euro cacs℠

ISACA®
Serving IT Governance Professionals

"I will work in concert with my peers."

PKI – Achieving Business Benefits Through Large-Scale Integration

Carlo Harpes

Steve Purser

March 2007

Objectives

- Explain what is PKI
- Examine the reasons behind deploying PKI.
- Present a step by step approach to prepare a PKI project…
  - looking at key questions driving the requirements.
  - presenting arguments for in-house and outsourcing.
  - showing how to build a business case for a strategic approach.
  - discussing how to identify and involve stakeholders.
  - presenting the strategic roadmap.
- Help you to learn from others and put the right focus.

Agenda

- Introduction
  - Background on Luxtrust
  - What are we trying to achieve?
  - What is PKI?
- Key steps in implementing PKI
  - Building the Business Case.
  - Defining the Strategic Roadmap.
  - Considering implementation issues and problems
- Lessons learned
  - Summary
  - The right focus

Background on Luxtrust S.A.

– 2000: Luxtrust – ABBL

- Business Case study by PWC for banks,
- Draft dig. signature and e-commerce law

2001: Luxtrust – banking sector projet (2001)

- Cost and technical architecture evaluation for pilot

2003: Luxtrust GIE: Government joining (2/3 of part)

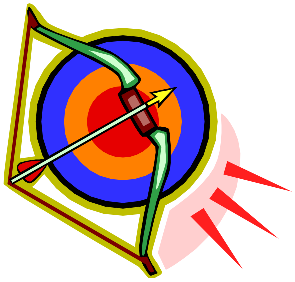
- RFP to complete study behond pilot
- Full business plan
- Study by Certipost

2005: founding Luxtrust S.A. (Government: 2/3 of parts)

- 2006: RFP to Certification service providers (in Lux)
- 2007: Activity start (e-passport since 9/2006)
- Server certificates, Smart cards,
- advanced signature based on signing server

What are we trying to achieve ?

- In order to decide whether or not we have been successful in making the most of PKI, we need to be clear about our goals.
- As with any security-related technology, we deploy PKI to mitigate certain risks.
- It is critically important to realise that PKI and authentication are not the same thing. In particular, they do not mitigate the same risks.
- PKI mitigates a highly-specific risk in a particular domain.



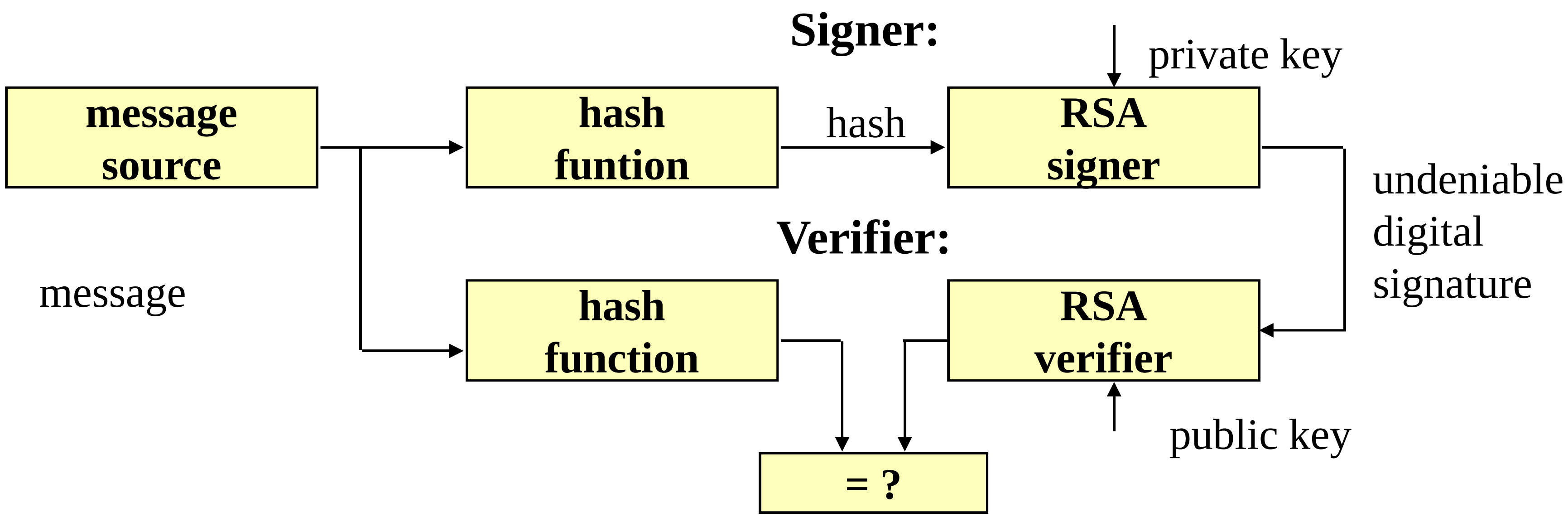
What is PKI?

PKI (Public Key ***Infrastructure***), cf. ISO 15945: 2002

The system consisting of TTPs, together with the services they make available to support the application (including generation and validation) of digital signatures, and of the persons or technical components, who use these services.

NOTE – Sometimes the persons and the technical components participating in a PKI, by using the services of TTPs, but not being TTPs themselves, are referred to as end entities. An example of a technical equipment used by an end entity is a smartcard which may be used as a storage and/or processing device.

What is Public Key Cryptography?



Signer:

private key

message source

hash funtion

hash

RSA signer

undeniable digital signature

Verifier:

message

hash function

RSA verifier

public key

= ?

RSA is the most used Public Key Algorithm
Private and Public keys are linked

Core Problem of Public Key Systems

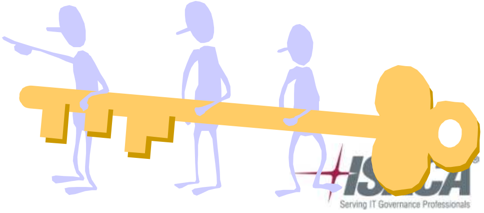
How does a Verifier know that the Public Key used for verification really belongs to the expected person ???

Solution:

He trusts an Authority that provides this assurance.

Thus:

We need not only Crypto, but an *infrastructure* to provide this trust.



What is PKI?

PKI Components

1) Certification Authority (CA)

- Create certificates (signer’s Identity+Public Key, signed by CA)
- Links Signer and Verifiers
- Defines usage rules
- Distributes certificates and certificate status (LDAP, OCSP)
- Revokes certificates (CRL management) (24/24 service)

3) Registration Authority (RA)

- Physical verification of signer
- Keep records of signer identity
- Sents Certificate Request to CA
- Delivers certificate and Key token (chip card)

What is PKI?

PKI Components

…

3) Security Policies

- Laws and regulations
- Certificate Policy (CP)
- Certificate Practice Statement (CPS)
- Certificate hierarchy, cross-certification

4) PKI-enabled Applications

5) Private Signing Environment

- Files, chip cards, Secured PC, Signing terminals, etc

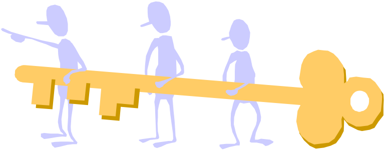
What PKI Doesn’t Do

- Most organisations need to do business over third-party networks, often with counter-parties that they have never met. Customer will not come because you have a PKI.
- Network security services are used to protect business transactions over potentially hostile networks.
  - PKI is not necessary to implement cryptographic security services – this is the role of cryptography.

Some Other Problems ….

- The fact that we can be sure that we are in communication with Mr. Muller of Austria tells us nothing about the character of Mr. Muller!
- If Mr. Muller signs a message and does not honour his obligations, the legal system may not recognise the importance of digital signatures.
- In the area of code signing, this type of problem was demonstrated by the ActiveX Exploder control.

Trust is more than
just authentication



What PKI Does Do

- PKI provides a trust framework to support network security services using public-key cryptography.
- When correctly implemented, PKI resolves the core problem of public-key systems.
- PKI MAY resolve other issues too.
  - The registration process may allow us to place more trust in Mr. Muller – It all depends on what checks are carried out.
  - PKI often facilitates standardisation and can bring economies of scale.

Agenda

- Introduction
  - What are we trying to achieve?
  - What is PKI?
- Key steps in implementing PKI
  - Building the Business Case.
  - Defining the Strategic Roadmap.
  - Considering implementation issues and problems.
- Lessons learned
  - Summary
  - The right focus

Key Steps in Implementing PKI

1. Understand the risks and opportunities.
2. Verify the requirement.
3. Look at outsourcing versus in-house.
4. Build the business case.
5. Get the buy-in of the business.
6. Produce a strategic roadmap.
7. Identify key implementation issues and problems.
8. Plan – Do – Check – Act.

1) Understanding Risks&Opportunities

- The decision to implement any new technology should be based on a thorough understanding of both opportunity and risk.
- This is not easy for a technology such as PKI, which is a support technology.
- The opportunities associated with PKI itself are more likely to be realised in the long-term.
- However, the risks of using PKI are both short-term and long-term.
- PKI is therefore clearly a *strategic initiative*.

Opportunities & Risks

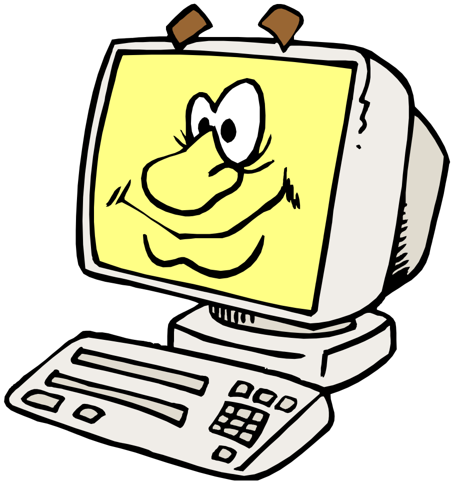
- Example Opportunities
- Establishes a formal trust framework.
- Enables Internet-facing applications.
- Can be used to standardise and decrease time to market for new applications.
- Can be used to achieve economies of scale.
- It may be possible to use PKI as a revenue generator.

- Example Risks
- Might prove to be too costly.
- If applications are PKI-enabled, maintenance might be problematic.
- It can be difficult to maintain the required skill-sets.
- May ultimately be too unwieldy for the enterprise.

2) The Requirement (I)

- PKI represents a substantial investment - requirements must be clearly understood and documented.
- In general, requirements will be associated with:
  - Reducing risk exposure.
  - Generating revenue.
  - Decreasing costs.
- Great care needs to be taken when selling PKI on the basis of a pilot project … but this can help gain initial support.

Example Pilot Applications



- Electronic commerce.
- Internet Home Banking.
- Web-based purchasing.
- E-mail .
- Remote access.
- Web publication to selective groups.
- Virtual Private Networks.
- Internal authentication.

2) The Requirement (II)

- Examples of risk reduction include:
  - Reducing claims through non-repudiation.
  - Using PKI as a driver to standardise cryptographic services (reduced risk through simplification).
- Examples of revenue generation include:
  - Selling PKI services to third parties.
  - Commercialising PKI-enableds applications.
- Examples of cost-cutting include:
  - Reducing administration costs through economies of scale.

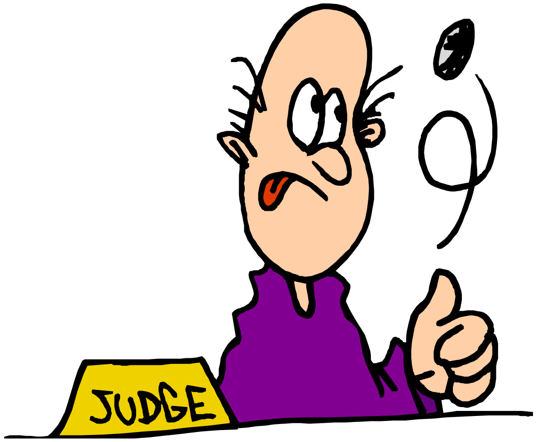
3) In-House versus Outsourcing (I)

- In-House
- More direct control.
- High administration overhead.
- Possibility to charge for the service.
- Extensive infrastructure requirements.
- Liability has to be assumed internally.

- Outsourcing
- Less direct control.
- Low administration overhead, but this service must be paid for !
- Unlikely to be offered as a chargeable service to clients.
- Infrastructure responsibility of service provider.
- PKI provider may offer some degree of liability protection.
- Dependency

3) In-House versus Outsourcing (II)

- In general, smaller institutions or institutions deploying applications associated with a lower level of risk should consider outsourcing.
  - This may not be possible for legal or regulatory reasons.
- Whilst outsourcing is still an option for high-risk applications, there are several issues to take into consideration:
  - Liability in the event of an incident.
  - Commercial stability of service supplier.
  - Impact on reputation.



3) In-house & Outsourcing Pitfalls

- There was more focus on the technology than on the risks we were seeking to mitigate.
- PKI was seen as a prestigious technology and too many organisations opted for in-house development.
- Ongoing support requirements were often greatly under-estimated.

4) Building the Business Case (I)

- The business case for PKI will reflect the opportunities and risks we have identified.
- As with the requirements, costs and benefits can be classified in three areas
  - Reduction in risk,
  - revenue generation and
  - decreased costs
- For most organisations, a business case built on revenue generation s unlikely - the revenue stream would have to offset considerable investment.

4) Building the Business Case (II)

- Major Costs
  - Consultancy fees. ☹
    - Development of procedures and documentation.
    - Development of legal documents.
  - Hardware and software. ☹
    - PKI core components.
    - Optional components.
  - Staff costs. ☹
    - Ongoing administration costs.
    - Enabling applications to use the PKI infrastructure.
  - Insurance and liability cover. ☹

4) Building the Business Case (III)

- Major benefits
  - Reduction in risk.
    - Commercial grade cryptography.
    - Clearly defined roles and responsibilities.
    - Strong contractual framework.
  - Increased control.
    - Standardisation of procedures.
    - Simplification of underlying mechanisms.
  - Scalability.
    - Public-key systems scale better than symmetric-key systems.

4) … Using ROI Calculations

- Evaluating the ROI will require quantifying the risk.
- Quantitative risk calculations may be dangerous since they depend on rough estimate.
  - However, the calculation only needs to be accurate enough to support the decision.
  - Common sense examples and approximate calculations can be very convincing.
- Certain risks are hard to evaluate (e.g. loss of market image). Here, it may be acceptable to use a qualitative argument.

4) … ROI Calculation Example

Investment:		k€	
Software costs	=	500	
Hardware costs	=	400	
Yearly maintenance costs * 5	=	900	
Staff & service provider costs	=	700	
			2 500
Generated revenue	=	0	(nothing sold)
Generated cost savings :			
Efficiency gain of 3 administrators	=	2 310	
Savings due to electronic registration process	=	2 500	
Added Value:			
Direct cost of customer incidents	=	5 650	
Indirect cost (loss of customer)	=	40 000	

Based on but highly conservative estimate of impact on customer base.

ROI = (0 + 4 810 – (– 45 650)) / 2500 = 20,18

4) Business Cases – Pitfalls

- For many companies, PKI was justified by the pilot project.
  - The vision stopped at the pilot project, which meant that the long-term benefits were neither foreseen nor realised.
  - In particular, the lack of a strategy made it difficult to build on the initial implementation.
- Running costs and operational complexity were often underestimated.
- Choosing PKI as a technical solution (tactical aspects) without considering business benefits (strategic aspects).
- Many organisations thought that they would be able to sell trust services (as side effect)
  - Customers want secure applications.

5) Involving Stakeholders

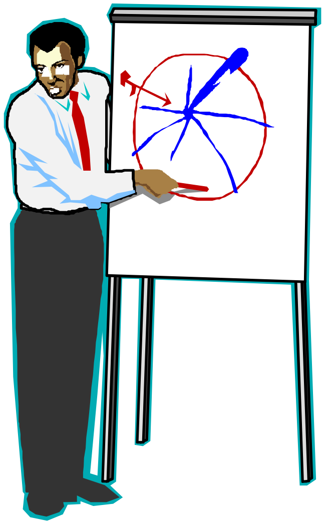
- Who are the stakeholders?
  - Primarily the business lines, but also…..
  - Risk management/Audit.
  - The legal department.
  - IT Production and infrastructure teams.
  - IT Development teams.
- The pilot project is used to get the stakeholders on board, but the strategic approach should be clear from the start.

5) Involving Stakeholders (II)

- Avoid bombarding the business with technical details. Concentrate on alternatives.
- Obtain the product roadmap and aim to influence products within the near future.
- Avoid trying to retrofit legacy systems unless this is absolutely necessary.
- The development teams are key players. It is important to introduce toolkits and development aids at an early stage.

6) The Strategic Roadmap (I)

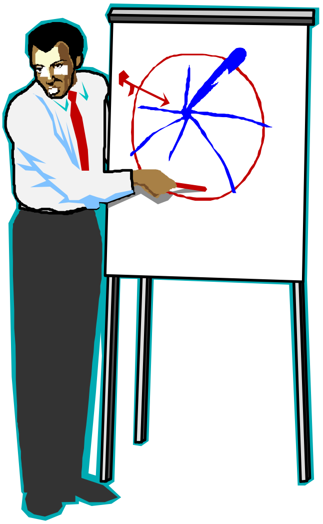
- It is essential to plan for a widespread usage from the beginning.
- Consider defining a phased approach, with specific goals for each phase, for example:
  - Phase 1 – Secure Web Access (pilot).
  - Phase 2 – Customer-facing applications …



- Prioritise key applications, but don't ignore quick wins – these buy credibility.
- Look for third party products, which are PKI-enabled.

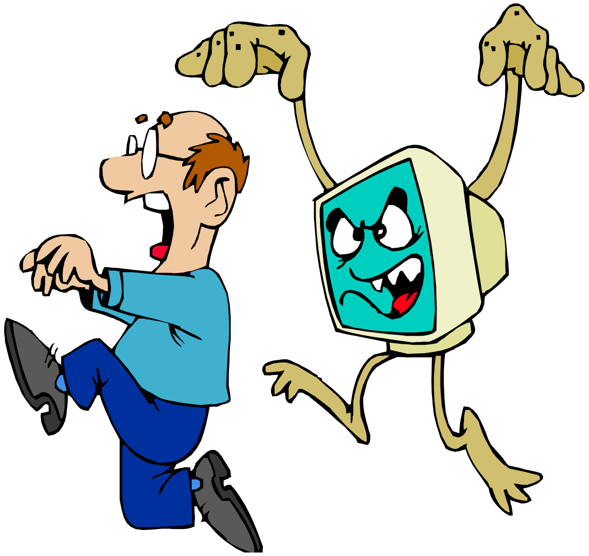
6) The Strategic Roadmap (II)

- ROI will be gradual, but must be predictable.
- The strategic roadmap provides the major milestones in PKI deployment.
  - Deployment of core system.
  - Enabling of key applications.
- Consider using an architectural approach.
  - If deployed, PKI should be a key component of the Security Architecture.
  - The latter offers security services to other security components, applications and middleware.



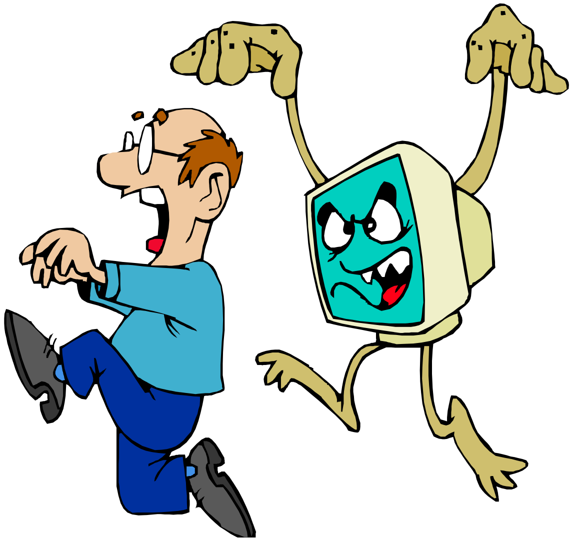
7) Typical Issues & Problems (I)

- Interpretation of certificates
  - Legacy applications do not recognise certificates. Those which do recognise certificates do not always do so in a standard fashion.
  - Many applications do not recognise certificate extensions.
- Standards
  - There are many standards, but they are not all based on the same principles - It is important to adopt a coherent group of standards.



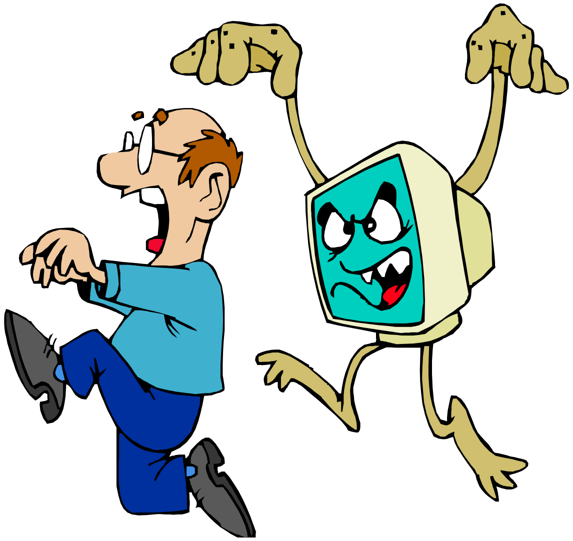
7) Typical Issues & Problems (II)

- Compatibility of commercial products
  - Many of the existing products on the market do not inter-operate with each other or with existing software.
- Support for Tamper Resistant Equipment
  - Integrating TRE is complex and time-consuming.
  - Support for memory cards is relatively advanced, but expect to work hard to implement more sophisticated Smart Card features.



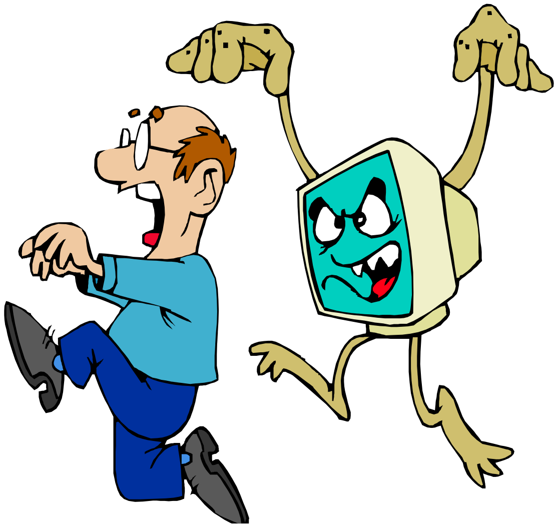
7) Typical Issues & Problems (III)

- Current revocation models may not be able to support B2B requirements.
  - The OCSP Protocol is a notable exception.
- Initial user acceptance may be difficult to obtain.
  - There is often a local installation to be carried out and initially, the user may have more passwords to remember!
  - There may be opposition to signing usage agreements.
  - User awareness training should begin at an early phase.



7) Typical Issues & Problems (IV)

- PKI expertise is expensive and difficult to find.
  - Highly paid external service providers may be seen as a threat to core team members.
  - Transfer of skills is important.
- Ongoing administration needs to be planned well in advance.
  - PKI administration is not trivial.
  - Administrators:
    - Are customer-facing
    - Need to be trained
    - Need to understand PKI



7) … Pitfalls

- In many cases, complexity proved to be a problem.
  - For instance, developing code to exploit a PKCS#11 interface is not trivial.
- In many cases, end users were not sufficiently prepared for the impact of PKI.
  - Users often have to take responsibility for their key pair.
  - Smart cards are secure, but they require both a modification of the workstation and a change in the users behaviour.

7) … Pitfalls

- Implementations too technically focussed.
  - PKI is about technology and procedures.
  - The latter require a lot of thought and can be quite onerous.
  - Logistics can have an important impact on the project’s success – e.g. distribution of out-of-band secrets.
  - Training requirements were often underestimated.
  - Liability is an important issue in any system that implements a trust framework

8) Plan-Do-Check-Act

- Prepare a project plan
- Implementation & test
  - Requirement for development and test environments.
- Rollout
  - Users need to be trained.
  - Special equipment may be required.
  - Help Desk and technical support may be required.
- Administration
  - Estimate and plan for increased administration effort.
  - Probable requirement for backup and on-call support.

Agenda

- Introduction
  - What are we trying to achieve?
  - What is PKI?
- Key steps in implementing PKI
  - Building the Business Case.
  - Defining the Strategic Roadmap.
  - Considering implementation issues and problems
- Lessons learned
  - Summary
  - The right focus

Summary of Lessons Learned (I)

- Solutions should be determined from a careful consideration of opportunity and risk.
  - – PKI is yet another example of the technology trap.
  - – Many organisations got caught up in the media hype and vendor push.
- It is critical to distinguish between tactical and strategic requirements.
  - – Many organisations deployed PKI to satisfy a tactical requirement.
  - – It is very difficult to achieve a reasonable ROI from a tactical deployment.

Summary of Lessons Learned (II)

- PKI has a relatively high initial deployment cost, but the real costs are the operating costs.
  - The business case should correctly reflect all costs.
  - It must be possible to clearly demonstrate that the benefits outweigh the costs in the long term.
- By aiming for a high level of integration, we achieve a number of benefits:
  - Economies of scale.
  - Standardisation.
  - Increased speed and efficiency.

Summary of Lessons Learned (III)

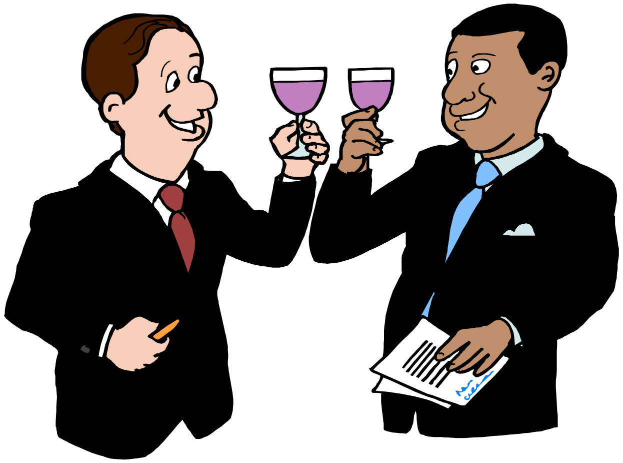
- In order to achieve this high level of integration, we need a strategic approach.
  - The strategy needs to be clear from the start.
  - All important stakeholders should be identified and prepared in advance.
- Implementation should not be too technically focussed.
  - Real security involves tools & procedures.
  - Projects should give equal weight to both aspects.

Summary of Lessons Learned (IV)

- End users need to be prepared for change.
  - This requires time – it can’t be an afterthought.
  - Don’t make assumptions about the behaviour of the user – ask wherever possible.
- Staff need to be trained.
  - It is important to ensure that skills are transferred from service providers to core staff.
  - There will be a need for regular training to keep these skills up to date.

The Right Focus

- Our major aim is to achieve the right level of residual risk – everything else is secondary.
- Only we can judge what the right level is.
  - Where security-related risk is concerned, we're all individuals.
- If we do this correctly, the business case should speak for itself.
  - Risk must be included.
  - If we can't produce a convincing business case, why are we doing the project?



The Right Focus

From all 5 PKI components, focus on …

The Right Focus

From all 5 PKI components, focus on

the PKI-enabled **Applications** & Services

About the Authors

Carlo Harpes is

- Senior Security Consultant
- Founder of itrust consulting s.à r.l.
- Associated Assistant Prof. at Univ. of Luxembourg
- Founder and board member of CLUSSIL and ANSIL

Steve Purser is

- Director ICSD Cross-Border Security Design and Administration
  Clearstream Services, Luxembourg.
- Founder of CLUSSIL
- Author of “A Practical Guide to Managing Information Security” (Artech House, 2004).

PKI – Achieving Business Benefits Through Large-Scale Integration

Thank you for your attention

harpes@vox.lu

stephen.purser@clearstream.com