Tan Teck-Lee
Chief Innovation and Technology Officer

"Cryptography and digital security: future needs and challenges seen from a commercial perspective"

French-German- Singaporean "Applied Cryptography" workshop

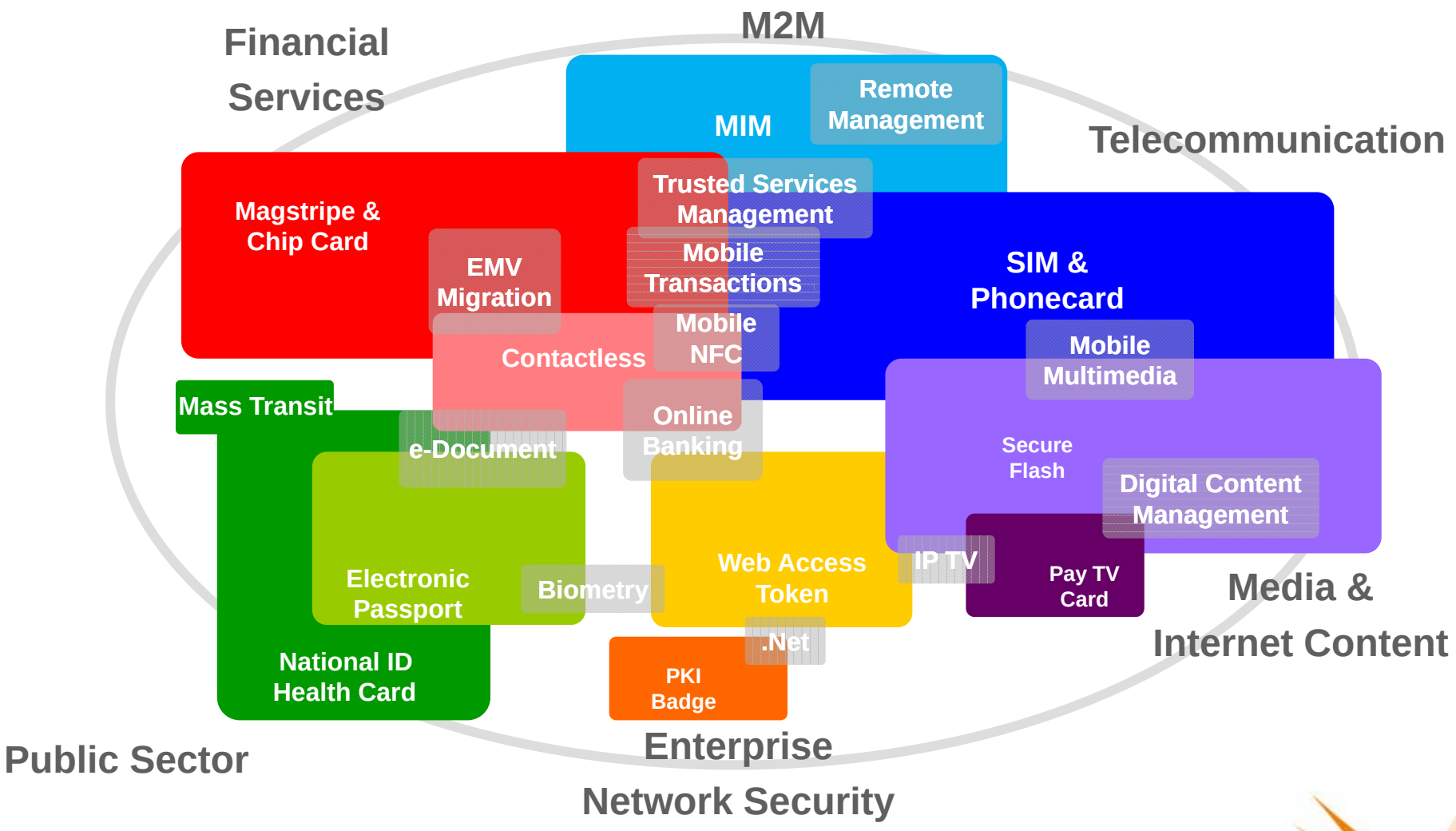
Agenda

- Short introduction of Gemalto mission
- The vision of a World critically in need of digital security
- Beyond 2010: from application centric to user centric security
- A view on commercial needs around cryptography
- Conclusion

Gemalto makes people's everyday interactions with the digital world secure and easy

Gemalto provides end-to-end solutions for digital security,
from the development of software applications,
through the design and production of secure personal devices
such as smart cards, ePassports and secure tokens,
to the deployment of managed services for our customers

Gemalto is at the heart of digital convergence



Security expertise

- **Internationally renowned team in security and cryptography at the forefront of new anti-fraud techniques**
  - 50 specialists, of whom 15 PhDs in security & cryptography
  - Over 250 patents in cryptography & security
  - Sophisticated laboratory to simulate and counter security attacks
- **Large number of security certificates**
  - More than 40 products Common Criteria and ITSEC certified, including 20 EAL4+, 2 EAL5+ and EAL7 certifications
  - Our sites are certified by most security organizations like MasterCard®, VISA, GIE-CB, Moneo, American Express etc.
- **Best software implementation of latest security standards**
  - 75% of the security of a smart card comes from the OS, 25% from HW protection mechanisms

Biometrics

Advisor to standards incl. ISO-SC37, AFNOR and COST-2101; dedicated R&D team with 10 years of experience

Secure Web Authentication

Zero-footprint, encrypted mutual-authentication for web sessions

Secure Printing

Industry-leading know-how in laser-secured engraving/embossing and secure colour technologies

A World critically in need of digital security

Digital security is concerned with making digital interactions secure and easy

More freedom for people to better enjoy their digital lifestyle…

- Buy things **fast & easy**, in shops or online, and knowing your credit card is safe
- Maintain company's **cloud-based** information system integrity when faced with **malicious attacks**
- Keep track and manage **in privacy** your healthcare scheme
- Retrieve fast and securely your **personal data** after losing your mobile phone
- Cross a metro gate in **less than 1 second** at peak hours without hassle
- Stay in control of your different **virtual identities** in a World where work and private life are increasingly blended
- If you live in emerging economies, **protect your cash** by sending it to your family via your mobile phone

Example: Network security has become top-of-mind issue for enterprises and banks

Computer Crime & Security Survey [1]
"Most Critical Issues for 2007/2008"

Top Issues	*# of Response**
Data protection & application software vulnerability security	73
Policy & regulatory compliance	63
ID theft and leakage of private info	58
Virus & Worms	52
Management involvement, risk management or supportive resources	47
Access Control	43
User education, training, and awareness	43
Wireless infrastructure security	41
Internal network security	38

Worldwide Banks' 2007
Top 10 Strategic Initiatives [2]

Rank	*Initiatives*
1.	Security / fraud
2.	Payment disruption / convergence
3.	Customer-centricity initiatives
4.	Risk management
5.	Compliance
6.	Core banking
7.	Channel investment
8.	Enterprise infrastructure integration and sourcing
9.	Profitability and performance management
10.	Integrated financial supply chain

(1) CSI/FBI 2006, Annual Computer Crime & Security Survey; (2) Financial Insights, an IDC company, #FIN205373, Feb 2007
* Based on 426 respondents, from CSI survey of 616 computer security practitioners in the US

Example: the future of Healthcare and security

Q:" What are your organization's key benefits and challenges in wireless technologies?"

Key Mobility Benefits	Key Mobility Challenges
▪ Reduced Manual Errors	▪ **Security and Privacy concerns**
▪ Increased order fulfillment accuracy	▪ Cost of Hardware
▪ Increased employee productivity efficuency	▪ Cost of Software, integration, service and support
▪ Increased compliance accuracy for quality reporting	▪ Difficulties integrating mobile apps, existing infrastructure
▪ Regulatory and /or industry compliance.	▪ Interference/Performance problems

Security concerns topped the list for 42 % of healthcare decision-makers in North America, in EMEA, and in APAC

Source: Motorola Healthcare Barometer Survey April 2009 -3500 IT Decision Makers from across 14 countries and 4 continents

There is a need to offer solutions that provide a safe and simple user experience

Digital security protects and enhances digital interactions

Digital security is concerned with protecting…

- **Digital Identity**: individuals, subscribers, access rights
- **Digital Assets**: information, content, software application
- **Digital Transactions**: payments, data transmission, and access provision

For the benefit of individuals' freedom, by making them…

- **Personal**: unique and private to each individual
- **Convenient**: easy and intuitive with minimum complication
- **Trusted**: effective and reliable

There are many solutions addressing a variety of uses for different groups of buyers: are they fully addressing the needs of increasingly educated digital users?

	Service Providers	(Online) Merchants	IT Departments	Public Administrations	Consumers
Applications	• Subscriber Management • Web Login • Secure Payment • Digital Signature Validation	• Secure Online Payment • Digital Signature Validation • Digital Media Protection	• Identity & Access Management • Data Encryption • Fraud Detection • Antivirus & Content Filtering • Network Firewall & VPN	• Travel Document • Citizen Identity • Healthcare • e-Government Services	• Antivirus • Secure Storage • Media Decryption • Parental Control
Examples of Buyers	• Mobile Network Operators • TV Broadcasters • Internet Service Providers • Financial Institutions • Credit Card Issuers • Online Auction Operators	• Digital Content Provider • e-Commerce Website	• S&P Global 1200 • SMEs • Government Agencies • Educational Institutions	• Governments & National Printers • Federal Agencies & Police • Insurance Organisations	• You, me and our 'in-law's' • Teenagers – the Google Generation

Illustrative - not complete list

Beyond 2010: from application-centric security to user centric security

Digital security: beyond 2010

- In 5 years each of us will carry at least five secure personal devices:
  - In our mobile phone interconnect with multiple networks (telecom, sensors,..)
  - In our wallet with devices and cards for payment, ID, healthcare, driver license, public transport etc
  - In our pockets for physical access to corporate facilities, digital rights management with our digital player/camera, and as our car keys
  - In our suitcase with our passport/ID, connected to our PDA and our PC for network authentication and digital signature
  - In our homes with PayTV decoders, advanced Home Automation etc
  - In our electric cars for traffic control and electricity reloading

- Our belief: the increasing multiplicity of tokens to manage our virtual identities life will eventually lead to the mergence of simpler, user-centric (friendly and controlled) personal credential objects providing trust and privacy to end-users.

Gemalto vision: eGo, when security is me

- Easy UWB pairing between smart objects thanks to Intra-body communication

- A single sign-on based on fingerprint sensor

- **A wearable device containing your personal credentials**

- Delivers user-centric privacy thanks to a trust network controlled by the user

Friendly…

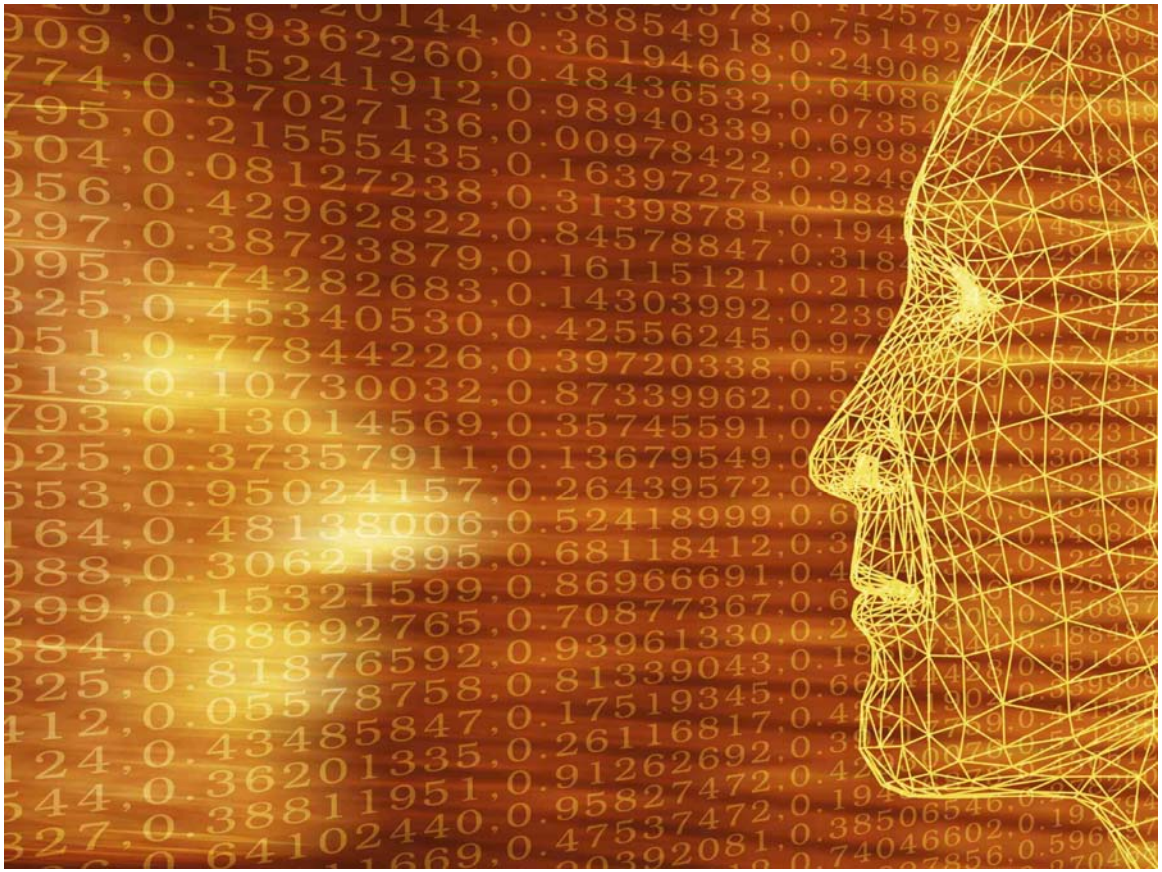
No more user name/password with my eGo belt!

- Pierre has:
  - touched his mouse
  - Worked within his private environment
- Pierre did not need to:
  - Enter a login and a password
  - Insert a card

Safe…

Only my swimming suit , my bath-towel,
and my waterproof eGo watch!

- Eve has:
  - closed her home door
  - Stepped into her car
  - Drove to the beach
  - Purchased a bottle of iced tea
  - Placed a phone call
- Eve did not need to:
  - Be concerned about leaving anything on the beach during her bath



A view on commercial needs around cryptography

Mid-term trends and research opportunities

- Digital security in commercial schemes is a definite need but its successful implementation relies on two factors:
  - Ease-of-use for consumers: example is eGo, Crypto-biometry
  - Performance (speed, reliability): example deploying PKI transactions in a mass transit scenario [ALIKE protocol]

- We believe, as Gemalto, about the importance of the paradox between empowering end-users for privacy while allowing legitimate authorities to exploit usage data
  - Generalization of public key based commercial systems
  - Need for anonymization and privacy preserving protocols around core digital concepts such as e-money, e-voting, e-services by government and industry.
  - Need for security framework for personal, enterprise and state data on public cloud infrastructure

Conclusion

- The World is becoming digital, there is no turning back
- The relevance of the digital World to people and enterprises in developed and emerging economies is now attracting high risks on privacy and digital identity attacks
- By 2020, each user will experience an exponential need of digital identities in a fully networked physical and virtual World.
- We predict the need for a user-centric management of credential ensuring privacy while fighting digital identity theft
- User-friendliness of user authentication as well advances in efficient privacy-preserving cryptography protocols are key to the adoption of such visionary framework by users, enterprises and public institutions