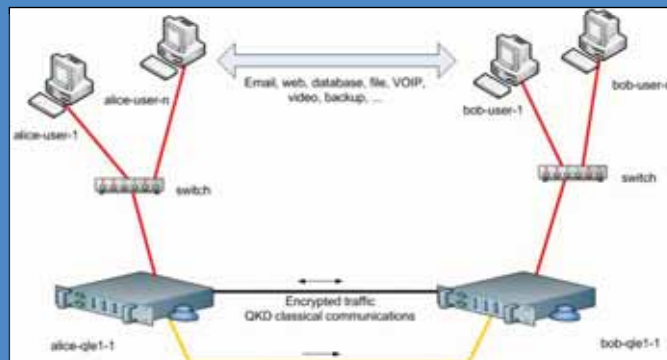
# Network Attached



SafeNet Luna SA



# Network Attached



## Inside Security Devices

---

- ▶ Are these devices secure?
  - ▶ Ignore vendor claims – making marketing claims are easy
  - ▶ Require independent verification- FIPS 140, CC
- ▶ Are all devices essentially the same?
  - ▶ What is actually inside
- ▶ Don't rely entirely on the device
  - ▶ Plan for failure of the security controls
  - ▶ Where appropriate include overlapping controls
  - ▶ Plan for failure of the overlapping controls

---

25

## Inside Security Devices

---



---

26

# Inside Security Devices

---



27

# Inside Security Devices

---



28

# Inside Security Devices

---



# Inside Security Devices

---

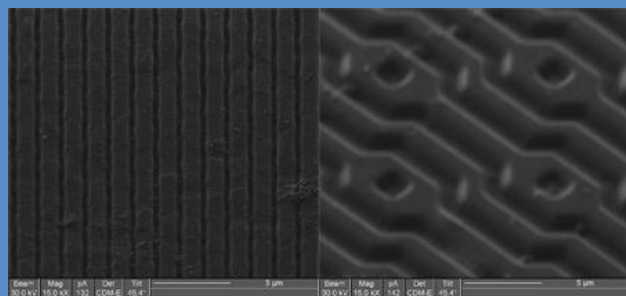
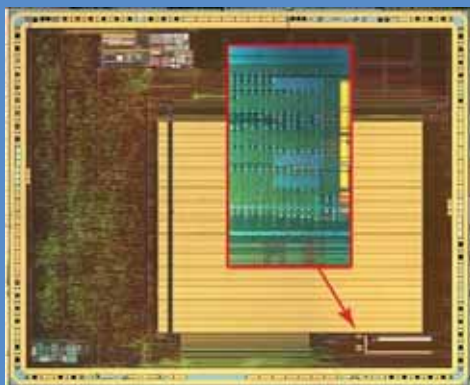


# Inside Security Devices



31

# Inside Security Devices



32

# Comparison

---

## ▶ Standalone tokens

### ▶ Positives

- ▶ No end-user software integration as the human is the communication device
- ▶ Simple to explain; widely used – familiar concept
- ▶ Mature technology
- ▶ Can be used over the phone – it does not require a computer
- ▶ Doesn't require trusting the users platform

### ▶ Negatives

- ▶ Battery runs out so have to regularly re-purchase (expensive)
  - ▶ Using the human as the connection to the device limits the amount of information that can be transferred
  - ▶ Huge variability between vendors in their engineering approach
  - ▶ Relying on security vendor to keep the 'secret' actually secret
- 

33

# Comparison

---

## ▶ USB attached tokens

### ▶ Positives

- ▶ Simple to explain; widely used – familiar concept
- ▶ Lots of vendor products to choose from
- ▶ Keyboard devices can make-like-the-human and directly enter the information
- ▶ Can be high-performance though often are not

### ▶ Negatives

- ▶ Cannot use without a computer
  - ▶ Often will require software installed on the target machine
  - ▶ Often just a smartcard 'dressed up'
  - ▶ Lots of vendor products to choose from
  - ▶ Often not supported in a virtualised environment
- 

34

# Comparison

---

## ▶ Smartcard - Contact

### ▶ Positives

- ▶ Simple to explain; widely used – familiar concept
- ▶ Can potentially load your own code into a “secure environment”
- ▶ Lots of vendor products to choose from

### ▶ Negatives

- ▶ Requires a reader
  - ▶ Requires software installed on the target machine
  - ▶ Often entangled with a complicated PKI rollout
  - ▶ Lots of vendor products to choose from
  - ▶ Very low performance
- 

# Comparison

---

## ▶ Smartcard or other Contactless

### ▶ Positives

- ▶ Simple to explain; widely used – familiar concept
- ▶ Lots of vendor products to choose from
- ▶ No issues with wear and tear on contacts
- ▶ Reduced heat or moisture issues

### ▶ Negatives

- ▶ Requires a wireless reader
  - ▶ Often will require software installed on the target machine
  - ▶ Often just a simple clone able ID
  - ▶ Lots of vendor products to choose from
  - ▶ Very low performance
-

# Comparison

---

## ▶ Phones and PDAs

### ▶ Positives

- ▶ Lots of vendor products to choose from
- ▶ Effectively adding software to an existing device so 'hardware' costs are zero making for a cheaper solution to deploy as the user has already paid the hardware cost

### ▶ Negatives

- ▶ Lots of vendor products to choose from
  - ▶ Lots of different phone operating systems, devices
  - ▶ Requires software installed on the target device
  - ▶ It is just another platform on which software can be installed so it is a software based solution (generally)
  - ▶ Substantially easier to 'attack'
- 

# Comparison

---

## ▶ PCI

### ▶ Positives

- ▶ Physically connected
- ▶ Substantially more functionality (in general)
- ▶ Typically high-performance

### ▶ Negatives

- ▶ Requires platform specific drivers
  - ▶ Does not work in a virtualised environment
  - ▶ Often has limited (or no) on-board storage
  - ▶ Generally more expensive
-

## Comparison

---

- ▶ Network attached
    - ▶ Positives
      - ▶ Able to be located 'anywhere'
      - ▶ Substantially more functionality
      - ▶ Typically high-performance
      - ▶ If vendor uses standard protocol does not require platform specific drivers or can be supported on any platform the vendor chooses to 'port' their client-side software to
        - E.g. OASIS Key Management Interoperability Protocol (KMIP)
      - ▶ Blinking lights
    - ▶ Negatives
      - ▶ Substantially more expensive
      - ▶ Not feasible as an end-user device
- 

39

## Comparison

---

- ▶ Every security device has positives and negatives
  - ▶ Which device is suitable for your specific problem requires a more detailed analysis
  - ▶ Often more than one type of device is the 'right' answer
- 

40

# Security Toolbox

---



---

41

# Local Deployment Examples

---

- ▶ Australian Banks
  - ▶ Consumer Security Tokens
  - ▶ Business Security Tokens
- ▶ Queensland Government Smartcard Licence

---

42

# Australian Organisations

## ▶ RSA Tokens



Westpac



Suncorp Metway



ANZ Bank

## ▶ Vasco Tokens



Bank of Queensland



Teachers Credit Union



Commonwealth Bank



# Queensland Smartcard Licence



## Local Deployment Examples

---

- ▶ Banks - Nationally
  - ▶ Unknown challenge response tokens
  - ▶ 100,000+ LCD-based security tokens
  - ▶ 1,000,000+ SMS-based authentication
- ▶ Queensland Government
  - ▶ 20,000+ LCD-based security tokens (estimate)
  - ▶ 15,000+ smartcards (estimate)
  - ▶ 20,000+ ISO/IEC 24727 smartcards
    - ▶ Will go to approximately 3.5 million over the next five years

## Next Steps

---

- ▶ What do you have to do to “get some security”
- ▶ The strategy some folks seem to use:
  - ▶ Pick a vendor at random
  - ▶ Pick a device from the vendor at random
  - ▶ Integrate device into your environment
    - a) Pick pre-integrated products
    - b) Pay the vendor to integrate
    - c) **Pay a consultant to integrate**
    - d) Integrate yourself

## Next Steps

---

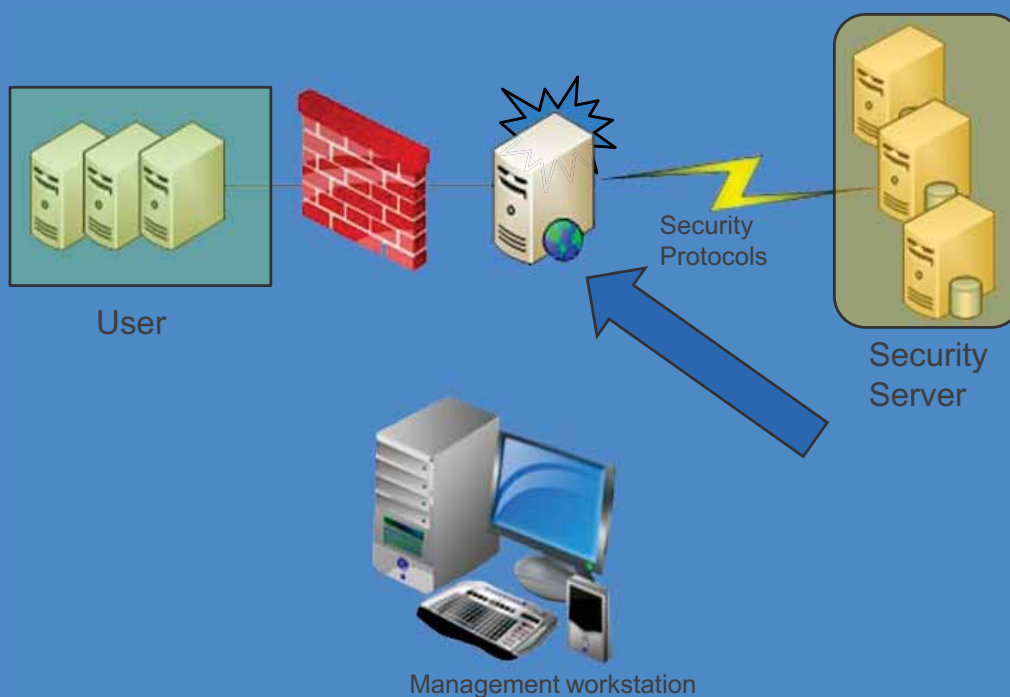
- ▶ If integrating yourself
  - ▶ You've got the token/smartcard/device
  - ▶ How do you get the yes/no answer
  - ▶ Where do you integrate
  - ▶ How do you determine if you've "got some security"

---

48

## Generic Architecture

---



---

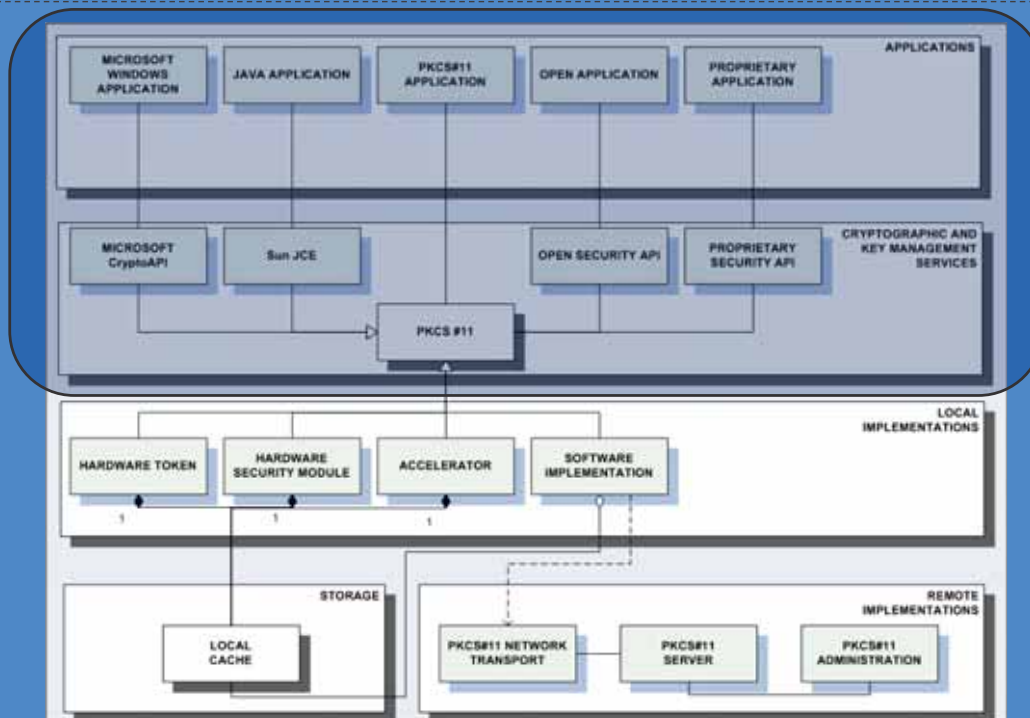
49

# Authentication Standards

- ▶ Challenge Response Authentication Protocol (CHAP, MS-CHAP)
- ▶ Password Authentication Protocol (PAP)
- ▶ Extensible Authentication Protocol (EAP)
- ▶ HTTP Basic Access Authentication / Digest Authentication
- ▶ Kerberos
- ▶ Security Assertion Markup Language (SAML)
- ▶ Simple Authentication and Security Layer (SASL)
- ▶ S/KEY
- ▶ Secure Sockets Layer (SSL) / Transport Layer Security (TLS)
- ▶ Web Services Security (WSS)
- ▶ RADIUS, LDAP, KMIP, etc

50

# Application Programming Interfaces



51

## Application Program Interfaces

---

- ▶ PKCS#11 Cryptographic Token Interface (Cryptoki)
  - ▶ Microsoft CryptoAPI (CAPI)
  - ▶ Sun Java (JCE, JKS, JSSE)
  - ▶ Generic Security Services API (GSS-API)
  - ▶ Open Source (OpenSSL, Cryptlib, Crypto++, NSS)
  - ▶ PC/SC
  - ▶ ISO/IEC 7816 (APDUs)
  - ▶ ISO/IEC 24727
  - ▶ Vendor specific proprietary APIs
- 

52

## Authentication Standards

---

- ▶ OATH
  - ▶ <http://www.openauthentication.org/> [url]
  - ▶ Initially primarily backed by Verisign
  - ▶ Many vendors now provide physical tokens
  - ▶ Does not specify a full system



54

# Authentication Standards

---

- ▶ Challenge Response Authentication Protocol (CHAP)
  - ▶ RFC1334, RFC1994
    - ▶ Widely used in dial-up services
- ▶ Extensible Authentication Protocol (EAP)
  - ▶ RFC3748
    - ▶ Widely used to negotiate authentication protocol between dial-up client and server or client-server authentication
- ▶ Generic Security Services API (GSS-API)
  - ▶ RFC1508
    - ▶ Generic security services specification. Typically further defined in other protocols built on top of this generic framework.

# Authentication Standards

---

- ▶ HTTP Basic Access Authentication
  - ▶ RFC2616
    - ▶ Username + password. Typically used in combination with SSL/TLS (aka HTTPS)
- ▶ Kerberos
  - ▶ RFC1510
    - ▶ Network authentication protocol. Used in Microsoft Windows 2000 and above.
- ▶ Microsoft Challenge Handshake Authentication Protocol
  - ▶ MS-CHAP v1 – RFC2433
  - ▶ MS-CHAP v2 – RFC2759
    - ▶ CHAP dialects as Microsoft extensions. Used for remote workstation support.

# Authentication Standards

---

- ▶ Password Authentication Protocol (PAP)
  - ▶ RFC1334, RFC1994
    - ▶ Older PPP/SLIP protocol with passwords in clear text.
- ▶ Security Assertion Markup Language (SAML)
  - ▶ OASIS-SAML
    - ▶ Defines XML based security assertions and profiles for exchanging messages and transport bindings.
- ▶ Simple Authentication and Security Layer (SASL)
  - ▶ RFC2222
    - ▶ Method for adding authentication to communication protocols

---

57

# Authentication Standards

---

- ▶ S/KEY
  - ▶ RFC1760, RFC2289
    - ▶ One time password system based on hashing.
- ▶ Secure Sockets Layer (SSL) /  
Transport Layer Security (TLS)
  - ▶ RFC2246
    - ▶ Security protocol supported in web browsers and web services with support for public key infrastructure and one party or mutual authentication.
- ▶ Web Services Security (WSS)
  - ▶ OASIS-WSS
    - ▶ Enhancements to base SOAP messaging to support security via message integrity, confidentiality, and authentication. Supports tokens.

---

58

## Application Programming Interfaces

---

- ▶ PKCS#11 Cryptographic Token Interface (Cryptoki)
  - ▶ PKCS#11 extensions for OTP defined
- ▶ Microsoft CryptoAPI (CAPI)
  - ▶ CryptoAPI extensions for OTP defined
- ▶ Availability of standard interfaces from multiple vendors remains a problem in some areas with interoperability. As with any technology, actual testing of vendor devices is required.

## Application Programming Interfaces

---

- ▶ Smartcard Level Interfaces
- ▶ ISO/IEC 7816
  - ▶ EMV, GSM, PC/SC, OCF
    - ▶ Open Platform
    - ▶ Common Access Card
  - ▶ APDU command sets documented by vendors
  - ▶ APDU command sets and data format standardised in various contexts
- ▶ ISO/IEC 18013 – Electronic Driving License
  - ▶ Freely available implementations
  - ▶ Commercial implementations
- ▶ NIST Personal Identity Verification (PIV) + FIPS201

# Application Programming Interfaces

---

## ▶ ISO/IEC 24727

- ▶ Framework for a large range of possible realisations
- ▶ Can be simply a middleware interface (no defined API)
- ▶ Only one deployment of ICC resident stack so far

## ISO/IEC 24727 Part 2

“This part of ISO/IEC 24727 maximizes the fungibility of independent realizations of its prescriptions.”

## ISO/IEC 24727 Part 5

5656 pages

---

## Next Steps

---

- ▶ How do you determine if you’ve “got some security”
    - ▶ What is the threat
    - ▶ Detect Bad Things
    - ▶ Prevent Bad Things
-

## Security Objectives

---

- ▶ Document the threat posed by the attacker
    - ▶ What do they want
    - ▶ What can they get if they defeat the 'security'
    - ▶ What is the worth to the attacker
    - ▶ What is it worth to the issuing organisation
  - ▶ Ensure that the security mechanisms are targeted
    - ▶ **If you cannot elaborate the threat then you have no means to determine if you've successfully defended against that threat**
  - ▶ Ensure that the security mechanisms overlap
- 

65

## Security Objectives

---

- ▶ Make it hard for the attacker to "impersonate"
    - ▶ Provide proof of authenticity
      - ▶ Prevent cloning
      - ▶ Prevent impersonation
    - ▶ Provide a range of mechanisms that those performing the checks can use
      - ▶ Requires knowledge of the security mechanisms
      - ▶ Anything not known cannot be used in a front-line fraud check
    - ▶ Provide layered mechanisms
    - ▶ Provide detection
- 

66

## Security Approaches

---

- ▶ Require physical presence at a known location
  - ▶ Secure the premises with 'traditional approaches'
- ▶ Require physical action
  - ▶ Preclude software 'automating away' the security controls
- ▶ Require multiple participants
  - ▶ Use the participants checks on each other as a supplemental control
  - ▶ Require subversion of multiple participants in order to 'defeat' the security of the system

---

67

## A concrete example

---

- ▶ In order to sign a certification authority certificate
  - ▶ Separate participant required for 'computer room' entry
  - ▶ Two participants required for 'ceremony room' entry
  - ▶ Separate participant required to perform system login
  - ▶ Separate participant required to perform application login
  - ▶ Three out of five participants required to present physical security tokens
- ▶ Electronic locks with audit records
- ▶ Paper sign in records
- ▶ System activity audit records
- ▶ Independent HSM signed audit records

---

68

## A simple example

---

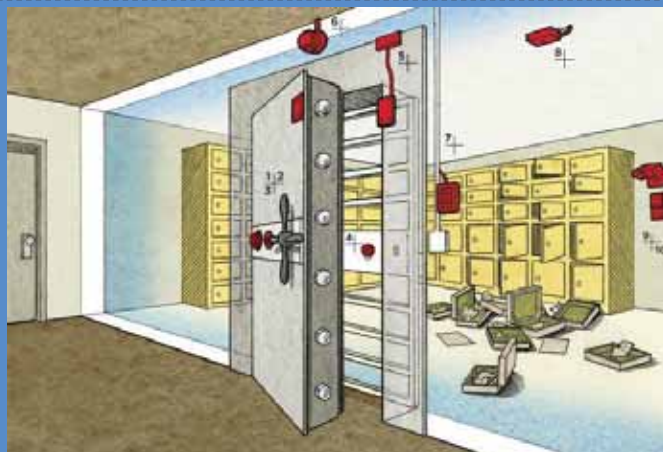


69

Source: [www.wired.com](http://www.wired.com)

## A simple example

---



### The Door

1. Combination dial (0-99)
2. Keyed lock
3. Seismic sensor (built-in)
4. Locked steel grate
5. Magnetic sensor
6. External security camera

### The Vault

7. Keypad for disarming sensors
8. Light sensor
9. Internal security camera
10. Heat/motion sensor

70

Source: [www.wired.com](http://www.wired.com)

## Another example

---



## Queensland Smartcard Licence

---

- ▶ Originally Digital License Project (1999-2002)
- ▶ Renamed New Queensland Driver Licence (NQDL)
- ▶ NQDL named and smartcard technology selected (2002-2003)
- ▶ NQDL launched late 2003 for release in Oct 2006
- ▶ SLIP launched (April 2004)
- ▶ PPP EOI (August 2006), PPP Binding Bid (April 2007)
- ▶ PPP Withdrawn (Late 2007)
- ▶ NQDL RFOs (Late 2007 to Mid 2008)
- ▶ SLIP MoU signed (November 2008)
- ▶ Official staff trials (Aug 2010)
- ▶ Official launch (late 2010)
- ▶ Rollout to TMR CSC (during 2011)

## Queensland Smartcard Licence

- ▶ *“Approximately a quarter of Queensland businesses request the driver licence of consumers or employees, to substantiate driving authority, identity, address and age.”*
- ▶ *“Firstly, a Smartcard is significantly harder to duplicate, falsify or counterfeit than a laminate licence.”*
- ▶ *“Secondly, Public Key Infrastructure (PKI) will also enable a Smartcard licence to ‘self-authenticate’, confirming it is a genuine licence and not a reproduction.”*
- ▶ *“Thirdly, Smartcard licensing systems offer driver licensing authorities the potential to bind the holder more closely to their credential and prevent unauthorised use of the card. This may involve ... a personal identification number (PIN) ...”*

## Licence Fraud Statistics

Description	2007	2008	2009	Schoolies 2009
<b>Suspected fraudulently obtained Qld driver licences and Cards 18+</b>	<b>15</b>	<b>14</b>	<b>10</b>	<b>5</b>
Altered Qld driver licences and Cards 18+	34	11	7	2
False Qld driver licences and Cards 18+	21	15	42	0
Altered interstate driver licences	N/A	N/A	N/A	31

# Queensland Smartcard Licence

## ▶ “Key Security Features

- ▶ Digital photo and signature
- ▶ Computer chip that securely stores product and personal information
- ▶ Public Key Infrastructure (PKI) stored on the card’s chip
- ▶ A variety of overt and covert visual and technological security features, such as holograms and special inks
- ▶ Personal Identification Number (PIN) – a security feature to help prevent unauthorised use of your card and to allow you to transact with Transport and Main Roads in the future
- ▶ Shared secrets – answers to two questions from a list of security questions that will allow you to transact online with Transport and Main Roads in the future.”

# Shared Secrets



## Queensland Smartcard Licence

---

- ▶ *Smartcard Licence Interoperability Protocol (SLIP)*
  - ▶ *“The SLIP specifies data and technology platforms for Smartcard Licences, and was prepared in contemplation that one or more Australian licensing authorities implement Smartcards in their jurisdictions. Adopting this standard will ensure national interoperability, deliver infrastructure savings and save time and money. **It will also provide flexibility in government purchasing and avoid the pitfalls of vendor-specific proprietary standards that are not interoperable.** National and state/territory Transport Ministers ratified SLIP at the Australian Transport Council in November 2008.”*

## Queensland Smartcard Licence

---

- ▶ *Electronic Service Delivery*
  - ▶ *“The Australian Government Authentication Framework ... dictates that two-factor authentication is required for many medium and high risk transactions ...”*
  - ▶ *“Smartcard licensing systems offer strong authentication, opening up the possibility for government services on-line. This is not limited to licensing and registration services ... but could include other services within and across governments.”*
  - ▶ *“Smartcard licences could also be used to validate identity in on-line commercial transactions.”*
  - ▶ *“Licence holders could potentially use their PIN to allow access to information on their licence when transaction with a merchant with a Smartcard reader.”*

# Driver License – Front



79

# Driver License – Back



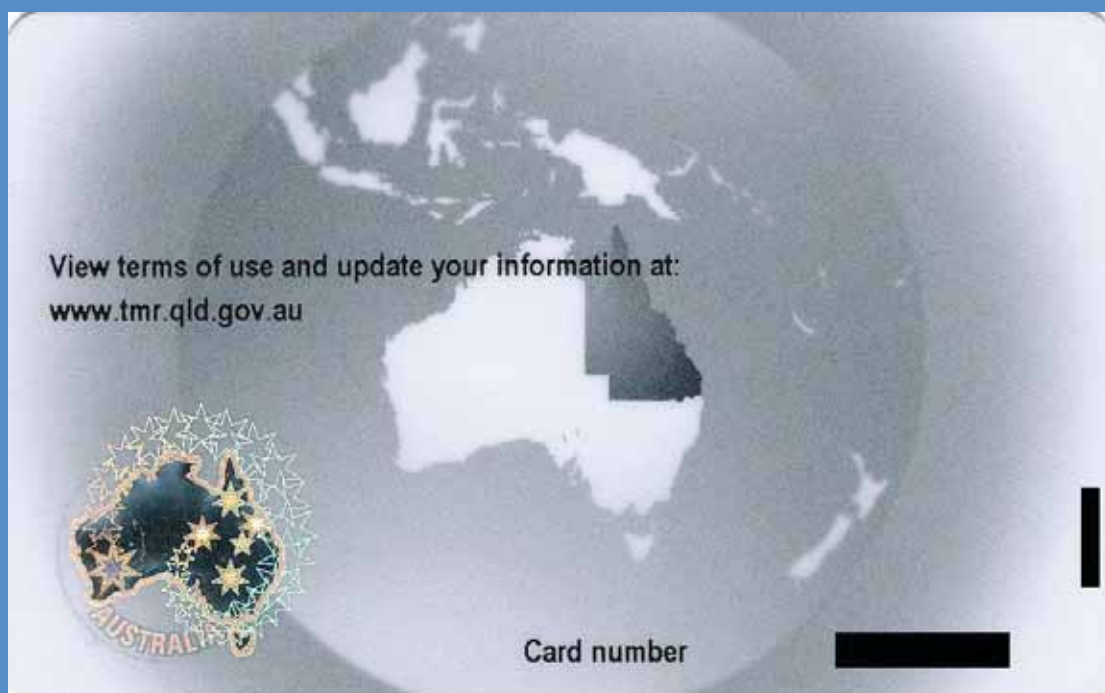
80

## Adult Proof of Age – Front



81

## Adult Proof of Age – Back



82

# Driver Licence

**Driver Licence** LICENCE NO. **123 456 789**

**CITIZEN**  
JOHN ANDREW

DOB **28 Aug 1867** Sex **M**  
Height **180**

Class	Type	Effective	Expiry
<b>C</b>	<b>P2</b>	<b>01.08.10</b>	<b>02.06.11</b>
<b>C</b>	<b>O</b>	<b>02.06.11</b>	<b>02.06.21</b>

Conditions **I,X1**

Queensland, Australia Drive safely  **Queensland Government**



# Heavy Vehicle Driver Licence

**Heavy Vehicle Driver Licence** LICENCE NO. **123 456 789**

**CITIZEN**  
JOHN ANDREW

DOB **28 Aug 1867** Sex **M**  
Height **180**

Class	Type	Effective	Expiry
<b>C</b>	<b>P2</b>	<b>01.08.10</b>	<b>02.06.11</b>
<b>C</b>	<b>O</b>	<b>01.06.10</b>	<b>02.06.11</b>

Conditions **1,X1**

Queensland, Australia Drive safely  **Queensland Government**



# Marine Licence Indicator

**Marine Licence Indicator**



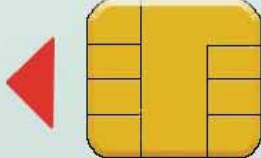
**LICENCE NO. 123 456 789**

**CITIZEN**  
JOHN ANDREW


DOB **28 Aug 1867** Sex **M**  
Height **180**

Type **PWCL** Effective **01.08.10**  
**RMDL** **01.08.10**

Conditions **Y**  
Card Expiry **01.08.20**



Queensland, Australia



**Queensland Government**

# Adult Proof of Age



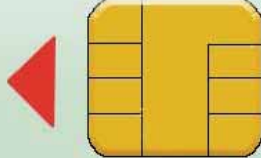
**Adult Proof of Age Card**

**REFERENCE NO. 123 456 789**


**CITIZEN**  
JOHN ANDREW

DOB **28 Aug 1867** Sex **M**

Card Expiry **01.08.20**



Queensland, Australia



**Queensland Government**

# Industry Authority

## Industry Authority

**AUTHORITY NO.**  
**123 456 789**

**CITIZEN**  
JOHN ANDREW



Queensland, Australia

Authority Type	Cond	Expiry
Taxi/Limo/Genr/Sche/TrMc	Y	11.12.10
Dangerous Goods Driver	Y	11.12.10
Driver and Rider Trainer	Y	11.12.10
Escort Vehicle Driver	Y	11.12.10
Tow Truck Driver	Y	11.12.10
Traffic Controller	Y	11.12.10



Queensland Government

87

Source: [www.qscid.com](http://www.qscid.com)

## What can you do with the smart cards

- ▶ Everything you can do with the existing laminated card

89

# What is on the smartcard?

The screenshot shows the QSCID Viewer application with the 'Data' tab selected. The interface is divided into several sections:

- Card Identifier:** IIN 90360078, CIN 1122AA3366
- Card Information:** ID 11223344556677, Issue 20100801, CIN 1122AA3366, Expiry 20200801
- Issuer:** IIN 90360078, Country AUS, Authority, State QLD, Department of Transport and Main Roads
- Card Holder Information:** NR 123456789, ID 11223344556677, Family Name CITIZEN, Given Name JOHN ANDREW, DOB 18670828, Sex M, Height 180, Enrolling Authority Queensland Government Department of Transport and Main Roads
- User Credentials:** PIN (masked), Password, Shared Secret 1 (Question/Answer), Shared Secret 2 (Question/Answer)
- Address Information:** Road 1234, SOMewhere, ST, Locality BRISBANE, State QLD, PostCode 4000, Country AUS

Buttons at the bottom include ID, CARDINFO, CHINFO, ADDRESS, PIN, TEST, ALL, and RESET.

90

Source: www.qscid.com

# What about ISO/IEC 24727?

The screenshot shows the QSCID Viewer application with the 'Discovery' tab selected. The interface displays a tree view of card data on the left and a detailed view of the selected data on the right.

**Tree View (Left):**

- E82881C11702
  - 1F
  - 20
  - 24
  - 25
  - 26
  - 30
  - 31
  - 32
  - 33
  - 3A
  - 52
  - 53
  - 5A
  - 5B
  - 5C
  - 5D
  - 6H
  - CCD
    - CCD
    - CurDate
    - CurDate
    - Version
    - Version
    - CardInfo
    - CardInfo

**Selected Data (Right):**

- 1F
  - protocol=1.1.24727.6.8 (SECURE\_PIN)
  - scope=1 (global)
  - authenticated=False
  - marker
    - SEQUENCE 0x10 (0x10 - 16)
      - [1] (0x01 - 1) 03
      - [2] (0x01 - 1) 00
      - [3] (0x08 - 8)
        - [0] (0x02 - 2)
          - [1] (0x02 - 2) '33' 33:33
  - Version.Version
    - SEQUENCE 0x10 (0x49 - 73)
      - SEQUENCE 0x10 (0x23 - 35)
        - [0] (0x04 - 4) 'SLIP' 53:4C:49:50
        - [1] (0x01 - 1) 01
        - [2] (0x18 - 24) 'www.tmr.qld.gov.au/cards' 77:77:77:2E:74
      - SEQUENCE 0x10 (0x22 - 34)
        - [0] (0x03 - 3) 'TMR' 54:4D:52
        - [1] (0x01 - 1) 01
        - [2] (0x18 - 24) 'www.tmr.qld.gov.au/cards' 77:77:77:2E:74

Buttons at the bottom include Discover, Clear, Expand, Collapse, and RESET.

91

Source: www.qscid.com

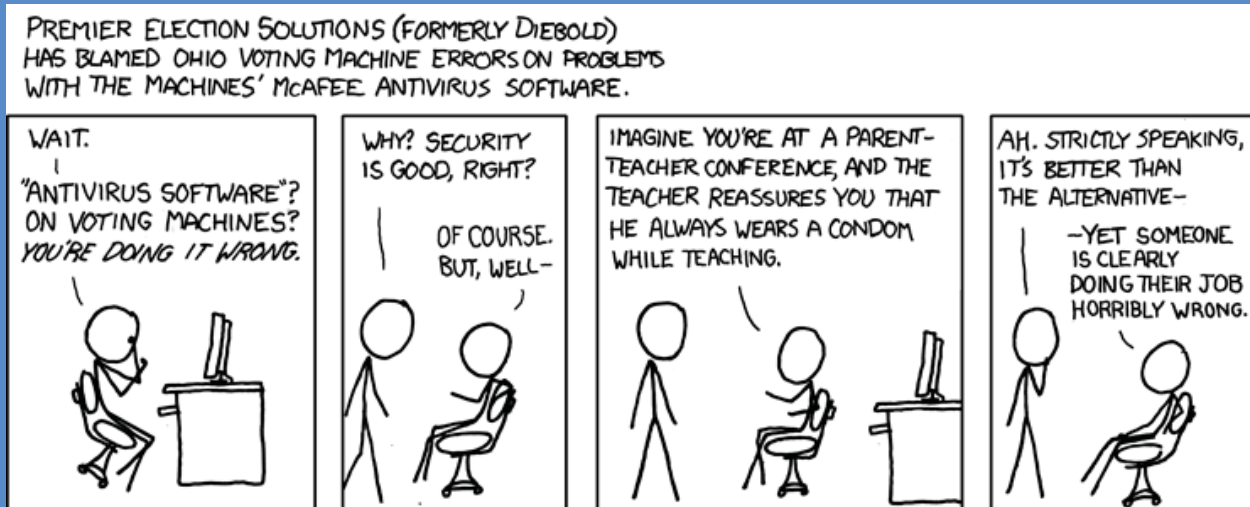
# What can you display?



92

Source: [www.qscid.com](http://www.qscid.com)

# Don't forget the real world context



Creative Commons Attribution-NonCommercial 2.5 License



93

Source: [http://imgs.xkcd.com/comics/voting\\_machines.png](http://imgs.xkcd.com/comics/voting_machines.png)

## Interoperability

---

- ▶ *“A common approach to ISO/IEC 24727 by SLIP and the NSF provides governments with an ‘open architecture’ that is non-proprietary and independent of particular vendors. This enables access to a global market with more suppliers, more competition and lower procurement costs.”*

Smartcard Licence Interoperability Protocol (SLIP) SLIP overview

## Interoperability

---

- ▶ Number of implementations of ISO/IEC 24272 with ICC Resident Stack and Department of Transport and Main Roads defined security protocols:

**2**

- ▶ Number of applications available to Queensland residents and businesses that can interface to the issued smart cards:

**1**

- ▶ Number of major security companies or smartcard technology providers supporting ISO/IEC 24272 with ICC Resident Stack and Department of Transport and Main Roads defined security protocols:

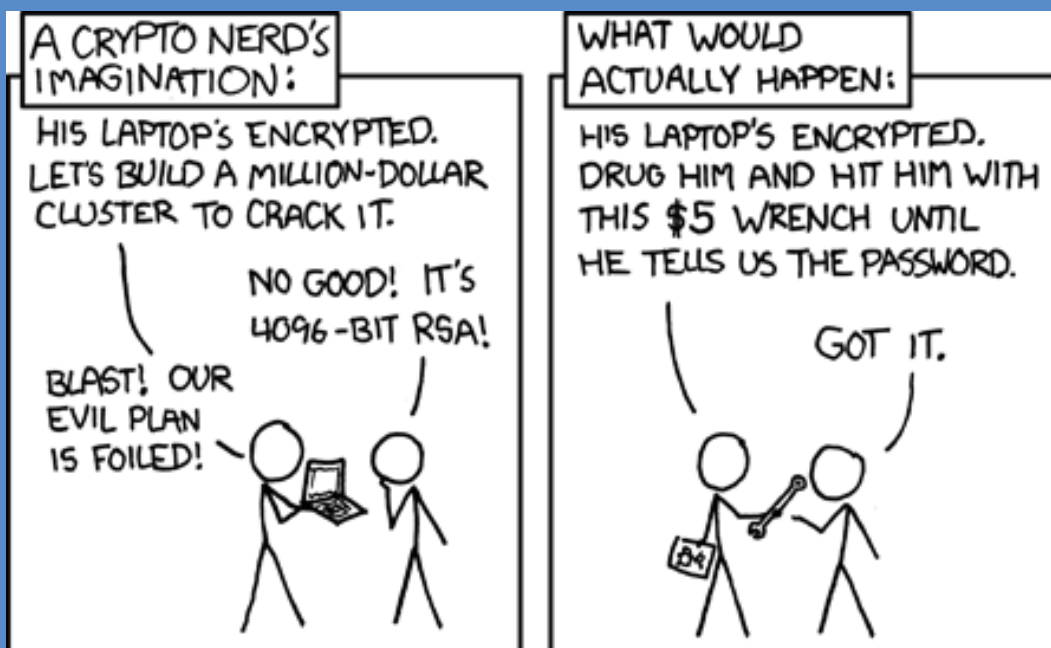
**0**

# Checking the new smartcards



96

# Don't forget the real world context



Creative Commons Attribution-NonCommercial 2.5 License



97

Source: <http://imgs.xkcd.com/comics/security.png>

## Survey

---

### ▶ Queensland Smartcard Licence

- ▶ 1) Have you experienced fraud with the Driver Licence
    - ▶ A) Never
    - ▶ B) Occasionally
    - ▶ C) Frequently
  - ▶ 2) Will you use the new smartcard
    - ▶ A) Yes
    - ▶ B) Maybe
    - ▶ C) Never
  - ▶ 3) Have you heard of ISO/IEC 24727
    - ▶ A) No
    - ▶ B) Only from the department
    - ▶ C) Yes
- 

## Survey

---

### ▶ Queensland Smartcard Licence

- ▶ 4) Your plans for future Smartcard usage
    - ▶ A) Plan to migrate to ISO/IEC 24727
    - ▶ B) No interest in ISO/IEC 24727
    - ▶ C) No plans to ever use any smartcards
  - ▶ 5) Your view on Qld Government issued smartcards
    - ▶ A) Good idea
    - ▶ B) Bad idea
    - ▶ C) Undecided
  - ▶ 6) Do you feel informed about the new smartcards
    - ▶ A) Yes - I know everything I need to know
    - ▶ B) No – I want more information
    - ▶ C) No – And I don't want to know
-

# Questions

---

Any questions?

Tim Hudson  
Cryptsoft Pty Ltd  
tjh@cryptsoft.com  
<http://www.cryptsoft.com/>

