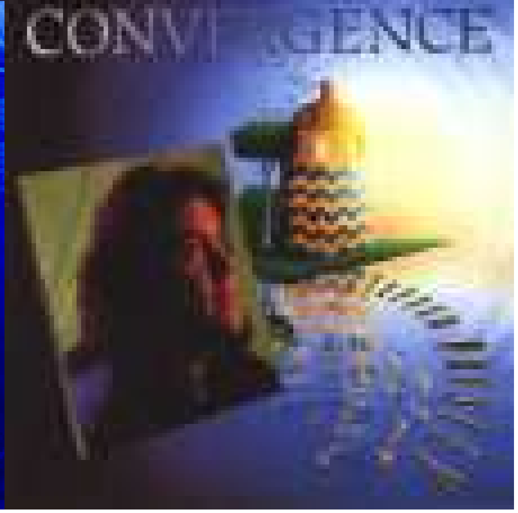
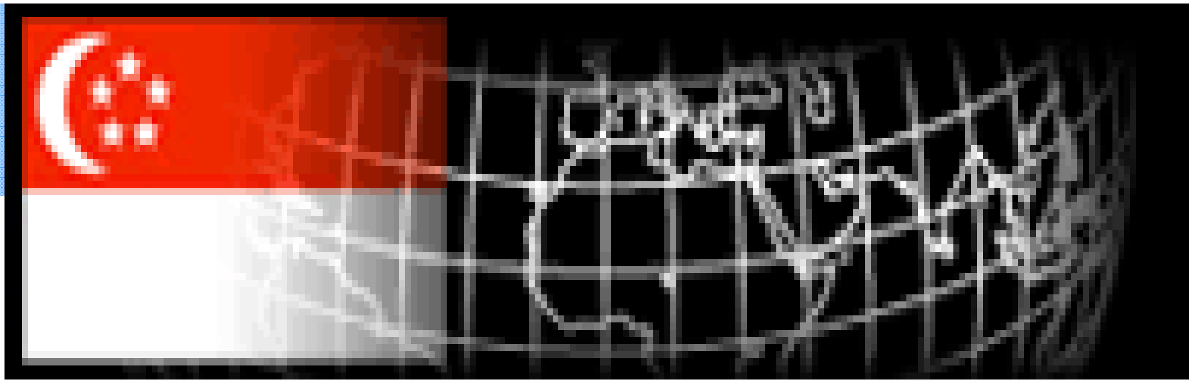
Securing the Intelligent Nation

Yu Chien Siang
Ministry of Home Affairs
Singapore



Agenda



- IT Security Challenges
- The Intelligent Nation
- Towards Intelligent Enterprises
- DORIS – Personal Security System
- Conclusion

Singapore, hi-tech future

Coming soon ...

Great Place Live !

ICT Security Threats Looming

Network Infrastructure Attacks

RFID attacks

Biometrics Attacks

E-passport Attacks

Social Engineering

Phishing

Spamming

Internet Fraud

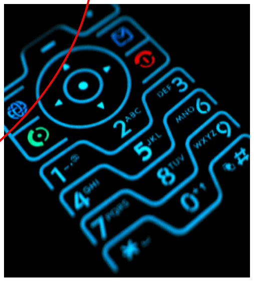
Identity Theft

Fake web sites

US$4.1m a yr lost productivity

Wifi Attacks

Cyber Espionage



Mobile Phone Virus

Cyber Terrorism

Worms

Trojans

15 percent of enterprise PCs have a keylogger

Source: Webroot's SpyAudit

Hacking

Increasingly Hostile ICT Security Landscape

- Future systems (Web 2.0) will be much more complex, harder to understand and control.
- IT Systems hold large data repositories that have to be accessed securely by large groups of users in new ways.

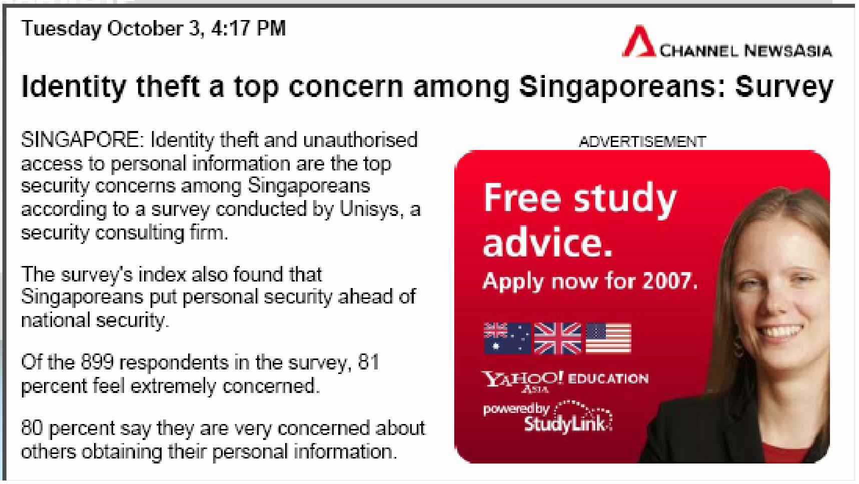
INTERNET TRICKSTER TAUNTS VICTIMS

'Catch me...

...if you can'

Over two dozen car enthusiasts in local online motoring forums cheated in cheap-parts scam

The Straits Times, 1 Nov 2006


Tuesday October 3, 4:17 PM

CHANNEL NEWSASIA

Identity theft a top concern among Singaporeans: Survey

SINGAPORE: Identity theft and unauthorised access to personal information are the top security concerns among Singaporeans according to a survey conducted by Unisys, a security consulting firm.

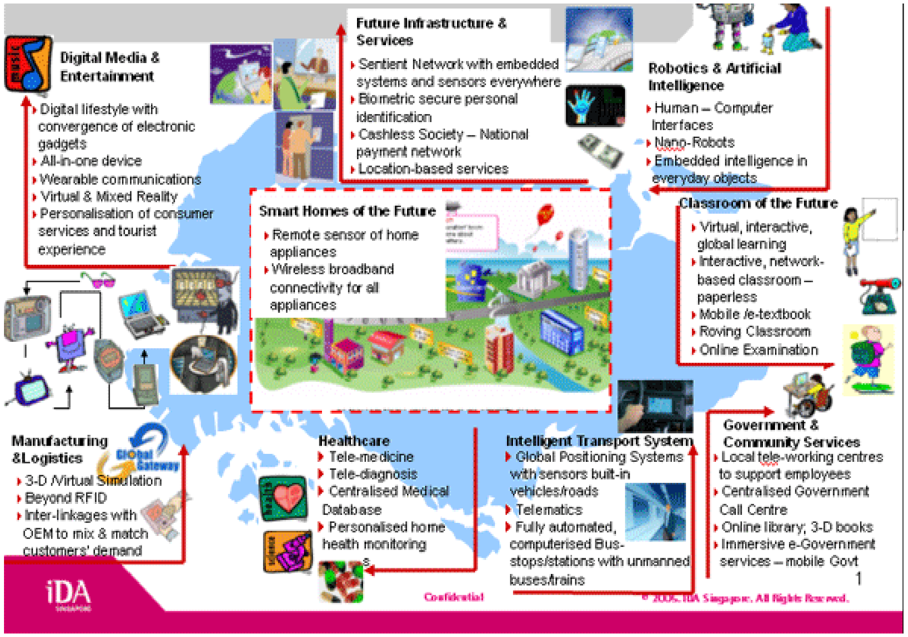
The survey's index also found that Singaporeans put personal security ahead of national security.

Of the 899 respondents in the survey, 81 percent feel extremely concerned.

80 percent say they are very concerned about others obtaining their personal information.

What to look out for ...

- **iN2015 programme**
  - Ubiquitous networks
  - Dynamically evolving and agile enterprises
  - Ambient Intelligence
  - Robots and Slave Agents



Digital Media & Entertainment

- Digital lifestyle with convergence of electronic gadgets
- All-in-one device
- Wearable communications
- Virtual & Mixed Reality
- Personalisation of consumer services and tourist experience

Future Infrastructure & Services

- Sentient Network with embedded systems and sensors everywhere
- Biometric secure personal identification
- Cashless Society – National payment network
- Location-based services

Robotics & Artificial Intelligence

- Human – Computer Interfaces
- Nano-Robots
- Embedded intelligence in everyday objects

Smart Homes of the Future

- Remote sensor of home appliances
- Wireless broadband connectivity for all appliances

Classroom of the Future

- Virtual, interactive, global learning
- Interactive, network-based classroom – paperless
- Mobile /e-textbook
- Roving Classroom
- Online Examination

Manufacturing &Logistics

- 3-D /Virtual Simulation
- Beyond RFID
- Inter-linkages with OEM to mix & match customers' demand

Healthcare

- Tele-medicine
- Tele-diagnosis
- Centralised Medical Database
- Personalised home health monitoring

Intelligent Transport System

- Global Positioning Systems with sensors built-in vehicles/roads
- Telematics
- Fully automated, computerised Bus-stops/stations with unmanned buses/trains

Government & Community Services

- Local tele-working centres to support employees
- Centralised Government Call Centre
- Online library; 3-D books
- Immersive e-Government services – mobile Govt

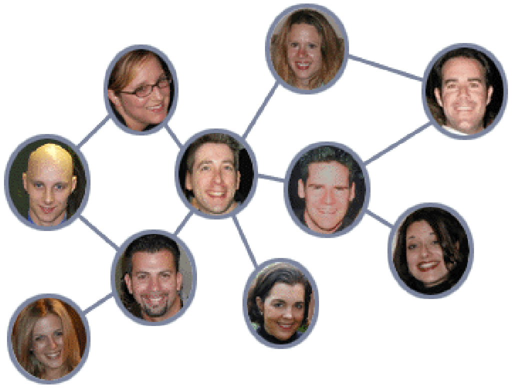
1

iDA

Confidential

© 2006, IDA Singapore, All Rights Reserved.

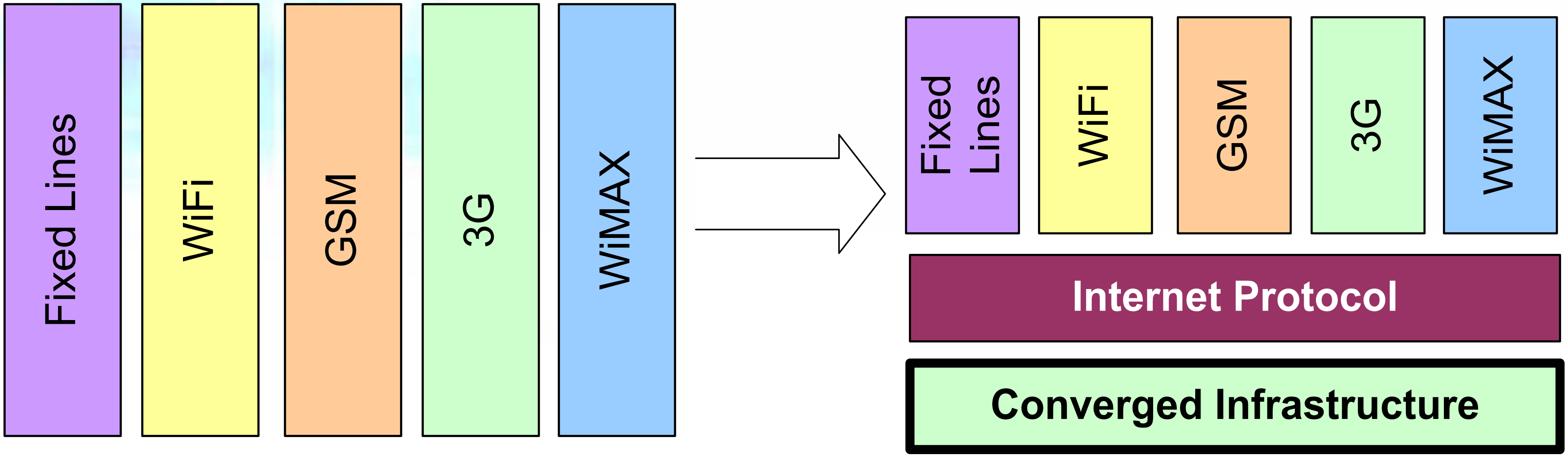
- Broad-based system convergence (Computing Wave)
- Virtual Highways and National IT Infrastructure
- involving grid/utility computing
- Pervasive Virtualisation
- Digital Social Economy



Opportunistic Transactions

- Share petrol money to drive up to Malaysia.
- Cab drivers become DHL.
- Answer needs from Yahoo Answers, story of ad hoc delivery man.

Convergence - ***Securely done!***



Fixed Lines

WiFi

GSM

3G

WiMAX

Fixed Lines

WiFi

GSM

3G

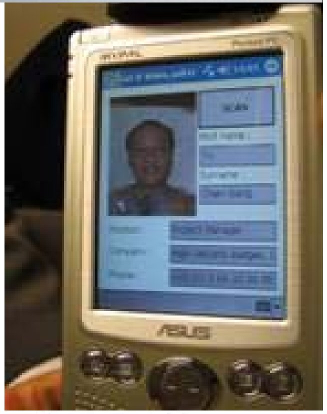
WiMAX

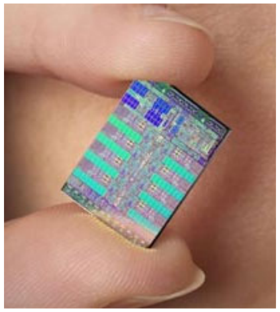
Internet Protocol

Converged Infrastructure

ePayments - ***Securely done!***

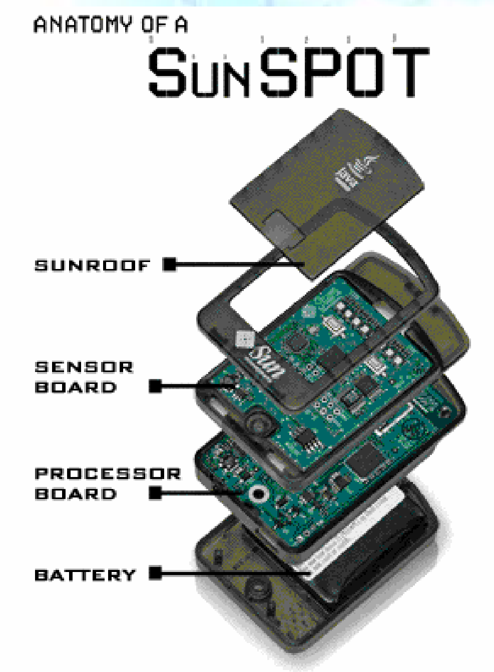
- ePayments
  - **Pay by Touch**
  - **eWallets**
  - **New Visa payments**
  - **CEPAS**





Payments going digital

Already Coming ...



Great Video Conferencing

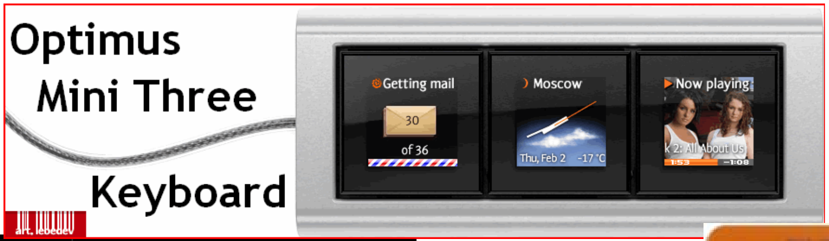
Wakamaru

Mitsubishi HI

Courtesy Mitsubishi Heavy Industries

Robot Guard

Optimus Mini Three Keyboard



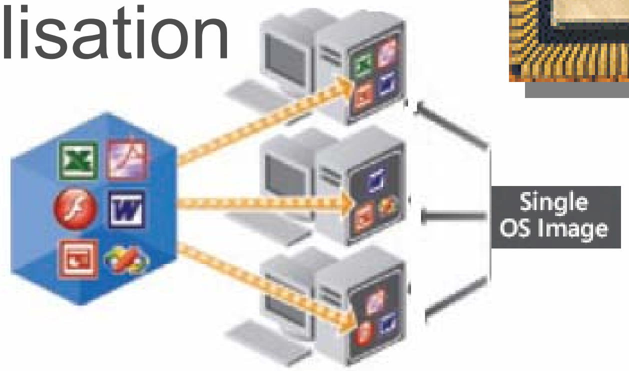
EXPERIMENTAL TECHNOLOGY FROM SUN MICROSYSTEMS LABORATORIES
PROJECT SUN SPOT
SUN SMALL PROGRAMMABLE OBJECT TECHNOLOGY

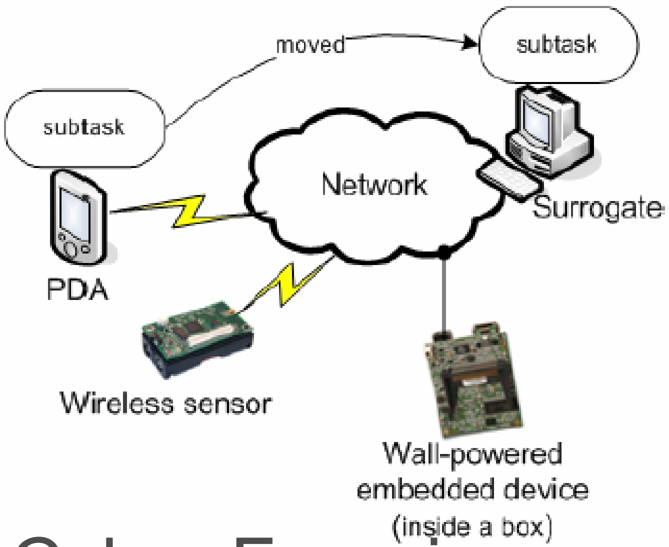
eInk concept

What's next

Better TPMs, HSMs

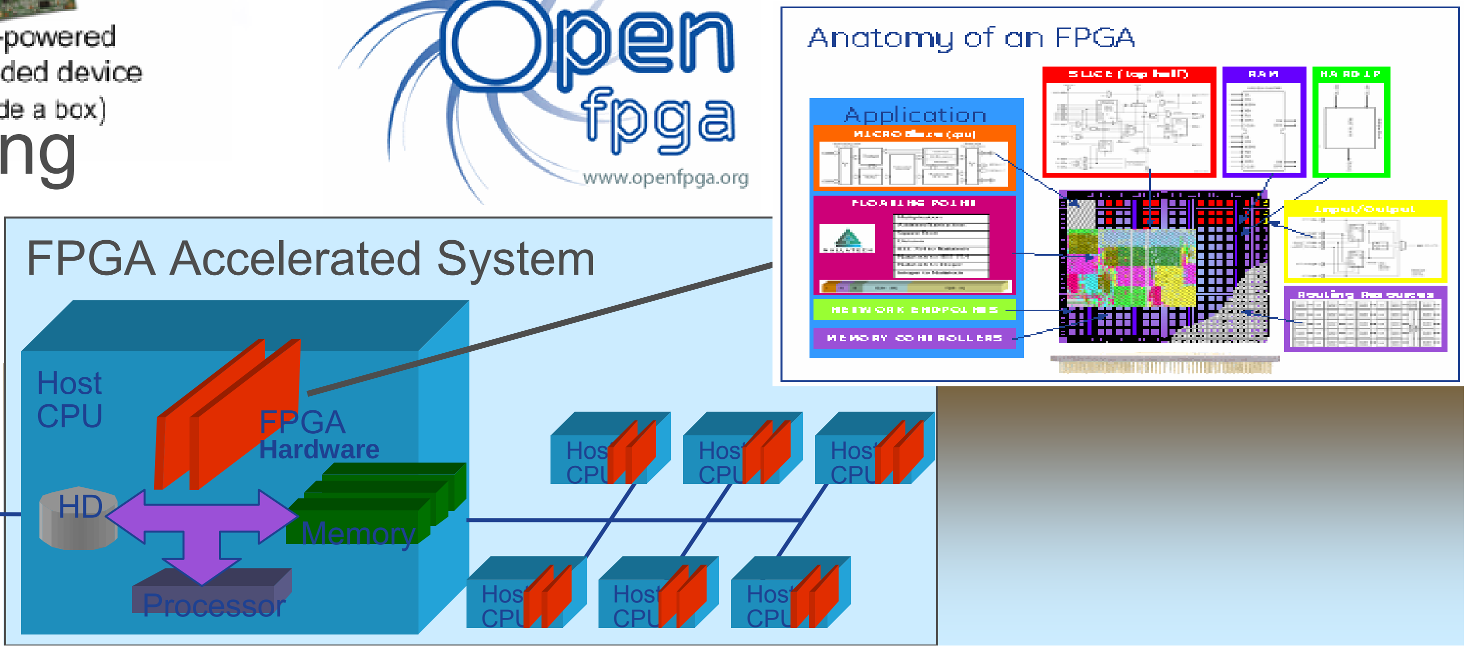
Application Virtualisation





Cyber Foraging

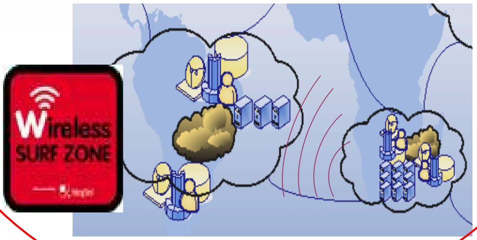
Reconfigurable hardware



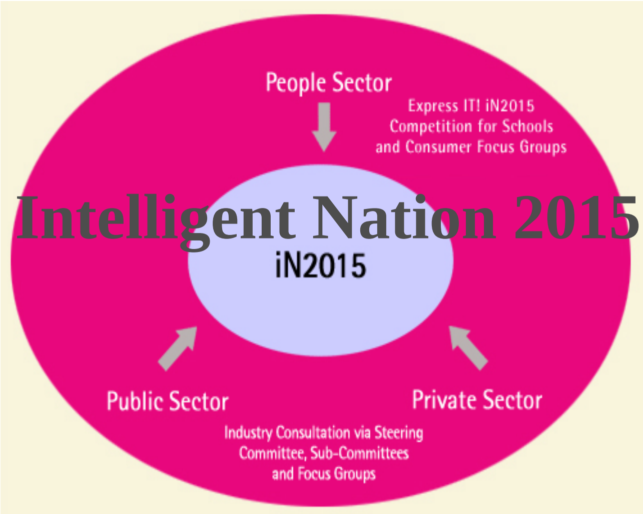
Singapore National Initiatives

National Authentication Infrastructure
NAI and DORIS
Student Card pilots,
Healthcare,
Tourist Card, Logistics

Wireless BroadBand Network
Wireless@SG



Intelligent Nation Biometrics Access Control
INBAC



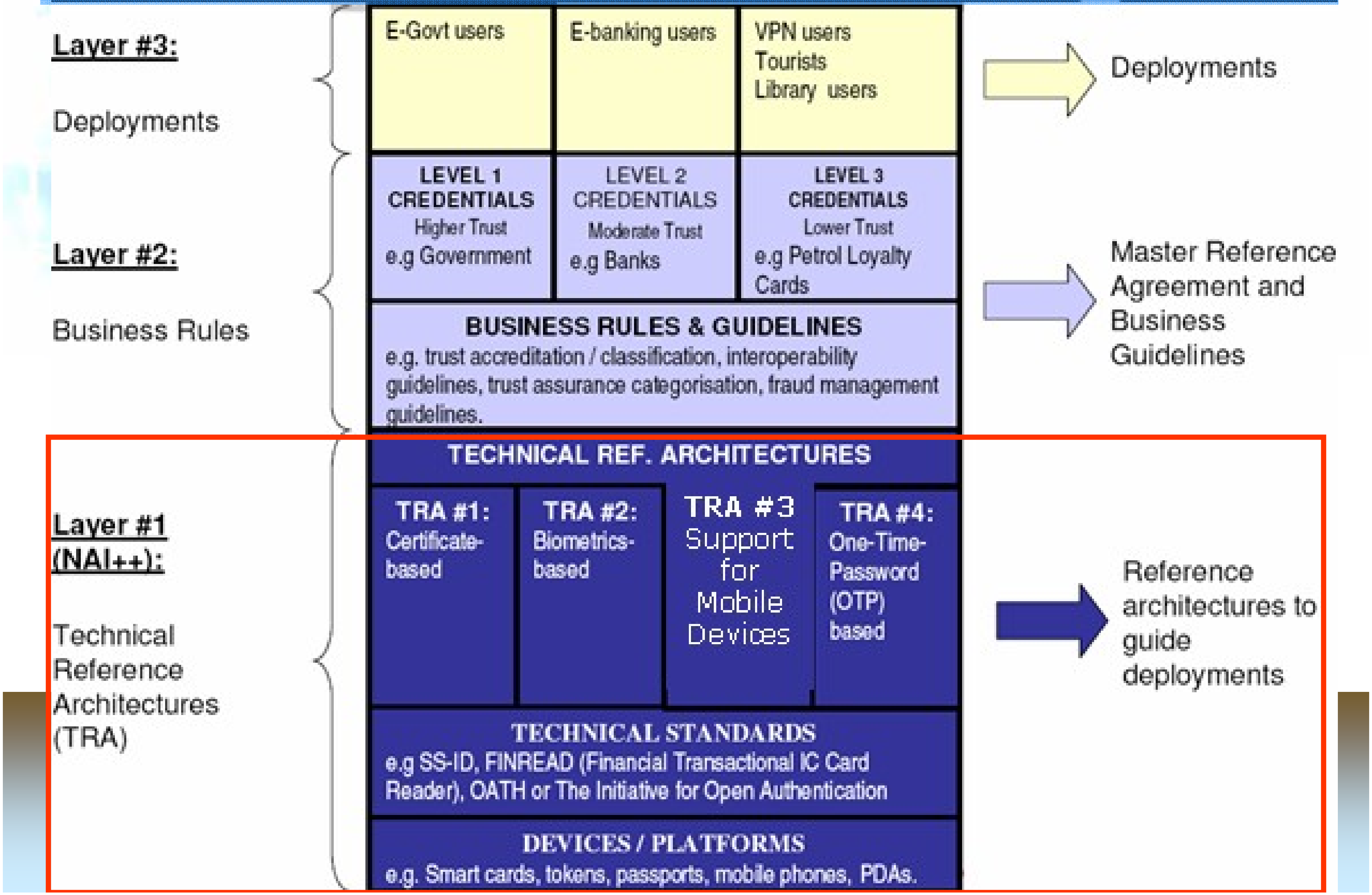
Intelligent Nation 2015

Singapore-Government
Delighting Customers, Connecting Citizens

The Singapore Government's vision
is to be a leading e-Government to
better serve the nation in the digital economy.

Standard Operating Environment
SOE

National Authentication Framework



Layer #3:

Deployments

E-Govt users

E-banking users

VPN users
Tourists
Library users

Deployments

Layer #2:

Business Rules

LEVEL 1 CREDENTIALS
Higher Trust
e.g Government

LEVEL 2 CREDENTIALS
Moderate Trust
e.g Banks

LEVEL 3 CREDENTIALS
Lower Trust
e.g Petrol Loyalty Cards

BUSINESS RULES & GUIDELINES
e.g. trust accreditation / classification, interoperability guidelines, trust assurance categorisation, fraud management guidelines.

Master Reference Agreement and Business Guidelines

Layer #1 (NAI++):

Technical Reference Architectures (TRA)

TECHNICAL REF. ARCHITECTURES

TRA #1: Certificate-based

TRA #2: Biometrics-based

TRA #3 Support for Mobile Devices

TRA #4: One-Time-Password (OTP) based

TECHNICAL STANDARDS
e.g SS-ID, FINREAD (Financial Transactional IC Card Reader), OATH or The Initiative for Open Authentication

DEVICES / PLATFORMS
e.g. Smart cards, tokens, passports, mobile phones, PDAs.

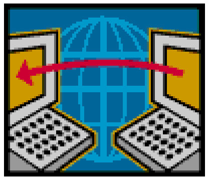
Reference architectures to guide deployments

NAI Ecosystem

GAI
Global Authentication Infrastructure

NID
National ID Providers

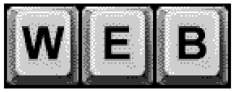
National SSP Regulator



eID Providers

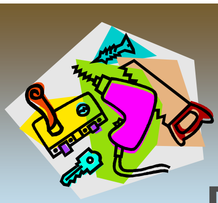
SSP
Security Service Providers

Authentication Operators



Internet Service Providers

System Service Providers



Device User

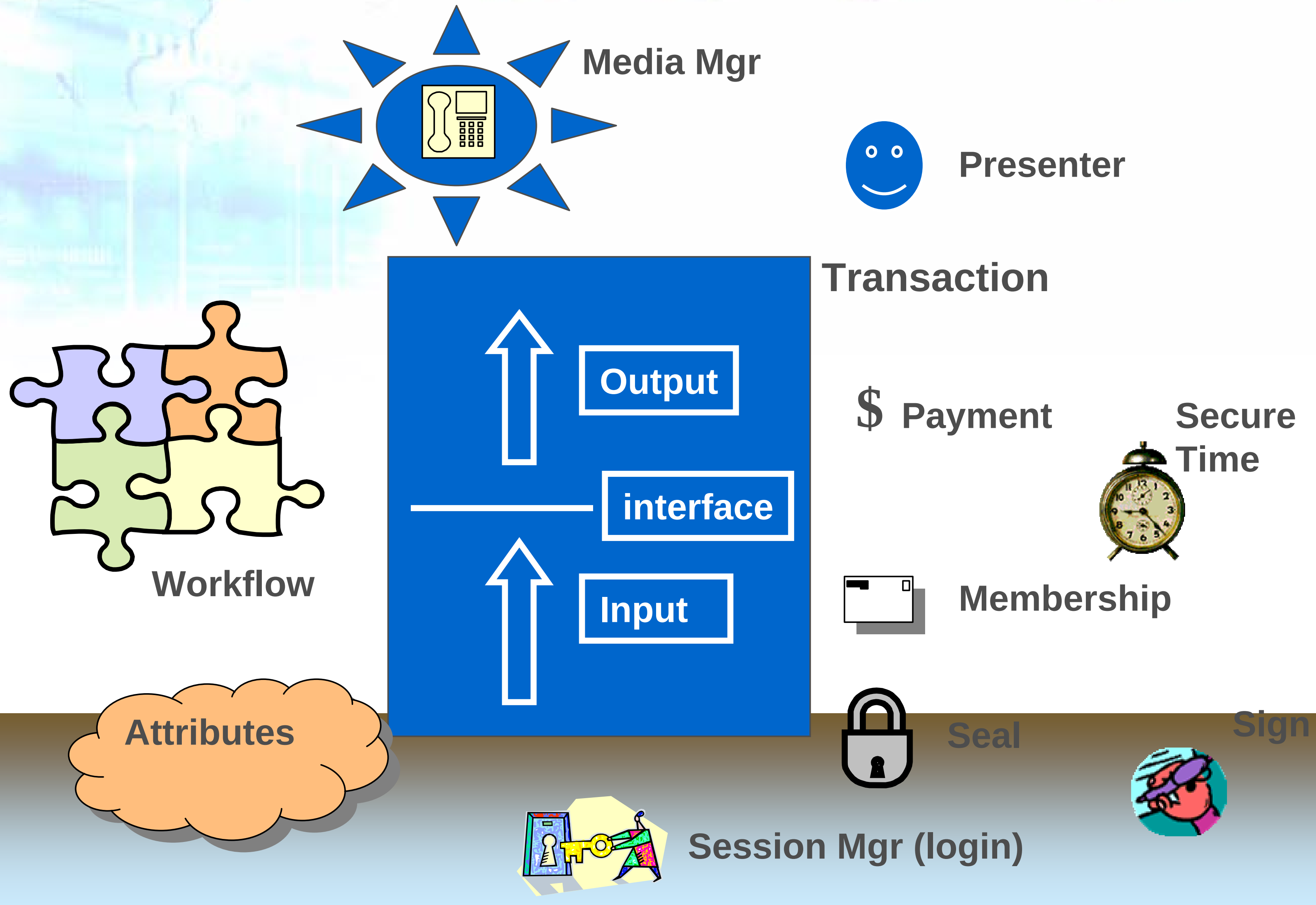
Human User

Software Object

Security Service Providers (SSP)

- **Traditional CA and Extensions**
  - Attribute certs
  - Biometric certs
- **Notary**
  - eLegal, eContracts
  - Archiving
- **Personal Security Mgt**
  - Registration Service and eForms Filling
  - Grid Storage
  - Virtual Backend
  - Login Mgr, SSO
  - Workflow Mgr
  - eBallpoint Pen and Personal Backup
  - Locked down execution
- **Secure Interfacing**
  - Medium Mgr (Linkup to networks, sensors, embedded systems)
  - Secure Services Mgt, AJAX and Webservices
  - Directory Lookups
- **Secure Collaboration and Social Networks**
  - Secure voice and conferencing
  - Community membership
  - Loyalty
  - Rights, Relationships and Roles Mgt
- **Secure Interaction and Presentation**
  - Privacy
  - Anonymity
  - Virtual Card Services
  - Remote Access
- **Secure Transaction**
  - Record level audit and mgt
  - Proxy Mgt
  - Attributes Mgt and Agent Engagement
  - Print, Send and Delivery
  - Secure Time (sync and timed release)
  - Secure Payment
  - Sign and Seal
  - eVoting

NAI Security Services



Media Mgr

Presenter

Transaction

Output

interface

Input

$ Payment

Secure Time

Workflow

Membership

Attributes

Seal

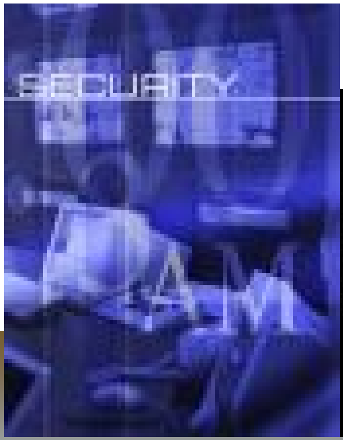
Sign

Session Mgr (login)

Inventing own weapon - DORIS

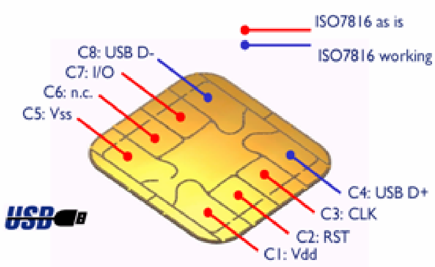
(Digital **O**nline **R**egistration and **I**dentification **S**ystem**)**

- **Open-architecture Personal Security System**

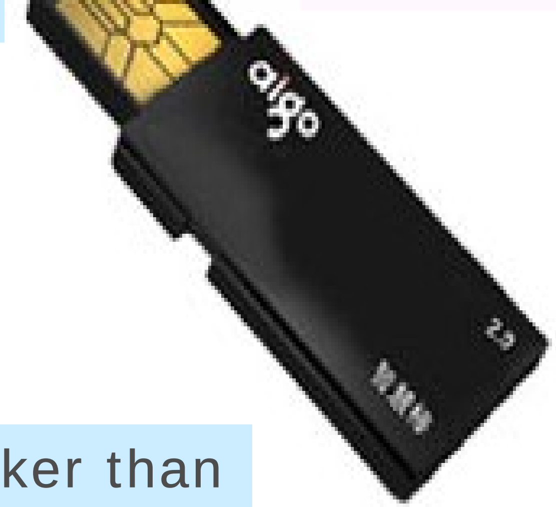


DORIS - Optimal Solution

- DORIS provides
  - **Electronic ID**
  - **Online authentication**
  - **Offline authentication (INBAC)**
- Based on Smart VIP



Tokens with Flat Surface



I-Stick, 2.5 x thicker than smart card. USB memory

Mobile DORIS

Bluetooth Phone or any Bluetooth-enabled Device

Mobile Phone with USB Port

Via Bluetooth or ZigBee (Z-SIM)

NFC Phone

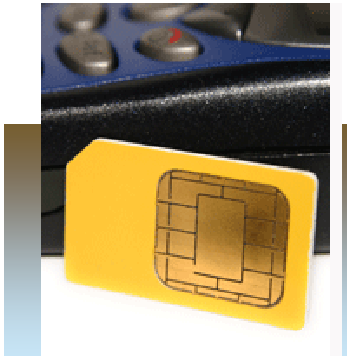
Via NFC

Via USB Stick Format

Different Form Factors for PDA/Phones

- SDiD
- xD
- NFC
- Secure MMC
- SIM overlay
- Next Gen SIM

Future Implementation



SIMoME™

Contactless SIMoME (quarter of 2007)

Mobile DORIS Challenges

- High Cost
- USB vs MMC as a High Speed Interface for SIM cards
- OS support for mobile phones, SIM toolkit is too primitive and not GUI friendly (like DOS).

Personal Protection Device like M16

Grenade Launcher

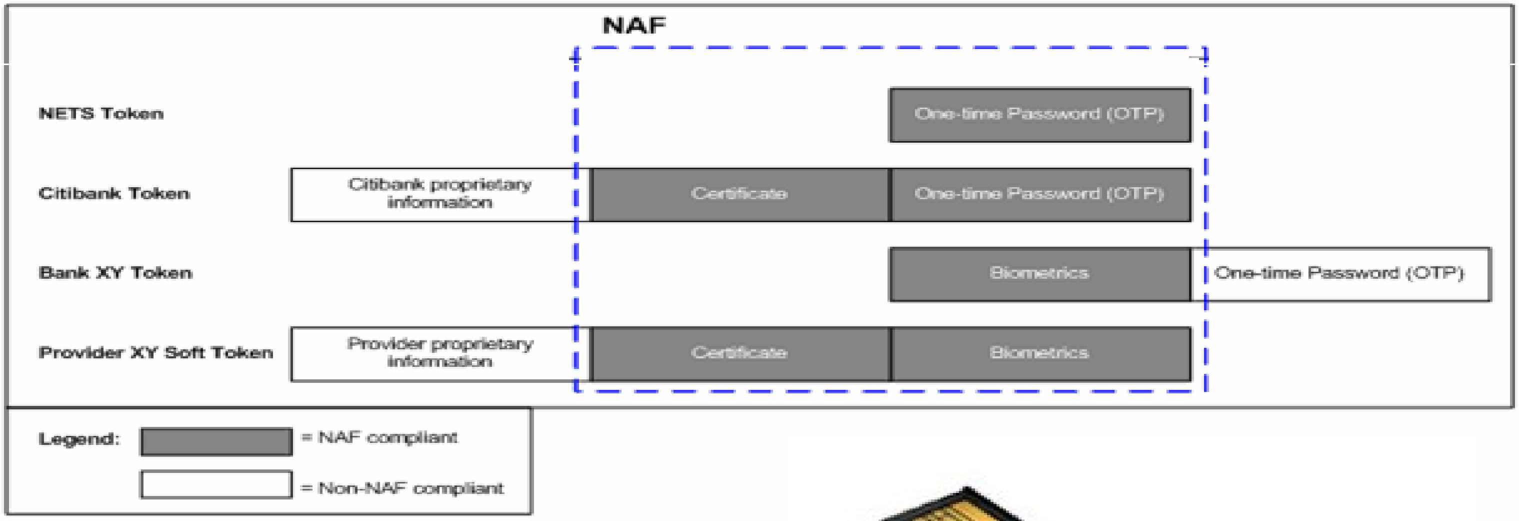
Bayonet

Accessories:
Tripod, scope, IR,
Laser sight, magazine

Different Bullets:
Tracer, Blanks, armour piercing

DORIS Demystified

- DORIS is not 2 Factor but n-factor supporting biometrics, ISO standards, Virtual Smart Cards and a Grid architecture.



NAF

NETS Token			One-time Password (OTP)	
Citibank Token	Citibank proprietary information	Certificate	One-time Password (OTP)	
Bank XY Token			Biometrics	One-time Password (OTP)
Provider XY Soft Token	Provider proprietary information	Certificate	Biometrics	

Legend: ▨ = NAF compliant

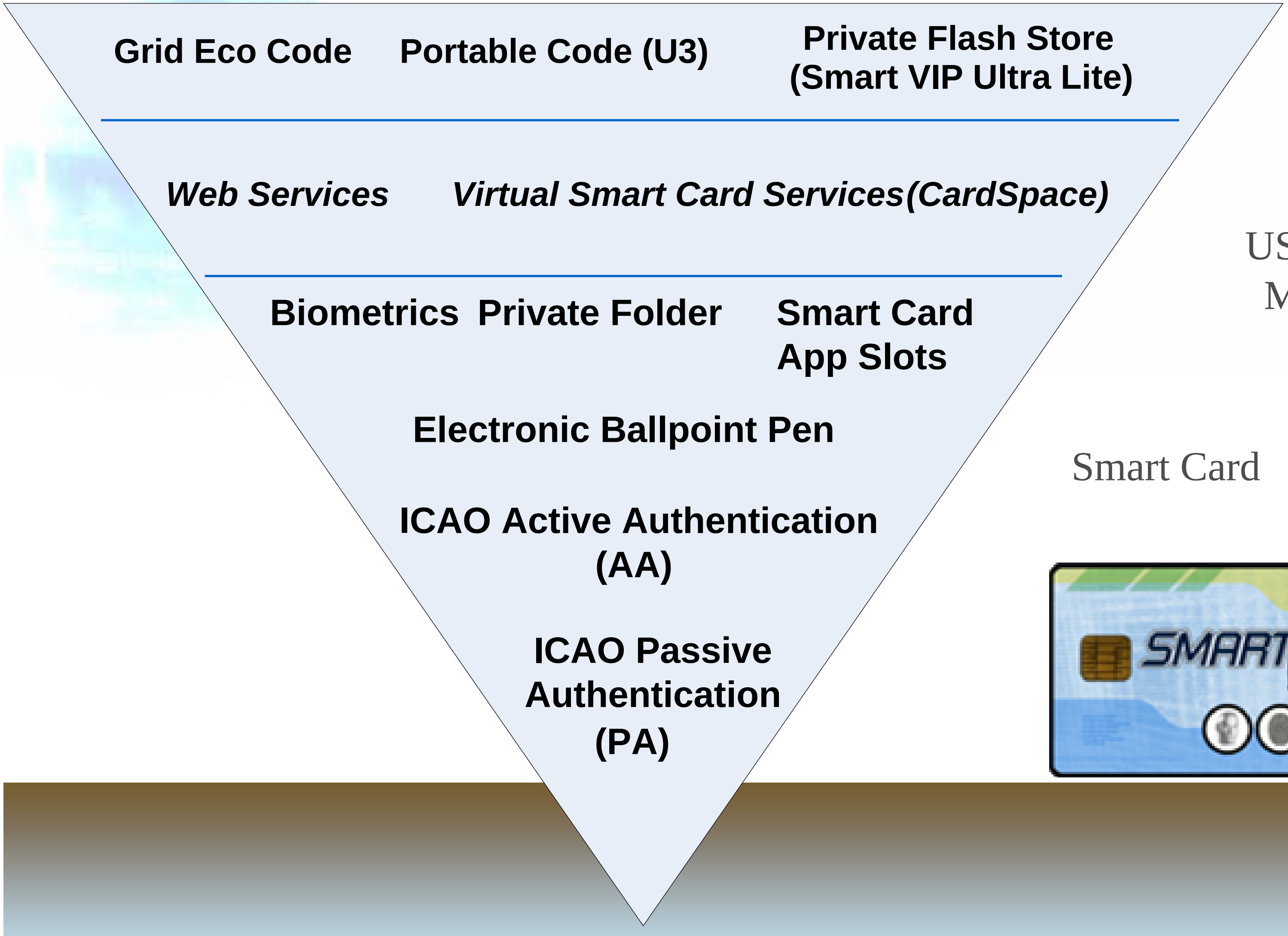
□ = Non-NAF compliant

Loaded inside DORIS

DORIS Memory Map

	Doris Mini	DORIS
SmartVIP Lite (DG3 now up to 6k)	8k	8k
OTP Applet (8K) - Removed	0k	8k
Certificate	2k	4k
Personal Folder (Scratch Pad)	~6k	~18k
App Slots (10x 1k slots)	10k	20k
Mifare Support	~1k	~1k
Keys (now with BioCrypto)	5k	5k
Total	**32k**	**64k**

DORIS Extensible Architecture



Grid Eco Code Portable Code (U3) Private Flash Store (Smart VIP Ultra Lite)

Web Services *Virtual Smart Card Services(CardSpace)*

Biometrics Private Folder Smart Card App Slots

Electronic Ballpoint Pen

ICAO Active Authentication (AA)

ICAO Passive Authentication (PA)

USB Flash Memory

Smart Card

Keep Operating System Simple

- Beyond PCs, beyond notebooks, beyond PDAs.
- Start from a small trusted core.
- Take over resources like CPU, mouse, Internet etc. Startup a Virtual PC.
- Talk to a trusted backend.
- Startup a Virtual Backend (remote server).
- Build your trusted applications dynamically and put everything on-demand.

Imagine – no need to carry a notebook or a PDA

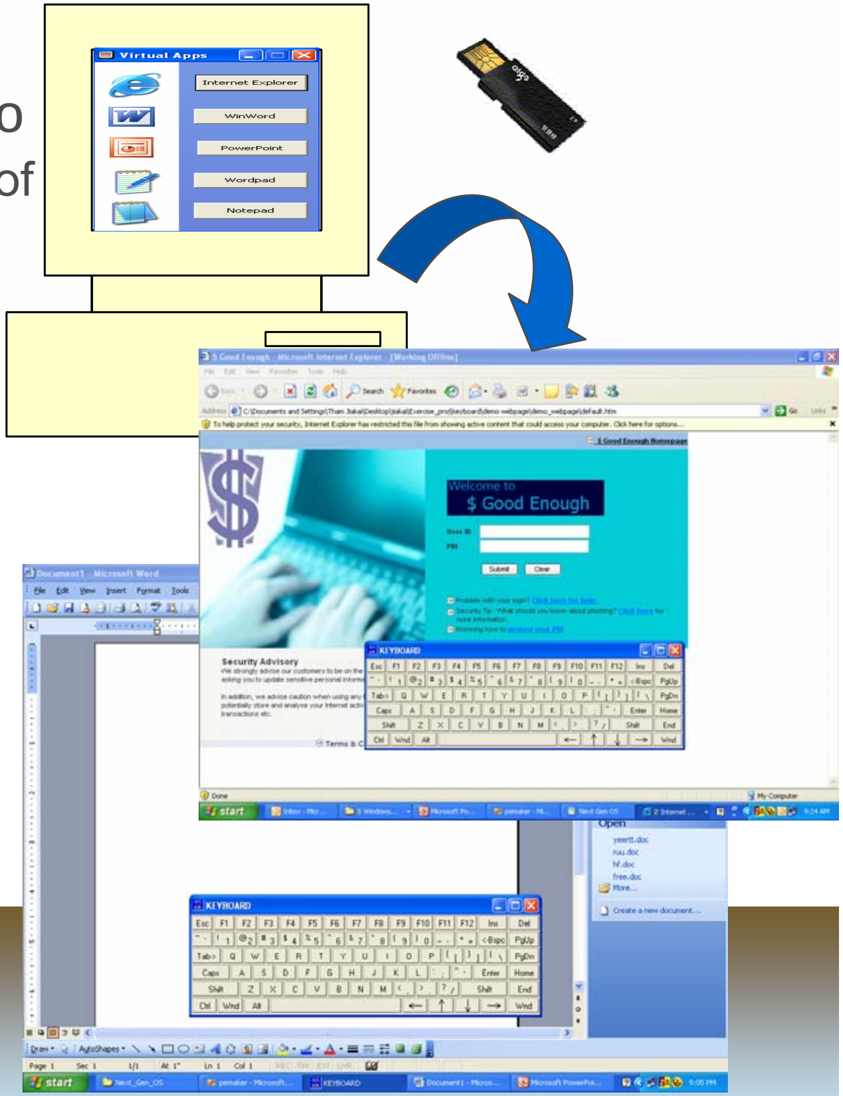
Dynamic Isolation of Virtualised Applications (DIVA)

- Like SunRay from Flash but offline too

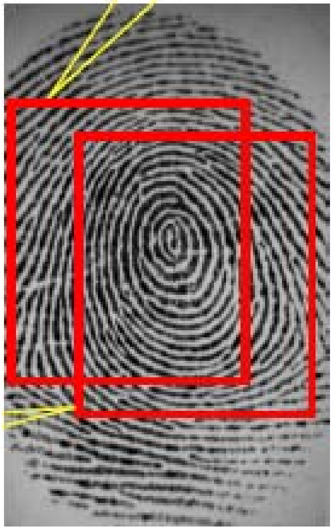
Prototype (in development) showing the concept of managing some common applications protected by DORIS (with flash) under a light protection “Sandbox”.

- Restrict applications’ File Input/Output transaction (no traces left on the host)

- Provide a Virtual On screen keyboard for secure user input (such as PIN) (bypasses user and kernel level keylogger), web SSO.



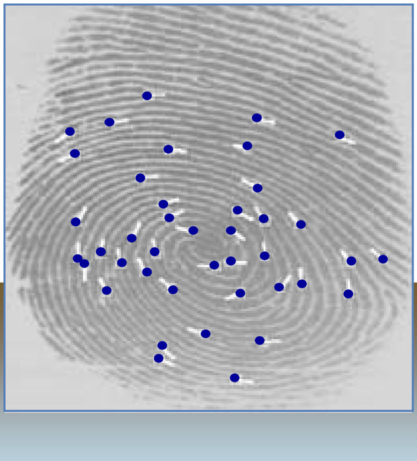
BioCrypto – What is BioCrypto?



- BioCrypto is the derivation of a cryptographic key upon presentation of a live biometric like fingerprint or iris by using external data, like obfuscation cum thresholding or error correction.

Privacy Positive Search, with BioCrypto

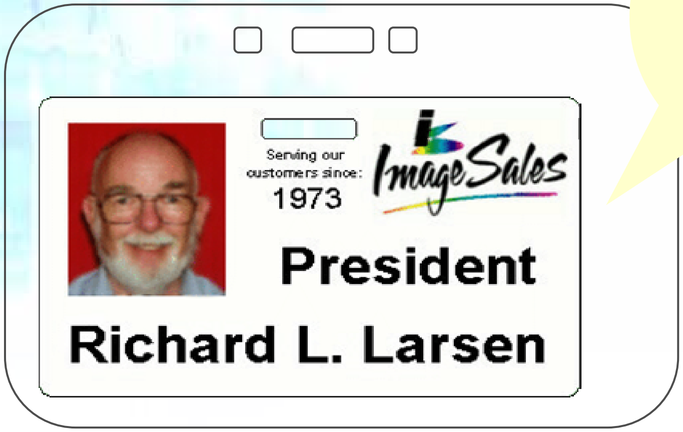
- Extension of BioCrypto to do search in <1 second for many (60) millions of records.
- Privacy positive, we can search but no one knows who is being searched.
- Optimisation for PDA and handphones based on online SmartVIP ultralite mode and a Fingerprint Certificate.



Privacy Positive Search

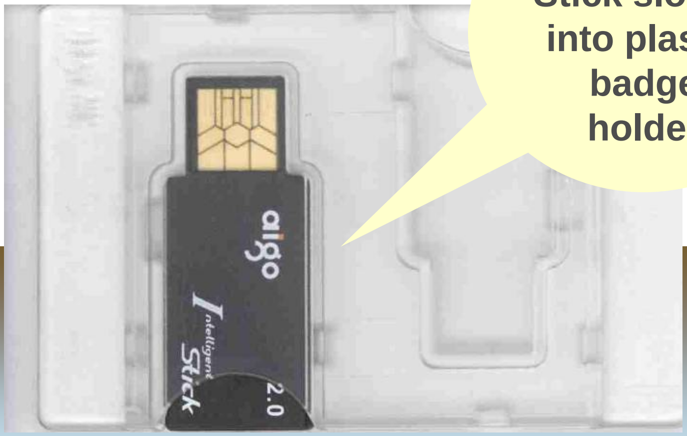
Innovative Design – Badge Holder

Front



“No chip” ID card placed in Card holder

Reverse



DORIS I-Stick slotted into plastic badge holder

Accessories

- Wrist straps with a DORIS holder as Corporate Gifts, Fashion accessory!
- Similar to handphones accessories
  - **Cover**
  - **Chain**
  - **Customisation & Personalisation (engraving, photos)**

Initial Ideas

- 3 options:
  - S$5 – Tri-interface chip only
  - S$20 to S$30 – Includes flash drive (512MB)
  - S$35 to S$60 – Secure Badge with fingerprint reader

Pilot Project @ SMU

- Student Card Project
- Issue DORIS I-Stick tokens to School of Information Systems students (about 600 in phase 1)
- Students to develop killer apps and others
- DORIS can support existing SMU gates

SMU Survey Results

Many many applications

Data Storage, like Flash Drive

Biometric fingerprint support

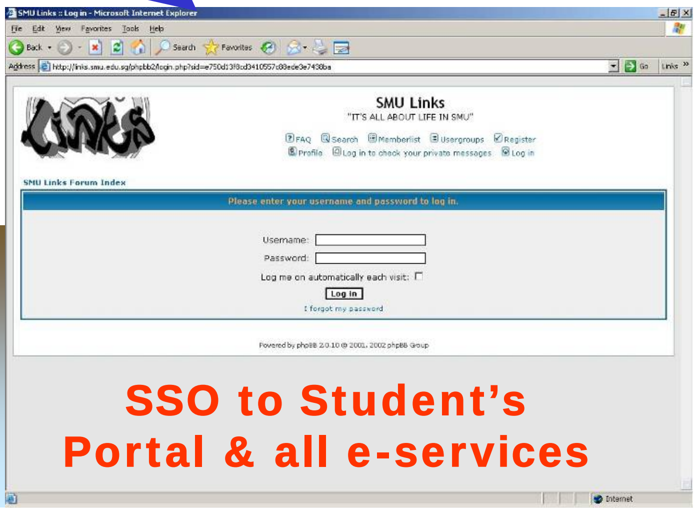
Photo ID

Visit Other Campuses

TRANSPORT (BUS, MRT)

CASHCARD (photocopying, locker rental, book borrowing, library fine payment, canteen, etc)

Door Access (labs, offices, LTs, seminar rooms)



SMU Links :: Log in - Microsoft Internet Explorer

http://links.smu.edu.sg/phpbb2/login.php?sid=e750d13f8cd3410557c88ede3e7438ba

SMU Links

"IT'S ALL ABOUT LIFE IN SMU"

SMU Links Forum Index

Please enter your username and password to log in.

Username:

Password:

Log me on automatically each visit: □

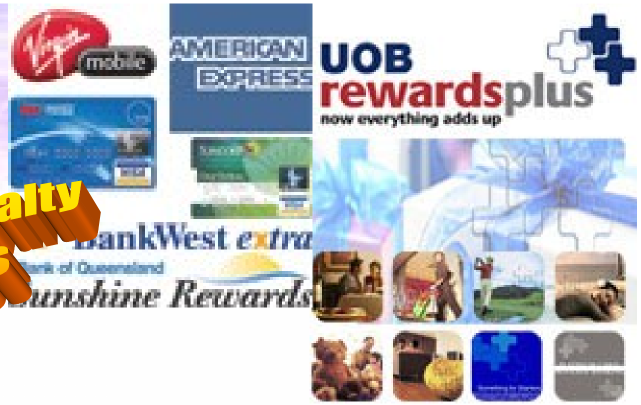
Powered by phpBB 2.0.10 © 2001, 2002 phpBB Group

SSO to Student's Portal & all e-services

How to handle loss?

Killer Applications

- E-government
- Health
- E-Payment support
- Telco – “Find me, Follow me” VoIP phone
- Tourist Promotion applications
- Grid storage and Web Services Code
- Integrated IHL Visitor Management System
- Virtual Smart Cards
- Loyalty
- Emergency Card
- Education
- Student
- CPF: Biometrics for the Aged



Aggregated Loyalty Programmes

Tourist Promotion

Visitor Registration System

Emergency Card

Foreigner ID Card

CardSpace with DORIS

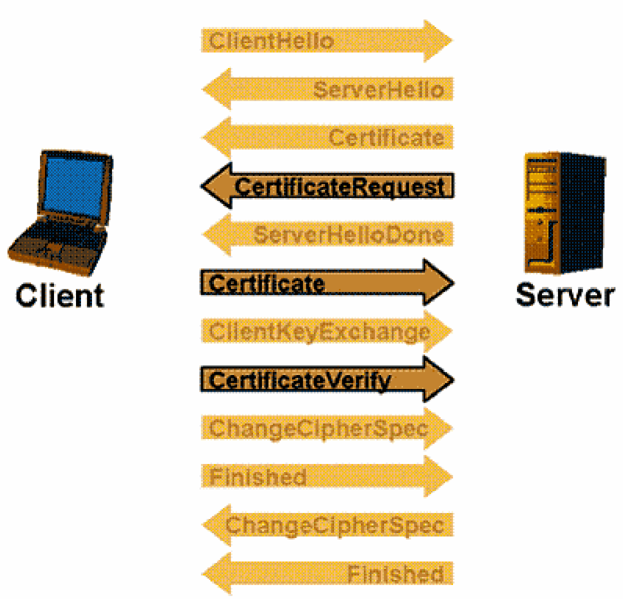
- Microsoft CardSpace is an identity selector for Windows
- Enable users to provide their digital identity online in a more simple and secure way
- DORIS token further enhance it security by providing a strong ‘n-factor’ credentials for authenticating the Microsoft Security Token Service (STS) when using CardSpace

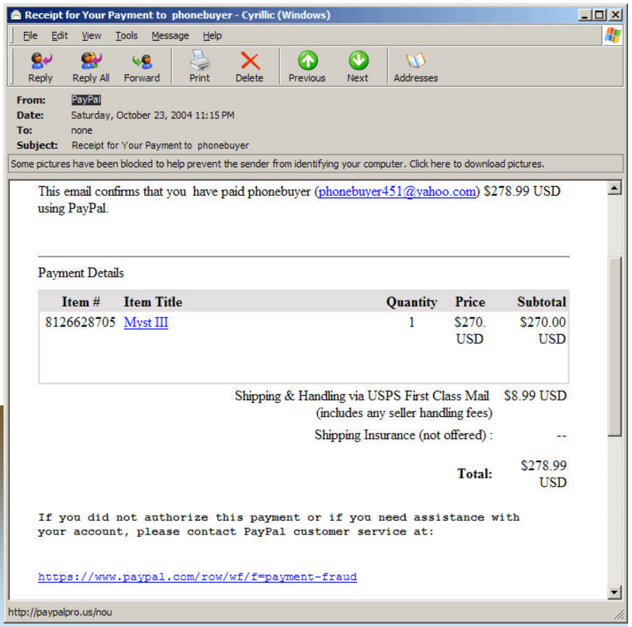
DORIS OTP

- DORIS OTP is based on OATH
- 8Kb Java applet
- 2.13Kb Java applet
- 0.3Kb Applet-less

Issues with OTP

- Security Risks
  - **Phishing**
  - **Man-in-the-middle attack**
- Need for end-to-end security
- Internet Engineering Task Force (IETF) Specification (RFC 4226) on OTP
  - **Need for secure channel to protect user's privacy and avoid replay attacks**
  - **Bi-Directional Authentication. Need to authenticate the validation server**
- Implementation via 2-way SSL




Receipt for Your Payment to phonebuyer - Cyrillic (Windows)
File Edit View Tools Message Help
Reply
Reply All
Forward
Print
Delete
Previous
Next
Addresses

From: PayPal
Date: Saturday, October 23, 2004 11:15 PM
To: none
Subject: Receipt for Your Payment to phonebuyer

Some pictures have been blocked to help prevent the sender from identifying your computer. Click here to download pictures.

This email confirms that you have paid phonebuyer (phonebuyer451@yahoo.com) $278.99 USD using PayPal.

Payment Details

Item #	Item Title	Quantity	Price	Subtotal
8126628705	Myst III	1	$270. USD	$270.00 USD

Shipping & Handling via USPS First Class Mail (includes any seller handling fees)	$8.99 USD
Shipping Insurance (not offered) :	--
Total:	$278.99 USD

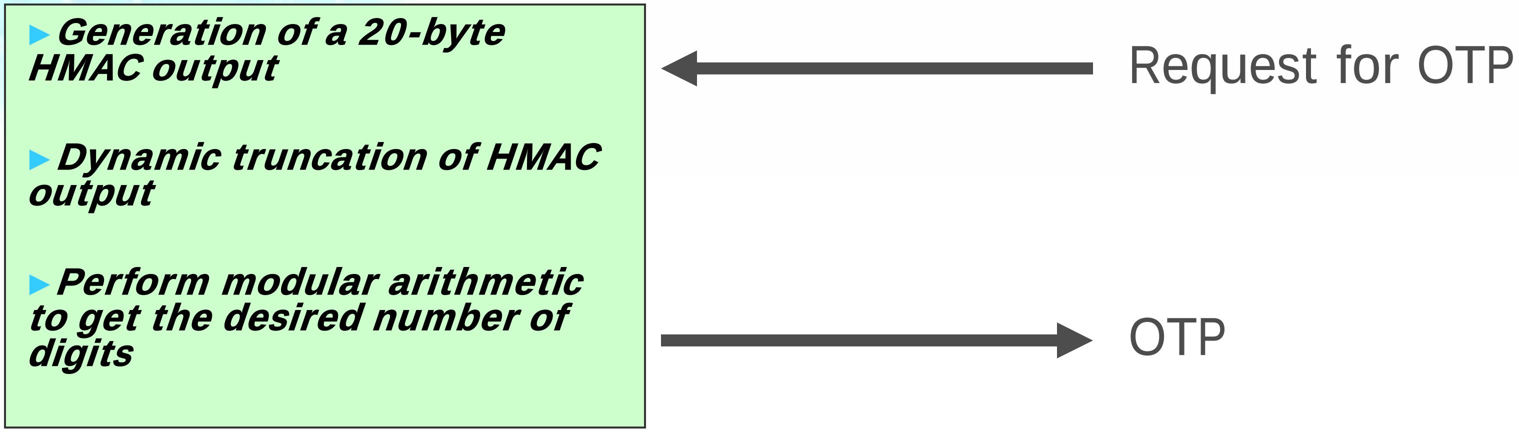
```
If you did not authorize this payment or if you need assistance with
your account, please contact PayPal customer service at:
```

https://www.paypal.com/row/wf/f=payment-fraud

http://paypalpro.us/nou

DORIS OTP

- 8KB Java applet



▶ ***Generation of a 20-byte HMAC output***

▶ ***Dynamic truncation of HMAC output***

▶ ***Perform modular arithmetic to get the desired number of digits***

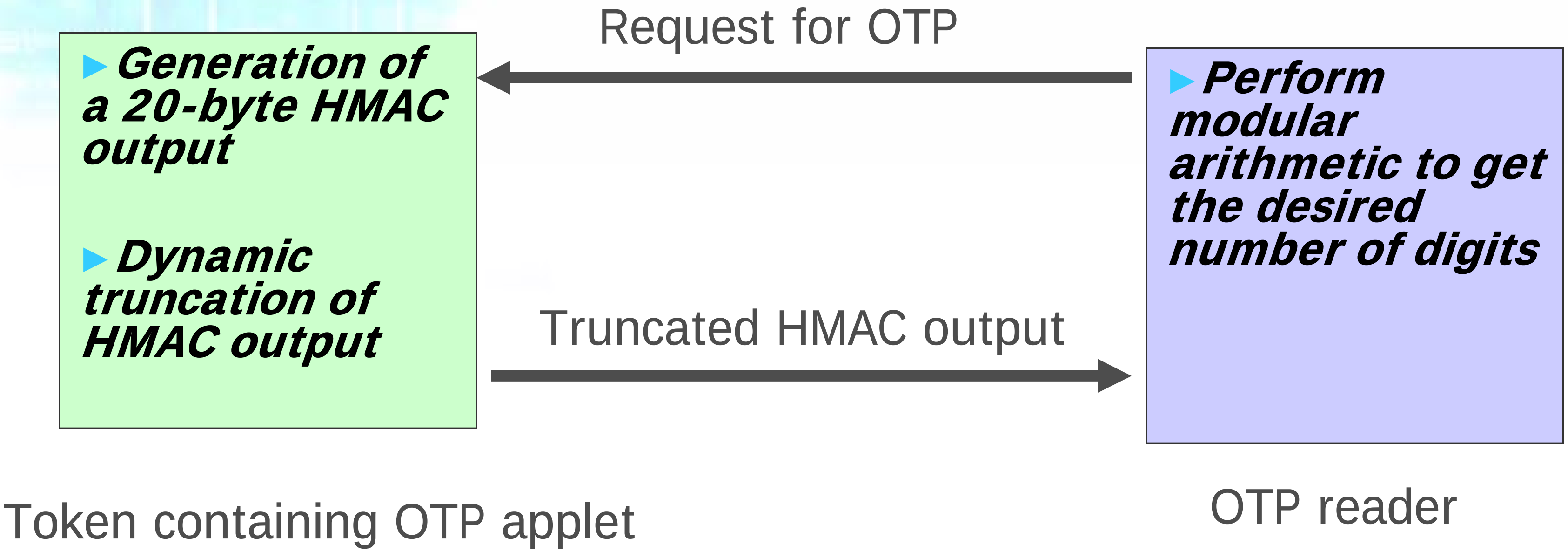
Request for OTP

OTP

Token containing OTP applet

DORIS OTP

- 2.13KB Java applet



Request for OTP

▶ ***Generation of a 20-byte HMAC output***

▶ ***Dynamic truncation of HMAC output***

Truncated HMAC output

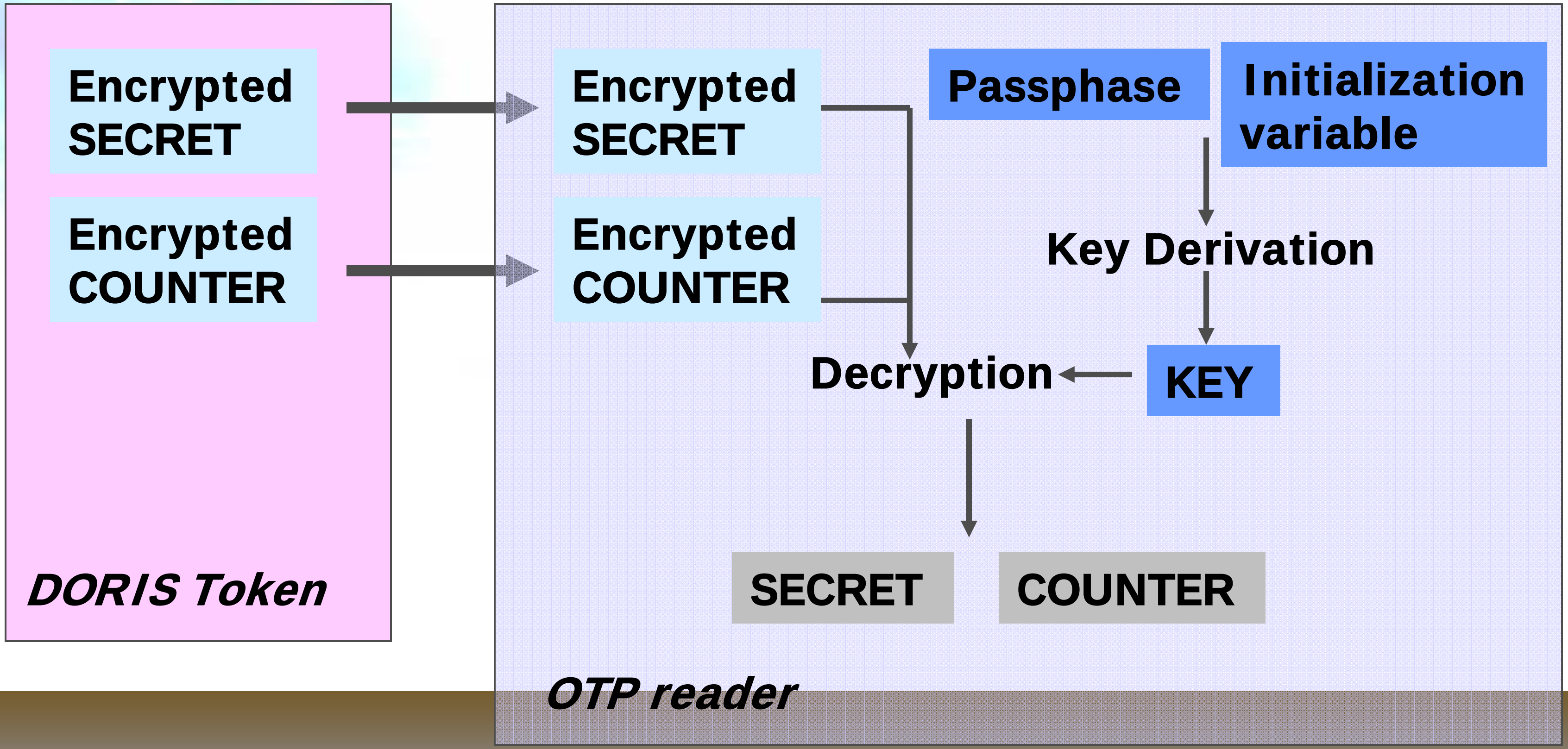
▶ ***Perform modular arithmetic to get the desired number of digits***

Token containing OTP applet

OTP reader

DORIS OTP

- 0.3KB Applet-less



Encrypted SECRET

Encrypted COUNTER

DORIS Token

Encrypted SECRET

Encrypted COUNTER

Passphase

Initialization variable

Key Derivation

KEY

Decryption

SECRET

COUNTER

OTP reader

DORIS OTP

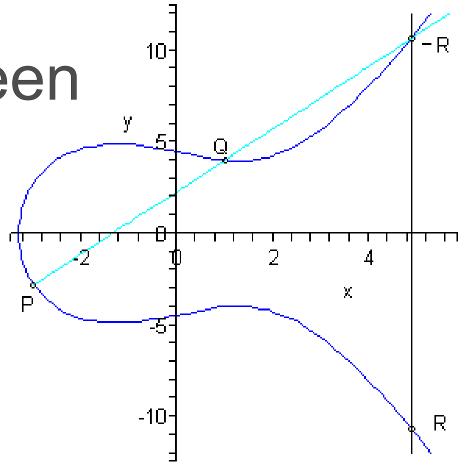
- Different solutions for different needs

	8K Java applet	2.13K Java applet	0.3K Applet-less
Size	8K	2.13K	0.3K
Security	Secret and counter never leave the token	Secret and counter never leave the token	Secret and counter leaves the Token hence OTP reader must be secure
Performance	594 ms	485 ms	531 ms
Deployment Considerations	Simple OTP readers can be issued to users	OTP readers to be issued to users must be able to do computation	User must be present when personalizing OTP reader and token

Our Open Source Efforts

- DORIS is based on ECC public key crypto.
- ECC libraries
  - **BorZoi (Dragongate Technologies Ltd) http://dragongate-technologies.com/products.html#borZoi**
  - **Mircal (Shamus Software Ltd) http://indigo.ie/~mscott/**
  - **OpenSSL (for P curves) http://www.openssl.org**
- OTP Java card applet
  - **MHA OATH http://www.ida.gov.sg/idaweb/techdev/infopage.jsp?infopagecategory=articles:techdev&versionid=1&infopageid=I3427**
- Demo codes
  - **Available at http://www.governmentware2006.com/download.html**

ECDSA Verification

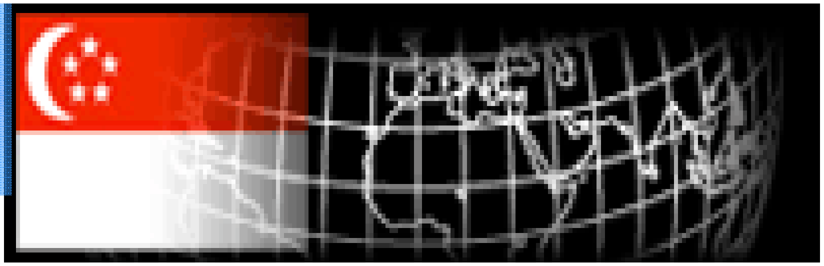


- DORIS token’s ECDSA P192 curve has been validated by NIST using tests described in Elliptic Curve Digital Signature Algorithm Validation System (ECDSAVS)

- ECDSA Validation List http://csrc.nist.gov/cryptval/dss/ecdsaval.html

- A simple test can be conducted by loading the test key pair into the ecdsa test applet and compute the signature based on the test messages

Joining Community ...



- We have now a community of more than 50 companies supporting DORIS. A good number of DORIS Pilot projects, based on DORIS tokens, on loan. Contact us, please.

We welcome you

Demonstrations

Basic DORIS features

- **Self Enrollment Kiosk**
  - Lucky Draw
- **Authentication**
  - Contact interface
  - Contactless interface
- **Electronic Signature**
  - Acrobat signing
- **Door Access System**

Application based

- **Mobile Doris**
  - SDiD card
  - NFC enabled phone
- **OTP (with and without pass phrase)**
  - PDA OTP Reader
  - NFC OTP Reader
  - Various Applet versions
- **DIVA**
  - Anti-key logging
  - SSO
  - File redirection
- **Cardspace**
  - eBanking DORIS login